ALASKA
Risk Assessment of Oil and Gas Infrastructure

Review of Select Foreign and Domestic Approaches to Oversight and Management of Risk and Recommendations for Candidate Changes to the Oversight Approach for the Alaska Petroleum Transportation Infrastructure

NOVEMBER 2010

PREPARED BY CYCLA CORPORATION
Under Contract to the Alaska Department of Environmental Conservation

NORTH SLOPE Spills Analysis

FINAL REPORT

EXECUTIVE SUMMARY

This report was developed to provide the State of Alaska with practical recommendations for future oversight activities for oil transportation. These recommendations reflect a review of risk management programs utilized by US and foreign safety agencies based on the author's direct experience from over thirty-five years carrying out risk assessments and implementing risk management systems.

Risk management can be viewed as three sequential steps: (1) risk assessment is a systematic investigation of design and operation of the physical system to disclose vulnerabilities and to put these vulnerabilities in the context of risk; (2) risk control involves the definition of the various possible actions to reduce or mitigate the identified risks, and the selection of the best overall set of actions that can be taken within the available resources; and (3) performance monitoring and feedback involve assessing the actual effectiveness of the selected risk management actions

The operator is ultimately responsible for the safe operation of its facilities; therefore, the primary job of regulators is to require practices that reinforce the operator's responsibility, and to knowledgeably oversee the implementation of those practices. This is typically accomplished through regulations. Regulatory approaches to risk management oversight range from the highly prescriptive ("command and control") regulations that mandate detailed actions and activities across the life of a facility to more process-focused regulations that describe the general characteristics of management systems and allow the operator to develop their own systems that satisfy those characteristics. Other regulatory approaches include performance standards and event reporting requirements. All are designed to provide oversight agencies information about how an operator is maintaining safe operating conditions and thereby reducing risks. Different regulatory approaches require different types of oversight expertise.

This report discusses candidate risk management and oversight systems based on models in place in other jurisdictions. Recommendations presented are designed to enhance Alaska Department of Environmental Conservation (ADEC)-specific risk management practices and to strengthen risk management practice across Alaska oversight agencies.

The author recommends three candidate future actions for risk management across Alaska agencies:

- **Avoid Agency-Led Risk Assessments -** The State of Alaska should not unilaterally undertake a Risk Assessment of its Petroleum Infrastructure without significant cooperation from operators;
- **Strengthen Regulatory Oversight by Evolution not Revolution -** focus on evolution and refinement of existing oversight system and processes rather than radical revision of the system; and

- **Require Operators to implement a Strategic Management Process -** designed to monitor and learn from experience, anticipate changes in the operating environment, and systematically allocate resources to manage recognized risks.

The author recommends three candidate changes that the ADEC should consider:

- **Expand Operator Reporting -** expand mandatory reporting to support improved oversight agency understanding of the effectiveness of operators' internal management systems;
- **Strengthen Operator Management Systems -** imposing additional requirements for operator management systems by promulgating new regulations that either reference existing standards or prescribe specific requirements; and
- **Strengthen Learning Processes -** strengthen the role of Alaska oversight agencies in evaluating underlying risk causes and use the resulting improved understanding of key causal factors to tailor additional requirements.

There is significant commonality in what these recommendations are designed to accomplish. The primary purpose is to strengthen the Alaska regulatory agency knowledge and awareness of risks, and to improve agency access to information on the operators' perspective on risk as well as on their plans to manage that risk.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose and Scope

The purpose of this report is to provide the State of Alaska with practical recommendations for future oversight activities for oil transportation based on review of risk management programs utilized by US federal and foreign safety agencies.

The recommendations discussed in Section 4 are separated into two components: candidate future actions the State of Alaska might undertake to strengthen its risk management efforts, and candidate changes the Alaska Department of Environmental Conservation (ADEC) might make. The primary purpose of the set of recommendations is to strengthen Alaska regulatory agency knowledge and awareness of risks, and to improve agency access to information on the operators' perspective on contributors to risk as well as on their plans to manage those risk contributors.

1.2 Background of Alaska Risk Assessment

The Alaska Risk Assessment (ARA) project was authorized by the Alaska legislature following the 2006 corrosion-related pipeline leaks on the North Slope. These leaks resulted in serious negative impacts on Alaska's oil production from 2006 through 2008. The primary product of the ARA project was initially intended to be a quantitative risk profile of the Alaska petroleum infrastructure that could be used by the State of Alaska to oversee management of risks, including but not limited to the risk of unplanned oil production outages.

An ARA methodology, developed by a contractor to the Alaska Department of Environmental Conservation (ADEC), was critically reviewed first by the Alaska public and interested outside parties, and ultimately by a committee of the Transportation Research Board (TRB). After considering the results of these reviews, ADEC decided to undertake a study of more limited scope, one designed to identify opportunities for reducing the risk of spills on the North Slope by thoroughly reviewing the causes of leaks experienced over the past several years, and to identify candidate preventive and mitigative measures to address these causes.

As a component of the revised ARA scope, ADEC decided to evaluate national and international risk management practices to obtain input to future decisions on what, if any, action the state should take to strengthen its risk oversight and management capabilities. This report is the result of that effort.

1.3 Report Structure

The report is structured into four sections supported by two Appendices.

Section 1 contains an Introduction, describing the report purpose, scope, background, and organization.

Section 2 considers the oversight and management of risks, discussing the major elements of regulatory oversight and exploring how risk relates to each of these elements. Emphasis is on the roles of understanding risk (risk assessment being just one tool), and overseeing the operator's management of risk. Both risk assessment and root cause evaluation are discussed as complementary aspects of overseeing operator management of risk. The importance of anticipating changes that have the potential to affect risk and of learning about the impact of factors which are not explicitly regulated are also discussed.

Section 3 discusses several different models for regulatory oversight of risk assessment and management, based on the experience of regulators in using risk assessment and risk management as part of their intervention approaches. It summarizes experience of the Nuclear Regulatory Commission in overseeing the nuclear power industry, the experience of the Pipeline and Hazardous Materials Safety Administration in using risk in its regulatory approach, and the experience in the UK, Norway and Australia with application of risk principles. It also discusses factors important to managing risk that are not typically regulated.

Section 4 provides recommendations for strengthening regulatory oversight in Alaska, based on the lessons from the application of risk thinking from other regulatory environments. Both project-level and department-level considerations are addressed, supporting conclusions and recommendations by reference to experience at other agencies.

Two Appendices provide background for the main report. Appendix A addresses risk management aspects of the US federal approach to regulating pipeline safety & health. Appendix B addresses the US experience in regulating safety risk at nuclear power facilities.

2 OVERSIGHT AND MANAGEMENT OF RISK

2.1 Risk Terminology

As used in this report, risk describes both the likelihood of occurrence (probability) and the impact (consequences) of a set of undesired events affecting public health and safety, the environment or economic interests. Operators of oil transportation infrastructure typically manage risk using controls - both engineered and procedural - that may be prescribed in regulation or implemented at their own discretion.

Risk management is the process by which an organization identifies and understands sources of risk, makes decisions on how to allocate resources to address these risks, and confirms the validity of these decisions using performance results. Risk management does not necessarily require detailed, technical models or warehouses full of operating data. What is required is a structured, traceable, and defensible investigative process. Models are needed, the most useful of which are very often quite simple, involving almost intuitive relationships in which failures lead to adverse consequences. Necessary information on historic problems leading to undesired events is often in the form of expert opinion, which, if necessary, can be converted into quantitative measures of risk. Improvements in safety efficiency, focusing on what is truly important, can thus be achieved without the expense of detailed quantitative analysis. Risk management can be viewed as three sequential steps: (1) risk assessment; (2) risk control and decision support; and (3) performance monitoring and feedback.

To assure the engineered systems and procedures are adequate to effectively manage risks, operators often choose to perform (and regulators occasionally choose to prescribe the need to perform) a risk assessment. *Risk assessment* is a systematic investigation of design and operation of the physical system to disclose vulnerabilities and to put these vulnerabilities in the context of risk. Addressing both the likelihood of possible events and the realistic consequences of the events should they occur allows a balanced perspective on the relative importance of the various events and the factors that contribute to these events. Risk assessment can be qualitative or quantitative, depending upon the problem being addressed. Risk assessment can range in complexity from an experience-based characterization of risks (inherently qualitative), to quantitative modeling involving carefully assembled data on equipment failure rates, human error likelihoods, and the likelihood of adverse consequences (such as crude oil releases). The sophistication of risk assessment must be tailored to fit the application as well as the form and availability of data. Some of the most valuable applications involve some of the simplest assessment models.

Risk control involves the definition of the various possible actions to reduce or mitigate the identified risks, and the selection of the best overall set of actions that can be taken within the available resources. For example, possible risk control activities might include: a) simple procedural constraints

on operations, b) rigorous inspection of physical condition and preventive maintenance programs, c) enhancements in training and awareness programs, and d) design features to make operations safer. Each of these options might reduce risk to varying degrees, and might require differing levels of cost. Selection of the best risk control strategies, within constrained budgets, is one of the most important aspects of risk management.

Performance monitoring and feedback involve assessing the actual effectiveness of the selected risk management actions. Within a risk management program, management doesn't make predictions and assumptions and then hope risk is reduced. The actual impact of the risk management decisions on safety, health, and the environment is assessed. Changes are made, if necessary, to improve results. The overall effectiveness of a risk management program depends on careful design of monitoring and feedback elements so that the impact of uncertainties in assessment or control decisions can be evaluated, and corrections can be made.

2.2 Regulatory Oversight

The primary job of regulators is typically overseeing the operators' risk management efforts. The basic principle regulators typically follow is the operator is ultimately responsible for the safe operation of its facilities, and the regulator should require practices that reinforce the operator's responsibility then provide knowledgeable oversight of implementation of those practices. This principle leads directly to the need for strong operator safety management systems and vigilant regulatory oversight of the effectiveness of these systems.

The basic functions of a "generic" regulatory agency are depicted in the blue shaded boxes in Figure 2-1. This figure is not intended to be comprehensive (e.g., R&D is excluded, as is agency exercise of legislative authority to issue a corrective action order that imposes requirements beyond the regulations), but rather to show the relationship among the actions a regulatory agency can take and their impact on an operator's management of risk.

As shown, there are several situations in which the understanding of risk and the factors that contribute to it can enter. The first situation (Box 1), before the regulatory agency is involved, occurs when the legislative body assembles information on risks of an engineered facility it is considering regulating. This information is the basis for legislative decisions on the scope of regulatory authority it will vest in the agency, and any constraints on how the agency will be directed to discharge its authority (Box 2). As discussed in Section 3 and Appendix A, requirements on a facility operator to carry out a risk assessment typically originate in the legislative mandate.

Beyond operator vigilance and attention to detail in operation, perhaps the most critical element in effective management of a high risk facility is continuing to learn about the factors that affect risk. Because the factors affecting risk change over time (e.g., with facility aging, changes in management practices, changes in facility design, and changes in the operating environment), learning is critically important for both the operator and the oversight agency. Opportunities to learn are depicted at several places in Figure 2-1.

As an agency inspects an operator (Box 4) it learns about the operator's vigilance and attention to detail - if only in its compliance practices. As operating experience is increased, both the operator and the agency can monitor reportable events (Box 5) and infer whether the existing controls are working or are deteriorating from trends in these events. Perhaps the best information on the effectiveness or

breakdown of controls is available from careful evaluation of reportable events (Box 6). Such "root cause" evaluations, when focused on events with significant consequences or events having unique characteristics, can identify unanticipated chains of events that defeat existing controls or can disclose breakdown of management systems that are often not explicitly regulated, but are critical to effective management of facility risk.

Boxes 7 and 8 in Figure 2-1 depict agency self assessment, considering both the effectiveness of its intervention approaches and the regulations on which it bases its oversight, and communication of additional jurisdictional authority to effectively manage facility risks - thereby closing the "feedback loop."

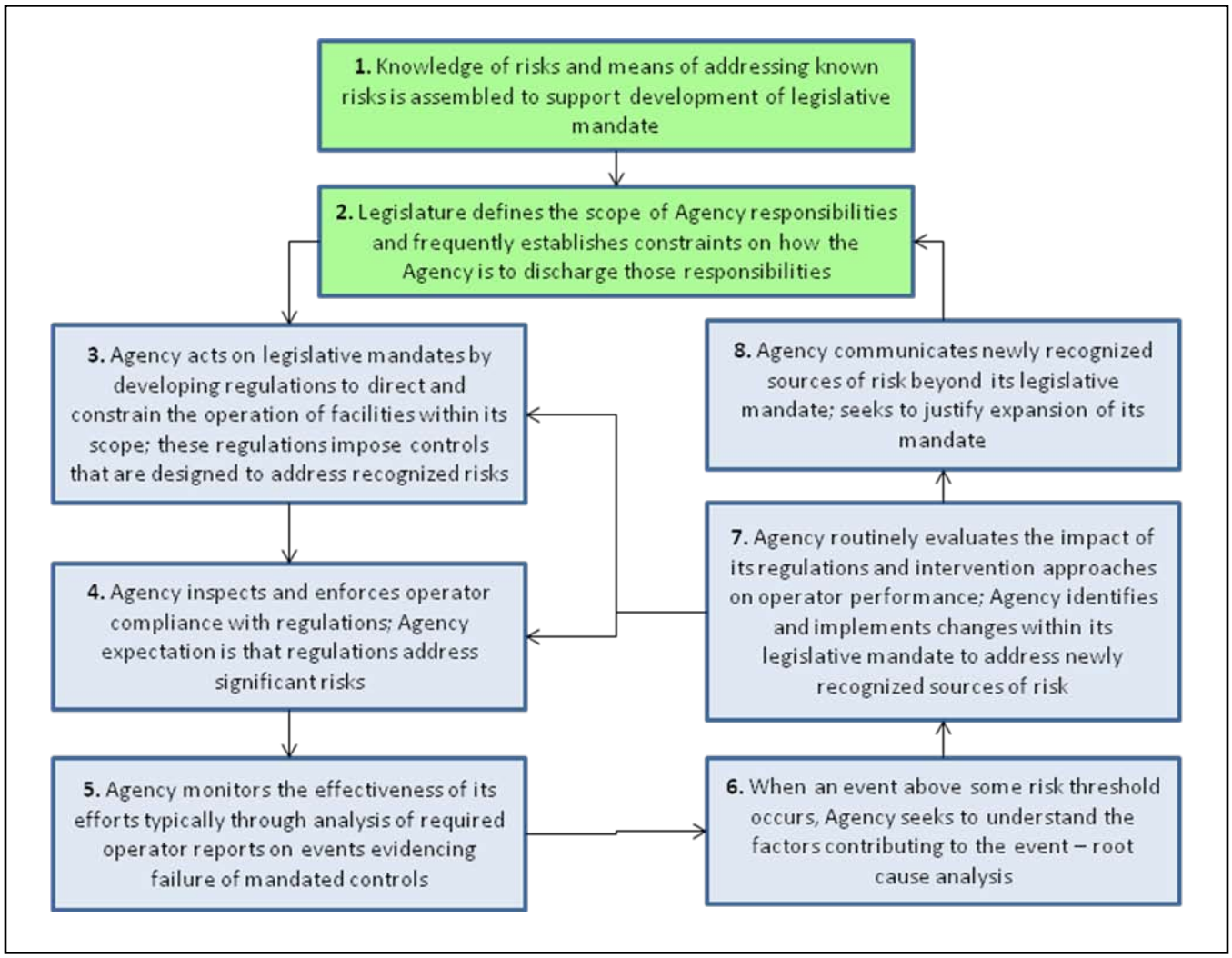


Figure 2-1. Basic functions of a Regulatory Agency – described in Risk Management terms.

2.3 Regulatory Approaches

Depending on the nature of the legislative mandate, agencies have a choice among several different types of regulations. Those most frequently used are discussed below. Each approach has its strengths and limitations, including the level of operational flexibility allowed, the level of trust the regulator places in the regulated entity, and the nature and level of expertise required to implement and oversee compliance with the requirements.

Highly prescriptive ("command and control") regulations

These types of regulations prescribe (command) detailed actions - across the entire life cycle of a facility, from design through decommissioning - needed to manage risks and assure the public interest is satisfied. An example is current PHMSA regulations that require the operator to assess, using acceptable technology, the integrity of transmission lines in high consequence areas at least every five years. Agency inspection and enforcement of this sort of regulation can be thought of as "control," hence the concept of "command and control" regulations.

Management process regulations

Management process regulations describe the general characteristics of the management systems needed to manage risks and assure the public interest is satisfied. An example is current PHMSA regulations that require the operator to have a program, with prescribed elements, for qualifying and maintaining the qualification of certain operations and maintenance (O&M) personnel.

Performance-based regulations

These regulations describe performance measures and the level of performance required against these measures necessary to assure management of risks to satisfy the public interest. An example is current EPA regulations that require the operators of certain facilities to maintain routine emissions below a specified threshold or on occasion to apply the best available technology to reduce emissions.

Event reporting requirements

Reporting requirements stipulate the form and content of data on events indicative of performance that is to be reported to the oversight agency. An example is current ADEC regulations that require the operators to characterize and report spills above a certain threshold.

Different regulatory approaches require different types of oversight expertise. For example, the historic PHMSA approach to oversight required inspectors who understand the details of implementation of controls to support determination of whether operator practices conform to requirements. To address new regulations that focus on requirements to implement management systems (e.g., Integrity Management, Operator Qualification), PHMSA has needed to develop a cadre of inspectors with a knowledge of management systems at a level required to judge whether or not an operator's system is being implemented consistent with requirements and is adequate to its purpose. European practice typically emphasizes management systems knowledge of inspectors to allow them to make needed judgments on system adequacy. To be effective, any oversight system needs to include capability to evaluate factors contributing to events that provide evidence of a breakdown of controls; often these factors go well beyond those explicitly included in regulatory requirements.

2.4 Potential Role of Risk Assessment in Oversight and Management of Risk

Risk assessment is an excellent tool for use by designers and operators in several applications, including:

- Creating a common language for communications among designer, operator and regulator throughout the life cycle of an engineered system;
- Investigating the impact of potentially important system interactions on risk of complex (diverse & redundant) safety, support (e.g., motive power) and administrative (e.g., operating and maintenance procedures) systems;

- Evaluating the merits of changes to operation and design based on their impact on risk, thereby supporting decision-making.

Conducting a formal risk assessment is just one part of managing risk. The nature and importance of contributors to risk change with time, reflecting aging as well as changes in management practices, operator knowledge, operating environment and modifications to the physical system itself. Unless a risk assessment is routinely updated to reflect these changes, it can only provide insight into risks (and therefore into potentially useful mitigative measures) at the time the assessment is carried out. Current risk assessment technology is incapable of identifying many major sources of risk (see discussion in Section 3.6). Risk assessment can, however, play important roles in risk management. Examples, certainly not an exhaustive listing, of these roles are briefly described below.

Evaluating the Adequacy of Facility Design

Risk assessment can be a valuable tool for an operator to use in evaluating the design adequacy of its facility before it is constructed. In this role the strengths of risk assessment tools, even in the absence of facility-specific data, can help investigate systems interactions of potential risk significance. Examples of systems interactions include: (a) the impact of loss of motive power in undermining design redundancy, (b) the impact of a local fire in undermining design redundancy, (c) the impact of single failures (e.g., a stuck open relief valve, flawed test or maintenance activity) on risk, and (d) the impact of catastrophic failure (e.g., pipeline rupture) of one facility on nearby facilities.

Evaluating the Effect of Different Test and Maintenance Strategies on Risk

One type of basic decision an operator must make in operating a high-risk facility is the test and maintenance strategy it will employ. Frequency of functional testing impacts risk as does whether maintenance is corrective, preventive or reliability based. These impacts can be investigated using risk assessment.

Evaluating the Impact of Characterization of Aging Effects

While risk assessment is not capable of determining the physical condition of a facility resulting from aging, it can, in combination with observations on factors like corrosion rates, inform decisions on how the frequency of assessment of physical condition impacts risk.

Evaluating the Relative Priority of Segments for Periodic Facility Assessment

This application is fundamental to the Integrity Management Program (IMP) required by PHMSA for transmission and, more recently, distribution pipelines. These regulations require operators to use risk assessment to identify which pipe segments represent the greatest risk, and therefore need to be assessed first.

Evaluating the Impact of new Knowledge on the Understanding of Risk

As experience is gained through the operation of facilities, the new knowledge can be used to improve risk assessment models and update the insights they offer on the importance of different contributors to risk. This application in the UK and Norway is discussed in Section 3.

Evaluating the Value of Applying New Technology

Most risky facilities are operated over decades, during which time technology affecting safe operation typically changes dramatically. Risk assessment can be used, and is used routinely in the UK and Norway, to evaluate the impact on risk of using newly available technology. This application is discussed in Section 3.

In all of these potential applications the risk assessment is typically carried out by the operator, who is intimately familiar with the facilities, how they are operated and lessons from operating experience. The role of the regulatory agency is typically to provide knowledgeable oversight of operator analysis and the decisions informed by that analysis. This role requires the regulator to be very familiar with the facility, and especially with the lessons learned from thorough analysis of the factors contributing to undesired events and their implications to facility risk.

3 MODELS FOR REGULATORY OVERSIGHT OF RISK ASSESSMENT & RISK MANAGEMENT

This section describes the experience of various regulators in using risk assessment and risk management as part of their intervention approaches. It summarizes experience in the UK and Norway with risk principles (more detail is in Appendix A), the experience of the Pipeline and Hazardous Materials Safety Administration (PHMSA) in using risk in its regulatory approach (more detail is in Appendix B), and the experience of the Nuclear Regulatory Commission (NRC) in using risk techniques to oversee the nuclear power industry (more detail is in Appendix B). It also discusses some typically unregulated factors – factors that cannot be characterized using current generation risk assessment models - that have been shown to be important to managing risks of complex facilities.

Part of the context these regulators must deal with is that severe events happen very infrequently, so regulatory oversight must be capable of inferring from minor events the potential for larger events. Techniques for doing this are more mature in the nuclear power industry where the safety systems are complex, redundant and diverse - characteristics that make formalized risk assessment more useful in investigating system effectiveness.

3.1 Norwegian Approach to Regulating Offshore Petroleum Facilities

The Norwegian Regulatory Process and its Evolution

Norway is very similar to Alaska in its heavy dependence on petroleum production as a mainstay of its economy. The first drilling operation on the Norwegian side of the North Sea started in 1966. Production started in 1971, and in the following years a number of major discoveries were made[1]. By 2006, Norway was the third largest exporter of natural gas and the sixth largest gas producer in the world. Petroleum production has contributed significantly to economic growth and financing of the expansive Norwegian public benefits programs.

Over the years the Norwegian model for regulating petroleum activities in the North Sea has evolved into one described as enforced self regulation. Developing and implementing the regulations has involved the tripartite cooperation of regulator, operator and unions; the resultant model is referred to as the Nordic model. This model developed in part in response to a series of significant accidents on North Sea facilities. Major features of this model evolved as follows.

- Initial Norwegian legislation in 1963 was focused on exploration and exploitation of undersea natural resources. It made no explicit reference to safety issues, but focused on clarifying Norway's rights to develop petroleum resources on the Norwegian continental shelf (NCS).

1 Braut, Geir Sverre and Lindoe, Preben H; "Risk Regulation in the North Sea: A Common Law Perspective on Norwegian Legislation"; **Safety Science Monitor**; Volume 14, Issue 1, 2010.

- Two sets of regulations developed in 1975 and 1976 began to address safety. These two sets of regulations describe requirements related to the design of safety systems and to the content of an emergency plan (addressing personnel safety, environmental pollution and economic loss), but they do not set up any substantive requirements related to safety performance. These regulations also emphasize the role of the regulator to approve the plans made by the licensee: All alterations shall be submitted to the Ministry or its authorized representative for approval by the public authorities concerned.
- The NPD (Norwegian Petroleum Directorate) regulatory guidelines for conceptual safety evaluation (CSE) studies were introduced in 1980. These guidelines introduced a quantitative cut-off criterion for nine types of accidents that could be excluded from further consideration if the maximum frequency of each accident type could be shown to be less than 10^{-4} per year.
- An Act in March of 1985 first introduced requirements related to prevention of safety events. It is explicitly stated that activities pursuant to this Act shall be conducted in a prudent manner and shall take due account of the safety of personnel and environment. It further states: The licensee shall at all times maintain efficient contingency preparedness plans with a view to countering accidents and emergencies, which may lead to loss of lives or personal injuries, pollution or major damage to property.
- New NPD regulations on implementation and use of risk analyses came into force in 1990, and new regulation on emergency preparedness appeared in 1992. These focused on the risk analysis process. The purpose of the risk analyses was to provide a basis for decision making among choices of risk reducing measures. According to the regulations the operator shall define safety objectives and risk acceptance criteria. The objectives express an ideal safety level. Thereby they ensure that the planning, maintenance and the further enhancement of safety in the activities are a dynamic and forward-looking process. Accidental events must be avoided (any actual accidental event is unacceptable). This means that risk is kept as low as reasonably practicable (ALARP), and attempts are made to achieve reduction of risk over time (e.g., to reflect technological development and operational experience). The need for risk reducing measures is assessed with reference to the acceptance criteria. The acceptance criteria and the basis for deciding them are to be documented and auditable.
- Another Act in March of 1992 required the operator to define its own safety objectives: In order to avoid or withstand accidental events, the operator shall define safety objectives to manage the activities. It further required: Risk analyses shall be carried out in order to identify the accidental events that may occur in the activities. Finally, it required the operator to define acceptance criteria. While there was no requirement for approval of resultant documentation by the regulatory authority, this Act did stipulate that the type, extent and submission timing of required documentation shall be stipulated by the Norwegian Petroleum Directorate (NPD) in consultation with the operator.
- In November of 1996 the next phase of legislation addressed three different types of issues: (a) avoiding waste of subsea petroleum resources, (b) maintenance of a high level of safety and its continued improvement in accordance with technology development, and (c) conduct of all activities related to safety and production in "a prudent manner", including provision for involvement by trade unions representing the operator's employees.
- An Act in August of 2001 strengthened the idea of risk acceptance criteria: Harm or danger

of harm to people, the environment or to financial assets shall be prevented or limited in accordance with the legislation relating to health, the environment and safety, including internal requirements and acceptance criteria. Over and above this level, the risk shall be further reduced to the extent possible. Assessments on the basis of this provision shall be made in all phases of the petroleum activities. This reinforced the "as low as reasonably practicable" (ALARP) provision.

- The 2001 Act also introduced the important idea that safety in petroleum operations is affected by factors beyond design and operation, and clarified that decisions on continuing improvements driven by application of the ALARP principle should be cost beneficial: In effectuating risk reduction, the party responsible shall choose the technical, operational or organizational solutions, which according to an individual as well as an overall evaluation of the potential harm and present and future use offer the best results, provided the associated costs are not significantly disproportionate to the risk reduction achieved.
- This Act further stipulated that the operator shall identify objectives whose attainment can be monitored: The objectives shall be expressed in such way as to make it possible to assess to what degree objectives have been achieved. Additionally, the party responsible shall set internal requirements, which put the regulatory requirements in concrete terms, and which contribute to achieving the objectives in relation to health, environment and safety. If the internal requirements are expressed functionally, criteria of fulfillment shall be established.
- New NPD Regulations relating to management of petroleum activities came into force January of 2002. The ALARP principle is one of the fundamental principles on which the regulations are based. The regulations in addition state that the operator shall formulate acceptance criteria relating to major accidents and to the environment. The acceptance criteria shall be used as the basis for evaluation of results from the various quantitative risk assessments (QRAs) and shall be given for: a) personnel on the installation as a whole, and for personnel groups that are particularly exposed to risk; b) loss of main safety functions; and c) pollution from the installation.
- Review of the applicable acts and regulations related to risk analysis and emergency preparedness in Norway shows that there has been an evolution toward increased use of functional requirements through reference to legal standards. In parallel there has been a decrease in the incorporation of specificity of requirements in the legislation.

Comments on Process Effectiveness

The so-called "Nordic Model" emphasizes functional requirements presented in high-level legal standards (e.g., conduct of all activities related to safety and production in a prudent manner). This requires participants in the petroleum sector – operators as well as regulators - to maintain a high level of competence and a willingness to improve continuously. If this assumption is valid, this form of regulation can be expected to lead to a continuously updated and effective regulatory regime.

A recent commentary on the Norwegian regulatory process[2] highlighted the possible over-reliance on quantification implicit in existing regulations. The 1980 NPD regulatory guidelines for CSE studies introduced a quantitative cut-off criterion for nine types of accidents - these could be excluded from

2 Aven, Terje; Vinnem, Jan Erik and Vollen, Frank; "Perspectives on Risk Acceptance Criteria and Management for Offshore Applications - Application to a Development Project"; **International Journal of Materials & Structural Reliability** Vol.4, No.1, March 2006, pp 15-25.

further consideration if the maximum frequency of each accident type could be shown to be less than 10^{-4} per year. These guidelines contributed in a positive manner to the use of formalized quantitative techniques for analysis of risk in the industry, and provided the basis for the industry and regulators to communicate regarding risk and acceptable risk. However, as recognized by the US Nuclear Regulatory Commission a few years later in developing quantitative risk goals for the US nuclear power industry, this approach also had the unfortunate effect of encouraging "number crunching" exercises with the potential diversion of attention away from real safety issues. Too much emphasis can be placed on the methodology and the 10^{-4} target, and quantitative gamesmanship can begin to dominate evaluations both in design and in the ALARP process.

Other potential weaknesses of the system include:

- In a regulatory system based on risk acceptance limits, the operator needs to demonstrate to the regulators that the limits have been met; this is often achieved by referencing the risk results. This system requires strong regulatory oversight, but regulatory review is sometimes rather superficial.
- With the ALARP approach, regulatory involvement needs to be both routine and substantive. Regulators need to implement an extensive evaluation process to determine if the operator has carried out a sufficiently thorough search for alternatives (e.g., possible risk reducing measures).

The use of high-level legal standards in regulatory practice requires a high level of trust between the regulator and the regulated community. The Norwegian approach requires mature participants with a high degree of competence and willingness to remain knowledgeable on technical matters. This approach is quite different from that typically used in the US where the regulators based their control strategy on suspicion toward the industry and inspection against clear prescriptive regulations with penalties for noncompliance.

However, the nature of companies involved in the Norwegian petroleum industry is now changing. A few years ago, there were fourteen or fifteen oil companies operating on the Norwegian continental shelf, all of them large, competent and well-organized companies. Today, this number has increased to seventy; many of these are small companies without much experience. The competition in the industry to hire and retain highly competent people is intense. These factors tend to weaken the underlying regulatory assumption of highly competent participants in the industry, potentially undermining the reliance on high-level legal standards as the basis for regulatory oversight.

Applicability to Alaska Pipeline Infrastructure

The Norwegian experience seems to highlight the potential value of Alaska regulators adopting an ALARP-like process for requiring operators to identify and evaluate the cost effectiveness of potential safety improvements - especially those related to new technology or suggested by thorough analysis of operating experience. Such a process could be adopted without the need for quantitative acceptance criteria, but guidance on cost benefit analysis would be needed to assure strong uniform implementation. This approach would require a cadre of Alaska regulators intimately familiar with developing pipeline safety technology and heavily involved in evaluating the underlying causes of events and possibly even close calls. Depending on the desires of Alaska lawmakers, whose legislative mandate would be needed, the process could focus on issues related to worker safety, public health and safety, environmental degradation, and/or economic sustainability. The dangers of quantitative

gamesmanship would need to be addressed by regulatory focus on substantive improvements rather than statistical manipulation.

3.2 Health and Safety Regulation in the UK

Great Britain Framework for Worker Health and Safety

The British Health and Safety Executive (HSE), in partnership with local authorities, works to protect the British public from the risks from work activities.[3] Great Britain has a tradition of health and safety regulation going back over 150 years. The present system came into being with the Health and Safety at Work etc Act (HSW Act) in 1974 with further significant modifications in 2008. This legislation has at its heart a simple but enduring principle - those who create risk are best placed to control that risk, whether employers, the self-employed or manufacturers of articles or substances for use at work.

The HSE enforces the law in many workplaces, including offshore gas and oil installations. Since the HSW Act was passed, HSE has been engaged in progressive reform of the law, seeking to replace detailed industry-specific legislation with an approach in which regulations, wherever possible, express goals and general principles, and detailed requirements are placed in codes and guidance. Approved codes have a special place in British health and safety law - they set out ways of achieving standards. Those who depart from a code must be prepared to show that their own approach is an equally valid way of meeting the legal requirements. In this way, flexibility is allowed for technological development within a framework set by mandatory regulations. Most aspects of environmental protection are not addressed by the HSE.

The Hazardous Installations Directorate within HSE is responsible for enforcing health and safety legislation in, among other facilities, upstream petroleum industries and pipelines transporting hazardous substances.

Most requirements are expressed as goals or targets which are to be met "so far as is reasonably practicable" (SFAIRP), or through exercising "adequate control" or taking "reasonable" steps. Qualifications such as these involve making judgments as to whether existing control measures are sufficient and, if not, what else should be done to eliminate or reduce the risk. SFAIRP means that the extent of the risk must be balanced against the difficulty involved (in terms of time, money or trouble) in controlling the risk further; additional controls are not necessary if the difficulty in implementing them would be grossly disproportionate to the risk, or to the reduction in risk that would be achieved. This judgment is an essential part of the risk assessment process and will be informed by approved codes of practice, published standards and HSE or industry guidance on good practice.

Regulations Affecting On and Off-Shore Installations

A paper by C. R. Timms offers a good summary of specific safety related regulations for the UK offshore and onshore processing sectors[4]. Safety Case Regulations (SCR)[5] apply to the offshore sector for oil and gas related processing, while the onshore process sector comes under the Control of Major Accident Hazards Regulations 1999 (COMAH)[6] regulations which are applicable to the chemical

3 The UK Health and Safety Executive, "A Guide to Health and Safety Regulation in Great Britain", **ISBN 978 0 7176 6319 4,** 2009.

4 Timms, C R, "IEC 61511 - An Aid to COMAH and Safety Case Regulations Compliance", IEE Event - Safety Instrumented Systems and IEC 61511, 02/12/2003.

5 The Offshore Installations (Safety Case) Regulations 1992 SI1992/2885 HMSO ISBN 0 11 025869 X.

6 Control of Major Accident Hazards Regulations 1999, SI 1999 No. 743 HMSO ISBN 0 11 0821920.

industry, some storage facilities, and industries where threshold quantities of dangerous substances are kept or used.

SCR came into existence for the UK Offshore oil and gas processing sector in 1992 to implement the findings of the Lord Cullen Enquiry[7] following the 1988 Piper Alpha offshore platform disaster, which took 167 lives.

SCR are underpinned by the Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations issued in 1995 (PFEER)[8], and the Offshore Installations and Wells (Design, Construction, etc) Regulations (DCR)[9]. PFEER is focused on identifying and preventing fire and explosion hazards, protecting persons from the effects, and assuring effective response to emergencies, while DCR seek to "ensure that the level of the integrity of the installation is as high as reasonably practicable at all times, and that risks to people on an installation arising from matters of integrity, are kept as low as reasonably practicable" (ALARP). This includes the design, modifications, operation and maintenance.

There are many similarities between the two regulations. Both require operators to demonstrate that they have a Safety Management System (SMS) in place as part of the overall management system. SCR require a Safety Case to be submitted to the UK Health and Safety Executive (HSE) for every offshore installation, while COMAH sites are required to submit a Safety Report. These reports have to address hazards with the potential to cause a major accident and demonstrate the adequacy of the Safety Management System.

It is generally accepted that the management of safety, like most other business management, is now a risk based function and that is the basis of the SMS within COMAH and SCR.

The essence of a Safety Management System is to demonstrate:

- The organization of personnel involved in major hazard management and provision of training;
- Identification of major hazards, likelihood and severity;
- Operational control including maintenance of plant, processes and equipment;
- Management of change including design of new installations and processes;
- Planning for emergencies;
- Monitoring performance; and
- Audit and review of the SMS.

The minimum information to be included in a Safety Report (or Safety Case) can be summarized as follows:

1. Information on the management system with a view to major accident prevention.
2. Presentation of the environment of the establishment:
   a. Site description, environment, geographical location etc.;

7 The Public Enquiry into Piper Alpha Disaster (Cullen Report) Cm 1310 Department of Energy HMSO 1990 ISBN 0 10 113102 X (2 volumes).

8 Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995. Approved Code of Practice and Guidance on Regulations L65 HSE Books 1995 ISBN 0 7176 0874 3.

9 Offshore Installations and Wells (Design and Construction, etc) Regulations 1996, SI 1996/913 HMSO 1996 ISBN 0 11 054451 X.

b. Identification of installations and activities presenting a major accident hazard; and
c. Description of areas where a major accident may occur.

3. Description of the installation:
   a. Main activities and products from the major accident risks perspective with proposed preventative measures; and
   b. Description and inventory of dangerous substances;
4. Identification of accidental risks and prevention methods:
   a. Details of possible major accident scenarios, triggers and probability;
   b. Assessment of the severity of the consequences of identified major accidents; and
   c. Description of technical parameters and equipment used for the safety of installations.
5. Measures of protection and intervention to limit the consequences of a major accident:
   a. Description of the equipment installed in the plant to limit the consequences of major accidents;
   b. Organization of alert and intervention;
   c. Description of mobilized resources, internal and external; and
   d. Summary of the elements necessary for the on-site emergency plan.

Regulations Affecting the Safety of Pipelines[10]

In the United Kingdom, pipeline safety management is governed by the Pipelines Safety Regulations 1996 (PSR) and carried out by the Health and Safety Executive (HSE). These Regulations involve a risk-based approach to safety and require pipeline operators to design, build and operate pipelines to ensure that they are safe, so far as is reasonably practicable (SFAIRP). Pipeline operators, known as duty holders, are required under law to be responsible for the safety of installations under their control. The Health and Safety Executive's Hazardous Installations Directorate (HID) is responsible for enforcing PSR.

The principal health and safety legislation in the UK is the Health and Safety at Work Act 1974 (HSW Act). It requires risks to employees, and others (NB), to be reduced SFAIRP.

The Pipelines Safety Regulations 1996 [PSR] were developed under the HSW Act. The overall aim is to ensure pipelines are designed and constructed properly and operated safely. PSR places the responsibility on operators of "major accident hazard pipelines" to notify HSE about their intended construction and operation. These notifications are assessed by pipeline specialist inspectors. The Regulations cover both onshore and offshore pipelines, are goal setting (i.e., they set out the objectives to be achieved but leave freedom on how these objectives are to be met), and allow risk-based approaches that have to satisfy the principles of SFAIRP.

PSR covers:

- Design of the pipeline;
- Safety Systems;
- Construction and installation;
- Examination and maintenance.

10 Report of the Corrib Technical Advisory Group to Minister Dempsey on an Appropriate Inspection and Monitoring Regime for the Corrib Project, May, 2006.

Certain pipelines are termed "major accident hazard pipelines" [MAHPs]. These include high pressure gas transmission pipelines. Operators of MAHPs are required to notify HSE before the construction, use and modification of the pipeline. These notifications provide HSE with the opportunity to assess compliance with PSR. However, the onus remains with the duty holder to justify that their pipelines are safe.

The Gas Safety (Management) Regulations 1996 (GSMR) require conveyors of natural gas to prepare safety cases to show they are safely managing the flow of gas in their networks. The main aim of the Regulations is to prevent supply emergencies which could have major safety implications for domestic consumers. The safety cases have to be accepted by HSE before gas can be transported.

Inspection

Assessment of the quality of health and safety management is an important element in HSE's approach to inspection. Companies are obliged by law to publish their health and safety policies and are increasingly encouraged to define and monitor their management systems. HSE's inspectors are trained in how to assess management systems, and are able to carry out audits.

Safety reports/cases for major hazard installations identify and evaluate the hazards and describe the management system and the precautions designed to prevent, control or minimize the consequences of any significant accident. In the case of offshore installations, an installation is not allowed to operate unless it has a current safety case which has been accepted by HSE.

The main object of inspection is to stimulate compliance with health and safety legislation and to ensure that a good standard of protection is maintained. If inspectors are not satisfied by the levels of health and safety standards being achieved, they have several means of obtaining improvements:

- Verbal or written information and advice.
- Improvement or prohibition notices. An improvement notice requires a violation to be remedied within a specified time. A prohibition notice is issued if there is, or is likely to be, a risk of serious personal injury, and it requires an activity to be stopped immediately or after a specified time unless remedial action is taken.
- For serious offences, a maximum fine of £20 000 may be imposed.
- In the case of a death resulting from a work activity, the need for a manslaughter investigation is always considered. Such manslaughter investigations, including corporate manslaughter, are conducted by the police, with assistance from HSE.

Managing Risk

Employers are required to document their approach to managing risks to health and safety at the workplace. This should include a clear statement of who is responsible for doing what. HSE places a strong emphasis both on leadership by management, and the meaningful involvement of workers in managing their own health and safety.

Risk assessment ensures that the employer's response in managing risk is appropriate to the risk. The principle of risk assessment is implicit in the HSW Act. It is also explicit in the Management of Health and Safety at Work Regulations which (together with existing legislation) implemented the European health and safety Framework Directive (89/391/EEC). HSE focuses on ensuring that risk assessment is a practical exercise that results in protection from real risks, not simply a paperwork

exercise; it therefore places emphasis on keeping paperwork fit-for-purpose and ensuring that actions identified are implemented in practice. HSE does not stipulate a single risk assessment methodology, allowing organizations to use different methodologies according to the circumstances. However, its guidance Five Steps to Risk Assessment sets out a straightforward methodology that subject matter experts (SMEs) can apply.

HSE's own approach to making policy decisions (e.g., whether regulations should be introduced, revoked or amended) is set out in its publication Reducing Risks, Protecting People: HSE's Decision-Making Process. The document sets out the stages in decision making, as well as the factors to be taken into account and is based upon the principle of tolerability of risk.

Recognizing the importance of decisions at the corporate executive and Board level to either bolster or undermine operational management efforts to manage safety, the UK passed the Corporate Manslaughter and Corporate Homicide Act of 2007[11], also referred to as the Turnbull Act. This Act provides the basis for prosecuting executives or Board members if they are found negligent in discharging their safety responsibilities.

A prosecutable offence occurs when "(1) An organization to which this section applies is guilty of an offence if the way in which its activities are managed or organized: (a) causes a person's death, and (b) amounts to a gross breach of a relevant duty of care owed by the organization to the deceased." The Act applies to, among other operations, all Corporations. It provides that "(3) An organization is guilty of an offence under this section only if the way in which its activities are managed or organized by its senior management is a substantial element in the breach referred to in subsection (1)".

While this approach may seem somewhat draconian by US standards, it underlines the realities that effective management of risks must include knowledgeable involvement by those who make resource decisions, and that there must be consequences for irresponsible decision making. Absent this involvement, no amount of risk assessment can prevent events that adversely impact the interests of workers, people living near industrial facilities, and people whose economic well-being depends on the smooth functioning of these facilities.

Applicability to Alaska Pipeline Infrastructure

The SFAIRP process used in the UK is similar to the ALARP process used in Norway, and the implications to regulation of the Alaska pipeline infrastructure are similar. A distinction of the overall regulatory approach in the UK, designed to promote corporate executive accountability for safe operation, is the Corporate Manslaughter and Corporate Homicide Act of 2007, also referred to as the Turnbull Act. This Act provides the basis for prosecuting executives or Board members if they are found negligent in discharging their safety responsibilities. Implementing a similar provision in Alaska would require a legislative mandate; could easily lead to court challenges; and, given the relatively rapid turnover of pipeline executives in Alaska, would require thorough evaluation of underlying causes of any event to hold one or more executives responsible for these causes accountable.

3.3 The Australian Approach to Pipeline Safety Management [12]

The Australian approach to managing pipeline safety has evolved from one dominated by prescriptive

11 Corporate Manslaughter and Corporate Homicide Act 2007, CHAPTER 19, July 26, 2007.

12 Tuft, Peter, "The Australian Approach to Pipeline Safety Management", Proceedings of IPC2008, 7th International Pipeline Conference, September 29-October 3, 2008, Calgary, Alberta, Canada, IPC2008-64622.

(command and control) requirements, derived from adaptation of pipeline safety standards used in the US (ASME/ANSI B31.4 (hazardous liquid) and ASME/ANSI B31.8 (gas)), to an approach involving elements borrowed from other countries as well as elements that are distinctively Australian. The most recent step in this evolution occurred in 1997 with a major revision of the Australian standard AS 2885. The elements in the Australian approach for new pipelines are summarized below.

- Oil and gas pipelines in Australia are designed, constructed and operated in accordance with AS 2885, a risk-based standard. While it does contain numerous design requirements, their application is flexible and to some extent dependent on the outcomes of a mandatory safety management study. The major elements of such a study are summarized below.
- There is a strong focus on identifying causes of failure and designing against them using a cause/control model of risk management; little use is made of quantitative risk assessment.
- Driven primarily by the fact that at least 80% of events in Australia are caused by external forces, pipeline design requirements for pressure resistance and resistance to external force are treated separately. Pipe in a high consequence area (defined in Australia as "a location where pipeline failure can be expected to result in multiple fatalities or significant environmental damage") must be able to resist rupture resulting from damage inflicted by excavation equipment expected to be in use in the pipeline location.
- For external events, the standard requires *"A pipeline shall be designed so that multiple independent physical controls and procedural controls are implemented to prevent failure from external interference by identified threats."*
- As part of the design process, a formal safety management study is required for any pipeline. Overall pipeline safety review involves a two step process:
  - Design Review: Identify every potential threat to the integrity of the pipeline, and if possible apply controls so that "failure as a result of that threat has been removed for all practical purposes".
  - Risk Assessment: Rank any remaining threats that are not fully mitigated, and ensure that the residual risk is reduced to a tolerable level.
- The ranking process makes use of expert judgment in qualitatively determining the likelihood and consequences of remaining (not fully mitigated) threats. The tool used in this ranking process is a risk matrix in which verbal descriptions of the level of potential consequences and the frequency of occurrence of possible events are used to capture expert opinion. One of five qualitative levels of risk is associated with each frequency/consequence pair. Requirements for corrective action are specified for each risk level. (Note, as early as the late 1980s the author developed and applied similar risk matrix models to support qualitative risk assessment using expert panels as part of processes leading to decisions on which risks were most significant and what mitigation measures were most cost effective. These applications were in the uranium enrichment business and at numerous hazardous facilities operated by the US Department of Energy.)

Applicability to Alaska Pipeline Infrastructure

The Australian approach represents a unique way to managing the pipeline risk beginning at the design stage. In Alaska it could be considered as a practical way to introduce risk management at the design stage of a new pipeline project. The use of the qualitative risk matrix would be worth

considering in Alaska as a tool for bringing together expert judgment in the Operator Strategic Management Process discussed in Section 4.2.

3.4 US Approach to Regulating Pipeline Safety and Health Risks

Over the past several years the Office of Pipeline Safety (OPS, the predecessor agency to PHMSA) has developed and implemented a different approach to structuring its regulations and to carrying out the inspections it uses to evaluate operator conformance with the provisions of these regulations.[13] Several new Rules have been promulgated incorporating provisions that are a combination of prescriptive, performance-based, and management-based. These regulations have introduced, for the first time, requirements to carry out and apply a risk assessment.

The new rules have been designed to allow operators flexibility in their approach to addressing the objectives of the regulations. One ingredient in the approach OPS chose is the imposition of "management-based" requirements. These requirements prescribe implementation of a program that includes the need for several management practices. The new rules allow some flexibility in which management practices are selected and exactly how they are implemented.

Prior to development of these regulations, OPS spent several years interacting with operators in the pipeline industry in the Risk Management Demonstration Program (RMDP). This program was successful in establishing a standard for risk assessment models, and in initiating a trust-building dialog with the industry.

Inspection against management-based provisions is different from inspection of purely prescriptive requirements. Management-based requirements provide flexibility in how operators evaluate, justify and change their practices to satisfy the intent of the rule within their unique operating environment. While such changes are designed to lead to improved performance, they will not immediately manifest themselves in recognizable changes in performance, so finely tuned measures of performance are needed to help evaluate the effectiveness of the new requirements.

Regulations requiring Integrity Management Programs (IMP) for hazardous liquid pipelines and gas transmission pipelines were established between 2000 and 2003. These rules require that pipeline operators analyze the risks associated with their pipelines, including threats that could cause pipeline accidents and the consequences that might result if pipeline accidents were to occur. The regulations included no explicit requirements on how the risks were to be analyzed, but did include requirements on how the risk models were to be applied. Required applications include prioritization of pipe segments for "assessment" (i.e., evaluation of their physical condition using inline inspection tools or equivalent technologies), and evaluation of candidate preventive and mitigative measures for application in addressing significant risks.

Integrity Management Programs for hazardous liquid and gas transmission pipelines provide for increased safety focus on segments of the pipeline that can affect high consequence areas (HCA). HCAs are defined differently for hazardous liquid and gas transmission pipelines, because of differences in the nature of the commodities. Hazardous liquids released from a pipeline in an accident remain on the ground, can enter streams and flow across the ground surface, and can affect populated areas, drinking water intakes, and threatened ecological resources. PHMSA maps the location of these critical resources and pipeline operators must determine which segments of their pipeline could affect

13 "Regulatory Process Changes at the Office of Pipeline Safety", International Pipeline Conference, IPC04-0539, Wiese, Jeff; von Herrmann, Jim; Wood, Paul; October 4-8, 2004.

them if an accident were to release hazardous liquid.

Gas released from a gas transmission pipeline rises and disperses in the atmosphere unless the gas is ignited. If ignited, accident consequences are limited to the immediate area where the gas was released and ignited. Pipeline operators identify HCAs by determining the area near their pipelines containing specified populations that might be affected if a pipeline rupture and explosion and fire would occur.

Operators of hazardous liquid and gas transmission pipelines periodically must inspect segments of their pipelines that could, in the event of an accident, affect an HCA using devices that can detect defects such as corrosion on buried pipelines. The priority for scheduling these segment inspections must be established using risk assessment models. The models must also be used to evaluate which additional preventive and mitigative measures are needed to protect the covered segments.

IMP regulations establish criteria that define defects that operators must repair within specified time limits when defects are discovered in segments that can affect an HCA.

The new IMP rule for gas distribution pipelines differs from those for transmission pipelines in two key areas:

- It does not limit attention to HCAs. Distribution pipelines are located in populated areas and an accident anywhere could affect people. The distribution IMP rule requires that operators evaluate and appropriately increase protection for their entire pipeline.
- It does not require periodic inspection. The inspection techniques used for other pipelines cannot be used on distribution pipelines, which consist of smaller pipes with many branches.

The new IMP rule for gas distribution pipelines, like the other IMP rules, requires that operators analyze the risks to their pipelines and implement additional and accelerated (AA) measures to protect them from threats.[14]

The IMP regulations for gas and hazardous liquid transmission pipelines have resulted in identification and repair of 35,146 physical defects: 3,291 in gas pipelines and 31,855 in liquid pipelines.

Applicability to Alaska Pipeline Infrastructure

Integrity Management Program (IMP) requirements have become a major new element of the PHMSA approach to regulating pipeline safety. Somewhat different requirements have been put in place for liquid transmission pipelines (nearly all of which can be inspected using in line inspection technology), gas transmission pipelines (many of which can only be inspected using "direct assessment" technology) and gas distribution pipelines (for which no physical inspection requirements are included in the regulation). Essential elements in all three approaches include requirements to continuously evaluate all available data to infer the potential for pipeline failure, and to develop and use risk models to identify areas of particularly high risk. Information on segment risk is then used either to accelerate re-inspection or to implement additional or accelerated actions to mitigate the risk. The State of Alaska might consider development of its own integrity management program requirements drawing on the IMP features developed by PHMSA.

3.5 US Experience in Regulating Nuclear Power Risks

The application of Probabilistic Risk Analysis in the regulation of the commercial nuclear industry has followed a tortuous path toward its current role as fundamental to informing safety decisions.

14 PHMSA published a final rule requiring IM programs for gas distribution pipelines on December 4, 2009.

Its initial use in the 1975 Reactor Safety Study (WASH-1400) was as a political communication mechanism designed to place the risk from nuclear plants in perspective with other more commonly encountered risks. Later it was used as a means of evaluating and supporting regulatory decisions on features needed to assure the safety of older nuclear plants having design and operational features dramatically different from the more standardized current generation plants.

It was during the evaluation of older, non-standard plants that the concept of risk management was first introduced by nuclear licensees as a means of using information on the major sources of risk to support better decisions on changes in regulatory mandated operational practice and design features. Still later, following the accident at the Three Mile Island plant, the insights from risk assessment were applied to develop and negotiate compliance schedules for a massive wave of new requirements. These compliance schedules resulted from a management process usually called an Integrated Resource Management System (IRMS).

Eventually concerns regarding the insufficiency of regulations on management of events "beyond the design basis" led to requirements to perform "consistent" Individual Plant Examinations (IPE). These studies provided the basis for broader industry consideration, in risk terms, of an array of operational issues on which highly prescriptive requirements were perceived to be both excessive and counterproductive. Eventually, the NRC and the nuclear industry began working together to use risk management as a means of customizing operational requirements to the unique features of each plant.

During this time the basis on which the NRC incorporates risk insights in its decision processes evolved. Early applications of risk assessment and management required no decisions, only the communication of available risk insights. Because of the political purposes of these early applications, the public debate on the risk results focused on the uncertainty of the data and analysis rather than on the inherent value of the risk insights in managing and regulating the plants. As selected licensees moved toward using the results of risk analysis to manage identified risks, the NRC became more receptive to using their regulatory discretion to provide relief on the means of satisfying requirements and on the time frame for compliance with these requirements. The regulatory foundation for the early NRC receptiveness was provided by special programs, such as the Systematic Evaluation Program (SEP), in which unique treatment of licensees was justified by the unique design and operational features of their facilities (e.g., small, old plants staffed by highly experienced staff).

The next wave of applications of risk assessment and management resulted from the NRC need to plug the regulatory gap associated with accidents beyond the design basis. This was accomplished by an industry sponsored effort to develop "consistent" methodologies to evaluate risks, and an NRC requirement to implement these methodologies. Thereby the NRC gained the ability to assess the need for additional plant-specific requirements to fill the regulatory gap, and the entire nuclear industry developed the models needed to evaluate plant safety and regulation issues in risk terms. This broad ability to understand plant risk has produced pressure by the industry to allow relief from some of the more onerous and expensive generic requirements. This broad industry desire for the NRC to consider risk in their decision process is leading to a replacement of the ad hoc regulatory decision process by one that is highly formalized and therefore "consistent" and repeatable. The need for the increased regulatory formalism seems clearly to result from the broader based industry interest in the use of risk assessment and management in regulatory interactions and resulting decisions.

As discussed in Appendix B, the accident at Three Mile Island provides an example of the importance of root-cause analysis and of communicating the lessons to the regulator and within the regulated

community. An event very similar in causality to the Three Mile Island (TMI) incident occurred prior to the Three Mile Island accident, at the Davis-Besse nuclear plant in the late 1970s. The event was nearly identical to the one that occurred nearly a year later at the TMI nuclear plant. The only difference was that the lead operator on duty recognized what was happening and took different action than he had been trained to take, thereby averting serious consequences. The implications of this event were not understood and communicated among the operators of the five plants with similar design. This seemingly simple act could have prevented the accident at TMI

Major conclusions from the NRC and nuclear industry experience with risk analysis and risk management include:

- Significant beneficial impact on design and operational safety has resulted from the application of risk analysis insights to the management of risks. Risk technology in the commercial nuclear industry was initially applied excessively for policy purposes and focused on risk analysis rather than risk management. This led to a narrow focus on tools, methods and data to the detriment of decisions and actions rooted in the insights of the analysis.
- Early risk analyses were carried out by the NRC and its contractors. This situation proved detrimental to recognition of the value of risk analysis and risk management by the nuclear licensees. Risk management began to gain favor only when the licensees took charge of the development and use of the risk models.
- Traditional prescriptive regulatory practice by its nature focuses attention on one part of the risk spectrum (e.g., design, inspection, testing) at a time. Risk analysis and management allow the effective integration of design and operational characteristics, thereby allowing trade-off strategies to be identified to best manage known risks. This capability continues to be especially valuable in the nuclear industry in developing and evaluating the safety implications of test, inspection and maintenance strategies that are alternatives to those imbedded in current regulatory standards.
- Over the more than thirty years when risk analysis and risk management have been used in the nuclear industry, the NRC has relied primarily on its general regulatory authority to require analyses and to make decisions on safety issues.
- Only after decades of application did the Commission see a need to formalize the internal processes for review and acceptance of risk-supported arguments through the development of Regulatory Guidance and Standard Review Plans. Historically, decisions have been made based on consideration of existing regulations and expert judgment on the validity of risk-supported arguments.
- Risk management programs, where they exist, have been defined by the licensee. However, the tools used in the risk management programs, that is the probabilistic risk analyses, have always been subjected to extensive expert review by the NRC and its contractors prior to the acceptance of arguments for changes to requirements supported by the application of these tools.
- The NRC has used risk-based measures of the importance of systems, structures and equipment to influence the frequency and depth of inspections.
- The NRC has developed a network of experts in risk assessment and risk management,

both within and outside the agency, who can be called upon to provide expert judgment or analytical services when needed. There is a formal internal training program for NRC employees that is currently being expanded to support the increased use of risk assessment encouraged by the 1995 Policy Statement.

Because of the long time during which probabilistic risk assessment and risk management have been in use within the NRC, these tools have received wide organizational acceptance as valuable supplements to existing requirements and practices. This acceptance has been fostered by the enthusiastic support of regulators who have been promoted to influential positions within the agency over the years.

Applicability to Alaska Pipeline Infrastructure

The principal implications of US nuclear risk regulatory experience to Alaska pipeline regulation are summarized below.

- The purpose of any risk assessment effort must be clearly defined at the outset; overemphasis on the political or public communication aspects may lead to under utilization of the resultant insights in managing risks.
- There are fundamentally important elements of a regulatory risk oversight program that build on and go beyond quantitative assessment of risk; most significant is aggressive evaluation of the causes underlying events that are critical to understanding and managing risk.
- Significant attention and effort are required to train and develop people skilled in evaluating operator risk management programs.
- Development of a mature risk oversight process requires the involvement of the industry over a long time frame during which the benefits to achieving shared objectives are demonstrated.

3.6 Summary of How Different Federal and Foreign Oversight Agencies Regulate Risk

Table 3-1 compares three different agencies: the Norwegian Petroleum Directorate (NPD), the Health and Safety Executive in the United Kingdom (HSE) and the Pipeline and Hazardous Materials Safety Administration (PHMSA) in the US.

Summary observations from the three regulatory programs include:

- Risk based decisions are the foundation of European regulatory process (in the US it is an after-the-fact overlay driven by Integrity Management Program (IMP) regulations).
- The UK has recently recognized the fact that risk regulation will not address all factors important to the management of risk by passing the Corporate Manslaughter and Corporate Homicide Act of 2007, also referred to as the Turnbull Act. This Act provides the basis for prosecuting executives or Board members if they are found negligent in discharging their safety responsibilities.
- The European regulations explicitly incorporate provisions, without changes to the regulations, for dealing with new information on risk and new technology to support risk management.
- The European approaches lead to the possibility that key provisions (ALARP and SFAIRP)

will be addressed by quantitative gamesmanship, which requires an even higher level of inspector skill to recognize.

- All three approaches require inspectors with expertise different from that needed to evaluate whether a prescriptive requirement has been satisfied; they must be able to make judgments on the adequacy of operator systems and practices.

Additional information on the NPD and the HSE regulations and programs is provided in Appendix A.

Table 3-1. Summary of different approaches to requiring and overseeing risk assessment.

Question	Norway - NPD	United Kingdom - HSE	US - DOT
What is the nature of the regulatory regime?	The Nordic Model – "enforced self regulation."	Regulations typically express goals and general principles, and detailed requirements are placed in codes and guidance.	Highly prescriptive requirements recently supplemented by management systems requirements.
Is a risk assessment mandated?	Yes, by the NPD; developing and implementing the regulations has involved the tripartite cooperation of regulator, operator and unions.	Yes, by the HSE. Pipelines Safety Regulations 1996 (PSR) include a risk-based approach to safety and require pipeline operators to design, build and operate pipelines to ensure that they are safe, so far as is reasonably practicable (SFAIRP).	Yes, by PHMSA in its Integrity Management Program regulations.
For what purpose?	Risk must be maintained "as low as reasonably practicable" (ALARP).	To provide the basis for decisions on actions to assure risk is "so far as is reasonably practicable" (SFAIRP).	To support implementation of Integrity Management Program (IMP) regulation.
Who carries out the risk assessment?	Operator	Operator	Operator
What is analyzed?	The approach evaluates the risk of harm or danger of harm to people, the environment and to financial assets.	The Regulations cover both onshore and offshore pipelines, are goal setting (i.e., they set out the objectives to be achieved but leave freedom on how these objectives are to be met), and allow risk-based approaches that have to satisfy the principles of SFAIRP.	Pipelines - focus is on High Consequence Areas.
Are methodologies specified?	No, but guidelines are provided.	No, but guidelines are provided.	No, but methodologies must be able to support specific risk-informed decisions.
What use is made of models & results?	The operator is required to define safety objectives and risk acceptance criteria, then to analyze risks to ensure they are met.	Models support operator decisions and regulatory oversight over design, construction and operation of pipelines to ensure that they are safe, so far as is reasonably practicable (SFAIRP).	Rank pipe "assessment." Choose preventive & mitigative measures.
How are continuing opportunities for improvement considered?	Through the ALARP process. In effectuating risk reduction, the operator chooses among technical, operational or organizational solutions.	Through the SFAIRP process.	Operators are required to update assessments and reconsider opportunities for preventive & mitigative measures.

Question	Norway - NPD	United Kingdom - HSE	US - DOT
What is the role of the regulator in a risk assessment process?	With the ALARP approach, regulatory involvement needs to be both routine and substantive. Regulators need to implement an extensive evaluation process to determine if the operator has carried out a sufficiently thorough search for alternative risk reducing measures. ALARP decisions are made on a cost-benefit basis.	HSE focuses on assessing compliance with PSR. An offshore installation is not allowed to operate unless it has a current safety case which has been accepted by HSE. Certain pipelines, including high pressure gas transmission pipelines, are termed "major accident hazard pipelines" [MAHPs]. Operators of MAHPs are required to notify HSE before the construction, use and modification of the pipeline.	PHMSA inspects reasonableness of assessment & its application in managing pipeline integrity.
How well does the process work?	The Norwegian approach requires mature participants (both operator and regulator) with a high degree of competence and willingness to remain knowledgeable on technical matters. This expectation has become less valid as the number of participants in the industry has significantly expanded.	The process seems to work, but requires inspectors who are experienced and competent in various types of risk assessment. Recently the UK has acknowledged the importance of decisions at the corporate executive and Board level, which are not evaluated in safety cases (see below).	The process is evolving, and requires a level of inspector expertise that is only now being developed. Presently the weakest part of implementation of integrity management regulations seems to be operator decisions on additional preventive and mitigative measures.
Does the approach seem to have application in Alaska?	This approach, which is the basis of the Norwegian regulatory system, carries with it the risk of possible over reliance on quantification. The implementation risk is that excessive effort will be expended in quantitatively justifying why no change is needed. The Norwegian system requires strong regulatory oversight, but regulatory review has been critiqued as sometimes rather superficial.	The approach is the basis of the UK regulatory system, so it would likely impose an excessive burden on operators in Alaska if it were added to the existing regulatory systems.	Broader application of the essential features of integrity management regulations to the entire Alaska pipeline infrastructure might increase the assurance of integrity, but it alone would not address the full spectrum of factors affecting the public interest.

3.7 Summary of Factors Important to Managing Risk that are Not Typically Regulated

Many of the factors that have contributed to events in Alaska are not typically addressed in risk assessments, nor are they covered by regulation. Recent evidence of this observation appears in three studies focused on British Petroleum (BP): one commissioned by BP and carried out by Booz Allen Hamilton following the North Slope spill events in 2006; another carried out by the US Chemical Safety Board (CSB) following the explosion and fire at the BP Texas City refinery in 2005; and the last commissioned by BP and carried out by an expert panel chaired by James Baker (The Baker Panel), also addressing the 2005 BP Texas City disaster.

These three expert evaluations of significant accident events highlight a number of factors that are rarely if ever regulated or even monitored by safety oversight agencies, including: safety management systems, safety culture, corporate safety oversight, and excess priority on budget issues. In spite of the criticality of these factors in managing safety (or environmental or production) risks, current generation quantitative risk evaluation methods typically ignore them, in large part because quantification of related risks would be extremely difficult. On the other hand, outside observers with requisite skills and experience can recognize the presence of these factors if they have access to people in an organization and the ability to observe management processes in operation.

Figure 3-1 below shows the scope of regulatory authority of the Pipeline and Hazardous Materials Safety Administration in overseeing pipeline safety. This figure makes the same point about the unregulated nature of many factors critical to performance as did the three expert groups that reviewed BP.

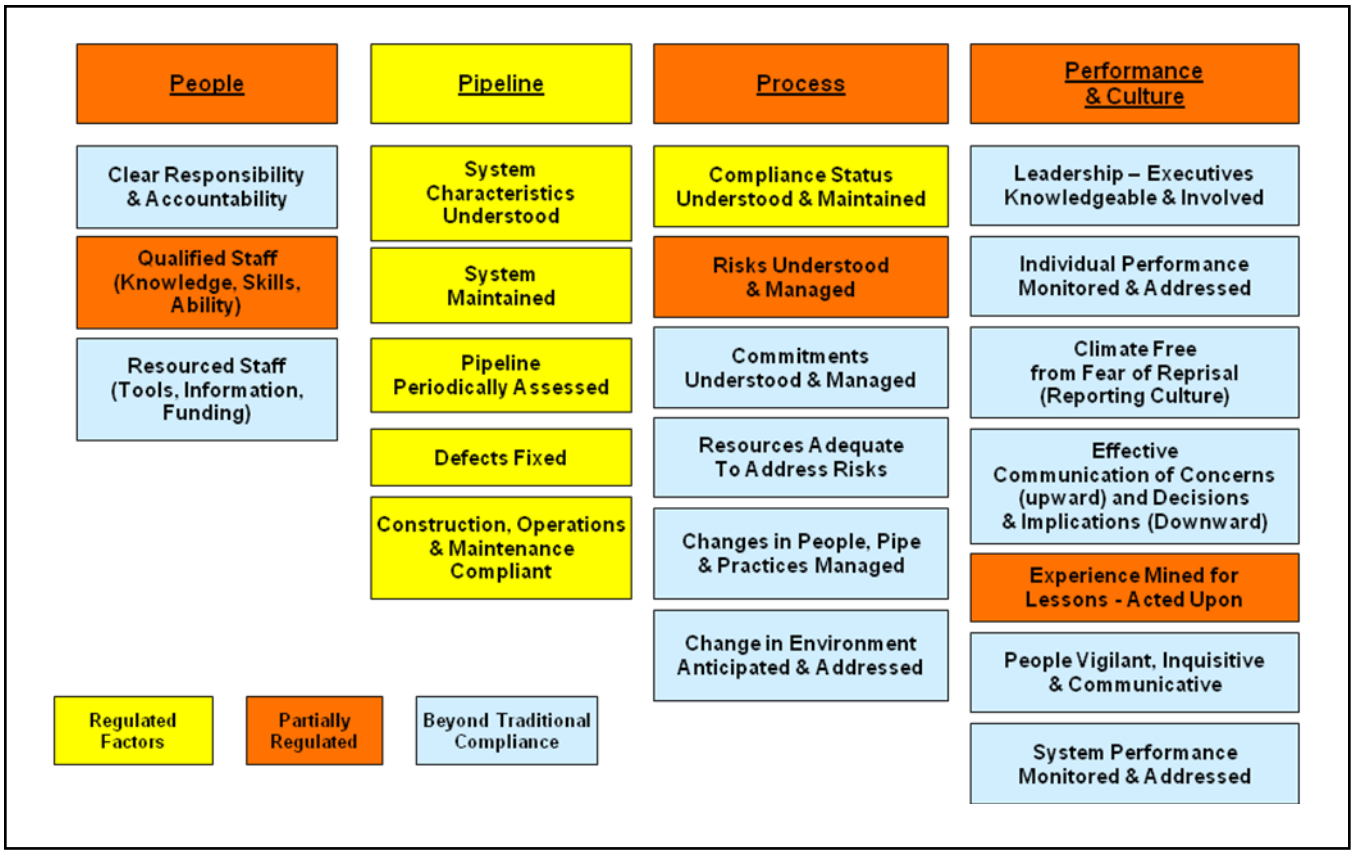


Figure 3-1. Organizational characteristics supporting high performance - scope of PHMSA regulation.

4 RECOMMENDATIONS FOR STRENGTHENING REGULATORY OVERSIGHT IN ALASKA

This section describes the relevance to Alaska of lessons in the application of risk management practice from other regulatory environments. Recommendations presented are designed to enhance ADEC-specific risk management practices and to strengthen risk management practice across Alaska oversight agencies.

Currently the Alaskan petroleum infrastructure is regulated by a network of State and Federal agencies, each having different jurisdiction, approach and expertise. While this oversight network seems largely to have been effective in looking after the varied interests of the people of Alaska, recent major pipeline spills on the North Slope are evidence that improvement in oversight may be possible.

In overseeing the operation of any complex and risky engineered system, the basic principle regulators typically follow is the operator is ultimately responsible for the safe operation of its facilities and the regulator should require practices that reinforce the operator's responsibility then provide knowledgeable oversight of implementation of those practices. The recommendations presented in this section align with this principle.

The recommendations are separated into two groups: future risk management actions for consideration across Alaska oversight agencies (Section 4.1), and candidate changes the Alaska Department of Environmental Conservation might make (Section 4.2). There is significant commonality in what the recommendations are designed to accomplish. The primary purpose of the set of recommendations is to strengthen the Alaska regulatory agency knowledge and awareness of risks, and to improve agency access to information on the operators' perspective on changing risks as well as on their plans to manage these risks. Additionally, Section 4.3 discusses practical considerations in enhancing oversight of risk management.

4.1 Recommended Future Alaska Oversight Agency Risk Management Activities

Recommendations for future risk management activities for agencies in Alaska are presented in response to two key questions:

- Considering the initial intent of the Alaska Risk Assessment (i.e., to assure satisfactory operation of the infrastructure for the next 50 years) should the State of Alaska continue to pursue a Risk Assessment managed by the State?
- Are there other regulatory oversight models that should be considered (e.g., nuclear) to address: aging infrastructure, the entire infrastructure (not just pipelines), and reliability & safety?

Considering the initial intent of the Alaska Risk Assessment (i.e., to assure satisfactory operation of the infrastructure for the next 50 years) should the State of Alaska continue to pursue a Risk Assessment managed by the State?

RECOMMENDATION 1 – The State of Alaska Should not unilaterally Undertake a Risk Assessment of its Petroleum Infrastructure

None of the regulatory agencies surveyed has attempted to unilaterally carry out a risk assessment of facilities they oversee. The level of knowledge of the design, management and operational experience required to carry out a meaningful risk assessment is too great for most regulators. Furthermore, any risk assessment represents a snapshot in time of risks; to have continuing value the assessment must be maintained to reflect the current design, operational practice and knowledge. Maintenance of a risk assessment is typically beyond the scope of oversight agencies. Additionally, risk assessment is not designed to contribute to understanding the condition of the pipeline infrastructure. Consequence screening could help operators determine where the consequences of potential failures are greatest, thereby informing decisions on where infrastructure characterization (e.g., using in-line inspection or other technology) is most critical. That is the approach the U.S, Pipeline and Hazardous Materials Safety Administration has taken in its Integrity Management Program (IMP) regulations. Those regulations begin by defining High Consequence Areas (HCAs), and then require operators to determine which segments of pipe if they failed could affect those areas, and finally to periodically assess (i.e., evaluate the physical condition of) those segments.

In Alaska, virtually all locations are areas of potentially high consequences, so a different type of consequence screening would be required. Examples could include screening based on the potential size of a spill or on the degree of disruption of the petroleum supply associated with a pipe failure.

Are there other regulatory oversight models that should be considered (e.g., nuclear) to address: aging infrastructure, the entire infrastructure (not just pipelines), and reliability & safety?

There are numerous practices used by the regulatory agencies studied that have application in strengthening oversight of the Alaska pipeline infrastructure. The remaining recommendations draw on these practices.

RECOMMENDATION 2 – Strengthen Regulatory Oversight by Evolution not Revolution

The Alaska petroleum transportation infrastructure has been in place for several decades. Numerous State and Federal Agencies have well established roles in overseeing the safety and environmental compliance of an even larger number of individual operators. Attempting wholesale restructuring of this regulatory system is impractical for the existing infrastructure; therefore considering an evolutionary approach to improving the effectiveness of regulatory oversight seems appropriate. The remaining four recommendations are designed to support an evolutionary improvement in oversight of the existing pipeline infrastructure in Alaska.

RECOMMENDATION 3 - Require Operator Strategic Management Process

Critical operator performance management functions, which are even more critical on the North Slope where the petroleum crude characteristics are changing significantly and the processing and transport infrastructure is aging, include:

- Monitoring and learning from operating experience - including conducting thorough root cause analysis and monitoring leading indicators of future performance;

- Anticipating changes in the operating environment; and
- Systematically allocating resources and taking action to address important lessons and anticipated changes.

Examples of major changes having the potential to impact safe operation of Alaska's petroleum facilities include:

- Changes in the climate;
- Changes in the likelihood of serious natural events (e.g., seismic, ground movement, volcanic activity, discontinuity of permafrost, avalanches or landslides);
- Changes in the flow rate and physical/chemical characteristics of crude oil; and
- Cascading impact of the factors above on support structures and critical infrastructure (e.g., bridges, power supply).

An oversight agency typically has access neither to the information nor to the staff resources necessary to effectively carry out the three functions listed above, but they should be able to monitor and evaluate the effectiveness of related operator programs. Table 4-1 provides additional guidance and criteria that such a program would need to satisfy. Such an innovative regulatory oversight approach would provide the regulatory agencies a significantly better window into operators' understanding of risks and their decisions on how to manage these risks. While not yet applied in the pipeline industry, such a strategic oversight approach has been applied in the U.S. commercial nuclear power industry for over twenty-five years. There it is referred to as "Integrated Resource Management System" (IRMS). An oversight approach that imbeds a similar concept can be designed to have the advantages of the European ALARP and SFAIRP process without the reported disadvantage implicit in these systems. The disadvantage is these requirements often lead to "dueling PhD" discussions on subtleties of complex risk analysis rather than focusing attention on real technical and operational issues.

Table 4-1. Strategic Resource Management Program for Alaska Petroleum Infrastructure.

Guidance on a Strategic Resource Management Program
To reduce the likelihood that recent problems experienced by North Slope operators recur, Alaska regulators need to require operators to develop, implement and maintain a comprehensive program designed to: • Monitor and learn from operating experience - including conduct of thorough root cause analysis and monitoring leading indicators of future performance; • Develop and carry out a forward-looking evaluation of their operations leading to a complete Path Forward Program Plan for addressing existing issues and developing concerns on a time frame consistent with their priorities; and • Institutionalize the planning process in a Strategic Resource Management Program (see criteria below) so new issues are actively identified and, based on their significance, incorporated in the Path Forward Program Plan. Because the best approach to resolving all concerns may not presently be known, the planning process will necessarily include strategic studies leading to additional actions to be integrated into the Path Forward Program Plan. Oversight agencies should consider how best to work with North Slope operators first to ensure the strength and integrity of the Path Forward Program Plan, then to monitor operator progress in implementing and amending the Plan to reflect both new operating experience and the results of strategic studies. This process will contribute significantly to assuring oversight agency concerns are addressed effectively and to minimizing the occurrence of future concerns.
Criteria for a "Path Forward" Plan
Operators of the Alaska petroleum infrastructure should satisfy the following criteria in developing and implementing a Path Forward Program Plan. Operators will document for agency review: 1. Operators will document for agency review: a. The process they propose to use to prepare the Path Forward Program Plan, including the time frame on which the Plan will initially be completed and the subsequent update frequency; and b. The processes they use for monitoring and learning from operating experience - including conducting thorough root cause analysis and monitoring leading indicators of future performance. 2. The Path Forward Program Plan will be comprehensive in treating recognized and anticipated issues related to the safe (and/or highly reliable or environmentally sound) operation of operator facilities; 3. The Path Forward Program Plan will incorporate the results from a comprehensive, operator-conducted risk analysis of the system and the organizational entities impacting its safe operation; 4. The Path Forward Program Plan will incorporate the results from some form of strategic analysis carried out to characterize the impact on pipeline system safety (and/or reliability or environmental soundness) of changes in the pipeline system, the environment in which it operates and the people on whom its safe operation depends; 5. When issues are identified (e.g., changing feed stock flow rate and characteristics) for which resolution requires further study, the Path Forward Program Plan will include these strategic studies, and will incorporate recommended resolution strategies resulting from the strategic studies when they have been completed; 6. The Path Forward Program Plan will define the time frame on which recognized issues will be resolved, and the time frame will be consistent with the importance of the issues; 7. Any constraints (e.g., financial, management capacity, availability of qualified workforce, weather, availability of necessary hardware) affecting the time frame for issue resolution will be described in documentation for the Path Forward Program Plan; and 8. The implementation status of the Path Forward Program Plan will be updated periodically and status information will be made available for regulatory agency review. A Path Forward Program Plan consistent with the above criteria must be a living document, updated periodically to reflect changes in safety (and/or reliability or environmental) concerns and knowledge of the systems and the environment in which they operate.

4.2 Recommended ADEC Activities

The discussion of candidate changes for ADEC addresses two key questions:

- Is the current "Command and Control" method of industry oversight satisfactory or should it be supplemented to improve its effectiveness?
- How might the current oversight model be improved to help ensure the continuing integrity of the existing infrastructure?

Is the current "Command and Control" method of industry oversight satisfactory or should it be supplemented to improve its effectiveness?

Command and control is an essential element of the U.S. approach to regulating risky industries. While it has been effective, it does have its limitations. Chief among these limitations is that regulators must anticipate potential risks early enough to promulgate new highly prescriptive regulations to address the risks, and must be knowledgeable and prescient enough to know the best controls to prescribe to address the risks. These are difficult conditions for a regulator to meet in a static situation, but nearly impossible to meet under the ever-changing conditions in petroleum production and transport in Alaska.

In any supplement to the current regulatory structure the regulator should require practices which reinforce the operator's responsibility then provide knowledgeable oversight of implementation of those practices. One constructive change to the current set of requirements would be addition of a Strategic Management Process requirement as described above. This would allow Alaska regulators to evaluate how well the operators learn from experience, anticipate changes that could affect risk, and act to manage this knowledge. To support its knowledgeable oversight of an operator's strategic management process, the regulatory agency could strengthen the reporting aspect of the current command and control system by strengthening operator reporting and agency analysis of reported data.

RECOMMENDATION 4 - Expand Operator Reporting

Mandated reporting by operators is a very significant basis for oversight agencies monitoring operator performance and learning from operational experience. Recent experience with applying the ADEC leak data base to understand the factors contributing to reported leaks has underlined the need for expanded reporting requirements. A cross-agency (State & Federal) team should be assembled and commissioned to examine current reporting requirements, operator reporting practice and agency report evaluation practice, then to identify opportunities to expand reporting requirements and report applications.

RECOMMENDATION 5 - Strengthen Operator Management Systems

One way to supplement the current command and control oversight system would add regulations requiring operators to strengthen their internal management systems. This would deal directly with the major deficiencies of command and control regulations by imposing requirements designed to strengthen the way operators recognize and management risks.

While it would require additional legislative authorization, imposing additional requirements on the management systems of petroleum infrastructure operators could address some of the underlying causes of recent problems. This could be accomplished in one of two ways, either by promulgating

new regulations that reference industry standards for guidance (which is the typical approach in Europe), or by promulgating regulations that prescribe detailed requirements to be covered in management systems (which is the typical approach in the US). The specific systems that should be required, or existing requirements reviewed for adequacy, include:

- Quality management - especially important for new pipelines; requirements can be built around ISO 29001, "Specification for Quality Programs for the Petroleum, Petrochemical and Natural Gas Industry", ANSI/API Specification Q1, Eight Edition, December 2007;
- Integrity management - building on current PHMSA regulations for transmission pipelines;
- Management of change - the absence of which has and will continue to be a major contributor to events;
- Systems and processes designed to reinforce safety culture (e.g., processes encouraging communication of "surprises", corrective action system (reporting culture), employee concerns program (reporting to circumvent dysfunctional managers), professional disagreement resolution process, operator learning process, management of accountability (commitment management));
- Performance monitoring and trending systems - including leading indicators;
- Operator risk and resource management - risk recognition, significance evaluation, identification of candidate solutions, ranking of candidates, resource-constrained selection, implementation, effectiveness monitoring (this option is expanded in the section below); and
- Processes supporting sustainable performance - many of the processes listed above are ingredients in an overall process supporting sustainable improvement.

How might the current oversight model be improved to help ensure the continuing usefulness of the existing infrastructure?

As stated early in this section, the primary purpose of the set of recommendations is to strengthen the Alaska regulatory agency knowledge and awareness of risks, and to improve agency access to information on the operators' perspective on risk as well as on their plans to manage these risks.

RECOMMENDATION 6 - Strengthen Learning Processes

Perhaps the most important action Alaska oversight agencies can take, which should require no additional legislative authority, is to strengthen their role in characterizing underlying or root causes of spills and other significant events and close calls. Systematic evaluation of underlying causes is perhaps the richest source of information on factors that are not effectively addressed in regulation or are receiving insufficient attention from operators. Current efforts by both State and Federal agencies to extract the maximum information and insight from significant events and close calls should be reviewed and strengthened as necessary. The effectiveness of operator efforts to learn from their own operating experience should also be examined, and new requirements or agency pressure should be used to strengthen this learning. Continuous learning processes are a basic part of all agencies studies.

4.3 Practical Considerations in Expanding Risk Oversight

In examining ways in which risk assessment might strengthen current oversight practice to better

protect the interests of the people of Alaska, the oversight agencies needs to consider several practical limitations, including:

- Many of the factors which have contributed to events in Alaska are not typically addressed in risk assessments, nor are they covered by regulation; thorough root cause analysis in Recommendation 6 will address this deficiency.
- Different Alaska state agencies have oversight responsibility for different parts of the system and for assuring different public interests, yet no agency seems to have authority to carry out an infrastructure-wide evaluation; cross-agency collaboration in identifying data assembly and analysis needs (Recommendation 4) will be a step toward expanded collaboration.
- Oversight responsibility is currently shared among several state and federal agencies; creating opportunities for cross-agency collaboration, such as in evaluating the results of operator Strategic Management Process (Recommendation 3) can allow diverse agency capabilities to strengthen understanding of operator risks and to focus agency direction on needed improvements.
- Imposing a new set of risk-related requirements would lead to the need for specialized staff expertise - for both the operators and the oversight agencies - which are currently in limited supply in Alaska, and would need to be developed.
- There are numerous companies directly involved in the production, transportation and refining of petroleum products in Alaska; not all of these organizations have strong managers, management systems and technical capability; failures at facilities operated by many of these organizations can adversely affect public interests, not to mention undermine regulatory credibility. Thus any change to regulatory approach that depended on the presence of strong operator management would not be effective for all operators.

To deal with changing the oversight of the range of companies currently being regulated, each having significantly different capabilities, several factors need to be considered. First, the operator must ultimately be responsible for the safe operation of its facilities; the best course for the regulator is to require practices that reinforce the operator's responsibility and provide knowledgeable oversight of implementation of those practices. These practices must focus on prevention of events adversely affecting the public interests; however, since events do occasionally occur, detection and preparation to respond to events are important adjuncts.

Second, the regulator must understand the implications of operating experience (especially "significant" events) to the nature and importance of contributors to risk. By far the best ongoing source of knowledge on new sources of risk or changes in the importance of recognized sources is thorough analysis of the underlying (root) causes of events that occur. Another important source of knowledge is careful analysis of operator-reported performance data and trends. By their nature, root causes cannot easily be captured in routine reporting forms. Root causes typically involve complex interactions among management systems, field personnel actions and equipment failures, all occurring within the context of the operator's safety culture. A regulator cannot simply ask for routinely reported "root cause data," it must require the operator to undertake and report the results from a thorough analysis of these complex interactions. The regulator should itself carry out root cause analyses of the most significant of the events, where "significance" should be defined based on severity of event consequences and on apparent uniqueness of the event.

Finally, for many of the candidate actions discussed above, in which strengthened requirements or enhanced oversight would contribute to assuring responsible operator behavior, inspectors must be evaluated to assess their need for expanded qualifications. Careful selection, training and on-job development of inspectors will likely be required to assure they have the knowledge and skills needed to make the judgments for effective oversight. The difficulty in redeveloping experienced inspectors to perform functions such as root cause analysis or inspecting operator implementation of new management systems should not be underestimated.

APPENDIX A: US FEDERAL APPROACH TO REGULATING PIPELINE SAFETY & HEALTH RISK

This Appendix summarizes approach taken to overseeing the risks from pipelines by the Pipeline and Hazardous Materials Safety Administration (FHMSA), an agency in the US Department of Transportation (DOT).

Parts of this description are abstracted from the paper coauthored by the author of this report: "Regulatory Process Changes at the Office of Pipeline Safety", International Pipeline Conference, IPC04-0539, Wiese, Jeff; von Herrmann, Jim; Wood, Paul; October 4-8, 2004. The Federal Agency OPS discussed in the paper is the Office of Pipeline Safety a precursor agency of the Pipeline and Hazardous Materials Safety Administration (PHMSA), in the US Department of Transportation (DOT).

A.1 Introduction: Motivation and Mandate

In March of 1993, a pipeline owned by one of the largest US petroleum products pipeline companies ruptured near Reston, Virginia, just outside of Washington, DC. Almost ten thousand barrels of fuel oil were spilled and eventually reached the Potomac River. Just a few years later, a pipeline owned by this same company spilled over twenty thousand barrels of fuel oil into a river in South Carolina. In March of 1994, a natural gas line in Edison, New Jersey ruptured and ignited, sending a fireball into the sky that could be seen 30 miles away in New York City.

Although pipelines had a relatively good safety record in the US, and OPS was proud of its regulatory efforts over its short history, these accidents clearly revealed the need for improvements both in how pipelines were operated and in how they were regulated. These pipeline accidents produced significant media coverage that led to considerable pressure for improved oversight from Congress, other federal and state agencies, and the public. The public's faith in the pipeline industry and in the ability of OPS to regulate that industry was called into question.

The management at OPS realized it was time to consider some fundamental changes in the regulation of pipelines. Industry leaders also realized they needed to consider some fundamental changes in their operation of pipelines. OPS and industry leaders jointly arranged a Pipeline Safety Summit in June 1994 to discuss new ideas and potential new paths. A wide variety of stakeholders from the public, local government, and environmental groups were invited to join the discussion.

The new approach conceived at that summit has evolved and is now referred to as Integrity Management Program (IMP). IMP has subsequently been codified in several new rules incorporating prescriptive requirements as well as provisions that are both performance-based and management-based.

A.2 Initiatives to Revitalize Pipeline Regulation

The new rules include the hazardous liquid integrity management program (IMP) rules for large and small operators, the operator qualification rule, and the gas integrity management program (IMP) rule. These new rules have been designed to allow operators flexibility in their approach to addressing the objectives of the regulations. Such flexibility is needed because of the significant differences in the

pipeline infrastructure operated by each company, and the corresponding need to acknowledge these differences to assure the objectives of regulation are achieved without imposing needless burden on the operators. Promulgation of solely prescriptive "one-size-fits-all" regulations is inconsistent with the variations present in the infrastructure operated by the US pipeline industry.

The rules noted above have sometimes been inappropriately characterized as entirely "performance-based", implying that the objectives of the regulation are stipulated and operators are allowed a high degree of flexibility in how to attain and measure the attainment of the regulatory objectives. While such an approach might be desirable, it is difficult to design and implement because of the complexity involved in real-time measurement of the progress in attaining the objectives of the regulations. This difficulty is exacerbated when the objectives are the prevention of incidents and accidents that occur very infrequently.

While the approach OPS has chosen does include performance-based elements, it is better characterized as "management-based" since it requires implementation of a program that either explicitly includes or implies the need for several management practices. While the new rules allow some flexibility in which management practices are selected and in exactly how they are implemented, the rules also prescribe certain "auditable" requirements where little flexibility is allowed.

An example of a management-based provision is the requirement in the IMP rules for the operator to implement a risk assessment process and to use the results from this process in various ways, including supporting establishment of pipeline assessment priorities. (Note, the terms "pipeline assessment", "baseline assessment" and "pipeline integrity assessment" are used here and in the IMP rules to mean application of in-line inspection, pressure testing, direct assessment, or an alternative inspection technology.) Another example is the requirement to integrate data from various sources, including pipeline integrity assessments, to support identification of potentially hazardous conditions that would not necessarily be evident from a single source of data.

Inspection against provisions of a management-based rule is different from inspection of a purely prescriptive rule. A management-based rule provides flexibility in how operators evaluate, justify and change their practices to satisfy the intent of the rule within their unique operating environment. While such changes are designed to lead to improved performance, they will not immediately manifest themselves in recognizable changes in performance.

The ultimate proof of the effectiveness of operator programs will be demonstrated through a continuing review of performance trends. However, regulatory bodies cannot await performance results to demonstrate the effectiveness of operator programs. Therefore, inspection of operator implementation of the new rules has included not only evaluation of compliance with its prescriptive provisions, but also evaluation of the completeness and anticipated effectiveness of the documented approaches designed to satisfy the objectives of the rules.

A.3 Integrity Management Program Regulations

Regulations requiring Integrity Management Programs (IMP) for hazardous liquid pipelines were published on December 1, 2000, and January 16, 2002. Regulations for gas transmission pipelines were published December 15, 2003. The requirements in these regulations lay out comprehensive IMP requirements. These rules have four primary objectives:

- Accelerate integrity assessments (e.g., in-line inspection or pressure testing) in locations

where a release might have significant adverse consequences;

- Improve operator integrity management systems;
- Improve public assurance in pipeline safety; and
- Improve government's role in the oversight of pipeline integrity.

The IMP rules require that pipeline operators analyze the risks associated with their pipelines, including threats that could cause pipeline accidents and the consequences that might result if pipeline accidents were to occur. The regulations included no explicit requirements on how the risks were to be analyzed, but did include requirements on how the risk models were to be applied. Required applications include prioritization of pipe segments for "assessment" (i.e., evaluation of their physical condition using inline inspection tools or equivalent technologies), and evaluation of candidate preventive and mitigative measures for application in addressing significant risks.

Prior to development of these regulations, OPS (the predecessor agency to PHMSA) spent several years interacting with operators in the pipeline industry in the Risk Management Demonstration Program (RMDP). This program was successful in establishing a standard for risk assessment modeling, and in initiating a trust-building dialog with the industry that underpinned the eventual need to disclose information to the regulator about the operators' perspective on pipeline risks.

The IMP regulations required pipeline operators to take actions to evaluate the condition of covered pipeline segments and to protect their pipelines from threats that could cause accidents. Hazardous liquid pipeline operators were also required to take actions to minimize the consequences from potential pipeline accidents.

The IMP regulation for hazardous liquid and gas transmission pipelines provide for increased safety focus on segments of the pipeline that can affect high consequence areas (HCA). HCAs are defined differently for hazardous liquid and gas transmission pipelines, because of differences in the nature of the commodities. Hazardous liquids released from a pipeline in an accident remain on the ground, can enter streams and flow across the ground surface, and can affect populated areas, drinking water intakes, and threatened ecological resources. PHMSA has mapped the location of these critical resources and pipeline operators must determine which segments of their pipeline could affect them if an accident were to release hazardous liquid.

Gas released from a gas transmission pipeline rises and disperses in the atmosphere unless the gas is ignited. If ignited, accident consequences are limited to the immediate area where the gas was released and ignited. Pipeline operators identify HCAs by determining the area near their pipelines containing specified populations that might be affected if a pipeline rupture and explosion and fire would occur.

Approximately 73,000 miles of hazardous liquid pipelines (of 168,000 total miles subject to regulation) have been designated as able to affect an HCA. These pipeline segments are either in an HCA or are in locations where released hazardous liquid could reach an HCA. Approximately 19,000 miles of gas transmission pipelines (of 291,000 regulated miles) are in an HCA.

Operators of hazardous liquid and gas transmission pipelines periodically must inspect (assess) segments of their pipelines that could, in the event of an accident, affect an HCA using devices that can detect defects such as corrosion on buried pipelines. The priority for scheduling these segment inspections must be established using risk assessment models. The models are also supposed to be used to evaluate which preventive and mitigative measures are needed to protect the covered segments.

IMP regulations establish criteria that define defects that operators must repair within specified time limits when defects are discovered in segments that can affect an HCA. Operators of hazardous liquid pipelines have repaired more than 26,000 defects in pipeline segments that could affect an HCA since IM inspections began in 2001. Operators of gas transmission pipelines have repaired more than 2,600 defects in HCA segments since IM inspections began in 2004.

The new IMP rule for gas distribution pipelines differs from those for transmission pipelines in two key areas:

- It does not limit attention to HCAs. Distribution pipelines are located in populated areas and an accident anywhere could affect people. The distribution IMP rule requires that operators evaluate and appropriately increase protection for their entire pipeline.
- It does not require periodic inspection. The inspection techniques used for other pipelines cannot be used on distribution pipelines, which consist of smaller pipes with many branches.

The new IMP rule for gas distribution pipelines, like the other IMP rules, requires that operators analyze the risks to their pipelines and implement additional and accelerated (AA) measures to protect them from threats. PHMSA publish a final rule requiring IM programs for gas distribution pipelines on December 4, 2009.

A.4 Distinctions of the IMP Regulations

The IM rules are based on a set of management-based requirements (referred to as "Program Elements" in the rules) that are fundamentally different from the previously existing, largely prescriptive pipeline safety requirements. The evaluation of operator compliance with these requirements involves the inspection of management and analytical processes - aspects of operator's business that are not reviewed in standard PHMSA compliance inspections. PHMSA has gained significant experience with the fundamentally different approach to oversight needed to assure operators are developing and implementing effective integrity management programs.

Through its inspection program, PHMSA has found that operators generally understand what portions of their pipeline systems can affect high consequence areas, and have made significant progress in conducting integrity assessments for these areas. However, the development of effective management and analytical processes, and quality data and information to support these processes still requires considerable attention from some operators. While most operators appear to be headed in the right direction, fundamental changes to management systems require time and management commitment.

After several years of integrity management development and associated inspection, PHMSA has gained additional experience about how to perform this new type of inspection. An important change in the program took place in late 2004 when the five PHMSA Regional Offices took over the scheduling, inspection program, and other aspects of managing the IM inspections.

A.5 A New Approach to Inspection and Enforcement

OPS adopted several mechanisms to aid in the inspection of the management-based provisions of the new rules. These mechanisms are designed to promote conformance with several guiding principles, including:

- Conduct of complete inspections that are tightly aligned with requirements stated in the rule
- Striving to inspect and enforce these requirements consistently
- Assure stability of the regulatory process in a way that allows incorporation of lessons from ongoing studies, new R&D and industry experience
- Ensure that the rule and related activities lead to appropriate increases in regulatory and public confidence in pipeline integrity

The mechanisms OPS has adopted include:

- Developing inspection protocols
- Providing detailed guidance to inspectors
- Assembling and answering "frequently asked questions" (FAQ)
- Training and evaluating inspectors

The first mechanism, inspection protocols, has been designed to (a) improve the communication of regulatory expectations with states and the industry, (b) support improved consistency of inspections conducted by various regulatory groups, and (c) provide assurance of the stability of the acceptance criteria associated with the rules. The protocols developed for the hazardous liquid and for the OQ rules, and for gas IM are simply questions that support exploration during the inspection of how each operator meets provisions of the rules.

One of the historic problems encountered with the use of management-based rules is the potential for ambiguity of acceptance criteria. Such potential ambiguity can leave operators concerned about consistency in what individual inspectors will determine to be adequate, and may make it difficult for OPS and its state partners to consistently and fairly assess hundreds of operators across the country. With the objective to allow significant flexibility in how operators design their programs while promoting innovation and continuous improvement, OPS has developed mechanisms for more clearly establishing and communicating common expectations between regulators and operators of what constitutes an acceptable IM Program.

One such practical mechanism that has successfully been used is an extensive set of frequently asked questions (FAQs), which are answered and posted on publicly available websites. Numerous stakeholders, including representatives from industry, regulatory agencies and the public, pose these FAQs. Once responses have been drafted and cleared through knowledgeable state and federal experts, the FAQs provide a major source of practical and useful information to operators about the meaning of provisions in the rule.

In addition to inspection protocols and FAQs, OPS has also developed detailed inspection guidance for its field inspectors to help assure consistent reviews for all operators. The protocols and inspection guidance go beyond checklist approaches to support development of an integrated understanding of an operator's program.

OPS has also initiated a variety of communications activities to improve common understanding of its programs among regulators, industry and public stakeholders. OPS has conducted a series of public workshops, and will continue to hold such events as part of its overall strategy to significantly enhance the information flow among OPS, states, industry, and the public.

Through IM inspections supported by detailed protocols and inspection guidance, OPS judges the expected effectiveness of an operator's program. However, OPS does not rely solely on inspections to evaluate operator success. The IM Rule also includes requirements for operators to develop their own performance measures and performance monitoring programs. The actual results achieved must still relate to the effectiveness of the programs developed. Although OPS believes that the inherent difficulty in the pipeline industry of developing unambiguous and timely performance measures makes sole regulatory reliance on performance results impossible, requirements for operators to develop and track performance metrics is an important adjunct to the prescriptive and management-based elements of the regulation.

Initial inspections focused on evaluating compliance with prescriptive provisions of the rule. However, regulators need a tangible basis on which to assure that each operator being inspected understands regulatory expectations associated with the performance aspects of each new rule, and that it intends to meet these expectations over a reasonable time period. Therefore, regulators will continue to look for tangible evidence in an operator's program that the operator is planning for future improvements to its program in the coming months and years. This evidence could take the form of a plan or other approach that (a) describes the approaches the operator is taking to satisfy regulatory expectations and (b) clarifies the time frame on which these actions will be completed. Review of this evidence was an integral part of early inspections.

A.6 Changes Needed in Regulatory Practice

The changes described above in the regulations themselves must necessarily be accompanied by changes in the regulatory approach to inspection and enforcement. Several factors are important in allowing regulators to meet the challenges presented by the new regulations, including:

- The number of inspectors
- The skill mix of inspectors
- The relationship between inspections designed to verify compliance and those to evaluate management process adequacy
- The quality and accessibility of processes and information needed to support focusing inspections on underperforming operators and key issues

To assure that the nation's pipeline infrastructure is operated in compliance with regulations and in the interest of the public living near the lines, several types of monitoring are necessary. Pipeline monitoring needs to focus on three characteristics: (a) the condition of the pipeline and support equipment, (b) the qualification of the people who operate and maintain the pipeline and support equipment, and (c) the effectiveness of the management systems and processes used to direct and control operation and maintenance. Ultimately operators that have effectively addressed these three characteristics will be able to demonstrate the effectiveness of their efforts through current performance and trends in performance results.

The recent significant improvements in the regulations governing the qualification of people and in the processes and systems needed to support integrity management discussed above are expected to lead to significant future improvements in performance results.

APPENDIX B: US NRC EXPERIENCE WITH THE USE OF RISK MANAGEMENT

This Appendix summarizes approach taken to risk oversight of nuclear power facilities by the U S Nuclear Regulatory Commission (NRC).

B.1 Regulatory Authority

The Atomic Energy Act of 1954 authorized the Atomic Energy Commission to issue licenses for commercial nuclear generating plants and to adopt safety regulations for them. In 1974 Congress passed the Federal Energy Reorganization Act that separated the regulatory and promotional activities of the Atomic Energy Commission with the latter responsibilities being assigned to the Nuclear Regulatory Commission (NRC). The primary requirements driving cost effective regulation are (the broadly applicable federal law requiring cost-benefit analysis of new requirements) and the back-fit Rule (10 CFR 50.109). At present there are no specific regulations requiring risk management, but the NRC has used its "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants" (50 FR 32138; August 8, 1985) as the basis for requiring all licensees of Nuclear Power Plants to complete and submit a Probabilistic Risk Analysis (PRA) that investigates and quantifies the overall risk associated with operating their plant(s). In addition, the Commission has issued a policy statement on "The Use of Probabilistic Risk Methods in Nuclear Regulatory Activities" (Federal Register, August 16, 1995) that describes the historical evolution of the use of probabilistic risk analysis at the NRC and provides a conceptual structure for the expansion of this use.

B.2 Summary of Risk Management Experience at the NRC

The first major effort of the NRC related to risk management was its publication of WASH-1400, also known as the Reactor Safety Study. The primary motivation of WASH-1400 was to try to "rationalize" the nuclear power debate by putting nuclear power risks in perspective with other societal risks. WASH-1400 developed a quantitative assessment of total risk together with a quantitative statement associated with the uncertainty on this level of risk. This result was then used to argue the "acceptability" of this risk through comparison with other accepted societal risks (e.g., lightning, automobile accidents).

Significant, on-going technical debate over the models and data ensured that the quantitative conclusions of the Reactor Safety Study would not be accepted as the basis for a public policy decision on nuclear power safety. However, the risk assessment itself produced results that turned out to be very enlightening and useful in improving safety. Prior to the WASH-1400 risk analyses, most safety analyses, design, and procedures were based on the assumption that the most important event to protect against was the "Large Loss of Coolant Accident" (Large LOCA), defined to be a double-ended guillotine break of the largest reactor coolant pipe. However, the risk assessment performed in WASH-1400 determined that smaller breaks and leaks from the primary coolant system and failures of the reactor shutdown system were actually more important from a risk standpoint. This resulted because these accidents were much more likely to occur, and could also lead to levels of public health consequences comparable to the large pipe break accidents. Thus, the Reactor Safety Study demonstrated the difficulty of producing technical consensus on quantitative measures of risk. It also

demonstrated that the process of risk assessment, by systematically examining the logical ways that systems and components can fail, can produce new information or organize existing information in a way that can significantly change the focus of safety regulation, operation, and research.

WASH-1400 was a risk assessment performed under the direction of the regulator, not the product of an operating company risk management program. The first real risk management program in the nuclear industry, in which the results of a risk assessment were directly used by management to guide risk control decisions, was the Big Rock Point risk management program developed by Consumers Power Company in 1980. This was also the first situation in which the NRC accepted the principle that "one size doesn't fit all" and used risk-based arguments to accept an operator's compliance with the spirit rather than the letter of existing regulations.

A historical note: the accident at Three Mile Island, which occurred after the publication of WASH-1400, was a small loss of coolant accident caused by a stuck open relief valve, the general type of accident predicted in WASH-1400 to be the most risk significant, but generally neglected prior to the publication of WASH-1400. Also of importance to the overall practice of risk management, and an example of the importance of root-cause analysis and of communicating the lessons to the regulator and within the regulated community is an event that occurred at the Davis-Besse nuclear plant in the late 1970s. The event was nearly identical to the one that occurred nearly a year later at the Three Mile Island (TMI) nuclear plant. The only difference was that the lead operator on duty recognized what was happening and took different action than he had been trained to take, thereby averting serious consequences. The implications of this event were not understood and communicated among the operators of the five plants with similar design. This seemingly simple act could have prevented the accident at TMI

In the aftermath of the Three Mile Island accident, the NRC promulgated a wide variety of new requirements. However, Big Rock Point was a small, older reactor. The NRC recognized that many of the new requirements didn't make sense for Big Rock Point and requirements to implement these changes might lead to the permanent shut-down of the reactor. Consumers Power performed a risk assessment of the plant, analyzed the contributors to risk, and determined what could be done to manage these risk contributors. The company looked at reductions in risk that could be expected from the new regulatory requirements and compared these reductions to a set of company-defined plant-specific improvements that addressed the underlying concerns, but in a much more cost-effective manner. After extensive review and negotiation, the NRC accepted the alternative measures suggested by Consumers Power, and provided exemptions from many of the new requirements.

At this point in the evolution of risk management within NRC, forward thinkers in the agency were beginning to appreciate the value of risk management as an engineering tool to focus and guide regulations and operating practices, rather than as merely a quantitative demonstration of acceptable levels of risk.

While the Big Rock Point experience was valuable, the reactor was quite small and in special circumstances. The NRC took a significant step in 1981 to expand the concept of a risk-based, customized regulatory scheme. Northeast Utilities, one of the early companies to embrace nuclear power, was asked to participate in an Integrated Safety Assessment Program (ISAP). The purpose of this program was to utilize Risk Assessment as the basis for a) identifying the major contributors to risk, b) determining the best way to address these risk contributors, and finally, c) developing a compliance schedule based on implementing the most significant risk management changes earliest,

and deferring or eliminating the less effective changes. While this program again represented the application of risk assessment and risk management in a special situation, the subject plant was one of the ten oldest operating nuclear power plants in the country, it introduced the idea that both defining approaches to achieve compliance and developing compliance schedules could benefit significantly from the insights provided by Probabilistic Risk Assessment (PRA).

As noted above, following the accident at the Three Mile Island plant, the NRC assembled an extensive safety "wish list" and required all nuclear plant licensees to comply with these new requirements. The financial and management burden associated with implementing these requirements, most of which were highly prescriptive rather than performance-based, was extraordinary. To allow this burden to be managed, several utilities developed an approach, similar to the ISAP concept, called the Integrated Living Schedule (ILS) or the Integrated Resource Management System (IRMS). Among the early adherents to this approach were Iowa Electric and Toledo Edison. The primary feature of this process was the development of a priority list of needed changes and the negotiation of compliance schedules with the NRC. The priority list was developed based on simple decision models that used risk "attributes" as the primary decision parameters. Negotiations on implementation schedule were based on the NRC perception of the appropriateness of the priority list and on the reasonableness of constraints such as financial, time and management capability. The "living schedules" were often formalized using license conditions, and included explicit description of the conditions under which regulatory approval was needed to make changes.

About the same time as the NRC and utilities were beginning to use IRMS as the basis for negotiating compliance schedules, the NRC was making internal use of the insights from risk assessment to support decisions on the priority of safety-related research projects. Other innovative NRC applications of risk assessment included the use of measures of the risk significance of safety equipment to focus field inspections on the most significant equipment and failure modes.

In parallel to the constructive applications of risk assessment in the management of reactor safety noted above, the NRC began to develop a quantitative safety criterion. The idea behind this criterion was to embody in regulation a quantitative measure of the maximum level of acceptable risk associated with an operating nuclear reactor. The program to develop this criterion was carefully designed to engage all stakeholders in the safety of nuclear reactors to assure that the resulting criterion would have wide acceptance. The NRC underestimated the difficulty both of defining a safety criterion that could serve as the basis for regulation, and of gaining the approval of the diverse nuclear power interest groups. After several years work and considerable expenditure, the effort produced a set of "quantitative safety goals" with no associated regulatory enforcement mechanisms.

After the initial regulatory chaos following the accident at the Three Mile Island plant subsided, the NRC began consideration of how to fill the regulatory void associated with conditions "beyond the design basis". The industry, fearing another costly and non-productive wave of new requirements, instituted its own comprehensive investigation of severe accidents (Industry Degraded Core Rulemaking - IDCOR), and used this investigation as the basis for a continuing dialog with the NRC. One of the results of these interactions was the development of an industry methodology intended to consistently analyze the risk associated with each type of nuclear reactor. This methodology, called Individual Plant Examinations (IPEs), has been applied by all nuclear licensees to characterize their plant risk profile. The NRC next completed an extensive and costly review of all of these IPEs and analysis of the risk from external events such as earthquakes, major fires and floods. In addition, the

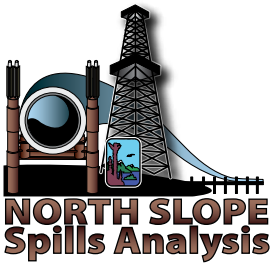
NRC has required application of the IPE studies as the basis for developing procedures on how to manage very low probability severe accidents, that is accidents involving physical degradation of the reactor core.

While the intention of the IPEs was to provide a consistent basis for regulatory consideration of severe accident risks, the IPE studies themselves have retained sufficient uniqueness to frustrate the original purpose. Indeed, a potential adverse side effect of the IPEs was to focus NRC and industry interactions away from the management of risks and back toward the assessment of risks. Some utilities have, however, used the requirement to perform IPEs as the impetus to begin a more constructive application of risk management designed to customize generic regulations to the unique design features and operational characteristics of their plants. These constructive applications are being encouraged by the NRC through the PRA policy statement having the following provisions:

- The use of PRA in all regulatory matters should be increased to the extent supported by the state-of-the-art in PRA methods and data, and in a manner the defense-in-depth philosophy.
- PRA should be used to reduce unnecessary conservatism associated with current regulatory practice.
- PRA evaluations should be as realistic as practicable and supporting data should be publicly available.
- Uncertainties in PRA evaluations need to be considered in applying the Commissions safety goals for new generic requirements.

Next, the NRC in cooperation with the nuclear industry has embarked on a somewhat more aggressive and certainly more formalized application of risk management. This effort, labeled "risk-informed regulation", was intended to formalize the approach used by the industry in presenting arguments having a risk management component, and to formalize the approach used by the NRC in reviewing and accepting changes to regulated practice proposed by nuclear licensees. The bases of this program were (a) preparation by the NRC of regulatory guidelines defining how licensees should package and submit requested changes, (b) preparation by the NRC of Standard Review Plans describing how they should review and approve requested changes, and (c) pilot evaluations by several licensees of a wide range of regulated practices which the licensees desire modify. Examples of these practices include:

- **Maintenance Rule implementation:** The maintenance Rule encourages the application of risk insights in determining the safety significance of systems, structures, and components for use in setting performance goals and in defining maintenance program features commensurate with plant safety. The NRC will use these same insights to determine the level (equipment, train or system) and frequency of monitoring.
- **Risk-informed technical specifications:** This pilot focuses on modification of allowed outage times (for maintenance) of safety equipment consistent with the risk presented by the outage.
- **Graded quality assurance:** This pilot defines the level of quality assurance controls consistent with safety (risk) significance.
- **In-service testing and inspection:** This pilot defines the frequency of testing and inspection consistent with the safety (risk) significance of the element.


NORTH SLOPE
Spills Analysis