Risk Assessment for New Technologies Technical Note

Submitted to
The Bureau of Safety and Environmental Enforcement (BSEE)

Submitted by
ABSG CONSULTING INC.
1525 Wilson Blvd., Suite 625
Arlington, VA 22209
(703) 351-3700

September 2015

BPA Contract # E13PA00008
Task Order # E14PB00078
Deliverable #A & B

Executive Summary

As the dynamic offshore industry moves into deeper, harsher and colder environments, operators propose new and emergent technologies to address the operational needs for drilling and production. The development of new technologies is advancing at a rapid rate and governing industry codes and regulations often cannot develop at the same pace. Establishing systematic processes for review and acceptance of proposed new design and technology concepts, to assess readiness and identify and address associated risks, will support technology innovation while ensuring safe and environmentally responsible operations. Tailored reviews are necessary given that the required level of review will vary depending on the new technology application. Any new technology evaluation process should be flexible and take these variations into consideration.

The objective of this technical note is to provide technical details associated with the risk assessments accompanying a new technology submission. This technical note provides an overview of risk assessment methodologies considered by the operator and submitted to the Bureau of Safety and Environmental Enforcement (BSEE) for review as part of the request for new technology application approval. The proposed risk assessment methodologies are applicable to both existing and new technologies.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The Bureau of Safety and Environmental Enforcement (BSEE) is responsible for the oversight of exploration, development, and production operations for oil and natural gas on the Outer Continental Shelf (OCS). BSEE's regulation and oversight of Federal offshore resources ensures that energy development on the OCS is safe and environmentally responsible. The functions of BSEE include oil and gas permitting, facility inspections, regulations and standards development, safety research, data collection technology assessments, field operations, incident investigation, environmental compliance and enforcement, oil spill prevention and readiness, review of operator oil spill response plans, oversight of production and development plans, and resource conservation efforts.

As the dynamic offshore industry moves into deeper, harsher and colder environments, operators propose many new and emergent technologies to address the operational needs for drilling and production. 30 CFR 250.200 defines *New* or *unusual* technology as equipment or procedures that:

1. Have not been used previously or extensively in a BSEE OCS Region;
2. Have not been used previously under the anticipated operating conditions; or
3. Have operating characteristics that are outside the performance parameters established by this part.

Operators are required to review all of their equipment and procedures to determine if it qualifies as a new or unusual technology under the above definition. If identified as a candidate, the operator submits a request to BSEE for the evaluation and approval of the proposed new technology. This request is typically made through the submittal of a project specific Deep Water Operations Plan (DWOP). Conceptual approval of non-project specific new technologies can come through the BSEE Technical Assessment Section (TAS) or the BSEE District Operations Support.

The main objective of the submittal is to demonstrate that the proposed new technology presents an increased or equivalent level of safety in accordance with current OCS practices. This can be challenging for new technologies since there may not be any existing industry codes and regulations. Therefore, it is critical that BSEE undertake a systematic process for the review and approval of proposed new design and technology concepts to assess readiness, and identify and address associated risks. Tailored reviews are necessary given that the required level of review will vary depending on the new technology application. The new technology evaluation process should be flexible and take these variations into consideration.

The guide "*Assessing the Use of New Technology on the Outer Continental Shelf*" provides guidance to operators on BSEE's new technology evaluation process and related submission requirements. The three main steps in the new technology evaluation process are:

1. New Technology Assessment
2. Risk Assessment
3. Barrier Assessment

The new technology assessment step helps determine if the submission involves new technology, new operating conditions, or both, and categorizes the new technology for further evaluation. There are four categories to consider in the first part of the new technology assessment:

1. Known Technology, Known Conditions
2. Known Technology, Different or Unknown Conditions
3. New Technology, Known Conditions
4. New Technology, Different or Unknown Conditions

Figure 1 illustrates the new technology assessment framework. Category One involves known technology used in known conditions and requires no additional analysis. Categories Two and Three involve changes to either the area/conditions or the technology. Analysis of new technology in these two categories focuses on the changes in the technology or the condition. Category Four involves changes to both the area/conditions and the technology, therefore more in-depth analysis is suggested.

Operators considering the use of new technology in categories Two, Three and Four must conduct analysis to identify major accident hazards and identify the barrier functions affected (see Steps 2.1, 3.1 and 4.1 in **Figure 1**). Next, the operator identifies the relevant barrier critical systems (see 2.2.1, 3.2.1 and 4.2.1 in **Figure 1**) and conducts any additional risk assessments identified during the initial hazard identification, focusing on the changes to either the technology and/or the condition (see Steps 2.2.2, 3.2.2 and 4.2.2 in **Figure 1**). Finally, the operator conducts a barrier analysis to identify barrier attributes and their success criteria (See Steps 2.3.1, 3.3.1, and 4.3.1 in **Figure 1**).

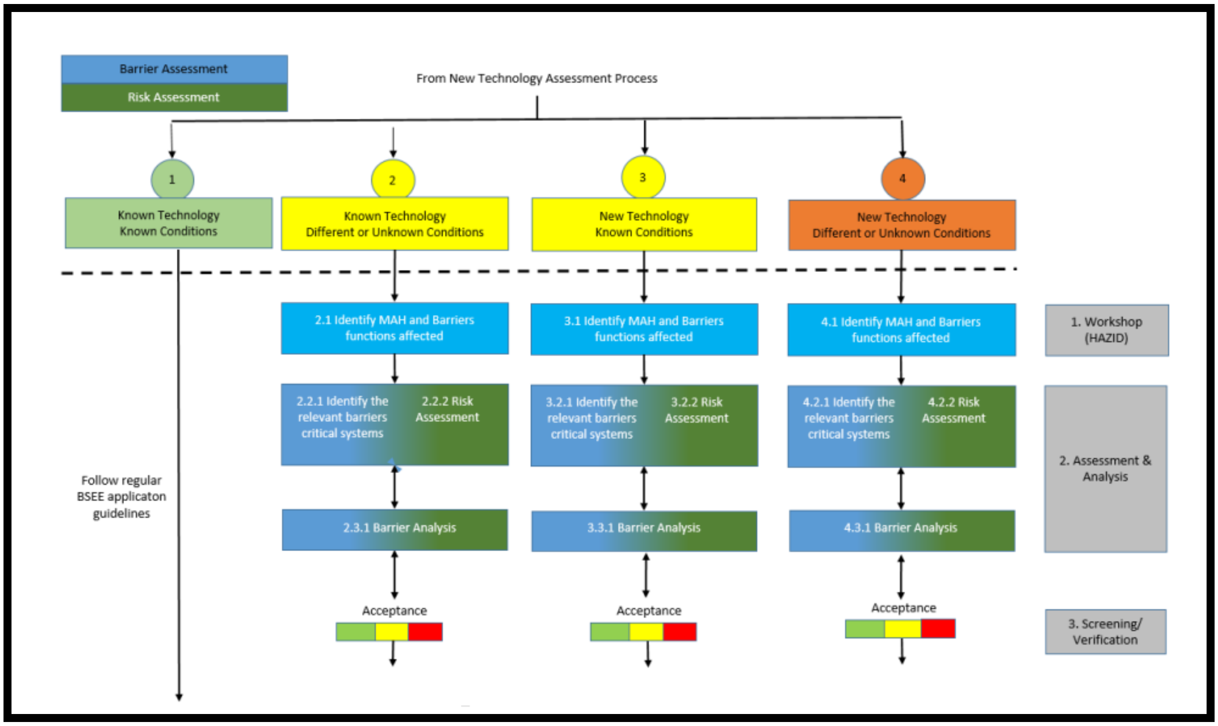

Figure 1: New Technology Assessment Framework

This technical note provides technical details associated with the risk assessment portion of this framework and establishes a clear understanding of Major Accident Hazards (MAHs) and risk assessment methodologies considered by the operator and submitted for BSEE's review as part of the request for new technology application approval. The risk assessment methods contained in this guide are applicable to both existing and new technologies.

The main assumption considered throughout this technical note is that the new technology application submitted for BSEE's evaluation is a barrier or is an element of a barrier. For example, new material being used in the barrier or completely new technology proposed (replacing an existing barrier) to meet the barrier function.

1.2 Identify MAHs affected conditions and/or new technology

For workflows two through four, the first step (shown in **Figure 1**) covers an identification of the relevant MAHs. In addition to the identification of MAHs, the task involves identification of relevant barriers affected by the modification/addition/condition change. The applicant (the operator in most cases) should perform this identification with the assistance of relevant Subject Matter Experts (SMEs). A Hazard Identification (HAZID) Study is the most effective technique to systematically identify hazards and relevant barriers. The HAZID is an integral part of the application process as it will form the baseline of any subsequent work. The focus of the HAZID will depend on which workflow is relevant; for example, whether new conditions or new technology are most prevalent, or a combination of the two. Possible degradation of any current barriers or an increase in the consequence of an unwanted incident is a key point to investigate. The following are the main objectives covered in this step:

- Identification of MAHs: Identification of the MAHs for the relevant operation and determining how to address changes in technology or conditions that affect the MAHs.
- Identification of affected barrier functions for control, prevention and/or mitigation of the defined MAHs: Identification of barrier functions established for preventing/mitigating the relevant MAHs and the effect of new technology or conditions.

When identifying MAHs and affected barrier functions, the HAZID workshop should focus on identifying the unknowns related to the new technology and conditions and should ensure that the overall design takes into account that there may be unidentifiable threats and responses using current industry experience.

1.3 Risk Assessment Methodologies

Table 1 presents different methods for conducting a risk assessment. The selection of the risk assessment methodology will depend on the results of the HAZID. Appendix A contains a detailed description of risk assessment methods

Table 1: Common Risk Assessment Methods

• Hazard Identification	• Failure Modes and Effects Analysis (FMEA)	• Preliminary Risk Analysis (PrRA)
• Hazard and Operability (HAZOP) Analysis	• Change Analysis	• Interface Analysis
• Event Tree Analysis (ETA)	• Trend Analysis	• Management Oversight Risk Tree(MORT)
• Fault Tree Analysis (FTA)	• Pareto Analysis	• Probabilistic Risk Assessment (PRA)
• Layer of Protection Analysis (LOPA)	• Relative Ranking/Risk Indexing	• Safety and Risk Evaluation using Bayesian Nets (SERENE)
• What-if Analysis	• Pairwise Comparison	• Integrated System Hazard Analysis
• Bowtie Analysis		

2. Risk Assessments for Categories of New Technology

2.1 Category One: Known technology in known conditions

For this category there are no expected changes from traditional submissions and therefore regular BSEE application guidelines are applicable for these types of submissions.

2.2 Category Two: Known technology – Different or unknown conditions

This category of new technology includes well-known and established technology applied in different or unknown conditions.

2.2.1 Workshop (HAZID)

The initial HAZID meeting (Step 2.1 shown in **Figure 1Error! Reference source not found.**) should cover topics concerning the new conditions. For example, different or unknown conditions for this scenario workflow may consist of deepwater operations or operations in the Arctic. Hazard identification includes those particular to the environment, area, and conditions in question as well as establishing potential changes to the nature, severity, or frequency of occurrence of MAHs. In addition, the relevant barrier functions against the identified MAHs should be addressed, along with their expected changes in functionality in new conditions.

2.2.2 Risk assessment

Once the MAHs have been identified, the risks they present to personnel, environment and facilities should be evaluated either qualitatively, semi-quantitative or, if appropriate, quantitatively. The complexity of the risk assessment should be commensurate with the hazards involved with consideration for management of uncertainties and critical data. The risk assessment normally involves the identification of initiating events, identification of possible accident sequences, estimation of the probability of occurrence of accident sequences and assessment of the consequences. Evaluating the acceptability of the estimated risk is based upon risk tolerance criteria appropriate to the particular situation.

Operations in new conditions could have an effect on the consequences of the identified MAHs and be addressed in the risk assessment. The risk assessment (Step 2.2.2) will focus on these changes for the identified MAHs. If the operation is in an environmentally sensitive area such as the Arctic, the environmental impact (i.e. consequences) from spills, dependent on size, could have a significant impact on the environment. Environmental conditions can also affect the consequences on the facility or in modules/areas, leading to a higher exposure of risk to personnel and impairment of safety functions or safety critical elements (structural integrity, safe area etc.). The focus of the risk assessment may be relatively high level, as there may be uncertainties associated with operations in new conditions. Therefore, the results of the assessment should be considered in accordance with the validity of the assumptions and the robustness of data used in the assessment.

2.2 Category Three: New technology - Known conditions

This category involves the application new technology in known conditions.

2.2.3 Workshop (HAZID)

For the HAZID in this case (Step 3.1), the focus is on how new technology can affect the existing barriers in place. It should also address whether the application of new technology could potentially have an increasing effect on the consequences of any unwanted incident or if the application of the new technology results in any additional consequences.

2.3.2 Risk assessment

The addition of new technology could potentially have an effect on the consequences of any identified MAHs and needs to be addressed (Step 3.2.2). Subsequently, a risk assessment should be performed (Step 3.2.2), dependent on the results of the HAZID. If the HAZID does not identify any issues that might result in changes of the consequences or probability of a major accidental event occurring due to introduction of new technology, the risk assessment will be limited and based on the barrier verification study. If the barrier critical systems retain their functionality and no changes in consequences or probability of occurrence are expected, the expectation is that the risk level will not increase for the relevant operation. If the HAZID does find that the application of new technology will lead to an increased consequence level, then an extended risk assessment should be performed to assess changes in the risk level.

2.3 Category Four: New technology - Different/ unknown conditions

This category is the most complicated application involving unknown factors concerning both technology and conditions.

2.3.3 Workshop (HAZID)

The HAZID addresses hazards related to both new technology and unknown conditions, with particular attention to any correlation between the factors. This last part will be critical, and the choice of SMEs to properly identify and assess hazards is critical.

2.3.4 Risk assessment

The risk assessments performed under this workflow will likely be larger and more complex compared to the other workflows. This is the most complicated scenario with possible changes to both the frequency and the consequence parts of the risk picture. Initially, a mapping of the effects on consequence attributed to changes in technology and conditions should be performed. The risk assessment (Step 4.2.2) will use input from the HAZID as well as input from the barrier verification study. In some cases, select barriers may be degraded due to new technology, new conditions or a combination of both, and will need to be reflected in the risk assessment. A sensitivity analysis on the risk assessment is recommended to assess the effect on changes in barrier functions.

Appendix A: Risk Assessment Methods Comparison Matrix

RAM	Description	Data Needs	Strength	Weakness	Application
Hazard Identification (HAZID)	The HAZID study is a brainstorming exercise of the possible causes and consequences of hazardous events. The objectives of the HAZID study are to identify and assess the potential hazards and their causes and consequences. It is used for early identification and assessment of potential hazards and their causes and consequences associated with the physical layout, operation and maintenance activities. It can be applied to all or part of the facility or it can be applied to analyze the operational procedures (e.g., physical layout, cargo and fuel storage location relative to collision, high fire risk areas, accommodations, and means of egress to muster areas and lifesaving appliances, bunkering, maintenance, etc.).	• Basis of Design • Process Descriptions • Process Flow Diagrams (PFDs) • General Arrangement of facility • Main Equipment List • Main Equipment sizing incl. main process parameters • Site Meteorological data • Area map • Site layout • Qualitative / statistical data on the number, types and size of vessels (Automatic Identification System [AIS] data) (Optional in preliminary stages) • Typical Marine Operations	HAZID Focuses on facility and non-process related hazards.	Typically high-level assessment with limited identification of initiation and intermediate events. Quality of assessment very dependent on subject matter experts who participate.	Can be used for all types of systems to identify the major hazards
Hazard and Operability (HAZOP) Analysis	The HAZOP study technique is a systematic review of the system design to identify and evaluate safety hazards of the system, and to identify operability problems which could compromise the system's ability to achieve the design intent. Its objective is to identify hazard and operability problems resulting from deviations from the process's design intent that could lead to undesirable consequences. The HAZOP analysis technique uses special guide words for (1) suggesting departures from design intents for sections of systems and (2) making sure that the proper safeguards are in place to help prevent system performance problems.	• Cause and Effect charts • Process Descriptions • Process and Instrument Diagrams (P&IDs) • PFDs • Results of consequence assessments (Optional to be used for ranking purposes) • Process Design Basis • Material Balance • Fire and Gas detection layouts and description	HAZOP focuses on process hazards specially for the fluid and thermal systems	Need well defined design for HAZOP being effective Time consuming Quality of the assessment depends on the SME No means to assess effectiveness of existing or proposed controls	HAZOP is best suited for assessing hazards in facilities, equipment, and processes and is capable of assessing systems from multiple perspectives: • Design • Physical and Operational environments • Operation and procedural controls Can also be applied to electrical systems (EHazOp), but not as easily applied

RAM	Description	Data Needs	Strength	Weakness	Application
Event Tree Analysis (ETA)	ETA is an inductive analysis technique that uses decision trees to model the possible outcomes of an event that can produce an accident of interest. Probabilities and frequencies can be added to the analysis to estimate risks numerically.	• Process Description • PFDs • Design Basis • Results of Hazards identification • Facility location (onshore/offshore) • Environmental conditions • Personnel on board • Hazardous inventory details • Fire and Gas detection layouts and description • Information on barriers and controls and their probabilities (for quantitative analyses)	A risk assessment technique that effectively accounts for timing, dependence, and domino effects among various accident contributors that are cumbersome to model in fault trees	Limited to one initiating event. An event tree is not an exhaustive approach for identifying various causes that can result in an accident. Other analysis techniques, such as HAZOP, what-if, checklist, or FMEA, should be considered if the objective of the analysis is to identify the causes of potential accidents. Can overlook subtle system dependencies. The paths at each branchpoint in an event tree are conditioned on the events that occurred at previous branch points along the path. For example, if ignition of a flammable release does not occur, there is no fire for subsequent lines of assurance (e.g., fire protection systems) to fight. In this way, many dependencies among lines of assurance are addressed. However, lines of assurance can have subtle dependencies, such as common components, utility systems, Operators, etc.These subtle dependencies can be easily overlooked in event tree analysis, leading to overly optimistic estimates of risk. • Quality of the analysis results depends on the quality of the documentation and the expertise of the subject matter experts • Unavailability of reliable and applicable data for many applications • Requires trained personnel to conduct the study	Generally most applicable for assessing system safeguards or response of particular systems or procedures once an event occurs. Useful in assessing mechanical and control systems, as well as modeling human responses.

RAM	Description	Data Needs	Strength	Weakness	Application
Fault Tree Analysis (FTA)	FTA is a deductive technique that graphically models how logical relationships between equipment failures, human errors, and external events can combine to cause specific accidents of interest. Probabilities and frequencies can be added to the analysis to estimate risks numerically.	• Process Description • PFDs • Process Design Basis • Results of Hazards identification • Facility location (onshore/offshore) • Environmental conditions • Personnel on board • Hazardous inventory details • Fire and Gas detection layouts and description • Data on failure rates (i.e., component failure data for quantitative analyses)	Includes human errors and common-cause failures	Narrow focus. Fault tree analysis examines only one specific accident of interest. To analyze other types of accidents, other fault trees must be developed. Quantification requires significant expertise. Using fault tree analysis results to make statistical predictions about future system performance is complex. Only highly skilled analysts can reliably perform such quantifications.	Generally applicable for almost every type of risk assessment application, but used most effectively to address the fundamental causes of specific accidents dominated by relatively complex combinations of events • Can be used as an effective root cause analysis tool in several applications – to understand the causal factors of an accident – to determine the actual root causes of an accident Generally most applicable for assessing electrical, mechanical, control and communication systems, in which the system or operation can be broken down into discrete components or events.
Layer of Protection (LOPA) Analysis	LOPA is a technique to systematically identify and assess the number and strength of layers of protection against major accident hazards. This information is used to make consistent and rational decisions on the adequacy of existing or proposed layers of protection.The Layer of Protection Analysis (LOPA) provides a consistent basis for judging if there are sufficient Independent Protection Layers (IPLs) to control the	• Cause and Effect charts • Process Descriptions • P&IDs • PFDs • Results of consequence assessments (Optional to be used for ranking purposes) • Process Design Basis • Material Balance	• Requires less time and resources than for a Quantitative Risk Assessment (QRA) • More rigorous than HAZOP. • The benefit applies especially	• It is not intended to be a hazard identification tool. LOPA depends on methods used toidentify the hazardous events and to identify a starting list of causes and safeguards. • Criteria for risk tolerance must be established • LOPA is a simplified approach	Applicable to process industries

RAM	Description	Data Needs	Strength	Weakness	Application
	risk of an accident for a scenario. LOPA is limited to evaluating a single cause-consequence pair as a scenario. The objective of LOPA is to address accident scenarios too complex or whose consequences are too severe to rely solely on qualitative risk judgment. The primary purpose of LOPA is to determine if there are sufficient IPLs against an accident scenario.	• Fire and Gas detection layouts and description	to scenarios that are too complex for a pure qualitative assessment. One can use it as a screening tool for QRA. • Takes credit for barrier effectiveness • Helps in deciding IPLs for reliable process operations • It facilitates the determination of more precise cause-consequence pairs	and should not be applied to all scenarios. The amountof effort required to implement LOPA may be excessive for some risk-based decisionsand is overly simplistic for other decisions. • LOPA analysis tends to drive initiating cause likelihoods to higher levels than actualfield experience. • It can only be applied to one cause/consequence pair.	
What-if Analysis	What-if analysis is a problem-solving approach that uses loosely structured questioning to (1) suggest upsets that may result in accidents or system performance problems and (2) make sure the proper safeguards against those problems are in place.	• Cause and Effect charts • Process Descriptions • P&IDs • PFDs • Process Design Basis • Material Balance • Fire and Gas detection layouts and description	A simpler alternative method to a HAZOP to identify hazards and may be useful if detailed design information is not available	• Quality of assessment very dependent on subject matter experts who participate. • Difficult to audit for thoroughness and for new or novel applications it would difficult to incorporate structured checklists.	Applicable to all types of systems and at various stages of design
Bowtie Analysis	Similar to LOPA, bowtie analysis is a technique for identifying layers of protection for major accident hazards, but bowtie enables analysts to consider multiple scenarios simultaneously. Bowtie is a particularly effective technique for communicating the relationships between prevention/mitigation layers and the scenarios that address.	• Process description • HSE Management system • Emergency response plan/resources • HazOp Study reports/Hazard Identification results/Hazard and effects registers	• The graphical representation the bow tie diagram can give a clear picture of what are often complex safety management systems. • Clear links between management	• Bow Tie analysis requires a high level of knowledge regarding a system and the components of the system that relate to its safety • It is difficult to link to quantitative techniques • It doesn't use Boolean logic • Requires software tool.	Applicable to all types of hazard scenarios (i.e., process) (e.g., loss of containment and non-process) (e.g., enterprise risk management).

RAM	Description	Data Needs	Strength	Weakness	Application
			systems and safety are shown • Helps in Gap analysis of HSEMS Helps in accident investigation and route cause analysis • Supports LOPA		
Failure Modes and Effects Analysis (FMEA)	FMEA is a reasoning approach best suited for reviews of mechanical and electrical hardware systems. The FMEA technique (1) considers how the failure modes of each system component can result in system performance problems and (2) makes sure the proper safeguards are in place. A quantitative version of FMEA is known as failure modes, effects, and criticality analysis (FMECA). It is also used as the basis for defining and optimizing planned maintenance for equipment because the method systematically focuses directly and individually on equipment failure modes.	• Process description • Process design basis • P&IDs • PFDs • Cause and effect charts • Operation philosophy • Maintenance philosophy • Facility Map/Layout(s) • Historical failure data (if any) • Historical incident/accident reports	A systematic, highly structured assessment relying on evaluation of component failure modes and team experience to generate a comprehensive review and ensure that appropriate safeguards against system performance problems are in place	• Examination of human error is limited. • Focus is on single-event initiators of problems • Examination of external influences is limited • Results are dependent on mode of operation • More suitable for well-defined systems	• Used primarily for reviews of mechanical and electrical systems, such as fire suppression systems and vessel steering and propulsion systems • Used frequently as the basis for defining and optimizing planned equipment maintenance because the method systematically focuses directly and individually on equipment failure modes • Effective for collecting the information needed to troubleshoot system problems
Change Analysis	Change analysis looks logically for possible risk effects and proper risk management strategies in changing situations (e.g., when system layouts arechanged, when operating practices or policies change, when new or different activities will be performed).	• Cause and Effect charts • Process Descriptions • P&IDs • PFDs • Results of consequence assessments (Optional to be used for ranking purposes) • Process Design Basis • Material Balance • Fire and Gas detection layouts and description	Systematically explores differences from the normal operations that can lead to the undesired risk and events that can contribute towards the risk concept simple	Generally requires an alternative concept that can be easily defined in terms of discrete changes or deviations from an existing or proven application.	Can be used for all types of systems, but generally for systems where changes in design or operation can be compared to existing system

RAM	Description	Data Needs	Strength	Weakness	Application
			tool		
Trend Analysis	Trend analysis is a technique to analyze historical accident and near miss data over time to identify consistent trends to predict future accidents. This technique is best suited to high frequency/low severity profiles.	• Historical failure data • Historical Incident/accident report/data • Process description	• The use of numbers makes the analysis more exacting. • A trend analysis can be replicated, checked, updated and refined when necessary.	• Since a trend analysis is based on verifiable data, it can be subjected to thorough scrutiny for validation. • Historical data may not give a true picture of an underlying trend.	Can be applied to any system with well-defined data sets on failure modes and previous incidents
Pareto Analysis	Pareto analysis is a ranking technique based only on past data that identifies the most important items among many. This technique uses the 80-20 rule, which states that about 80 percent of the problems are produced by about 20 percent of the causes.	List of problems with facts	Gather facts about the problem, using Check Sheets or Brainstorming, depending on the availability of information	• Requires well defined data sets for analysis • It focuses on the past data points only	Can be applied to any system with well-defined data sets on failure modes and previous incidents
Relative Ranking/Risk Indexing	Relative ranking/risk indexing uses measurable features of an operation or facility to calculate index numbers that are useful for comparing risks of different options. These index numbers can, in some cases, be related to actual performance estimates.	• Facility description • Actual and worldwide information of relevant accident/incident	• Accepts a high degree of complexity • Scale able to include multiple risk factors • May be used with a variety of quantitative and qualitative evaluation criteria	• May require significant effort in establishing risk factors and evaluation criteria • May require significant effort in breaking down risk into many components • Results may be difficult to correlate directly with absolute risks • Quality depends on the SME	Flexible for any type of risk
Preliminary Risk Analysis (PrRA)	PrRA is a simplified approach to accident-based risk assessment. The main goal of the technique is to define the risk related to important accident scenarios. This team-based approach relies on SMEs examining the issues. The team suggests possible accidents, most important contributors to accidents, and protective features. The analysis also identifies the risk of the accidents and identifies recommendations for reducing risk.	• Process/facility information • General Arrangement of facility • Main Equipment List • Site Meteorological data • Area map	Aids in ensuring safety, modifications less expensive early in the design phase	• High-level analysis. The preliminary risk analysis focuses on potential accidents of an activity; therefore, the failures leading to accidents are not explored in much detail. The high-level, general nature of the analysis introduces a level of uncertainty in the results. • General recommendations. One result of the analysis is the	Used primarily for generating risk profiles across a broad range of activities, such as in a port-wide assessment

RAM	Description	Data Needs	Strength	Weakness	Application
				development of recommendations for reducing risk. Due to the high-level nature of the analysis, these recommendations are typically general in nature instead of focused on attacking specific issues.	
Interface Analysis	Interfaces are important because they are everywhere. However, current approaches for managing safety risks at interfaces often only consider technical aspects and whilst some include considerations of man-machine interfaces few consider non-technical (e.g., organizational) interfaces. An approach to systematically identify, assess and manage non-technical interface risks. The emphasis of the approach is on bringing both parties together to work jointly to manage the interface risks.	• Process/facility information • PFDs/P&IDs • Equipment list/data sheets • Area map • Operation philosophy • Maintenance philosophy • Incident Records	Can be applied to • User interface or man-machine interface, where a person interacts with a machine or piece of equipment. • Different departments in an organization, for example operation, maintenance, safety, human resources, finance, procurement etc. • A project that is made up of a number of sub-projects or work streams.	Like HAZOP, effectiveness depends on procedures used and thoroughness of application.	Used primarily for system involving multiple interfaces
Management Oversight Risk Tree (MORT)	MORT is a comprehensive, analytical, disciplined method for determining the causes and contributing factors of major incidents. The MORT chart is the key diagram for the whole MORT system safety program. This chart sets down, in an orderly way, all the potential causal factors for accidents. Analysis is carried out by means of a fault tree.	• Process/facility information • PFDs/P&IDs • Equipment list/data sheets • Operation philosophy • Maintenance philosophy • Incident Records	• Highly detailed. A full MORT diagram or tree contains more than 10,000 blocks. • Very effective in identifying underlying management root causes of hazards. • Can also be used	• Time-consuming and costly. Should be used for only the most difficult or high profile events. • MORT is not a technique that would be used in the field. The analysis would therefore start with an accident report and possibly a sequence diagram • MORT therefore uses similar symbols and logic to that used in FTA	• MORT not only looks at what happened during an incident, but traces causal factors back to management systems to identify why events happened, thereby departing from strict FTA logic.

RAM	Description	Data Needs	Strength	Weakness	Application
			to predict the adequacy of control elements already in place to prevent accidents. • Provides a systematic method of evaluating the specific control and management factors that caused or contributed to the accident.		
Probabilistic Risk Assessment (PRA)	Probabilistic risk assessment is an integration of failure modes and effects analysis (FMEA), fault tree analysis, and other techniques to assess the potential for failure and to help find ways to reduce risk. It involves the development of models that delineate the response of systems and Operators to accident initiating events. Additional models are generated to identify the component failure modes required to cause the accident mitigating systems to fail. Each component failure mode is represented as an individual "basic event" in the systems models. Estimates of risk are obtained by propagating the uncertainty distributions for each of the parameters through the PRA models.	• Process description • Process design basis • P&IDs • PFDs • Cause and effect charts • Operation philosophy • Maintenance philosophy • Facility Map/Layout(s) • Component failure data	Provides comprehensive characterization of variability in the risk estimates	Time consuming and costly May provide inaccurate results if sufficient data is not available	Used primarily to evaluate risks associated with the complex systems,
Safety and Risk Evaluation using Bayesian Nets (SERENE)	The SERENE method is concerned with the functional safety of complex systems, In a complex system the demonstration of functional safety must take account of both random and systematic failures. Systematic failures include those that result from design errors. All complex systems are potentially subject to systematic failures, but this difficulty applies most of all to software, for which systematic failures are the only form of failure.	• Process description • Process design basis • P&IDs • PFDs • Cause and effect charts • Operation philosophy • Facility Map/Layout(s) • Failure rates / conditional probabilities	Bayesian Networks (BNs) form the core technology in the SERENE method. These allow the specification of risk models that represent the key factors and their inter-relationships	Quality of the assessment depends on the SME	Primarily used for evaluation of programmable electronic systems with emphasize on systematic failures

RAM	Description	Data Needs	Strength	Weakness	Application
			(qualitative model) with probability values and distributions estimated via expert judgement or from data (quantitative model). With the SERENE tool large-scale risk BN models can be built quickly and efficiently.		
Integrated System Hazard Analysis	Specific integrated analyses are appropriate at a minimum to evaluate interactions: • Human - Human Interface Analysis • Machine - Abnormal Energy Exchange, Software Hazard Analysis, Fault Hazard Analysis • Environment - Abnormal Energy Exchange, Fault Hazard Analysis The interactions and interfaces between the human, machine and the environment are evaluated by application of the above techniques, also with the inclusion of Hazard Control Analysis; the possibility of insufficient control of the system is analyzed.			An integrated approach is not simple, i.e., one does not simply combine many different techniques or methods in a single report and expect a logical evaluation of system risks and hazards.	Specific integrated analyses are appropriate at a minimum to evaluate interactions: • Human - Human Interface Analysis • Machine - Abnormal Energy Exchange, Software Hazard Analysis, Fault Hazard Analysis
Environmental Risk Assessment (ERA)	ERA is a detailed and systematic approach to assess a variety of environmental risk scenarios by estimating the probability or likelihood of occurrence and severity of the consequences of incidents for a proposed project or project's activities. The assessment of environmental effects is focused on species at risk and areas which have a potential for impact from projects and activities (e.g., eco-systems in the water, coastal environment including beaches, fish farms and related industries in the area).The ERA assess all environmental effects including those arising from accidents and malfunctions, and the effects of the environment on the project.	• Process description • Process design basis • P&IDs • PFDs • Cause and effect charts • Operation philosophy • Maintenance philosophy • Site Meteorological data • Site layout • Area map • Historical Incident/accident report/data • Statistical data on the number and types of species	A structured process that provides a detailed understanding of the consequences and effects associated with project activities such as operational discharges (e.g., drill waste, produced water)	Quality of assessment is dependent on subject matter experts who participate. The assessment of environmental risk should be implemented by a team consisting of a diverse range of relevant operational and environmental experts.The environmental impact is dependent on the amount and type of spillage, weather conditions (i.e., wave heights, wind and current speeds) and time and amount to arrive at sensitive	Applicable for a range of projects in different environments.

RAM	Description	Data Needs	Strength	Weakness	Application
		in the area	and emissions (e.g., noise, unnatural light, and air contaminants), presence of structures (e.g., rig, pipeline, survey vessel), and accidental releases (e.g., spills).	areas. An environmental consequence assessment of spillage may be complex and time consuming.	