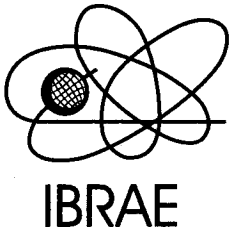

Nuclear Safety Institute

Russian Academy of Sciences

(IBRAE RAN)

Project Arrangement between the Department of Energy (DOE) of the United States of America, and the Nuclear Safety Institute (IBRAE) of the Russian Federation for Coordination of Emergency Preparedness/Response Activities

ANNEX 4

Milestone 8
Final Report on

Refined Risk Assessment Methodology at Hazardous Industrial Facilities and Facilities Handling Radioactive/Nuclear Materials

IBRAE RAN supervisor: Dr. A.V. Shickin

Moscow

2004

EXECUTIVE SUMMARY

History of the project

The U.S. (Department of Energy) and Russia (EMERCOM and MINATOM), under the aegis of the Joint Coordinating Committee for Radiation Effects Research (JCCRER) and the Arctic Council's Emergency Prevention, Preparedness and Response working group are conducting a series of pilot projects to develop a risk assessment methodology / source control process for reducing the potential for emergencies at facilities handling radioactive or other hazardous materials.

The projects are being implemented in accordance with the Russian-American Agreement on “Cooperation in research on radiation effects for the purpose of minimizing the consequences of radioactive contamination on health and the environment” signed on January 14, 1994, and the Project Arrangement Between the Department of Energy of the United States of America, and the Nuclear Safety Institute (IBRAE) of the Russian Federation for Coordination of Emergency Preparedness/Response Activities.

The projects include the development of a risk assessment methodologies document and on-site facility risk assessments at selected hazardous industrial facilities. The assessment includes the application of national technical and regulatory standards and the application of the international ISO 14001 and ISO 14040 Environmental Management Systems standard [1,2].

The hazardous industrial facility selected for the first pilot project is the drinking water and sewage treatment utility in Apatity, Murmansk region, Russian Federation. The enterprise supplies water to the population and industrial facilities of Apatity city and adjacent territories applying chlorine-related technologies. In accordance with the Russian legislation the enterprise is not referred to the category of “Hazardous industrial facilities” due to the fact that chlorine reserve of the storehouse does not exceed 25 t at a time. The first pilot project produced two reports: *Risk Assessment Methodology at Hazardous Industrial Facilities* (Working Draft), and *Analysis of Risks of Emergencies to Population and Territory, and Development of Measures to Reduce the Risks as Applied to the Apatityvodokanal Utility*.

The second phase of this project has been at a MINATOM factory handling radioactive and/or nuclear materials. FSUE «SSC RF Scientific and Research Institute of Nuclear Reactors» (FSUE «SSC RF NIIAR») located in Dimitrovograd city of Ulyanovsk region - was selected as such type of enterprise. Presently FSUE «SSC RF NIIAR» is the largest scientific and research center of Russia in the field of nuclear power which operates research nuclear reactors, material science facilities and radiochemical laboratories. Fuel element and fuel assembly research department (FRD) is the facility for risk assessment methodology approbation. FRD conducts study of full-scale fuel assemblies and elements of power reactors (VVER-440, VVER-1000, RBMK and BN) and pilot fuel elements tested in research reactors. Process equipment provides for the opportunity to deal with the items of the activity up to 10^5 Ci (3.7 PBq). The second pilot project produced three reports: *Legislative regulation of radiation safety at nuclear fuel cycle facility, Refined Risk Assessment Methodology at Hazardous Industrial Facilities and Facilities Handling Radioactive/Nuclear Materials* and *Study of safety conditions of SSC RF NIIAR fuel research department*.

Approach

Risk assessment at hazardous industrial facilities is an integral part of industrial safety management. Risk assessment is the systematic utilization of all available information to identify hazards and estimate risks of probable unexpected events. The main goals of risk assessment are to provide company or facility decision-makers information on:

- the hazardous material within a facility and a rank order of the greatest to least potential risk/threat;
- identification and status of facility safety features, and
- reasonable recommendations to reduce the risk.

This information is used to prepare plans to manage potential incidents arising from the handling of hazardous, radioactive or nuclear materials. In turn, decision-makers can use international standards and best practices such as the ISO 14001 process to establish prevention, preparedness and response programs based on relative risk and/or recommendations resulting from the effectiveness of systems and programs to manage

the hazards. To these ends, agency management can establish a structure and programs to address these risks through the implementation of international or modified country-specific policies and programs that define objectives and targets to achieve end results.

A critical outcome of the risk assessment is aimed at obtaining the results to determine and implement corrective measures, develop improved directives, instructions, action plans for continuous enhancement of production process in terms of safety. Of course, the audit and review of hazardous activities will be essential components to ensure that the environmental policy is complied with; and, that the environmental management system (EMS) remains appropriate to the risks identified and the program(s) to minimize those risks.

The current revised edition of the risk assessment methods is applicable for introduction of EMS based on ISO 14001 standard. To this end the document introduces some terms and definitions used in ISO 14001 and, simultaneously, the terms and definitions used in risk assessment and management, where it is applicable. At the same time, the methods can also be used separately.

International Atomic Energy Agency developed several documents (IAEA-TECDOC-994, 1998, IAEA-TECDOC-727 (Rev. 1), 1996), intended for support of projects on development of strategy of management of integral risks for large industrial areas with nuclear facilities. The work in this project is in concord with IAEA recommendations on risk management, which are based on complex assessment of risk and assigning of priorities.

This report developed for these pilot projects highlights three basic areas that are critical to an effective risk assessment. These are:

1. A thorough description of the risk assessment phases:

- work planning and organization;
- accident hazard identification (energy sources) :
  a) hazardous chemical inventories,
  b) radioactive and nuclear materials inventory, and
  c) Accidental hazards.
- risk assessment; and
- development of recommendations to manage and ultimately reduce the risk.

2. A survey of the state of the art in risk assessment methods and criteria and appropriateness for the selection and application of these methodologies based on available data, design criteria, and industrial operations.

3. Methodological foundation of risk matrix construction and the examples of risk matrixes for hazardous industrial facilities and nuclear- and radiation-hazardous facilities.

4. Requirements to documentary registration of results of the analysis of the risk, long-term programs providing development on management of risk.

One important documentation element is the theoretical basis for the processing. This is extremely important when the process reacts two or more hazardous chemicals to produce a valuable chemical and waste products. For maintenance of a level of safety of the enterprise it is necessary to create and support library of the technical information which contains the data about actual conditions at the facility. Specifically:

- Chemicals, radioactive or/and nuclear materials, their inventory and hazards
- Process piping and instrument diagrams
- Operating and maintenance procedures
- Employee participation and training
- Equipment integrity

LIST OF THE PROJECT DEVELOPERS

From the Russian side:

From FSUE «SSC RF NIIAR»:

- Usoltsev V.Yu. – contract manager, RS section head, RS chief expert;
- Kizin V.D. – RSD leading scientist, Ph.D.;

From – IBRAE RAS:

- Linge I.I. –deputy director, Doctor of Engineering Science;
- Shikin A.V. - senior scientist;
- Bakin R.I. – laboratory head;
- Frolova O.B. - junior scientist.

From the U.S. side:

- Bruce Russell — JS&A Environmental Services, Inc;
- Tomas I. McSweeney — Ph.D., P.E., Technical Leader Process safety and Risk Management.

The document "*Methods of risk assessment for hazardous facilities (intermediate report)" was prepared with participation of the following specialists of the Russian Cnter "Khlorbezopasnost"*:

- Steblev A.V.— chief specialist;
- Kareva E.I. — research assistant;
- Hubih E.V. — engineer.

TABLE OF CONTENTS

INTRODUCTION

Both increases in quantity and power consumption of hazardous chemicals used in industry and the increased technological complexity of modern enterprise technologies and operational modes require the development of a mechanism ensuring reasonable assessments of safety criteria for such production facilities considering the probability and consequences of potential accidents.

Both identification of hazards and risk assessment are considered as prerequisites for risk management plan (RMP) development to ensure environmentally safe management of operations in accordance with the ISO-14001 standard. Hazard identification should be an integral part of any existing operational system. Risk is usually estimated by determination of hazard probabilities and impacts (consequences) of possible incidents that could occur at industrial facilities.

It should be noted that risk assessment enables facility management to correctly determine measures to monitor and control hazards or prevent accidents at the hazardous industrial facility (HIF).

Risk management means the systemic approach to decision making processes and implementation of practical measures to prevent accidents, reduce the risk of industrial accidents, and protect human health and life, property and the environment.

Figure 1 shows the phases to be implemented for risk management plan development.

The methodology to assess the risk establishes risk-related principles, terms and conditions, general requirements to the procedures and results record-keeping, and represents basic methods for hazard and accident risk assessment at HIF.

This risk assessment methodology document that is being developed to be consistent with Russian Federation regulations and guidance documents developed by the Russian Federation, the IAEA, and international industry best practices. The methodology document is intended to be applied at hazardous industrial, radioactive and nuclear facilities. The differences among these classes of facilities is handled by providing general guidance in the main body of the document and then providing specific guidance to the various facility types in annex's. This methodology should provide the cornerstone

for the basis of a continuous (or continual) improvement program of a facility's environmental management system.

This “methodology” is intended for the experts of the organizations operating HIF.

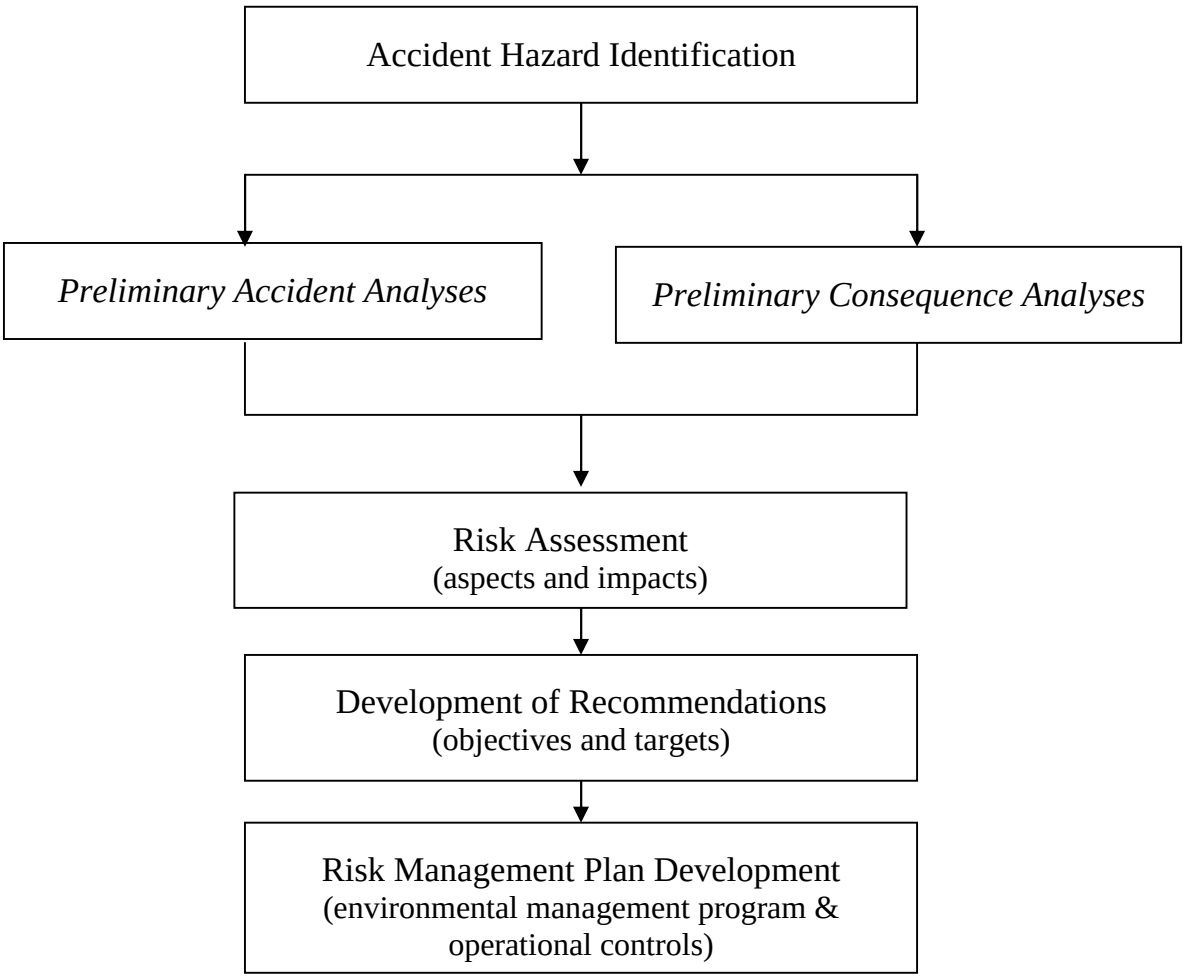

Figure 1. Main Phases of Risk Management Plan Development

In the ISO 14000 framework, as shown in Figure 2, Risk Assessment plays a central role. The figure shows the analysis begins with several planning tasks that result in a baseline assessment of the facility's risk. Once the risk has been determined, then the continuous improvement loop requires that the organization's management monitor the risk, identify where improvements are needed, and then implement the improvements that are shown to be cost effective. For an existing facility, since the process is a continuous improvement loop, it is always possible to perform a risk assessment and then go back and identify the attainable performance measures and objectives. As part of the improvement process, management might identify ways to improve the facility's performance and the decision is made to improve performance; the facility's performance objectives might similarly be tightened. Throughout the process, there are three elements that are understood. One, the facility's management is committed to the continually improving the performance of the facility. Two, that the facility's performance will be periodically audited; and three, that the basis for judging performance will be the facility's risk assessment. Imbedded in these elements is the assumption of thorough documentation because an undocumented system can neither be assessed nor audited.

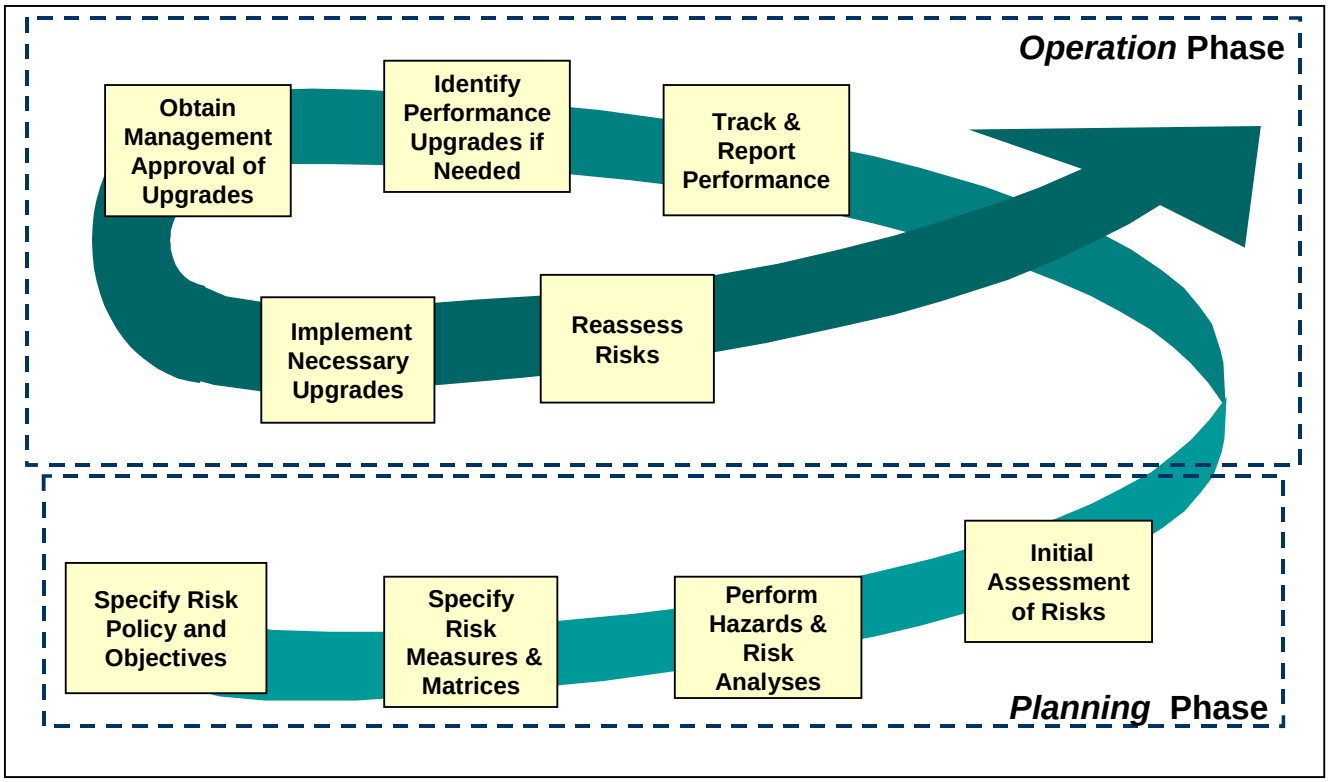

Figure 2.The Continuous (or Continual) Improvement Process

Management commitment is essential to the risk assessment process, the development and execution of the risk management plan and the continuous

improvement cycle. Comprehensive and thoughtful documentation provides essential information for Management Audits and form the basis for a Continuous Improvement Program. It is only possible to perform a good risk assessment with adequate documentation, it is also only possible for management to audit the processes and execute improvements with a well documented risk assessment and risk management plan.

1. Basic terms and DEFINITIONS

Accident, accident scenario, accident sequence: An unplanned event or sequence of events that results in undesirable consequences. An incident with specific safety consequences or impacts.

Administrative Control: A procedural requirement for directing and/or checking engineering systems or human performance associated with plant operation

Catastrophic Failure: results in human death, property significant damage, grievous damage to the environment.

Consequence: The direct, undesirable result of an accident sequence usually involving a fire, explosion or release of toxic, radioactive or nuclear materials. Consequence descriptions may be quantitative or qualitative estimates of the effects of an accident in terms of factors such as health impacts, economic loss, and environmental damage.

Consequence Analysis: The analysis of the effects of incident outcome cases independent of frequency or probability.

Continual Improvement: Process of enhancing the environmental management system to achieve improvements in overall environmental performance in line with the organizations environmental policy.

Critical (non-critical) Failure: is dangerous (non-critical) for human life, causes (no impact) significant damage to property and impact to the environment.

Engineered Control: A specific hardware or software system designed to maintain a process within safe operating limits, to safely shut it down in the event of a process upset, or to reduce human exposure to the effects of an upset.

Environment: Surroundings in which an organization operates including air, water, land, natural resources, flora, fauna, humans and their interrelation.

Environmental Aspect: Element of an organization’s activities, products or services that can interact with the environment.

Environmental Impact: any change to the environment, whether adverse or beneficial, wholly or partially resulting from an organization's activities, products or

services. A significant aspect is an environmental aspect that has or can have a significant environmental impact.

Environmental Management System: The part of he overall management system that includes organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing achieving, reviewing, and maintaining the environmental policy.

Environmental Policy: Statement by the organization of its intentions and principles in relations to its overall environmental performance which provides a framework for action and for the setting of its environmental objectives and targets.

Hazard: An inherent physical or chemical characteristic that has a potential for causing harm to people, property, or environment. In this document it is the combination of hazardous chemicals, radioactive/nuclear materials, an operating environment, and certain unplanned events that could result in an accident.

Hazard identification: The pinpointing of material, system, process, and plant characteristics that can produce undesirable consequences through the occurrence of accident.

Hazardous chemicals: Flammable, oxidizing, inflammable, explosive, toxic chemicals as well as substances affecting environment. The classes and list of hazardous chemicals are given in Attachment 1 to Federal Law “On Safety of Hazardous Industrial Facilities” of July 21, 1997, No 116-FZ.

Hazardous industrial facility: A facility or production enterprise, mentioned in Appendix 1 of the Federal Law "On industrial safety of hazardous industrial facilities" No. 116-Fz dated by 21.07.97. In this document it means facility or production enterprise where hazardous chemicals of actual accident risk are used, manufactured, reprocessed, stored or transported.

Human Factors: A discipline concerned with designing machines, operations, and work environments to match human capabilities, limitations and needs. Among human factor specialists, this general term includes any technical work (engineering, procedure writing, worker training, worker selection, etc.) related to the person in operator-machine systems.

Accident damage means money's worth damages (losses) in industrial and non-industrial areas, including environmental impacts caused by the accident at hazardous industrial facility.

Low-Probability Consequence Failure*:* means failure which can not be referred to any of three categories because of the consequences.

Nuclear materials: materials which contain or can generate fissile nuclear substances.

Facility Handling Radioactive/Nuclear Materials, Nuclear and radiation hazardous facility: – a facility or its part, or an installation, where radioactive/nuclear materials are used, manufactured, reprocessed, stored or transported.

Radioactive Materials, Radioactive Substances – other substances (not nuclear materials), emitting ionizing radiation.

Risk: A measure of economic loss, human injury, or environmental damage, in terms of both the incident likelihood and the magnitude of the loss, injury, or damage.

Risk Analysis: The systematic evaluation of the risk associated with potential accidents at complex facilities or operations.

Risk Assessment: A process by which the results of a risk analysis (i.e., risk estimates) are prepared for use in decisions, either through relative ranking of risk reduction strategies or through comparison with risk criteria.

Risk Management: The systematic application of management policies, procedures and practices to the tasks of analyzing, assessing, and controlling risk in order to protect employees, the general public, and the environment, as well as company assets, while avoiding business interruptions.Risk-Based Decisions. Choosing one alternative over another based on an estimate of relative risk.

2. Risk assessment implementation

Accident risk assessment at hazardous industrial facilities (hereinafter referred to "risk assessment") is an integral part of industrial safety management. Risk assessment means the systematic utilization of all available information to identify hazards and estimate the risks of probable unexpected or abnormal events.

The main goals of accident risk assessment at hazardous industrial facilities are to submit to decision-makers:

- real information on the status of HIF industrial safety;
- data related to the most hazardous (weak) points in terms of safety; and
- reasonable recommendations to reduce the risk.

In turn, decision makers can use the ISO 14001 process, or other management systems, to establish priorities based on relative risk and or effectiveness of management systems recommendations. To these ends management can establish a structure and programs to address these risk through the implementation of an environmental policy and programs, and define objectives and targets. A critical outcome of the risk assessment process is to facilitate planning, control, monitoring, identification and implementation of corrective actions. Of course, the audit and review of hazardous activities will be an essential component of a risk management plan or environmental management program to ensure that the environmental policy is complied with; and, that the environmental management system (EMS) remains appropriate to the risks identified and the program(s) to minimize those risks.

Risk assessment process includes the following major phases:

- work planning and organization;
- accident hazard identification (energy sources):
  - hazardous chemical, nuclear and radioactive materials inventories,
  - process characteristics (high temperature, pressure, concentration, etc.),
  - operating environment and
  - accidental hazards;
- hazard evaluation (preliminary risk assessment):
  - preliminary accident analyses,
  - preliminary consequence analyses;

- quantitative risk assessment;
- development of effective programs to control risk levels and, where appropriate, formulate recommendations to reduce the risk, and
- risk management plan development.

The essence and main requirements of each risk assessment phase are specified below.

2.1. Work planning and organization

At this phase it is necessary:

- to describe the hazardous industrial facility under consideration;
- to specify information sources; and
- to determine the purposes and goals of the risk assessments to be undertaken.

The individual responsible for facility operation, e.g. the director, usually determines general purposes and goals.

Accident risk assessment as well as hazard and operational readiness analysis are usually carried out at HIF by a special team of specially trained individuals. In the United States and in many European countries, both the requirement to use a team of trained individuals and the makeup of the team has been codified into the country's regulations. The group consists of experts, in addition to the director, and those individuals responsible for technical issues and involved in supporting activities. The group should not be too large. The optimal number is 5-7 technical experts. Duties of each participant should be precisely determined.

For example, to assess a small-scale typical chemical facility (i.e., HIF), the team would include one individual that has been trained as a leader, technical experts familiar with the technical limits of operation and one or two members of the operating staff. The team has to be diverse with individual backgrounds capable of identifying process upsets, the possible progression to an accidental release and the release consequences. The technical disciplines represented on the team will commonly include the following experts:

- mechanical engineer;
- chemical engineer;
- instrumentation and control engineer;
- environment and safety engineer;
- operator of the installation; and
- the director.

Participation of a team of experts on nuclear and radiation safety is required for nuclear and radiation hazardous facilities.

The team membership should remain constant for the duration of the assessment. However, in the case when problems arise in solving of some of the technical problems, the team leader may ask for assistance of the specialists that have the required experience and knowledge.

The team should posses sufficient competence to develop relevant technical recommendations. The range of risk reduction measures may include, but is not limited to: reductions in the amount of materials used; safe handling, operating and storage practices; alternative materials; the reliability of protective devices; equipment maintenance; personnel training programs; equipment upgrades (best available prevention technology); and management of external hazards (e.g., regulatory change, supplier management).

To ensure quality of risk assessments, it is necessary to use the knowledge of accident regularity and development at similar hazardous industrial or nuclear facilities. If the results of risk assessments conducted for similar hazardous industrial facility(ies) or technical devices employed at hazardous industrial facility are available, such results should be used as input information. However, it should be demonstrated that facilities and processes are similar and existing differences will not introduce significant changes to the assessment results.

Typically, for hazardous industrial facilities the of risk assessment are:

- to verify whether operational conditions meet industrial safety requirements reflected in the related regulatory documents;
- to clarify the information related to main hazards and risks;
- to identify risks not necessarily addressed in regulatory or guidance documents;

- to develop recommendations to organize the activity of the facility, enterprise and potentially higher administrative bodies; and
- to enhance operational and maintenance instructions related to the improvement of industrial safety management.

To reach these goals it is necessary to collect and analyze information related to the HIF or industrial enterprise under consideration in accordance with the work plan, in particular:

- main components of the industrial facility;
- information related to radioactive and/or nuclear materials or hazardous materials used at the facility;
- information on assignment of organizational responsibilities among personnel;
- information related to the organizations located nearby which may be affected;
- information related to villages (or population centers) located nearby which may be affected even in case of maximum hypothetical accident;
- principle flow chart;
- process information, including piping and instrument diagrams (P&Ids) and written operating procedures;
- layout of the main technological equipment with radioactive and/or nuclear materials hazardous materials;
- list of the main process equipment with radioactive and/or nuclear materials hazardous materials;
- description of controls, normal operational limits, action points, and alarm points; and
- information on hazardous chemicals distribution in the equipment.

Recommendations regarding the form of record-keeping / reporting of the above information are introduced in Attachment A.

To select and justify risk assessment methodology it is necessary to take into account purposes and goals of the analysis, complexity of the facilities under consideration, availability of the required information, and qualification of the experts involved in the assessment.

2.2. Accident Hazard identification

The main goals of the accident hazard identification phase are to detect and accurately describe all sources of hazards and to develop and understanding of the order of magnitude of their consequences.

In order to identify accident hazards it is necessary to determine all critical elements of the industrial systems, technical devices, technological units or processes which require serious assessment and those that are of less interest from a safety perspective.

When dealing with any industrial system, its personnel should be considered as one of critical links, and in many cases the "human factors" represents a rather important characteristic regarding general safety of a system. As an example, for chlorine use, in accordance with statistics, over 60% cases of violating safety of technological processes at industrial enterprises (of non-nuclear complex) are due to erroneous actions of the responsible personnel. Note that over 50% of such violations resulted from insufficient, incorrect or inadequate information of operator on actions to be undertaken. Therefore examination of opportunities of erroneous actions and causes are important parts of accident hazard identification. At this stage the equipment, regular training, technological procedures, instructions and directives and personnel qualifications must be considered in close interconnection.

Accident hazard identification results in:

- List of hazards present at the facility (see Attachment B1, List of Potential Hazards)
- List of unexpected or abnormal events (see Attachment B2, Accident Hazard Identification and Risk Assessment: emergencies in the context of ISO 14001).
- specification of risk-based decision criteria (consequence and frequency) and their relationship to the facility's accident hazards (environmental aspects) that will be used to assess accident risks (environmental impacts). (See section 2.4).
- description of the sources of hazards, risk factors, conditions for and development of unexpected events (e.g. probable accident scenarios); and
- preliminary accident and consequence analyses [1].

[1] For example, hazard indicators of the used chemicals, consequence analyses for specific accident scenarios etc. may be presented, if necessary, under hazard identification.

At the end of the accident hazard identification phase future areas of risk assessment activities are selected, often on the basis of the relative risk rankings of accident hazards having significant impact(s). The following may be considered as options for future actions:

- the decision to stop further assessment due to insignificant hazard or sufficient preliminary assessments; and
- decision to conduct more detailed hazard analysis and risk assessment;
- development of preliminary recommendations to reduce hazards.

To identify hazards and to further assess the risk it is necessary to gather, develop and document the information listed in Attachment A to this Report including recommendations with regard to reporting forms and format.

Classification of the facility as hazardous industrial facility is carried out in the process of identification considering identified features specified in Attachment 1 to Federal Law "On Safety of Hazardous Industrial Facilities" of July 21, 1997, No 116-FZ.

The results of identification are reported in the form of "Identification list for hazardous industrial facility" specified in Attachment A to this report (table A8).

2.3. Risk assessment

Main goals to be reached in the risk assessment phase are:

- to determine frequency, quantitative or qualitative, of initiation of all unexpected events;
- to assess consequences of unexpected event; and
- to summarize risk assessment results.

Generally, risk assessment methods can be classified as either qualitative or quantitative. There are practical uses for both types of risk assessments. Qualitative assessments are frequently used in initial scooping type assessments where the goal of the assessment is to investigate at all the processes and systematically consider the

interaction of all the hazardous materials and energy sources that could result in an undesirable consequence. Considering the risks with and without the engineered and administrative controls present demonstrates the adequacy of the controls and provides valuable information for reducing risks if the quantitative phase of the risk management assessment process, described in the following paragraphs, is not performed. Unless required by regulation, quantitative methods because they are more time consuming to evaluate, are typically performed only for facilities with inventories of hazardous, nuclear or radioactive materials that are above a specified regulatory threshold value. If the facility inventory is below the threshold or if a threshold has not been established, it might be decided to apply quantitative assessment methods on the most significant scenarios or bounding accident scenarios. The following sections will describe first the qualitative and the quantitative methods and give recommendations on their application.

A list of methodological materials recommended for risk assessment of accidents at hazardous industrial facilities is given in Attachment F.

2.3.1. Description of qualitative risk assessment methods

Qualitative Methods that will be considered in this sect are:

- Safety Review;
- Checklist Analysis;
- Relative Ranking;
- What-If Analysis;
- Failure Modes and Effects Analysis (FMEA);
- Hazard and Operability Study (HAZOP); and
- Human Reliability Analysis (HRA).

Safety Reviews are commonly walkthroughs by a team of experienced professionals, internal or external, to identify plant conditions or operating procedures that could lead to an accident and result in injuries, significant property damage, or environmental impacts. They have been used in the United States by the Department of Energy as a way of

evaluating the safety of facilities that perform similar operations with similar materials. The reviewers are aware of the state-of-the-art safety practices and look for their implementation in these facilities. Team members are selected based on their specific level of expertise, such as chemical safety or emergency response, and during the walkthrough of the facility and its operation, focus attention on their selected area of expertise.

Checklist Analyses are a form that asks the assessor to identify the presence of various safety items that are required to be present at the facility. These items might have been specified in hazards analysis documents or normative documents as being important to safety. They might be constructed from a list of safety items that would be expected to be present based on the types of hazards posed at the facility. Checklists are commonly included with technical assessments reports to management. Such checklists show that all the required elements specified by management and/or regulations have been included in the report.

As a result, the Checklist Analysis will contain a list of questions and answers on compliance of the facility to the safety requirements and safety assurance instructions. The checklist Analysis is different from the What-If due to a wider presentation of the initial information and the consequences of violation of safety requirements. These methods turn out to be the simplest (especially taking into account auxiliary and unified forms which facilitate analysis and presentation of results), cheap (the results may be obtained by a single individual within a day) and most effective in investigation of the safety of well-studied facilities with known technology or facilities with minor risk of a major accident [3].

Relative Ranking are a series of tables with blank boxes, some simply check boxes that are completed for the facility being assessed. One of the most commonly used tools that falls in this category is the DOW Chemical Exposure Index Guide [4] and the Fire and Explosion Index Guide, that some chemical companies use to assess their risk level. The user of the guides performs a series of calculations using equations and figures specified in the guides to obtain a Chemical Exposure Index (CEI) and a Fire and Explosion Index for the chemicals being used at the facility. For the chemical with the highest CEI, a Containment and Mitigation Checklist is filled out. This checklist contains a total of 21 items, including things like “all hoses inspected and tested

regularly" to "emergency procedures (related to this exposure potential) in place and annual drill held." If any of these 21 items is not present, it is reported as a finding in the management report. For the Fire and Explosion Index, a series of boxes are filled out that are used to estimate the F&EI value. This value is then multiplied by a loss control credit factor that takes into consideration the factors for safety features to obtain a radius of exposure. The processes where exposure radiuses include normally occupied areas would be the first candidate areas to receive additional improvements. The end products of the assessment are the completed forms attached to a report identifying recommended safety improvements. The recommended changes are referenced back to a weakness identified in the completed forms and checklists.

What-If Analysis, as the name implies, asks a series of questions. Each question becomes a line in the scenario analyses table. The columns in the table (see Table 1) contain the What-If question, the 'Consequence/Hazard,' 'Recommendation,' 'Responsible Individual' and a final column for the responsible individual to "Initial and Date' when the recommendation was addressed and resolved.

If an interdisciplinary team of experts uses this method, team members can address many of the questions. So therefore it is often useful to modify the column titles and add a column called "Safeguards" or "Controls," where the various preventative, protective and mitigating engineered controls (safety systems) and administrative controls can be listed (see Table 2).

Table 1.What-If Table Example

#	What If?	Consequence/ Hazard	Recommendation	Responsible Individuals	Initial and Date
1	Water was lost from the pool	Contamination of lower room below pool, possible damage to fuel from loss of cooling, and over exposure of personnel in fuel storage area	Investigate possibility of large pool water loss not being detected Investigate possibility fuel will be damaged from loss of water	Personnel familiar with alarms and cleanup system Fuel Behavior Expert	
2	Too much water added to pool	Smaller consequences than scenario 1	Bounded by Scenario 1, no fuel damage		

Table 2.Modified What If Table Example

#	What If?	Scenario Description	Safeguards	Consequences	Comments
1	Too much water was lost from the pool	Contamination of lower room below pool, possible damage to fuel from loss of cooling	Low Level Alarm on Pool Water Level and Periodic Surveillance of Lower Room	Release of radioactivity in excess of regulatory limits, and over exposure of personnel in fuel storage area	Action Item 1: Investigate possibility of fuel clad rupture if water level lowers to expose fuel in pool Action Item 2:…
2	Too much water added to pool	Contamination of lower room below pool	High water level alarm and periodic surveillance of lower room	Exposure of personnel in lower room below pool	Bounded by Scenario 1, no fuel damage

As a general rule, if the team does not have the information needed to evaluate the incident, it is valuable to include an action item. When the action items are met, the team would come back and fill in the missing assessment information. For many of the What If questions the risk assessment team will judge the 'Consequence/Hazard' level to be acceptable and no action is required. Including entries where no action is required, enables reviewers and facility management to more easily judge the comprehensiveness of the analysis. If such 'acceptable' questions are documented, it is also possible for later analysis teams to re-evaluate the operation and determine that nothing has changed to invalidate the initial conclusions regarding those acceptable scenarios.

Failure Modes and Effects Analysis (FMEA) is usually performed at a component or subcomponent level, commonly to look for weaknesses in the component's design.

Like the What-If Analysis the results are normally summarized in tabular form. The common columnar elements of the table are the 'Component', 'Description' of when used or relied upon, 'Failure Mode,' 'Effects,', 'Safeguards,' and 'Actions.' A typical goal of such an analysis is to look for single point failures, an element of the system, which if it fails, would prevent the component from fulfilling its safety function or warning the operator that it is not functioning properly. For example, if an alarm is being relied upon for safe operation, when any single component within the alarm fails, it should fail in a manner that warns the operator that it can not longer perform its safety function. In some circuitry, the sound of the alarm on component failure is different from the sound of the alarm triggered when a dangerous situation is present. The important design feature is to

insure that the operator is alerted when the alarm is malfunctioning. Since there are other components that might also prevent the operator from being alerted when the alarm circuitry is inoperable, the Failure Modes and Effects Analysis will not eliminate the need for periodic testing of the complete alarm system.

If it was concluded that there were several failures where the operator would not be warned of a malfunctioning alarm, the assessment team should generate an action item statement in the "action" column for that entry. In the interim, more frequent testing of the integrated alarm system might be proposed.

Failure Mode, Effects Analysis may be extended to form a quantitative Failure Mode, Effects, and Criticality Analysis (FMECA).

Hazard and Operability Analysis (HAZOP) evaluates the consequences on the system of deviations from design conditions. This procedure is designed to be performed by an interdisciplinary team whereas analysis methods that make extensive use of check lists can often be performed by a single analyst. HAZOP Analysis corresponds to the level of assessment demonstrated by FMEA in terms of complexity and quality.

The team of individuals divides the process up into a series of study nodes, specifies the design intent for that node and uses a series of key words to identify accident scenarios that may pose unacceptable levels of risk. The specific content of a combination of the keywords and technological parameters is individual for each process. The following is an example of creating deviations using guide words and process parameters (see table 3).

Table 3. Creating deviations by HAZOP

Guide Words		Parameter		Deviation
NO	+	FLOW	=	NO FLOW (No forward flow when there should be)
MORE	+	PRESSURE	=	HIGH PRESSURE (Pressure are more of than there should be)
AS WELL AS	+	ONE PHASE	=	TWO PHASE (More (two) phases present than should be)
OTHER THAN	+	OPERATION	=	MAINTENANCE (What may happen other than continuous operation, e.g.,

maintenance)

The goal of the HAZOP is to insure that no single failure will lead to a dangerous situation. One common example that frequently occurs in a chemical plant is the situation where two reactive chemicals are added to a process to produce the desired product chemical. If the reaction occurs in the reactor designed to control the production of the chemical adequate safeguards are usually present. However, if the failure of one component will result in the 'reverse' flow of one reactive chemical in the feed tank of the other, then the chemical reaction will occur in an area of the process where no safeguards are present. It is important to identify any study nodes where such single component failures could occur in the process.

The HAZOP procedure was designed to systematically analyze continuous processes where reactive and highly hazardous chemicals are handled. Thus the emphasis on 'no', 'less than,' 'too much,' and 'reverse' flow. It is easy to see how such process upsets involving reactions are highly exothermic can cause severe consequences. Similar upsets involving batch processing are also possible. In batch processing the key word 'skip' for skipping a step must be considered and 'reverse' takes on the added meaning of reversing the order of the batch processing steps. Since the definition of 'batch' processing can be extended to include any stepwise process any type of process can be assessed using the HAZOP technique.

The columns in a HAZOP table are quite similar to those in a What-If and Failure Modes and Effects Analysis table. For each study node, a table is developed that contains the design intent at the top of the table followed by a columnar table with the 'Item,' 'Guide Word' causing the deviation, 'Cause,' 'Consequences,' 'Safeguards,' and 'Actions.' Just as with the What-If analyses, the focus is on action items to improve safety. Similarly, it is considered extremely valuable to include scenarios where the consequences and/or safeguards are considered adequate. One way of minimizing these scenarios is to develop a cross-reference table where the deviation guide words, such as 'high' form one axis and the process variables associated with components such 'pressure' for a study node such as a 'storage tank,' or 'purification system' for the other axis. The deviation is only considered applicable for those components where a check mark has been entered in the cell forming the interaction between the two axes. For

example, the guideword ‘high’ would not be applied to the parameter ‘pressure’ for water pool since it is impossible to raise the pressure above atmospheric pressure. ‘High pressure” might be a meaningful deviation for a ‘purification system’ that contains a ‘pump.’ Such a matrix also serves as a check list to ensure that all the applicable deviations are considered for each study node. A study node typically contains a logical grouping of components, such as a pump, its controls, and the piping and valves associated with the pump.

Human Reliability Analysis (HRA) is a systematic identification and evaluation of the factors that influence performance of personnel during normal and emergency operation. These factors include: environmental conditions (e.g., if a person must perform the critical action while using a full face respirator, the error rate will be higher than if the same critical action were performed in an air conditioned control room), a person professional skill and knowledge, psychophysical capabilities, and the performance of information representation system and the process controls. The purpose of HRA is to identify potential human errors and their effects, or to identify the underlying causes of human errors. The analysis can be also used to develop the recommendations to reduce the likelihood of such errors. Human Reliability Analysis is usually performed in conjunction with other risk assessment techniques. For example, in a case when a branch point in an event tree is available wherein the success or failure depends on a trained person performing a critical sequence of actions. The person may fail to perform the first task but then detect the error and recover before performing the next critical task. At each critical step the probability of performing the step correctly is estimated. If there are multiple steps, then the probability of successfully completing critical sequence is the multiplication of the probability of successfully completing each step. For more details on this method the reader is referred to [5, pp. 183-192; 6, pp. 29-30; 7].

2.3.2. Description of quantitative risk assessment methods

Methods of quantitative risk assessment are characterized by calculation of the risk parameters and present a further development of qualitative methods. As a rule, quantitative assessment requires higher qualification of the experts and a greater amount of information on the facility, region of its location and the processes.

Quantitative Methods considered in this attachment are the following:

- Quantitative Scenario Analyses;
- Failure Mode, Effects, and Criticality Analysis
- Event Trees;
- Fault Trees;
- Cause-Consequence Analyses; and
- Simulation Models.

Quantitative Scenario Analyses. All the tabular qualitative analyses methods, What-If, HAZOP, and FMEA methods can be translated into quantitative analysis methods by adding columns that quantify the scenario frequency and scenario risk. The consequence and safeguards columns, if not estimated in a quantitative manner, must also be quantified. This is normally accomplished by simply adding a quantitative expression to what was developed for the qualitative assessment. The effectiveness of the engineered and administrative controls can be quantified by considering the accident likelihood and consequences and with and without the controls. The likelihood without the controls is estimated by removing the probability that the control is unavailable at the time the accident is initiated from the overall accident failure likelihood. The consequences might also be larger with out the control present.

When the safeguards column of a qualitative assessment method is quantified, the modification normally takes the form of a mathematical statement added under the descriptive statement that was developed when the qualitative risk assessment was performed. As an example, in the safeguards column of the qualitative assessment for a specific scenario, the assessment team might have listed an alarm and operator training as two safeguards that are being relied. To quantify that column, the fraction of the time the there might be a failure for the alarm to sound might be estimated by the risk assessment team to be *0.* Similarly, for the *0.*999 fraction that it does sound, the operator, because of the training program, might make the correct response *0,*99 fraction of the time. Thus the probability of an incorrect response, would be expressed mathematically as *0.001+0.999*(1-0.99) = 0.011*. The effectiveness of the training is converted to a failure

rate by subtracting the judged effectiveness of the training from *1*. This is an example of how the results of a human reliability analysis could be factored into the risk equation.

The frequency of the scenario, a new column in the table, would be developed by estimating the frequency of the initiating event and any other conditions that are required to cause the undesirable event. For example, if the undesirable event is a major fire that would release radioactive material in excess of release limits, the components that must be present would be, the radioactive material, excess combustible material and an ignition source. The risk assessment team would first estimate the frequency of having the radioactive material present. Conservatively this is often assumed to be one. Then they would estimate that probabilities that there would be too much combustible material present and that an ignition source when the radioactive material was present. For an operating facility, the probability that too much combustible material is present can often be obtained from operating records. Conservatively is often assumed that the ignition source is always present. If that is the case, that probability would be assigned a *1*. The effectiveness of the safeguards system, the fire suppression system, would be included in the safeguards column, not in the scenario frequency column. The probability that the fire suppression system is not available at the time of the fire can often be obtained from records of fire suppression tests performed at the facility being analyzed and facilities using similar fire suppression systems. This points out the value of National Failure Databases that can be used at any facility when performing risk assessments.

Failure Mode, Effects, and Criticality Analysis (FMECA). For this analyses each type of failure is ranked taking into account three main components of criticality – the probability (or frequency) of a failure, the possibility of identification of a defect prior to start of operation and the severity of failure consequences. The criticality parameter of a failure is a quantitative value, which takes into account the probability of a failure during the whole period of operation and the severity of possible consequences. The concept of criticality is close to the concept of risk and may be used in quantitative analysis of the risk of an accident.

The results of the analysis are presented as a list of equipment, probable failure modes and causes including frequency, consequences, criticality, failure detection devices (indicators, instrumentation and control etc.), and of recommendations to reduce hazard.

The quantitative values of criticality parameters may be used in setting the priorities of the corresponding correction actions.

Table 4 gives classification matrix of assessment of frequency and significance of failures (recommended by International Electrotechnical Commission (IEC) standard [8]) taking into account the severity of consequences. There are four groups to be analyzed which may be damaged by failure: personnel, population, property (equipment, structures, buildings, product items, etc.) and the environment

Table 4 uses the following criteria of failure classification taking into account consequence severity:

- catastrophic failure – results in human death, property significant damage, grievous damage to the environment;
- critical (non-critical) failure – a threat of life loss, critical facility damage, environmental impact present (absent); and
- with negligible consequences – does not correspond to any of the first three.

The matrix determines the following categories of failures:

A – quantitative risk assessment or specific safety measures to reduce the risk are required;

B – quantitative risk assessment or specific safety measures are expected;

C – - qualitative risk assessment or some safety measures are recommended; and

D – assessment and specific (additional) safety measures are not required.

Table 4. "Probability-consequence severity" matrix

Failure	Failure frequency per year	Failure consequence severity			
		Catastrophic	Critical	Non-critical	With negligible consequences
Frequent	> 1	A	A	A	C
Probable	$1\text{-}10^{-2}$	A	A	B	C
Possible	$10^{-2}\text{-}10^{-3}$	A	B	B	C
Seldom	$10^{-3}\text{-}10^{-4}$	A	B	C	D
Practically impossible	$<10^{-4}$	B	C	C	D

Criteria, given in table 4 are used for ranking of the hazards and determining the overall level of risk of an industrial facility. In this case rank A corresponds to the highest (unacceptable) level of risk of the facility, which requires immediate actions on safety assurance. Correspondingly, indexes B and C represent intermediate levels of risk, which require further analysis and detailed study of failure mechanisms. Rank D corresponds to the safest conditions, when there is no need for further study of failure causes.

This matrix may be successfully used at the stage of preliminary risk assessment for identification of the scenarios for detailed risk assessment.

FMEA and FMECA methods are used for analysis of projects of complex technical systems or in modification of hazardous facilities. The analysis is carried out by a team of experts (3-7 individuals) within several days or weeks, dependent on the complexity of the task. The method is described in more details in [5, pp. 113-139; 7].

Event Tree Analysis (ETA) allows to track the possible accident situations caused by personnel errors, external impacts, equipment failures or process interruption, which are chosen as initial [6, pp. 30-31; 7]. Event Trees are commonly used where there is a clear timeline for the accident progression. Event tree analysis is a "forward-looking" process, with the experts examining the chains of possible events (intermediate events) starting from the initial event and leading to the accident (the final event). The initial event and the following intermediate events actually describe the possible paths of incident evolution. An expert views the possible safety measures directed at elimination of the influence of the initial event at each stage. The success or failure of the safety measures is incorporated into the event tree and forms a branch point. One could place more than two branches at any of the branch points if there were intermediate states of failure. While the accident progression might consider several branches, for all but facilities with complex control systems, two or three branches are usually sufficient to model the failure of the engineered and administrative controls. While there are frequently several controls that could be included in the accident sequence, because common cause failures will frequently defeat several controls simultaneously, it is best to select two or three controls that are believed to be independent and credit them for safety. The probability of the initial event can normally estimated from the operating history of the facility or from the operation of similar facilities at other locations. The frequency of

a separate event or a scenario is estimated by multiplying of the frequency of the initial event by the conditional probability of accident evolution along this scenario.

A typical event tree is shown in Figure 3. In the example, the probability of detecting the loss of pool water is placed at 0.99 or 99%. The probability of the level detector not alarming is placed at 0.01 or 1%. Here, alarm failure means that the operator did not detect the emergency signal due to some reasons. The second branch determines the possible conditions of fuel element claddings and the corresponding probabilities under the condition that the loss of water took place. The probability of clad failure from over heating is placed at 0.01 or 1%.

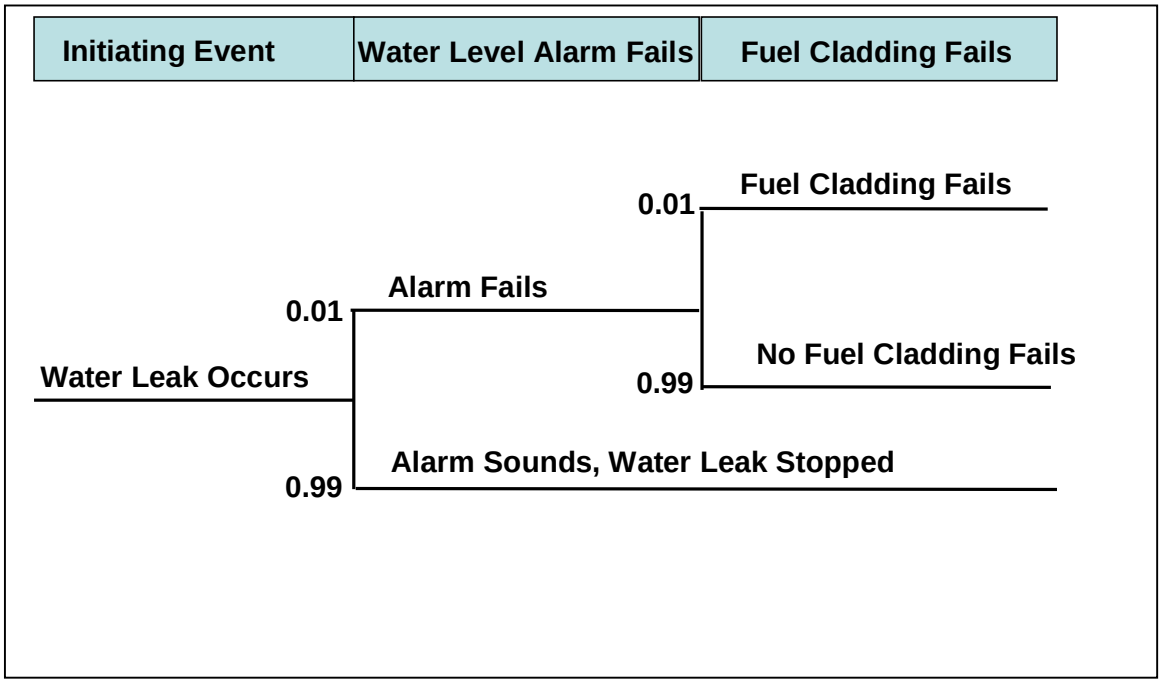

Figure 3. Event Tree for Loss of Spent Fuel Pool Water

Event trees are a way of summarizing success and failure paths on the same diagram. There are basically three event sequences shown on the diagram. Each begins with the water leak occurring. Assume the frequency of a water leak is once every ten years, or 0.1/year. Then one accident sequence is the water leak occurring, the alarm failing and the fuel clad failing. The alarm is a safeguards component. The frequency of that event sequence occurring is 0.1* 0.01*0.01 or 10^{-5}/year. The second event sequence is the water leak occurring, the alarm failing but no fuel clad failure. The likelihood of that event sequence is 0.1*0.01*0.99 or 9.9×10^{-4}/year. The success path is the leak occurs, the alarm sounds and the leak is stopped before significant loss of pool water occurs. The frequency of that event sequence is 0.1*0.99 or 9.9×10^{-2}/year. If the risk must be quantified, then based on the significance criteria being used to assess the risk, the

consequences associated with all three accident sequences would be estimated. In the case of the bottom branch, since the alarm system functioned as designed, in all likelihood there would be no consequences. The middle branch would have somewhat higher consequences because there would be exposures during cleanup and the top branch would have the highest consequences because there would be both releases to the water and potentially to the atmosphere. If a risk matrix, as described in Attachment C, is being used to model risk, it is then easy to place all three of the event sequences shown in figure 1 on the risk matrix. For complex systems it is not unusual to have event trees with hundreds of branches and it is not uncommon to use fault trees, described next, to estimate the branch probabilities. Irrespective of the number of branches, the results can always be described as a series of event sequences. In this way, the results are exactly like the Quantitative Accident Scenario table that was previously described. Event trees provide a way of displaying the logical structure of the scenario table, showing that there is a logical sequence to the accident sequences being evaluated.

Fault Tree Analysis (FTA) is used for identification and analysis of possible causes of accident situation initiation [9, pp. 28-29]. Fault Trees, like Event Trees are a logical way to display may accident sequences. To form fault tree for a Top event (accident, specific failure) the expert at first identifies the intermediate causes of the event of interest. Each of the intermediate causes is studied as an intermediate event and is similarly examined until all of the initial events (initial causes) will be found. These causes may include equipment failures, personnel errors, external impacts. The logic operations of "OR" and "AND" are used to combine the initial event so that they reliably lead to the Top event – the accident situation.

As an example figure 4 shows a possible event tree for the top event – fuel cladding failure from loss of pool water. The symbol labeled “1” is an “and” gate and the symbol labeled “2” is an “or” gate. Operation "AND" means that the event above happens in case of simultaneous occurrence of the events below (this corresponds to multiplication of the probabilities for assessment of the probability of the event above). Operation "OR" means that the above event may happen as a result of occurrence of either of the events below (i.e. the probabilities of these events are added up)

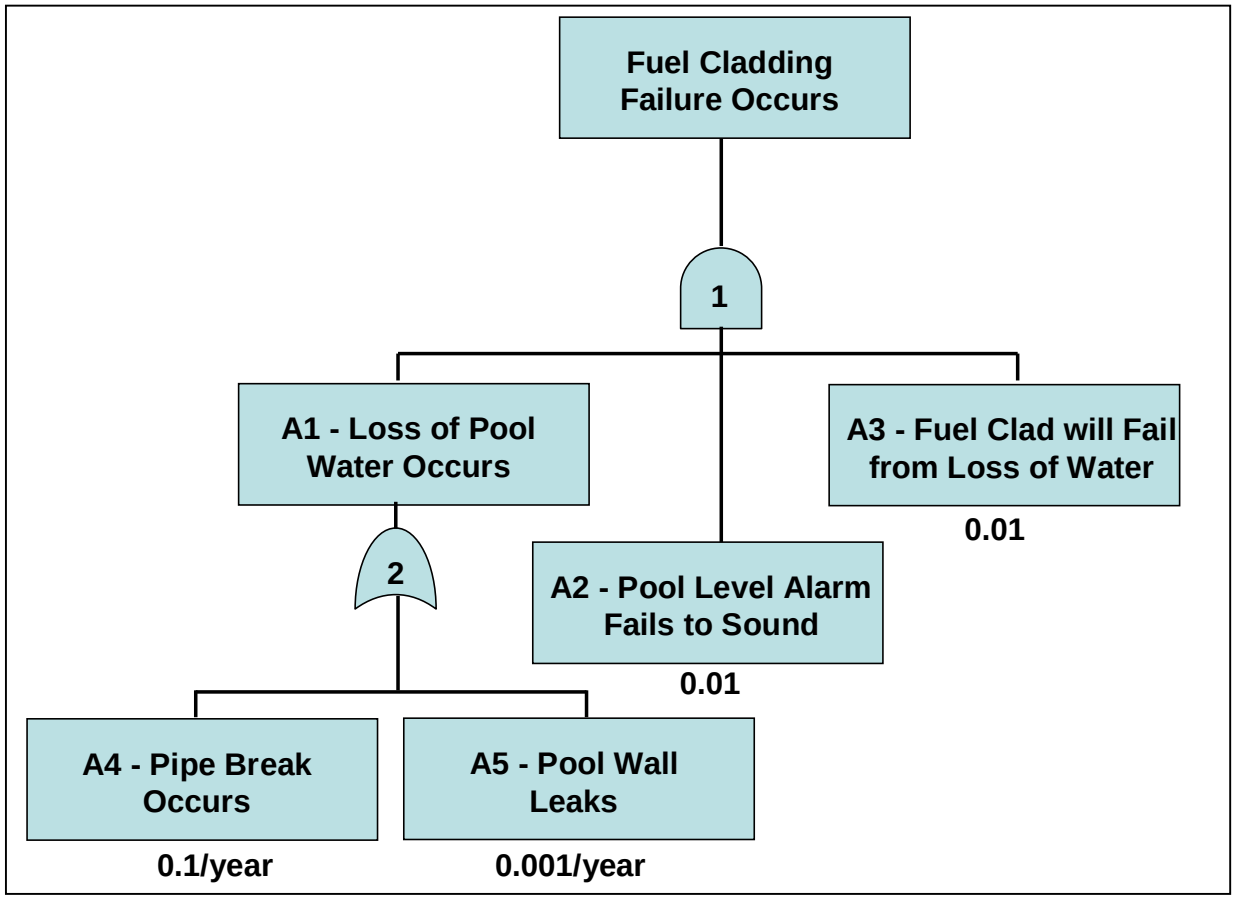

Figure 4. Fault Tree for Breach of Cladding Failure

The fault tree was drawn on an accident sequence that is similar to the event tree previously described to show the differences. It can be seen that whereas the event tree looked at several outcomes, the fault tree focuses on only one. The fault tree also has embedded event sequences that are called "cut sets." They represent all the logical event sequences that could lead to the top event. In the fault tree shown in Figure 4, there are two cut sets. One cut set is A4, A2 and A3 and the second is A5, A2 and A3. The frequency of the first is 10^{-5}/year and the frequency for the second is 10^{-7}/year. The first cut set was also shown in Figure 3. However, whereas the event tree considered other 'top events', the fault tree considered a second release path that was not considered in the event tree shown in Figure 3. While the second release path could have been shown in the event tree, nothing was lost by not considering that event sequence because it has a lower probability than the cut set that was initiated by the pipe failure. Clearly the consequences of a fuel clad failure would be the same whether on not the loss of water occurred from a pile break or a leak through the wall so the fault tree really is only being used to estimate the frequency of the top event.

It is certainly possible to develop this fault tree further. For example, A2, the pool water low level alarm failing to sound could be developed into additional branches. Similarly, since the pool is lined, for a leak through the wall to occur, the lining must be

defective and there must be a crack in the wall. The tree should be developed down to the level where failure data can be obtained. For example, if there is no way to detect the leak in the liner, then there is no advantage gained by developing A5 any further. Another example: if one of the leak paths had been a leaky valve, and there is good data on the frequency of valve leaks, they would probably have to be large leaks to threaten the fuel, then the fault tree should not be developed down to the failure of the components of the valve.

As was pointed out previously, since the fault tree offers a way of calculating the frequency of the top event, making the top event the failure probability of a branch in the event tree provides a means of quantifying an event tree branch probability that might not otherwise be easily quantified. Thus where there is the possibility of major environmental impacts should an accident occur and complex safety systems have been installed to reduce the frequency of these undesirable accidents, it is not uncommon to model the risk using event trees to identify the may release sequences and fault trees to estimate the branch probabilities for the most important branches.

Cause Consequence Diagrams are a specialized risk assessment tool that combines the inductive reasoning features of an event tree with the deductive reasoning features of a fault tree. Essentially the top event of the fault tree becomes the initiating event of the event tree. For more details on this method the reader is referred to [7].

Simulation Models are seldom used in risk assessments because they are very difficult to use. Basically, each parameter is considered as a random variable and the state of the system at any point is expressed as a probability distribution. In the example shown in Figure 3 and 4, the time the water leak occurred would be considered as a random variable, the size of the leak would be expressed as a probability distribution, the level of the pool would be a distribution and the likelihood someone would be present in the facility would be shown as a time distribution. Various outcomes as a result of possible operator actions could be considered and for each a probability would be assigned. The distributions could take on many forms, ranging from the common bell shaped normal or lognormal distributions to a uniform distribution between the two extremes. A Monte Carlo type code would then be used to simulate the leak for thousands of times. For each simulation, the time of each leak, its size, and the pool level, and all the probabilities would be selected using a random number generator.

Those that are expert in the use of simulation models would probably say that they can get the risk distribution for a specific facility operation quite quickly. The learning curve for mastering this technique is very long. Since the data requirements are significant, the results using this method are frequently more sensitive to the availability and quality of the input data. For a facility that has operated many years and has collected a lot of performance data over the operational period, like the variation in the depth of the pool water, the data requirements are probably not an issue.

2.3.3. Selection of Risk Assessment methods and recommendations on their application

To select risk assessment methods it is necessary to take into account: the type of hazardous industrial facility under consideration; nature of accident hazards; availability of the resources to conduct the assessment; experience and qualification of the consulting experts; availability of required information; objectives of the assessment; and any regulatory requirements that must be met by the assessment.

To select and apply risk assessment methods the following requirements should be met:

- method(s) should be scientifically and in some case legally (by regulation) justified and correspond to hazards under consideration;
- method(s) should demonstrate the results in the manner enabling better understanding of hazard and identify the ways to reduce the risk;
- method(s) should be tailored to the availability of information, for example, if the process piping and instrument diagrams are not available, meaningful HAZOPs can not be performed;
- method(s) should be iterative and auditable;
- method(s) should be tailored to meet the objectives of the risk assessment, and
- the assessment methods should be familiar to the team performing the assessment and the team should be trained in using the method.

Probably the most important criteria are the regulatory requirements. As an example, in both the Russian Federation and in the United States, for nuclear power reactors, the regulatory agency expects to see event trees to describe the failure sequences for postulated design basis accidents with fault trees used to estimate the branch probabilities for the event tree branches. Both the event tree and fault trees can be quite large, in some cases, over 100,000 possible combinations of failure sequences might be analyzed to estimate the probability for one branch of the event tree. In Europe, facilities containing large quantities of hazardous chemicals are required to conduct quantitative risk analyses to demonstrate the potential for fatalities in the vicinity of the facility following a potential accident is in an acceptable range.

The second most important criteria are activities or phases of operation. As shown in table 5, if the process is just being designed, the amount of detail regarding the equipment design and even the location where the facility might be constructed could be unknown. In such situations, qualitative methods such as checklists and the qualitative What-If Analyses are frequently all the data will support. During the design phase, the suite of methods that can be used expands significantly because the safety systems are beginning to be specified and it is appropriate to use more detailed methods. For chemical facilities, the HAZOP is ideally suited to be used to demonstrate that there is no scenario which has a single point failure, i.e. not protected by at least one engineered or administrative control. Just prior to start-up, and during operations, all the procedures have been written and the piping and instrumentation diagrams have been prepared so detailed, quantified risk assessment methods can be used. During operation, the availability of process performance data, including the performance of controls, makes it possible to use actual data to populate any of the more detailed risk assessment methods, such as event trees and fault trees. The availability of such detailed data also facilitates use of detailed methods when major plant upgrades, i.e. reconstruction, are being planned. The following symbols are used in table 5: 0 — the least appropriate method of analysis ; + — the recommended method; ++ — the most appropriate method.

Table 5. Recommendations to select risk assessment methods

Method	Activity or Phase of Operation				
	Location (pre-design work)	Design	Commissioning or decommissioning	Operation	Reconstruction
What-If Analysis	++	++	++	++	+
Checklist Analysis	++	++	+	++	+
Hazard and Operability analysis	0	++	0	++	++
Failure type and consequence analysis	0	+	0	+	++
"Event and failure trees" analysis	0	+	0	+	++
Quantitative risk assessment	0	0	0	+	++

Another criterion for selecting a risk assessment method is the availability of prior results. It is quite common to perform a less detailed screening type qualitative hazards assessment during Accident Hazard Identification. Qualitative methods such as What-If and HAZOPs could be used to develop several hundred postulated accident sequences and then as the accident sequences are being evaluated, the team might identify 10 or 20 potentially significant scenarios that are both representative and bounding of the hundreds of scenarios listed in the hazard screening. These 10 to 20 scenarios represent a set of scenarios that are ideally suited to be brought into one of the quantitative scenario analyses methods described in the section 2.3.2. The advantage of developing the quantitative risk assessment from a qualitative one is evident. There is a tremendous savings in effort that can be realized by building on what has been done previously. Since the 10 to 20 potentially significant scenarios have been selected as both representative and bounding, there is no need to quantify hundreds of scenarios. This enables the limited resources of the risk assessment team to devote their efforts to the scenarios that are believed to be truly important to understand and control. (See attachment B for additional details and discussion of determining significance.)

There are two additional criteria that need to be considered. One is the expertise of the risk assessment team and the last is auditability of the results. If there is no regulatory requirement to use a specific method and the team is familiar with What-If type analyses, then rather than trying to learn a new method, the best risk assessment will be realized by using with the What-If method. Regarding auditability, it is important that management be able to review the results and it is also important that the documented results be available to process personnel. All the methods described in this document meet the auditability criteria.

2.3.4. Scenario-Based Risk Assessment: Selecting a Suite or Combination of Risk Assessment Methods

It is assumed that as during the Accident Hazard Identification phase of the assessment, a scenario based qualitative method has been used to document a comprehensive set of accident scenarios. Such a set would have systematically identified and qualitatively evaluated a broad set of possible accidents. To develop this comprehensive list of accident scenarios, it is necessary to identify the energy sources that could initiate the release, the quantities of hazardous material present, and then to systematically consider all possible release mechanisms. The final step of the Accident Hazard Identification phase is do identify those accidents sequences that are representative of a class of accidents and also bound many other accident sequences. By identifying this set of representative accidents, it is frequently possible to demonstrate that as few as 10 to 20 accidents sequences bound several hundred-accident sequences that were documented during the Accident Hazard Identification phase.

In many cases this bounding is quite easy. Similar accident scenarios can occur in many parts of the operation, probably with equal likelihood. If the probability of the initiating event is equally likely anywhere in the facility, the bounding scenario would be in the area of the facility with the greatest inventory of hazardous material and therefore would pose the highest consequence. Since the frequency of the similar scenarios is judged to be the same, this scenario with the greatest release clearly bounds the others. Similarly, scenarios judged to be more frequent and having similar consequences are selected as bounding as well. A common reason for selecting a scenario as bounding

based on frequency is the number of operations performed. If in one area of the facility, an operation is performed a thousand times a year and an similar accident scenario can occur in another process area where only a hundred operations are performed a year, the more frequent operation will clearly have the higher risk. The point of the screening is to not be forced to quantify hundreds of scenarios that are not bounding accidents, accidents that pose the greatest risk because of the quantity released or the frequency of the release.

When qualitative accident sequences are the outcome from the Accident Hazard Identification phase, then it follows that the easiest way to quantify the 10 to 20 bounding scenarios is to one of the quantitative scenario analysis methods described in the section 2.3.2. As described in the description of the quantitative scenario analysis methods, in order to quantify the bounding scenarios that up to this point have only been qualitatively evaluated, it will be necessary to quantify the frequency of the scenario, the effectiveness of the controls and perhaps the magnitude of the consequences. There are many techniques that could be used for quantifying these terms. Some might utilize additional methods listed as quantitative analysis methods in section 2.3.2. For example, if the availability of a engineered or administrative control can not be estimated from operational data, then a fault tree might be developed to estimate the probability that the control might not be able to stop the progression of the accident sequence or mitigate its consequences. Similarly, if the recovery from a process upset is dependent entirely on the correct actions of the operations staff, then a HRA study might be performed to identify the probability that the critical operation might not be performed correctly. When there are several possible outcomes to a scenario, say a complete failure, a partial failure and no failure, then an event tree might be developed and quantified to model the multiple outcomes. Because of the many and varied circumstances that might arise, even when quantifying as few as 10 scenarios, the risk assessment team night use all the quantitative risk assessment methods listed in section 2.3.2. The choice of the best way to quantify the terms in the bounding scenarios ultimately resides with the risk assessment team leader.

2.4. Criteria for ranking the consequences of accidents and their frequencies

This section contains specification of risk-based decision criteria (consequence and frequency) and their relationship to the facility's accident hazards (environmental aspects) that will be used to assess accident risks (environmental impacts).

The previous section listed the various techniques that might be used to quantify accident scenario risks. The quantification of an accident scenario can be divided into four steps. The first and second steps are to quantify the accident sequence frequency and consequences based on the facility's accident hazards. The next two steps, described in this section, develop risk based decision criteria that are used to prioritize all the accident sequences being evaluated based on risk.

This section presents several tables showing several ways to rank the significance of both the frequency and consequences of accidents. Beginning first with consequences, Table 6 shows a consequence scale that has been used for a hazardous Industrial facility (Apatityvodokanal Utility working draft). Table 7 shows a similar table for a nuclear or radioactive material processing facility (NIIAR working draft). The scale shown in Table 6 is the International Nuclear Event Scale (INES), developed by the IAEA [11, p.8]. Both table 6 and table 7 have two common consequence ranking characteristics. First of all there are multiple consequence measures on the same table. In the case of the HIF table, the general public and workers are both placed on the same scale. In the case of the INES scale, the consequences are measured for impacts beyond, the site, impacts on the site and loss of levels of protection. It is not uncommon to see four or five different environmental impacts placed in the same consequence table. The additional impact scales are accommodated by adding additional columns to the table. If a particular accident scenario is determined to be a 5 for one consequence measure and a 3 for the other, when filling out the consequence part of the scenario table, what is usually done is to list both and then take the highest number as the consequence level for the scenario being evaluated. The second common characteristic is that an accident can frequently be placed on the scale without a lot of detailed analysis. The risk assessment team can frequently agree to a consequence level without using an atmospheric dispersion code to estimate the consequences.

Table 6. Categories of accident consequence severity for HIF

Categories of impact to health under analysis of process hazard				
On site		Reasonably anticipated impact to health	Off site	
Category	Qualitative description		Category	Qualitative description
6+	Extremely high	Numerous fatalities or numerous evidences of chronic diseases	7+	Catastrophic
5	Very high	Fatalities or evidences of chronic diseases	6	Extremely high
4	High	Immediate decline in health or chronic diseases	5	Very high
3	Medium	Injured with long period of disability or serious impact to health, hospitalization is required	4	High
2	Low	Medical treatment	3	Medium
1	Very low	Negligible impact to health	2	Low

Table 7. General Structure of the INES Scale

	Field of impact		
	Impact beyond the site	**Impact on the site**	**Worsening of the echeloned protection**
7 Major Accident	**Major Release: Wide spread health and environmental effects**		
6 Serious Accident	**Significant Release: Likely to require full implementation of planned countermeasures**		
5 Accident with Off-Site Risk	**Limited Release: Likely to require partial implementation of planned countermeasures**	**Severe Damage to Reactor Core/Radiological Barriers**	

4 **Accident without Significant Off-Site Risk**	**Minor Release:** **Public exposure of the order of prescribed limits**	**Significant Damage to Reactor Core/Radiological Barriers;** **Fatal Exposure of a Worker**	
3 **Serious Incident**	**Very Small Release:** **Public exposure at a fraction of prescribed limits**	**Severe Spread of Contamination/** **Acute Health Effect to a Worker**	**Near Accident:** **No safety layers remaining**
2 **Incident**		**Significant Spread of Contamination/** **Overexposure of a Worker**	**Incidents with Significant Failures in Safety Provisions**
1 **Anomaly**			**Anomaly Beyond the Authorized Operation Regime**
0 **Deviation**	**No Safety Significance**		

As commonly used, the consequence scales shown in tables 6 and 7 are used with all the engineered and administrative controls in place and correctly functioning. As will b be described in the next section on sensitivity and uncertainty analysis, some regulatory bodies require that the consequences be estimated both with and without the controls in place so that the importance of the controls being relied upon for safety can be evaluated. Where the unmitigated consequences are extremely high, the engineered systems, structures and their components being relied upon must be constructed to the highest quality control standards, be subjected to tests that document they can perform their control function when subjected to the accident environment, and their testing and maintenance is controlled with formal programs. Redundant systems must frequently be installed to assure the required level of performance.

If the frequency and consequence levels are now quantified for the What-If scenarios described in section 2.3.1, the What-If table must be modified to include a Frequency column as shown in table 8 below. Since it is normally impossible to demonstrate that one scenario is bounding, several scenarios with differing consequences and likelihood's

and relying on different controls are often selected from the accident sequences identified in the hazard evaluation (preliminary risk assessment) phase.

Table 8. Modified What-If Table Example with Safeguards, Consequences and Frequency Quantified

#	What If?	Scenario Description	Safeguards	Consequences	Frequency	Comments
1	Too much water was lost from the pool	Contamination of lower room below pool, possible damage to fuel from loss of cooling	Low Level Alarm on Pool Water Level and Periodic Surveillance of Lower Room Probability of safeguards component failure, 0.001 for alarm and (1-0.999)*0.01 that operator will incorrectly respond to alarm resulting in probability of surveillance failure of 0.011	Release of radioactivity in excess of regulatory limits, over exposure of personnel in fuel storage area Based on table 7 the consequences would be assigned to severity level 3	Probability of large break 0.001/year; times probability of a failure of the surveillance system of 0.01 results in a frequency for this scenario of 10^{-5}/year.	Documented resolution of Action Item: 1 concludes no fuel cladding rupture will occur

While the consequence ranking scales in Tables 6 and 7 have been used in the two examples developed using this methodology, it must be pointed out that a search of the literature will uncover many additional consequence scales. Table 9 presents a simpler scale that could be used as well. If the scale is not dictated by the regulator, the choice of which scale to use is ultimately the responsibility of the facility manager. The manager will frequently ask to risk assessment team to formulate a recommendation for approval by the manager.

Table 9. Definition of Public Safety Consequences [14].

Category	Description
1	No injury of health effects
2	Minor injury or minor health effects
3	Injury or moderate health effects
4	Death or severe health effects

While consequence scales can have several consequence scales in the same table, frequency scales are always one dimensional. The real distinction is whether on not the frequency is numerically quantified or just expressed in words. Tables 10 and 11 show two different types of frequency scales in common use.

Table 10. Frequency Category Definitions

Category	Description
1	Not expected to occur during the facility lifetime
2	Expected to occur no more than once during the facility lifetime
3	Expected to occur several times during the facility lifetime
4	Expected to occur more than once a year

For facilities with large inventories of hazardous materials, placing all the accidents that are not expected to occur in the facility lifetime in one category is most likely too gross a division. For such facilities, table 10 would not be recommended. If table 11 were used, the frequency of all the accidents would have to be estimated to with two decades, i.e. between 10^{-2} and 10^{-4}/year. While this is often suitable for facilities with significant inventories of hazardous materials but few large energy sources to cause the release of the materials, i.e. a nuclear fuel handling facility, for nuclear reactors, a one decade scale is expected by the regulators.

Table 11. Example: Failure Frequency per year

Failure	Failure frequency per year
Frequent	> 1
Probable	$1\text{-}10^{-2}$
Possible	$10^{-2}\text{-}10^{-4}$
Seldom	$10^{-4}\text{-}10^{-6}$
Practically impossible	$<10^{-6}$

As was the case with the consequence scale recommendation, if regulatory bodies do not specify the frequency scale that must be used, the selection of a scale is ultimately the

responsibility of the facility manger. Once again, the manager will often rely on the risk assessment team to formulate a recommendation.

In formulating the recommendation, cost factors should be considered. For a facility that has been operating for many years or for an new facility that has a design that is similar to a facility that has been operating for many years, the risk assessment team can often agree that a specific accident scenario probably falls in the "seldom" frequency category without analysis. However some degree of analysis is required to demonstrate that the accident scenario frequency is between 10^{-4} and 10^{-5}/year. If the team judges that the frequency is close to the one of the break points in the scale, the conservative frequency is often chosen.

As stated previously, it is often possible for the risk assessment team to place each of the accident scenarios being quantified on one of the consequence scales without performing any detailed consequence analyses. If this is the case, the cost of evaluating the scenarios is reasonable. However, in cases where the regulatory agency requires a detailed consequence analysis to be performed to estimate the bounding scenarios, then the amount of effort expended to estimate consequences for each accident scenario can be quite large. Since required by regulation, there is no alternative but to invest the effort in performing the detailed consequence assessments, even at the accident hazard evaluation stage.

2.5. Development of Risk Matrix for the Prioritization of Risks

As was stated in the introduction of section 2.4, the quantification of facility risk can be broken down into 4 steps. The first two steps, consequence and frequency estimation have been discussed in section 2.4. This section will focus on the techniques to estimate risk and then use the resulting risk levels to prioritize which accident scenarios control the facilities risk level. Once the controlling accident scenarios have been determined, it is possible to identify risk reduction strategies that will reduce the facility's risk in a cost-effective manner. This last step is not part of this risk assessment document.

As a result of several major industrial accidents, Chernobyl and Bhopal being among the most severe, almost every major industrial country has sought out ways to identify and better manage the risks associated with operating major industrial facilities. While the impetus was the result of major accidents, the recommendation to perform the risk

assessment more formally gained strong support from accident investigation teams who found that the accident scenarios that resulted in the very severe consequences were frequently known, they were just dismissed because of inadequate analysis. In the European Union, some of these requirements have been formulated into Regulations and are binding on all member countries [12].

As a result of these post accident investigations, it has become generally recognized that ensuring the protection of the environment is a responsibility that must be shared by workers, facility managers, and the regulators. Additionally, a documented risk management program has become a common way to assign responsibilities for carrying out critical elements of the program and also monitoring that these elements that assure protection of the environment are implemented and are effective. The risk matrix, with consequence levels on one side and frequency on the other has become a common way to identify those accidents that pose the greatest risk and thereby enable facility managers to make informed decisions regarding the need to reduce the risk levels associated with these accidents. Once the need to reduce the risk level has been identified, equipment and programs that lower the risk either by reducing the consequences or the frequency of the accident can be evaluated using the same risk matrix.

It is important to point out that there are alternatives to the use of a risk matrix. In 1996, the European Community passed Council Directive 96/82 EC (Saveso 2) [13], which requires that all facilities with quantities of hazardous chemicals above a specified amount meet a specific set of requirements. The most significant requirements are to have: 1) a documented safety analysis, 2) an accident prevention program and 3) an emergency response plan. The Saveso 2 directive specifically excludes nuclear and radiological facilities. However these are covered under similar directives, such as the EURATOM directive 97/43/Euratom dated 30 June 1997.

While Saveso 2 provides a framework for protecting the population in the vicinity of a facility, the implementation of the directive can be different in each of the member countries. Neither the German nor the French implementation of the directive uses a risk matrix. The German regulations focus on safety features. High hazard facilities are required to install state-of-the-art safety features whereas lower hazard facilities are permitted to have commonly available safety features. France regulates all the hazardous processing facilities based on maximum credible accidents. In both these countries, since

the frequency associated with any postulated accident is not estimated, there is no requirement to quantify the risk (frequency times consequence) for any accident scenarios. All the other countries ensure safety by managing the risk associated with a suite of credible accident scenarios. Risk matrices or the continuum of the risk matrix, a risk curve, play an essential role in all these risk management programs.

The following discussion and describes: the structure of the risk matrix, the role for risk matrices, show some example risk matrices, provide some guidelines for constructing risk matrixes and then lastly use the guidelines to select an example risk matrix. This process shown should not be considered unique, just reasonable. Ultimately the facility manager, in conjunction with guidance and requirements provided by regulatory agencies, must specify a matrix that fulfills the goals and objectives of their environmental management program.

Risk Matrix Structure

A risk matrix is two dimensional and is comprised of two parts: consequence displayed on the y axis and frequency of occurrence (failure frequency on the x axis). If the risk for the scenarios must be quantified, then the units on the two axes have to be numerical. Using logarithmic scales often enables all the selected accidents from the most frequent to the most severe to be placed on one figure, as shown in figure 5.

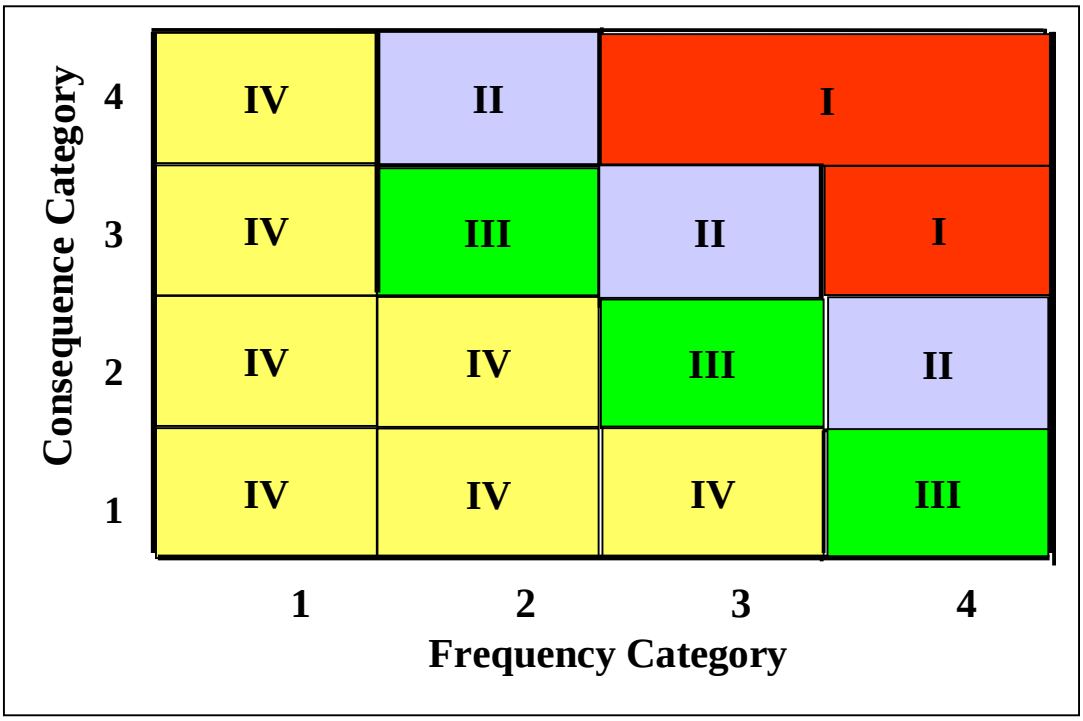

Figure 5. Example of a Qualitative Risk Matrix

As the risk assessment team goes through the bounding accident scenarios, what is often done is to use the number for the accident scenario and place it in the proper cell in the risk matrix. It is then possible to perform the final step in the assessment process. Identify any accident scenarios that fall in the *I* and *II* regions of the risk matrix. The definition of the risk categories is for this figure is shown in table 12.

Table 12. Definition of Risk Categories

Number	Category	Description
I	Unacceptable	Should be mitigated with engineering and/or administrative controls to the risk ranking of III within a short time period
II	Undesirable	Should be mitigated with engineering and/or administrative controls to a risk ranking of III within a year
III	Acceptable with Controls	Should verify that procedures or controls are in place
IV	Acceptable as is	No safety improvements needed

Role of Risk Matrices

When performing risk analysis, the team of individuals making the assessment will frequently identify scenarios of concern and recommend upgrades in the safety systems. When the report is written to the management recommending the upgrades, if there is no prioritization of the upgrades, the management has a difficult time determining which upgrades to make and how quickly they should be made. Is the concern something that needs to be addressed in a few months, in the next year, or when there is money to make the upgrade? Is there one upgrade that will resolve several safety concerns? By placing each of the bounding accident scenarios in a cell in the risk matrix, it is possible to begin the process of prioritizing which accident is of the greatest safety concern and needs to be addressed first. Similarly, those scenarios of lower risk can safely be put off and addressed after the most serious concerns have been addressed.

In most textbooks on risk management, the authors will emphasize that the facility's management should concur with the proposed risk matrix. In some countries, such as Netherlands [14] and the United Kingdom, the risk matrix is specified by the regulator. Some facilities, as a result of performing prior risk assessments, may have developed a risk matrix. In both these cases, the role of the risk matrix has already been specified and when it is presented to management as part during the planning stage for the assessment, it is being presented just to for information. There is no decision to be made. If on the

other hand the facility does not have a risk matrix, what is normally done is for the team leader of the risk assessment to develop a proposed risk matrix and present it to the facility's management at the meeting where permission to carry out the risk assessment is being sought. Thus the planned risk matrix is just one of the agenda items the risk assessment leader presents to management in the meeting where the schedule, scope, and staffing requirements for conducting the risk assessment is also discussed with the facility's management. Following the meeting, the risk assessment team should have the approval of the management regarding the scope of the assessment, the permission to use facility personnel, and the acceptance of the risk matrix as the prioritizing tool.

General guidelines for constructing of risk matrices

As the use of risk matrices becomes more common, some common guidelines can be offered when one is needed.

Ideally the risk matrix should reflect the decisions that have been made in the past regarding safety improvements. For example, if a serious accident occurred in the past, how severe was it and what actions were taken to improve safety?

Have the regulatory authorities established a set of criteria that must be met by the risk matrix. For example, in some countries, the frequency of a serious core disruptive accident in a nuclear power reactor should be less than 10^{-4} per year. This requirement becomes a point on any risk matrix being developed.

One must start with the definitions of the consequence and frequency terms in tables 9 through 12 are examples of such tables that are used in conjunction with figure 5. Should the definitions be qualitative or quantitative?

This will depend somewhat on the regulatory environment. If there is a country requirement that the risk be quantified, then the consequence and frequency definition must be quantitative. If the safety analysis for a facility already breaks accidents into a series of accident classes, then these should be used.

It is important to build on what is already available. For example, in the United States, the documented safety analyses for non-reactor facilities that process nuclear and radioactive materials quantify the likelihood of each of the documented accident scenarios to within two orders of magnitude. In other words, the analysis will state that the frequency of a scenario is unlikely and the unlikely is defined as having a frequency of occurrence between 10^{-2} and 10^{-4} per year. Unless something will be gained from

quantifying the frequency more accurately, two decade frequency bins should be used in the risk matrix.

Unless there already a breakout of severities, there is normally nothing gained by using more than 4 risk severity, consequence, or frequency levels. Frequently three, high, moderate, and low will suffice.

It is important to get management approval for any risk matrix before starting the assessment. They are the decision makers that must allocated the money when the risk assessment team comes back with many action items, some of which are to be fixed within a few months. If the normal process of responding to safety concerns is to identify a plan of action to improve the safety within three months instead of having the improvement completed in three months, then this should be reflected in the action statements that are associated with the risk levels.

In summary, the development of the risk matrix should reflect the decision making process that management is willing to commit to implementing and should build on what already exists and has been implemented at the facility.

An example of a risk matrix for hazardous industrial facilities and the corresponding recommendations are given in Attachment C (Risk matrix for hazardous industrial facilities). This matrix can be used to define the priority of the risks at chemically-hazardous facilities.

See Attachment D, (Construction of a risk matrix for nuclear and handling radioactive-dangerous facilities), for detailed recommendations and guidance on developing a risk matrix for facilities handling radioactive or nuclear materials.

Summary

In the section 2.3. - 2.4. have presented a systematic process of quantitatively estimating the risk associated with operating hazardous facilities. Experience has shown that it is a logical process that can be performed with reasonable effort. The end result is an increased understanding of the facility's risk and more importantly, by identifying and evaluating the bounding scenarios, it is possible to identify risk management strategies to monitor the current operations and over time continuously lower the risk level associated with operating the facility.

2.6. Data Uncertainty Analysis and Sensitivity Analysis

It is advisable to perform a sensitivity analysis and data uncertainty analysis for substantiation of the reliability of quantitative assessment of the scenarios. There are three types of uncertainty that are typically evaluated, data uncertainty, model uncertainty and general quality uncertainty. Each will be described in this section.

Data Uncertainty Analysis

When quantitatively modeling accident scenarios using point values for parameters as opposed to distributed values, and the risks associated with the operation are significant, it is important to determine if using other values for parameters, such as failure rate data, would significantly change the risk level for the accident scenario being evaluated. The uncertainty analysis typically considers other sources of data, perhaps another facility used a higher or lower value for a failure rate. Would use of that facility's value, affect the level of risk at the facility being analyzed? These uncertainty discussions are normally documented as the data is being presented. An uncertainty analysis need not be performed for each parameter value used. The risk assessment team can use their expert judgment to identify those parameters values that might be highly uncertain and warrant some discussion. If the analysis is thought to be robust because there are good values for all the parameters, it is just appropriate to state that conclusion in the data section of the report.

Model Uncertainty

Model uncertainty looks at the basic assumptions underling the analysis and seeks to determine if changes in the assumptions would change the risk ranking assigned to any accident scenario. This is one of the reasons why it is important to explicitly list all the underlying model assumptions. From such a list it is possible to systematically consider each assumption and possible alternative assumptions that are reasonable and could have been used. For example, if it were assumed that the concentration of radionuclides in a spill was dependent on the amount spilled, then an uncertainty analysis might assume that the concentration was the same for all spills. If the analysis model assumed a single ended pipe break, the sensitivity analysis might consider a double ended break. If the effect of such changes results in no change in the risk ranking for any scenario, then it

will have been demonstrated that the uncertainty in the modeling is not likely to affect the risk levels assigned to the accident scenarios.

General Quality Uncertainty

There is no systematic analysis method that can be used to estimate general quality uncertainties. These uncertainties address the concern that the bounding scenarios selected for quantitative analysis might not be bounding if a larger number of scenarios had been quantified. The best way to address general quality uncertainties is to provide a well documented and structured approach to performing the risk assessment. Such an approach begins with the identification of hazards, systematically identifies a broad spectrum of accidents in the preliminary risk assessment process, selects a set of bounding accidents that are shown to be pose the highest consequence within the frequency range assigned to the accident, and ends with the quantification of the risk of bounding accidents. Accident initiators arising from external events, engineered system failures and human errors should all be considered. If all the accidents being quantified fall into one frequency range or all the consequences are assigned to one consequence level, then there would be concern that the general quality uncertainty would be too high. Similarly if all the quantified scenarios are for one process step, unless it could be clearly shown that process step is clearly bounding, there would be concern that the general quality uncertainty would be too high. However if the steps outlined in this document are followed, then the scenario selection and quantification process will be well structured and the general quality uncertainties will have been addressed. The following statement might be used to address concerns about general quality uncertainties.

> "This analysis has considered three types of initiating events: 1) those initiated by personnel errors, 2) those resulting from mechanical failures and 3) those induced by external events, including natural phenomena. All initiating events fall into one of these three types of initiating events. Furthermore, the report looked at the history of incidents that have occurred at the facility since operations started to ensure that the most common initiators were considered. The accidents selected for quantification include all three types of initiators, incorporate accidents that have occurred during operations and cover a range of consequences and frequencies. Thus general quality uncertainties are considered to be small."

Sensitivity Analysis

Sensitivity and uncertainty analyses are closely coupled. The uncertainty analysis, recognizing that the actual risk associated with facility operation can never be fully known, looks at the data, model and quality of the analysis and determines that the models being used to quantify the risks represent a close approximation to the actual risks associated with facility operation. Once the models have been shown to be a reasonable reflection of the actual facility risk profile, then the goal of the sensitivity analysis is to study the importance of the parameters that comprise the elements of the risk model. The sensitivity S_j to parameter j is defined as the change in the risk per unit change in that parameter:

$$S_j = \Delta R_j / \Delta P_j$$

Where ΔR_j is the change in risk and ΔP_j is the change in the parameter j.

The parameter being analyzed can be a probability or a change in the behavior of a component. That component need not be a engineered system used to ensure safety although the probability that a safety related component will perform its function is frequently the focus of the sensitivity analysis. There are two basic types of sensitivity analysis used: analyses of the initial data and the model.

Risk Level Sensitivity to the Changes in the Initial Data

Analysis of *the sensitivity of the initial data* studies the influence of changes in initial data (for example, frequency of initial situations, components of failure intensities, probabilities of operator errors etc) on probabilistic safety parameters [5, стр. 72-74]. We took a scenario of an accident connected with fuel element storage pool as an example. A leak from the storage pool occurs due to the personnel error (not closing of the valve).

The following consequences are expected (see table 13):

- in the extreme case 60 m^3 of water will leak from the storage pool;
- The personnel will receive the dose that is lower than the allowable one during deactivation operations.

The following of the protection systems may fail (see table 13):

- systems of water level monitoring;

- systems of dose rate monitoring;
- insufficient monitoring of the rooms by personnel.

Let us now consider the probabilistic safety parameters (the values are given in table 13):

P_1 - probability of the initial event;

P_2 - probability of the protection system failure

$P = P_1 * P_2$ — probability of refusal of all system;

$P_S = 1 - P_1 \cdot P_2$ — probability of faultless functioning of the system.

If the value of P_S does not satisfy the operator from the point of view of safety, then either the probability of the initial event P_{1N} or the probability of protection system P_{2N} failure may be lowered. The new value of the probability of faultless operation is calculated to find out lowering of which of the probabilities will give the best effect. If we lower P_{1N} — $P_{S1} = 1 - P_{1N} \cdot P_2$; and if we lower P_{2N} — $P_{S2} = 1 - P_1 \cdot P_{2N}$. If $P_{S1} > P_{S2}$, then it is advisable to invest in lowering the probability of the initial event. If $P_{S2} > P_{S1}$, then lowering the probability of the protection system failure will be a better investment. If $P_{S1} = P_{S2}$ lowering both parameters is equal.

Table 13. Analysis of initial data sensitivity.

Item	Accident sequence (accident scenario)	What can fail?	Probability (frequency), $year^{-1}$	Lowering the probability value	New P_c value
1	***Not closing of the valve***. 60 m^3 leaked from the SP. Minor exposure of the personnel during deactivation works	Systems of water level monitoring, dose rate monitoring, room inspection	$P_1 = 0.02$. $P_2 = 0.2$ $P = 0.004$ $P_S = 0.996$	$P_{1N} = 0.01$ $P_{2N} = 0.19$	$P_{S1} = 0{,}998$ $P_{S2} = 0{,}9962$ $P_{S1} > P_{S2}$

In the current case the analysis demonstrates that lowering the probability of the initial event will be the best investment.

Sensitivity analyses of model always look at the assumptions and it is intended to demonstrate that the risk level assigned to the facility is robust. To make it one needs to answer on the following questions:

1. Is there any likelihood that the number of operations will be higher next year?
2. Would this change the facility's risk level?
3. Might the consequences of the accident be higher next year?
4. If the facility being analyzed were a spent fuel examining facility, is it possible that over the next few years that testing might begin on a new type fuel?
5. Would the risk level change significantly if these changes occurred?

Having received answers to all above-stated questions, we should be sure, that possible changes in the operations at the facility or the way the accidents are being modeled will not significantly change the facility's risk level. If a sensitivity analysis is performed, it is normally reported immediately after the section showing the initial presentation of the risk assessment results but before the findings and recommendations section.

Use of Sensitivity Analysis to Determine the Importance of Components

The previous section compared the change in risk level when a 1% decrease is made in two of the failure probability values. This can be extended to look at the importance of components The approach that will be taken is based on the method that has been used in presentations to the United States Nuclear Regulatory Commission. What is done is the estimate the overall risk level and then look at changes in the risk level as each component is assumed to be in the failed state at all times and then assumed to always be available to perform its function. The assumption that the component is always failed is equivalent to operating the facility with the component not present. Similarly, if the component always performs its function, that represents the lowest risk that can ever be achieved if the current performance of the component is made perfect. While such a state can never be attained, frequent inspections and maintenance can frequently make the component availability nearly perfect. To show an example of how the component sensitivity is determined, consider the event tree shown in Figure 6. In this figure there are two components being relied upon to control the level of risk. One is an administrative control, the presence of staff at the facility and one is an engineered control, the remote alarm system. The initiating event is the frequency of a cooling system rupture of 0,02/year, or one in 50 years. The cause of the failure could be as a result of a personal error, a mechanical failure or an external event. The probability of the facility being attended and therefore detecting the leak promptly is 0.62. Similarly,

Initiating Event	Cause of Failure	Facility Attended	Remote Alarm	Path	Probability	Outcome	Scenario Risk
			Not annunciated				
		Not detected	1.00E-02	1	2.48E-05	1 Sv	3E-08 Sv/yr
		6.20E-01	Alarm given				
	Personal Error		9.90E-01	2	2.46E-03	1 mSv	3E-06 Sv/yr
	2.00E-01	Detected					
		3.80E-01		3	1.52E-03	1 mSv	2E-06 Sv/yr
			Not annunciated				
		Not Detected	1.00E-02	4	9.92E-05	1 Sv	1E-04 Sv/yr
		6.20E-01	Alarm given				
Cooling system rupture	Mechanical Failure		9.90E-01	5	9.82E-03	1 mSv	1E-05 Sv/yr
2.00E-02	8.00E-01	Detected					
		3.80E-01		6	6.08E-03	1 mSv	6E-06 Sv/yr
			Not annunciated				
		Not Detected	5.00E-01	7	6.20E-07	10 Sv	6E-06 Sv/yr
		6.20E-01	Alarm given				
	External Event		5.00E-01	8	6.20E-07	1 mSv	6E-10 Sv/yr
	1.00E-04	Detected					
		3.80E-01		9	7.60E-07	1 mSv	8E-10 Sv/yr

Figure 6. Event Tree for Loss of Cooling Water and Resulting Room Contamination

the estimated reliability of the remote alarm system is 0.99, meaning that it will fail with a probability of 0.01. Using this example let's assume the consequences of the contamination are estimated for each branch of the event tree to range from 1 mSv to 10 Sv depending on the extent of the contamination following the failure. The final column multiplies the probability of the branch times the outcome to obtain the branch risk. The facility risk for the accident sequence represented by this event tree is the sum of all the branch risks or 1.2 x 10^{-4} Sv/yr. To estimate the importance of having personnel present, the probability that the facility is attended is set to zero. The resultant event tree is shown in Figure 7. The resultant facility risk is 2.7 x 10^{-4} Sv/yr, about a factor of 2 higher than the base risk.

Initiating Event	Cause of Failure	Facility Attended	Remote Alarm	Path	Probability	Outcome	Scenario Risk
			Not annunciated				
		Not detected	1.00E-02	1	4.00E-05	1 Sv	4E-05 Sv/yr
		1.00E00	Alarm given				
	Personal Error		9.90E-01	2	3.96E-03	1 mSv	4E-06 Sv/yr
	2.00E-01	Detected					
				3	0.00E00	1 mSv	0
			Not annunciated				
		Not Detected	1.00E-02	4	1.60E-04	1 Sv	2E-04 Sv/yr
		1.00E00	Alarm given				
Cooling system rupture	Mechanical Failure		9.90E-01	5	1.58E-02	1 mSv	2E-05 Sv/yr
2.00E-02	8.00E-01	Detected					
				6	0.00E00	1 mSv	0
			Not annunciated				
		Not Detected	5.00E-01	7	1.00E-06	10 Sv	1E-05 Sv/yr
		1.00E00	Alarm given				
	External Event		5.00E-01	8	1.00E-06	1 mSv	1 E-09 Sv/yr
	1.00E-04	Detected					
				9	0.00E00	1 mSv	0

Figure 7. Event Tree for Case where not credit is taken for the Facility being Attended

If the facility was assumed to be attended but the remote alarm was removed, (this figure is not shown) the resultant total risk rises to 1.3 x 10^{-2} Sv/yr indicating that the much more reliance is being placed on the remote alarm than on the facility personnel being present to promptly detect a leak.

The sensitivity assessment also looks at the perfect system where either the personnel always promptly detect the leak or the remote alarm always sounds. If the facility is assumed to be always attended, such that the leak will always be detected promptly, then the recalculated risk is shown in Figure 8.

Initiating Event	Cause of Failure	Facility Attended	Remote Alarm	Path	Probability	Outcome	Scenario Risk
Cooling system rupture 2.00E-02	Personal Error 2.00E-01	Not detected	Not annunciated	1	0.00E00	1 Sv	0
			1.00E-02 Alarm given	2	0.00E00	1 mSv	0
			9.90E-01	3	4.00E-03	1 mSv	4E-06 Sv/yr
		Detected 1.00E00		4	0.00E00	1 Sv	0
	Mechanical Failure 8.00E-01	Not Detected	Not annunciated	5	0.00E00	1 mSv	0
			1.00E-02 Alarm given	6	1.60E-02	1 mSv	2E-05 Sv/yr
			9.90E-01	7	0.00E00	10 Sv	0
		Detected 1.00E00		8	0.00E00	1 mSv	0
	External Event 1.00E-04	Not Detected	Not annunciated	9	2.00E-06	1 mSv	2E-09 Sv/yr
			5.00E-01 Alarm given				
			5.00E-01				
		Detected 1.00E00					

Figure 8. Event Tree for Case where Facility is Always Attended

The resulting total risk is 2.4 x 10^{-5} Sv/yr, a factor of 5 lower than the base case. If the remote alarm system was assumed to never fail, the resulting risk is 2.1 x 10^{-5} Sv/yr. Since the risk improvement for the two components is approximately the same, and the reduction from the base case is relatively small, a factor of 5, if the risk level for the base case is not acceptable, any recommended upgrades would probably be made solely on cost considerations. Is it cheaper to have the facility occupied for more hours during the week or is it cheaper to upgrade the remote alarm system reliability? If more frequent testing would upgrade the reliability of the alarm system then this would probably be the cheaper upgrade. However, since any upgrade will only result in a reduction by a factor of 5, improvements in risk from other activities might result in a larger reduction in the overall facility operating risk. Alternatively the team might look for other ways to reduce the risk, perhaps by lowering the water loss rate and therefore the amount of cleanup required.

The above set of figures show how sensitivity analyses can be used to evaluate possible risk improvements. In a facility, there are likely to be several systems that pose significant risk so there might be several event trees using different engineering and administrative controls to maintain an adequate level of safety at the facility. In addition, the sensitivity analysis need not be limited to the reliability of engineered and administrative controls. One could look at modifications to the design of the waste water collection system using the same techniques. Since the total facility risk is the sum of the event tree sequences for all the event trees. It follows, that if the remote alarm system is also a part of the other event trees then its importance will be even higher than shown by performing a sensitivity analysis on the event tree shown in Figure 6. It also follows that if other event trees use different engineered or administrative controls, then these other controls might be more important in managing risk levels than the two represented in Figure 6. Sensitivity studies such as shown in this section often become the basis for the recommendations developed in the next section.

2.7. Development of the recommendations to reduce risk

Development of the recommendations to reduce the risk is the final phase of risk assessment. Recommendations contain reasonable measures to reduce the risk based on risk assessment results.

Measures to reduce the risk may be of technical nature and (or) administrative one. General estimation of efficiency and reliability of the measures affected the risk as well as implementation costs are critical for measure selection.

When operating a hazardous industrial facility, administrative measures may compensate for limited capacities to undertake wide technical measures to reduce the risk. Such measures for example include, but are not limited to: limited operations, operating pressures and power, facility (system, unit, etc.) closure.

To develop measures to reduce the risk it is necessary to take into account that the simplest and cost-effective recommendations as well as future measures are to be elaborated at the very beginning due to possible resource limitations. The sensitivity analyses techniques described in Section 2.6 can frequently identify areas where improvements will most significantly reduce the overall risk of operating the facility. Prioritizing the plans to reduce risk by considering both their implementation costs and

their associated risk reduction benefits ensures that any recommendations that are formulated will use the facility's limited resources wisely.

In most cases accident prevention measures are as a rule priority safety measures. Selection of safety measures to be undertaken has the following priorities:

- Measures to reduce probability of emergency including:
  - Measures to reduce probability of incident;
  - Measures to reduce probability of incident growth to accident; and
- Measures to reduce accident consequence severity having the following priorities. The following order of preference should be used when selecting safety features:
  - Design basis measures of hazardous industrial facility (e.g. load-carrying structures, stop valves). Passive systems, such as walls, barriers, or drain tanks, are usually more reliable than active systems, such as pumps or low water level alarms.
  - Measures related to emergency protective systems (e.g. application of gas analyzer).
  - Measures related to readiness of operating organization to localize and eliminate accident consequences.

It is recommended to keep two alternative goals of optimization if it is necessary to justify and estimate the efficiency of proposed measures to reduce the risk:

- To ensure maximum risk reduction of hazardous industrial facility operation considering existing resources; and
- To ensure cost-effective risk reduction up to permissible level.

To determine priority measures to be undertaken to reduce the risk under existing or limited resources it is required:

- To determine measures to be implemented under existing financial resources;
- To rank these measures basing on cost-benefit indicators.

2.8. Criteria independent partner qualities of an estimation of risk

A diagram of the continuous improvement spiral (ISO 14001) shows that the initial assessment of risk is followed by additional steps where performance is monitored, needed upgrades are proposed and then management is asked to approve the proposed upgrades. While management involvement is only shown at one step, since resources must be committed at each step in the process, management must also accept the initial assessment of risk before resources are expended to continue the improvement spiral activities. Prior to accepting the results of the assessments and acting on the recommendations, facility managers frequently request and independent check of the assessment. If the risk assessment must be presented to a regulator, the regulator's technical staff will also perform and document their review of the assessment as part of the regulatory acceptance process. Thus, one or more independent reviews of the assessment are common. The AIChE book titled: *Guidelines for Chemical Process Quantitative Risk Analysis* [15] lists five review criteria: Completeness, Comprehensiveness, Consistency, Traceability and Documentation, The same guidebook defines each of these terms. The statements describing each of the criteria in more detail have been augmented based on and IAEA Technical Document, titled: *Regulatory Review of Probabilistic Risk Assessment (PRA) Level 1* [16] and the experience of individuals who have conducted independent reviews. The expansion, including one more criteria, Validity, is presented in the blue text.

Six Criteria for Evaluating the Adequacy of a Probabilistic Risk Assessment:

1. Completeness. Treatment of the full range of tasks, analyses, and model construction and evaluation should be assured. The completeness issue is the most significant in any risk analysis. It includes such diverse concerns as identification of initiating events, determination of plant and operator responses, specification or component failure modes, physical process analyses, and application of numerical data. Possible operational states, such as normal operation, emergency operation, standby and maintenance states must be considered. As an aid to completeness, some regulations require that the assessment be performed by a small team of individuals (5-7) who collectively have a thorough understanding of system operations, including its behavior

when operated outside its design envelope as a result of component failures or operator errors.

2. Comprehensiveness. A Probabilistic Risk Assessment is unlikely to identify every possible initiating event and event sequence. The aim is to ensure that the significant contributors to risk are identified and addressed. Assurance must be provided that comprehensive treatment is given to all phases of the study in a manner that provides confidence that all significant incidents have been considered. A thorough and documented review of accidents and near accidents that have occurred either for the system being analyzed or similar systems located elsewhere can used as and aid during the assessment development and most importantly as a check point after the analysis has been completed. The system boundaries must be carefully selected such that major risk contributors are included in the assessment. This insures that the performance of one system component is not optimized at the expense of another. Management should allocate sufficient resources, time, people and tools, to accomplish the risk assessment scope within the specified schedule. The schedule should allow time for multiple iterations through the risk assessment, thereby enabling additional data to be collected or tests to be performed on components whose uncertain performance most affects system risk levels.

3. Consistency. Consistency in planning, scope, goals, methods and data within the study is essential to a credible assessment. Equally important is an attempt to achieve consistency from one study to another, especially in methodologies and in the application of data, in order to allow comparison between systems or plant designs. In many cases, the acceptability of an activity is based on its comparability (risk) with other similar activities. The use of standardized methods and procedures enhance comparability. Since probabilistic risk assessments have been routinely performed for many years, an acceptable risk tolerance level has developed. In some countries this risk tolerance level has been codified into regulations. Systems operating far from acceptable risk levels or from levels attained by substantially similar systems will be seriously questioned. Either the assessment will be judged to be inadequate of the system design and operation unacceptable. Risk acceptance criteria must be established to judge if the system can be safely operated and once established must be applied uniformly throughout the assessment.

4. Validity. The scope of the assessment must be broad enough to cover the range of operational conditions that the system could reasonably experience during its lifetime. The model and data uncertainty must be evaluated and shown to not be within acceptable ranges. Considering reasonable levels of uncertainty, the performance of the system should remain within acceptable performance limits. The results of the assessment should be based on expected system performance. When point values are used for parameters, mean values should be used. Sensitivity analyses should be performed to demonstrate that assumptions regarding system performance are reasonable. Similarly, current assessments should consider the information developed in prior risk assessments having similar purposes and objectives. When scenario risk assessment methods are being used, if is often cost effective to perform a qualitative screening as the first iteration, reserving the more comprehensive quantitative assessment for those scenarios that are shown to be significant risk contributors in the qualitative assessment. For risk assessments that are based on logic structures, e.g. fault trees, successive iterations should focus on the risk significant branches, evaluating the need for better data and/or the need to develop additional branches. A final review should look to see that past incidents are incorporated in the model and that their frequency and consequences are appropriate. Any computer codes used in the analysis should be validated and verified.

5. Traceability. The ability to retrace the steps taken, that is, reconstruct the thought process to reproduce an answer, is important not only to the reviewer and regulator but also to the study team. Since assessments frequently make use of information from many reference sources, such as data bases of human performance factors and component failure rates, it should be possible to trace the data used in the analysis back to a specific item in the reference sources.

6. Documentation. The documentation associated with a probabilistic risk assessment is substantial. Large amounts of information are generated during the analysis and many assumptions are made. The information must be well documented to permit an adequate technical review of the work, to ensure reproducible results, to ensure that the final report is understandable, and to permit peer review and informed interpretation of the study results.

2.9. Risk analysis result documenting requirements

The risk analysis process should be documented. The scope and format of a risk analysis report depend on the objectives of the risk analysis done. In the report, it is recommended to include the following (if not otherwise required by legal and regulatory documentation):

- title page,
- executive summary
- list of performers with positions, scientific titles, names of organizations,
- table of contents,
- objectives and purposes of the risk analysis done,
- description of the hazardous industrial facility analyzed,
- description of risk assessment approach or methodology(ies) employed
- description of emergency process models,
- hazard identification results,
- risk assessment results,
- generalization of risk assessments including the “weakest points”,
- risk reduction recommendations,
- conclusions, and
- list of references.

Attachment A. Data necessary for HAZARD identification and follow-up risk assessment and recommendations for its representation

It is recommended to tabulate the data on the “Basic Constituents of Hazardous Industrial Facility (HIF) ” and “Information on Hazardous Substances Handled at HIF” as given below (Tables A1 and A2).

The Table “Basic Constituents of Hazardous Industrial Facility” is recommended to include the columns:

- “HIF constituents”, and
- “Brief description of HIF constituents”.

For the “HIF constituents” column it is recommended to give the name of a constituent and its serial number. As constituents it is recommended to indicate bays, installations, shops, storage facilities and other elements integrating devices or their aggregate due to their process or administrative lines and incorporated into the facility.

For the “Brief description of HIF constituents” column it is recommended to give the purpose, composition, design production capacity, technique (method) employed by each constituent.

The Table “Information on Hazardous Substances Handled at HIF” is recommended to outline the following data on each constituent listed in table A1:

- name of hazardous substances handled at a given facility constituent,
- amount of the hazardous substances indicated, and
- identification attributes.

Table A1

Basic Constituents of Hazardous Industrial Facility

Constituent	Brief description of facility constituents			
	Purpose	Composition	Design capacity, thsnd t/year	Technique applied
1. Chlorine production		Building 11 (electrolysis) Building 12 (evaporation and brine treatment)	150	Diaphragm electrolysis technique
…	…	…	…	…

Table A2

Information on Hazardous Substances Handled at HIF

Substance				Identification attributes						
Name	Amount, t	Individual hazardous substance, t	Flammable gases, t	Flammable liquids		Toxic substances, t	Highly toxic substances, t	Oxidants, t	Explosives, t	Environmentally hazardous substances, t
				In storage, t						
1. CHLORINE PRODUCTION										
1. Chlorine	700	700								
2. Sulphuric acid	150					150		150		
3. …	…	…	…	…	…	…	…	…	…	…
Total for the facility		700	…	…	…	…				
Limiting amount		25				200		200		

In doing so it is recommended to provide for the information on those hazardous substances which amount exceeds 10% of the threshold values indicated in the Federal Law “On Safety of Hazardous Industrial Facilities”, Attachment 2.

In the column “Substance” it is recommended to indicate the name of a hazardous substance as per GOST (State Standard), TU (Technical Specification), etc.

The column “Amount” should indicate a total amount of each hazardous substance at a given constituent of the hazardous facility.

The columns “Identification signs” are recommended to contain the data for each hazardous substance on its amount in the corresponding sub-column (the types of hazardous substances are to be determined basing on the Federal Law “On Safety of Hazardous Industrial Facilities”, Attachment 2, Tables 1 and 2).

In cases where one and the same substance may be attributed to different types, e.g. “Flammable gases” and “Toxic substances”, the amounts of such substance are to be indicated in both columns. For individual substances it is sufficient to indicate their amounts in the “Individual hazardous substance” column.

Table “Information on Hazardous Substances Handled at HIF” is to be ended with the columns “Total” and “Limiting amount”.

The column “Total” should contain a total amount of each type of hazardous substances present at the facility.

The column “Limiting amount” should contain the values of limiting amounts of hazardous substances as per the Federal Law “On Safety of Hazardous Industrial Facilities”, Attachment 2, Tables 1 and 2.

The substances, which are used to characterize an industrial facility as a hazardous one, are derived from the table “Information on Hazardous Substances Handled at HIF”. The determination of the industrial facility as such is done by comparison of the total amount of a hazardous substance present at the facility with its limiting values established in the Federal Law.

It is recommended to tabulate the data on distribution of hazardous substances over the facility equipment in the constituent-by-constituent manner as given below in table A3.

Table A3

Data on distribution of hazardous substances over the facility equipment

Process unit, equipment			Amount of hazardous substance, t		Physical conditions of hazardous substance presence		
Name of unit	Name of substance, equipment; # on Diagram, hazardous substance	Number of equipment pieces	In equipment piece	in unit	State of aggregation	Pressure, MPa	Temperature, ^{0}C
1.CHLORINE PRODUCTION							
Storage unit № 1	Cask Pos.1 chlorine	30	1.0	40.0	Liquid, gas	3.5	ambient
…	…	…	…	…	…	…	…
In total, hazardous substance – chlorine at the "Chlorine Production" constituent, t							
to include	in vessels (apparatuses), t						
	in pipelines, t						

It is recommended to use the data presented in the Table "Data on distribution of hazardous substances over the facility equipment" as the input data for calculation of a hazardous substance amount involved in various hypothetical scenarios of accidents.

It is recommended to present the "Data on Facility Personnel as per Facility Organizational Units and Constituents with Indicating Its Average Number and Maximum Number of Shift Personnel On Duty " in the tabulated format as below (table A4).

Table A4

Personnel Allocation Data for Main Industrial Site of "EnskPlastic" Plant

Facility constituents	Personnel, persons		Name of organizational unit	Personnel, persons	
	average	maximum shift		average	maximum shift
Vinyl chloride production	160	240	Building 1	50	80
			Building 2	40	60
Constituent # of the declared facility	…	…	…	…	…
In total at facility:				…	…

The “Data on Neighboring Organizations”, which may be affected by an accident with indicting the distance from the facility boundary and number of personnel in maximum shift on duty, is recommended to present as a table after the facility risk analysis and identification of probable accident affected areas have being done.

An example table is given below in table A5.

Table A5

Data on Neighboring Organizations

Name of organization	Distance from the facility boundary	Number of maximum shift on duty personnel, persons
1. DHP 1	900 m to the south	70
2. Trucking company	1200 m to south-west	100
…(other neighboring organizations)	…	…

The “Data on Neighboring Settlements”, which may be affected by an accident with indicting the distance from the facility boundary and maximum number of population, is recommended to present as a table after the facility risk analysis and identification of probable accident affected areas have being done. An example table is given below in table A6.

Table A6

Data on Neighboring Settlements

Name of settlement	Distance from facility boundaries	Population, persons	Type of development
1. Rabochi	900 m to south	170	Urban-type village; 2-store brick mansions
…(other neighboring settlements)	…	…	…

The data on “characteristics of hazardous substances” is recommended to present as the table below in table A7.

Table A7

Hazardous substance characteristics

N п/п	Parameter name	Parameter	Source of data
	2	3	4
1.	*Name of substance*		
1.1	Chemical		
1.2	Commercial		
2.	*Formula*		
2.1	Empirical		
2.2	Structural		
3.	*Composition, %*		
3.1	Basic product - basic substance's fraction of total mass, not less than		
3.2	*Admixtures* (to identify) - water fraction of total mass, not more than		
	- NCl_3 fraction of total mass, not more than		
	- non-volatile residue fraction of total mass, not more than		
4.	*General data*		
4.1	Molecular weight		
4.2	Boiling temperature, ^{o}C (at pressure 101 kPa)		

4.3	Density at 20°C, kg/m^3		
5.	*Fire and explosive safety data*		
5.1	Flash point		
5.2	Self-ignition temperature		
5.3	Explosive limit		
6.	*Toxic hazard data*		
6.1	PLC in the bay air		
6.2	PLC in atmospheric air		
6.3	Lethal toxic dose LCI_{50}		
6.4	Threshold toxic dose PCI_{50}		
7.	*Reactivity*		
8.	*Smell*		
9.	*Corrosiveness*		
10.	*Precaution measures*		
11.	*Human impact data*		
12.	*Protection means*		
13.	*Substance neutralizing measures*		
14.	*First aid measures*		

The “Schematic Process Diagram" indicating the major process equipment and describing in brief the process with regard to the facility constituents” is recommended to present in a constituent-by-constituent manner.

It is recommended to indicate in the Schematic Process Diagram the cut-off valves installed at the stage, unit boundaries.

The “Layout of major process equipment to treat hazardous substances” is recommended to present in a constituent-by-constituent manner.

It is recommended that each Schematic Process Diagram has its own major process equipment layout.

The “Layout” should also indicate locations of control boards, operator’s rooms, switchboard rooms, door openings, dikeing, emergency equipment (fire extinguishers, hydrants, personal protective equipment, communications equipment, etc.).

The “List of major process equipment to treat hazardous substances” for the declared facility is recommended to present in a constituent-by-constituent manner.

It is recommended that the Table “List of major process equipment to treat hazardous substances” includes the following columns:

- “Equipment position number as per the Schematic Process Diagram”;
- “Name of equipment and material” (to indicate the base material the equipment is made of):
- “Number of equipment pieces”;
- “Location” (location of the equipment):
  - “Purpose” (in accordance with the description of technology); and
  - “Technical characteristics” (for tank-type equipment: dimensions, volume and capacity; for compressor pumps: production capacity; for pipelines: length and diameter).

The identification results obtained by an organization operating the hazardous industrial facility are documented in the form of a table below (table A8).

Table A8

Identification Form of Hazardous Industrial Facility[1]

1. Hazardous industrial facility		
1.1.	Full name of facility	
1.2.	Location (address) of facility	

[1] In paras. 1.1, 1.2, 4.1 — 4.4 the free right-hand field is to be filled out; in the right-hand field of paras. 2.1—2.5 and 3.1 — 3.5 the symbol ✓should mark the relevant hazard attribute and facility type codes.

2. Hazard attributes of facility

2.1.	Receipt, use, reprocessing, generation, storage, transportation, destruction of hazardous substances indicated in the Federal Law "On Safety of Hazardous Industrial Facilities", Attachment 1.	21 ✓
2.2.	Use of equipment operated under pressure more than 0.07 MPa or at water heating temperature more than 115 ^{0}C	22 ✓
2.3.	Use of stationary hoisting devices, moving ramps, rope ways, funiculars	23
2.4.	Production of melts of ferrous and non-ferrous metals and alloys on their basis	24
2.5.	Mining, mineral processing and underground operations	25

3. Type of facility

3.1.	Facilities where hazardous substances are present in the amounts equal or exceeding the amounts established in the Federal Law "On Safety of Hazardous Industrial Facilities", Attachment 2	31
3.2.	Other than the facilities listed in para. 3.1 of this list where hazardous substances are present in the amounts less then the amounts established in the Federal Law "On Safety of Hazardous Industrial Facilities", Attachment 2	32
3.3.	Other than the facilities listed in paras. 3.1 and 3.2, which possess the hazard attributes indicated in paras. 2.1 — 2.5 of this list	33

4. Operating organization *(in accordance with the its Charter)*

4.1.	Full name of organization	
4.2.	Mailing address of organization	

4.3.	Telephone, facsimile number	

4.4.	Superior agency	

In summary, to conduct a risk assessment it is necessary to:

1. Review and analyze:
    - accidents and failures occurred to the facility in question;
    - accidents occurred to similar facilities; and
    - possible causes and factors facilitating initiation and development of accidents at the facility in question.
2. Identify possible accident scenarios.
3. Evaluate amounts of hazardous substances involved in the accident.
4. Calculate probable accident affected areas.
5. Assess a possible number of affected persons.
6. Assess possible damage.

A list of methodological materials recommended for risk assessment of accidents at hazardous industrial facilities is given in Attachment E.

Attachment B1. Screening for Potential Sources of Hazard

At as the first step in performing a preliminary hazards assessment, it is often useful to go down a list such as the following and identify which of the hazards might be present at the facility. If one of the hazards can not result in a release of hazardous, radioactive, or nuclear material to the environment or the accidental exposure of a worker, then it is appropriate to just state that the hazard presents is either *not present* or is considered to present a *negligible hazard*. If it is present and can be quantified, then it is appropriate to quantify the magnitude of the hazard. For example, if impact is

Table B-1. Screening for Potential Sources of Hazard

Hazard	Basis for Including or Excluding from the Analysis
Acceleration (uncontrolled – too much, too little)	
Inadvertent motion	
Sloshing of liquids	
Translation of loose objects	
Deceleration (uncontrolled – too much, too little	
Impacts (sudden stops)	
Failure of brakes, wheels or tires	
Falling objects	
Fragments or missiles	
Chemical Reaction (non-fire, can be subtle over time)	
Dissociation (product reverts to separate components)	
Combustion (new product formed from mixture)	
Corrosion, rusting, etc	
Electrical	
Shock	
Burns	
Overheating	

Ignition of combustibles	
Inadvertent activation	
Explosion, electrical	
Explosion	
Commercial explosive present	
Explosive gas	
Explosive liquid	
Explosive dust	
Flammability and Fires	
Presence of fuel – solid, liquid or gas	
Presence of strong oxidizer – oxygen, peroxide, etc	
Presence of strong ignition source – welding torch, heater	
Heat and Temperature	
Source of heat (non-electrical)	
Hot surfaces, burns	
Very cold surfaces, burns	
Increased gas pressure caused by heat	
Increased volatility caused by heat	
Increased activity caused by heat	
Mechanical	
Sharp edges or points	
Rotating Equipment	
Reciprocating equipment	
Pinch points	
Weights to be lifted	
Stability/toppling tendency	
Ejected parts or fragments	
Pressure	
Compressed gas	
Compressed air tool	
Pressure system exhaust	
Accidental release	
Objects propelled by pressure	

Water hammer	
Flex hose whipping	
Static	
Container rupture	
Over-pressurization	
Negative pressure effects	
Leak of Material	
Flammable	
Toxic	
Radioactive	
Corrosive	
Slippery	
Radiation	
Ionizing radiation	
Ultraviolet radiation	
High intensity visible light	
Infrared radiation	
Electromagnetic radiation	
Laser radiation	
Toxicity	
Gas or Liquid - Asphyxiant - Irritant - Systemic poison - Carcinogen or Mutigen	
Combination product	
Combustion product	
Vibration	
Vibrating tools	
High nose source level	
Mental fatigue	

Flow or jet vibration	
Supersonics	
Miscellaneous	
Contamination	
Lubricity	
Add other hazards not included above and unique to this facility?	

Attachment B2. Accident Hazard identification and risk assessment: emergencies in the context of ISO 14001

ISO 14001 requires that environment aspects be identified that may result from normal (routine) operations as well as from abnormal operations (system failures or accidents leading to an emergence situation). The following figure B2-1 products seweral examples of products, activities or services that can lead to environment impacts from normal and/or abnormal operations.

Environmental Aspects

Potential Aspects Applicable to an HIF / Nuclear Facility

Contribution from Normal and Abnormal Operations

Aspect	Normal	Abnormal
Toxic materials discharged to Potable Water Supply	☒	☒
Volatile Organic Carbons (VOC) Emissions	☒	☐
Scrap Generation	☒	☐
Solid Waste Generation	☒	☒
Fresh Water Use	☒	☐
Electricity Use	☒	☐
Release of Chemicals or Radionuclides	☒	☒

*note that these aspects result from activities involved in the production of products and services

Figure B2-1. Accident Hazard Identification and Risk Assessment: Understanding Abnormal Operations in the context of ISO 14001

Notes: The discharges of radioactive materials to the potable water supply are zero during normal operations. There could be radionuclides released to the potable water supply as a result of abnormal operations, that is an accidental release or discharge. The term used in this risk assessment methodology for significant releases resulting from abnormal operations is accident hazards. Similarly, scrap generation could occur from normal operations and also from abnormal operations (accident cleanup), though scrap

generation would be dominated by normal operations. Exposure to toxic chemicals and radionuclides is certainly possible from normal and abnormal operations, from accidents.

Risk assessment can only be applied to abnormal operations. It can be used as a tool to assist EMS managers to identify and define and environmental aspects that may have significant impacts on the environment. The development of risk management plans is akin to the ISO 14001 requirements to develop objectives and targets and environmental management programs for aspects having significant impacts as well as for instituting administrative or operational controls.

While normal and abnormal operations may share some common environmental aspects, normal operations may be different from abnormal operations in several ways.

1. The environmental limits are different for normal and abnormal operations. The limits are much lower from normal operations because of the effects of buildup in the environment. If follows that the risk based decision criteria (consequence and frequency) should be or are different as well.
2. For abnormal operations the objectives and targets of an risk management or environmental management program might for example have two components, frequency reduction and impact (consequence) reduction. For normal operations, the environmental targets will almost always be impact reduction.
3. The impact data from normal operations can be obtained by direct surveillance whereas the impact data from abnormal operations can only be inferred from a systematic analysis of postulated component failures and human errors, e.g. risk analysis. For example, survey / monitor members of the general public or workers and put them in a whole body counter and measure their radioactive uptake and show that environmental targets you established for normal operations are being met. An organization can monitor their continuous improvement over time. Since the severe accidents have not occurred, it is only possible to estimate how much uptake members of the public will receive, the impacts can only be measured for the accidents that have occurred and those that have occurred will always be a small subset of the postulated accidents. It follows that it is relatively easy to establish environmental targets for normal operations and much more difficult to establish objectives and targets for abnormal operations.

4. A well-designed HIF or radiological and nuclear facility will have very low impacts from normal operations. If there are no measurable releases - and that is what they said for the airborne release path - then the only possible environmental target would be to maintain zero releases from the facility. However one can always affect abnormal releases by establishing objectives and targets that reduce the likelihood of an abnormal condition, the likelihood of releases, or the consequences of a release should one occur.

To these ends, defining "significance" is crucial, as this will lead to the list of activities that will be the primary focus of activities managed by the EMS. Defining significance is essential for identifying and rank ordering priorities to focus resources, develop Objectives and Targets (ISO 14001 Section 4.3.3) through risk assessment or other environmental assessment techniques, (including regulatory assessment, ISO 14040, etc.), an in turn develop environmental management programs (ISO 14001 Section 4.3.1) for each significant aspect.

All other aspects would be addressed as normal operations under "Operational Controls" (ISO 14001 Section 4.4.6) along with those that are identified as significant.

There are many ways to define significance. The following are some examples.

- Develop a likelihood and severity or risk matrix to rank order aspects. This approach is very useful if the major aspects are the result of abnormal operations
- Some organization rank order all regulated impacts as significant. This approach is very useful if major aspects are the result of normal operations.
- Stakeholder interest (i.e., general public, media, environmental groups, legislators)
- Use of the likelihood severity (risk) matrix to identify major environmental aspects for abnormal operations and the rank ordering of environmental aspects associated with normal operations and stakeholder interests.
- Percentile ranking within a distribution of scores, which could be a mixture of quantitative, regulatory, and stakeholder interests.

Typically, significance is defined by the organization:

Traditional EMS defines significance as a function of scale, severity, probability, and duration of impact, and should consider:

- air emissions
- releases to water
- waste management
- contamination of land
- use of raw materials and natural resources
- other local and community issues

Mangers may consider three ways to frame significance:

- Look in: What could stop our ability to do our mission? What would advance it? What are leadership priorities?
- Look out: What damages or helps host communities? What most helps or hurts how they see us?
- Look forward: What changes are expected -- new missions, equipment, siting, etc? How can we re-position to expedite those changes or reduce costs and impacts?

In the example table (see table B2-2) below, information developed from the risk assessment for accident hazards or abnormal operation can be used to assess aspects and impacts: frequency, consequence and, legal requirements. The risk matrices including risk reduction action rankings/statements can be used to help identify aspects from abnormal operations having significant impacts.

Table B2-2. Aspects and Impacts: example table

ASPECTS	ACTIVITIES	IMPACTS	Legals & other requirments	RISK/ LIKELIHOOD	CONSIQUENCE/ MAGNITUDE	RATING	SIGNIFICANT

Attachment C. Risk Matrix for hazardous industrial facilities

Figure C1 shows a possible risk matrix and the corresponding action statements are shown in the figure and also in Table C1.

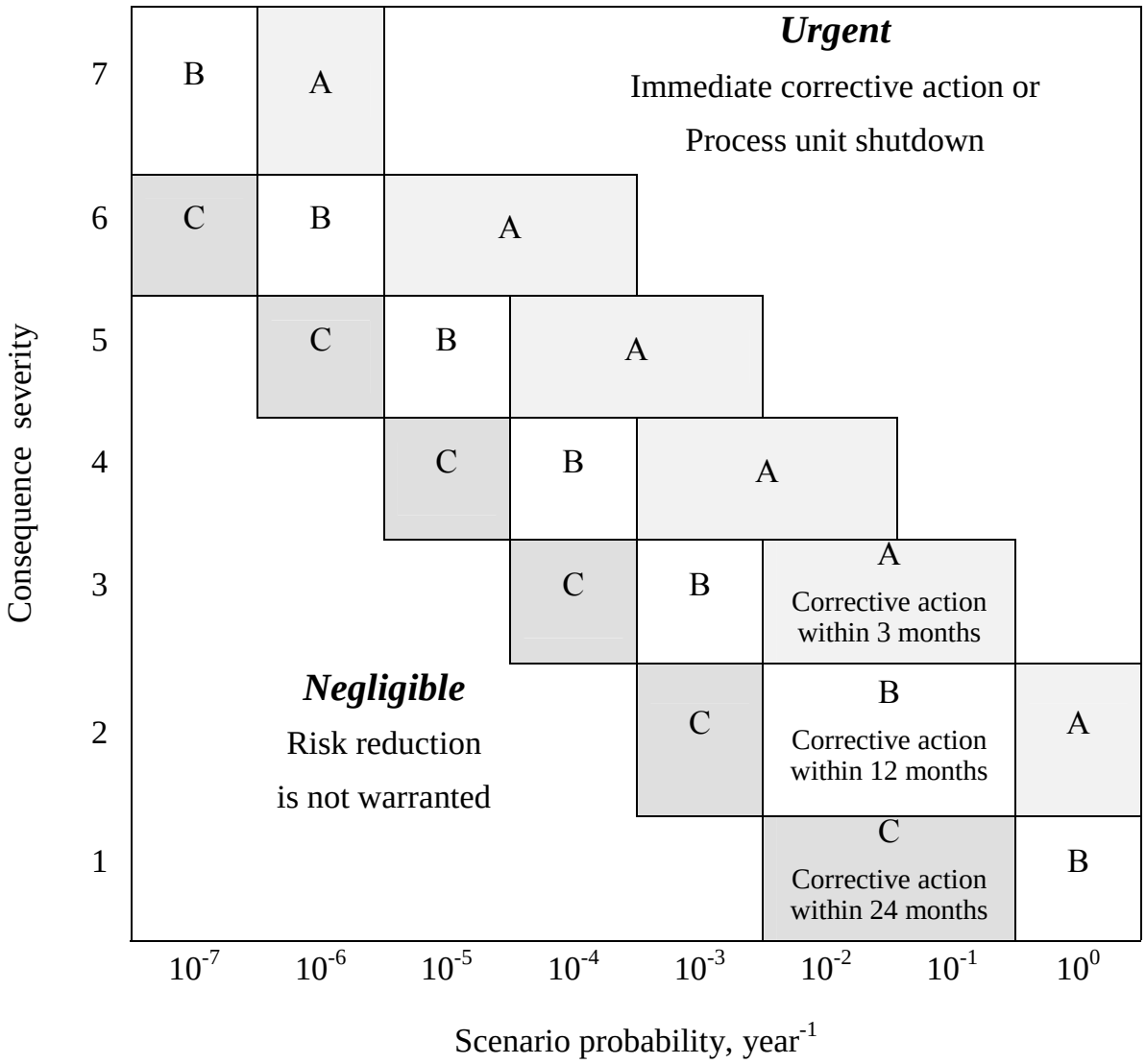

Figure C1. Quantitative Risk Matrix

Table C1. Risk Reduction Action Statements for Figure B1

Category	Risk reduction action statements
A	Based on the As Low As Reasonably Achievable (ALARA) principle, implement risk reduction measures within 3 months
B	Based on the As Low As Reasonably Achievable (ALARA) principle, implement risk reduction measures within 12 months
C	Based on the As Low As Reasonably Achievable (ALARA) principle, implement risk reduction measures within 24 months

Some care must be taken in developing the risk reduction action statements. The statements shown in table C1 leave little leeway to the facility manger. If there is one of the bounding accident scenarios is shown to fall in the Category *A* risk level, then the manager must implement a program to reduce that scenario out of Category *A* and ideally below Category *C* within 3 months. There are risk scenarios, the loss of coolant accident in nuclear power reactors being one of them which could fall in the *A* category and it would not be possible to reduce the level to below a *C* in 3 months. What is being done instead is to develop new reactor concepts that will not have any accident scenarios in the *A*, *B* or *C* category but that will take 20 years.

Using the risk criteria shown in Figure 1, it is not possible to quantify the risk level for the accident scenario developed in Section 2.4 and shown in table 8.

Therefore for quantitative risk assessment the table needs to be modified by adding the "risk" column (see table C2).

Table C2. Modified "If other than…?" Table Example with Risk Column Added and Quantified

№	What If?	Scenario Description	Safeguards	Consequences	Frequency	Risk	Comments
1	Too much water was lost from the pool	Contamination of lower room below pool, possible damage to fuel from loss of cooling, and over exposure of personnel in fuel storage area	Low Level Alarm on Pool Water Level and Periodic Surveillance of Lower Room Probability of safeguards component failure, 0.001 for alarm and (1-0.999)* 0.01 that operator will correctly respond to alarm resulting in probability of surveillance failure of 0.01	Release of radioactivity in excess of regulatory limits Based on Figure 3 the consequences would be assigned to severity level 3	Probability of large break 0.001/year; times probability of a failure of the surveillance system of 0.01 results in a frequency for this scenario of 10^{-5}/year.	Based on the frequency and consequence estimate, using Figure 5, the risk level for this scenario is a *D*, no risk reduction is warranted	Documented resolution of Action Item: 1 concludes no fuel cladding rupture will occur

Attachment D. Construction of a risk matrix for facilities using nuclear power

General approaches to construction of the risk matrix are applicable to all types of hazardous activities. Nevertheless, the specific character of the consequences and the events themselves in the field of nuclear technologies should be taken into account in the risk matrix that is constructed for facilities using nuclear power. In construction of the matrix

- the corresponding range of probabilities of the events was determined;
- various examples of event classification were examined and the scale of ranking the events according to their severity was chosen;
- the priorities of the correcting measures dependent on the results of risk assessment were set.

Probabilistic scale

The probabilistic scale in the range of 10^{-7} – 10^{0} $year^{-1}$ was set on the basis of analysis of normative documents, materials of probabilistic safety analyses of some nuclear and radiation hazardous facilities of Russia and expert assessments.

In particular, the average weighted probability of a severe accident at modern Russian reactors RBMK and VVER is assessed as 10^{-4}(reactor-years)$^{-1}$[17] and lower. The active international and domestic standards set the probability of a severe accident accompanied with the destruction of the core at the level of 10^{-5} (reactor-years)$^{-1}$[18] for the currently designed reactors of the next generation. The development of advanced reactors based on the concept of "natural safety" takes into account probability of core destruction in the range of 10^{-7} – 10^{-8} (reactor-years)$^{-1}$. An event with the probability of 10^{-7} is judged by the specialists as nearly excepted and is taken as the lower limit in the matrix.

It is advisable to set the upper limit at the level of 10^{0} $year^{-1}$. The statistics shows that the events characterized by this level of probability include disruptions in the operation of the nuclear power using facilities that did not lead to lowering of the level of safety of the facility. These include violations of safety measures, failures and false action of the equipment etc.

Scale of consequence severity

Different classifiers are used dependent on the purpose and the field of application of the scale of classification of events at the facilities using nuclear power. The area of radioactivity spreading is one of the simple and obvious criteria characterizing the severity of event consequences. According to this criterion the events are divided into [19]:

- on-site (the radioactive substances (RAS) released beyond the equipment limits);
- local (release of RAS in the limits of the sanitary protection area that exceeds the set standards);
- general (release of RAS beyond the sanitary protection area that exceeds the set standards).

Such a scale can be most effectively used in identification of means and resources in planning and organization of actions aimed at liquidation of the accident consequences.

Analysis of various classifiers revealed that they are specific for each of the nuclear radiation hazardous facilities. Normative documents of Gosatomnadzor of Russia provide for categorization dependent on the features and consequences of the operation violations of various types of nuclear and radiation- and radiation-hazardous facilities (NPP, research reactors, nuclear fuel cycle facilities etc.) All the violations are divided into accidents and incidents, and categorization is specific for each type of the nuclear radiation hazardous facilities [20, 21]. In particular, there 4 categories of accidents and 11 categories of incidents set for NPP. Classification for nuclear fuel cycle facilities includes 6 categories of accidents and 5 categories of incidents. Accident of maximum level (A01) for NPP is classified as "*Release of the radioactive substances to the environment as a result of a severe beyond design-basis accident which may lead to serious radiation injuries among NPP personnel and population, harmful effect on health, contamination of large territories. Transboundary transport of radioactive substances is possible. Long-term radiation impact on the environment*". Accident of maximum level (A01) for nuclear fuel cycle facility is classified as "*Radioactive release to the environment that lead to exceeding of level B criteria of urgent decision-making at the initial stage of the accident in the areas beyond the control area of nuclear fuel cycle facility*". NRB-99 provide for three population protection measures at the initial stage of a radiation

accident: sheltering, iodine prophylaxis and evacuation. It also sets intervention levels A and B for each of the measures. Decision on implementation of the protective measure is taken on the basis of comparison of the predicted dose prevented by a measure with levels A and B. If level B is exceeded then the corresponding measure should be implemented even if it will lead to disruption of normal activities of the population and functioning of the territory. If we take sheltering as a protective measure, then NRB-99 sets the prevented population exposure dose of 50 mGy and more as level B. The value is an order of magnitude lower than the one that can cause serious radiation injuries.

The more general classification used for assessment of accident severity from the point of view of safety, is International Nuclear Event Scale (INES) [11]. The scale is applicable to any event connected treatment of nuclear materials and radioactive substances including events during their transportation. The classification procedure includes an analysis of an array of quantitative and qualitative criteria such as the condition of the protective barriers, safety systems, the amount of the release to the environment, population and personnel dose levels. Such a generalized approach may be used not only for classification of scenarios of real events, but also for classification of scenarios of events considered in risk assessment. Taking into account the more universal character of INES, it was decided to use this scale and classification procedure for ranking of the scenarios according to the severity of the consequences.

Risk matrix for nuclear power using facilities

The draft of risk matrix for nuclear power using facilities suggested in the current work is shown below (see fig. D1).

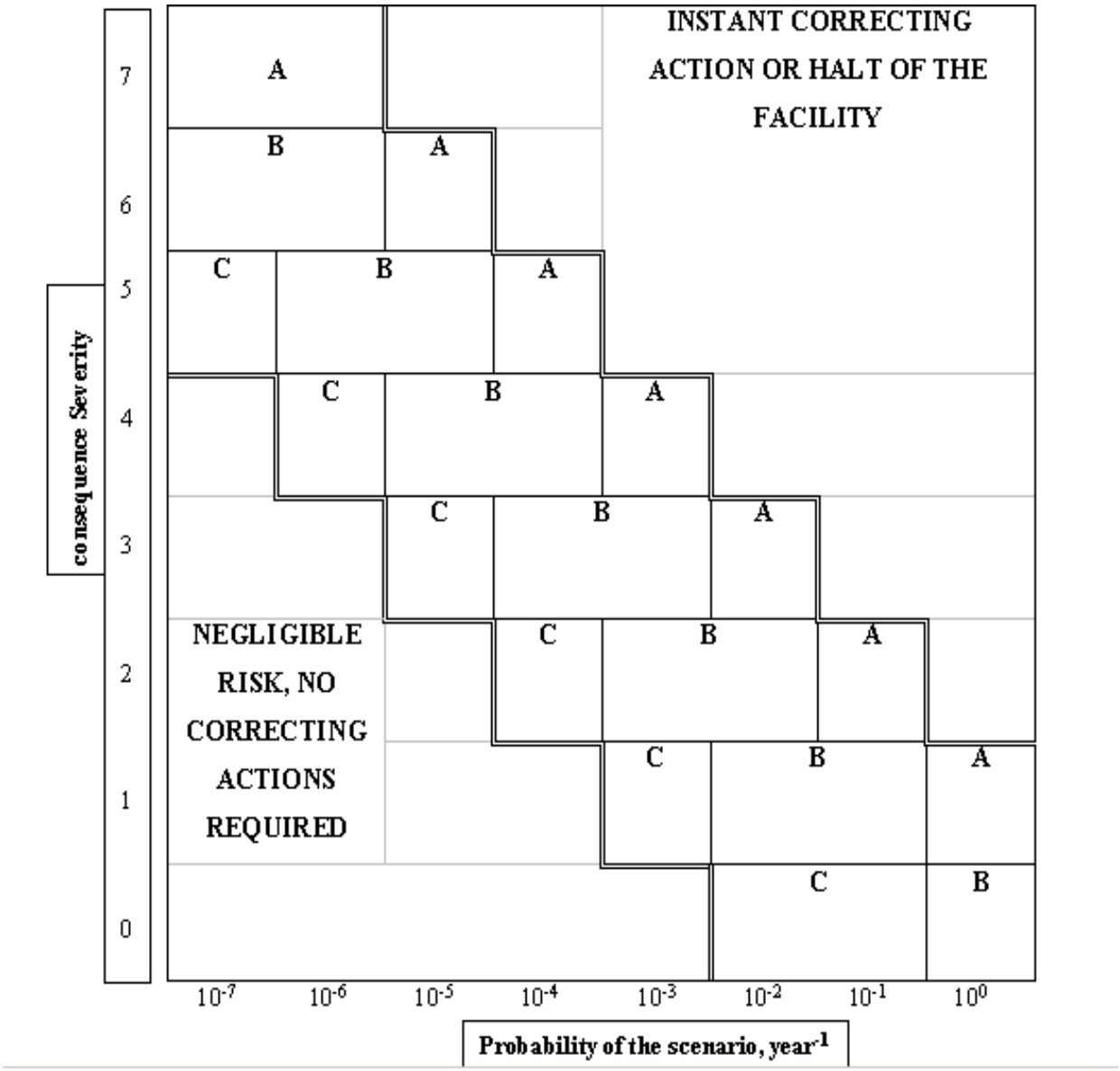

Figure D1. Risk matrix for facilities using nuclear power

The area within the double line is the risk corridor, where planning and implementation of corresponding correction measures is required. The area below the line represents negligible risks, where correction measures do not guarantee lowering of the risks. The area above the line represents impermissibly high risks. Urgent safety measures or halting the operation of the facility is required in case of such risks.

The risk corridor for the risks that require protection measures has various areas marked A, B, C, which determine the criticality of the scenarios and urgency of carrying out the corresponding measures. This requires some comment. The terms of realization of such actions are not set in Russia. At the same time, as it was mentioned above, any disruption of operation mode of a nuclear fuel cycle facility must be examined by the

commission within 15 days. A report and a plan of correction measures are worked out based on the results of the work. They contain the executors and the terms of works, which are sent to all similar facilities. The terms of the measures are set by the management of the facility in agreement with federal inspection agencies taking into account the complexity of the works and their cost. Therefore, the terms given in the risk matrix should be considered as approximate terms. It seems that it is advisable to distinguish urgent (3 months), planned (12 months) and long-term (24 months) correction actions. If we speak about the urgent measures (A), it needs to be specified that they are interpreted first of all as unplanned measures carried out according to separate programs of technical and organizational direction developed on the basis of the risk matrix. As practice of correction measures implemented after the violations of level 0 and 1 shows, such measures are generally carried out within three months. However, in general, implementation of such works may last for several years in the case when the measures affect such problems as, for example, changing the design. Category B is interpreted as inclusion of measures developed on the basis of risk assessment in standard annual reports and safety assurance plans (see above). Category C includes perspective measures, which are recommended for consideration.

Ranking of the area limited with a double line to categories A, B and C was done on the basis of expert assessments. Events with minimum category of severity and probability level of 10^0 were ranked as category B due to the following arguments. Such deviations are negligible from the point of view of safety, but due to their frequency they are treated as nearly inevitable and thus require systematic work on reduction of their number.

Normative documents of federal and facility levels also demand carrying out planned measures directed at reduction of facility affect on human and environment (see above).

It is recommended to carry out an analysis, develop and realize a program of measures for events with lower possibilities (10^{-1}-10^{-2} $year^{-1}$), but the terms of realization are not critical in this case (category C).

Events that lead to consequences of the first category (anomaly), the possibility of which is assessed as 10^0 $year^{-1}$, were ranked as category A. Such events require urgent detailed assessment and carrying out correction measures. In case of lower possibilities

(10^{-1}-10^{-2}), correction measures may be implemented under annual program of measures directed at raising of the safety (B).

The possibility of a severe accident for modern Russian reactors RBMK and VVER was assessed at the value of 10^{-4}(reactor-years)$^{-1}$ and lower. According to the severity scale, such an accident may correspond to category 4 and above. Such a condition requires systematic work on raising of the safety according to the opinion of the experts.

Scenario of a major accident, the possibility of which was assessed by the experts as 10^{-7} (reactor-years)$^{-1}$ (practically improbable event) requires detailed examination and taking of urgent countermeasures according to the matrix. The situation corresponds to modern state of work on designing of perspective nuclear reactors, which are designed to have the possibility of core destruction of $10^{-6} – 10^{-7}$ (reactor-years)$^{-1}$.

The matrix given has the following differences if compared to the risk matrix used in chemical industry (see section 2.5):

- wider range of severity of the consequences of an event;
- specific criteria for assessment of consequence severity were used;
- the critical area, where immediate correction action is required, was widened for events with probability higher than 10^{-5};
- the area of negligible risk was narrowed.

The constructed risk matrix may be used for development of program of measures aimed at enhancing the safety at a stage of facility operation based on relative risks.

Attachment E. List of methodological document recommended for use while conducting risk analysis of hazardous industrial facilities

1. RD 08-120-96. Methodological guide on risk analysis of hazardous industrial facilities.

2. PB 09-170-97. General explosion safety rules for explosion and fire hazardous chemical, petroleum chemical and oil refining plants.

3. PB 03-182-98. Safety rules for overland liquid ammonia storage facility.

4. PB 13-01-92. Unified safety rules for conduct of blasting operations.

5. NPB 105-95. Identification of explosion and fire hazard categories of premises and buildings. — M.: State Fire Protection HQ of the Ministry of Interior of the Russian Federation.

6. NPB 107-97. Identification of fire hazard categories of outdoor facilities. — M.: State Fire Protection HQ of the Ministry of Interior of the Russian Federation.

7. RD 52.04.253-90. Methodology for prediction of scale of noxious substance contamination resulted from accidents (collapse) at hazardous chemical facilities and transport (approved by CDHQ of the USSR).

8. Chemical accident consequences assessment methodology (“TOKSI” method) as agreed upon with Gosgortekhnadzor of Russia (letter of 03.07.98 № 10-03/342), RTC «Promyshlennaya Bezopasnost» (Industrial Safety), 1999.

9. Methodology for assessment of consequences of emergency fuel and air mixtures as agreed upon with Gosgortekhnadzor of Russia (letter of 03.07.98 № 10-03/342), RTC «Promyshlennaya Bezopasnost» (Industrial Safety), 1999.

10. Methodology for forecasting an engineering situation of cities and regions in case of emergencies. — M.: v/ch 52609, 1991.

11. Methodological guide for forecasting and assessment of chemical situation in case emergencies. — M.: All-Russia Research Institute for Civil Defense and Emergencies, 1993.

12. Methodology for earthquake consequence assessment./Collected methodologies on forecasting of possible accidents, catastrophe and natural disasters in the RSE (Book 1), M.: Ministry of the Russian Federation for Emergencies, 1994.

13. Collected methodologies on forecasting of possible accidents, catastrophe and natural disasters in the RSE (Books 1 and 2), M.: Ministry of the Russian Federation for Emergencies, 1994.

14. Prevention of major accidents. Practical Guide. Developed with participation of UNEP, MBT and WHO/Transl. fr. Engl.; ed. By E.V. Petrosyans. M.: MP «Rarog», 1992. — 256 p.

15. Manual of Industrial Hazard Assessment Techniques. Office of Environmental and Scientific Affairs. The World Bank.

16. Assessment of chemical hazard of process facilities. Methodological recommendations. Novomoskovsk Advance Training Institute for Managers and Specialists of Chemical Industry, Tula, 1992.

17. IEC Standard «System reliability analysis. Analysis of failure type and consequences». Publ. 812 (1985 г.). M.: 1987.-23 p.

18. EC 1025: 1990 — Fault tree analysis (FTA) / IEC standard «Fault tree analysis », 1990.

19. GOST R 27.310-93. Analysis of types, concequences and criticality of failures. Basic provisions.

20. Provisional recommendations on the development of accident localization plans for chemical processing facilities. (Gosgortekhnadzor of the USSR, 05.07.90)

21. RD «Methodological Guide for accident risk assessment of oil-trunk pipelines». Approved by JSC «Transneft», Order № 152 of 30.12.99; agreed by Gosgortekhnadzor of Russia, letter of 07.07.99 № 10-03/418.

22. Industrial Guide for analysis and assessment of risk related to technological impacts to humans and environment due to construction and operation of facilities for mining, transportation, storage and reprocessing of hydrocarbon raw materials to improve their reliability and safety. 1st edition / RJSC «Gasprom», 1996. — 209 p.

23. Methodological Recommendations for assessment of environmental efficiency of processes /Kirillov O.T., Vorobiev A.S., Shubin K.V., LenNIIgiprokhim, 1987-39 p.

24. Guiding Principles for Chemical Accident Prevention, Preparedness and Response - Guidance for Public Authorities, Industry, Labor and Others. OECD, Paris, 1992

25. American Institute of Chemical Engineers, Center for Chemical Process Safety: various publications on chemical process safety management and risk assessment

Attachment F. List of documents

1. Convention on Safety Regime Compliance Control in the field of the Use of Nuclear Energy (Paris, 1957).
2. Convention on Third Party Liability in the Field of Nuclear Energy (with modifications by Additional Protocol of January 28, 1964, and of November 16, 1982) (Paris, 1960).
3. International Convention on Safe Containers (CSC) (Geneva, 1972).
4. Convention on Early Notification of a Nuclear. 1986.
5. Convention on Assistance in case of a Nuclear Accident or Radiological Emergency. 1986.
6. Convention on Environmental Impact Assessment in a Transboundary context. 1991.
7. Convention on Transboundary Effects of Industrial Accidents (Helsinki, 1992).
8. Convention on Nuclear Safety. 1994.
9. Convention on Civil Liability for Nuclear Damage. 1997.
10. Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management. 1998

Federal laws

1. Federal law № 116-FZ of 21.07.1997 «On Industrial Safety of Hazardous Industrial Facilities".
2. Federal law № 69-FZ of 21.12.1994 «On Fire Safety».
3. Federal law № 117-FZ of 21.07.1997 «On Safety of Hydraulic Engineering Facilities».
4. Federal law № 5154-1 of 10.06.1993 «On Standardization».
5. Federal law № 170-FZ of 21.11.1995 «On the Use of Atomic Energy».
6. Federal law № 181-FZ of 17.07.1999 «On Fundamentals Of Labor Protection in the Russian Federation».
7. Federal law № 3-FZ of 09.01.1996 «On Radiation Safety of Population».
8. Federal law № 125-FZ of 24.07.1998 «On Compulsory Social Insurance against Accidents».

9. Federal law № 52-FZ of 30.03.1999 «On Sanitary and Epidemiological Well-being of Population».
10. Federal law № 7-FZ of 10.01.2002 «On Environmental Protection».
11. Federal law № 96-FZ of 04.05.1999 «On Ambient Air Protection».
12. Federal law № 225-FZ of 30.12.1995 «On Natural Resources».
13. Federal law № 1 13-FZ of 19.07.1998 «On Hydrometeorological Service».
14. «Water Code of the Russian Federation».
15. Federal law № 174-FZ of 23.11.1995 «On Ecological Expertise».
16. Federal law № 31 –FZ of 26.02.1997 «On Preparedness Activity and Mobilization in the Russian Federation».
17. Federal law № 28-FZ of 12.02.1998 «On Civil Defense».
18. Federal law № 151-FZ of 22.08.1995 «On Emergency Rescue Services and Rescuer Status».
19. Federal law № 68-FZ of 21.12.1994 «On Protection of Population and Territories against Natural and Man-induced Emergencies».
20. «Criminal Code of the Russian Federation».
21. «Labor Code of the Russian Federation».
22. «Administrative and Procedural Code of the Russian Federation».
23. Federal law № 68-FZ of May 12, 2000, On organizations' administrative responsibility for breach of the legislation in the field of the use of atomic energy.
24. Federal law № 29-FZ of April 3, 1996, On financing of extremely radiation and nuclear hazardous industrial enterprises and facilities.

Regulatory legal acts of the President of the Russian Federation

1. № 1355 of November 12, 1992. On State Regulatory Authorities (with modifications № 710 of July 9, 1997, and № 922 of August, 7, 1998.
2. № 1923 of September 15, 1994. On priority measures for improvement of nuclear material accounting and security system.
3. № 389 of April 20, 1995. On additional measures strengthening control of compliance with environment safety requirements for spent nuclear fuel reprocessing.
4. № 166 of February 8, 1996. On improvement of nuclear fuel cycle enterprise management.

5. № 1012 of July 2, 1996. On Guarantees for Safe and Stable Functioning of Russian Federation Nuclear Power.
6. № 26 of January 21, 1997. On Federal Bodies of Executive Power Authorized for State Safety Regulation in the field of Atomic Energy.

Regulatory legal acts of the Government of the Russian Federation

1. № 505 of July 22, 1992. On Approval of Procedure for Inventory of Sites and Facilities for Mining, Transportation, Reprocessing, Application, Collection, Storage and Disposal of Radioactive Substances and Ionizing Radiation Sources on the Territory of the Russian Federation.
2. № 238 of March 7, 1995. On List of Enterprises and Organizations with Radiation and Nuclear Hazardous Facilities involved in Development, Production, Operation, Storage, Transportation, Disposition of Nuclear Weapons, Components of Nuclear Weapons, Radiation Hazardous Materials and Products (with modifications of July 27, 1996).
3. № 773 of June 29, 1995. On Approval of Procedure for Acceptance of Spent Nuclear Fuel from Foreign Nuclear Power Plants for Further Reprocessing at Russian Enterprises and Return of Radioactive Waste and Materials Generated during Reprocessing thereof.
4. № 291 of March 16, 1996. On Approval of Provisions for Procedure on Transfer of Radioactive Substances and Products thereof to and from the Russian Federation (with modification of December 27, 1996).
5. № 677 of June 11, 1996. On Measures for Implementation of Decree № 166 of the President of the Russian Federation of February 8, 1996, “On Improvement of Nuclear Fuel Cycle Enterprise Management“.
6. № 1205 of October 14, 1996. On Concept of State Nuclear Material Accounting and Control System
7. № 93 of January 28, 1997. On Procedure for Development of Radiation and Hygienic Certificates for Organizations and Territories
8. № 306 of March 14, 1997. On Decision-Making Regulations for Siting and Construction of Nuclear Installations, Radiation Sources and Storage Facilities.

9. № 392 of April 5, 1997. On Approval of Provisions for Ministry of the Russian Federation for Atomic Energy.
10. № 865 of July 14, 1997. On Approval of Provisions for Licensing in the field of the Use of Atomic Energy.
11. №1298 of October 11, 1997. On Approval of Regulations for State Accounting and Control System for Radioactive Substances and Radioactive Waste.
12. № 1511 of December 1, 1997. On approval of Provisions for development and adoption of federal standards and rules in the field of the use of atomic energy and list of federal standards and rules in the field of the use of atomic energy.
13. № 746 of July 10, 1998. On approval of Rules for state nuclear material accounting and control system.
14. № 426 of June 1, 2000. On approval of Provisions for social and hygienic monitoring.
15. № 962 of December 15, 2000. Provisions for state accounting and control of radioactive substances and radioactive waste in the Russian Federation.
16. № 204 of March 19, 2001. On state competent authority for nuclear and radiation safety under transportation of nuclear material, radioactive substances and products thereof.
17. № 265 of April 22, 2002. On approval of Provisions on Federal nuclear and radiation safety authority of Russia.

Federal standards and rules in the field of the use of atomic energy

1. General Safety Provisions for Nuclear Power Plants. OPB-88/97. NP -001-97 (PNAE G-01-011-97). Approved by Order No.9 of Gosatomnadzor of Russia of November 14, 1997. Effective as of July 1, 1998. Previous document: General Safety Provisions for Nuclear Power Plants. (OPB-88) PN AE G-1-011-89. Gosatomenergonadzor of USSR, 1990. Effective for a period of July 1,1990 - June 30, 1998.
2. Safety Rules for Nuclear Power Plant Radioactive Waste Management NP -002-97. PNAE G-14-41-97. Approved by Order No.7 of Gosatomnadzor of Russia of September 29, 1997. Effective as of July 1, 1998.
3. Provisions for Investigation Procedure and Record of Nuclear Power Plant Operation Violations. NP -004-97 (PNAE G-12-005-97). Approved by Order No.12 of Gosatomnadzor of Russia of December 19, 1997. Effective as of July 1, 1998.

4. Previous document: Provisions for Investigation Procedure and Record of Nuclear Power Plant Operation Violations. PNAE G-12-005-91. Gospromatomnadzor of USSR, Minatomenergoprom of USSR. Effective as of October 1, 1991. Provisions for procedure of emergency announcement, urgent information transmission and emergency assistance to nuclear power plants in case of radiation hazardous situations. NP-005-98.
5. Requirements to the content of safety assessment report for nuclear power plants with VVER. Reactors. NP-006-98 (PNAE G-1-036-95). Approved by Order No.7 of Gosatomnadzor of Russia of May 3, 1995. Effective on August 1, 1995. Modification №1 approved in 1996. Modification №1 of June 1, 1996.
6. Safety rules for commercial reactor decommissioning. NP-007-98. Gosatomnadzor of Russia, 1998.
7. Nuclear Safety Rules for Critical Test Bench. NP-008-98. Gosatomnadzor of Russia, 1998.
8. Nuclear Safety Rules for Research Reactors. NP-009-98. Gosatomnadzor of Russia, 1998.
9. Regulations for design and operation of confining safety systems of nuclear power plants. NP-010-98. Gosatomnadzor of Russia, 1998. Preceding document: Regulations for design and operation of confining safety systems of nuclear power plants. PNAE G-10-021-90. Approved by Order № 4 of Gospromatomnadzor of the USSR of May 4, 1990. Effective on April 1, 1991.
10. Requirements to Quality Assurance Program for Nuclear Power Plant. NP-011-99. Gosatomnadzor of Russia, 1999.
11. Safety Rules for Nuclear Power Plant Unit Decommissioning. NP-012-99. Gosatomnadzor of Russia, 1999.
12. Spent Nuclear Fuel Reprocessing Installations. Safety Requirements. NP-013-99. Gosatomnadzor of Russia, 1999.
13. Rules for Investigation Procedure and Record of Violations involving Radiation Sources and Radioactive Substances Applied in National Economy. NP-014-2000. Gosatomnadzor of Russia, 2000.

14. Standard Action Plan for Personnel Protection in Case of an Accident at Nuclear Power Plant. NP-015-2000. Minatom of Russia, Gosatomnadzor of Russia. Effective in 2000.
15. General Safety Provisions for Nuclear Fuel Cycle Facilities. NP-016-2000 (OPB OYaTTs). Gosatomnadzor of Russia, 2000.
16. Basic requirements to nuclear power plant unit life extension. NP-017-2000. Gosatomnadzor of Russia, 2000.
17. Requirements to the content of safety assessment report for nuclear power plants with BN reactors. NP-018-2000. Gosatomnadzor of Russia, 2000 .
18. Collection, reprocessing, storage and conditioning of liquid radioactive waste. Safety requirements. NP-019-2000. Gosatomnadzor of Russia, 2000.
19. Collection, reprocessing, storage and conditioning of solid radioactive waste. Safety requirements. NP-020-2000. Gosatomnadzor of Russia, 2000.
20. Gaseous Radioactive Waste Management. Safety Requirements. NP-021-2000. Gosatomnadzor of Russia, 2000.
21. Requirements to justification of nuclear facility design life extension. NP-024-2000. Gosatomnadzor of Russia, 2000.
22. Requirements to nuclear material balance zones at nuclear installations and nuclear material storage facilities. NP-025-2000. . Gosatomnadzor of Russia, 2000.
23. Provisions for Investigation Procedure and Record of Nuclear Power Plant Operation Violations. NP-027-01. Gosatomnadzor of Russia, 2001.
24. Safety Rules for Research Nuclear Installation Decommissioning. NP-028-01. Gosatomnadzor of Russia 2001.
25. Basic Rules for Nuclear Material Accounting and Control. NP-030-01. Gosatomnadzor of Russia. 2001.
26. Nuclear Power Plant Siting. Basic Safety Criteria and Requirements. NP-032-01. Approved by Order № 10 of Gosatomnadzor of Russia of November 8, 2001. Effective on April 30, 2002. Preceding document: Nuclear power plant siting. Basic safety criteria and requirements. PNAE G-03-33-93. Approved by Order № 11 of Gosatomnadzor of Russia of December 2, 1993. Effective on January 1, 1994. Preceding document: Requirements to nuclear power plant siting. 1987. Approved by Bureau of USSR Council of Ministers for fuel and energy complex (protocol № 14 of

October 22, 1987). Approved by Gosatomenergonadzor of the USSR. Effective on 01.12.1987.

27. Nuclear safety rules for reactor installations of nuclear power plants.(PBYa RU AS-89). PNAE G-1-024-90. Gospromatomnadzor of the USSR. Effective on September 1, 1990. Modification №1 of December 27, 1999.
28. Requirements to the content of safety assessment report for nuclear power plants with VVER reactors. PNAE G-1-036-95. Approved by Order № 7 of Gosatomnadzor of Russia of May 3, 1995. Effective on August 1, 1995. Modification №1 approved in 1996. Modification №1 of June 1, 1996.
29. Record of external impacts of natural and man-induced origin to nuclear and radiation hazardous facilities. PNAE G-05-035-94. Approved by Order № 4 of Gosatomnadzor of Russia of April 9, 1995. Effective on July 1, 1995.
30. Safety rules for nuclear fuel storage and transportation at nuclear facilities. (PBYa T-HT-90). PNAE G-14-029-91. Approved by Order № 12 of Gospromatomnadzor of the USSR of 31.10.1991. Effective on July 1, 1992
31. General safety provisions for research reactors. (OPB IR-94). PNAE G-16-34-94. Approved by Order № 11 of Gosatomnadzor of Russia of December 30, 1994. Effective on July 1, 1995. Amendment №1 of December 27, 1999.
32. Radiation safety standards. (NRB-99). SP 2.6.1.758-99. Minzdrav of Russia, 1999. Preceding document: Radiation safety standards NRB-76/87. 3-d edition, revised and amended. USSR Ministry of Health. Moscow ENERGOATOMIZDAT. 1988.
33. Basic sanitary rules for radiation safety (OSPORB-99). Chief State Sanitary Inspector, 29.12.1999. Preceding document: Basic sanitary rules for dealing with radioactive substances and other ionizing radiation sources. (OSP-72/87). 1987 . Minzdrav of the USSR. Amendment № 5789-91 of June 10, 1991, “Limitation of population exposure to natural ionizing radiation sources” (this document duplicates paragraph 1.4 OSP-72/87).
34. Sanitary rules for design and operation of nuclear power plants. (SP AS-99). Minzdrav of Russia. 1999. Agreed by Gosatomnadzor of Russia.
35. Sanitary rules for design and operation of research nuclear reactors. (SP 1128-73). Minzdrav of the USSR. 1973.

36. Sanitary rules for design and operation of critical test benches. (SP-KS-88). Minzdrav of the USSR. 1988.
37. Sanitary standards for nuclear enterprise and installation design (SNP-77). Minsredmash of the USSR.1978.
38. Radiation Safety Rules for Nuclear Power Plant Operation. (PRB AS-89). Minzdrav of the USSR. 1989.
39. Radiation safety rules for railway transportation of nuclear power plant fuel. PRB-88. Minzdrav of the USSR, GKAE of the USSR, Minsredmash of the USSR, MT of the USSR. 1988. Supplementary document: Safety rules for transportation of spent nuclear fuel of nuclear power plant of EAC member states. Part 1: Railway transportation. Economic Assistance Council. Executive Committee. Moscow. 1988.
40. Safety Rules for Radioactive Substance Transportation. (PBTRB -73). Minzdrav of USSR, GKAE of USSR, MIA of USSR. 1974.

References

1. GOST R ISO 14001-98 «Environmental management systems —Specification with guidance for use.»

2. GOST R ISO 14040-99 « Environmental management — Life cycle assessment — Principles and framework ».

3. RD 03-418-01. Methodical instructions on carrying out of the analysis of risk of dangerous industrial objects. // Safety of work in the industry. Gosgortekhnadzor of Russia. – 2001. №10. - P. 40-50.

4. Dow Chemical Company, Fire and Explosion Index Hazard Classification Guide, American Institute of Chemical Engineers, New York, New York, USA, 1989.

5. Statistical methods of analysis of safety of complex technical systems: Textbook/ Alexandrovskaya L.N., Aronov I.Z., Elizarov A.I. and oth.. / Edited by. Sokolov V.P. - M.: Logos, 2001. – 232 p.

6. Akimov V.A., Bodrikov O.V., Ulyanov S.V., Sorogin A.A., Glebov V.U., Elohin A.N. Methodology and the basic practical results of works by a complex estimation of risk from extreme situations natural and техногенного character for the population and territory of regions // Questions of the analysis of risk. – 2000. Book 2. №3-4. - Pp. 18-57.

7. Guidelines for Hazard Evaluation Procedures, 2nd Edition, with Worked Examples, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, U.S.A. 1992.

8. GOST 27.310-95. Reliability in technical equipment. The analysis of kinds, consequences and criticalities of refusals // Substantive provisions. Minsk: Standards Publishing House, 1996. – 19 p.

9. IEC Standard «Technic of system reliability analysis. Method of analysis of type and consequences of failures». Publication 812 (1985). Moscow: 1987.-23 p.

10. Henli E., Kumamoto X. Reliability of technical systems and estimation of risk. - M.:1984. – 387 p.

11. The International Nuclear Event Scale (INES) Users Manual, 2001 Edition, International Atomic Energy Agency, Vienna, 2001.

12. Higson, D. J., Interpretation of Risk – Criteria, Major Industrial Hazards – Technical Papers, The Warren Center for Advanced Engineering, University of Sidney, Sidney, Australia, 1986, p A3-1.

13. Council Directive 96/82/EC of December 9, 1996 on the control of major-accident hazards involving dangerous substances, Official Journal of the European Communities, No L 10, 14.1.1997, p13.

14. Bottelberghs, P. H., Risk Analysis and Safety Policy Developments in the Netherlands, Journal of Hazardous Materials, 71, 2000.

15. Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, New York, 1989, p 50.

16. Regulatory Review of Probabilistic Safety Assessment (PHA) Level 1, IAEA TECDOC-1135, International Atomic Energy Agency, Vienna, Austria, February 2000.

17. Gordon B.G. Legal and Normative basis of regulating of nuclear and radiation safety in the use of atomic energy, MIFI, Moscow, 2000.

18. Sh.Hirshberg, A.Strupchevski. Comparison of accident risks in various power systems. How acceptable are they? IAEA bulletin 41/1/1999.

19. Safety of nuclear power plants, Concern «Rosenergoatom», 1994.

20. Provisions on the procedure of accounting and investigation of violations in NPP operation, NP-004-97, Moscow, 1998.

21. Provisions on procedure of accounting and investigation of violations in operation of facilities of nuclear fuel cycle. Bulletin of Gosatomnadzor of Russia № 1(25)-2003.