Letter Report

Transportation Research Board
of The National Academies

Technical Peer Review of a Proposed Risk Assessment Methodology on Alaska's Oil and Gas Infrastructure

SUMMARY

In the aftermath of the discovery of extensive corrosion in two oil transit lines in the Greater Prudhoe Bay Field on Alaska's North Slope (in March and August 2006), the Prudhoe Bay Field was shut in for an extended period with a corresponding significant financial impact on the State of Alaska while the corrosion problems were investigated. Subsequently, the State of Alaska commissioned a major risk assessment of the oil and gas infrastructure in the state to identify and mitigate any other potentially significant impacts to State revenue, as well as to the environment and to safety.

The State requested that the Transportation Research Board (TRB) of The National Academies perform a technical peer review of the proposed methodology for the risk assessment designed by Doyon Emerald Consulting Group LLC and American Bureau of Shipping Consulting (Doyon Emerald–ABS), the contract team hired by the Alaska Department of Environmental Conservation (ADEC) to design and conduct the assessment. After a review of the available documentation and meetings in Washington, D.C., and Anchorage, Alaska, to gather public, industry, government, and expert input, the committee found the proposed risk assessment methodology to be problematic in three main areas: (*a*) the management plan was not feasible given real-world constraints, (*b*) the proposed risk methods were too detailed and lacked a sufficient top-down perspective necessary for capturing the important risks, and (*c*) the proposed results were static and stopped well short of providing the State with a set of tools for evaluating risk mitigation opportunities.

The committee recommends that for future risk assessment efforts the State should (*a*) revise the scope of the project, focusing first on risks to infrastructure reliability followed by

studies on environmental and safety concerns; (*b*) focus assessment efforts by using a combination of top-down and bottom-up approaches; (*c*) work with industry from the earliest possible moment so that common goals can be identified and mutual cooperation can be ensured; and (*d*) focus on an end goal of risk management including, where practicable, methods to increase system robustness (using technology, management controls, or both) by enhancing early (developing) problem identification and implementing real-time system modifications that avoid or decrease the potential for catastrophic losses.

1. STUDY OBJECTIVE AND CHARGE

To help ensure a successful outcome of the risk assessment of Alaska's oil and gas infrastructure, the State requested that TRB conduct a technical peer review of the proposed design for this risk assessment. The contractor's risk assessment (solicited as a one-time engineering-oriented appraisal of the condition of the infrastructure) was required to include identification, quantification, and evaluation of current and future significant risks from a systems-level perspective and a methodology by which mitigation and management options could be evaluated. In addition to the technical peer review, the TRB committee was asked to recommend improvements to the risk assessment design that would assist the State in achieving its goals (e.g., determination of the appropriate scope to focus limited resources, a comparison of the feasibility of top-down and bottom-up approaches, and options for encouraging industry participation).

The primary inputs to this committee's effort were the Interim Report[1] and the Proposed Risk Assessment Methodology[2] developed by the contract team of Doyon Emerald–ABS. In addition, the committee gathered public, industry, government, and expert input at meetings held in Washington, D.C., and Anchorage, Alaska. At an organizational meeting in Washington in April 2009, the committee was briefed on its charge by the sponsor (ADEC) and on the status of the proposed methodology by the contractor team. In May 2009, the committee attended government, stakeholder, and industry meetings in Anchorage to receive input from relevant

[1] Doyon Emerald–ABS. 2009. *Comprehensive Evaluation and Risk Assessment of Alaska's Oil and Gas Infrastructure, Phase 1—Interim Report.* Alaska Department of Environmental Conservation, January 16, 2009.
[2] Doyon Emerald–ABS. 2009. *Comprehensive Evaluation and Risk Assessment of Alaska's Oil and Gas Infrastructure: Proposed Risk Assessment Methodology, Revision 1.* Alaska Department of Environmental Conservation, March 20, 2009.

State and federal government agencies, pipeline owners and operators, developers of the proposed risk assessment, other experts and stakeholders, and the State Agency Oversight Team (SAOT) for the risk assessment.[3]

The purpose of the briefings was to share with the committee the views and concerns of other technical experts and stakeholders about how the proposed risk assessment should account for the risks and consequences identified by stakeholders and Doyon Emerald–ABS. Following the meetings and discussions, the committee prepared this letter report outlining its findings, recommendations, and rationale for reaching those conclusions.

The committee's report is organized in seven sections. The next section provides background on Alaska's oil and gas infrastructure; the events that led up to the decision to commission a formal, comprehensive risk assessment; and the selection of a contractor to carry out the work. Section 3 provides an overview of the methodology proposed by Doyon Emerald–ABS that the committee was asked to review. The committee provides its evaluation of the proposed methodology in the fourth section. The fifth section includes case studies of past high-risk events that the proposed methodology would not have identified. Section 6 contains recommendations and guidance for follow-on studies. In the final section, the committee comments on prudent next steps that the State of Alaska could take to better identify and manage risks to its oil and gas infrastructure.

2. BACKGROUND CONTEXT

Alaska is dependent on oil and gas production as a primary revenue source and will be for the foreseeable future. Thus, the integrity of the oil and gas infrastructure must be maintained to ensure continuing production while simultaneously protecting Alaska's environment and the safety of operational personnel and the general public. Portions of Alaska's complex oil and gas infrastructure have been in place since the early 1960s, and some have surpassed their originally engineered life span; however, as demonstrated in 2006 when part of Alaska's North Slope oil

[3] The SAOT includes representatives from various agencies—ADEC, Department of Natural Resources (including the State Joint Pipeline Office and the Petroleum Systems Integrity Office), Alaska Department of Public Safety/State Fire Marshall's Office, Alaska Oil and Gas Conservation Commission, Alaska Department of Labor and Workforce Development, Department of Law, Department of Revenue, and University of Alaska College of Engineering and Mines—and provides oversight and guidance to the contract team for the Alaska Risk Assessment.

production was interrupted because of a series of three spills resulting from previously unidentified corrosion, failures in any one component of the system directly affect the system as a whole. These incidents led to the announcement in May 2007 by Alaska Governor Palin of a 3-year initiative—the Alaska Risk Assessment (ARA)—to report on the status of the existing oil and gas infrastructure, components, systems, and hazards; to evaluate the ability to operate Alaska's oil and gas infrastructure safely for another generation; and to identify and rank risks based on consequences to State revenue, safety, and the environment.

Alaska's oil and gas infrastructure—which includes production on the North Slope, production in Cook Inlet, transport via the Trans Alaska Pipeline System (TAPS), and loading onto tankers at the Valdez Marine Terminal (VMT)—is a critical component of the State's economy. Losses in production of oil or natural gas may have significant consequences on State revenues and jobs. At the same time, a failure could also cause a range of impacts on the environment, human health, and safety.

Major Infrastructure Components

North Slope Production Facilities

There are eight primary operating areas on the North Slope that process oil and natural gas. The Prudhoe Bay Field, which is the largest on the North Slope and the largest in the United States, was discovered on March 12, 1968, and production began on June 20, 1977. The field, which is estimated to have contained 25 billion barrels of oil, is operated by BP on behalf of itself and the other owners, ExxonMobil and ConocoPhillips. Other producing areas were developed after Prudhoe Bay and still more prospects remain to be developed. The North Slope facilities consist of oil, gas, and water separation; gas dehydration, compression, and reinjection; water treatment and reinjection; and natural gas production. Oil is then transported from each of the facilities via common carrier pipelines to Pump Station (PS) 1, where it enters TAPS for transportation to the VMT, from which it is transported to destinations primarily on the West Coast of the United States.

Trans Alaska Pipeline System

TAPS, which is owned by a consortium of oil companies and operated by Alyeska Pipeline Service Company on their behalf, connects Alaska's North Slope oil fields to the VMT, where the crude oil is loaded onto tankers that transport it to refineries. The 800-mi pipeline begins at PS 1 on the Arctic Ocean at Prudhoe Bay and crosses three mountain ranges, more than 800 rivers and streams, three major earthquake fault lines, broad expanses of tundra, and numerous caribou and moose migration paths. The single 48-in. diameter pipeline was built between 1975 and 1977 at a cost of about $8 billion.

Approximately half the length of TAPS is buried, and the remainder is elevated in order to keep the permafrost it traverses from melting. Oil emerges from the ground on the North Slope at about 110°F, cools as it travels 13 days from PS 1 to the VMT, and arrives at about 65°F. Heat exchangers built into the vertical support members (VSMs) that suspend the elevated sections of TAPS prevent the permafrost from melting and thereby prevent the VSMs from sinking. The VSMs were designed to accommodate some horizontal and vertical movement, and the above-ground line was laid out in a zigzag pattern to allow for thermal expansion and any movement associated with earthquakes. Where TAPS goes underground in the permafrost, the pipeline exterior is refrigerated. The TAPS infrastructure includes a marine terminal, 11 pumping stations (only 5 of which are currently in operation), 78,000 VSMs, 174 main-line valves, several refrigeration plants, 13 major bridges, and many access roads.

Valdez Marine Terminal

The VMT is located in Port Valdez at the southern terminus of TAPS and is operated by Alyeska Pipeline Service Company on behalf of the owners of TAPS. The terminal receives crude oil from TAPS and has the capability of storing the oil and loading it onto tankers for transport to refineries. The VMT, which covers over 1,000 acres, has facilities to meter, store, transfer, and load the crude oil. There are 18 storage tanks, 15 of which are permitted to be in service, with a capacity of 535,000 barrels per tank; however, at any give time, one or more might be undergoing maintenance. There are also three fixed berths and one floating berth at the

terminal—of these only two fixed berths are currently in operation; berths B1 and B3 were decommissioned in 2005.

Cook Inlet Facilities

Cook Inlet facilities include 16 offshore oil and gas production platforms and 5 onshore production and processing facilities providing platform support, as well as numerous onshore central oil and gas production facilities, the Drift River Terminal facility, and pipelines. The Cook Inlet Pipe Line Company's Drift River Terminal facility is located near Kenai, about 90 mi southwest of Anchorage, Alaska. This facility has been used for temporary storage of crude oil for almost 40 years. Nearly 70% of Alaskans (and all of Anchorage) rely on natural gas from Cook Inlet to generate electricity to heat homes and businesses and to provide fuel for industrial processes. Through 2007 more than half the gas produced either was processed and exported as liquefied natural gas (LNG) or served as feed stock to nitrogen fertilizer operations at the Agrium chemical plant in Nikiski. In 2008, however, the Agrium plant was closed due to a shortage of natural gas supply in Cook Inlet.

History of Operation and Incidents

Current oil production from North Slope facilities is about 700,000 barrels per day (bpd), the bulk of which is from the Prudhoe Bay Unit with a production of almost 400,000 bpd; the eight other units account for the remainder. Cook Inlet facilities were adding another 14,000 bpd until the shut-in due to the threat of continued eruptions from Mt. Redoubt. It is believed that daily production will be somewhat less at the Cook Inlet facilities as they come back on-line (ADEC, personal communication, October 1, 2009). Natural gas production from the North Slope reservoirs is currently 8,400 mcf[4] per day, most of which is reinjected into the oil-bearing formations. The Cook Inlet facilities provide 600 mcf per day.

TAPS began operation in 1977. Peak flow reached 2.1 million bpd in 1988, but in 2008 because of reduced production at the North Slope, the pipeline operated at 700,000 bpd, and for 2009, based on the most recent information, is just over 663,000 bpd due to maintenance on the

[4] Mcf, a unit of measure for natural gas, is 1,000 ft^3.

system (ADEC, personal communication, October 1, 2009). Since its start-up, TAPS has survived several earthquakes, has been ruptured by a deliberate explosion, and has been punctured by gunshot. It experienced about 30 to 40 small spills a year until about 1995, after which the number of spills declined sharply. The total spill loss from 1997 to 2000 was only 7 barrels. The operating experience of the production facilities during this period has been generally similar, with minor incidents occurring over the years, none of which resulted in major outages or significant losses of production.

However, concerns over the integrity of the state's oil and gas infrastructure were heightened during 2006. In March of that year, there was a spill from a BP pipeline on the North Slope, which was the result of corrosion in the pipeline system, and that spill was followed by two additional ones in August 2006, also caused by corrosion. The impact of the corrosion was severe enough to require replacement of 16 to 22 mi of North Slope lines connecting the Prudhoe Bay oil field to TAPS, leading to the partial shutdown of oil production, which resulted in Congressional hearings on system integrity and state and federal oversight.

History of the Risk Assessment Process

Given recent infrastructure incidents and concerns with the integrity of the system, in 2007 the State of Alaska appropriated $5 million for a comprehensive risk assessment of Alaska's oil and natural gas infrastructure (referred to as the Alaska Risk Assessment or ARA). According to the State of Alaska, in order to rank the relative risks within this complex system by priority, a rigorous and systematic approach was needed to assess the current condition of Alaska's oil and gas infrastructure. A risk assessment may be used to identify the risks associated with the infrastructure and to develop remedies to mitigate those risks. The purpose of the risk assessment is to "identify those infrastructure items, components, systems, and hazards that demonstrate the greatest probability for a failure which would lead to negative impacts to overall safety, the environment, or reliability. This risk assessment will not specifically address the risks and threats from security issues or intentionally man-made hazards such as terrorism or sabotage, but will include the risks and threats posed by natural hazards" (ADEC 2008, 23).[5]

[5] ADEC. 2008. *Request for Proposal: Comprehensive Evaluation and Risk Assessment of Alaska's Oil and Gas Infrastructure*. RFP 2008-1800-7379. March 14, 2008.

The scope of the proposed risk assessment includes Alaska's entire oil and gas production, storage, and transportation system from wells to marine terminal loading arms. It includes the North Slope production and the oil transportation system infrastructure but does not include tankers or marine transportation systems. The oil and gas infrastructure of Cook Inlet is included in the initial phase of the project. The risk assessment, as envisioned by the State, has three major phases:

- Phase 1: design risk assessment methodology,
- Phase 2: implement risk assessment methodology to identify risk factors,
- Phase 3: analyze risk assessment data, recommend mitigation measures, and develop final report.

ADEC intends the risk assessment to be a cooperative effort, incorporating input from relevant State and federal agencies, industry, local government, and other stakeholders. "The initial phase [Phase 1] will solidify the project scope and methodology. This includes developing objectives, data collection strategies, and a risk assessment methodology that will yield meaningful information in regards to the relative risks to Alaska's oil and gas infrastructure, as well as potential interventions to mitigate these risks" (ADEC 2008, 23).[6] The risk assessment will include (*a*) a one-time engineering-oriented appraisal of the condition of the infrastructure; (*b*) identification, quantification, and evaluation of current and future significant risks from a systems-level perspective; and (*c*) a methodology by which mitigation and management options can be evaluated.

In June 2008, ADEC contracted with a team from Doyon Emerald–ABS to design and implement the project. The contract was for $4.1 million and covered two years of work. Doyon Emerald–ABS developed a series of steps to complete the work, the first three of which are relevant for this report.

[6] ADEC. 2008. *Request for Proposal: Comprehensive Evaluation and Risk Assessment of Alaska's Oil and Gas Infrastructure*. RFP 2008-1800-7379. March 14, 2008.

Step 1: Assess Stakeholder Concerns

In the first 7 months of the contract (June 2008 through January 2009), Doyon Emerald–ABS gathered data; held stakeholder and industry meetings to obtain input of State and federal agencies, local government, industry, environmental groups, and the public; and prepared an interim report.

Step 2: Develop Risk Assessment Methodology

In the next 3 months (January 2009 through March 2009), Doyon Emerald–ABS used the findings of the interim report to solidify the project scope and methodology. This step included developing objectives, data collection strategies, and a risk assessment methodology intended to yield meaningful information with regard to the relative risks to Alaska's oil and gas infrastructure as well as potential interventions to mitigate those risks. Doyon Emerald–ABS published their Proposed Risk Assessment Methodology on March 20, 2009.

Step 3: Receive Feedback on Proposed Methodology

The proposed methodology was available for public review until June 2, 2009. During this time, the TRB committee was tasked with conducting a peer review of the methodology. As part of the review, the committee was also asked to recommend overall improvements to the risk assessment design that would aid the State in achieving its goals (e.g., determination of the appropriate scope to focus limited resources, a comparison of the feasibility of top-down and bottom-up approaches, and options for encouraging industry participation).

3. OVERVIEW OF DOYON EMERALD–ABS METHODOLOGY

To provide an overview of the proposed methodology, the summary section from the Doyon Emerald–ABS proposal is included here. Minor modifications and formatting changes have been made for readability, but this is essentially an excerpt from their proposal.

Methodology Inputs

The proposed methodology is based on best risk assessment practices combined with insights and information gained during the first part of Phase 1 of the project. In addition to existing information and data review activities, Phase 1 included a comprehensive stakeholder consultation process to obtain key stakeholder input into the scope and methodology for the ARA.

The following operational hazard assessment and natural hazard assessment approaches were reviewed and selected:

- *Operational Hazard Assessment* – Hazard Identification (HazID) techniques, event tree analyses, what-if analyses, consequence analysis methods (e.g., modeling for releases, fires, explosions), and failure modes and effects analyses (FMEAs).
- *Natural Hazard Assessment* – Based on the American Lifelines Association (ALA) Guidelines, a consensus document based on industry and government efforts to develop and document natural hazard assessment techniques.

Other inputs to the methodology development included the following:

- *Integrity Management Standards and Practices* – System integrity efforts are designed to address failure mechanisms or factors that contribute to pipeline and other equipment failures.
- *Comparable Risk Assessment–Related Projects* – Comparisons of publicly available large-scale and complex risk assessment projects, as well as Alaska infrastructure projects, were made in terms of similarity of objectives, scope, and applicability to current infrastructure.
- *Stakeholder Input* – Stakeholder input from a wide variety of groups and regions including state agencies, federal agencies, local governments, nongovernmental organizations (NGOs), native organizations, and the public was incorporated into the proposed methodology. Stakeholders provided input on initiating events and significant consequences, as well as data source recommendations that have been used to customize the proposed operational hazards and natural hazards assessments.

Physical Infrastructure Scope

The Physical Infrastructure Scope has been defined to establish the infrastructure components that are included within the physical scope of the project. A comprehensive list of in-scope facilities and major components for the three infrastructure regions was developed for each operating area considered to be in the scope of the risk assessment for the North Slope, Cook Inlet, and TAPS. The information included is summarized from a master data record that was developed to capture and organize the infrastructure facilities and associated components within the scope of the project.

In general, for the North Slope and Cook Inlet, the project scope begins at the wellbore (inclusive of the well) of the production or service well but does not include issues associated with reservoirs, formations, and associated down-hole production. For all three regions, the scope ends at the point of delivery, and does not include downstream infrastructure or distribution systems.

- *North Slope*: Production facilities and pipelines that deliver oil to Pump Station (PS) 1 in Prudhoe Bay, including components in the following North Slope units: Kuparuk River Unit, Colville River Unit, Milne Point Unit, Oooguruk Unit, Prudhoe Bay Unit, Duck Island Unit/Endicott, Northstar Unit, Badami Unit. Pipelines common to multiple units and facilities are also included.
- *Cook Inlet:* Sixteen offshore oil and gas production platforms, five onshore production/processing facilities providing platform support, numerous onshore central oil and gas production facilities, the Drift River Terminal facility, and pipelines.
- *TAPS:* The pipeline and facilities that transport oil from PS 1 to the VMT, including the Trans-Alaska pipeline, the fuel gas line from PS 1 to PS 4, pump stations, and the VMT, up to the marine terminal loading arms.

Risk Assessment Organizational Structure and Data Management

The oil and gas infrastructure will be partitioned into manageable segments, or nodes, for analysis purposes. A node consists of a system or a set of components or equipment that is part of a facility located in a defined geographic location. The amount of equipment in a node may vary from one singular component or major piece of equipment to many components in a system that work together to perform a singular function or process.

The geographic location of a singular node may encompass a small local area around a facility, a few acres, or dozens of square miles. Process material contained in the equipment, proximate worker and public populations, and local environmental sensitivity are factors that will be considered in creating nodes for some facility systems.

During the analysis process, hundreds of scenarios will be documented to address both the operational and natural hazards that are applicable to each piece of the infrastructure.

Facilities in the North Slope, Cook Inlet, and TAPS regions will first be categorized by type. North Slope facilities can be categorized as one of three different types: *central oil and gas*, *gas handling*, and *support facilities*. Cook Inlet facilities include *offshore oil and gas production platforms*, *onshore central oil and gas processing facilities*, and the *terminal facility*. TAPS facilities include the *pump stations* and the *VMT.*

Facilities will be segmented into major components or systems for the analysis, based on the functions or processes of the individual facility type. Pipelines in the North Slope and Cook Inlet may require pipeline segmentation for longer, subsea or cross-country pipelines which have specific isolatable pieces and may cover large distances. The TAPS pipeline will be divided into segments for nodal analysis based on the segments between pump stations, and as appropriate, factors such as the ability to isolate the section, environmental sensitivity of the area, anticipated spill response measures for the area, the type of line (above or below ground), and natural hazards applicable to the region or local area.

The use of a nodal analysis is very common practice for conducting risk assessments and for maintaining organization in the execution and documentation of a study of such large magnitude.

The nodal approach is a sequential and methodical way of examining all potential initiating events or failures that can occur anywhere in the overall "system of systems." Application of this nodal approach addresses the initiating events or failures that occur within a singular node while considering the consequences or impacts of such an event on a system-wide scale. This is commonly referred to in terms of assessing "Global Consequences." The risk assessment will include the documentation of all of the credible consequences from a single node initiating event as they cascade through the entire scope of the oil and gas infrastructure, considering the consequences in both the upstream and downstream affected nodes. This concept of "consider local causes, but account for global consequences" is a commonly implemented approach for a wide variety of risk assessment projects.

Preliminary Infrastructure Risk Screening

Preliminary risk screening is a common risk assessment methodology used to focus risk assessment resources on the most significant population of nodes. A Preliminary Infrastructure Risk Screening of each node will be performed after the infrastructure has been organized into specific nodes. Nodes that do not have the potential to create significant consequences will be eliminated from further risk analysis. The screening process and criteria will be used to postulate worst case credible events for each node such as equipment failures due to mechanical breakdown, human error, or natural hazards, and will conservatively estimate the potential consequence for the following three types of risk categories to be evaluated:

- *Safety Consequences* – Potential safety impacts to both infrastructure workers (occupational) and to members of the public.
- *Environmental Consequences* – Loss of containment/spill events that have the potential to create adverse effects on the external environment.

- *Reliability Consequences* – Unexpected loss of revenue to the State from unplanned outages of oil and gas production.

Categories have been developed for each of these consequences. If the node has a potential impact greater than the bottom (lowest) category for a given type of consequence (i.e., safety, environmental, reliability) the node will be carried forward into the detailed risk analysis for that type of consequence. If the node does not have a potential impact greater than the bottom (lowest) category for any of the three risk types, the node will be excluded from further risk assessment activities since it would not have the potential to result in significant failure.

Operational Hazard Risk Assessment

The operational hazard risk assessment involves estimating the infrastructure risks that can be attributed to equipment failures from mechanical failures and human errors. Failure modes will be identified for equipment in those nodes that could potentially have significant impacts, as identified by the preliminary screening of infrastructure. For these particular equipment failure modes, data will be gathered from published references and from meetings or workshops with owners/operators of the infrastructure. The data will be combined using applicable statistical methods, and a failure frequency will be estimated.

The consequences of each scenario (i.e., the impact on safety, the environment, and system reliability) will be calculated using material release rate models, material dispersion models, fire and explosion models, safety impact models, release isolation time and equipment repair/restoration time data (which must both be collected from the owners/operators), an environmental impact model, and production interruption information. The combinations of equipment failure frequencies and consequences (safety effects, environmental impact, and production loss) will be used to estimate risk for the node.

Operational hazards include the following types:

- Fires and explosions (which can result from hydrocarbon releases),

- Spills and leaks (e.g., due to natural aging process--corrosion, abrasion, wear and fatigue),
- Equipment malfunctions,
- Loss of infrastructure support systems (e.g., power),
- Changes in process conditions (e.g., composition--heavy oil, increased quantities of solids produced, and throughput decline), and
- Human error (due to worker fatigue, not following proper procedures, resource availability, etc.)

Safety Risk

The purpose of the safety risk assessment component of the operational hazard risk assessment is to estimate potential harm to workers on site at infrastructure facilities and to the public in nearby communities. The safety risk calculation will include three major tasks in the proposed methodology:

1. Consequence Analysis – Evaluation of physical effects of incidents on people;
2. Likelihood Analysis – Estimation of incident frequencies; and
3. Risk Calculation – Calculation of risks, which are a combination of likelihood and consequences/impacts, and presentation of results.

Safety consequence analysis is focused on the following issues: 1) The quantity and duration of the hydrocarbon material released; 2) the release distance and form of the released material into the atmosphere; and 3) the final form of the released material. Once the magnitude of the hazardous event has been determined, the potential impact on local operations personnel and/or the public will be determined based on relevant staffing and population data. Modeling of worst-case release events and mitigations to protect people from such incidents will either be obtained from facility siting studies requested from facility owners/operators, or will be performed using software and specific infrastructure and hydrocarbon release data for infrastructure lacking an available facility siting study.

The likelihood analysis is composed of two consecutive tasks: estimation of the failure frequency (i.e., likelihood of failure) for components followed by analysis of the frequency (i.e., likelihood) of significant hazardous operational events. Generic industry-wide reliability data and facility-specific data will be combined to estimate component failure frequencies specific to Alaska's oil and gas infrastructure, using the Bayesian updating tool. For pipeline segments, the scoring method will also be used. Event tree techniques will then be used to identify and estimate the frequency of operational hazardous event outcomes.

Environmental Risk

Loss of containment of vessels (i.e., tanks, pressure vessels and other types of vessels used for the storage or processing of oil and gas) and pipelines containing liquid will result in a spill on the ground or into water, depending on the location of the spill. The environmental risk assessment component of the operational hazard risk assessment is focused on the likelihood, size, and type of spills of hydrocarbon and seawater streams to the external environment. The process of environmental risk assessment includes significant hazardous operational events that potentially result in significant spill scenarios that have been identified through the FMEA technique.

The environmental consequence analysis will address the numerous contributing factors that are associated with spill impacts. These include 1) sensitivity of the surrounding external environment, 2) composition/type of fluid stream that is released, 3) release quantity or volume of fluid released, and 4) recoverability of spill volume and remediation efficiencies. An environmental consequence score will be calculated for each of the release events that are considered, based on the index values that are assigned in each of the contributing factor categories. Likelihood analysis will be performed similar to the safety likelihood analysis described above. The environmental risk methodology for operational hazard scenarios is based on the likelihood of the spills (i.e., likelihood of equipment failure causing a spill scenario) and the environmental consequence of the resulting spill.

Reliability Risk

The purpose of the reliability risk assessment component of the operational hazard risk assessment is to analyze the potential for oil and gas production losses that are significant enough to materially affect state revenue. The model provides an estimate of production outages, defined by barrels of production lost, which can subsequently be used by the State to quantify dollar impacts to the State using the Department of Revenue (DOR) State Revenue Forecast model at a given point in time.

The reliability risk methodology for operational hazard scenarios is based on the frequency of the initiating event for a scenario, the estimated production impacts, and duration of the event. In the reliability assessment, the first step will be to prepare reliability block diagrams (RBDs) documenting the production process flows. Using the RBDs and other design information, a what-if analysis for the node will then be performed to identify scenarios that result in significant production losses.

Scenario frequency estimates will be made that reflect generic industry-wide reliability data, facility-specific data, and engineering judgment. When necessary, event trees will be used to analyze the sequence of failures, operator errors, and other factors that contribute to the scenario occurrence. The level of production impact (e.g., 100% of node flow, 50% of node flow) and the duration of that impact will be estimated for each scenario selected for analysis, with input from facility operators/owners.

Natural Hazard Risk Assessment

A natural hazard risk assessment will be performed as a supplement to the operational hazard assessment to estimate the risk of natural hazard events that can cause significant impacts. Natural hazards are phenomena that occur in the environment, external to the oil and gas infrastructure and its operations. Natural hazards include atmospheric, hydrologic, geologic, and wildfire events that, because of their location, severity, and frequency, have the potential to affect the oil and gas infrastructure adversely.

As with the operational hazard risk assessment methodology, preliminary risk screening will be used to focus risk assessment resources for the natural hazard assessment on the most significant population of nodes. The first step of the natural hazard screening is to identify those natural hazards that are applicable to the node. For each applicable hazard event, the equipment associated with the node will then be reviewed to determine if it is vulnerable to failure for that natural hazard. If the node passes these two screening steps (i.e., a specific natural hazard is applicable and equipment in the node is vulnerable to that hazard), likelihood and damage for the applicable natural hazards will be assessed using a detailed risk assessment model based on industry guidance for natural hazard assessment.

The nodes will be screened against 10 pre-selected natural hazard classes which were developed during Phase 1 based on input from the stakeholder consultation process. The project team's natural hazards experts combined and reorganized these stakeholder recommendations to make up the following classes of natural hazards to be considered as part of the assessment:

- Earthquakes,
- Tsunamis,
- Volcanoes,
- Coastal erosion,
- Permafrost thawing,
- Severe storms,
- Floods,
- Severe currents,
- Avalanches, and
- Forest fires.

The detailed natural hazard assessment methodology is based on consensus procedures developed specifically for natural hazard assessment of oil and gas pipeline systems by the ALA. Extensions will be applied to the ALA approach to make it applicable to areas of the Alaska oil and gas infrastructure that are not pipelines or pipeline associated facilities (e.g., offshore platforms),

and address natural hazards within the scope of the project that are not currently covered by the ALA guidance.

For those nodes found to have a potential for significant consequence(s) during preliminary screening, and at high exposure for specific natural hazard applicability and vulnerability during natural hazard screening, a more detailed evaluation will proceed. The detailed assessment consists of the following steps: 1) identify and quantify natural hazards, 2) identify and quantify the damage states of nodes, 3) consider existing mitigation measures, and 4) estimate the infrastructure natural hazard risks. Implementation of this methodology will result in the definition of natural hazard scenarios, estimation of the frequency and consequence for those scenarios, and allow natural hazard risk to be included in the project risk profile for the Alaska oil and gas infrastructure.

Due to the large number of different hazards to be considered and the physical scope of the infrastructure to be considered, the general approach will be to implement the Level 1 approaches recommended by the ALA guidelines and comparable approaches (where practical) for infrastructure items not covered by those guidelines.

Risk Assessment Results

Operational and natural hazard assessments will be summarized and presented to the State during the final phase of the ARA project. The summary will include a discussion of 1) components of the final risk assessment database tools, 2) the three ways data will be summarized for presentation to the State and how these formats might be used by the State in future risk management efforts, and 3) how risks in each of the three consequence categories can be compared.

Risk data from the operational and natural hazard assessments will be compiled into a database of the individual scenarios considered as part of the overall risk assessment. After the risk assessment database is populated, the risk assessment results will be summarized and presented in three different formats that will help the State and other users to visualize the results of the project. The basis for these formats will be “major risk contributors” and “contributing factors.” Major risk contributors are the individual nodes or groups of nodes that present the most risk.

Contributing factors reflect the characteristics of the scenarios or nodes (e.g., locations, component types, failure type) that are common to several relatively important risk contributors. Presentation formats will include

- **Risk Matrices** – shows the number of events by risk level (based on frequency and consequence) *(Safety, Environmental, and Reliability consequences)*
- **Risk Histograms** – shows total estimated frequency for events assigned to each of the consequence categories *(Safety, Environmental, and Reliability consequences)*
- **Risk Summaries** – shows percentages of safety and reliability risk based on characteristics of the scenario and node. *(Safety and Reliability consequences)*

Risk summaries will be provided for the following: Facility, Facility type, Operating area (i.e., North Slope, Cook Inlet, TAPS), Owners/Operators, and Natural hazard (when applicable). A number of risk comparisons can be made using results from this project. Risk for a particular node of the Alaska oil and gas infrastructure is estimated by analyzing the risk of various scenarios involving that node. A specific node may have multiple scenarios that present significant risks.

Similarly, a single scenario may result in significant risks in one, two or all three of the classes of consequence of interest specific to this project (i.e., safety, environmental, or reliability risk). Within a single consequence class, different scenarios can be compared by frequency, or consequence, or their estimated risk.

A final ARA report will document the results of the risk assessment. The primary outcome of this project will be a risk profile of the Alaska oil and gas infrastructure that can be used by the State to manage the risk of unplanned oil and gas production outages from significant hazardous events. Such risk management decisions include answering questions such as:

- What risk management initiatives should be pursued?
- What risk management initiatives should not be pursued?

- How much money should reasonably be spent on risk management?
- How should that money be spent to obtain the most value?

4. TRB COMMITTEE EVALUATION OF PROPOSED METHODOLOGY

Assessing the economic, environmental, and safety risks associated with Alaska's oil and gas infrastructure is a large, complex task. Any successful methodology will have to be feasible given real-world constraints, analytically rigorous, and useful to the State. The committee believes that the proposed methodology falls short on all three criteria and believes that the method, as described, cannot be implemented given the time and budget constraints imposed by the State. The proposed methodology, as described, appears to be too data intensive given the available resources. It assumes significant industry cooperation that is neither promised nor likely to be forthcoming. Even if industry were willing and able to provide all of the data requested, it appears unlikely that the proposed methods are doable and would be useful in identifying and ranking the risk components of the physical and operational infrastructure system. A request by the TRB committee for a "worked example" of one small part of the proposed method was not possible without significant additional funding. Even if the method were successful in uncovering risk factors, the output of the project in the proposed format was not designed to be useful to the State in their risk management decision making. Some of these problems originate with the State and its Request for Proposal (RFP), but much of the responsibility resides with the approach taken in the proposed methodology.

The following discussion of the proposed methodology's limitations is organized roughly in the order that a risk assessment would be conducted (i.e., data collection, model building, and results presentation).

Is the Proposed Method Feasible?

An effective risk assessment methodology has to account for the intrusion of constraints from the real world. Deadlines need to be met and budgets cannot be exceeded. Although 2 years was

allocated for this project (ADEC 2008),[7] over 7 months were consumed by the first step of Phase 1, during which time stakeholder inputs were assessed and the actual assessment methods were developed; then another 2½ months were used to develop the proposed risk assessment methodology, followed by another 3 months of briefings and information gathering on stakeholder and industry comments on the proposed methodology. This left less than a year to complete the actual risk assessment. The committee was not privy to the staffing levels available to the contract team, but the scope of the proposed work would likely overwhelm even the best team.

To make the project doable with the given time and funding constraints, the contract team was apparently expecting to draw upon significant industry cooperation and voluntary assistance. In one of the documents, the gratis industry contribution was pegged at 50,000 h for a 6-month period (approximately 25 man-years of work, that is, 50 industry personnel solely working for 6 months to provide data) (ADEC, personal communication, May 7, 2009). The contract team needed industry assistance in completing all aspects of the proposed work including obtaining detailed facility descriptions and historical failure data, assessing accident response performance, and generating accident scenarios.

In addition, it was unclear that the contract team had a clear idea as to what specific data were needed to complete the assessment. It appears that the team's plan was to cast a very broad net and collect as much information as possible from various industry sources and then to sort through it and select what they needed. This unfocused data-capture request raised legitimate concerns with industry. Not knowing how the data that they provided was going to be used and how access to it was going to be controlled caused significant apprehension for industry. With pending legal actions from State and environmental groups seeking to limit oil and gas activities, industry was hesitant to provide all their data. From the industry perspective, the data requests were orchestrated in such a way that there were large potential downside risks and little, if any, upside benefit (Alaska Oil and Gas Association, personal communication, May 6, 2009).

Industry had not agreed to such a commitment and, though there was some modest cooperation from a few companies, in the end, industry effectively decided not to participate in the project. In the interim, the dispute over data exchange led to a series of actions and reactions

[7] ADEC. 2008. *Request for Proposal: Comprehensive Evaluation and Risk Assessment of Alaska's Oil and Gas Infrastructure*. RFP 2008-1800-7379. March 14, 2008.

from both industry and the State. Data safe rooms and data confidentiality agreements were being investigated, but the suggestion by the contract team and the State that legislation be used to compel industry to provide data in order to move the process along added both uncertainty and time to the process. It was clear that useful legislation was not possible to solve the impasse in the time allotted for the project. To make matters worse, the team did not have a fallback position in place and had never thought through the impact or design of an alternative methodology if industry did not cooperate. The impact on the proposed methodology of the fact that industry was unlikely to participate was just beginning to be understood by all parties when the committee started its evaluation, and it was through the TRB committee's investigation that the implications of industry's decision became obvious to the State, eventually contributing to the decision to let the contract with Doyon Emerald–ABS expire on June 30, 2009, at the end of Phase 1.

Is the Proposed Method Analytically Rigorous?

A totally separate question is if the management constraints (i.e., time and budget) had not been placed on the contract team and if industry had been fully cooperative, could the methodology have been successful? The Doyon Emerald–ABS proposed methodology was based on the classic probabilistic risk assessment (PRA) approach, which defines risk as the set of triplets:

$R = \{(s_i, p_i, x_i)\}$

where

s_i = a scenario identification or description,
p_i = probability of that scenario, and
x_i = consequence or evaluation measure of that scenario (i.e., the measure of damage).[8]

[8] Kaplan, S., and B. J. Garrick. 1981. On the Quantitative Definition of Risk. *Risk Analysis*, Vol. 1, No. 1, pp. 11–27.

This underlying approach is well founded and has been used effectively across a wide range of applications. The specific approach proposed by Doyon Emerald–ABS takes the infrastructure system and breaks it down into thousands of nodes that represent functional parts of components of larger facilities. In order to limit the scope of the project, the proposed methodology describes a prescreening process by which these nodes are evaluated, not by their risk but by their potential to cause harm. At this nodal level, separate analyses were done for each of the three metrics (reliability, environmental, and safety) with each having its own cut-off criteria as to what constituted a significant impact. There were thousands of potential nodes. Although this screening approach can be effective, it is also data intensive and threshold selection can be (and was in this case) controversial. In addition, the sum of many minor impacts linked by initiating events could be significant but missed in this screening method.

The Doyon Emerald–ABS methodology document is not explicit as to whether a top-down modeling approach is adopted, although some of the techniques for such an approach are among the methods described in the proposal. The methodology seems to be focused on analyzing a great many nodes in the pipeline infrastructure system, potentially leading to a failure to see the forest for the trees. It was not clear to the committee whether the detailed, bottom-up approach could transition smoothly to a top-down systems view. For example, as with any large, complex system, problems often develop at the interface between major components, especially when the components on either side are controlled by different organizations. It was not clear if the proposed method would be able to highlight the importance of these connections and account for the bureaucratic hand-off failures that can (and do) occur. (Three examples of actual events that threaten the entire infrastructure are described in the following section and highlight the importance of this class of problems.)

To account for the myriad ways that failures could occur, the proposed methodology planned to evaluate the nodes by using a large set of scenarios. These scenarios should have been developed from a network (system) perspective, not a nodal (component) perspective. Recognition of the evolving condition of the infrastructure should be highlighted. Possible scenarios include

- Equipment malfunction;
- Natural disasters (e.g., earthquakes, tsunamis, volcanoes, coastal erosion, permafrost thawing, severe storms, floods, and avalanches) that challenge multiple facilities simultaneously;
- Fire and explosion;
- Loss of infrastructure support (power and communications);
- Loss of integrity caused by corrosion that is not adequately managed, degradation of materials (such as coatings), abrasion, wear, and fatigue;
- Operational hazards caused by a chain reaction of failures;
- Human error (caused by both omission and commission);
- Aging workforce that is not kept up-to-date through training;
- Changes in process (e.g., strategic reconfiguration, station manning, black start conditions); and
- Lack of regulatory oversight.

From this partial list, the proposed method addresses the first half to some degree. For example, some common mode failures were explicitly mentioned (e.g., loss of electrical infrastructure), but it was difficult to determine the extent to which system-wide concerns of the second half of the list would be handled. The committee acknowledges that some of these risk contributors (e.g., organizational factors) are hard to assess quantitatively; however, the proposed methodology does not offer an alternative, and it was the committee's understanding that the contract team was excluding any risk factor that could not be quantified in probabilistic terms. Another major ambiguity was that the method by which risk scenarios would be generated was not clearly explained or demonstrated.

Steps to ensure that the scenarios covered the range of possible and important initiating events were not delineated. Once again, industry participation was critical for this part of the method. For example, information from industry is the only way to determine how likely a certain type of failure is at a node for a given scenario and how operators are trained to respond to control the damage. As recognized by Doyon-ABS in their proposal, infrastructure-specific models of nodal and system response to failures cannot be developed on a generic basis. In addition, it was not clear how the interdependencies were to be identified among the system-level scenarios leading to combinations of reliability, safety, and environmental risk.

Is the Proposed Method Responsive to the State's Needs?

One of the State's top goals was to use the project to help determine risk management opportunities that would enhance the reliability, reduce the environmental risk, and reduce the human health and safety risk of the oil and gas infrastructure. The proposed methodology's deliverables stopped well short of meeting this need. Risk rankings of components and nodes are not sufficient to evaluate risk mitigation opportunities. The proposed outputs would be static in paper form. Relating intervention opportunities to the overall risk of the system would not be possible. Opportunities to reduce risk can take many forms (e.g., replacing aging pumps, increasing the training of emergency response personnel, or adding communication protocols among organizations), none of which could be evaluated with the proposed methodology's results.

A review of past problems with the infrastructure (like those mentioned in the case studies section) and how the method could have been used to identify not the specific event, but the class of problems represented by the event would have provided a significant boost to the credibility of the approach. However, when asked, the contract team stated that it was unlikely that such an approach would have helped.

In addition, because certain likely and important scenarios were excluded from the study by the State (e.g., malicious and terrorist attacks), it was impossible to determine the true value of a particular intervention. Any benefit that an intervention would accrue for reducing the impact of an act of vandalism could not be added into the analysis. By focusing only on a specified number and type of scenarios, the approach could obscure important risk mitigation opportunities. This difficulty was due, in part, to the language of the RFP prepared by the State of Alaska.

The committee's concern for what would be included in the final product of the proposed work is not a condemnation of risk assessment methodology per se—quite the contrary. A well-designed, pragmatic risk assessment is precisely the methodology needed by the State. Risk assessments are designed to allow for not only the ranking of risks but also the investigation and evaluation of alternatives to reduce those risks. The proposal stopped short of taking this next logical step that was originally requested by the State.

5. CASE STUDIES TO DEMONSTRATE LIMITATIONS OF PROPOSED METHODOLOGY

Presented here are three examples of actual scenarios that led to a significant risk to large portions of, if not the entire, system and to significant loss of revenue to the State and risk to the environment and the safety of workers. These scenarios provide some ground truth to any proposed method. How effective would the proposed method have been in identifying the class of problems represented by these actual events? Could the results be used to determine the value of risk mitigation opportunities? The committee's comments on these points are discussed in the assessment of the proposed methodology, in Section 6.

A. Prudhoe Bay Oil Spills (2006)

Summary

The State of Alaska's revenue derived from North Slope oil production was severely affected during 2006 when the operator shut down Prudhoe Bay production in the aftermath of two pipeline spills.

Background

On March 3, 2006, an oil spill was discovered on the Greater Prudhoe Bay Western Operating Area oil transit line between Gathering Centers 1 and 2. The spill resulted from pitting-type corrosion that caused an almond-sized hole. On August 6, 2006, there were two leaks on the Eastern Operating Area oil transit line between Flow Stations 1 and 2. The subsequent investigation raised concerns about the condition of the lines and about the possibility of additional leaks. While significant, none of the spills would have directly caused the loss of considerable State revenues. However, the initial uncertainty as to the underlying causes of the spills and the concern that other significant spills might occur resulted in the suspension of production for a 2-month period while an investigation took place for this area. It was subsequently determined that many factors contributed to the two spills.

- It was believed that the corrosion prevention program that had been implemented, along with routine management and regulatory oversight, was adequate to avoid corrosion problems;
- A leak-detection system was in place but had a history of false alarms and could not be relied upon by operating personnel;
- Continuing pressures to limit costs might have influenced decisions to defer the use of scrapers and smart pigs; and
- The characteristics of the pipelines (i.e., low-pressure operations) exempted them from some regulatory requirements.

Conclusions

The direct cause of the loss of State revenue was the decision by the operator to halt production in order to conduct an investigation aimed at avoiding additional significant spills. The major contributing factors were failures of management systems and prior operator decisions. Because of those failures, other spills could have occurred virtually anywhere in the pipeline network at any time without warning. As stated in Section 6, Comment 2, it appears highly unlikely that the proposed risk assessment methodology would have identified these types of failures or weaknesses rooted in the management systems and organizational interfaces.

B. PS 1 Near-Miss Incident (January 15, 2009)

Summary

A problem with a routine pigging operation in a production pipeline feeding PS 1 allowed light product to enter the pumping station, causing PS 1 to shut down for 34 minutes and causing the incoming crude oil stream, which had a high volume of entrained gas, to be diverted to tankage. When some of the material was vented to the atmosphere, only the absence of a source of ignition prevented an explosion and fire, with catastrophic consequences at PS 1. If a failure at PS 1 is not fixable in days, the entire TAPS and the North Slope fields would have to be shut down.

Background

A routine pigging operation on a line feeding PS 1 was being conducted by production operating personnel with the knowledge of TAPS personnel. However, at some point in the pigging operation the pig became stuck in the line. Unknown to the operators during a several-hour period, light material bypassed the stuck pig, entered PS 1, and eventually was released from atmospheric vents on the station's two break-out tanks. Fortunately, the wind was from a direction such that there was no source of ignition. Several factors contributed to this near miss:

- The work plan for the pigging project was inadequate since it failed to recognize the potential for a stuck pig, the proper pig-tracking procedures, and the possible consequences of problems that might be encountered in the operation;
- The Process Safety Analysis conducted by the production operations staff was incomplete, did not consider potential downstream consequences of operating problems, and did not involve the pipeline's operations personnel; and
- When an unexpected problem occurred in executing the pigging operation, there was a communications failure between the production personnel doing the pigging and the pipeline personnel operating PS 1.

Conclusions

An inadequate work plan and communications failures allowed a potentially catastrophic event to occur. The initiating event (a pig being stuck) was not normally related to any of the production facilities (e.g., pipes, valves, tanks). As described in Section 6, Comment 2, it is not likely that the proposed risk assessment methodology would have considered failure of management systems to prevent the propagation of the initiating event.

C. VMT Inventory (Winter 2008–2009)

Summary

As a result of the global economic turmoil in the fall and winter of 2008–2009, demand for petroleum products and thus for crude oil dropped sharply. One impact was that customers for Alaskan North Slope crude curtailed deliveries into their refineries. That, together with the effects of winter weather, caused the VMT storage tanks to approach their upper capacity. If those conditions had persisted, TAPS would have had to shut down, and North Slope production would have had to be shut-in, with a severe economic impact to the State of Alaska.

Background

The North Slope crude oil logistics system, which includes North Slope production, TAPS, marine transportation to move the crude to refineries in the lower 48 states, and those refineries, has limited storage capacity to accommodate unusual events, whether they are operating situations (including weather) or are driven by external economic considerations. The system, which involves many facilities and all sorts of infrastructure, also involves many organizations (multiple production operators, pipeline and terminal operators, shipping companies, refineries, logistics operators, and others). Coordination during periods of unusual events is made more difficult by conflicts among the myriad parties, with potential financial and legal repercussions for decisions that might be in the best interest of the system but not that of individual participants. For example, during the last few days of 2008 and the first few days of 2009, a combination of severe weather in Valdez that caused the curtailment of marine loading operations and of operating problems in pump stations at the northern end of TAPS caused temporary shutdowns of TAPS, as well as temporary curtailments of North Slope crude oil production because of a lack of storage capacity. If those curtailments had lasted longer or been coupled with other operating problems, the impact on State revenue could have become significant.

Conclusion

A situation such as the curtailed demand for North Slope crude oil this past winter had the potential to cause the shutdown of TAPS for an extended period, which would have carried with it the risk of operating issues in the harsh Arctic winter and the potential for an extended outage with severe consequences for State revenue. The proposed methodology would not have recognized such a situation (e.g., fluctuations in the oil market) since it was explicitly outside the scope of the work (as specified by the State) to be considered.

6. RECOMMENDATIONS AND GUIDANCE FOR FOLLOW-ON STUDIES

The Alaskan oil and gas infrastructure system is large, diverse, and complex. To adopt a classical PRA approach in the WASH 1400[9] paradigm for the entire system while accounting for three impact metrics (i.e., reliability of the system, environmental damage, and safety concerns) is an enormous task. In order for the work to be completed in a timely fashion and yield results that are useful to the State, the process has to be bounded and focused. Although there is no question that including all three metrics is beneficial and politically desirable, the State should determine what effect their inclusion has on the quality, timeliness, and usefulness of the project. At the same time, the scope has been narrowed by excluding several likely sources of initiating events (e.g., terror attacks and vandalism). To put the risks to the system into meaningful perspective, all major sources of risk should be included. Important mitigation opportunities could be overlooked because of a focus on only a subset of the initiating events.

To reduce the modeling and computation burden, the project should use an appropriate level of detail, not adding layers of models and variables where little risk is present and not glossing over important functional relationships for the goal of efficiency. How to achieve this appropriate level is difficult to specify a priori because it is only from a holistic perspective that the overarching risks can be identified. For a problem of this size and complexity, a hybrid approach that integrates top-down and bottom-up analyses could be used to screen out

[9] U.S. Nuclear Regulatory Commission. 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. Technical Report WASH-1400 (NUREG 75/014). October 1975.

unimportant areas and focus the research effort where the detail is likely to have impact. Historically, parts of the infrastructure system that lie at the interface between the different controlling organizations have been a major source of risk and should be thoroughly investigated in the study.

Because of tight time constraints, the project cannot afford to re-create existing data sets or analyses. The project would be hurt if it had to rely on outdated or unnecessarily uncertain or ambiguous data. The project should have access to information with a focus on relevance. Casting a broad net and requesting all data and then sorting for relevance does not build trust with the data sources. In a similar vein, the project should have access to experts that exist throughout the system (e.g., state and national regulators, industry, and government officials). Their experience and knowledge can rapidly help to structure the problem. Having experts decide to not sit at the table can dramatically add to the time to complete the project and reduce the value of the final product.

The points of the previous paragraphs highlight the need for complete cooperation and buy-in from industry. They hold much of the relevant information and expertise. Although work-arounds can be constructed for data gaps created by industry not participating, the usefulness of the risk assessment effort would be limited. Engaging industry can be accomplished in several ways with a combination of carrots and sticks, but it is important that whatever the level of engagement, it be determined very early in the project's life so that appropriate methods can be applied. Building a methodology around expected industry participation and then at a later date finding a very different situation will kill a project.

Throughout the project, it is important not to lose perspective on how the results of the effort will be used by the State. A static paper document would provide little value to the State if it wants to evaluate the usefulness of various risk mitigation and risk management alternatives. A well-designed dynamic tool that allows for exploration of future scenarios involving possible risk mitigation options is much more valuable than a well-written report describing the status quo.

These key points are described in detail in the following five comment sections. The areas to be covered include

1. Revising the scope of the project to allow for the sequencing of work with an initial focus on reliability of the systems followed by the environmental and safety concerns, and expanding the focus to include all important sources of initiating events;
2. Focusing research efforts by using a combination of top-down and bottom-up approaches;
3. Working with industry from the earliest possible moment so that common goals can be identified and mutual cooperation can be ensured;
4. Focusing on the interfaces and linkages in the system; and
5. Focusing on the risk management process, not on a one-time effort.

Comment 1: Change in Scope

There is agreement among all stakeholders that the Alaska oil and gas infrastructure should be managed so as to ensure safe and environmentally sound operations. At the same time, it is critical that the infrastructure operate in a planned way without unexpected outages, that it be reliable. Only with reliable operations can members of the oil and gas industry make sound business decisions and the State of Alaska anticipate its revenue from oil and gas operations. Ranking across these three important goals by priority is already a difficult task, but the complexity of the infrastructure system dramatically increases the size of the problem. Because of this situation, the committee recommends a change in scope in which the three risks (environment, health and safety, and reliability) are addressed sequentially instead of simultaneously and that the reliability study be completed first.

Virtually every physical element of the oil and gas infrastructure, including every piece of equipment and every section of pipe, has the potential to be the source of a leak or a release of hydrocarbon and consequently has the possibility of causing harm to the environment. Similarly, every element of infrastructure has the potential to be the location of unsafe operations and consequently to harm to people, whether or not they are associated with the operations.

Most stakeholders consider any harm to the environment and to individuals, no matter how small, to be unacceptable. The oil and gas industry and the operators of its infrastructure should be working diligently and taking all prudent and reasonable steps to minimize the risk of events that will harm the environment and people.

The universe of elements of the oil and gas infrastructure that could be the source of harm to the environment and to people is very large. However, the portion of that universe that could represent a significant impact on reliability is quite small. In addition, most of the actions that could trigger a spill or release or cause harm to an individual are relatively simple and isolated. In contrast, the causes of events that lead to significant reliability and revenue issues tend to be complex and to involve multiple components of the infrastructure, human error, and failures of organizational and management systems.

Of necessity, assessing the environmental and safety risks requires a detailed, granular, bottom-up look at every element of the infrastructure, since every element could be the location of a failure. In essence, every single element must be assessed to identify how it might fail (and thereby cause harm), the likelihood of such failure, and the consequences of the failure. Such an approach requires the acquisition, analysis, and management of massive amounts of data. Although it is important that oil and gas operators conduct such analyses, the vast majority of failures will not be the cause of significant reliability consequences.

For example, a leak or release from a section of pipe will, by definition, cause some amount of harm to the environment and could be the source of some harm to one or more individuals, depending upon the circumstances. However, except in unusual situations, a leak or release is unlikely to cause significant harm to the budget of the State of Alaska, unless the leak was an indicator of a much larger systemic problem (e.g., lack of a proper maintenance or corrosion-monitoring program). Another example is the situation that might result from the failure of a technician to properly and fully tighten a flange on a piece of equipment. As in the first example, the resultant spill or release would harm the environment and could cause harm to people, but it would be unlikely that the budgetary impact would be large.

Major reliability events might have their origin from a spill or a release, but other factors such as the time and location of the event, the involvement of other infrastructure, or the failure of management systems would be the factors adding to the complexity and scope that turn a small or modest-sized event into one of large proportions. The approach to assessing the risks of major reliability and financial events generally requires a different approach than would be used for the environmental and safety risks discussed earlier. Rarely is such a large-scale event associated with a single or even just a few elements of the infrastructure. Rather, such events might include communications failures involving two or more operating organizations, human

factors issues (such as fatigue and poorly designed control systems), failures of management systems (such as management of change and hiring and training), or events outside the oil and gas infrastructure that propagate into the infrastructure. As one might expect, a detailed, bottom-up analysis of all of the infrastructure elements is unlikely to identify such overarching factors that would lead to major events.

The type of assessment that is most likely to be productive in identifying major reliability events would start with the identification of situations that could cause major financial impacts. The extended shutdown of TAPS would be such an example. The second step would be to identify the types of situations that would cause such a shutdown. They would not typically be single, isolated leaks, spills, or releases that could, for example, result from the growth of a corrosion pit. However, more generalized corrosion that causes thinning of the pipe wall over lengths of the pipeline sufficient to require replacement of large parts of the pipeline could have a significant financial impact because of the shutdown during repair and replacement. Additional examples of events that could cause such situations might be a serious marine incident that causes the VMT to be unable to load cargoes, an incident at one of the refineries connected to the pipeline that propagates into TAPS, an operating upset in the production facilities on the North Slope that culminates in the destruction of PS 1, and so forth. The identification effort should attempt to consider all elements of oil and gas operations, including exploration, production, refining, and pipeline and marine transportation, as well as government agencies at many levels and all phases of operations, including design, construction, operation, and maintenance. Following the identification of those situations that might lead to major reliability events, it would be possible to conduct specific, detailed analyses in order to develop mitigation strategies to eliminate or at least to manage the risks.

In summary, the operating events that most often cause harm to the environment and to individuals are typically quite different from those events that will cause major financial harm to the State of Alaska. It is important to address both classes of events, but the approaches and tools that will be most effective are quite different for each. Because of the complexity of the overall system, the committee recommends first taking a broad, top-down approach that will yield quick, useful results with regard to major financial and reliability events, and then following that with a more detailed, bottom-up approach that focuses on environmental and safety concerns. Having the second study build on the first would lead to a much stronger

product because of a better understanding of data needs, analytic model requirements, and scenario designs.

Comment 2: Combining Top-Down and Bottom-Up Approaches

Alaska's oil and gas infrastructure is a complex "system of systems." As such, an effective risk assessment method should

- Use a top-down approach that focuses on the analysis of the system as a whole and only adds details as needed, and
- Pay special attention to the interfaces between the major systems and installations.

A top-down approach provides a high degree of assurance in terms of coverage and completeness of high-risk items without requiring detailed analysis of possibly hundreds of thousands of components, elements, and contributing factors. A scenario-driven, top-down risk analysis of a system of systems can initially focus on identifying the key system-level failure modes and propagation mechanisms. The aim would be to develop the main classes of risk scenarios, leaving smaller variations within such scenarios and the enumeration of their specific causes to a more detailed analysis when and if needed. The need for details may arise, for instance, in reducing uncertainty in risk estimation or in evaluating risk management strategies. Accordingly, a risk model of a complex system of systems that would start with a highly abstracted model may in the end have a non-uniform level of detail. The so-called bottom-up analysis approach, such as FMEA or Hazardous Operations (HAZOPs) analysis, can provide the analytical and modeling tools when details are needed in a top-down analysis process.

Among other benefits, a top-down approach

- Controls the amount of qualitative and quantitative data needed,
- Offers early qualitative insights into system-wide risk vulnerabilities, and
- Provides a frame of reference to relate past incidents and accidents to a broader risk management perspective.

Comment 3: Engaging Industry from the Beginning

There is a "chicken-and-egg" dilemma between the methodology used to assess the risk and the data available to satisfy the proposed risk models. It is currently impossible to know what data will eventually be made available for future studies. However, regulatory mandates made by the State could be used to provide increased data access, but that legislation would require a clear notion of the expected methodology's data needs to prevent a "fishing expedition" that makes industry anxious and resistant. At the same time, developing a fully fleshed-out methodology that relies on data that never become available sets the State up for a repeat of the problems with the previous contract. To work around these problems, several steps could be taken:

- Engaging industry early in the process: If industry can be brought along from the beginning as an important part of the team, so that the study design has direct and tangible benefits to their operations, their cooperation is much more likely to occur.
- Justifying all data requests: All data that are collected by the risk assessment contractor should be clearly related to specific outcomes of the project. Clearly showing the tangible relationships between data requests and project goals will not only improve participation from industry but will also give the State justification for regulatory legislation mandating data access.
- Involving regulatory agencies: In addition to industry buy-in, it is necessary that the various regulatory agencies that have responsibilities for oil and gas infrastructure in Alaska also buy in and supply information to the contractor carrying out this study. Requesting information from companies that they have already provided to regulators will be seen as government inefficiency. In addition, companies have a legal responsibility to provide regulators with information on incidents, but unless new legislation is passed, companies have no such legal responsibility to provide information to the contractor who will be carrying out this study.
- Proposing a flexible methodology: Because of the uncertainty of data availability, the risk assessment contractor should use an approach that can work around various possible contingencies. Methods that provide valuable results regardless of final industry cooperation should be in place.

Comment 4: Focus on Human and Organizational Factors and System Interfaces

Although there could conceivably be completely different problems in the future (e.g., earthquakes, tsunamis, effects of climate change), many years of experience with aging oil and gas infrastructure in other jurisdictions indicate that material degradation is one of the major causes of reliability risk. In fact, it appears that the only problem with the oil and gas infrastructure that has had a direct and major economic impact on the State of Alaska is corrosion that was not adequately managed, indicating that a satisfactory integrity management system was not being implemented at that time. This evidence points to the importance of explicit incorporation of organizational and human factors into the risk assessment, something that is poorly integrated in the Doyon Emerald–ABS methodology. Lack of quantitative data is often the stated reason for not including human and organizational factors in systems risk assessments. Although this lack might be valid in some cases, because of the importance of the human and organizational risk sources, a qualitative assessment of their role and impact is essential as a minimum, particularly in determining the need for and effectiveness of risk management strategies.

These types of organizational problems are even more important when the infrastructure system is viewed in its entirety. A system of systems is typically formed from interconnected sectors and systems that are functionally and physically different, each possibly owned and operated by a different company or government entity and often subject to different environmental conditions, operational and management approaches, and different regulatory requirements. Such clusters of interconnected entities are often vulnerable to interface failures. Interfaces could be along one or more of the foregoing dimensions, covering physical, functional, and organizational boundaries.

TAPS is a system of systems. Although risk sources within each of the constituent systems may be well known and well managed by the corresponding owner or operator, the physical and organizational interfaces are subject to failure mechanisms such as gaps and lapses in communications and coordination among the interfacing entities and inadequately designed barriers against failure propagation from one to another. Acknowledging the importance of the role that human factors play in both the initiation of an incident and its propagation is critical. Simplifying assumptions involving human factors (e.g., maintenance and inspection protocols

will always be followed, or in the case of an accident, emergency personnel will respond consistently with no variability) will hide the true risk and minimize the importance of many risk mitigation options. Examples of failure propagation at TAPS interfaces are described in the three case studies in Section 5 of this report.

The risk assessment methodology should recognize the importance of such hidden vulnerabilities and devise an effective approach to identify them. The Doyon Emerald–ABS methodology has not articulated an approach to this issue.

Comment 5: Usefulness for Risk Management

Future RFPs need to define clearly the goals of the State of Alaska and the importance of being able not only to identify but also to manage risk from the oil and gas infrastructure. A successful methodology should show how it will contribute to those goals through the following steps:

- Modeling (both qualitatively and quantitatively) the oil and gas infrastructure in Alaska: Only with a baseline model of the current operations can possible risk mitigation options be evaluated. This baseline need not be an exhaustive node-by-node model but should include qualitative judgment when appropriate.
- Identifying key weaknesses in the system that could disrupt oil and gas production and transmission and reduce revenues: The baseline model can be used to identify the components and scenarios that are likely to lead to significant failures of the system. If this step is properly done, higher-level organizational problems that span multiple parts of the system can be spotlighted.
- Evaluating options for reducing the risks (e.g., new regulations, inspection protocols, training programs, hardware replacement): Only by having a forward-looking tool can possible future states of the infrastructure be evaluated. A successful project should allow for the systematic investigation of what-if analyses that compare different risk mitigation opportunities. The infrastructure system of systems is dynamically affected by the organizations that operate, manage, and maintain it. The final product of this effort should provide a means for understanding how decisions made by these organizations affect the infrastructure's reliability.

Modeling of the system is of course necessary in order to have a representation of the entire oil production and transport system at a proper level of abstraction and granularity so that the possible risk scenarios (including causes and consequences of upset conditions and failure mechanisms) can be identified. The same model would be the basis for calculating the likelihood of the risk scenarios (using probabilities or qualitative scales). By ranking the risk scenarios according to their likelihood and consequences, key system weaknesses can be highlighted along the various risk dimensions (reliability, safety, and environment). It is against such weaknesses that different preventive or mitigation measures can be evaluated if the risk model provides ways to introduce the effects of such measures. In general, particularly for complex systems, risk models require appropriate computer software to facilitate the evaluation of the risk impact of various risk reduction measures. Without an automated tool, risk management would be hard if not impossible.

The foregoing goals should be recognized as different from the goals of the oil and gas producers in Alaska, who are more focused on costs and profits. The State's goals can be achieved by developing an overall model that includes components of well production, in-state transmission, in-state storage, out-of-state shipping, and all activities that could disrupt their operation. Excluding any of these major components will result in an analysis that misses important interactions and potential risks.

What can cause the reliability of existing oil and gas infrastructure to deteriorate? From experience with other aging systems, the main causes of reduced reliability are degradation of the materials from which this infrastructure was constructed, primarily the steel and the coatings that were originally installed to protect the steel, and human or management errors compounded by complacency, lack of training, and workforce turnover. The real issue is the management of infrastructure integrity, and the contractor would be well advised to include a focus on this aspect and to identify the management system that is in place to ensure continued integrity. Development and implementation of an integrity management system can go a long way to reducing future risk. Conversely, in the absence of a comprehensive and rigorously enforced integrity management system at every company that owns or operates infrastructure, the future risk will be high. This is the basic nature of aging infrastructure.

The methodology should include a baseline analysis indicating current failure trends and actions that have been taken in response to past failures. Figure 1 illustrates the common

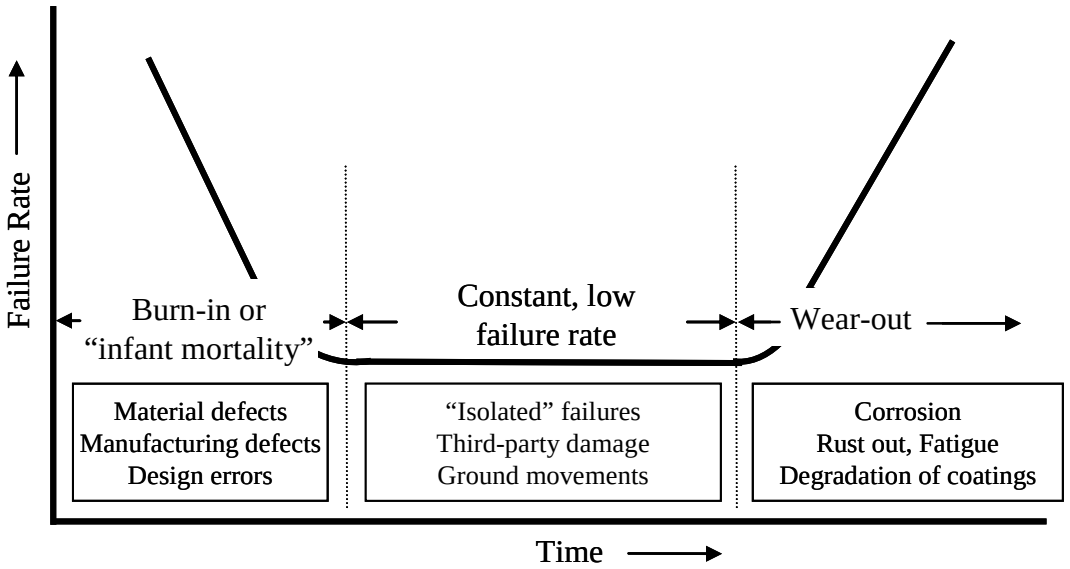

FIGURE 1 Common Failure Rate Curve (bathtub curve).[10]

"bathtub curve" for failure rate as a function of time. For the Alaska oil and gas infrastructure, the State is correct to be interested in an assessment of future risk, considering that much of this infrastructure would be regarded as an aging system, having operated for more than 30 years.

As part of a top-down approach, it would be valuable for the contractor to define, by using actual failure data for each year of operation, a graph of the type shown in Figure 1 to establish where the Alaska oil and gas infrastructure is on the curve. This type of analysis can be used to provide input for predicting future performance.

7. CONCLUSIONS

The committee believes that the classical detailed triplet approach to risk assessment (identification of initiating events, resulting consequences, and associated probabilities), as implemented by the contract team, will not be the most useful or productive product for the purposes of the State. Because of its myriad elements and dynamic, coupled actions and

[10] Adapted from Muhlbauer, W. K. 2004. *Pipeline Risk Management Manual: Ideas, Techniques, and Resources*, 3rd ed. Elsevier, Amsterdam, p. 1/6.

interactions, the totality of the Alaska oil and gas infrastructure can be considered a complex adaptive system. The interactive complexity of such a system is subject to "system accidents,"[11] in which multiple failures among components interact in unexpected ways to produce nonlinear, large-scale, or catastrophic failure. The Doyon Emerald–ABS methodology, both in its architecture and implementation plan, has severe limitations in identifying significant system-wide risk scenarios and quantifying corresponding likelihoods. The methodology offers a clear strategy for a modular, bottom-up representational model of the oil and gas infrastructure components and systems and facilities (nodal model). However, the approach for developing the most likely risk scenarios from such a detailed nodal model is also from the bottom up, which in the committee's opinion is highly ineffective if not totally misdirected. For a system as complex and multifaceted as Alaska's oil and gas infrastructure, high-risk events are more easily found through a top-down system view in which details are progressively added as needed.

It is possible that the most productive approach, at least for the events of highest consequence, is to take a comprehensive, primarily qualitative approach that identifies and describes those system aspects that have a potential for causing system accidents, based partly on analysis and evaluation of historical events (Section 5), while extending and interpreting lessons learned with a global systems perspective. These aspects would be described in enough functional detail that the problems could be clearly understood and appreciated and thus shared and communicated among stakeholders. From this understanding risk management options could be developed and more detailed modeling planned.

The ultimate value of a risk assessment is in its ability to identify important system vulnerabilities against which risk mitigation options are defined and evaluated. One of the major deficiencies of the proposed methodology is that it has limited its scope to quantifiable vulnerabilities, leaving out many of the hard-to-quantify organizational and human contributors to risk. Such factors, however, are likely to be the causes of many important risk scenarios in the oil and gas infrastructure.

Any risk assessment must make many practical modeling trade-offs. There are always important trade-offs between complexity and uncertainty, between precision and accuracy, and between completeness and communicability (understandability), as well as schedule and budget constraints. The risk assessment methodology should make these trade-offs explicit while

[11] Perrow, C. 1984. *Normal Accidents: Living with High-Risk Technologies.* Basic Books, New York.

avoiding succumbing to the uncertainty of the complexities of the Alaska oil and gas infrastructure system. At the same time, false precision should not obscure accuracy, and transparency should be emphasized.

In the next RFP, the State should keep a focus on an end goal of risk management including, where practicable, risk management options that rely on control or prevention and where not practicable, methods to increase system robustness (using technology, management controls, or both) by enhancing early (developing) problem identification and implementing real-time system modifications that avoid or decrease the potential for catastrophic losses.

Enclosure A

Committee on Alaska's Oil and Gas Infrastructure
Risk Assessment Peer Review

Committee

Paul S. Fischbeck, Carnegie Mellon University, Pittsburgh, PA, *Chair*

Robin K. McGuire, Risk Engineering, Inc., Boulder, CO

Ali Mosleh, University of Maryland, College Park, MD

Shirish Patil, University of Alaska, Fairbanks

Richard A. Rabinow, The Rabinow Consortium, L.L.C., Houston, TX

R. Winston Revie, CANMET Materials Technology Laboratory, Natural Resources Canada, Ottawa

Chuck Vita, URS Corporation, Seattle, WA

TRB Staff

Beverly Huey, Senior Program Officer

Stephen Godwin, Director, Studies and Special Programs

Amelia Mathis, Senior Program Assistant

Enclosure B

Acronym List

ABS	American Bureau of Shipping
ADEC	Alaska Department of Environmental Conservation
ALA	American Lifelines Association
ARA	Alaska Risk Assessment
Bpd	barrels per day
DOR	Department of Revenue
FMEA	failure modes and effects analysis
HazID	hazard identification
LNG	liquefied natural gas
Mcf	1,000 ft^3
NGO	nongovernmental organization
PRA	probabilistic risk assessment
PS	pump station
RBD	reliability block diagram
RFP	request for proposal
SAOT	State Agency Oversight Team
TAPS	Trans Alaska Pipeline System
TRB	Transportation Research Board
VMT	Valdez Marine Terminal
VSM	vertical support member