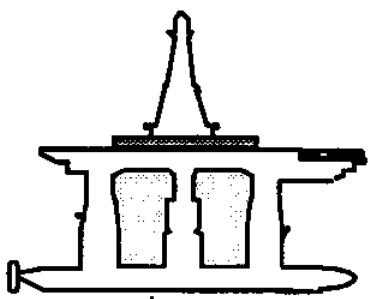
MANAGEMENT OF HUMAN ERROR IN OPERATIONS OF MARINE SYSTEMS



Modeling the Effects of Human Errors From Post-Mortem Marine Casualty Studies

by

William H. Moore

&

Robert G. Bea

Report No. HOE-92-4
August, 1992

Department of Naval Architecture & Offshore Engineering
University of California, Berkeley

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Modeling the Effects of Human Errors From Post-Mortem Marine Casualty Studies

by

William H. Moore
Department of Naval Architecture & Offshore Engineering
University of California at Berkeley

&

Robert G. Bea
Professor, Department of Naval Architecture & Offshore Engineering
and Civil Engineering
University of California at Berkeley

1.0 INTRODUCTION

Approximately 65% of catastrophic marine related accidents (e.g. *Exxon Valdez* and *Piper Alpha*) are the result of compounded human and organizational errors (HOE) during operations. Yet to date there is no structured quantitative approach to assist engineers, operators, and regulators of marine systems to design human and organizational error (HOE) tolerant systems. No considerations have been established to include human and organizational errors as an integral part of the design, construction, and operation of tankers and offshore structures [Bea & Moore, 1991].

Analyses of post-mortem accident studies lead to a greater understanding of the effects of HOE in accident sequences. This report establishes a methodology for formulating qualitative and quantitative models to identify and correlate the impacts of human factors on marine casualties. In addition, the model developments assist engineers, operators, and regulators in determining HOE management alternatives in developing future operating policy and procedures. These methodologies are applied to two well-documented case studies: the grounding of *Exxon Valdez* and the *Piper Alpha* disaster. The models are used as a framework to construct general models for two classes of marine accidents: tanker groundings and process leaks during simultaneous production and maintenance on platforms. Examples for evaluating recommendations and newly developed operating procedures are evaluated for both models.

2.0 BACKGROUND

Development of accident framework models is the third of five tasks proposed by the Joint Industry Project *Management of Human Error in Operations of Marine Systems.* The purpose of these tasks are to:

(1) Identify, obtain and analyze well documented case histories and databases of tanker and offshore platform accidents whose root causes are founded in HOE.

(2) Develop an organizational classification framework for systematically identifying and characterizing the various types of HOE.

(3) Develop general analytical frameworks based on real-life case histories to characterize how the HOE's interact to cause accidents. The case histories are post-mortem studies (*Exxon Valdez* and *Piper Alpha* disasters) and existing operations (tanker loading & discharge and offshore crane operations).

(4) Formulate quantitative analyses for the case histories based on probabilistic risk analysis (PRA) procedures using influence diagrams. Perform quantitative analyses to verify that the analyses can reproduce the results and implications from the case histories and general statistics of marine accidents.

(5) Investigate the effectiveness of various alternatives to reduce the incidence and effects of HOE. Evaluate the costs and benefits in terms of risk reduction (products of likelihood and consequences).

The *Management of Human Error In Operations of Marine Systems* project is int he process of examining the effects of HOE in two forms: post-mortem studies (*Exxon Valdez* and *Piper Alpha* disasters) and current operation studies (loading & discharge of tankers and crane accidents for offshore platforms). The objective of this report is to examine the development of accident framework models using post-mortem studies. Model developments for current operating case studies for HOE analyses are the subject of a future project report.

The *Exxon Valdez* and *Piper Alpha* disasters have been selected as the case histories for HOE analyses. The choices were based upon the quality, completeness, accessibility, and availability of information related to the accident sequences. The grounding of *Exxon Valdez* and subsequent spill resulted in the passage of the Oil Pollution Act of 1990 (OPA 90) mandating limitations in crew workhours, studies in navigation, requirements for tanker tug escorts, construction of double-hull tankers, and other requirements. The *Piper Alpha* disaster has resulted in 106 specific recommendations [United Kingdom Department of Energy, 1990] leading to changes in United Kingdom Offshore Continental Shelf (OCS) legislation and regulations which are estimated to take from two to five years to implement [McIntyre, 1991]. The *Piper Alpha* disaster

has also led to reassessments of offshore design and operations in U.S. OCS waters [Institute of Marine Engineers, 1991].

Further analysis of these regulations and recommendations lead to assessing their practicality in potentially reducing the risks and/or consequences of catastrophic marine accidents. Current changes in operational procedures resulting from accident analyses may elevate the operational system from a specific class or type of error involved in that accident. However, unforeseen or latent problems may be the result of the new procedure or policy. For example, the *Oil Pollution Act of 1990* (OPA 90) requires all new U.S. flagged tanker builds to be double-hulled to reduce the consequences of hydrocarbon spills in the event of collision or grounding (allision). The decrease in vessel capacities (as much as 40%) result in a demand for additional vessels to keep pace with demand potentially leading to a greater rate of vessel collisions [Bea & Moore, 1992].

Two preliminary studies were conducted on both the *Exxon Valdez* and *Piper Alpha* disasters to establish a framework from which to examine the primary human, organizational, and technological contributions to the accidents and form the basis for which to construct qualitative and quantitative models [Paté-Cornell, 1992; Roberts & Moore, 1992]. These studies and their respective accident reports form a basis for the post-mortem models discussed in this report.

3.0 POST-MORTEM STUDIES FOR ACCIDENT ANALYSES

The report by Moore & Bea (1992) discusses the levels at which safety information data is obtained and analyzed. Accident and incident reports (post-mortem studies) are the most commonly available and used data sources for tanker and offshore platform operations. Figure 1 shows the levels of safety information from examination of both error types and tokens [Reason, 1992]. Nevertheless, human and organizational errors through post-mortem analyses have both advantages and drawbacks. These advantages and drawbacks are both qualitative (examination of accident sequences, investigative biases, etc.) and quantitative (e.g. probabilistic updating of system failure rates) in nature. The following insights into the advantages and drawbacks of post-mortem analyses lead to the conclusion of the importance in integrating case study knowledge (accident trends in case study analyses) with theories regarding the underlying causes of accident events (assessing contributing causes in accident trends).

3.1 Advantages of post-mortem studies for HOE analyses

The importance of post-mortem studies in marine casualty studies are the following:

(1) *Intensive studies of a single case can reveal the influences and correlation of underlying and contributing, direct, and compounding causes to a complex set of accident events over time* [Reason, 1990]. Case studies are a method of examining prevailing circumstances and conditions (environment or operational) unique to a specific accident scenario which may otherwise be difficult to capture (*20/20* hindsight).

(2) *Post-mortem studies may reveal classes of accident causing factors or scenarios which may have been latent or overlooked* [Paté-Cornell, 1992]. For example, the complex interactions of causes and events surrounding the *Piper Alpha* disaster could easily been overlooked or suggested as so remote that is disregarded as a potential accident scenario. Post-mortem studies of *Piper Alpha* have revealed many of the sub-system failures not otherwise noticed [Paté-Cornell, 1992; Institute of Marine Engineers, 1991; United Kingdom Department of Energy, 1988, 1989, 1990].

(3) *Post mortem studies provide valuable information for probabilistic updating of system failure rates conditional upon human, organizational, conditional and prevailing contributing factors* [Paté-Cornell, 1992]. Bayesian updating (conditional probabilities) are an important quantitative component to the analysis of overall failure rates of the systems in light of the scarcity of accident and incident data in the marine industry [Bea & Moore, 1991; Laroque & Mudan, 1982].

3.2 Drawbacks of post mortem studies for HOE analyses

Though post-mortem studies provide valuable insight into examining HOE in marine casualties, the following limitations exist:

(1) *Post-mortem studies do not capture all factors involved in an accident or incident sequence* [Reason, 1990]. Casualty studies do not necessarily include complete and accurate information which is available. Unlike the aviation industry, near miss data is virtually non-existent in the tanker and offshore platform industries [Moore, 1991]. Reports can be biased towards the experiences of the investigative parties. The information may be incomplete or not entirely capture the complex set of circumstances, actions, decisions, and causes surrounding an accident sequence. In addition, post-mortem studies or accident reports can be biased towards examining problems which can be comparatively easy to addressed than more critical underlying problems. For example, many accident reports tend to focus on technical problems and fixes, retrofixing of systems or disciplining of personnel rather than address more underlying contributing HOE factors.

(2) *Many accident reports primarily focus on attributing blame* [Reason, 1990; Paté-Cornell, 1992]. Marine casualty investigations should not be directed at assessing blame, but focus on providing greater insight into the interactions between circumstances, events, decisions, and causes of HOE. Catastrophic marine accidents are the cumulation of compounded factors contributed by parties across organizational levels over an extended period of time. Assessing blame tends to draw focus away from the primary goal of determining HOE management alternatives by reducing risks and/or consequences of a marine operating system.

(3) *Focus on determining the probability of failure of a unique set of circumstances surrounding an accident after the fact can lead to inaccurate assessments of risk* [Paté-Cornell, 1992]. Low probability - high consequence technologies are statistically vulnerable to low probability estimates of system failures [Freudenburg, 1988]. Post-mortem study analyses should focus on probabilistic modeling and assessments of classes of accidents, not on specific cause and event sequences which are unique to a documented case study due to the lack of specific patterns and trends [Reason, 1992]. Though, the analyses of series of post-mortem studies can lead to insight into accident trends and error management alternatives. There are currently no formal updating scheme in which historical data of particular accident sequences are used to obtain posterior distributions of parameters leading to the accident event [Oliver & Yang, 1990].

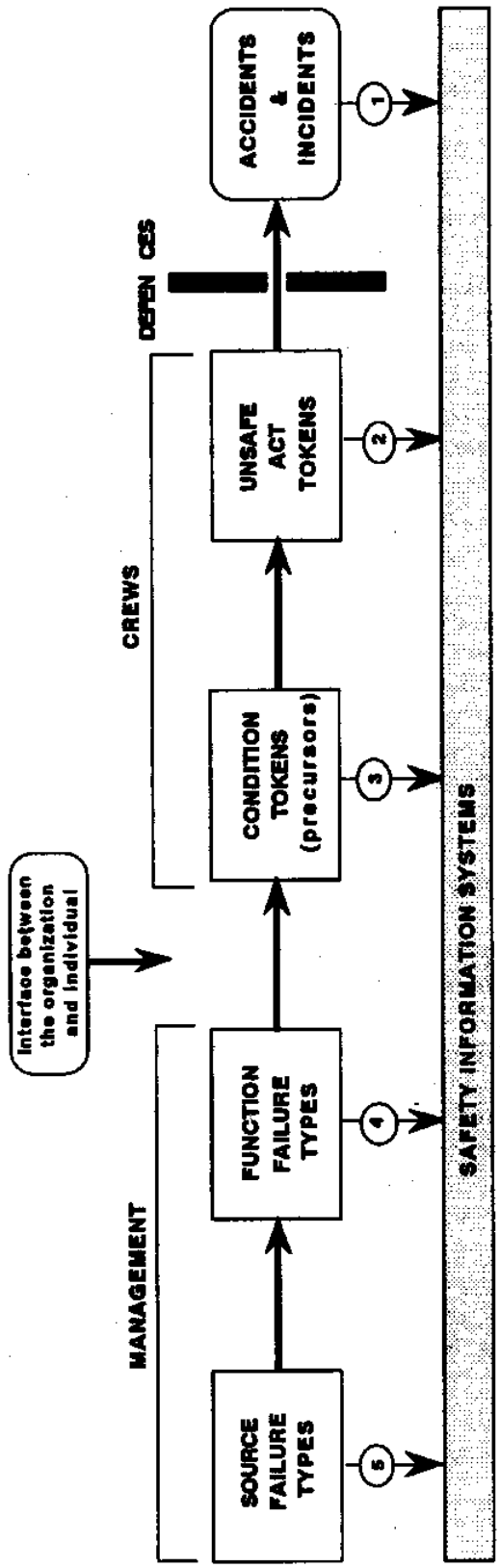


Figure 1: The basic elements of safety information system as they relate to the type-to-token stages involved in accident causation. [Reason, 1992]

4.0 DEVELOPING ACCIDENT FRAMEWORK MODELS FROM POST-MORTEM STUDIES

As mentioned in Chapter 3, the use of post-mortem studies as a source of information to construct accident model frameworks have both advantages and disadvantages. This chapter discusses a systematic method in which to model specific HOE related events, decisions, and actions are used to formulate models of classes of marine accidents (e.g. vessel groundings or collisions, high pressure gas fires aboard production platform, or simultaneous production and maintenance, etc.). Chapters 5 further develop the modeling framework using the *Exxon Valdez* and *Piper Alpha* disasters as case study examples.

Four principle steps are involved in the developments of a post-mortem study model: (1) structuring the relevant events, decisions, and actions specific to the accident scenario, (2) applying human and organizational error classifications to identify contributing HOE factors, and (3) development of a model representative of a "class of accidents" of which the post-mortem case study was related, and (4) determining a general set of contributing HOE causes related to actions, decisions and events leading to the particular class of accidents.

4.1 Establishing Frameworks for Classes of Accident Models

The intent of the project is to develop (and verify) PRA models for operations of tankers and offshore platforms to include the reliability effects of human and organizational factors. The general method is to integrate elements of process analysis and organizational analysis in assessing the probability of system failure [Bea, 1989; Patè-Cornell & Seawell, 1988; Patè-Cornell & Bea, 1989]. Figure 2 provides a schematic description of the structure of this integration model. The first phase (which does not appear in this diagram) is a preliminary *probabilistic risk analysis* (PRA) to identify the key subsystems or elements of the system's reliability. The second phase is an analysis of the process to identify the potential problems for each of the subsystems and their probabilities or base rates per time unit or per operation.

Given that a basic error occurs, the next phase is an analysis of the organizational procedures and incentive system to determine their influence on the occurrence of basic errors and the probability that they are observed, recognized, communicated, and corrected in time (i.e., before a system failure event).

The basis for developing accident model frameworks has been established by Paté-Cornell (1992). The risk analysis model is extended to include relevant decisions, actions and organizational features in the risk assessment and risk management. Figure 3 is a hierarchical representation of the root causes behind systems failures. The primary level represents basic events affected by decisions and actions influenced by organizational policy, procedure and culture. This procedure requires the modeler(s) to establish an exhaustive set of contributing events and determine relevant decisions and actions specific to the class of accidents of interest (explosions, fires, groundings, collisions, etc.).

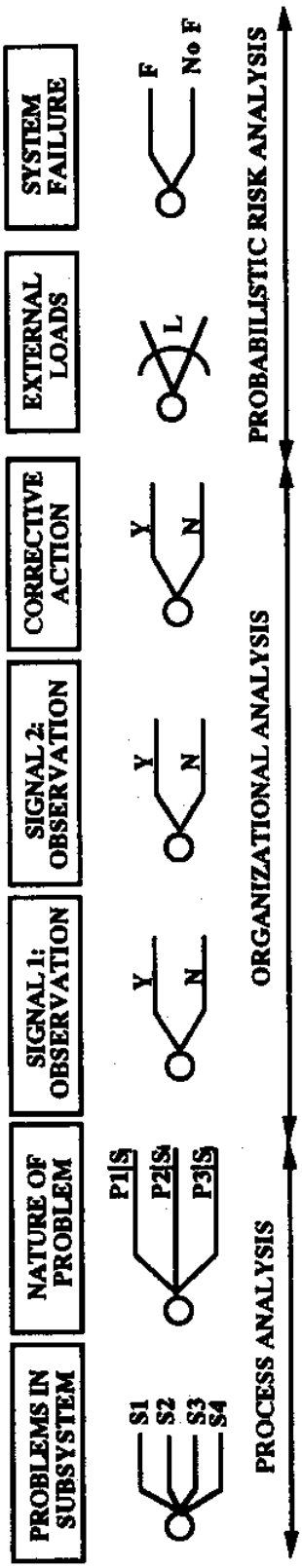


Figure 2: Structure of the generalized reliability model including organizational features and error detection [Paté-Cornell & Bea, 1989]

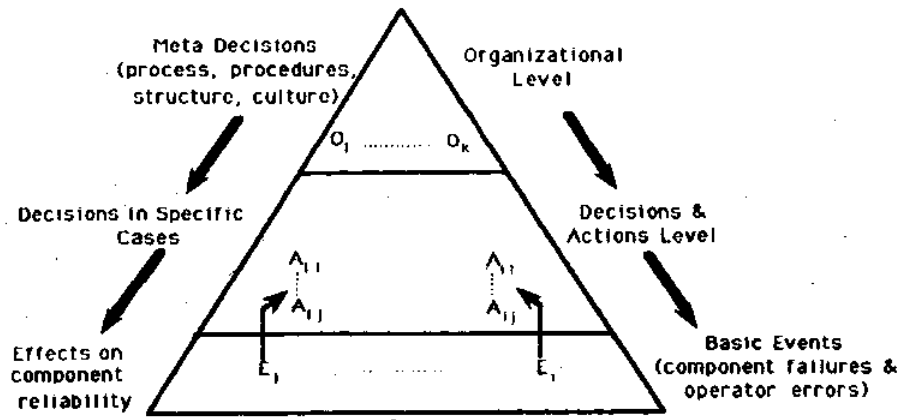


Figure 3: Hierarchy of root causes of system failures: Management decisions, human errors, and component failures [Paté-Cornell, 1992]

A probabilistic model of the process includes determining the set of possible initiating accident events (in_i) and final states ($fist_m$) of the system. The probability of loss of components (platform, vessel, revenue, life, injury, etc.) to the system can then be represented by:

$$p(loss_k) = \sum_i \sum_m p(in_i)\ p(fist_m|in_i)\ p(loss_k|fist_m) \qquad \forall\ k. \tag{1}$$

($\forall\ k$: "for all values of k")

The model is expanded to include relevant decisions and actions (A_n) constituting an exhaustive and mutually exclusive set of decisions or actions affecting the marine system at different stages during the lifetime of the vessel or platform. These decisions and actions can be examined from the front-line operating crew level through to top-level management.

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n)\ p(in_i|A_n)\ p(fist_m|in_i, A_n)\ p(loss_k|fist_m, A_n) \quad \forall\ k. \tag{2}$$

The effects of organizational procedures and policies on the risk are determined through examining the probabilities of the actions and decisions conditional on relevant organizational factors (O_h). The probabilities of various degrees of loss can be examined conditional upon different contributing organizational factors. Further developments into the quantitative aspects of HOE is the subject of a future report.

$$p(loss_k|O_k) = \sum_i \sum_m \sum_n p(A_n|O_k)\, p(in_i|A_n)\, p(fist_m|in_i, A_n)\, p(loss_k|fist_m, A_n) \qquad (3)$$

4.2 Influence Diagrams

One such method of developing accident framework models for PRA analysis is through the use of *influence diagrams*. Influence diagramming is a form of PRA modeling which allows greater flexibility in examining HOE and HOE management alternatives. There are distinct advantage for using influence diagramming as an alternative to standard event/fault tree analyses. Influence diagrams are used to organize conditional probability assessments required to determine unconditional probabilities of failures of specified target events [Phillips, *et al.*, 1990]. In standard decision tree analysis, decisions are based on all preceding aleotory and decision variables [Howard & Matheson, 1981]. However, not all information is necessarily available to a decision maker. In addition, information may come from indirect sources or not the specific order in which the decision tree is modeled. It is not necessary for all nodes be totally ordered in an influence diagram. This allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagram modeling [Howard & Matheson, 1981].

As described by Howard (1990), the components of an influence diagram are: (1) *decision* and *chance nodes*, (2) *arrows*, (3) *deterministic nodes*, and (4) *value nodes*. Shown in Figure 4, decisions are represented by square nodes which can be a continuous or discrete variable or set of decision alternatives. Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes can be continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node signify that the probability assignments of the node are conditional upon the node from which the arrow originated. Deterministic nodes are those in which outcomes depend deterministically upon its predecessors. A value node is designated by the author to be: "the quantity whose certain equivalent is to be optimized by the decisions" of which only one node may be designated in the diagram. These nodes are represented by a rounded edge double-border rectangle. A description of influence diagrams are discussed in Howard & Matheson, 1991.

4.3 Structuring Relevant Events, Decisions and Actions: An Influence Diagram Representation

To establish the set of events which have occurred in a specific accident sequence, the modeler may wish to construct a preliminary influence diagram representation of the accident. The preliminary model representation is not an influence diagram per se, but a representation of the specific events, actions, and decisions which occurred during the accident event. The purpose of the preliminary model is to assist the user in establishing the relevant contributing factors unique to the specific accident sequence [see Figures 13 and 16]. No probabilistic assessments are made from the preliminary model. In addition, it can assist the user in identifying critical areas where: (1) further

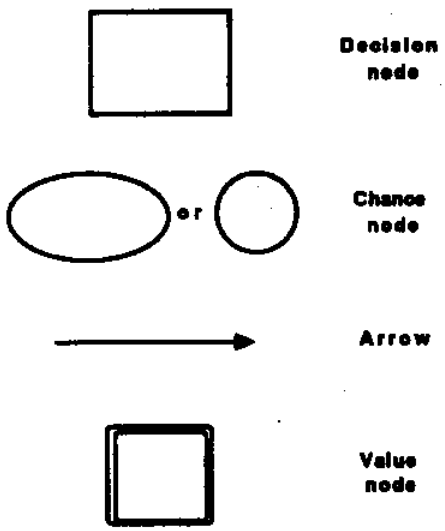


Figure 4: Influence diagram characterizations

detailed studies may be warranted, or (2) if properly managed or controlled, could have reduced the risk or consequences of the accident.

As shown in Figure 5, the modeling process begins with a specific accident model formulation and results in the development of an influence diagram model for a particular class of accidents. The influence diagram models encompass the class of accidents in which the post-mortem model is a representative. The development of influence diagram models (and preliminary model representations) should be the effort of a group of experts. Discussion of differences in opinion of relationships between events and their causes illicit the development of more realistic models [Phillips, *et al.*, 1990]. The models are developed through an iterative process discussed between experts to determine relavant influences and correlations between subsystems and operations.

The modeling process follows the same method discussed by Paté-Cornell (1992). This includes the structuring of a target event (e.g. platform fire, vessel grounding, etc.) which is the final result of contributing events, decisions, and actions. The first step is to develop a model representing dependencies between relevant events. Events can be categorized into three states:

(1) *Contributing/underlying events*: The set of events which lead to an initiating accident event. Contributing/underlying events are those occurring prior to the initiating accident event contributing to the reduction of reliability or increase of risk for the system. For example, a tanker departing from a traffic separation scheme (*Exxon Valdez*) or an offshore platform simultaneously producing and conducting production process maintenance (*Piper Alpha*).

(2) *Initiating/direct accident events*: The immediate accident event(s) resulting in the casualty. For example, a tanker grounding or the initial explosions aboard a production platform subsequently lead to a compounding of events (e.g. oil spill, loss of life and platform).

(3) *Compounding events*: The progression of events which lead to compounding of accident consequences. For example, attempting to dislodge *Exxon Valdez* from Bligh Reef after grounding results in a larger spill, or increasing the flow of gas from satellite platforms *Claymore* and *Tartan* to *Piper Alpha* thus fueling the fire.

Examples of the influence of events in accident sequences for tanker and offshore production platform are shown in Figure 6. For the tanker, the underlying/contributing event is the vessel deviating from the traffic separation scheme. The initiating/direct accident event is the vessel grounding, and the compounding event is dislodging the vessel from the rocks. Similarly, a diagram representation for simultaneous production and maintenance leads to an initial explosion and consequently loss of life and platform. These examples are explored further in the following chapters.

The next step is to establish contributing decisions and actions influencing the set of accident events. The dependencies between events, decisions and actions are represented by arrows leading from decisions and actions to relevant events as shown in Figures 7 and 8 for the tanker and offshore platform examples.

The final step entails expanding the diagram to include the influences of HOE factors and operating environmental conditions upon events, decisions and actions (see Figures 9 and 10). Moore & Bea (1992) have developed an HOE taxonomy for addressing contributing HOE factors and environmental operating conditions. Environmental conditions (temperature, waves, smoke, fire, etc.) can potentially influence events, decisions, actions and human and organizational errors. For example, crews operating in high noise environments (e.g. tanker engine room or platform production module) are subject to errors in communication due to the inability to hear verbal exchanges of information between individuals.

4.4 Developments of Influence Diagrams: Templates for Further HOE Analyses

One of the keys to the development of an effective models is to determine the goals and preferences of the user. For example, tanker or offshore platform operators may wish to establish models that enable them to focus on specific areas to allocate limited resources. These goals and preferences may be established in the model to examine the effects of the operating alternatives as the driving force by balancing safety, economic, and production costs and benefits. On the other hand, regulators and policy makers may wish to establish environmental, economic and social risks and costs of specific tanker and offshore operations. In short, the models would vary to project the preferences of the user in examining costs and benefits of these operations.

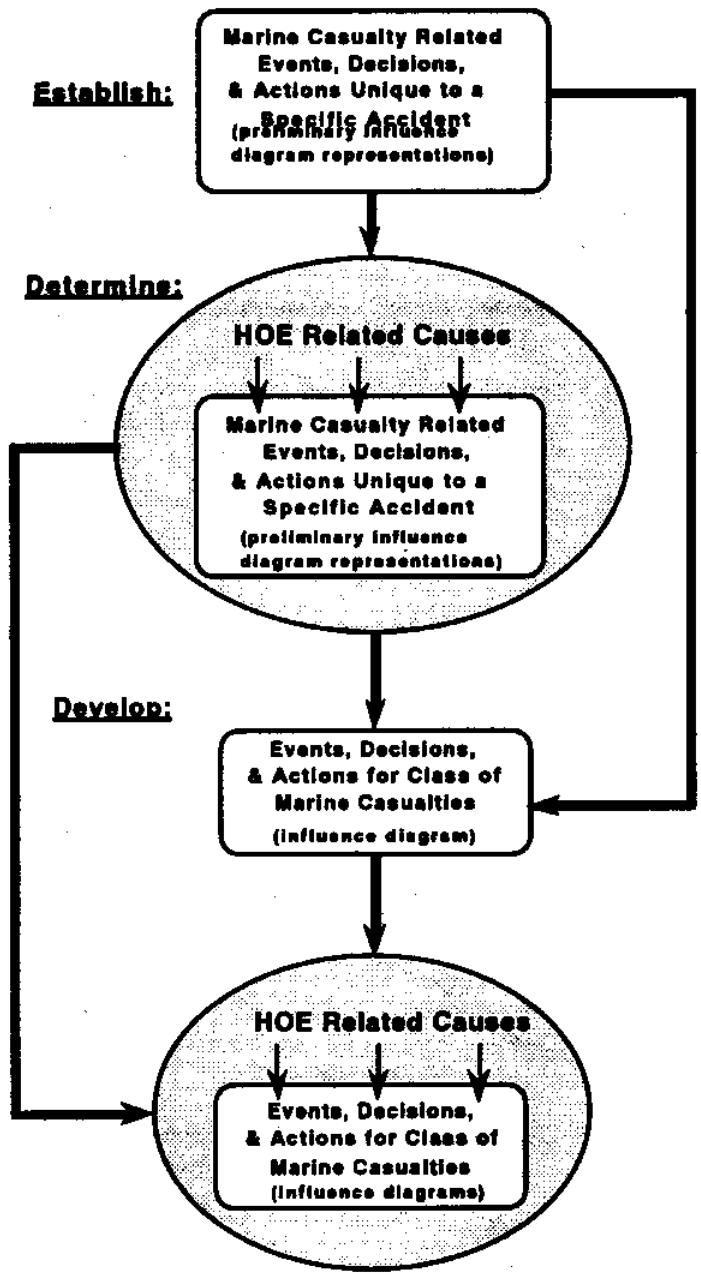


Figure 5: Flowchart of post-mortem studies in developing accident framework models

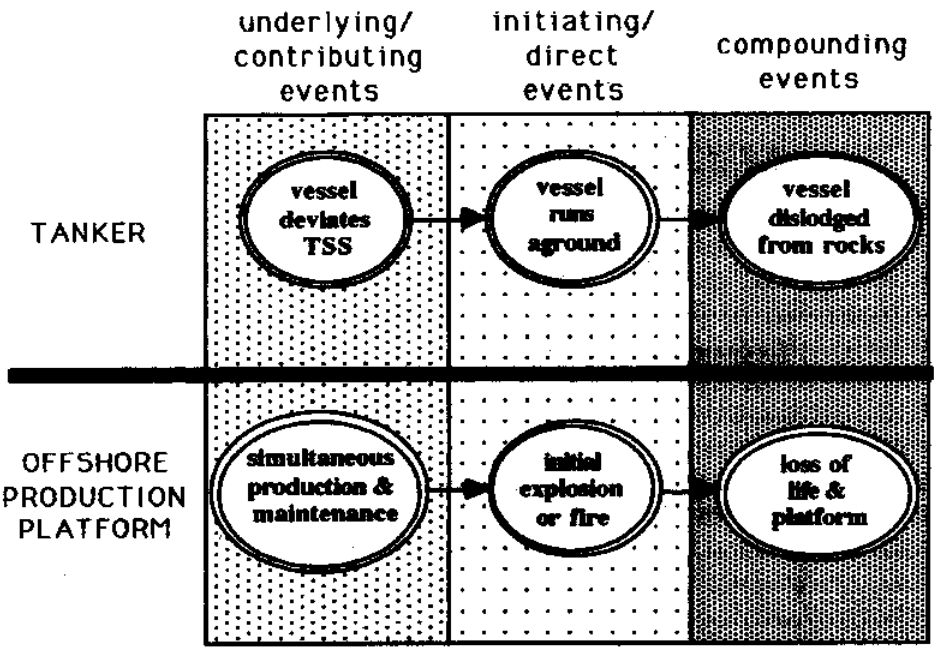


Figure 6: Examples representing progression of accident events

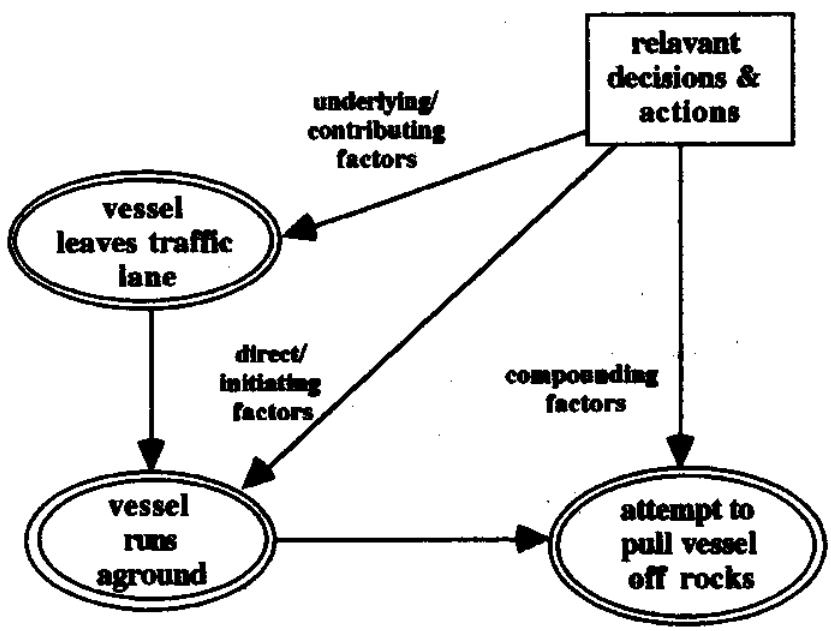


Figure 7: Accident event dependencies upon relevant decisions and actions for tanker grounding [Moore & Bea, 1992]

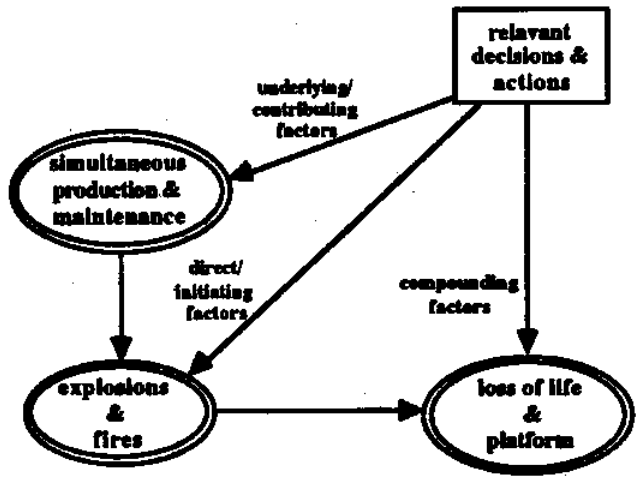


Figure 8: Accident event dependencies upon relevant decisions and actions for production platform fire while conducting maintenance [Moore & Bea, 1992]

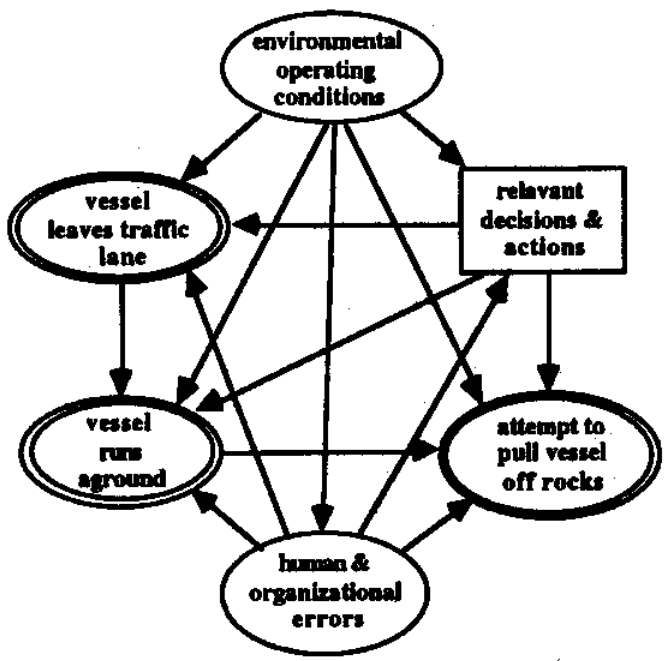


Figure 9: Accident event dependencies upon relevant decisions, actions, environmental conditions, and HOE factors for tanker grounding

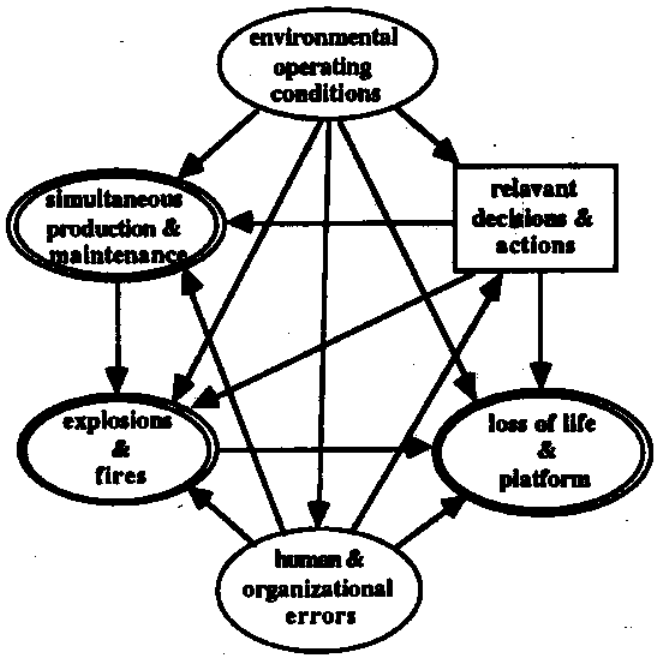


Figure 10: Accident event dependencies upon relevant decisions, actions, environmental conditions, and HOE factors for production platform fire while conducting maintenance

The complexity of the model must be weighed against the time, available resources, goals and preferences of the user. A primary issue in model development is striking a balance between a general models or highly detailed examinations of specific operations. The users must ask themselves if the marginal value of information gained as the model being constructed becomes more complex worth the addtional input of resources. For example, the user may wish to establish a general framework model with only limited detail and spend more time on analysis and examining the effects of sensitivity and uncertainty in the model. Yet another individual or group may wish to develop a detailed model at a substantial cost in time and resources. This preference allows the user to examine detailed aspects of human performance or limit the level of ambiguity and uncertainty in the model.

Regardless of the level of detail in which the modeler may wish to include, each model begins with a *template* diagram which forms a basis for a specific operation. The template is a diagram involving the most relevant factors affecting a class of accidents or specific operation. The development of a model diagram is cyclic process. The preliminary model diagram can be used to construct a general template. Development of a model are an iterative process. The structure of the model should be shown to key players in the operation (managers, front line operators, regulators, consultants, etc.) to discuss whether the models are consistent with their judgments and experiences [Phillips, *et al.*, 1990]. If results are not consistent with case history examples and general quantitative measures, further refinements are made.

5.0 CASE STUDIES

The following chapter discusses two case studies to develop influence diagram representations (specific accident models) and their associated influence diagrams (templates of a particular class of accidents). Quantitative assessments are made to obtain probabilities of specified target events. Alternatives for HOE management are then assessed to determine their impact upon reducing the probabilities of target events for that particular accident class.

The preceding chapter discussed methods for developing accident framework models to examine the impact of human and organizational factors in marine casualties. This chapter examines applying the framework modeling methods to two post-mortem study examples. Moore (1992) and Paté-Cornell (1992) have examined preliminary structuring of events, decisions, and contributing HOE causes leading to the *Exxon Valdez* and *Piper Alpha* disasters. Applying the HOE taxonomy developed by Moore & Bea (1992), contributing, direct and compounding HOE's are correlated with events, decisions, and actions leading to the accidents.

5.1 The Grounding of *Exxon Valdez*

5.1.1 Preliminary model representations

Roberts & Moore (1992) have established the primary contributors to the grounding of *Exxon Valdez*. This model incorporates critical factors both aboard *Exxon Valdez* and at the vessel traffic center (VTC) in Valdez. It is assumed that the underlying/contributing event is the deviation of the vessel from the traffic separation scheme (TSS). The grounding of the vessel is the direct/initating event and the attempt to dislodge the vessel from the rocks is the subsequent compounding event leading to the additional loss of cargo. Figure 11 shows the initial diagram of relations between events, decisions and actions leading to the grounding.

Intermediate events, decisions and actions are related to the primary events and directly influence the grounding events. Conscience actions and decisions were made by the master to: (1) deviate from the TSS, (2) depart from the bridge during transit, and (3) place the tanker on autopilot and "load up" program. Each of these actions and decisions are represented as decision nodes.

In establishing environmental and HOE causes surrounding the accident, the three primary accident events leading to the grounding are shown in Figure 12. The direct influences of HOE and environmental causes on primary and intermediate events, decisions and actions are shown in the final representation in Figure 13. The grounding model forms a basis from which the influence diagram template is developed.

5.1.2 Influence diagram of vessel groundings/collisions

An underlying factor in the events leading to the grounding of *Exxon Valdez* was the decision to deviate from the TSS. Once a vessel deviates from a specific TSS within navigible waters, potential hazards (vessel traffic, reefs, currents, etc.) can greatly increase the risk of transit. Figure 14 is an influence diagram model of vessel deviation from an established traffic schemes. The diagram is a template to account for general factors that

can influence a potential grounding or collision. The deviation from the traffic lane is shown as a deterministic action based upon the events and actions occurring around the vessel and all other factors are probabilistic in nature. The vessel deviates the TSS for lane obstructions and tide variations in light traffic where there is better maneuverability but are not able to do so in moderate or heavy traffic. In analyses of tanker groundings and collisons, the following general questions are addressed in developing the infuence diagram.

(1) Did the vessel deviate from a previously established traffic scheme? If so, was it a conscience decision to do so? It is assumed in the model that conscience decisions were made to deviate from the scheme and was not inadvertant.

(2) Is the direction of the vessel being properly monitored? Monitoring can be either internal (vessel crew) or external (vessel traffic center). The monitoring of the vessel is directly related to whether a grounding or collision will occur.

(3) Were environmental factors involved in the decision to deviate from the traffic separation scheme (ice in the lane, waves, tide, etc.)? Was vessel traffic a factor in the decision to deviate from the traffic scheme?

(4) Are ship system factors involved in the grounding of the vessel? For example, the vessel may loose power, steering, or navigation capabilities?

(5) Were human and organizational errors involved in the decision to deviate from the traffic separation scheme and/or monitoring of vessel path?

Figure 14 is a general influence diagram representing the relationship between the factors in question. The grounding of *Exxon Valdez* falls within this general class of accidents. Table I displays the outcomes within each node of the diagram. The probabilities (and conditional probabilities) of outcomes presented are those of "expert" opinion and are at input the discretion of the user. Developments of frameworks for probabilistic updating of HOE influences on accident factors are the subject of a following report. These probability distributions represent expert opinion and are supported by limited quantitative data. The subject of quantifying human and organizational errors in operations of marine systems are the subject of a future report.

5.1.3 Evaluating the grounding/collision models

The next step is to evaluate the model to determine base rates of groundings and collisions per unit time dependent upon the factors presented. There is flexibility in reducing the models to examine the impact of various factors upon the target grounding/collision event. As an example, the effects on collisions and groundings resulting from human, organizational, and system errors are addressed independently. Analyses of combinations from the effects of various factors are left to the discretion of the modeler.

The probabilities of the grounding/collision dependent upon human errors, organizational & management errors, and system errors are given in Table II after reducing the influence diagram model shown in Figure 14. Higher frequencies of collisions than groundings related to HOE factors were observed (5 to 10 times greater frequency).

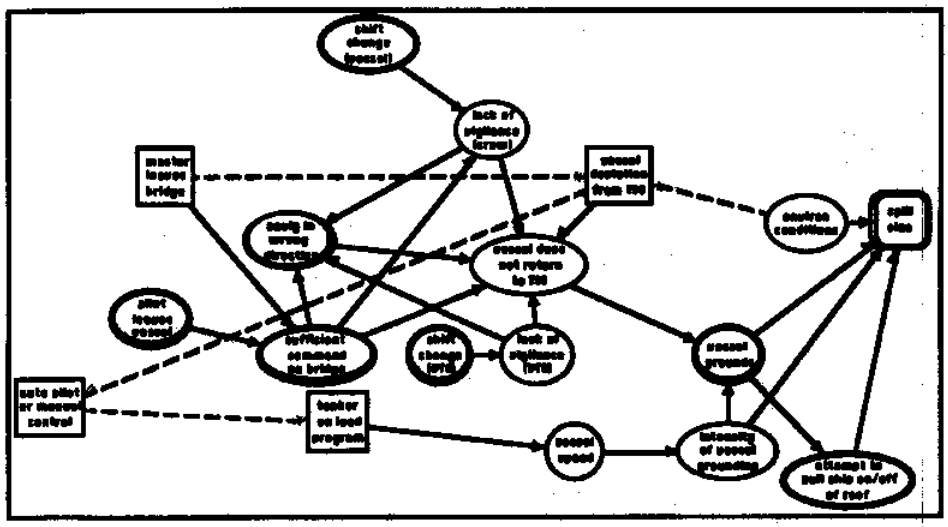


Figure 11: Influence of events and decisions leading to the grounding of *Exxon Valdez*

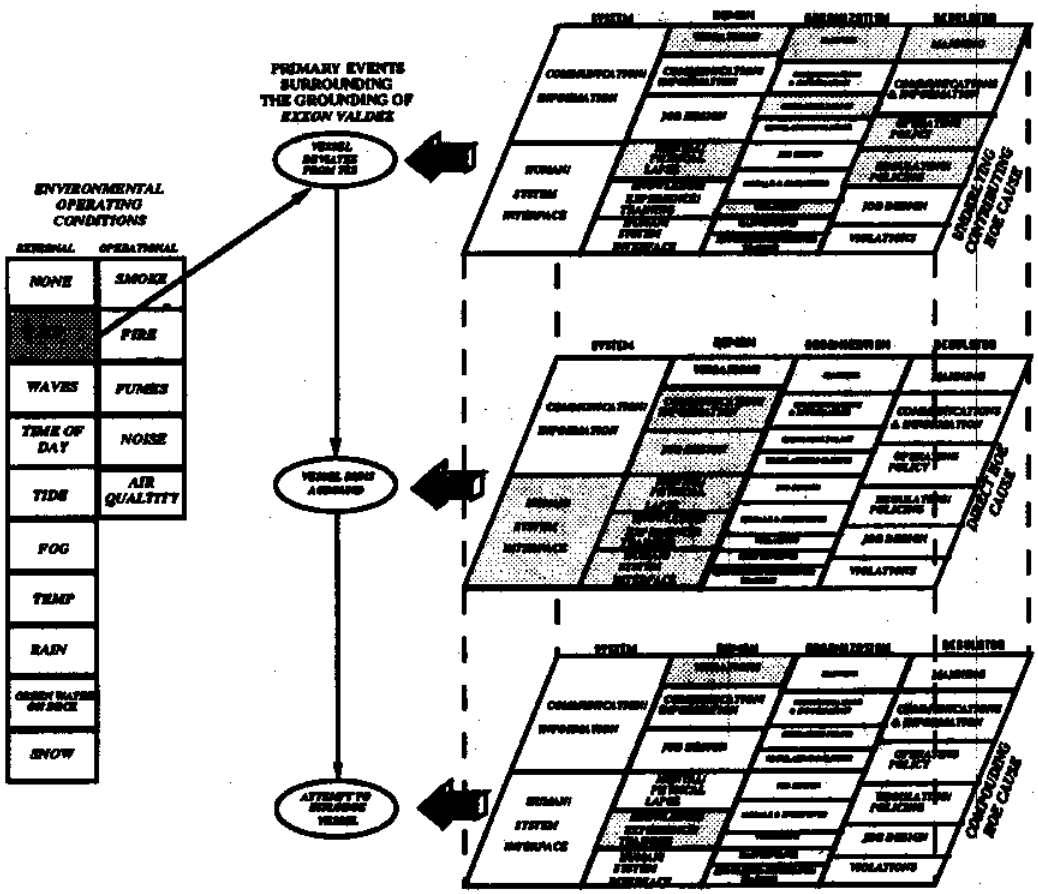


Figure 12: HOE influences on the events surrounding the grounding of *Exxon Valdez* [Moore & Bea, 1992]

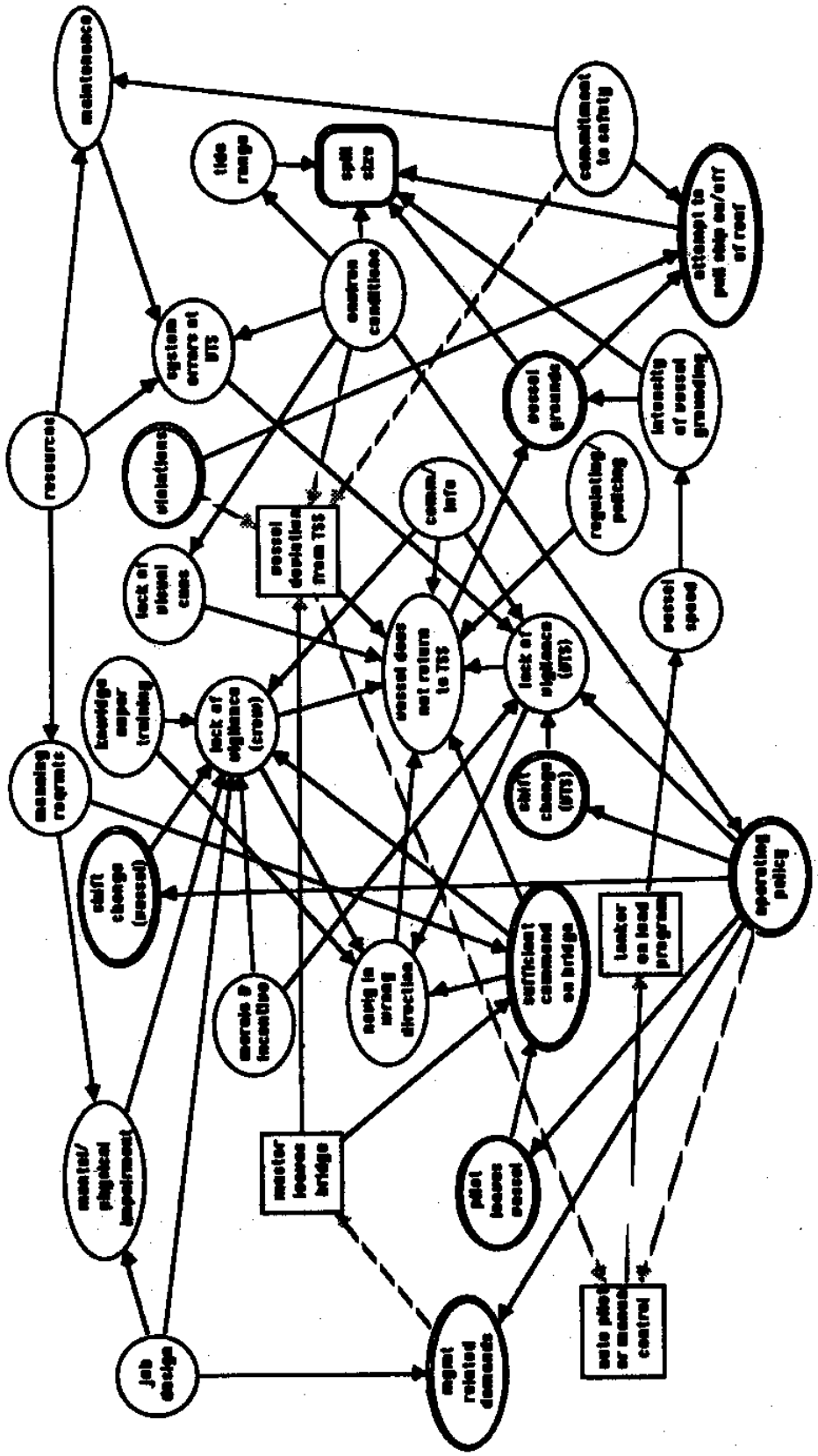


Figure 13: Events surrounding the grounding of the tankship *Exxon Valdez*

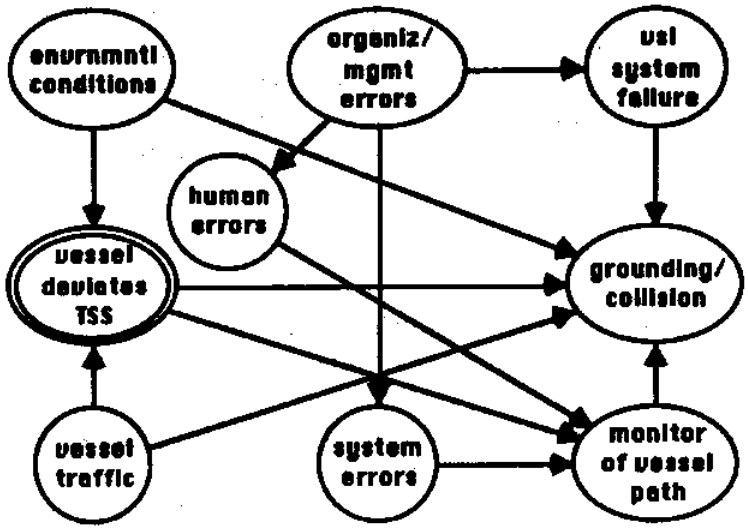


Figure 14: Influence diagram model of factors surrounding tanker grounding or collision

Table I: Outcomes within each node of vessel grounding/collision influence diagram

organiz/mgmt errors	**envrnmntl conditions**	**human errors**
none	*none*	*none*
manning	*lane obstrct*	*violations*
comm/info	*waves*	*comm/info*
oper policy	*wind*	*job design*
regul/policing	*tide*	*mntl/phys lapse*
job design		*knwl/expr/trng*
moral/incent	**vessel traffic**	*hum/syst intrfc*
violations	*light*	
maintenance	*moderate*	**vsl system failure**
knwl/exp/trning	*heavy*	*operational*
		failure
vessel deviates TSS	**monitor of vessel path**	**system errors**
no TSS dev	*monitor*	*none*
TSS dev	*no monitor*	*comm/info*
		hmn syst intrface
	grounding/collision	
	none	
	grounding	
	collision	

From Table II, the modeler can then examine the critical areas where human, organizational or system errors create the largest frequencies of the grounding/collision target event. For example, all categories of human errors are relatively equivalent in probability of groundings ($O(10^{-3})$). Yet violations, communication/information, mental/physical lapses and knowledge/training/experience have relatively higher frequencies.

Table II: Conditional probabilities of groundings or collisions based upon human, organizational, and system errors

	Probability [grounding/collision] error]/yr
Human errors	
none	0.00101 / 0.006718
violations	0.001161 / 0.011094
comm/info	0.001117 / 0.010187
job design	0.001 / 0.007412
mntl/phys lapse	0.001086 / 0.012878
knwl/expr/trng	0.001084 / 0.012664
hum/syst intrfc	9.84E-4 / 0.006803
Organizational/management errors	
none	9.65E-4 / 0.005638
manning	9.78E-4 / 0.006755
comm/info	9.71E-4 / 0.006097
oper policy	9.84E-4 / 0.006356
regul/policing	9.93E-4 / 0.007041
job design	9.68E-4 / 0.006016
moral/incent	9.77E-4 / 0.006471
violations	0.001117 / 0.009389
maintenance	0.001889 / 0.027862
knwl/exp/trning	9.83E-4 / 0.0063
System errors	
none	0.001008 / 0.006759
comm/info	0.001502 / 0.023191
hmn syst intrface	0.001429 / 0.01999

5.1.3.1 Evaluating HOE management alternatives: Violations and OPA 90

Two examples of management alternatives are addressed in this section. Violations on the front line operator level and evaluation of tug support for vessel transit specified by the *Oil Pollution Act of 1990* (OPA 90). These examples represent alternatives directly available to the operator from an internal source (internal control of violations by its operators) and evaluation of alternatives from an external source (regulations being placed upon the operator).

5.1.3.1.1 Violations

Moore & Bea (1992), define violations as intentional unsafe acts such as routine and exceptional violations or acts of sabotage. Violations of are particular concern to organizations. Limited resources for operations at times dictate that corners be cut to keep pace with the demands of the operation. However, there can be a fine line between "cutting corners" and violations. As previously discussed, organizational culture, policies and procedures affect the decisions and actions carried out by front line operators. The management regulating and policing and better incentive structures can reduce the impact of violations by the frontline operator level. This can include constructive incentives such as reporting near miss accidents, directives towards process safety, or availability of needed resources.

Two alternatives are evaluated for control of violations on the operator level. Alternative 1 is to establish a better incident reporting system to better control the actions of frontline operators similar to the *Aviation Safety Reporting System* (ASRS) which receives, processes, and analyzes voluntarily submitted aviation incident reports by pilots, air traffic controllers and other industry sources. Alternative 2 is the elimination of "on time" arrival incentive structure for vessels. Each alternative is presumed to reduce the number of violations by a factor of 10.

Each alternative effect the frequency of violations but Alternative 1 is expected to have an additional impact upon policing and regulating errors at the organizational level. This control of violations has an impact of reducing policing and regulating errors by a factor of 2. Alternative 2 has an additional impact of reducing mental and physical lapses on the human error level as a result of not needing to maintain strict schedules of loading, discharge, departures and arrivals. This is presumed to reduce mental and physical lapses on the operator level by 3.

Table III shows the probabilities of groundings/collisions evaluated from the influence diagram shown in Figure 14 compared with the alternatives described above by a factor of 2 for groundings and a factor of 3 for collisions. Both management alternatives reduce the probabilties of grounding or collision. Discussion of differences in opinion of relationships between events and their causes illicit the development of more realistic models [Phillips, *et al.*, 1990]. The models are developed through an iterative process discussed between experts to determine relavant influences, correlations, and probabilities between subsystems and operations.

Table III: Evaluation of HOE management alternatives to control operator violations

	Probability [grounding/collision] violations]/yr
No management alternatives	**0.001015 / 0.00699**
Management alternatives	
***Alternative 1*: Reporting system**	**0.000715 / 0.002955**
***Alternative 2*: Delivery system**	**0.000515 / 0.002456**

5.1.3.1.2 Oil Pollution Act of 1990

Since the grounding of *Exxon Valdez*, the most influential changes in tanker operations has been the *Oil Pollution Act of 1990* (OPA 90). OPA 90 addresses a wide variety of tanker operation issues and are representitive of current HOE management alternatives. As an overview, Title IV of OPA 90 [Connaughton, 1990]:

(1) mandates that the Coast Guard tie into the National Driving Register to detect individuals with drunk driving convictions;

(2) increases Coast Guard authority to deny or revoke mariner licenses and documents;

(3) authorizes removal of incompetent personnel;

(4) increases Coast Guard authority to deny entry of foreign vessels into the U.S. waters on the grounds of deficient manning;

(5) limit crew workhours aboard tankers to 15 hrs/day but no more than 36 hours in any 72 hour period;

(6) mandates the Coast Guard conduct studies on vessel traffic and tanker navigation;

(7) requires all new tanker builds to be double-hulled in addition to the phasing out of existing tankers beginning in 1995 and concluding in 2010; and,

(8) require the Coast Guard to designate areas where two licensed personnel are required on the vessel bridge and tug escorts are necessary.

Figure 15 is an influence diagram representing the addition tug support to tank vessels during transit through navigable waters. The tug support is presumed available during all environmental conditions except for high seas (waves). In the event of a vessel system failure the tug support would be available. It is presumed that the tug(s) escort the vessel and are able to monitor the vessel path. The effect of the tug support is ain increase in the probability of reliably monitoring of vessel path and a reduction of the probaiblity of grounding/collision by a factor of of reliable operations by a factors of 10. The result is

a reduction of the probabilities of both grounding and collision by a factor of 5 as shown in Table IV.

Additional analyses can be performed to examine the effects of limiting crew workhours and manning (human errors); additional bridge personnel during transit or addressing navigational issues (monitoring vessel path); and, licensing and personnel issues (organizational errors).

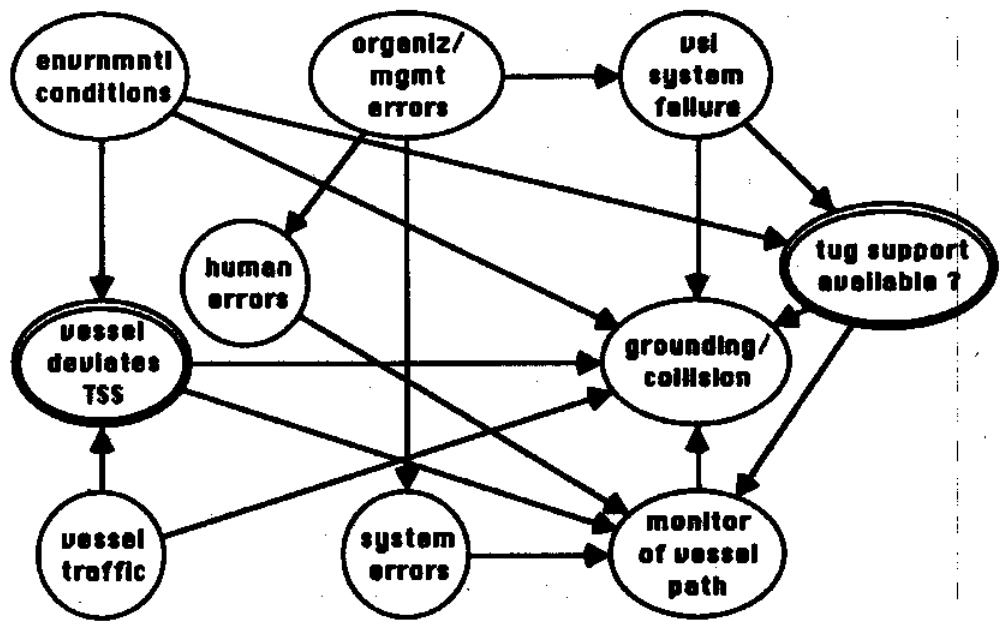


Figure 15: Influence diagram model designed to model affect of tug support

Table IV: Evaluation of HOE management alternatives to add tug support to tanker vessels

	Probability [grounding/collision] violations
Tug support	**1.43E-4 / 0.001187**

5.2 Simultaneous Production and Maintenance on *Piper Alpha*

5.2.1 Preliminary model representations

Primary factors leading to the *Piper Alpha* disaster were the decisions to conduct critical process maintenance and produce hydrocarbons simultaneously [Paté-Cornell, 1992; United Kingdom Department of Energy, 1990]. Miscommunication between control room and maintenance crews regarding the status of the maintenance on condensate pump A led to the condensate pump B gas leak. This has raised considerable interest in addressing the permit to work system to better communicate the status of maintenance for offshore platform operations [Lee & McMillan, 1992; Allen, 1990; Bremner, 1990; Kyle, 1990; Lee & Venkataramanan, 1990]. Another concern in analyzing the accident was the loss of fuel containment which led to the compounding of catastrophic events. Fuel containment was lost in Module B, Module C, jet fuel storage on the deck, and gas risers from the Claymore and Tartan platforms.

Figure 16 is an influence diagram representation of the events, decisions and actions surrounding the *Piper Alpha* disaster. It is presumed that there are three primary factors which occurred in the accident sequence: (1) simultaneous production and maintenance, (2) intial explosions & fires, and (3) loss of life and platform.

Intermediate events decisions and actions are related to the primary events and directly influence the eventual outcome. Conscience decisions were made to produce (103,000 bbl/day) and conduct process critical maintenance (PSV 504 on condensate pump A in Module C) concurrently. The maintenance status of condensate pump A was not communicated between the maintenance and control room personnel (failures in permit to work system). Condensate pump A was started by control room personnel once condensate pump B had tripped leading to a process leak. Ignition of the fuel sources and the subsequent fires and explosions led to the loss of electical power, offshore installation manager (OIM), control room and emergency systems. These factors led to loss of safe refuge, escape routes, rescue capabilties, loss of life and platform.

The impact of smoke, fire, and fumes also resulted in the escalation of catastrophic events. Figure 17 shows the impact of HOE's and environmental operating conditions upon the primary accident events. The accident occurred at night immediately after a maintenance crew change and is related to the explosion/fire event. The loss of life and platform were affected by smoke, fire and fumes at various stages as the accident progressed.

5.2.2 Influence diagram of simultaneous production & maintenance leading to fires and explosions

In developing the general influence diagram model, the following issues were of particular concern in the aftermath of the disaster. These issues apply to a general class of accidents for offshore production platforms. First, was the decision by management to conduct process maintenance and produce simultaneously. Second, was the event of a process leak resulting from the level of operation which led to the series of explosions and fires. Third, was the breach of fuel containment leading to additional fuel sources which escalate the fire to a level of catastrophic consequences. The *Piper Alpha* disaster was an incident falling within this particular class of accidents. Studies prior to the *Piper Alpha*

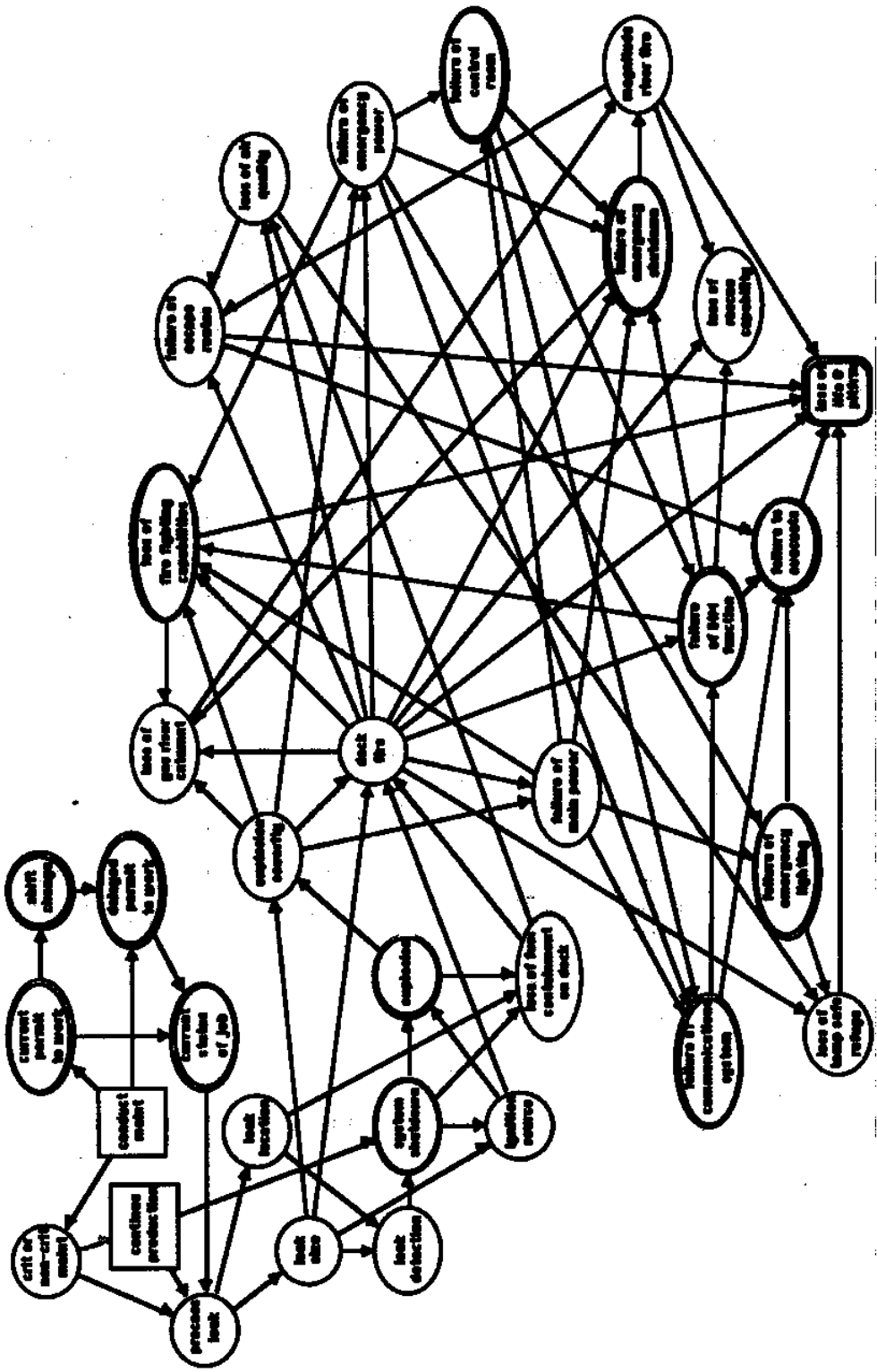


Figure 16: Influence diagram representation of the *Piper Alpha* disaster

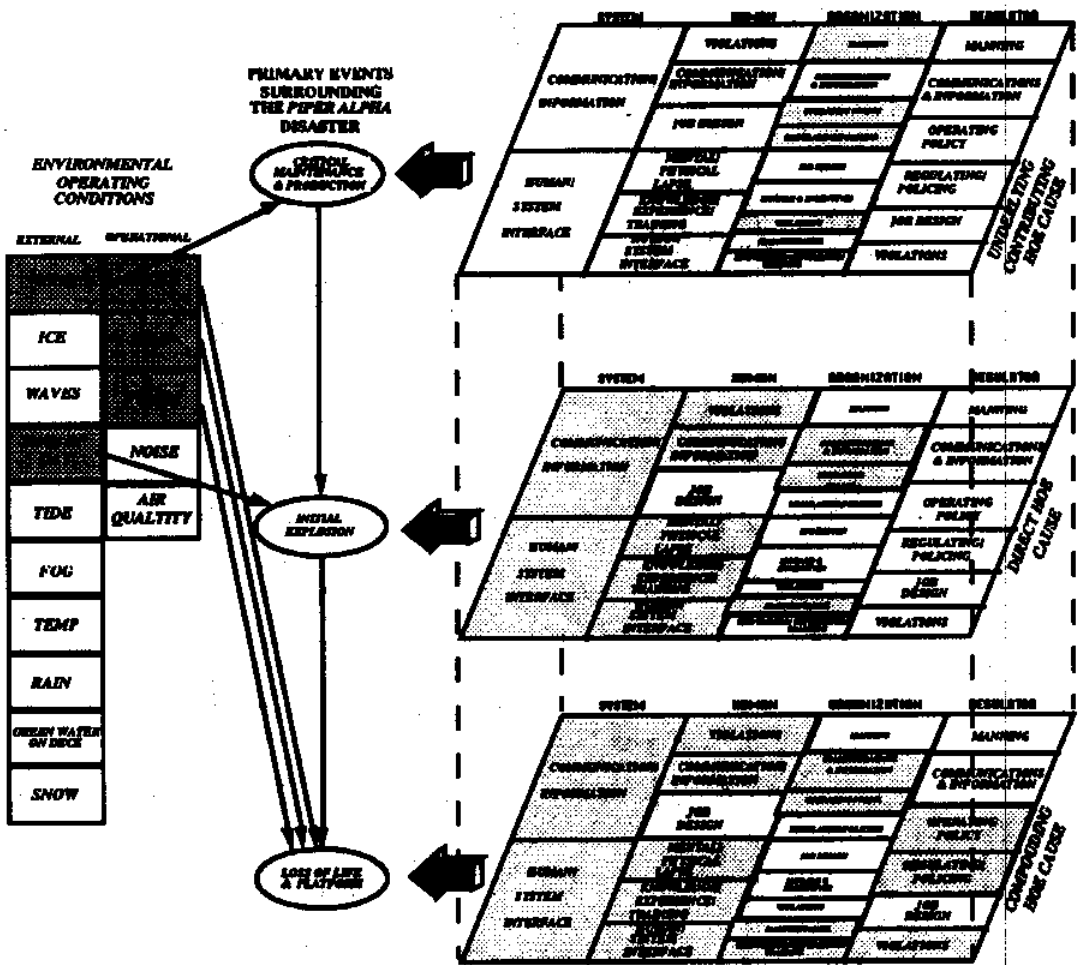


Figure 17: HOE influences on the events surrounding the *Piper Alpha* disaster [Moore & Bea, 1992]

The influence diagram shown in Figure 18 demonstrates the stages of an accident beginning with the decision whether to conduct maintenance and produce simultaneously and the impact the decision has on a potential process leak and potential fire or explosion resulting in a loss of fuel containment. The primary goal is to control the loss of fuel containment in the event of an explosion or fire.

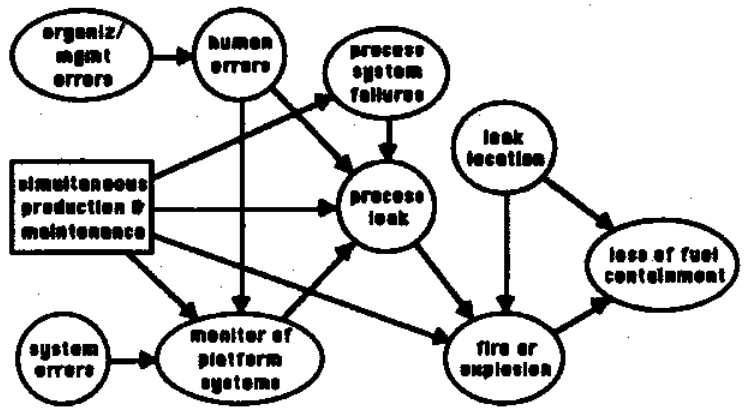


Figure 18: Influence diagram model of the impact of simultaneous production and maintenance on process leaks, explosions, fires, and loss of fuel containment

disaster had shown that 76% of all United Kingdom offshore continental shelf (UK OCS) accidents occurred while conducting maintenance operations [Lee & McMillan, 1992].

The model shows the initial decision to produce and maintain simultaneously. The decision is directly related to process leaks, process system failures, and the monitoring of platform systems. Organizational errors have a direct impact upon human errors at the frontline operator level. Human errors influence the process leaks (maintenance) and the monitoring of the platform systems (control room). Process leaks are also influenced by process system failures (process disturbances) and the human or automated monitoring of the production operation.

Fires and explosions are influenced by process leaks, the leak location and the level at which the production and maintenance are being conducted. For example, higher production outputs during process critical maintenance have greater influence on the explosion or fire event. The leak location and fire or explosion influence the loss of fuel containment aboard the platform. Fuel containment refers to piping, fuel storage, production risers, etc.

Similar to the tanker model above, the probabilities (and conditional probabilities) of outcomes presented are those of "expert" opinion and are at input the discretion of the user. Developments of frameworks for probabilistic updating of HOE influences on accident factors are the subject of a following report. After reduction of the influence diagram shown in Figure 18 conditional upon HOE factors, Table V shows the conditional probabilities of explosions or fires based upon the production/maintenance decisions. The explosion or fire is the particular intiating event to be avoided.

Explosions and fires are less frequent during non-process maintenance[1] (approximately a factor of 2 for human errors and a factor of 3 for organizational and system errors). For human errors, the human/system interface has a higher frequency of accident occurances. This may be attributed to problems in the control room as a result of sub-systems being shut down for maintenance or repair and system status information may be incomplete or incorrect. This is also evident with regard to system errors. Communications/ information and human system interface have comparitively higher frequencies of occurance.

The loss of fuel containment is the compounding event to be avoided in wake of an explosion or fire. Table VI shows: (1) the annual probabililties of explosions and fires conditional upon simultaneous production and maintenance schedules, (2) the annual probabilities of loss of fuel containment dependent upon explosions and fires and simultaneous production and maintenance schedules. The annual probabilities of loss of fuel containment are 2.5 times higher for producing and process critical maintenance operations than producing during non-process critical maintenance. The probabilities of loss of fuel containment in the event of explosion or fire are the same for both critical and non-critical maintenance operations.

5.2.3.1 Evaluating HOE management alternatives: Permit to work system & process leak detection and control

This section discusses two HOE management alternatives for the accident class discussed above. First is the *permit to work system* to account better exchange of communication and information between maintenance crews and control room operators. The second is the issue of process leak detection and control before a process leak leads to an explosion or fire. Similar models discussing issues of manual and automated shutdown of are previously exemplifed by Bea & Moore (1992) for tanker pump room fires.

5.2.3.1.1 Permit to work system

In wake of the *Piper Alpha* disaster, the Lord Cullen Report (1990) the permit to work system for offshore maintenance operations has been undergoing a restructuring process. As mentioned previously, one of the primary contributors to the disaster was process leak resulting from the lack of communication between maintenance crews and control room operators. In a study of UK OCS platform safety, 76% of all accidents occurred during maintenance and 30% of these accidents were related to failures in the permit to work system [Lee & McMillan, 1992].

The influence diagram shown in Figure 19 is a futher devleopment to accommodate crew changes and communicating status of maintenance operations. The model distinguishes between production and maintenance decisions. The maintenance location, duration, equipment, and reliability (abilties of maintenance crew) are included in the model. To account for of maintenance operation, the duration, job status, crew changes, communication of job status (permit to work system) directly or indirectly influence the magnitude

---

[1] *Process critical maintenance* refers to maintenance on machinery and equipment directly related to production and processing hydrocarbons (seperators, compressors, risers, etc.). *Non-process critical maintenance* refers to maintienance that does not directly affect the production process (accommodations, utilties, etc.)

of a process leak. To further develop the model, additional modifications were made to account for magnitudes of production (maximum, moderate, or none) and process leaks (small, moderate, or large).

Table V: Conditional probabilities of explosions and fires based upon production and maintenance operations

	Probability [explosion/fire] error]/yr	
	proc critical maint & production	non-proc maint & production
Human errors		
none	2.2E-5 / 2.2E-5	9.0E-6 / 9.0E-6
violations	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
comm/info	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
job design	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
mntl/phys lapse	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
knwl/expr/trng	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
hum/syst intrfc	1.65E-4 / 1.65E-4	4.8E-5 / 4.8E-5
Organizational/management errors		
none	2.4E-5 / 2.4E-5	9.0E-6 / 9.0E-6
manning	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
comm/info	3.5E-5 / 3.5E-5	1.3E-5 / 1.3E-5
oper policy	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
regul/policing	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
job design	3.1E-5 / 3.1E-5	1.2E-5 / 1.2E-5
moral/incent	2.9E-5 / 2.9E-5	1.2E-5 / 1.2E-5
violations	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
maintenance	2.8E-5 / 2.8E-5	1.1E-5 / 1.1E-5
knwl/exp/trning	2.6E-5 / 2.6E-5	1.3E-5 / 1.3E-5
System errors		
none	2.5E-5 / 2.5E-5	1.0E-5 / 1.0E-5
comm/info	3.7E-5 / 3.7E-5	1.3E-5 / 1.3E-5
hmn syst intrface	4.3E-5 / 4.3E-5	1.4E-5 / 1.4E-5

Table VI: Conditional probabilities of explosions and fires based upon production and maintenance operations

Probability [explosion/fire] maintenance schedule]/yr	
proc critical maint & production	**non-proc maint & production**
2.5E-5 / 2.5E-5	**1.0E-5 / 1.0E-5**

Probability [loss of fuel containment | maintenance schedule & explosion or fire]/yr		
	proc critical maint & production	**non-proc maint & production**
Fire	**0.098956**	**0.114853**
Explosion	**0.11544**	**0.119265**

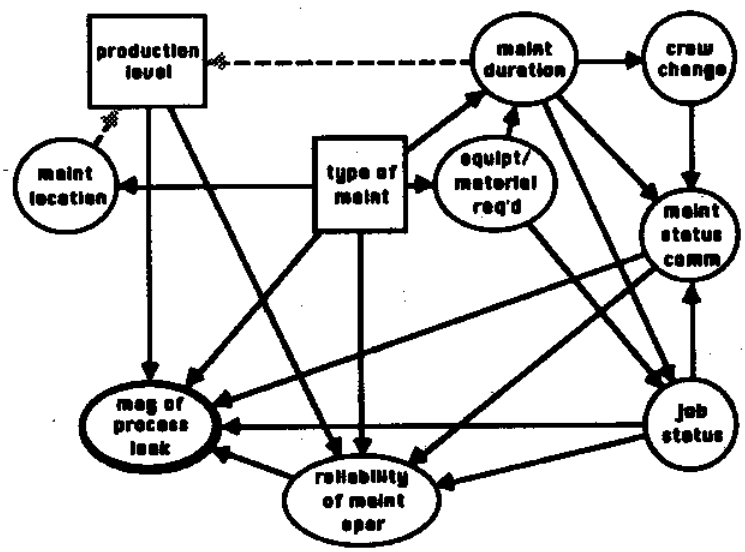


Figure 19: Influence diagram model of the impact of simultaneous production and maintenance with crew changes on process leaks, explosions and fires

The models were reduced to determine the influences on magnitudes of process leaks from production levels, types of process maintenance (critical and non-critical), communication of status of maintenance and maintenance duration. Table VII shows the conditional probabilities of process leaks conditional on these factors prior to management alternatives.

As a management alternative, the permit to work system is upgraded to allow for greater communication of maintenance status. The alternatives are to have better trained operators and maintenance crews, computerization of permit to work system, greater emphasis on detailed communication of status of job status during crew changes. If these programs result in an increase of maintenance status communication by a factor of 10, there is generally observed a reduction in the probabilties of leaks by a factor of 2 for maximum production levels during critical process maintenance. However, for maintenance during moderate production, little change in probability of leaks are observed.

5.2.3.1.2 Process leak detection and control

Detection and control of process leaks can be conducted both manually and automatically. The ability to detect and control process leaks are dependent upon the sensitivity of the detection system, experience, knowledge and training of the operating crew, and the technology available in the detection and control system.

Errors can also be exacerbated by poorly engineered systems that invite errors. Such systems are difficult to construct, operate, and maintain [Melchers, 1987; Ingles, 1985; Moan, 1983]. New technologies can compound the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well operated systems [Perrow, 1984]. Emergency displays have been found to give improper signals of the state of the systems [United Kingdom Department of Energy, 1988b;Perrow, 1984].

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems [Paté-Cornell, 1986]. As observed in Figure 20, if the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive causing frequent false alarms, operators will eventually cease to respond to the warning signals.

Figure 21 provides a schematic description of a simple mishap. Once a mishap has been initiated, the objective is to return the system to normal before it reaches a critical threshold. A mishap is differentiated into three psychological factors: *perceiving, thinking*, and *acting*. The perception stage begins with initiation of the mishap. The initiation of the problem is followed by a warning signal (see Figure 20). The warning is then perceived and the source of the problem is recognized. The thinking stage begins with the identification of the problem and decisions regarding the proper course of action are evaluated. The mishap is baced upon with execution of a plan and the system is returned to a normal operating status or escalates to a critical state.

Though errors occur, they are influenced by cultural and moral values, corporate responsibilities and organizations, and individual training, craftsmanship, and integrity. The individual, organizations, and societies all play important roles in human errors which lead to dangerous states and can result in catastrophic consequences.

To examine the leak detection and control an expanded influence diagram has been developed. Figure 22 is an influence diagram to account for loss of fuel containment in the event of: (1) detection and control of the process leak, (2) ignition of leak, (3) system shutdown in the event of explosion or fire, and (4) failure of power, deluge and blowout panel systems. The concern is to reduce the the probability of the explosion or fire event.

As mentioned previously, process leak detection and control are dependent upon the sensitivity of the detection system, experience, knowledge and training of the operating crew, and the technology available in the detection and control system. If management has invested in better training (crisis management), experience and knowledge (better incentives to qualified operators), detection (human - system interfacing, system communication and information) and emergency shutdown systems. The reducution of the influence diagram model focuses on the influence of detection and control of process leaks upon explosions or fires and are summarized in Table VIII. Control and detection systems lead to a 25% decrease in the number of explosions and fires if the leak is detected and contolled. If the leak is not controlled there is a 30% reduction in the events of fire and explosions for detected and uncontrolled leaks (possibly the result of better crisis management and understanding of the system).

Table VII: Conditional probabilities of process leaks dependent upon production level, maintenance type, duration and communication of status

production level	type of maint	status of maint	duration of maint	process leak magnitude	P[leak] (prior)	P[leak] (post)
maximum	process critical	communic status	less than a shift	sm leak mod leak lg leak	0.075 0.0012 0.0	0.0375 0.00125 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.096486 1.76E-4 0.0	0.04832 1.68E-4 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.020823 0.685277 .2939	0.495 0.45 0.055
"	process non-critical	communic staustus	less than a shift	sm leak mod leak lg leak	0.020823 0.832122 0.147055	0.003402 0.896907 0.099691
"	"	"	greater than a shift	sm leak mod leak lg leak	.002667 0.0 0.0	0.002667 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	.002667 0.0 0.0	0.002667 0.0 0.0
"	non-process critical	communic status	less than a shift	sm leak mod leak lg leak	6.3E-4 0.0 0.0	6.04E-4 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.45 0.055 0.0	0.45 0.055 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.82952 0.092952 0.0	0.887892 0.098789 0.0
"	non-process non-critical	communic status	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
moderate	process critical	status commun	less than a shift	sm leak mod leak lg leak	0.0075 0.00125 0.0	0.0075 0.00125 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.009649 1.76E-4 0.0	0.009664 1.68E-4 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.9495 0.05 5.0E-4	0.9495 0.05 5.0E-4
"	process non-crit	status communic	less than a shift	sm leak mod leak lg leak	0.902082 0.097897 2.1E-5	0.90034 0.099656 3.0E-6

Table VII: Conditional probabilities of process leaks dependent upon production level, maintenance type, duration and communication of status (cont.)

production level	type of maint	status of maint	duration of maint	process leak magnitude	P[leak] (prior)	P[leak] (post)
moderate	process non-crit	status communic	greater than a shift	sm leak mod leak lg leak	2.67E-4 0.0 0.0	2.67E-4 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	6.3E-5 0.0 0.0	6.0E-5 0.0 0.0
"	non-process critical	status communic	less than a shift	sm leak mod leak lg leak	0.005 5.0E-4 0.0	0.005 5.0E-4 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.009217 7.8E-5 0.0	0.009865 1.3E-5 0.0
"	"	stuatus not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	non-process non-critical	communic stauts	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
none	no leaks	no leaks	no leaks	no leaks	0.0	0.0

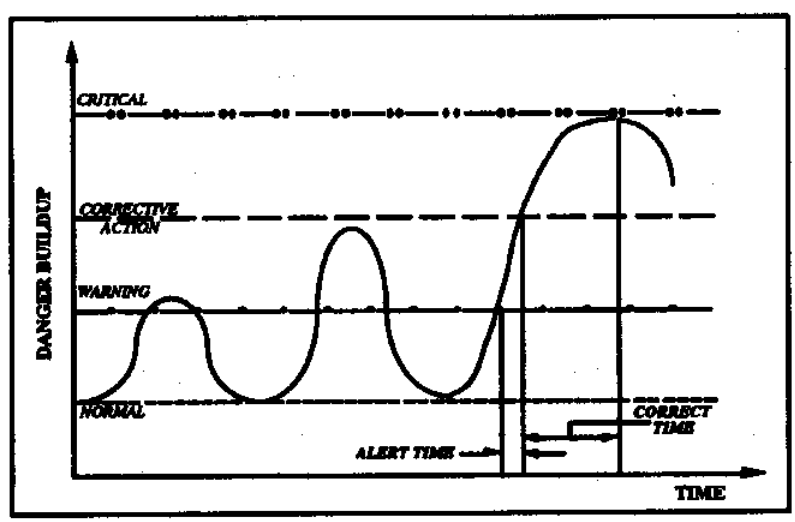


Figure 20: Danger buildup function [Paté-Cornell, 1986]

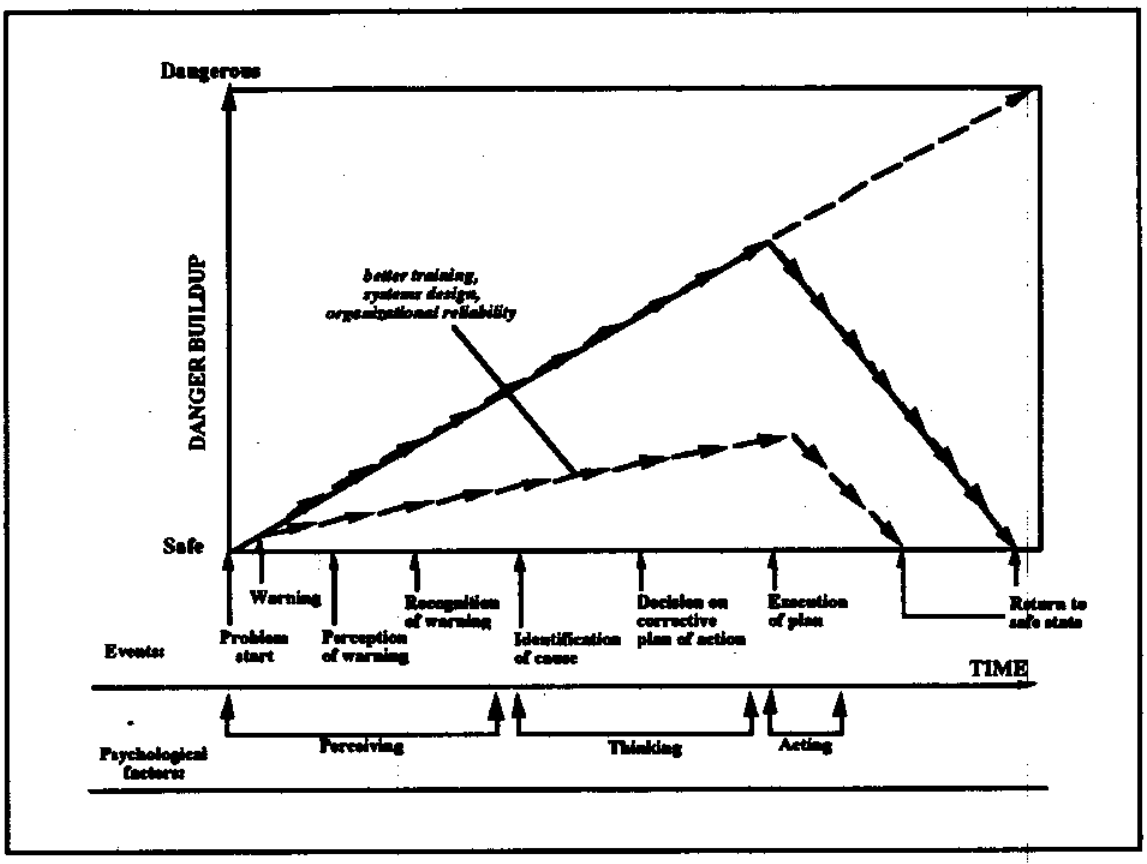


Figure 21: A simple model of a mishap[Bea & Moore, 1991]

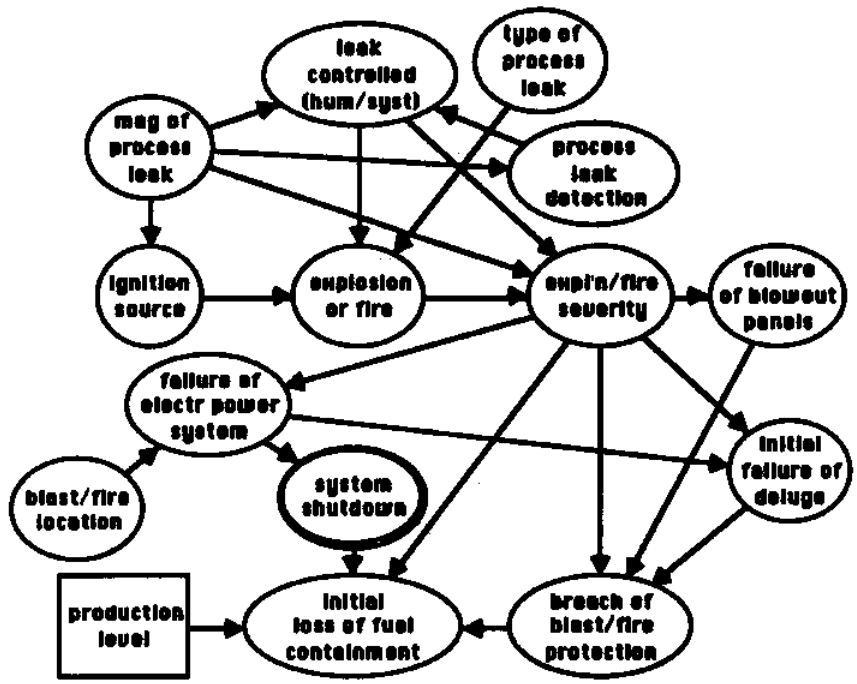


Figure 22: Influence diagram model of the impact of explosions, fires, and loss of fuel containment

Table VIII: Probabilities of explosion or fire conditional upon process leak detection and control

leak control	process leak detection	explosion or fire	P[explosion or fire] (prior)	P[explosion or fire] (post)
lk control	detected	none	0.99463466	0.99594834
"	"	fire	0.00268267	0.00202583
"	"	explosion	0.00268267	0.00202583
no leak control	"	none	0.12917219	0.30985401
"	"	fire	0.43541391	0.34507299
"	"	explosion	0.43541391	0.34507299
"	not detected	none	0.58486529	0.53675497
"	"	fire	0.20756735	0.23162252
"	"	explosion	0.20756735	0.23162252

6.0 CONCLUSIONS

Post-mortem studies provide a basis in which to construct probabiliistic models (influence diagrams) of general classes of accidents. Analyses of post-mortem accident studies lead to a greater understanding of the effects of HOE in accident sequences. In addition, post-mortem model developments assist engineers, managers, and regulators in determining the impact of HOE management alternatives through model analysis.

A lack of quantitative information limits assessment of conditional probabilities of accident related factors. Therefore, we must rely on expert opinion and limited data sources. Nevertheless, developments of influence diagram models assist users in determining and examining complex interactions of human, organizational, and systems.

7.0 ACKNOWLEDGMENTS

This paper is funded in part by a grant form the National Sea Grant College Program, National Oceanic and Atmospheric Administration, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17 through the California Sea Grant College, and in part by the California State Resources Agency. The views expressed herein are those of the authors and do not necessarily reflect the views of NOAA or any of its sub-agencies. The U.S. Government is authorized to reproduce and distribute for government purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U.S. Coast Guard, the U.S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

8.0 REFERENCES

Allen, C.S. Applications of computer permit to work systems for offshore installations. *Cullen Inquiry paper No. 757.* 1990.

Bea, R.G. Human and organizational error in reliability of coastal and ocean structures. Proceedings of the *Civil College Eminent Overseas Speaker Program, Institution of Engineers*, Australia. December 1989.

Bea, R.G. & Moore, W.H. Improving operational reliability of marine systems: Management of human and organizational errors. *New Challenges to Organizations, High Reliability Organizations*, McMillan: New York, 1992. (In prep.)

Bea, R.G. & Moore, W.H. Management of human and organizational error in operational reliability of marine structures, *Proceedings, Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Designs and Codes.* Houston, TX. April, 1991.

Bremner, R. Work permit management, use of a computer makes information more widely available. *Proc. IBC Conference on Offshore Hazards and Pheir Prevention.* 1990.

CASMAIN, USCG casualty database. 1981-1990.

Connaughton, S.T. Vessel pollution prevention and response considerations. *New Oil Pollution Act of 1990 Conference.* Government Institutes, Inc. 1990.

Dynamic Research Corporation. Role of human factors in marine casualties. Final report prepared for the U.S. Coast Guard. Contract number N00024-85-D-4373. June, 1992.

Freudenburg, W.R. Perceived risk, real risk: Social science and the art of probabilistic risk assessment. *Science*, Volume 242, October, 1988.

Howard, R.A. From influence to relavance to knowledge. From *Influence diagrams, belief nets and decision analysis.* (Chapter 1) Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990.

Howard, R.A. & Matheson, J.E. *Influence Diagrams.* Copyright © 1981.

Ingles, O.G. Human error, and its role in the philosophy of engineering. Doctoral Thesis, University of New South Wales, Australia, 1985.

Institute of Marine Engineers. Offshore Operations Post *Piper Alpha*. Proceedings of the February 1991 Conference, London, England. 1991.

Keeble, J. *Out of the Channel: The Exxon Valdez Oil Spill in Prince William Sound.* New York: HarperCollins Publishers. 1991.

Kyle, S.R. Key elements of a permit to work system. *Proc. IRM/ROV 90.* 1990.

Laroque, G.R. & Mudan, K.S. Cost and benefits of OCS regulations: Volume 3 - preliminary risk analysis of outer continental shelf activities. Arthur D. Little, Inc. Cambridge, MA. 1982.

Lee, B.S. & McMillan, W.S. A knowledge based system for offshore permit to work management. *Proc. of Second International Offshore and Polar Engineering Conference.* 1992.

Lee, B.S. & Venkataramanan, S. Decision support system for work permits. *Proc. IRM/ROV 90.* 1990.

Ling, W.C.T. & Williamson, R.B. Application of fault tree analysis to ignition of fire. Presented at the Western State Section / The Combustion Institute Paper no. 78-65, Fall Meeting, Laguna Beach, CA. Prepared for the U.S. Department of Energy under Contract no. W-7405-ENG-48. 1978.

Marton, T. & Purtell, T.W. Investigations in the role of human factors in man related marine casualties. U.S.Coast Guard Internal Report. (Reference) 1990?

McIntyre, S.R. Recent and pending changes in the United Kingdom regulatory system affecting mobile offshore drilling units. Proceedings of *Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Designs and Codes.* Houston, TX. April, 1991.

Melchers, R.E. Structural reliability analysis and prediction. Brisbane, Australia: Ellis Horwood Limited, Halsted Press: a division of John Wiley & Sons, 1987.

Moan, T. Safety of offshore structures. *Proc.of Fourth International Conference on Applications of Statistics and Probability in Soil and Structural Engineering.* 1983.

Moore, W.H. & Bea, R.G. A practical human error taxonomy for marine related casualties. Research Report No. 92-3, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. June, 1992.

Moore, W.H. The grounding of *Exxon Valdez*: An examination of the human and organizational factors. *Society of Naval Architects and Marine Engineers*, Northern California Section. April, 1992.

Moore, W.H. Human and organizational error in marine systems: A review of existing taxonomies and databases. Research Report No. 91-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. July, 1991.

Oliver, R.M. & Yang, H.J. Baysian updating of event tree parameters to predict high risk incidents. From *Influence diagrams, belief nets and decision analysis.* (Chapter 12) Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990.

Panel on Human Error in Merchant Marine Safety. Human error in merchant marine safety. Maritime Transportation Research Board, National Academy of Sciences. Washington, D.C. 1976.

Paté-Cornell, M.E. A post-mortem analysis of the *Piper Alpha* accident: Technical and organizational factors. Research Report No. 92-2, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. January, 1992.

Paté-Cornell, M.E. & Bea, R.G. Organizational aspects of reliability management: Design, construction, and operations of offshore platforms. Research Report no.89-1, Department of Industrial Engineering and Engineering Management, Stanford University. 1989.

Paté-Cornell, M. E. & Seawell, J.P. Engineering reliability: The organizational link. Proc. of *ASCE Specialty Conference on Probabilistic Mechanics, Structural, and Geotechnical Safety*. Blacksburg, Virginia. 1988.

Paté-Cornell, M. E. Warning systems in risk management. *Risk Analysis*, Vol. 6, No.2. 1986.

Perrow, C. *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, Inc., 1984.

Phillips, L.D., Humphreys, D.E. & Selby, D.L. A socio-technical approach to assessing human reliability. From *Influence diagrams, belief nets and decision analysis*. (Chapter 13) Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990.

Reason, J. *Human Error*. Cambridge University Press: New York. 1990.

Reason, J. How to promote error tolerance in complex systems in the context of ships and aircraft. (Reference ?) 1992.

Roberts, K.H. & Moore, W.H. A Gordian Knot: Into which sailed the *Exxon Valdez*. Research Report No. 92-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering, University of California, Berkeley*. January, 1992.

U.S. Department of Interior, Minerals Management Service. Accidents associated with oil & gas operations: Outer continental shelf 1956-1986. OCS Report MMS 88-0011. March, 1988.

United Kingdom Department of Energy. *Piper Alpha Technical Investigation: Interim Report*. Petrie Report. Crown: London. September, 1988a.

United Kingdom Department of Energy. *Piper Alpha Technical Investigation: Further Report*. Petrie Report. Crown: London. December, 1988b.

Moore, W.H. & Bea, R.G. Modeling the effects of human errors in post-mortem marine casualty studies. Research Report No. 92-4, Management of Human Error In Operations of Marine Systems Project, *Dept. of Naval Architecture and Offshore Engineering*, University of California at Berkeley. August, 1992.

United Kingdom Department of Energy. *The Public Inquiry into the Piper Alpha Disaster, The Hon Lord Cullen,* Volumes 1 & 2, HMSO Publications, London. November, 1990.