DISCUSSION PAPER

January 2011 ■ RFF DP 10-61

# Precursor Analysis for Offshore Oil and Gas Drilling

## *From Prescriptive to Risk-Informed Regulation*

Roger M. Cooke, Heather L. Ross, and Adam Stern

1616 P St. NW
Washington, DC 20036
202-328-5000 www.rff.org

RESOURCES FOR THE FUTURE

# Precursor Analysis for Offshore Oil and Gas Drilling: From Prescriptive to Risk-Informed Regulation

Roger M. Cooke, Heather L. Ross, and Adam Stern

## Abstract

The Oil Spill Commission's chartered mission—to "develop options to guard against … any oil spills associated with offshore drilling in the future" (National Commission 2010)—presents a major challenge: how to reduce the risk of low-frequency oil spill events, and especially high-consequence events like the *Deepwater Horizon* accident, when historical experience contains few oil spills of material scale and none approaching the significance of the *Deepwater Horizon.* In this paper, we consider precursor analysis as an answer to this challenge, addressing first its development and use in nuclear reactor regulation and then its applicability to offshore oil and gas drilling. We find that the nature of offshore drilling risks, the operating information obtainable by the regulator, and the learning curve provided by 30 years of nuclear experience make precursor analysis a promising option available to the U.S. Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) to bring cost-effective, risk-informed oversight to bear on the threat of catastrophic oil spills.

**Key Words:** catastrophic oil spills, quantitative risk analysis, risk-informed regulation

## Contents

# Precursor Analysis for Offshore Oil and Gas Drilling: From Prescriptive to Risk-Informed Regulation

Roger M. Cooke, Heather L. Ross, and Adam Stern*



## Summary of Conclusions and Recommendations

The *Deepwater Horizon* spill bears a striking resemblance to the Three Mile Island (TMI) disaster, an unprecedented catastrophic system failure resulting from a sequence of individual failures, no one of which was by itself unprecedented or catastrophic. After TMI, the U.S. Nuclear Regulatory Commission (NRC), recognizing the stepwise path to disaster, developed the Accident Sequence Precursor (ASP) program to identify and guard against the opening steps of a potential disaster sequence. In this initial scoping paper, we look at whether a similar precursor analysis methodology is worth exploring for the U.S. Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) oversight of offshore drilling. We conclude that it is, and we recommend further steps in that effort.

* Cooke, Chauncey Starr Senior Fellow; Ross, Visiting Scholar; Stern, Research Assistant, Resources for the Future, Washington, DC. The authors gratefully acknowledge the help of Christopher Hunter of the U.S. Nuclear Regulatory Commission, Accident Sequence Precursor program, in preparing this paper.

DISCLAIMER: This project was funded by the Department of Energy, National Energy Technology Laboratory an agency of the United States Government, through a support contract with Booz Allen Hamilton, Inc. 

### *Conclusions*

1. *Focus.* Precursor analysis targets outcomes—in this case, catastrophic oil spills—that are encompassed by broad regulatory oversight but are not the specific focus of that oversight. Given the dominant significance of such spills in the array of offshore harms to be guarded against by regulation, an effective purpose-built tool directed at spill prevention would improve oversight capability and respond to the learning from *Deepwater Horizon.*
2. *Rigor.* Existing regulatory arrangements to which precursor analysis would be added do not have the intellectual framework or quantification to recognize and evaluate spill precursor signals arising in day-to-day offshore operations. BOEMRE's new Safety and Environmental Management System regulation relies on a narrative description of hazards and their mitigation, not on rigorous data analysis and risk estimation. Although description is useful, it tends to be static and lapse into boilerplate repetition over time.
3. *Learning.* The regulator is the entity best positioned to develop a tool that can harness the power of cumulating offshore operating data to focus on spill prevention. Such a tool provides a learning framework for both regulator and operator as drilling proceeds, and it encourages the development of rigorous risk analysis within the operator community, as it has done in the nuclear sector.
4. *Experience.* NRC's Accident Sequence Precursor program, set up in a similar postcatastrophe situation to guard against future low-probability, high-damage system failure, provides the most established model for BOEMRE to consider in working toward a system of its own. Thirty years of experience with ASP will help BOEMRE evaluate how it may be useful to them and benefit from the learning curve it provides.
5. *Challenge.* There is no question that BOEMRE needs to build its scientific oversight capabilities using data from ongoing operating events, and no question that NRC has been able to do this successfully in the nuclear sector. Nevertheless, the challenge of introducing precursor analysis into offshore regulation is substantial. The number and diversity of regulated facilities, the variety of operating environments, the disparateness of operator characteristics and behavior, and the low baseline use of quantitative risk techniques make this an ambitious undertaking.
6. *Efficiency.* A successful oversight program requires considerable intellectual investment up front but limited manpower to run. NRC's ASP program now involves

about one man-year of effort to cover 104 commercial reactors, a fifth of its initial level. Anticipated budget stringency further strengthens the argument for analysis-leveraged versus manpower-intensive oversight.

7. *Imperative.* BOEMRE has a rich database and thorough regulatory authority to develop and operate a scientific, risk-informed oversight program directed at preventing catastrophic oil spills. Whatever the method chosen, and whatever the challenges encountered, it should now embark on that path.

### *Recommendations*

1. *Report.* We recommend that the Oil Spill Commission address explicitly in its report the desirability of adding to BOEMRE a risk-informed oversight capability focused on preventing catastrophic oil spills and based on data from ongoing operating experience on the Outer Continental Shelf (OCS).
2. *Follow-on.* If the Commission finds such a new capability desirable, it will not have the time or resources to flesh out risk-informed spill oversight during its tenure. We recommend that it set up, or cause to be set up, an expert group of individuals with technical skills in risk analysis, knowledge of offshore oil and gas operations, and familiarity with BOEMRE oversight practices and capabilities. This "precursor group" would take the next steps to develop options for BOEMRE to establish a risk-informed regulatory program directed at preventing catastrophic oil spills. We believe a small group of qualified personnel could develop such options in a six month time frame.

## Introduction

Comprehensive review of federally regulated offshore oil and gas activity in the wake of the *Deepwater Horizon* spill is driving wholesale reconsideration of government oversight approaches and capabilities. Consensus is emerging on the need to shift regulation by BOEMRE away from a traditional prescriptive regime based on command, control, and compliance to a modern risk-informed regime in which the achievement of clear safety goals is a shared responsibility of government and industry, each with clearly demarcated responsibilities. After the accident at Three Mile Island (TMI) on March 28, 1979, the U.S. Nuclear Regulatory Commission (NRC) embarked on such a shift, charting a long trajectory of innovation and refinement that continue to this day. A major element of their effort is the Accident Sequence

Precursor (ASP) program (Minarick and Kukielka 1982; Minarick et al. 1988; Minarick 1989; Cottrell et al. 1984), initiated in response to recommendations from the Lewis Committee review (Lewis et al. 1978) of the first comprehensive probabilistic risk analysis (NRC 1975).

Risk-informed regulation is indicated for sectors where industry is technology driven, with a high rate of innovation and the potential for low-frequency events causing substantial harm to the public and the environment. The regulator cannot remain on the sidelines of technological innovation but must engage industry as a full partner in the achievement of safety goals. This partnership is not achieved by regulatory fiat; rather, it emerges from an evolutionary process that involves growing the analytic skills for risk quantification within industry, generating a data flow to support risk quantification, and fostering a safety culture based on quantitative risk analysis.

This paper takes a first look at the role precursor analysis might play in BOEMRE's new regulatory regime. Section 1 presents a short background on quantitative risk methodology. Section 2 discusses the history of the ASP program within the shift to risk-informed regulation at NRC. Section 3 considers the application of ASP methodology to offshore drilling. Section 4 outlines how BOEMRE might build upon and extend current regulatory practice. Section 5 offers conclusions and next steps.

## 1. Background on Quantitative Risk Analysis

### *1.1 Risk-Informed Decisionmaking in Government Oversight*

The need for risk management in government oversight arises when an industry engages in activities that create the potential for low-frequency, high-consequence events—rare occurrences that could harm the general public and the environment. Risk management tools are used to proactively analyze the probability of such events based on past operational and test data. Risk values can be generated to monitor current operations and prioritize regulatory interventions. A number of federal agencies—the Federal Aviation Administration, the Environmental Protection Agency, the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, the Department of Energy, and the Food and Drug Administration—oversee industries whose activities pose significant risks to the public and therefore use risk management procedures in their regulatory process. Approaches to risk management in government agencies are not homogeneous, however. The focus here is on risk of engineered systems; the analysis of consequences of loss events is outside the present scope.

### *1.2 Basic Tools for Dealing with Risk*

Two basic tools used in operational risk management are probabilistic risk analysis (PRA) and accident sequence precursor (ASP) analysis. Both methods seek to answer the same risk-quantifying questions but differ in application and methodology. PRA was initiated in the aerospace sector; it models the failure probability of a complex system, such as a launch vehicle, in terms of failure probabilities of its components. These probabilities could be estimated from test data and used to predict system reliability in the absence of sufficient operating experience at the system level. ASP analysis is designed to operate on a population of similar systems. It trades in-depth system modeling for aggregate operational experience.

Each method has strengths and weaknesses. The basic modeling tools of PRA are event trees and fault trees. Event trees describe initiating events that threaten the system and map their progression as successive layers of engineered safeguards are challenged. Fault trees model the response of safety subsystems down to the component level. The in-depth modeling of PRA fault trees affords many insights into the risk and reliability of the system. Designers plan for their systems to function properly; they are not accustomed to assuming that each component fails or examining how the failures propagate through the system. That is exactly what PRA does. The modeling exercise itself often reveals weakness in system design, such as insufficient redundancy, insufficient separation in engineered safeguards, and imprudent mixing of system control and safety functions. On the downside, PRA has a very large appetite for data that is difficult to appease at the level of an individual system. Test data generated during the design phase may ignore reliability growth. Test data produced during operations may not reflect dependencies that arise in actual operations. Test and operational data at a specific facility may be insufficient to quantify all relevant occurrence rates of initiators and response probabilities of defensive systems, thus creating a need for data from other sources. These include “generic” data and subjective engineering judgment. Human error and human recovery are important aspects of risk management whose modeling and quantification are largely subjective.

ASP forgoes in-depth modeling at individual facilities and uses instead “generic” event trees. These event trees aim to reflect macroscopic design of the engineered safety systems. In the first generations of ASP implementation in the nuclear power industry, event trees were distinguished according to basic reactor type (boiling water or pressurized water) and initiator. The methodology requires an incident reporting system, and it requires analysts to map each relevant incident onto one or more generic event trees. The coarse-grained plant population perspective lacks specific detail but automatically captures system dependences that may be missed in PRA modeling, and it also captures human error and human recovery.

### *1.3 Illustrative ASP Calculation*

An example of a generic nuclear event tree is shown below (Minarick and Kukielka 1982). Rather than explain all the details, we simply note that it refers to a "loss of main feedwater" at a pressurized water reactor, possibly leading to severe core damage.[1] The tree starts with the initiator at the left. At each bifurcation the upward path is taken when the corresponding safety system functions properly; the downward path is taken when the system fails.

After several hundred facility-years of operating experience, there are enough data to estimate most of the safety system failure probabilities and many of the initiating event frequencies. Unavailabilities of safety systems revealed during scheduled testing are also mapped into the event trees as accident precursors. Gaps can be filled by more generic data.

Figure 2 shows the precursor at the Dresden 1 unit in Grundy, Illinois, in which the reactor failed to shut down (scram) under conditions (low primary drum level) that should have triggered a scram. Had this happened when the feedwater was still pressurized, it could have caused severe core damage. The particular conditions are described in the initiator box, and their probability is estimated at 0.56/year, or $0.56 \times 360/8760 = 0.023$ for the 360 hours during which this condition existed. The reactor scram failure is assigned probability 1. Given this initiator and given scram failure, severe core damage results if either the operator fails to detect the low drum level (probability 0.005) or if the operator does detect the level but the emergency condenser fails to provide core cooling (probability $0.995 \times 0.005$). The result is that the probability of severe core damage, given this precursor, is $0.023 \times (0.005+0.995 \times 0.005) = 0.000229$. This conditional core damage probability is the indicator of the severity of the precursor. Whereas the initiator in the generic event tree is loss of main feedwater, the probability calculation uses the specific type of main feedwater loss that triggers this particular sequence. The human error probabilities are generic.

---

[1] "Severe core damage" refers to a set of physical circumstances previously called core melt. In these circumstances, the core reaches temperatures (2,200°F) that cause the fuel rods to melt, as happened in the TMI accident of March 28, 1979, when about one-third of the core melted.

**Figure 1. Example Generic Event Tree: Loss of Main Feedwater with Successful Reactor Trip and Failed Auxiliary Feedwater and Secondary Heat Removal**

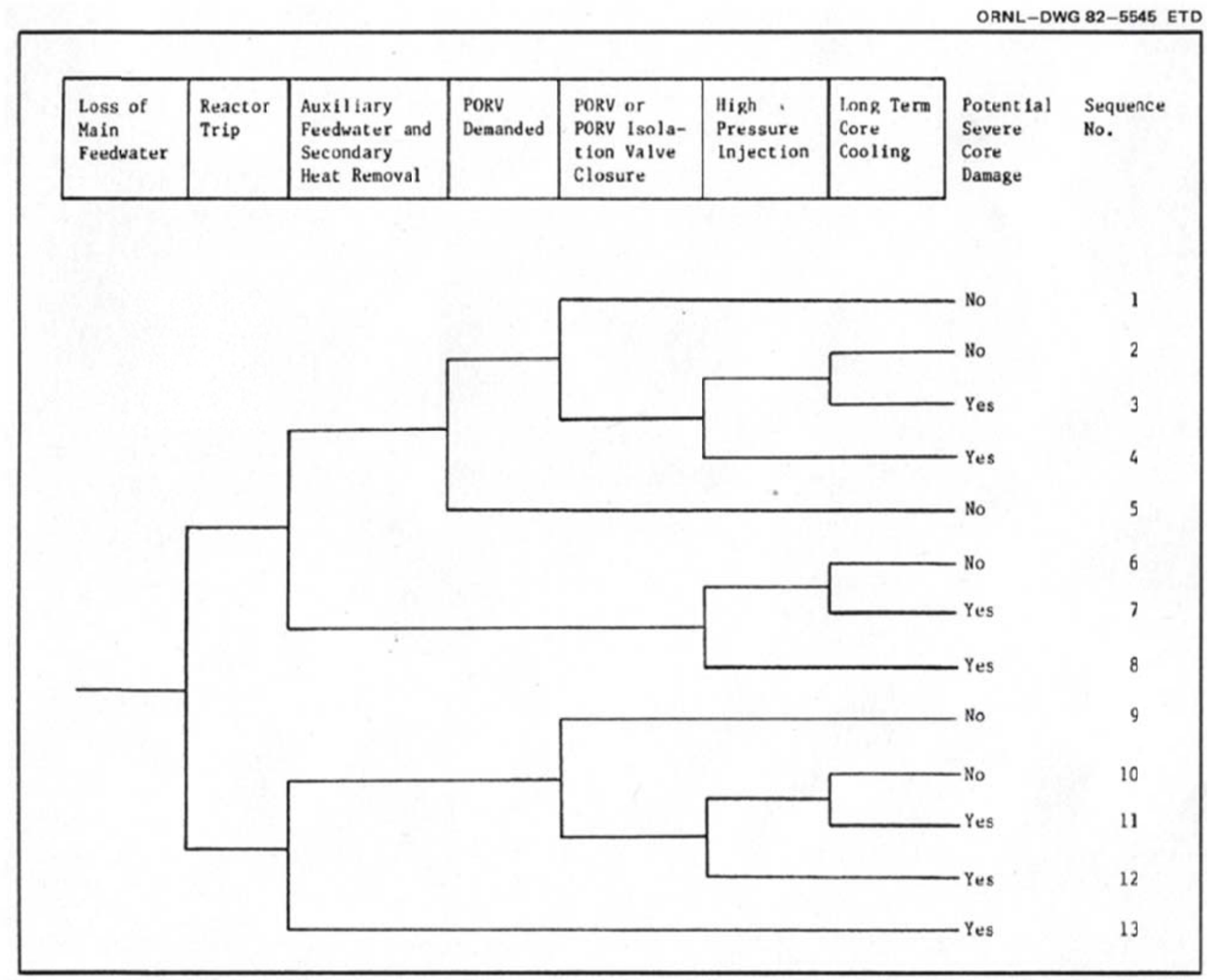
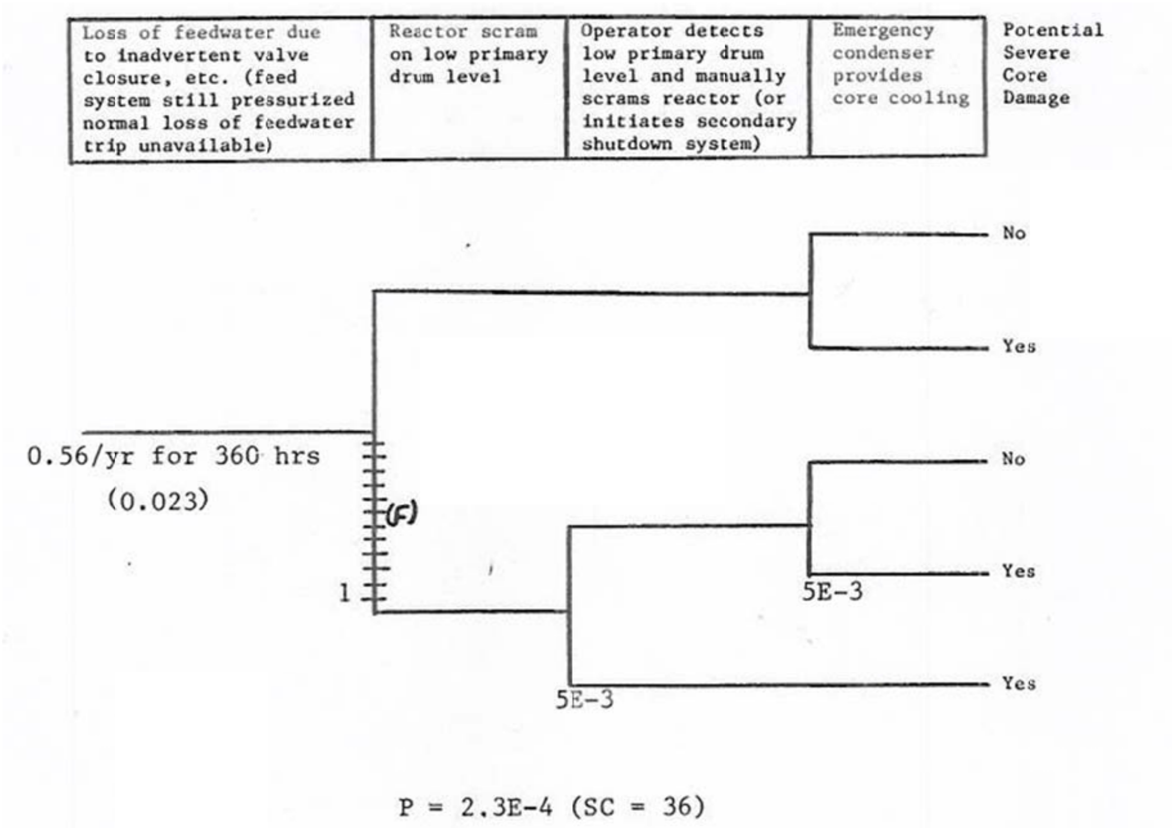


**Figure 2. Example Event Tree: Sequence of Interest for Failure of Three of Four Safety System Sensors for Primary Drum Level Scram at Dresden 1**




This illustrates how analysts calculate the conditional probability that this precursor would have led to a significant accident that posed risk to the public and environment. Conditional probabilities of severe loss events provide a tool for assessing the severity of each incident, assessing the historical performance at each facility, and assessing the temporal progression of the population-wide risk. For historical interest, the event tree corresponding to the Three Mile Island accident of March 28, 1979, and its corresponding generic event tree, are given in Appendix 1.

## 2. History of ASP Within Risk-Informed Regulation

Although its origins may be traced to the aerospace sector, the first comprehensive quantitative risk analysis was performed under contract with NRC (1975). After a turbulent reception by the scientific community, its “achievements and limitations” were reviewed in a report published shortly before the TMI accident (Lewis et al. 1978). The review committee recommended “that potentially significant [accident] sequences, and precursors, as they occur,” be subjected to quantitative risk analysis, and NRC's Office for Analysis and Evaluation of Operational Data subsequently developed the Accident Sequence Precursor program. The original objective was to analyze accident sequence precursors with the PRA tools already being used to analyze plant specific risk. This capitalized on the advantages of the ASP method, as noted above, and leveraged the synergy of having complementary risk tools.

The program's main objectives and scope were altered throughout the 1980s, and a more permanent set of objectives was put in place in 1993. NRC listed five main objectives for the ASP program:

- to identify and quantitatively estimate the risk significance of operational events;
- to determine the generic implications of operational events and characterize risk insights from these events;
- to provide supplemental information on plant-specific performance;
- to provide a check on PRAs; and
- to provide an empirical indication of industry risk and associated trends.

The current ASP program is supported by an institutionalized incident reporting system that requires all nuclear power plants to report to NRC all operational events that represent a deviation from the licensing basis or a failure or degradation of a safety function (NRC 1991). These "licensee event reports" have a strict format and guidelines to ensure that NRC captures all possible problems. Once collected, the reports are placed through a screening process to identify accident precursors, defined as "an initiating event or degraded condition that, when coupled with one or more postulated events, could result in a plant condition involving inadequate core cooling and severe reactor core damage" (Minarick and Kukielka 1982).

Once the precursors are identified, they are modeled in one or more generic event trees with various initiating events. In the year-end ASP reports, the precursors are ranked by their "conditional core damage probability," which gives the probability that a particular precursor will cause severe core damage. These results are used to identify the most dangerous precursors and are compared with those from previous years to identify industry trends. APPENDIX 2 shows some results from an NRC review in 2006. Significantly, the precursors in this review involving "degraded conditions"—unavailabilities of safety systems without the occurrence of an initiating event to challenge these systems—contribute significantly to the overall risk. These might easily be overlooked by an incident reporting system focused on initiating events.

A recent review (Kadak and Matsuo 2007) identifies the following factors as ingredients for a successful transition from prescriptive to risk-informed regulation:

- strong top management support and leadership both at the regulator and the licensee level;
- education and training in risk principles and probabilistic risk assessment;
- a slow and steady introduction of risk initiatives in areas that can show value to both regulator and industry;
- a transparent regulatory foundation built around safety goals; and
- development of a strong safety culture in industry allowing for more independence in safety compliance and risk management.

In the nuclear sector, the PRA methodology was originally launched through “generic PRAs” performed under contract with NRC (1975). These were later adopted by industry and specialized to unique facilities. In 1988, NRC requested that each licensee conduct an individual plant examination allowing the identification of plant vulnerabilities (NRC 1988). The “maintenance rule” of 1991 allowed licensees to develop risk-informed maintenance programs based on these plant examinations. According to Kadak and Matsuo (2007, 611), “It is generally agreed that the Maintenance Rule and its application was the first major attempt at using risk information in developing a regulatory compliance strategy.” Essential in the transition to a risk-informed regime was the fact that a small group of industry leaders formed a users’ group to further the application of risk analysis. “This small group influenced the overall industry position relative to risk-informed regulation and ultimately provided the focus for the Nuclear Energy Institute to begin an active dialog with the regulator on the adoption of the risk informed regulation and modifications to key rules” (Kadak and Matsuo 2007, 611).

A PRA focuses on detailed plant modeling, and it is appropriately developed and owned by the licensee. In contrast, the ASP method is focused on a population of facilities falling under one regulatory authority, and it is developed and owned by this authority. As operating experience accumulates, the synergies of PRA and ASP increase, each benefiting from the strengths of the other.

## 3. Precursor Analysis for Offshore Oil and Gas Drilling

Beyond a demonstrated potential for catastrophic system failure, the nuclear and offshore oil and gas sectors exhibit some important parallels supporting the utility of ASP analysis:

- each sector has a rich data history of relevant operational experience from which to observe past accident sequences and develop pertinent event trees;
- within each sector, installations, equipment and procedures are similar, such that regulated facilities can be grouped into a limited number of classes for generic analysis; and
- a baseline of operator logs and reports exists for each sector, plus regulator inspections and investigations on which to build the required information flow for precursor identification, monitoring, and evaluation.

This section considers each of these elements in turn.

### *3.1 Rich Data History*

From the earliest days of offshore activity in the 1940s, the U.S. Geological Survey, later the Minerals Management Service and now BOEMRE have kept files regarding operations and oversight on the OCS. Published reports from these records, and from industry compilations, provide insight into safety experience over those nearly seven decades. Papers by Danenberger (1993) and Izon, Danenberger and Mayes (2007) analyze blowouts— sudden, uncontrolled escapes of hydrocarbons— during the years 1971–2006. None of the 126 blowouts in this period approached the *Deepwater Horizon* event in severity: 77 involved striking pressurized gas pockets at shallow well depth before reaching target productive intervals, and 83 were controlled by sediments bridging or sealing the well or by gas depletion. Looking at incidents over the period 1979–1988, Sharples et al. (1989) assessed the nature and relative risk associated with jackup rigs— mobile platforms that stand on the sea floor, supported by three or more legs— compared with other rig types.

The blowouts analyzed by Danenberger and the accidents considered by Sharples are modest compared with the *Deepwater Horizon* disaster. But the conditions and events that led to those failures could result in great harm, were they to occur in other circumstances, notably those now being encountered on the deepwater OCS. Thus the historical record is a rich database for ASP development offshore, just as it was in the nuclear sector, where precursor analysis was built on an operating history of much more limited events than the unprecedented core meltdown that prompted it.

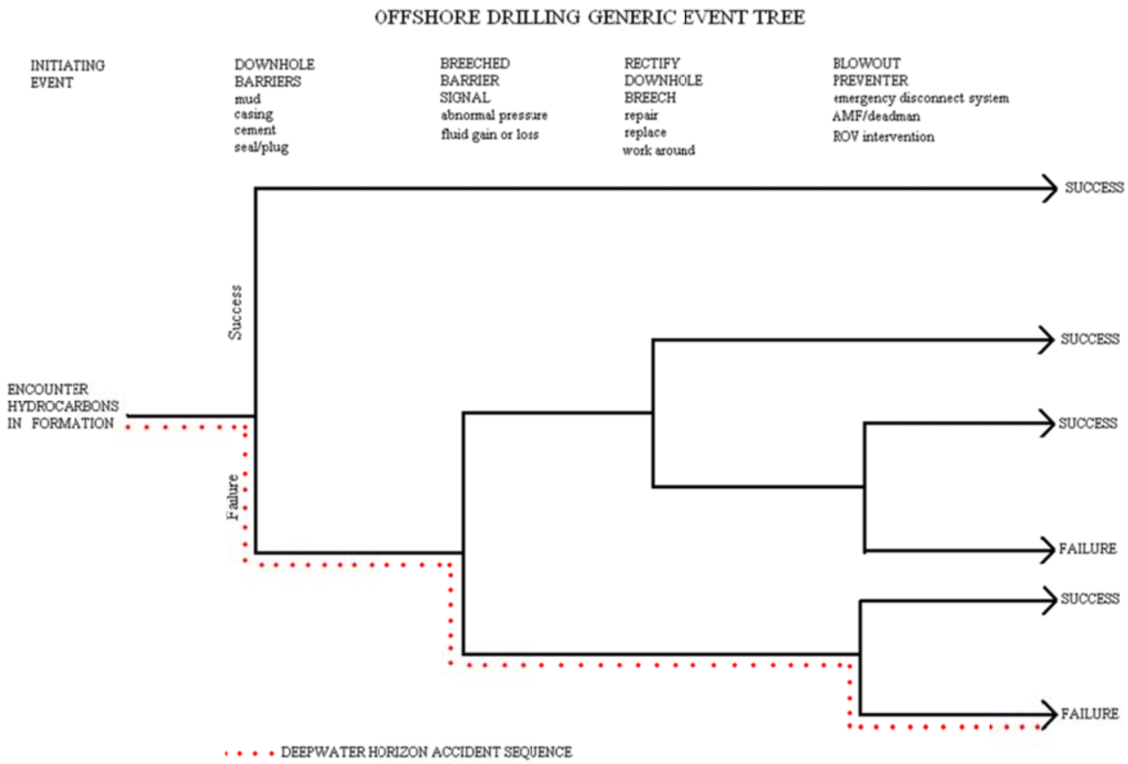
### *3.2 Generic Similarity*

As the interested public has learned from *Deepwater Horizon* reporting, offshore well drilling proceeds in a sequence of repetitive steps: drilling ahead with suitably dense mud to prevent fluid influx from the formations being penetrated; setting metal casing to enclose and reinforce the well segment just drilled before proceeding to drill a further segment with denser mud; cementing the casing that has just been set to secure it to the well wall and prevent any interstices that could allow hydrocarbons to migrate upward in the well; setting various hangars and plugs to ensure well strength and nonpenetration; and taking continual test measures, such as pressure readings and flow volumes, to confirm that well integrity is being maintained.

Consolidating into a few events the performance of this often complex sequence of “down-hole” steps, one can draw a very simple event tree, as in Figure 3. A failure of one or more down-hole barriers—mud, casing, cement, plugs—if not recognized through integrity testing and rectified, and if the blowout preventer fails, result in complete system failure, as occurred in the *Deepwater Horizon* accident sequence.

The tree in Figure 3 represents well control events at the broadest level of generic commonality. Trees for operational use will recognize different sequences of down-hole activities and potential accident paths. For example, one or more trees beginning with flawed cement as a “degraded condition” initiator are very likely to arise. Blowout analysis shows that cementing problems have increased significantly: they were associated with 46 percent of blowouts in 1992–2006 versus 26 percent in 1971–1991 (Danenberger 2007). As other features of offshore safety improved over the two periods, cementing performance did not. The first of eight major findings reported by the internal BP team investigating the Deepwater Horizon accident is, “The annulus cement barrier did not isolate the hydrocarbons” (BP Incident Investigation Team 2010, page 10).

**Figure 3. Offshore Drilling Generic Event Tree**




Many accident sequences will not be confined to down-hole events. The *Deepwater Horizon* sequence went far beyond the loss of well control and initial failure of the blowout preventer. It included failure on the rig to divert formation fluids and to prevent their ignition; repeated failures of remotely-operated-vehicles to activate the blowout preventer functions; failure to control the fire on the rig and prevent its sinking, causing collapse of the riser and multiple oil discharges on the seabed; and failure of a variety of containment structures and wellhead modifications to cap the outflow. The last three failures are distinctive to deepwater drilling with subsea blowout preventers, a difference between shallow water and deepwater drilling that ASP event trees will recognize. Other possible differentiations for early ASP recognition include exploration versus development drilling, drilling versus production, and bottom-founded rigs versus mobile offshore drilling units.

Event trees will also consider initiators external to drilling, such as storms, fires, ship collisions, mooring and station keeping failures, and seabed foundation problems, which appear amply in the historical record. Further extension can include other facilities that pose risks to the marine environment, notably subsea pipelines, which can deteriorate over time, rupture, or suffer damage from snagging or seismic activity.

The system failure of concern for all those event trees is “significant uncontrolled escape of hydrocarbons” (SUEH), analogous to “severe core damage” in the nuclear ASP program.

NRC began with two sets of simplified event trees, boiling water reactors and pressurized water reactors, in the early 1980s. It now performs precursor analysis using 78 risk models representing all 104 units in current commercial operation. These risk models use an event tree–fault tree linking methodology, and their proliferation over time has been the result of increasing fault tree specificity. A fault tree elaborates on the various ways an event tree failure (a “top event”) can occur. For offshore drilling, fault tree development that recognizes blowout preventer differentiation—optimal pressure rating, shearing, mix of ram types, redundancy, backup systems, etc. for different wells—will be an important part of powering up the ASP tool. Elaboration will happen over time. Both conceptual development and field implementation must walk before they can run; nevertheless, 30 years of NRC enhancement means that offshore oversight could start far along the ASP learning curve. An important part of that learning curve is seeing how the NRC created its earliest event trees and built up its capability from there. Another important part is seeing how regulator capability accelerated quantitative risk analysis capability in the regulated community.

### *3.3 Baseline Information*

ASP-informed regulatory oversight runs on focused, timely information about current operations. This information is a mix of required operator reports and regulator-generated data from inspections and investigations. The centerpiece is operator reports of specified events that the ASP program reviews against a specific set of screening criteria to identify those events that should be reviewed as candidate precursors. Those not screened out are subject to detailed ASP analysis using the relevant risk model (event tree plus any fault tree elaboration), which will itself be adapted as needed to recognize the operational event in question.

BOEMRE currently requires operators and other permit holders to immediately report any of a list of incidents involving material harm to workers or facilities or consequential operating irregularities (Incident Reporting Rule, 30 CFR 250.188). The agency may follow up such operator reports with an incident investigation, including panel meetings with subpoena power for testimony or documents, in order to prepare a public report that determines the cause or causes of the incident (30 CFR 250.191).

BOEMRE is also authorized and required by the OCS Lands Act to conduct scheduled on-site inspections of oil and gas operations at least once a year, plus periodic on-site inspections without advance notice (OCS Lands Act, Section 22(c)(1) and (2)). It performs these inspections using a checklist called the Potential Incident of Non-Compliance (PINC) list. These on-site inspections complete the suite of current operator and regulator safety documentation offshore, which parallels the enforcement reporting used by NRC to drive its ASP program. The Incident Reporting Rule, PINCs, and other elements of offshore safety oversight are discussed in more detail in Section 4.

### *3.4 Sector Differences*

Despite the parallels between offshore and nuclear safety regulation, there are also differences to recognize. First and foremost is the thoroughgoing quantification that NRC has been able to introduce into its risk-informed oversight. Offshore regulation has a long way to go in this regard. The move underway toward safety case management, building on experience in the United Kingdom and Norway, is an important start. BOEMRE has published in the *Federal Register* a final rule requiring offshore oil and gas operators to develop and maintain a safety and environmental management system that makes mandatory the currently voluntary practices in the American Petroleum Institute’s Recommended Practice 75 (BOEMRE 2010; API 2004). These practices include, among other elements, a facility-level risk assessment. That assessment, however, consists largely of nonquantitative narrative; rigorous numerical risk estimation will need considerable development. A shift to risk quantification by the regulator, as with an ASP program, will encourage operators to develop their own risk quantification processes for their individual facilities. NRC’s quality assurance plan uses probabilistic risk assessment models developed by licensees for their individual facilities to review its own risk models and results.

Offshore risk quantification may be aided by the increasing availability of automated data flows to real-time operating centers maintained by operators as a “second set of eyes” onshore. This is a stream of immediate information from which a focused ASP program could cull signals of potential precursor events. Although proprietary considerations would need to be taken into account, this potential for quick, efficient, focused, nondiscretionary signaling would be worth exploring.

Another sector difference is the number and variety of regulated facilities: 104 commercial nuclear plants versus approximately 6,500 active leases, 3,400 active platforms, and 37,000 approved applications to drill in the Gulf of Mexico. Cultural differences may also be important; commercial nuclear operators all participate in the Institute of Nuclear Power

Operations, an industry-run safety improvement organization, and have the same insurer, whereas the oil and gas industry has not traditionally engaged in such self-oversight or pooling arrangements. The multitude of facilities and the individualism of operators are both likely to introduce more disparity in the offshore regulatory universe than is observed in the nuclear sector.

One area of similarity is the use the regulator can make of precursor results. The main objectives of the NRC program were discussed in Section 2. Accumulating knowledge about sources and magnitudes of risk enables more focused and up-to-date oversight. Results offshore can help evaluate proposed well designs and modification and waiver requests. The regulator can track sector trends over time. Monitoring of individual operations and operators' performance can trigger calibrated regulatory responses, from closer monitoring, stationing on-site, fines, warnings, and shut-ins of components or facilities, to facility abandonment, equipment or procedure disallowance, or operator banishment.

## 4. Current Regulatory Structure and Amenability to ASP

The ASP program in the nuclear sector is made possible by a mandatory incident reporting system (the licensee event report) that identifies accident precursors. Reports are filed for events that take place at any time, including operations, testing, and maintenance. NRC inspectors are stationed at each facility. Though not part of the ASP program, which is run by the agency's Office of Research, these inspectors, by virtue of their presence, enhance the safety culture at each plant.

A 2004 comprehensive review of the history and practice of the ASP program in the nuclear sector (Sattison 2004) concludes with a list of lessons learned that can be directly applied to a future program for offshore oil and gas. Paraphrasing this review, a comprehensive accident precursor program should accomplish three goals:

- Identify the nature of accident precursors for the industry and define precursor categories based on accident sequences determined from full-scope risk assessments for the entire range of facilities and systems.
- Prioritize or rank precursor categories based on both frequency of occurrence and risk significance. Ranking by frequency of occurrence for each category of precursor indicates the weaknesses in facilities at risk for accidents. Ranking by risk significance focuses attention on the precursor categories that are most threatening. Because the

analyses of these two ranking methods are quite different, the program should establish procedures and criteria for each.

- Feed the results back to the industry. Analysis is useless unless it is reflected in the design, operation, and maintenance of facilities and systems. Vulnerabilities must be addressed to reduce the frequency of occurrence and to increase resistance to the consequences.

To accomplish those goals, an accident precursor program should have the following characteristics:

- The program should be owned by a competent authority and should provide insights into improving safety in the future.
- The program must be supported by an appropriate infrastructure for gathering operational data and assuring that the authority has access to data providers when more detailed information is needed. Barriers to full and honest disclosure, such as proprietary information and fear of repercussions, must be addressed. Industry members must have incentives (either voluntary or by regulatory action) for participating.
- The program should provide a trending and tracking system to correlate changes in industry design and practices with changes in the occurrence and nature of observed precursors.
- Systems and methods should be sensitive enough to identify an operational event as a precursor without generating too many “false detects” of events of little interest.
- Risk assessment in the industry must be mature enough to instill confidence that potential accident sequences have been identified and that the models used to assess events are sufficient and only need changes that reflect the configurations and operating practices of specific facilities.
- Analysis should be performed on a continual basis by a consistent team of analysts to ensure the timeliness and consistency of results.

The next section provides a quick scan of the incident reporting systems in the offshore oil industry, to assess their compatibility with the reporting requirements of an ASP program.

### *4.1 Potential Incidents of Noncompliance*

In current practice, all information regarding a breach in the operational or safety system is logged on-site; the report is then read during annual inspections by a BOEMRE official. Inspectors use a list of PINCs to determine whether a facility is operating up to standard. If a breach exists, an operator is issued a notice, called Incident of Non-Compliance (INC), with a warning, component shut-in, or a facility shut-in with the possibility of a civil penalty. As in the nuclear sector, component testing is conducted on a regular basis, but the record of results stays with the operator and is shared with an inspector only during inspections; in the NRC regime, incidents are reported to the regulator at the time they occur.

INCs that may signal a precursor to a SUEH are listed below. These events can be recorded during inspection and further investigated by a regulator to identify accident precursors. In the current regulatory regime, these BOEMRE investigations of potential SUEH precursors may be the closest system in place that can provide the necessary information.

**INCs of Possible Relevance for Accident Sequence Precursors**

- Platforms and structures structural integrity
- Accident reporting following fatalities, injuries, lost time, evacuation, loss of well control, fires, explosions
- During unannounced oil spill drill, ability to carry out plan
- Observed oil discharges reported
- Casing setting depths more than 100 ft total vertical depth from the approved application for permit to drill
- Drilling suspended when safe margin between drilling fluid weight in use and equivalent drilling fluid weight at the casing shoe not maintained.
- Flared or vented oil well gas in excess of 48 continuous hrs or 144 cumulative hrs during month
- Pipeline properly maintained
- Pipeline-to-electrolyte potential measurements
- Pipeline hydrostatic tests
- Pipeline (component) repair
- Pipeline failure

- Well flow potential test
- Well tests reports
- Calibration reports
- Major equipment failure
- Cable, pipeline, facility damage
- Annual self inspections
- Report on annual self-inspections
- Incident involving fatalities, injuries, lost time, evacuation, fires, explosions, collisions, structural damages, crane incidents, safety system damages, personnel/material handling activities, firefighting systems, all incidents with damages > $25K.

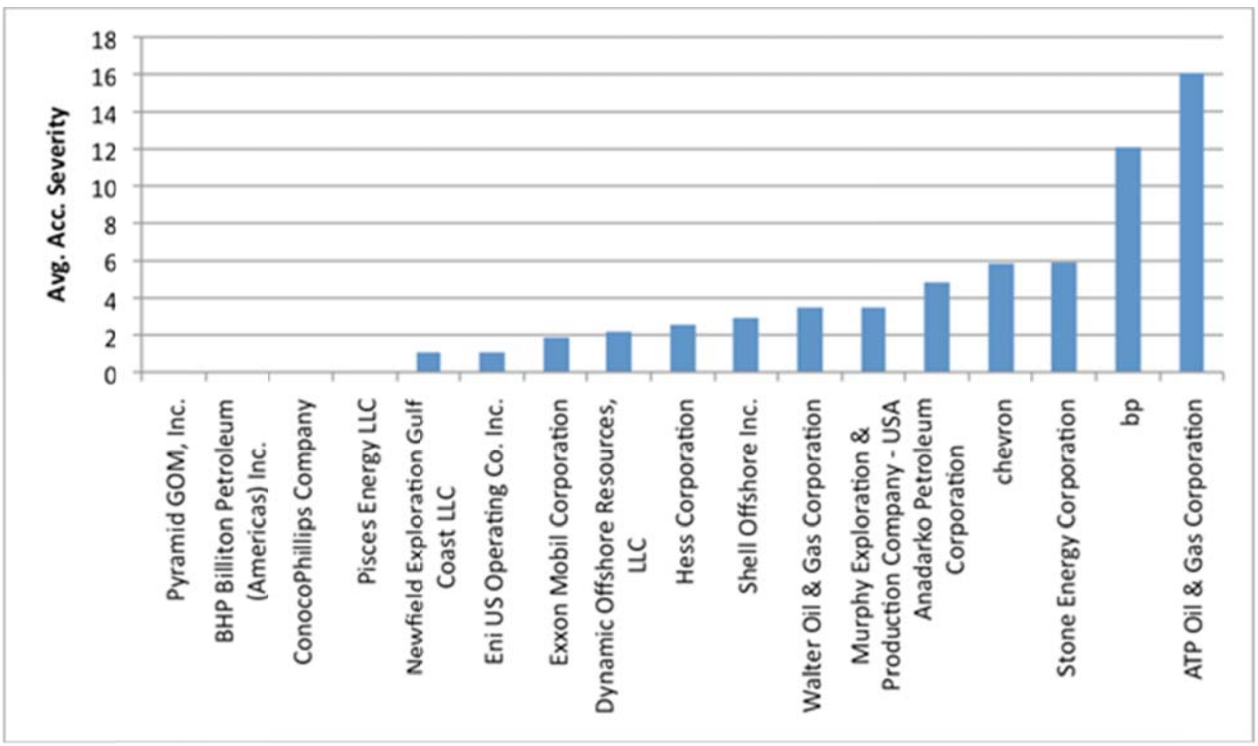
Using that list, inspectors may uncover accident precursors. However, the PINC system does not provide an ideal catchment, for these reasons:

- The precursors are discovered during the inspector's annual review of the logs, not reported by the operator when they occur.
- As noted in Section 2, unavailabilities and degraded conditions constitute a significant fraction of the nuclear precursors. It is not clear that unavailabilities discovered during routine testing and maintenance are always logged, especially if the discovery is accidental—as it often is.
- The great majority of the incidences of noncompliance would not be relevant for precursor analysis, and significant manpower effort is required to sift out the precursors. By comparison, in the ASP analyses for 2004 given in Appendix 2, 44 events were analyzed, leading to 17 accident precursors.
- The punitive nature of the PINC system discourages voluntary reporting of accidentally discovered unavailabilities.

For the above reasons, the PINC system is best suited to monitoring that required reporting mechanisms are in place and operational.

Accident and compliance data generated from this system are often used as a comparison measure for offshore operators (Slitor 2000). Although these values are useful in tracking operators' performance, they are not intended to measure the risk behind offshore drilling. For example, Figure 4 compares the average severity level per accident[2] for deepwater operators in the Gulf of Mexico. This measure reveals which operators experience the most severe accidents, but because an injury or fatality can be completely unrelated to a SUEH, as with a slip or fall off the platform, it cannot imply which operator poses the greatest risk of experiencing a SUEH. Similarly, incident investigations describe events leading to a SUEH but are not conducted for a simple unavailability or degraded condition that is necessary to quantify the risk. In the nuclear ASP program, licensee event reports are filed for all potential precursors with or without an initiating event (see Tables 2 and 3 in Appendix 2). Note that precursors with initiators include only one with a conditional core damage probability as high as $4 \times 10^{-5}$, whereas those without initiators have 3.

**Figure 4. Average Accident Severity per Deepwater Operator**




[2] The accident severity index is a measure created by BOEMRE and is calculated from the number of injuries, fatalities, the amount of property damage, and other factors. The higher the index, the more severe the accident.

### *4.2 National Response Center*

Any oil spill must be reported to the National Response Center, as stipulated in 30 CFR 254.46. These reports differ widely in format and scope; there are no uniform reporting guidelines. Event descriptions are sometimes anecdotal and derivative and do not analyze causes. Although this system can provide a valuable check on the completeness of other reporting conduits, it is not by itself capable of supporting an ASP program.

### *4.3 Incident Reporting*

In 2006, the Minerals Management Service revised its incident reporting requirements. The new Incident Reporting Rule (30 CFR 250.188) defines which incidents must be reported and broadens the scope of the reports, which must be submitted within 15 days. The following incidents fall under the mandatory reporting requirement:

- All fatalities.
- All injuries that require the evacuation of the injured person(s) from the facility to shore or to another offshore facility.
- All losses of well control. “Loss of well control” means the uncontrolled flow of formation or other fluids, whether to an exposed formation (an underground blowout) or at the surface (a surface blowout).
- Flow through a diverter.
- Uncontrolled flow resulting from a failure of surface equipment or procedures.
- All fires and explosions.
- All reportable releases of hydrogen sulfide (H2S) gas, as defined in §250.490(l).
- All collisions that result in property or equipment damage greater than $25,000. “Collision” means the act of a moving vessel (including an aircraft) striking another vessel, or striking a stationary vessel or object (e.g., a boat striking a drilling rig or platform). “Property or equipment damage” means the cost of labor and material to restore all affected items to their condition before the damage, including but not limited to the OCS facility, a vessel, helicopter, or equipment. It does not include the cost of salvage, cleaning, gas-freeing, dry docking, or demurrage.

- All incidents involving structural damage to an OCS facility. “Structural damage” means damage severe enough that operations on the facility cannot continue until repairs are made.
- All incidents involving crane or personnel- or material-handling operations.
- All incidents that damage or disable safety systems or equipment (including firefighting systems).

BOEMRE may decide to conduct an incident investigation under the authority of Sections 22(d)(1) and (2) of the OCS Lands Act (43 U.S.C. 1348(d)(1) and (2)). These are fact-finding proceedings with no adverse parties whose purpose is to prepare a public report that determines the cause or causes of the incident. Persons giving testimony may have legal representation.

The current incident reporting rule appears to provide an adequate vehicle from which to launch an ASP program. The following steps would lead to the establishment of an ASP-enabled incident reporting system:

1. Define the class of SUEH events.
2. On the basis of PRA models, design the set of generic event trees that have SUEH events as possible endpoints.
3. Ensure that all nodes in these generic event trees are captured in the incident reporting system, possibly requiring amendments to 30 CFR 250.188.
4. Design a control loop, possibly based on the PINC system, to ensure coverage of the incident reporting system, with appropriate sanctions for noncompliance.
5. Set up an analysis team within BOEMRE to map the SUEH-related incidents onto generic event trees.
6. Set up a review board consisting of industry and BOEMRE representatives.

The detailed design of an ASP-compliant incident reporting system melded with the current systems is outside the scope of this paper. Suffice to remark at this juncture that the nuclear ASP program has been greatly facilitated and streamlined by automated software support. At its inception, the nuclear ASP program involved an annual commitment of some five man-years. That has been reduced to about one man-year. Because the oil and gas offshore sector is much larger, the manpower requirements will surely be greater, but so will the efficiencies gained by automation.

## 5. Further Steps

A risk-informed regulatory regime requires a population-level, quantitative risk-monitoring capability owned and operated by the regulatory authority. The Accident Sequence Precursor methodology provides this capability. The existing legal framework appears adequate to establish an ASP program for offshore. Preconditions for successful implementation—in terms of history of operational experience, similarity of installations, and inspections baseline—appear to be met.

A prerequisite to any concrete steps toward deployment will be to conduct site visits with BOEMRE and with offshore industry, including operating companies, drilling companies and other service companies, to introduce the accident precursor methodology, encourage their input, and solicit their cooperation. Based on the results of these agency and industry interviews, developing an ASP program within the context of a risk-informed decision matrix for OCS activities will involve the following concurrent steps.

1. Develop one or more generic PRA models covering deepwater drilling and operations, as well as any shallow-water activities (drilling, operations, transport) that could pose significant risks to the public.
2. Incentivize operators to specialize and maintain their own site-specific PRA models and encourage a small group of industry leaders to form a users' group.
3. Create regulatory incentives for risk-informed regulation analogous to NRC's Maintenance Rule for the nuclear industry.
4. Design an ASP-enabled incident reporting system following the steps outlined in Section 4:
    a. Define the class of SUEH events.
    b. On the basis of PRA models, design the set of generic event trees that have SUEH events as possible endpoints.
    c. Ensure that all nodes in these generic event trees are captured in the incident reporting system, possibly requiring amendments to 30 CFR 250.188.
    d. Design a control loop, possibly based on the PINC system, to ensure coverage of the incident reporting system, with appropriate sanctions for noncompliance.
    e. Set up an analysis team within BOEMRE to map the SUEH-related incidents onto generic event trees.
    f. Set up a review board comprising industry and BOEMRE.

5. Design feedback mechanisms for involving industry in efforts to optimize industry-wide performance as measured by the ASP indicators.
6. Design an automation plan to streamline the ASP analysis.

Specifically, within a six-month period, a steering group capable of marshalling resources within BOEMRE and liaising with experts from industry could establish and coordinate two working groups. Group 1 would undertake tasks 1, 2, and 3. Creating an initial list of generic event trees (task 1) and developing actionable proposals (tasks 2 and 3) are achievable goals within six months. Group 2 would monitor task 1 of Group 1 while elaborating proposals for implementing tasks 4 and 5. The goal of automated reporting should inform and constrain the activities of both groups, for which purpose the steering group would ensure proper coordination. Whereas the development of automated reporting with attendant cost savings transpired over 30 years in the nuclear sector, a much shorter trajectory is necessary for BOEMRE because of the sheer volume of offshore activities.

## References

American Petroleum Institute (API). 2004. RP 75, Development of a Safety and Environmental Management Program for Offshore Operations and Facilities. Third Edition. May.

BOEMRE. 2010. Safety and Environmental Management Systems: Final Rule. *Federal Register* October 15. http://frwebgate1.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=lOmG2L/1/2/0&WAISaction=retrieve.

BP Incident Investigation Team. 2010. Deepwater Horizon Accident Investigation Report. September 8.

Cooke, R.M., and Goossens, L. 1989. The Accident Sequence Precursor Methodology for the Post-Seveso Era in Europe. *Reliability Engineering and System Safety* 27: 117–30.

Cottrell, W.B., J.W. Minarick, P.N. Austin, E.W. Hagen, and J.D. Haltis. 1984. Precursors to Potential Severe Core Damage Accidents: 1980-81, A Status Report. NRC Report NUREG/CR-359 I, Vols. 1 and 2 (ORNL/NSIC-217/VI and V2). Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, and Science Applications International Corp. July.

Danenberger, E.P. 1993. Outer Continental Shelf Drilling Blowouts, 1971-1991. Paper presented at 25th Annual Offshore Technology Conference, Houston, May 3–6.

Izon, D., E.P. Danenberger, and M. Mayes. 2007. Absence of Fatalities in Blowouts Encouraging in MMS Study of OCS Incidents 1992-2006. *Drilling Contractor* July/August.

Kadak, A.C., and T. Matsuo. 2007. The Nuclear Industry's Transition to Risk-Informed Regulation and Operation in the United States. *Reliability Engineering and System Safety* 92: 609–18.

Lewis, H.W., et al. 1978. Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission. NUREG/CR-0400.

Minarick, J.W. 1989. Revised LOOP Recovery and PWR Seal LOCA Models. Technical Letter Report ORNL/NRC/LTR-89/I I. Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, and Science Applications International Corp. August.

Minarick, J.W., and C.A. Kukielka. 1982. Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report. NRC Report NUREG/CR-2497 (ORNL/NOAC-232, Vol. 1 and 2). Union Carbide Corp. Nuclear Div., Oak Ridge National Laboratory, and Science Applications, Inc.

Minarick, J.W., et al. 1988. Precursors to Potential Severe Core Damage Accidents, 1986, A Status Report. NRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 5 and 6). Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, and Science Applications International Corp. May.

Modarres, M.L.E., and P. Amico. 1984. LER Categorization Report. Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, and University of Maryland, College Park. November 13.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. 2010. Charter. Washington, DC. July 15. http://www.oilspillcommission.gov/document/charter.

Sattison, M.B. 2004. Nuclear Accident Precursor Assessment: The Accident Sequence Precursor Program. Idaho National Engineering and Environmental Laboratory. http://www.riskinstitute.org/peri/images/file/NAE_89100.pdf.

SECY-06-0208. 2006. Status of the Accident Sequence Precursor Program and the Development of Standardized Plant Analysis Risk Models dated October 5, 2006. ADAMS Accession Number: ML061920242. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2006/secy2006-0208/2006-0208scy.pdf.

Sharples et al. 1989. "Jackup risk analysis reveals accurate hazard assessments," Offshore, PennWell Publishing Company, December, 1989.

Slitor, D. 2000. Measuring Safety and Compliance in the U.S. Offshore Oil and Gas Industry. Paper presented at Society for Petroleum Engineers conference, Stavanger, Norway, June 26–28.

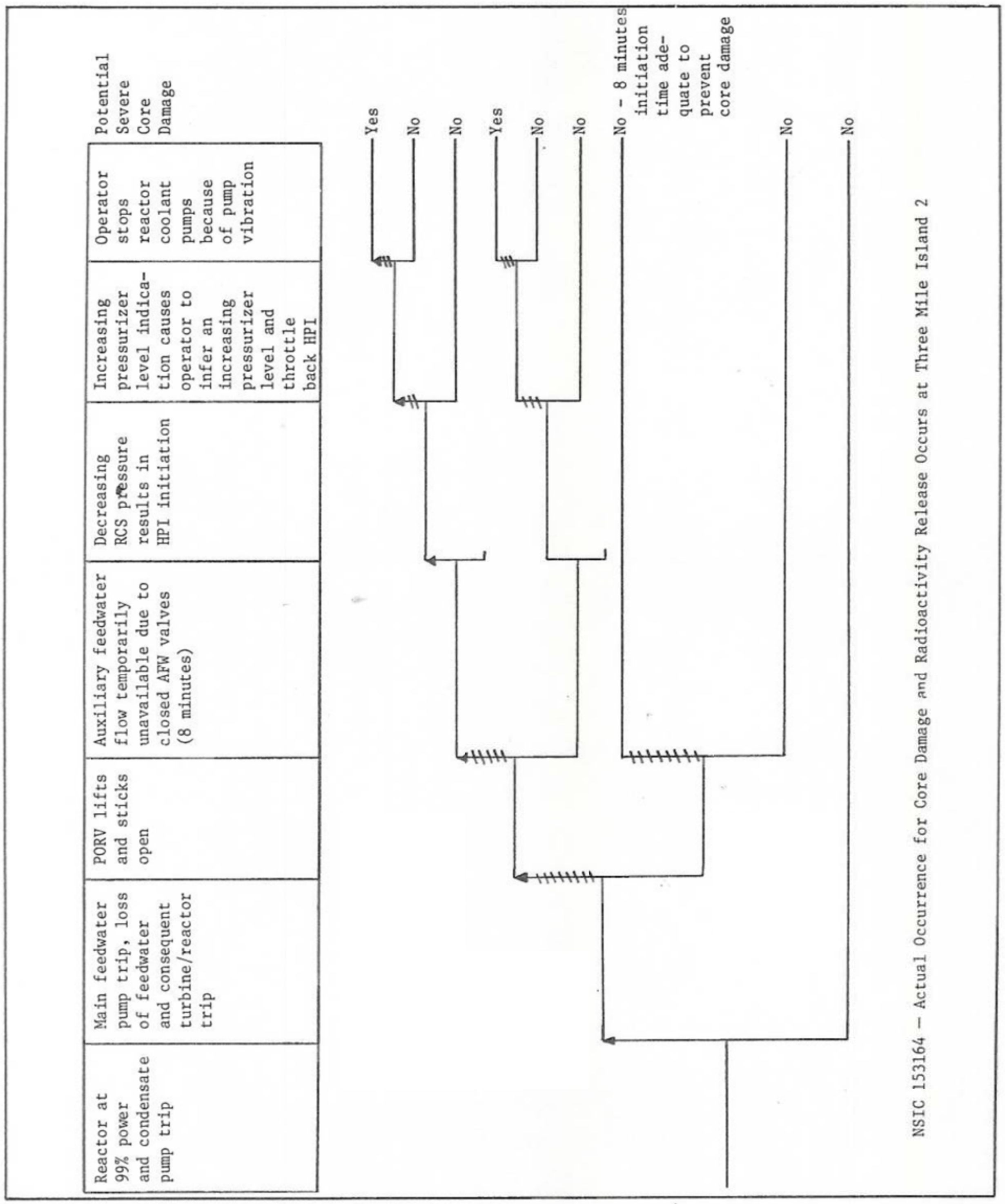
U.S. Nuclear Regulatory Commission. 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014). October. Available from National Technical Information Service, Springfield, VA 22161.

———. 1988. Individual Plant Examination for Severe Accident Vulnerabilities—10 CFR 50.54(f), generic letter 88-20. November 23.

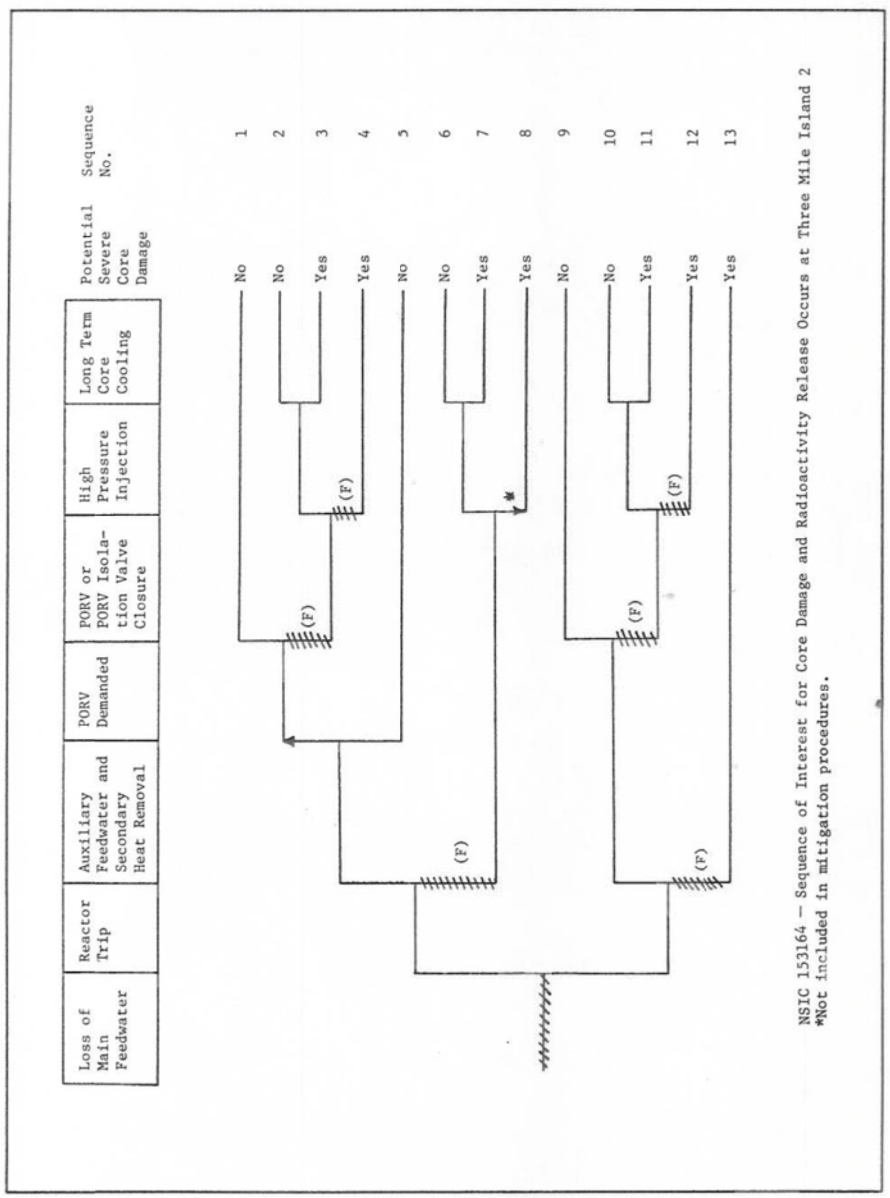
———. 1991. 10 CFR 50: Monitoring the Effectiveness of Maintenance at Nuclear Power Plants. *Federal Register* 56 FR 31306. July 10.

## Appendix 1. Three Mile Island Event Trees

**Figure 1. Precursor Event Tree for 1979 TMI Accident**



## Figure 2. Generic Event Tree for TMI-2 Precursor



## Appendix 2. Nuclear Sector Analysis and Review

The following tables are from "Status of the Accident Sequence Precursor Program and the Development of Standardized Plant Analysis Risk Models," dated October 5, 2006 (SECY-06-0208. 2006).

NRC staff members have sought to improve the timeliness of ASP analyses by streamlining the analysis and review processes. The analysis process now includes results from the "Significance Determination Process (SDP) and Management Directive (MD) 8.3, NRC Incident Investigation Program," when practicable, to avoid duplication of analyses and inconsistent outcomes. The review process has been changed to reduce the number of ASP analyses that undergo formal peer review, thereby reducing administrative and review burdens on staff and licensees for cases where formal peer reviews are considered of minimal value. However, rigorous independent reviews will continue to be performed by ASP program analysts.

**Table 1.** Status of ASP analyses (as of September 30, 2006).

| Status | FY 2004 | FY 2005 | FY 2006[a] |
|---|---|---|---|
| Analyzed events that were determined not to be precursors | 27 | 32 | 2 |
| Events to be further analyzed | -- | -- | 50 |
| ASP precursor analyses | 15 | 7 | –[b] |
| SDP (or MD 8.3) results used for ASP program input | 2 | 8 | –[b] |
| Total precursors identified | 17 | 15 | -- |

a. As of September 30, 2006, the staff has not yet screened all of the FY 2006 events and unavailabilities.
b. Based on historical data, expectations are that approximately 40 percent of ASP precursors will use SDP or MD 8.3 results.

**Table 2.** FY 2004 precursors involving initiating events (as of September 30, 2006).

| Event Date | Plant | Description | CCDP |
|---|---|---|---|
| 1/23/04 | Calvert Cliffs 2 | Reactor trip caused by loss of main feedwater and complicated by a failed relay causing overcooling. ***LER 318/04-001*** | $2\times10^{-6}$ |
| 5/5/04 | Dresden 3 | Plant-centered LOOP due to breaker malfunction. ***LER 249/04-003*** | $3\times10^{-6}$ |
| 6/14/04 | Palo Verde 1 | Grid-related LOOP with offsite power recovery complications due to breaker failure. ***LER 528/04-006*** | $9\times10^{-6}$ |
| 6/14/04 | Palo Verde 2 | Grid-related LOOP with an emergency diesel generator unavailable. ***LER 528/04-006*** | $4\times10^{-5}$ |
| 6/14/04 | Palo Verde 3 | Grid-related LOOP with offsite power recovery complications due to breaker failure. ***LER 528/04-006*** | $9\times10^{-6}$ |
| 9/25/04 | St. Lucie 1 | Severe weather LOOP caused by Hurricane Jeanne while the plant was shut down. ***LER 335/04-004*** | $1\times10^{-5}$ |
| 9/25/04 | St. Lucie 2 | Severe weather LOOP caused by Hurricane Jeanne while the plant was shut down. ***LER 335/04-004*** | $1\times10^{-5}$ |

**Table 3.** FY 2004 precursors involving degraded conditions (as of September 30, 2006).

| Event Date[a] | Condition Duration[b] | Plant | Description | ΔCDP |
|---|---|---|---|---|
| 11/3/03 | since plant startup | Surry 1 | Potential loss of reactor coolant pump (RCP) seal cooling due to postulated fire damage to emergency switchgear. ***LER 280/03-005*** | $1\times10^{-6}$ |
| 11/3/03 | since plant startup | Surry 2 | Potential loss of RCP seal cooling due to postulated fire damage to emergency switchgear. ***LER 280/03-005*** | $1\times10^{-6}$ |
| 1/4/04 | 720 hours | Brunswick 2 | EDG "3" unavailable due to jacket water leak. ***LER 325/04-001*** | $2\times10^{-6}$ |
| 2/3/04 | since plant startup | Turkey Point 3 | Triennial fire protection issues. ***LER 251/04-007*** | $7\times10^{-6}$ |
| 2/3/04 | since plant startup | Turkey Point 4 | Triennial fire protection issues. ***LER 251/04-007*** | $7\times10^{-6}$ |
| 2/19/04 | 61 hours | Palo Verde 2 | Failure to implement design of steam generator nozzle dam requiring an extended time in reduced RCS inventory configuration. ***IR 529/04-04, IR 529/04-09*** | $1\times10^{-5}$ |
| 3/17/04 | 1117 hours | Peach Bottom 3 | High-pressure coolant injection (HPCI) unavailable due to failed flow controller. ***LER 278/04-001*** | $2\times10^{-6}$ |
| 7/31/04 | 11 years[c] | Palo Verde 1 | Containment sump recirculation potentially inoperable due to pipe voids. ***LER 528/04-009*** | $4\times10^{-5}$ |
| 7/31/04 | 11 years[c] | Palo Verde 2 | Containment sump recirculation potentially inoperable due to pipe voids. ***LER 528/04-009*** | $4\times10^{-5}$ |
| 7/31/04 | 11 years[c] | Palo Verde 3 | Containment sump recirculation potentially inoperable due to pipe voids. ***LER 528/04-009*** | $4\times10^{-5}$ |

a. ASP event date is the discovery date for a precursor involving a degraded condition.
b. Condition duration is the time period when the degraded condition existed. The ASP Program limits the analysis exposure time of degraded condition to 1 year.
c. Exact date not given. LER states that condition had existed since 1992 when the new feedwater control system was installed before the power uprate.

CCDP = conditional core damage probability

LER = licensee event report