TEES

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

19th Annual International Symposium
October 25-27, 2016 • College Station, Texas

A Framework for Identification of Lessons Learned from Offshore Operational Data Using Barriers and Success Paths

William R. Nelson
DNV GL
1400 Ravello Dr.
Katy, Texas 77449
Presenter E-mail: bill.nelson@dnvgl.com

Abstract

One of the most pressing challenges facing the offshore industry today is the effective interpretation, decision making, and action identification using the large volumes of operational data that are being collected and stored. Offshore operators, drilling contractors, and third party suppliers have developed real time operations centers designed to support offshore operations. The Bureau of Safety and Environmental Enforcement (BSEE) has proposed requirements for the collection of offshore real time monitoring data, but how such data will be used to support regulatory decision making is not yet clear. Operating companies and original equipment manufacturers are designing and implementing new equipment with a very high degree of instrumentation and advanced diagnostics capabilities, leading to new sources of operational data that could be analyzed to further enhance reliability, reduce downtime, and increase safety.

The potential benefits to be realized from the collection and interpretation of such volumes of operational data are substantial. Individual organizations are already using the data to provide remote decision support for offshore operations as well as off-line analysis to enhance equipment reliability and plan maintenance activities. At a higher level, the potential benefits of analysis and interpretation of large volumes of operational data across organizational boundaries and at the industry level have been recognized but not yet realized. There has been much discussion regarding the promise of "big data analytics" to address these industry-level issues, but practical solutions are not yet available to deliver on the promises. However, a number of promising initiatives are underway. For example, the Society of Petroleum Engineers (SPE) and BSEE have initiated collaborative efforts to assess the processes, tools, and value of sharing and learning from offshore safety related data.

A critical component that must be developed for effective utilization of operational data at the industry level is a framework for interpreting operation experience that will protect data confidentiality while allowing consistent interpretation and identification of lessons learned. Such

a framework could support consistent application to identify lessons learned across discipline and organizational boundaries and the development of a "common language" for communication and consensus for action amongst industry and regulatory organizations.

DNV GL has developed a framework for interpreting operational data that is built on a combination of barriers and success paths. Using this approach, data from operational incidents can be interpreted in light of the effects on barrier health and the utilization of effective success paths for responding to degraded or failed barriers. The approach is built upon experience gained in interpretation of aviation incidents in the NASA Aviation Safety Reporting System (ASRS), identification of lessons learned from incidents and accidents in nuclear power plants, and assessment of lessons learned from major pipeline leak accidents. The approach is currently being used in a project with an offshore operator and a drilling contractor to support development of diagnostic algorithms and regulatory compliance assessment for new well control equipment and procedures for deepwater drilling. A unique feature of this application is the utilization of the barrier-success path framework to form the foundation of a common language for regulatory approval of the new equipment and procedures, as well as continuous regulatory compliance assessment during operations. The development process includes proactive interaction with regulatory personnel to identify pre-defined decision criteria and communication protocols for continuous compliance assessment during operation.

This paper summarizes experience gained in application of the barrier-success path approach for identification of lessons learned from operational experience in the commercial aviation, nuclear and pipeline industries and current developments for design of diagnostics and compliance assessment for deepwater drilling. The paper also summarizes the potential benefits for broader application of the approach for interpretation of operational data to support communication, decision making, and consensus for action across the industry including offshore operators, industry groups, regulatory authorities, and external stakeholders.

Summary of the Barrier-Success Path Approach and Application to Deepwater Offshore Drilling

The DNV GL barrier-success path approach 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 and interpretation of operational experience can be realized. The same framework that is used for organizing information needed to manage barriers and success paths during operation can also be used to interpret operational experience and incident reports.

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 1 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.

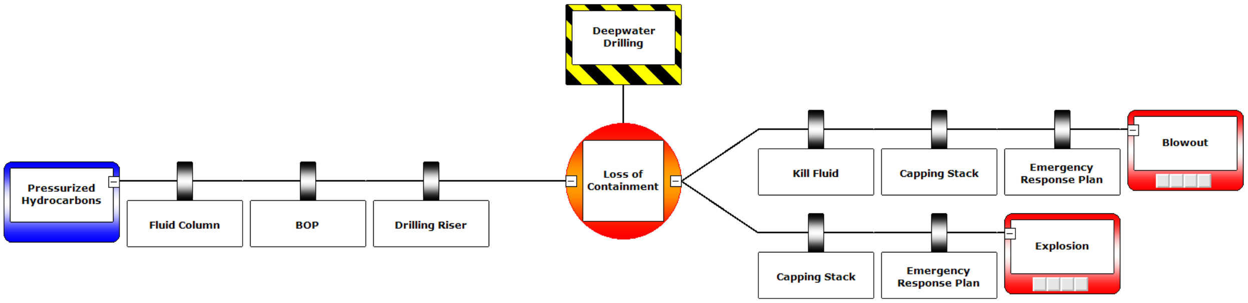


Figure 1. Bow tie diagram for deepwater drilling

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 2 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 shown in Figure 2 has been 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.

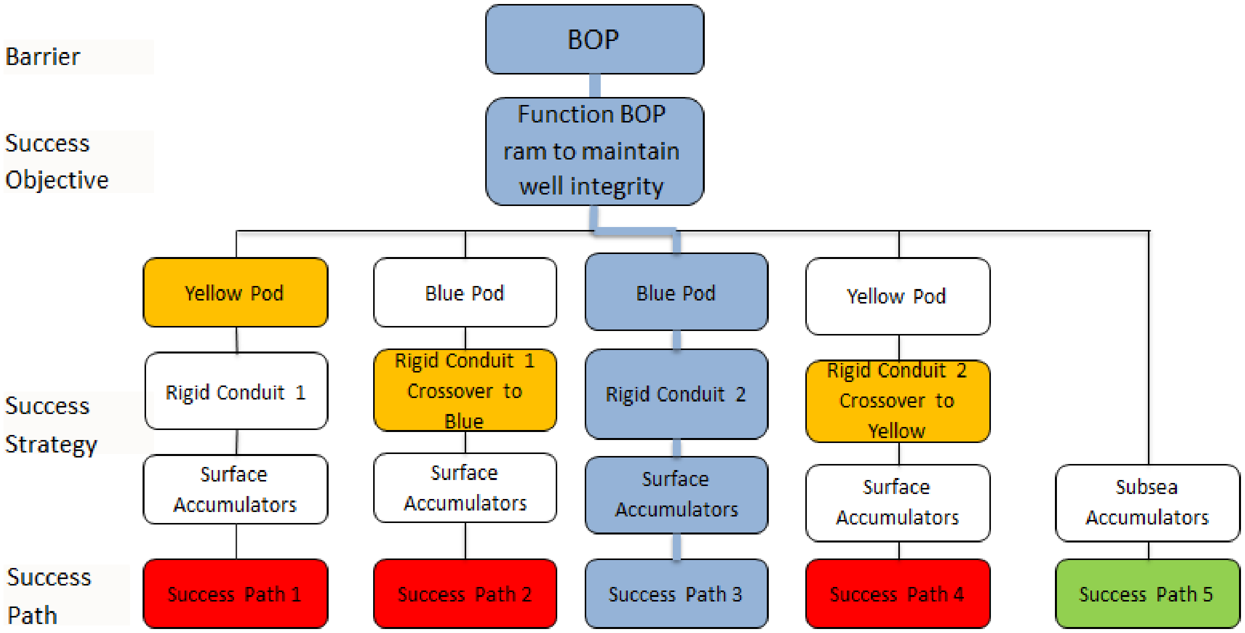


Figure 2. Response tree for the blowout preventer barrier for well integrity

Figure 3 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.

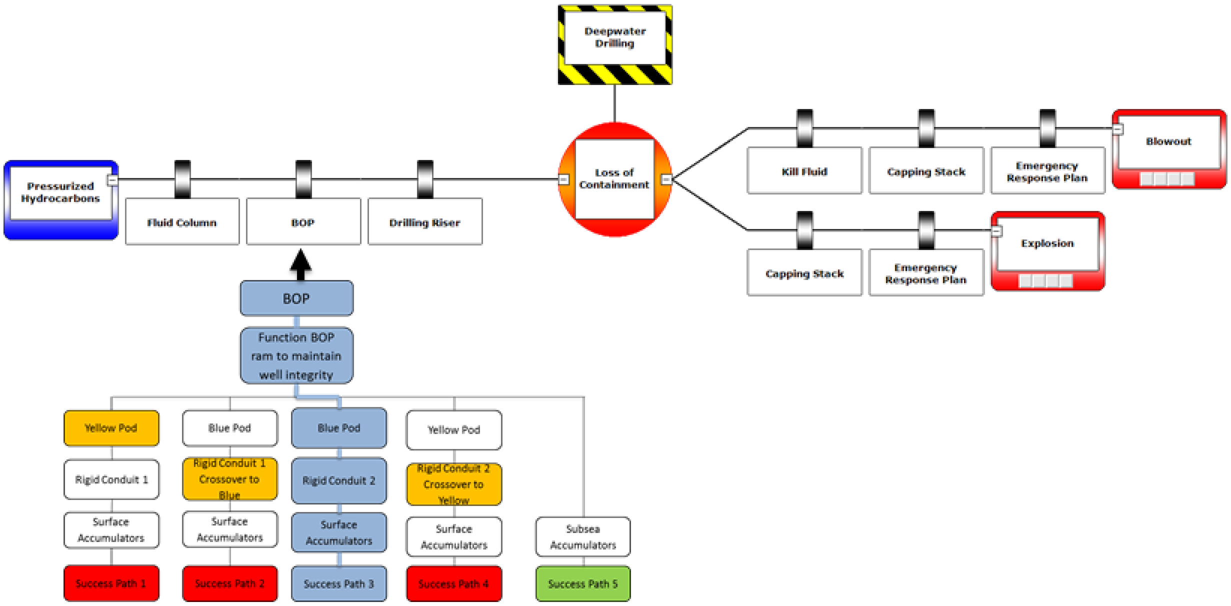


Figure 3. Combining bow tie diagrams and response trees for decision support for dynamic barrier management

Application of the Barrier-Success Path Approach to Identify Lessons Learned and Identify Corrective Actions for Incidents and Accidents

Since the early 1990's different versions of the barrier-success path approach have been used to organize information gained from the systematic review of accidents and incidents, to identify lessons learned and develop corrective actions. This approach has been applied in studies for commercial aviation, commercial nuclear power plants, and pipeline operations. These applications are summarized in the following sections.

Application to Altitude Deviation Incidents in Commercial Aviation

A study was performed by the Idaho National Engineering Laboratory (INEL) for the National Aeronautics and Space Administration (NASA) that used an early version of the barrier-success path approach to characterize pilot errors in advanced technology aircraft [3]. Both sequential event-based (barrier) and function-based (success path) perspectives were used to characterize the context in which the errors occurred. The focus of the study was to characterize pilot errors that occur when using automated cockpit systems. The particular errors that were analyzed were altitude deviations, that is, the failure to capture or maintain the altitude assigned by air traffic control. The sequential models of the pilot tasks were used to identify where in the sequence of prescribed tasks the error occurred. The functional models were used to identify the overall functional context in which the errors occurred, and whether the errors were due to inappropriate attention to functions other than those that were critical for the situation. The activities used to perform the analysis are described in the following sections.

Development of Task Models.

Models of the tasks that are performed to capture and maintain altitude in "glass cockpit" aircraft were developed. In order to provide a more complete picture of altitude deviation errors, two complementary perspectives were used, based on different approaches to the modeling of human error. The first, called the sequential model, was designed to show the prescribed sequence of actions involved in altitude maintenance, and the points at which errors can occur. The technique that was used to show the sequential modeling perspective was the Human Reliability Analysis (HRA) event tree. Two types of logic diagrams: 1) a probabilistic risk assessment (PRA) event tree and, 2) the related HRA event trees were incorporated in this analysis. The PRA event tree depicts a series of events and barriers comprising both human actions and hardware events that may be involved in altitude deviation scenarios. The HRA event trees depict the identified human actions decomposed into their critical subtasks.

The PRA event tree for altitude deviation events is presented in Figure 4. High level descriptions of the human actions and hardware events depicted on the tree are provided in Tables 1 and 2. The event tree depicts twenty-six scenarios representing the possible successes or failures of each barrier representing both human actions and hardware events. At each branch point the path upward represents success of the human action or hardware response, while the downward branch represents failure. Each human action appearing in the PRA event tree and described at a high level in Table 1 was further depicted in an HRA event tree. An example HRA event tree is presented in Figure 5. On this tree the branch to the left represents success of the human action while the path to the right represents failure.

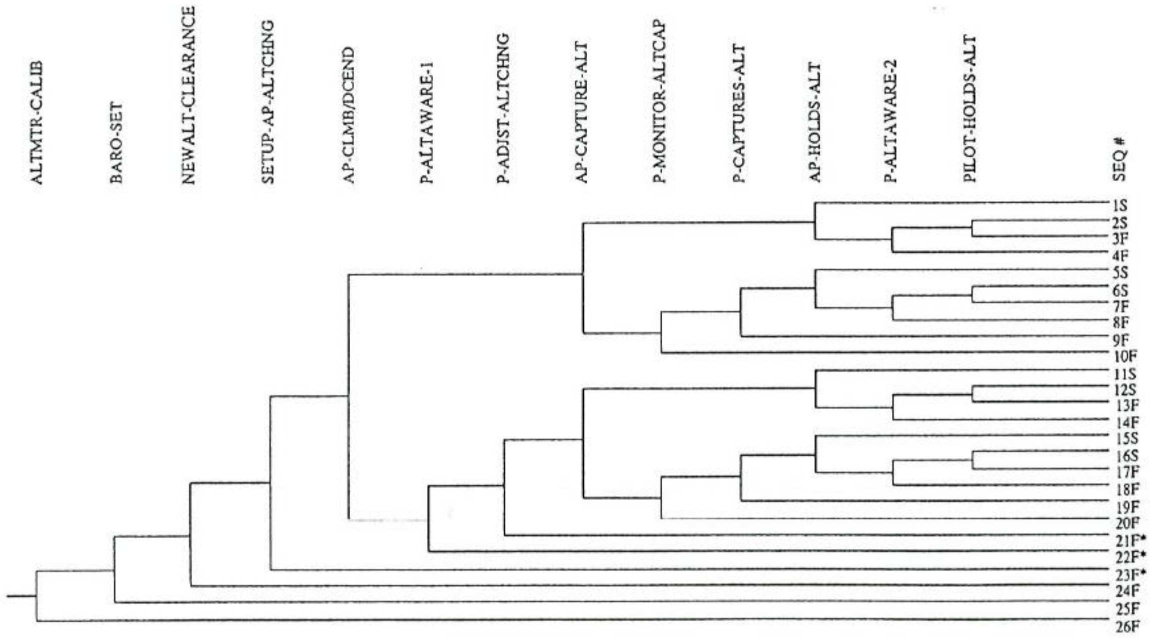
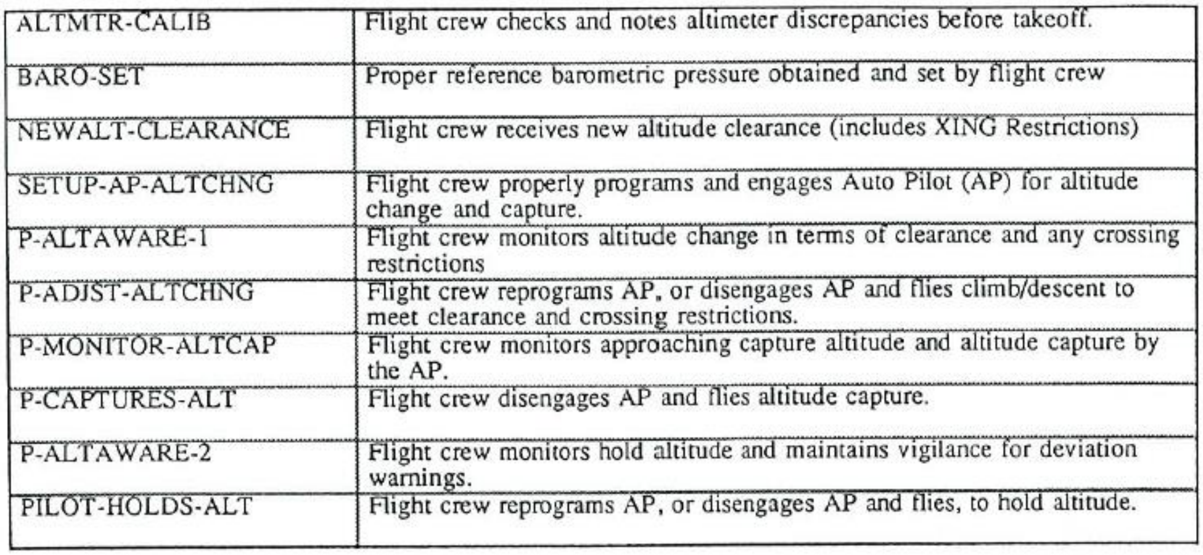


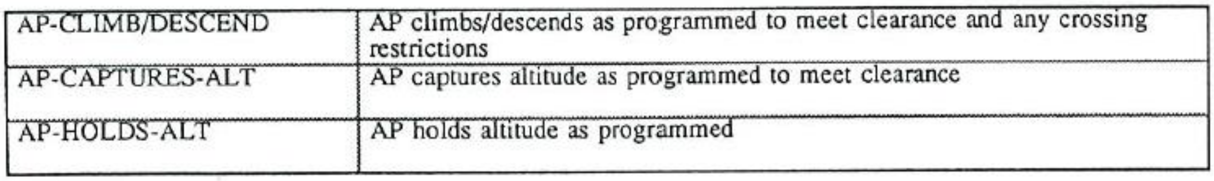
Figure 4. Altitude deviation event tree

Table 1. Human actions on altitude deviation event tree



ALTMTR-CALIB	Flight crew checks and notes altimeter discrepancies before takeoff.
BARO-SET	Proper reference barometric pressure obtained and set by flight crew
NEWALT-CLEARANCE	Flight crew receives new altitude clearance (includes XING Restrictions)
SETUP-AP-ALTCHNG	Flight crew properly programs and engages Auto Pilot (AP) for altitude change and capture.
P-ALTAWARE-1	Flight crew monitors altitude change in terms of clearance and any crossing restrictions
P-ADJST-ALTCHNG	Flight crew reprograms AP, or disengages AP and flies climb/descent to meet clearance and crossing restrictions.
P-MONITOR-ALTCAP	Flight crew monitors approaching capture altitude and altitude capture by the AP.
P-CAPTURES-ALT	Flight crew disengages AP and flies altitude capture.
P-ALTAWARE-2	Flight crew monitors hold altitude and maintains vigilance for deviation warnings.
PILOT-HOLDS-ALT	Flight crew reprograms AP, or disengages AP and flies, to hold altitude.

Table 2. Hardware events on altitude deviation event tree



AP-CLIMB/DESCEND	AP climbs/descends as programmed to meet clearance and any crossing restrictions
AP-CAPTURES-ALT	AP captures altitude as programmed to meet clearance
AP-HOLDS-ALT	AP holds altitude as programmed

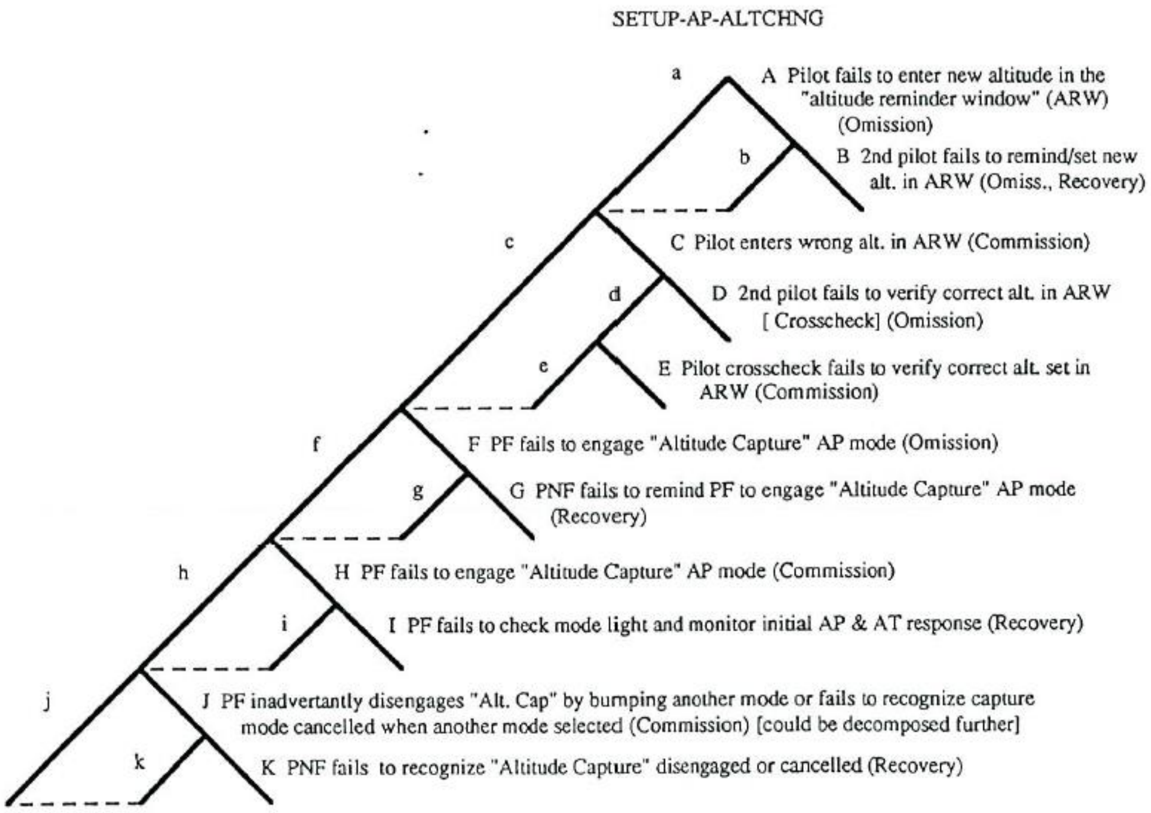

SETUP-AP-ALTCHNG
a
A Pilot fails to enter new altitude in the "altitude reminder window" (ARW) (Omission)
b
B 2nd pilot fails to remind/set new alt. in ARW (Omiss., Recovery)
c
C Pilot enters wrong alt. in ARW (Commission)
d
D 2nd pilot fails to verify correct alt. in ARW [Crosscheck] (Omission)
e
E Pilot crosscheck fails to verify correct alt. set in ARW (Commission)
f
F PF fails to engage "Altitude Capture" AP mode (Omission)
g
G PNF fails to remind PF to engage "Altitude Capture" AP mode (Recovery)
h
H PF fails to engage "Altitude Capture" AP mode (Commission)
i
I PF fails to check mode light and monitor initial AP & AT response (Recovery)
j
J PF inadvertantly disengages "Alt. Cap" by bumping another mode or fails to recognize capture mode cancelled when another mode selected (Commission) [could be decomposed further]
k
K PNF fails to recognize "Altitude Capture" disengaged or cancelled (Recovery)

Figure 2. Setup-AP-Altchng HRA Event Tree.

Figure 5. HRA event tree for altitude change

A functional model provides a complementary perspective to the sequential representation of flight crew tasks. The functional model is a hierarchical structure that starts at the top with an overall objective (for this project the overall objective was to safely complete a flight to a prescribed destination), the critical functions that must be performed to reach the objective, the tasks and subtasks that contribute to the performance of the critical functions, and the resource options (e.g. hardware systems) that are available to the crew for performing the tasks. The kind of hierarchical structures used in this study are called response trees because they graphically display the range of responses that are available to the crew for responding to challenges to the critical functions. Modern transport aircraft are designed so that there is more than one way to perform many of the critical functions, so that safety can be maintained even if certain component failures occur. The different methods for maintaining each critical function are referred to as success paths. Response trees can be exercised manually or by computer to show the effects of different combinations of hardware or human failures, and the options or success paths that remain available to the flight crew for coping with the situation.

The top level functional model that was developed for this project is shown in Figure 6. This model of flight includes six critical functions: Takeoff, Flight Control, Monitor Flight Conditions, Navigation Planning, Monitor Navigation Process, and Landing. Each critical function is broken down into tasks, and the tasks are further broken down into subtasks and the resources needed to perform each of the tasks and/or subtasks.

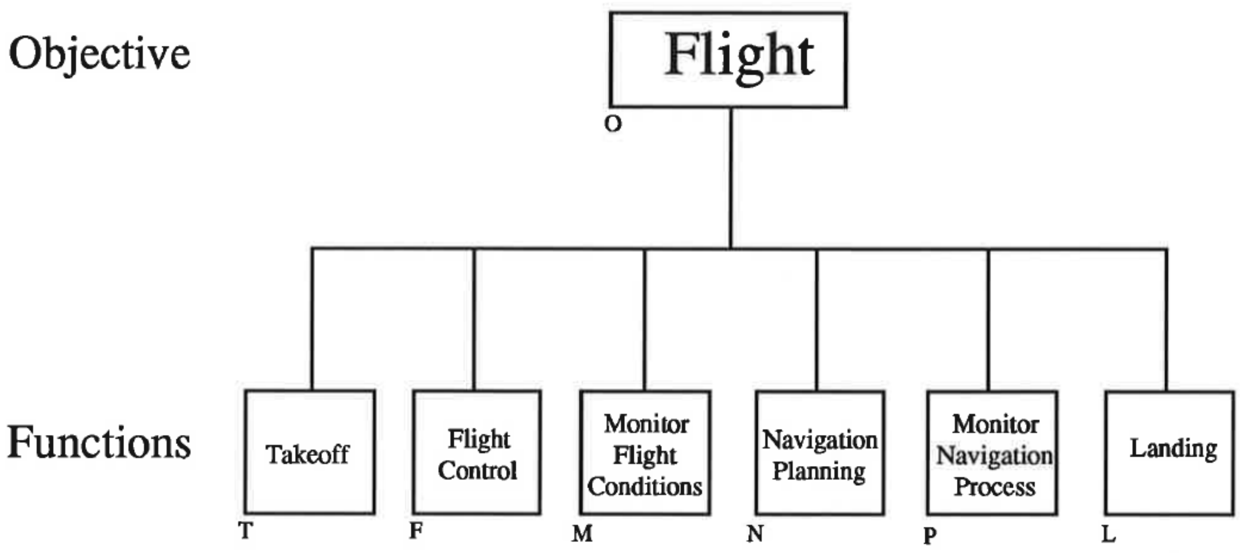


Figure 6. Overview of the functional model for flight

Figure 7 shows the detailed response tree for the Navigation Planning critical function. The response tree shows the tasks and subtasks that are needed to perform the Navigation Planning function, and the success paths or resource options that can be used to perform the tasks and subtasks.

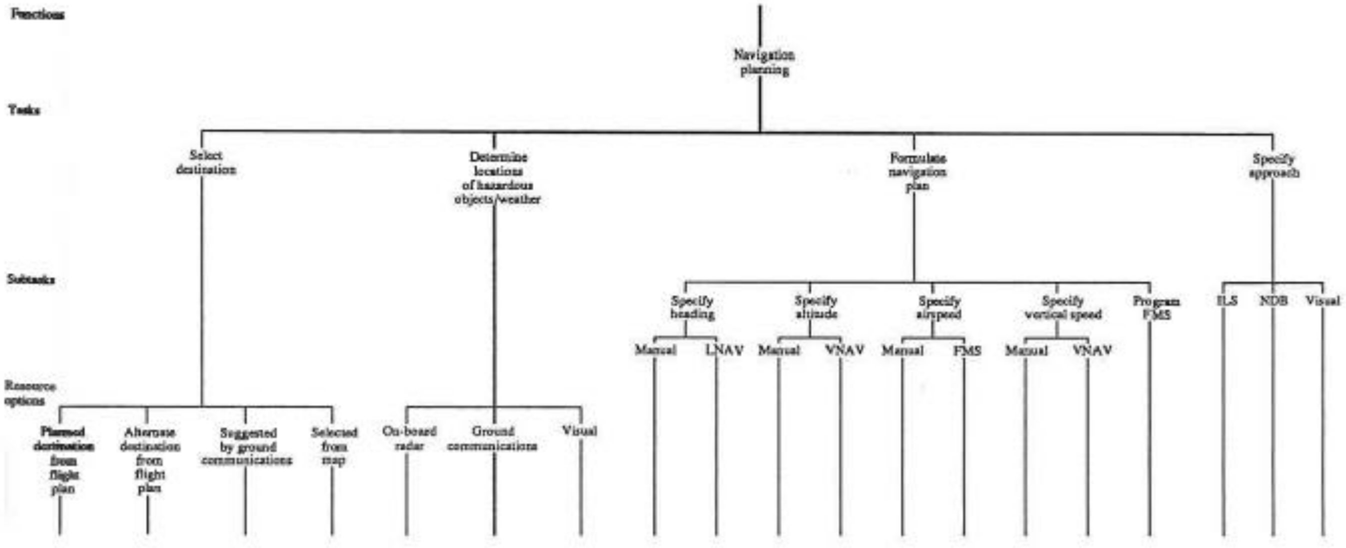


Figure 7. Response tree for the navigation planning critical function

Altitude Deviation Incident Data

The primary source of data used for the study of altitude deviation events was the Aviation Safety Reporting System (ASRS), NASA's third-party reporting system for incidents that occur in flight. The most common type of incident that is reported to the ASRS is altitude deviations, so the ASRS is a rich source of data regarding actual events.

Coding of ASRS reports

Two hundred Aviation Safety Reporting System reports were reviewed. These reports were generated by a search of the ASRS database for reports that referenced Advanced Glass Cockpit Altitude Deviations. The reports were drawn from full-form records and describe altitude deviations that occurred between April 1991 and January 1992. These ASRS reports were subjected to an initial screening to identify those where the advanced technology (e.g. autopilot, flight management system, etc.) actually played a role in the incident. Then, the remaining reports were “mapped onto” the sequential and functional models to allow consistent interpretation. Mapping of the ASRS report onto the sequential model highlighted the location in the sequence of actions where the error occurred, whether available recovery paths were used, and what interventions could have been used to prevent such errors. Mapping of the ASRS reports onto the functional model highlighted the context in which the error occurred, and whether inappropriate attention to other critical functions contributed to the occurrence of the error.

Identification of error categories.

The coded reports were next plotted on both the sequential and functional models to see whether any patterns emerged. The intent was to note whether the reports tended to cluster in certain areas of the functional and sequential models, or if the coded reports represented all areas of the models. These groupings were then examined to note where in the process of achieving and maintaining altitude the errors occurred. For purposes of this inspection and for visual presentation, the errors were mapped onto depictions of both models. The sample of ASRS reports analyzed for this study was relatively small, and not necessarily representative of the entire spectrum of errors that can lead to altitude deviations. Probably even more important are the contextual insights gained by examining the different error categories in the situational contexts in which they occurred.

Callbacks

The next step in the analysis was to perform callbacks on selected reports. Callbacks are the process by which ASRS personnel contact the individuals who submitted ASRS reports in order to obtain additional information about the circumstances of the specific incidents. An important feature of the approach was the use of the models to formulate specific questions targeted at the individual ASRS reports. This allowed reviewers to focus the callback to elicit information so that each specific report could be interpreted in context. The callback process was used in this study to further examine the effectiveness of the sequential and functional modeling tools.

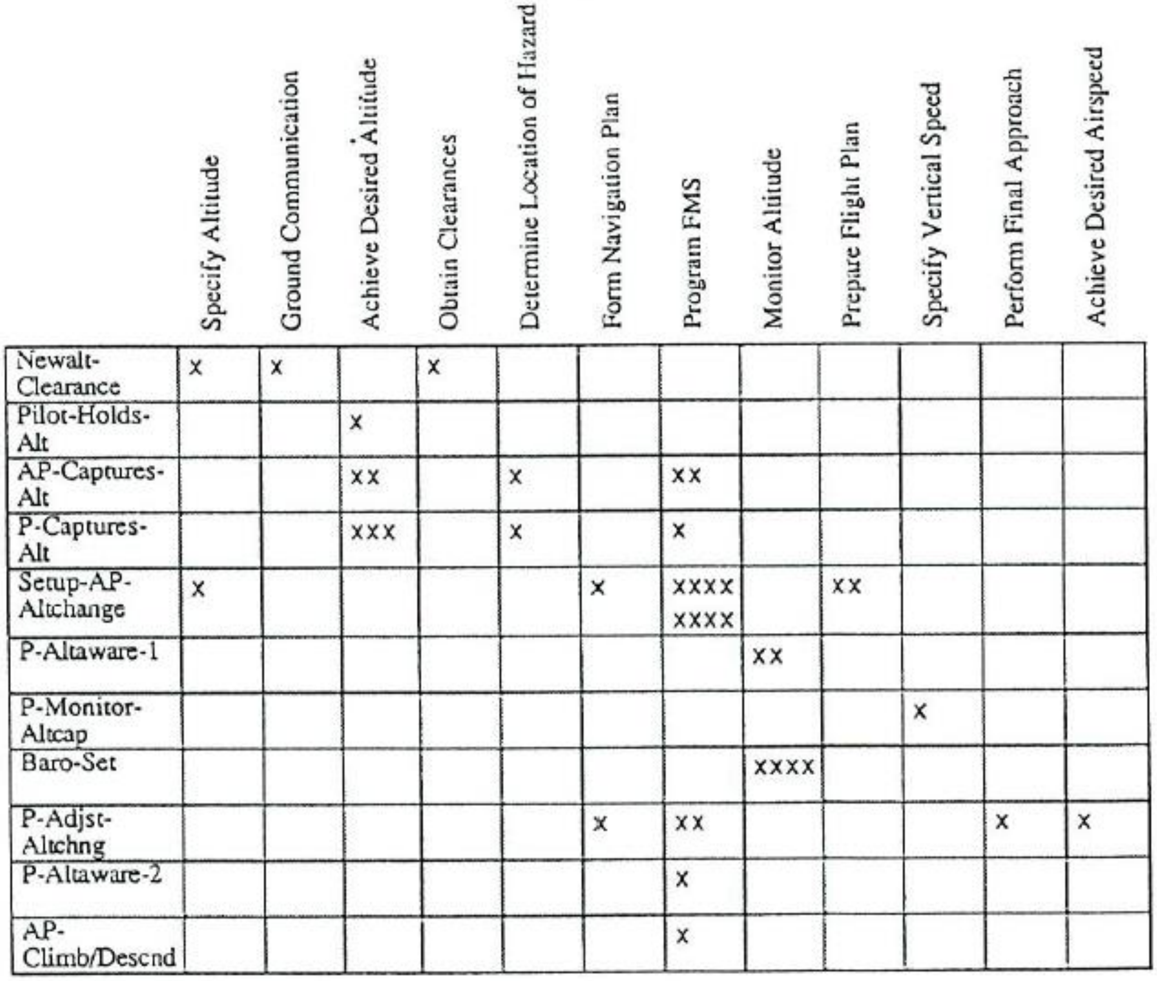
A set of callback questions was developed for 15 ASRS incident reports. The questions were derived from examination of the sequential and functional models. The coding of each report was examined in conjunction with the models to see what questions the model structure provoked (i.e., what questions needed to be answered to allow the coding of the report to extend further into the models). A set of generic questions was also established to collect additional information of general interest.

Results of the Review of Altitude Deviation Events

The application of model-based human error analysis revealed many things regarding the characteristics of altitude deviation events in advanced technology aircraft. The mapping of ASRS reports of altitude deviations has provided a systematic method for classifying the errors that occur. These classifications can then be used to suggest remedies for preventing the errors or mitigating their consequences.

A matrix of ASRS reports and their sequential and functional codes is shown below in Table 3.

Table 3. Matrix of ASRS reports coded by sequential and functional models



	Specify Altitude	Ground Communication	Achieve Desired Altitude	Obtain Clearances	Determine Location of Hazard	Form Navigation Plan	Program FMS	Monitor Altitude	Prepare Flight Plan	Specify Vertical Speed	Perform Final Approach	Achieve Desired Airspeed
Newalt-Clearance	x	x		x								
Pilot-Holds-Alt			x									
AP-Captures-Alt			xx		x		xx					
P-Captures-Alt			xxx		x		x					
Setup-AP-Altchange	x					x	xxxx xxxx		xx			
P-Altaware-1								xx				
P-Monitor-Altcap										x		
Baro-Set								xxxx				
P-Adjst-Altchng						x	xx				x	x
P-Altaware-2							x					
AP-Climb/Descnd							x					

As Table 3 shows, sequential codes were distributed among 11 of the 13 event trees, with SETUP-AP-ALTCHNG (setting up the autopilot for altitude change) having, by far, the largest grouping. Groupings also occurred within the functional model, with the largest grouping under "Program Flight Management System (FMS)". These results fit with the hypothesis of this study that the crew interaction with the advanced cockpit is a source of errors which lead to altitude deviations. Within the grouping of errors, it was observed that three specific types of errors were predominant.

- Errors that occurred because the flight crew did not understand the details of FMS functions. These types of errors could possibly be prevented by improved training regarding FMS functions, or the redesign of the systems so that the representation of status is more apparent to the crew.

- Errors that resulted from incorrect manipulation or monitoring of automated systems. This type of error could potentially be prevented by redesign of the displays and controls to provide better feedback to the flight crew.

- Errors that occur when the pilot understands the function of the autoflight systems, but errors have been introduced from an external source such as maintenance or design errors. These errors could potentially be prevented by a redesign of automated systems taking into account the pilots expectations of the system.

This study of altitude deviation errors led to a number of general observations about the factors that lead to these incidents. It appears that pilots have learned to rely on their automated systems, and have delegated control of not only flight functions, but also monitoring functions, to the automation. Thus, they are not watching for deviations to occur, but tend to assume that the autoflight systems will take care of altitude capture and maintenance. Some pilots seem to be predispositioned to assume that the automated systems will do what they (the pilots) expect them to do, when in some circumstances the automation "wants" to do something else. These factors imply that the role of the pilot has in some circumstances changed so that they are flying the flight management system rather than the aircraft itself. The final result is the relaxation of the pilot's instinct to "stay ahead" of the airplane and decreased vigilance regarding the maintenance of critical flight functions. Thus it is possible that advanced technology may in some cases actually reduce the flight crew's situation awareness.

Application to Nuclear Power Plant Work Protection Incidents

A project was conducted by DNV GL to apply a barrier management approach for evaluating work protection incidents at a major multi-unit nuclear power station. The project objectives were to identify common factors that contribute to work protection incidents, assess the effectiveness of existing barriers to prevent work protection incidents, and identify potential corrective actions that could strengthen existing barriers or add additional barriers to reduce the likelihood of work protection incidents or mitigate their consequences.

The main activity of this project was a work protection bow tie workshop conducted at the nuclear power station in August 2013. The workshop was attended by ten subject matter experts from the nuclear power station and two DNV GL personnel who served as the facilitator and scribe for the workshop.

The cornerstone of risk management is the development and maintenance of controls or barriers to prevent or mitigate risk events or accidents. For this study the risk events of interest were those that degrade or defeat barriers that are used to prevent or mitigate work protection accidents at the nuclear power station. Therefore an important step of this study was a systematic identification of these barriers and how they interact to prevent or mitigate such events.

Barrier analysis was performed in the work protection workshop by developing bow tie diagrams to illustrate the barriers that can be used to prevent or mitigate events that could lead to work protection accidents. The main focus of the workshop was development of a generic bow tie diagram for work protection processes at the nuclear power station. Both the left-hand (prevention) side and the right-hand side (mitigation) of the bow tie diagram were developed. However, since the focus of the project was to develop insights to prevent the occurrence of work protection incidents at the nuclear power station, far more attention was given to the left hand side of the bow tie diagram. However, for completeness the right hand side was developed at a high level, so that workshop attendees would have the complete context for understanding the effects of potential work protection processes for prevention and mitigation of work protection incidents.

Next, the generic bow tie diagram was annotated for each of 15 work protection incidents. This was accomplished by a thorough discussion of the specific sequence of events for each incident to determine where in the work protection process the failure(s) occurred. The barriers were then color coded to denote the performance of the relevant barriers for each incident, e.g. whether the barrier was effective in preventing the progression of the incident.

Following the development of the annotated bow tie diagrams, a summary bow tie diagram was developed to show how many times each barrier was compromised or failed across the 15 events, and which barriers were effective in detecting the deviation from accepted work protection practices so that an accident was prevented. This visual summary made it possible to quickly identify which barriers were bypassed most often in the work protection incidents.

The summary bow tie diagram was then examined to determine what changes could be made to strengthen the barriers that are intended to prevent work protection accidents. The recommendations were added to the summary bow tie diagram attached to the barriers they are intended to strengthen, and the diagram was color coded to show the barriers that should be strengthened, barriers and procedure steps that could be simplified, and additional new barriers that could be added.

The final activities of the workshop were to identify global recommendations that cut across individual barriers and could have significant impact on the overall reliability and effectiveness of the work protection processes. In addition, preliminary ideas were developed for next steps to be taken to improve work protection at the nuclear power station, including possible implementation of barrier management and bow tie analysis as ongoing processes.

The barrier management approach and work protection bow tie workshop at the nuclear power station were very effective in achieving the project objectives. The workshop was used to identify the barriers that are intended to prevent work protection incidents. Bow tie diagrams proved to be a very effective approach to identify the barriers, assess their performance across 15 different work protection incidents, and identify the critical problem areas where work protection practices should be enhanced. The use of bow tie diagrams allowed the group to be very efficient in developing the generic bow tie diagram, annotating it for the 15 incidents, summarizing the relative frequency of barrier failures, and develop consensus recommendations for implementation. In addition, global recommendations were developed for consideration by management of the nuclear power station.

Application to Pipeline Leak Accidents

A structured workshop was conducted in the control center of a pipeline operating company to assess the major human factors and control room management issues that contributed to a major pipeline leak accident, and the effectiveness of corrective actions that were subsequently implemented. This review was conducted to satisfy the requirement of the regulatory authority to employ an independent third party to evaluate the effectiveness of corrective actions that were implemented following the accident. DNV GL conducted the study using the same systematic barrier-success path approach that has been used for offshore drilling and production companies and a nuclear power station as described in the previous section.

The workshop was structured to include guided exploration of qualitative human factors issues as well as objective assessment exercises. The goal was to increase understanding and consensus among control center personnel regarding the health of current control room management and human factors practices, and to explore potential additional improvements that should be adopted or evaluated further.

The following exercises were used to develop and capture consensus of workshop participants regarding the adequacy of the human factors and control room management aspects of operations at the pipeline control center.

Develop safety objective tree for pipeline leak detection and response

Safety objective trees are a technique developed in the commercial nuclear power industry to systematically identify the strategies and resources that are available to maintain the Critical Functions for safe operation. A Critical Function is a group of actions and equipment functions that must be performed to achieve a given safety objective. A Challenge is a threat to continuous performance of the Critical Function and may include physical phenomena, equipment failures, and/or human errors. A Mechanism is a combination of conditions that can lead to a Challenge. Strategies are actions that can be taken to restore the Critical Function if it is degraded or fails.

The safety objective tree is a hierarchical structure that shows the Objective (e.g. safe pipeline operation), Critical Functions (e.g. pipeline integrity) that must be obtained to achieve the Objective, Challenges (e.g. reduction of wall thickness) that can degrade the health of the Critical Functions, Mechanisms (e.g. corrosion) that can lead to the Challenge, and risk management Strategies (e.g. leak detection and response) that can be used to restore degraded or failed Critical Functions.

Identify and assess effectiveness of strengthened and new barriers since the pipeline leak accident

A generic leak detection and response bow tie diagram was developed by DNV GL prior to the workshop and reviewed and updated by the workshop participants to more accurately reflect the barriers that are currently available to prevent or mitigate potential pipeline leak incidents. The enhancements instituted since the pipeline leak accident were reviewed and barriers that have been strengthened or added were identified. The bow tie diagram was then updated and color coded to clearly represent this information. Each barrier was assessed regarding its effectiveness as currently implemented.

The updated bow tie diagram was then reviewed to determine if additional actions could be taken to further strengthen barriers or add additional new barriers to maximize human factors aspects of the pipeline control center operations. The bow tie diagram was modified and color coded to show these recommendations. The results of this study were submitted to the regulatory authorities to demonstrate the effectiveness of the corrective actions that had been implemented since the major pipeline leak accident.

The barrier-success path approach proved to be an effective way to perform the assessment and present the results to the regulatory authorities. In addition, personnel of the pipeline operating company expressed the opinion that the use of the approach helped increase their understanding of the human factors and control room management issues for preventing and mitigating future pipeline leak incidents.

Application to Regulatory Compliance Assessment for Deepwater Offshore Drilling

The barrier-success path approach has been applied to development of diagnostic algorithms for an advanced blowout preventer (BOP) control system [4]. A detailed response tree was developed to identify the success paths that can be used to implement critical BOP functions, and the information and instrumentation that can be used to assess availability of the critical assemblies of the BOP control system.

In addition, the barrier-success path approach and the BOP control system information requirements analysis were used to establish decision criteria for regulatory compliance assessment and BOP pull/no pull decisions. The decision criteria are represented in a success tree logic model to facilitate understanding of current status of regulatory compliance and communication among operations, maintenance, and regulatory personnel. The ultimate goal is to agree in advance with regulatory personnel regarding the decision criteria for continued operation and pull/no pull decisions, to form the basis for discussion and consensus during drilling operations.

Figure 8 shows portion of the decision criteria logic model for regulatory compliance assessment for a generic BOP control system. The logic model is a success tree structure based on the requirements of API STD 53 for availability of BOP functions. The Top Event for the logic tree is “Criteria for Continued Operation.” The basic premise is that as long as the availability of BOP functions at the lower levels of the tree is such that the Top Event is satisfied, drilling operations can continue. This logic model is continuously monitored during drilling operations to determine if drilling can continue because the BOP control system complies with all regulatory requirements. The BOP control system response tree is continuously updated to assess the availability of key control systems assemblies, and the results are fed to the regulatory compliance logic diagram. If failures of BOP control system assemblies result in a situation where the available BOP functions do not meet regulatory compliance requirements, this provides clear indication that the drilling operations must be suspended and the BOP must be pulled to the surface for maintenance.

A major benefit of this regulatory compliance logic model is that decision criteria can be agreed in advance between operators and regulatory authorities such as BSEE. This means that discussions with regulatory personnel during operation can focus on the effects of BOP control system failures on the pre-established decision criteria, rather than requiring detailed review of piping and instrumentation diagrams (P&IDs) and the effects of individual component failures. This will facilitate consensus between operator and regulator on decisions for continued operation as long as the regulatory decision criteria are satisfied.

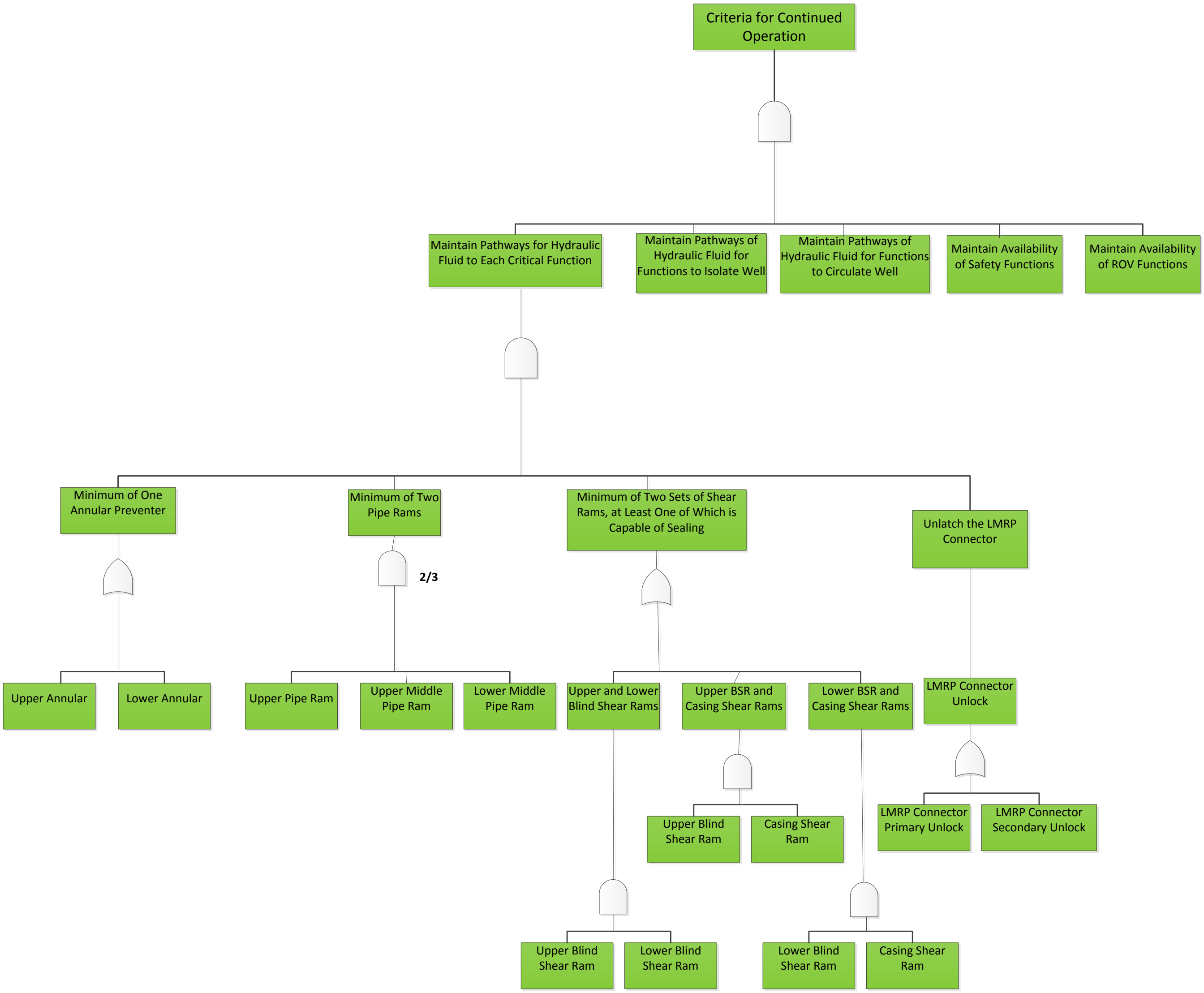

Criteria for Continued Operation
Maintain Pathways for Hydraulic Fluid to Each Critical Function
Maintain Pathways of Hydraulic Fluid for Functions to Isolate Well
Maintain Pathways of Hydraulic Fluid for Functions to Circulate Well
Maintain Availability of Safety Functions
Maintain Availability of ROV Functions
Minimum of One Annular Preventer
Minimum of Two Pipe Rams
2/3
Minimum of Two Sets of Shear Rams, at Least One of Which is Capable of Sealing
Unlatch the LMRP Connector
Upper Annular
Lower Annular
Upper Pipe Ram
Upper Middle Pipe Ram
Lower Middle Pipe Ram
Upper and Lower Blind Shear Rams
Upper BSR and Casing Shear Rams
Lower BSR and Casing Shear Rams
LMRP Connector Unlock
Upper Blind Shear Ram
Casing Shear Ram
LMRP Connector Primary Unlock
LMRP Connector Secondary Unlock
Upper Blind Shear Ram
Lower Blind Shear Ram
Lower Blind Shear Ram
Casing Shear Ram

Figure 8. Regulatory compliance decision criteria logic model for an advanced BOP control system

Application of the Barrier-Success Path Approach to Enhance Safety and Operational Efficiency

The barrier-success path approach provides a consistent framework for systematically reviewing operational experience and makes it possible for lessons learned from incidents to be directly fed back to improve management systems, procedures, and training and to identify potential design changes to enable more effective barrier and success path management. Figure 8 illustrates how evaluation of operational experience and incidents can be used to identify lessons learned that then can be used to improve barrier and success path performance to enhance safety and improve operational efficiency. The barrier-success path framework can be used to consistently interpret and apply design and operational information, and to serve as a common language for communication and consensus among operating companies, service companies, contractors, and regulatory authorities. A DNV GL Joint Industry Project entitled "Decision Support for Dynamic Barrier Management" has been organized to test the value of this approach by applying it to an offshore plug and abandon (P&A) case study. Thirteen organizations representing offshore operators, service companies, contractors, and regulatory authorities will participate in workshops to apply the approach and to evaluate its benefits for offshore operations and regulatory-industry communication.

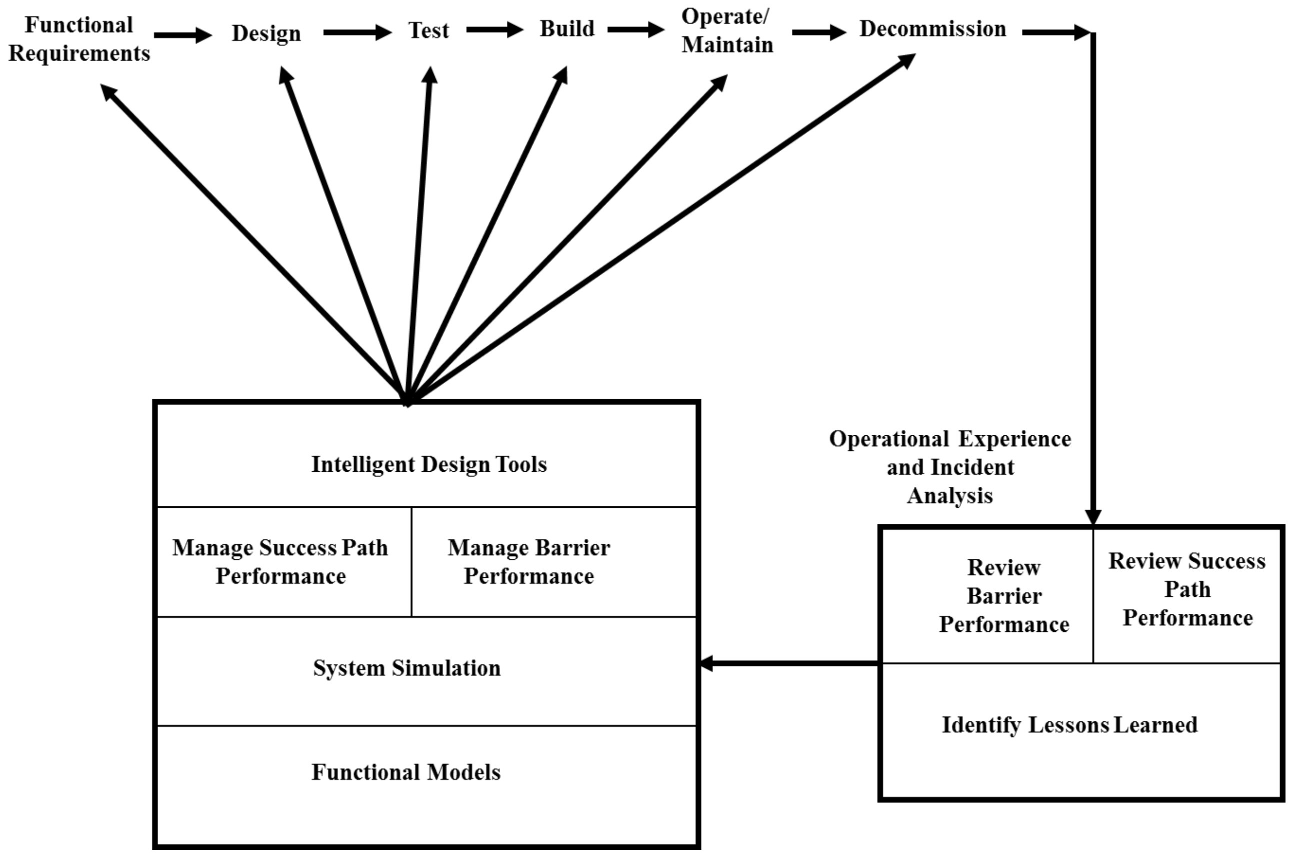

Functional Requirements
Design
Test
Build
Operate/ Maintain
Decommission
Intelligent Design Tools
Manage Success Path Performance
Manage Barrier Performance
System Simulation
Functional Models
Operational Experience and Incident Analysis
Review Barrier Performance
Review Success Path Performance
Identify Lessons Learned

Figure 8. Application of barrier-success path approach to interpret operational experience and enhance design, operation, and maintenance

Conclusions

A critical component that must be developed for effective utilization of operational data at the industry level is a framework for interpreting operation experience that will protect data confidentiality while allowing consistent interpretation and identification of lessons learned. Such a framework could support consistent application to identify lessons learned across discipline and organizational boundaries and the development of a "common language" for communication and consensus for action amongst industry and regulatory organizations. The barrier-success path approach described in this paper may form the foundation of a framework to organize and utilize the large volumes of design, operating, maintenance, and regulatory information in a form that will support critical decisions both within organizations as well as across stakeholder groups including regulatory authorities.

The barrier-success path approach combines proven concepts from the nuclear power, aerospace, and offshore industries to form a framework for organizing information that can be used throughout the system lifecycle to design, build, operate, maintain, and regulate complex systems such as nuclear power plants, commercial aircraft, oil and gas pipelines, and offshore drilling and production installations. The approach is particularly helpful in reviewing operational experience and incident reports to identify lessons learned that can be translated into corrective actions that will enhance the performance of barriers and success paths to enable enhanced safety and operating efficiency. Experience gained since the early 1990's in applying the approach to assessment of incidents and accidents in commercial aviation, nuclear power plant operations and worker protection, pipeline operations, and offshore drilling and production has demonstrated the value of the approach. The DNV GL Joint Industry Project "Decision Support for Dynamic Barrier Management" will enable a broader cross-industry exercise to test the approach and refine it for broader dissemination within the offshore oil and gas industry.

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.
3. W.R. Nelson, J.C. Byers, L.N. Haney, L.T. Ostrom, and W.J. Reece, "Lessons Learned from Pilot Errors Using Automated Systems in Advanced Technology Aircraft," American Nuclear Society Topical Meeting on Nuclear Plant Instrumentation, Control, and Man-Machine Interface Technologies, Oak Ridge, TN, April 18-21, 1993.
4. W.R. Nelson, "Improving Safety of Deepwater Drilling Through Advanced Instrumentation, Diagnostics, and Automation for BOP Control Systems," Offshore Technology Conference, Houston, TX, May 2-5, 2016.