
**U.S. NUCLEAR REGULATORY COMMISSION**
**OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS**
**DIVISION OF FUEL CYCLE SAFETY AND SAFEGUARDS**

# A COMPARISON OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT

**February 2011**
**Revision 1**

## Contents


EXECUTIVE SUMMARY ..... 3

INTRODUCTION AND OVERVIEW ..... 7

I. INTEGRATED SAFETY ANALYSIS BACKGROUND AND DESCRIPTION ..... 8

A. Definition of Integrated Safety Analysis ..... 8

B. Regulatory Uses of Integrated Safety Analyses ..... 8

C. Origins of Integrated Safety Analyses ..... 9

D. Development of Integrated Safety Analysis by the NRC ..... 9

E. Technical Features of an Integrated Safety Analysis ..... 10

II. PROBABILISTIC RISK ASSESSMENT BACKGROUND AND DESCRIPTION ..... 12

A. Definition of Probabilistic Risk Assessment in the Reactor Context ..... 12

B. Regulatory Status ..... 13

C. Development of Probabilistic Risk Assessment by the NRC ..... 13

D. Technical features of Probabilistic Risk Assessment ..... 14

E. Probabilistic Risk Assessment in Fuel Cycle Facilities ..... 15

III. CRITICAL EVALUATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT FOR SAFETY UNDER 10 CFR PART 70 ..... 15

IV. POTENTIAL APPLICATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT METHODS IN SIGNIFICANCE DETERMINATION FOR FUEL CYCLE OVERSIGHT ..... 20

V. EVALUATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT FOR USE IN RISK SIGNIFICANCE DETERMINATION ..... 21

SUMMARY ..... 29

REFERENCES ..... 29

## EXECUTIVE SUMMARY

Background and Introduction

The Staff Requirements Memorandum (SRM) from the Commission briefing of April 29, 2010 (Ref. 1), on revising the fuel cycle oversight program directed the staff of the U.S. Nuclear Regulatory Commission (NRC) to produce a concise paper comparing integrated safety analysis (ISA) and probabilistic risk assessment (PRA), "including a critical evaluation of how ISAs differ from PRAs." The SRM to SECY-10-0031, "Revising the Fuel Cycle Oversight Process," August 04, 2010, stated that the Commission expects the paper "to better inform proposed enhancements to the oversight process." Accordingly, this paper contains critical evaluations with respect to two different applications: (1) the intended safety purpose of ISAs under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 70, "Domestic Licensing of Special Nuclear Material," and (2) the proposed determination of risk significance in the fuel cycle oversight process.

The first evaluation is in the context of ISAs for their formal regulatory purpose within 10 CFR 70 Subpart H, "Additional Requirements for Certain Licensees Authorized To Possess a Critical Mass of Special Nuclear Material." The purpose of an ISA is to ensure that both licensees and the NRC have current and adequate information on the basis for safety of fuel cycle facilities. Section III of this paper discusses ISA and PRA with respect to this application. ISAs use quantitative PRA methods (event trees or fault trees) where applicable. Most ISAs use hazard and operability analysis (HAZOP) or other qualitative methods for accident identification, plus the risk index method of likelihood evaluation (Ref. 3). ISA's principal safety functions are identifying accidents and a set of items relied on for safety (IROFS) so that management measures are applied sufficient to assure that IROFS' safety functions support meeting the performance requirements of section 70.61. Currently approved ISA methods have been reviewed, and found to be acceptable for these purposes under Part 70. However, NRC staff reviewed only a subset of individual fuel cycle processes in detail. Therefore, approval of ISA methods does not amount to an endorsement that all analyses of all processes are correct in every respect. Rather the reviews have found reasonable assurance that ISA methods and programs were acceptable.

The second application in which ISA or PRA analysis methods are considered is in a risk significance determination process (SDP) for potential application to fuel cycle inspection findings. For this second application, quantitative risk information, as typically provided by PRA analysis, would be useful, compared to ISA risk index analysis. However, whether risk index or PRA-like analysis methods are used, ISA results often do not provide realistic estimates of accident frequencies or consequences, usually due to conservatisms. For example, some licensees do not credit all safety controls in their analyses, because the ISA only requires those controls that have been designated as IROFS and, therefore, are subject to management measures which assure their reliability and availability. Also, some consequence analyses are very conservative. This was acceptable for ISA's regulatory purposes, but is not appropriate for determining realistic risk significance. For this reason, ISA results for affected sequences related to specific inspection findings would have to be modified. Many (but not all) fuel cycle inspection findings affect only a few accident sequences. For this reason, it appears that, in such cases, it would be feasible for NRC staff to perform risk significance evaluation of these findings when they occur, provided that some supporting tools and data are developed, as described in SECY-10-0031. It is not necessary that all processes in all facilities be reanalyzed quantitatively in advance to implement such a case-by-case significance determination process. It is, however, clear that there will be situations where available methods or data are insufficient

for quantitative risk significance determination. These cases might be addressed through alternative or supplementary qualitative methods.

Integrated Safety Analysis

An ISA is a systematic analysis required by 10 CFR Part 70, Subpart H, for major fuel cycle facilities. In an ISA, a licensee must identify credible accident sequences that could lead to "high" or "intermediate" consequences as specified in 10 CFR 70.61, "Performance Requirements." The licensee's ISA must also specify the IROFS that prevent or mitigate the identified accidents and determine that the "likelihood" of these accidents meets the performance requirements of 10 CFR 70.61. The likelihoods may or may not be evaluated as numerical frequencies. The total frequencies of specified consequences to individuals are not summed over accident sequences. Licensees are then required to apply appropriate management measures to the IROFS to ensure that they are available and reliable to perform their intended safety functions when needed.

Licensees submit updated ISA summaries annually to the NRC. These summaries contain updated descriptions of methods, a list of all high and intermediate consequence accidents, and a list of IROFS. More detailed ISA information is available at fuel facility sites.

It should be noted that fuel cycle plants contain many different types of process equipment, with varying hazards and safety designs. Also, ISA methods vary among facilities. Therefore, the statements about ISAs in this paper usually apply only to certain situations and are rarely universal.

Probabilistic Risk Assessment

A PRA of nuclear power plants identifies potential accident scenarios and estimates their frequencies and consequences to obtain risk metrics. Different metrics are used in different regulatory applications. In fact, the scope, level of detail, and manner of quantification in a PRA should depend on the use to which its results will be applied. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," (Ref. 2) describes requirements for technical acceptability of a PRA. Unlike ISAs, PRA results are not directly evaluated for compliance with a regulatory performance requirement (e.g., risk limit). In one application of interest to this paper, reactor PRA has been used to produce tools for evaluating the quantitative risk significance of inspection findings. PRA technology for reactors has undergone significant development under NRC and Industry auspices. Extensive resources have been expended in developing PRA for reactors; and industry consensus standards have been established. Hence, PRA in reactor applications is much more a single, standardized technique than is ISA in fuel facility applications.

Integrated Safety Analysis and Probabilistic Risk Assessment Techniques for Assuring Safety under 10 CFR Part 70

ISAs consist of multiple analysis steps. The first stage of an ISA, identifying accident sequences, is essentially the same as would be done for a PRA. The NRC has provided guidance (Refs. 3 and 4) on the appropriate use of certain PRA techniques in ISAs. In general, licensees have followed this guidance, for example, by using event trees or fault trees for complex or quantitative analyses. But many fuel cycle processes have simple designs that do not require complex logic models.

Treatment on independence of controls may differ between an ISA and PRA. Power reactors sometimes use identical redundant components and have support systems, such as electricity, that are common to multiple safety systems. Fuel cycle processes typically do not have common support systems, and identical redundancy is uncommon. Criticality safety designs frequently comply with the industry standard of double contingency, which addresses independence. Provided that PRA techniques are used where appropriate, ISA and PRA should be comparably effective in the accident identification phase.

One difference between ISA and PRA in the context of safety is the treatment of the likelihood of accident sequences. For example, ISAs require that high-consequence accident sequences be shown to be "highly unlikely." This could be done by providing a reasonable best estimate of quantitative accident frequencies, and consequences. Although useful, a fully quantitative evaluation is not required. The demonstration that high-consequence accident sequences are highly unlikely could be made by using either qualitative or quantitative criteria, provided they are reasonably effective and objective. PRA aims to produce a reasonable quantitative estimate of a risk metric appropriate to its application. This typically requires a realistic frequency for each accident sequence needed. As part of ISA likelihood evaluations, most licensees have either quantified accident frequencies or applied the risk index method (see Ref. 3, Chapter 3, Appendix A); but these evaluations may be conservative rather than realistic. NRC staff licensing reviews have determined the acceptability of each licensee's criteria for likelihoods. Lessons learned about likelihood evaluation, based on ongoing ISAs and reviews, have resulted in staff guidance that is now incorporated as appendices to Chapter 3 of NUREG-1520, Revision 1 (Ref. 3). In individual instances, use of the ISA risk index method of likelihood evaluation, which is only an approximate method, could diverge significantly from a more realistic quantitative evaluation. Such instances, when found during reviews or inspections, have been corrected. Section III of this paper discusses the use of PRA techniques in ISAs, including each of the specific technical features mentioned in the SRM (Ref. 1).

Integrated Safety Analysis and Probabilistic Risk Assessment Techniques for Determining the Risk Significance of Inspection Findings

Section V of this paper describes one example of a hypothetical inspection finding in a typical fuel cycle process. The frequencies of accident sequences in this process are analyzed using two methods: the risk index method common in ISAs, and a fully quantitative, PRA-like method. The risk significance of the impact of the deficiency found during inspection is then quantified using both sources of frequency information. This example then is used as a reference point to discuss the differences between ISA and certain PRA methods that might be applied in this context. It should be noted that this type of quantitative risk significance determination is only applicable to ISA-related inspection areas, such as criticality, chemical, and radiological accident safety, and is not envisioned for application to other inspection areas, such as security or radiation protection under 10 CFR Part 20, "Standards for Protection Against Radiation." These other areas use significance determination criteria different from ISA-related safety. Although it appears feasible to conduct quantitative risk significance evaluations for many types of accident situations, it remains to be determined how to address situations where quantitative methods or data are unavailable. Unlike reactor PRAs, NRC has not developed methods and data for risk assessment of fuel cycle accidents. For this reason, it may be necessary to supplement a quantitative method, like that illustrated by the example in Section V, with more qualitative, but objective, criteria for significance classification.

Because many fuel cycle process designs are simple and involve only a few accident sequences, NRC staff would often be able to perform such evaluations of inspection findings.

Some data and tool development is likely needed to support such staff analyses. In any case, instances where methods or data are insufficient to assess risk are likely to occur.

Based on a survey of recent inspection results, there would be only about two quantitative evaluations required per plant per year. Thus, pre-evaluation of all sequences for all processes is not efficient compared to case-by-case evaluation.

## INTRODUCTION AND OVERVIEW

In the SRM presented at the Commission briefing held on April 29, 2010 (Ref. 1), the Commission directed staff to prepare a paper on ISA and PRA, "including a critical evaluation of how ISAs differ from PRAs." The SRM also directed that the comparison address specific technical features, such as end states, hardware failures, human errors, and accident sequence quantification.

To provide a general background, Section I of this paper describes ISAs, and Section II, PRAs. A "critical evaluation" implies a determination of adequacy for some specific purpose. That is, the adequacy or value of a method of analysis depends on its purpose or application. Therefore, Sections III and V contain critical evaluations of ISA and PRA, specifically with respect to their use for two particular applications:

(1) complying with 10 CFR Part 70 and acceptable safety (Section III)

(2) performing risk significance determination to support a risk-informed fuel cycle oversight process (Section V)

One difficulty in characterizing ISAs is that fuel facilities consist of many processes, each with its own hazards and control design. In addition, licensees use different analysis methods. Statements about ISAs in this paper recognize this variability, which is much greater than that between different reactor PRAs. For example, NRC guidance in NUREG-1520 (Ref. 3) and NUREG-1513, "Integrated Safety Analysis Guidance Document," issued May 2001 (Ref. 4) recommends PRA-like event trees and fault trees for complex designs or quantitative results. Two licensees use these PRA methods and quantify accident frequencies. Most of the other licensees use the semi-quantitative risk index method of NUREG-1520, using fault trees only for more complex situations.

The first phase of ISA is the identification of accident sequences. This is essentially the same as the initial phase of PRA. Thus, the main differences between the formal methods of ISA and PRA are accident sequence quantification and the use of combined metrics of risk. Because ISA's use PRA methods, the ISA versus PRA dichotomy is not as clean as it may sound.

This paper discusses features of ISA and PRA in two different contexts: safety assurance (in Section III) and risk significance determination (in Section V). Section V uses an example risk significance analysis as a starting point for discussion. This example creates a somewhat artificial ISA-PRA dichotomy by comparing: (1) use of an ISA with quantified event trees as in PRA; to (2) use of an ISA with the risk index method. The example then uses information from these analyses to evaluate risk significance.

The results of the Section III evaluation of compliance and safety are the following:

(1) Licensees have generally applied PRA methods for appropriate situations in the accident identification phase of ISAs.

(2) The staff performed an extensive review of ISAs of current licensees and found them acceptable to provide reasonable assurance of safe design and operation in the context of 10 CFR Part 70, Subpart H.

The results of the evaluation in Section V indicate that, in principle, it is feasible to use ISA results, supplemented in specific cases by additional information, as a starting point to estimate the quantitative risk significance of inspection findings. In particular cases, the desired data or assessment tools may not be available because development of such for fuel cycle processes has not been as extensive as for PRAs. Also, ISA results must be used with caution for estimating quantitative risk significance, as they have not been conducted for this purpose. This is true even if quantitative accident frequencies have been evaluated in the ISA, because such evaluations may be conservative. The NRC staff could often perform quantitative significance evaluations like the example in Section V for each inspection finding when it occurs. There would be no need to develop quantitative frequencies for all facility accident sequences in advance, since each deficiency would typically affect only a few sequences.

Basis for Evaluation of Integrated Safety Analyses

Each fuel cycle facility typically contains many processes with diverse hazards, such as toxic chemicals, fissile materials that could inadvertently be made critical, radioactive materials, and fire and explosion hazards. For this reason, multidisciplinary teams, not only the ISA and PRA expert, perform and review ISAs. Because of the large number of processes, the NRC review teams select a subset of process for detailed review. These detailed reviews typically include system walkdowns and interviews of system engineers during site visits. NRC staff ISA reviews produce technical evaluation reports that make findings on the facility's compliance with the regulations. However, the reports typically do not address the kinds of methods comparison evaluations this paper is undertaking. Consequently, in order to evaluate ISAs for this paper, it has been necessary to base generalizations about ISAs on consultation with a number of experienced NRC ISA review team members.

## I. INTEGRATED SAFETY ANALYSIS BACKGROUND AND DESCRIPTION

### A. Definition of Integrated Safety Analysis

In 10 CFR 70.62(c), the NRC defines ISA as a systematic analysis, required for major fuel cycle facilities, that identifies hazards, accident sequences, their consequences, likelihoods, and IROFS. The rule does not mandate specific methods for performing such analysis, but guidance appears in NUREG-1520 and NUREG-1513 (Refs. 3 and 4).

### B. Regulatory Uses of Integrated Safety Analyses

Performance Requirements

ISAs are directly used for compliance with the performance requirements in 10 CFR 70.61. The ISA is to identify all event sequences that could lead to high- or intermediate-consequence events, as defined in the regulation. The regulation specifies that high-consequence events must be highly unlikely, and intermediate-consequence events must be unlikely. The terms "highly unlikely" and "unlikely" must be defined by the licensee and reviewed and approved by NRC staff in accordance with the Standard Review Plan (SRP) (Ref. 3). In addition, 10 CFR 70.61 requires that processes be subcritical for all normal and credible abnormal conditions, with preventive controls as the primary means of protection. This regulatory use of ISA differs from PRAs, which are used to inform decisions but not directly to demonstrate compliance with criteria specified by regulation.

Identification of Items Relied on for Safety

The ISA process identifies a set of IROFS. When a structure, system, or component (SSC) is designated as an IROFS, certain regulatory requirements become applicable. These requirements include that the IROFS be sufficient to meet the likelihood and consequence requirements of 10 CFR 70.61. In addition, management measures must be applied to assure that IROFS are available and reliable. Changes to IROFS must be reported to the NRC annually.

Other Applications of Integrated Safety Analysis Results

ISA results have sometimes been used for applications other than compliance with the regulation, a licensing function. For example, ISA results were used by the staff to prioritize IROFS to be inspected during the operational readiness reviews of the gas centrifuge enrichment plants. In addition, the licensees provide annual updates to their ISA summaries with IROFS lists, and maintain failure logs that are useful in guiding regular inspections. The staff is currently revising inspection and enforcement guidance to make more effective use of ISA information.

## C. Origins of Integrated Safety Analyses

After two serious incidents in 1988 and 1991 at fuel cycle facilities, one of them a fatality caused by chemical effects, the NRC staff considered various possible regulatory reforms. The NRC decided to produce a new rule, Subpart H of 10 CFR Part 70 that brought chemical effects under NRC jurisdiction and required ISAs. The Statements of Consideration (Ref. 5) for this rule included the following statement about quantitative definitions of likelihood:

> However, the Commission has decided not to include quantitative definitions of ‘‘unlikely’’ and ‘‘highly unlikely’’ in the proposed rule, because a single definition for each term, that would apply to all the facilities regulated by Part 70, may not be appropriate.

After the rule became final, the NRC issued NUREG-1520 and NUREG-1513 (Refs. 3 and 4), which provided guidance on ISA methods, including likelihood evaluation and choice of systematic methods for identifying accidents based on the type of process to be analyzed. NUREG-1513 (Ref. 4) recommended use of PRA event tree and fault tree methods for complex control systems or when a quantitative evaluation of accident frequencies is needed. Two out of the nine ISAs performed to date made extensive use of such quantitative methods.

## D. Development of Integrated Safety Analysis by the NRC

NRC participation in the development of ISA methods was minimal. The agency adapted NUREG-1520 and NUREG-1513 (Refs. 3 and 4) from the chemical and nuclear reactor industries. The techniques recommended in NUREG-1513 (Ref. 4) are largely based on methods developed for compliance with the chemical safety requirements of the Occupational Safety and Health Act of 1970 (OSHA). In part, this was done to “complement and be consistent with the parallel OSHA and Environmental Protection Agency requirements,” according to the Statements of Consideration (Ref. 5) for Subpart H. As fuel cycle facilities performed the ISAs, questions arose about ISA methods, including evaluation of likelihood. These questions were discussed in workshops, and the NRC staff developed interim staff guidance (ISG) documents that are now incorporated as appendices to Chapter 3 of

NUREG-1520 (Ref. 3). Although SRPs provide limited example analyses, NRC staff and contractors did not perform extensive ISA models, as was done for reactor PRA.

## E. Technical Features of an Integrated Safety Analysis

The SRM from the Commission briefing on April 29, 2010, directed that ISA be compared to PRA with respect to certain technical features. This section describes how these features are dealt with in ISA; Section II describes the features in PRA. Section III provides a comparative evaluation of ISA and PRA with respect to safety and compliance under 10 CFR Part 70.

### End States

End states of accident sequences are defined in 10 CFR 70.61 as high or intermediate consequences. Specifically, "high" and "intermediate" are defined in terms of rem for radiation doses, and by qualitative criteria, such as "endanger the life," for chemical health effects. Different criteria are specified for workers and persons outside the controlled area. Most accident sequences that are identified in ISAs as exceeding these consequence thresholds involve consequences to the workers rather than the public. Relatively few accidents exceed the consequence levels of the rule for persons off site because of the distances involved and, often, the limited size of potential chemical or radiological source terms. Most of the hypothetical accidents listed in the ISAs are inadvertent nuclear criticality accidents. This is because fissile material is found throughout the facilities. The end state of a criticality accident sequence could be fatal for workers close to the accident location or a subacute dose to workers further away. Similarly, accident sequences whose end state is release of a toxic chemical could result in worker fatality or lesser effects depending on the direction and distance of the plume. Given such onsite events, ISAs typically assume that high consequences result and apply IROFS sufficient to make the event highly unlikely, rather than calculating consequences realistically. Offsite, consequences are more likely to be evaluated quantitatively. These offsite consequence evaluations are typically "worst case" rather than realistic estimates. In ISAs, total frequencies of fatality to individuals are not summed over all accidents.

### Accident Sequences Leading to End States

ISAs must identify all potential accident sequences that could result in the end state consequences defined in 10 CFR 70.61. This is accomplished by using a variety of methods (depending on the nature of the process and safety design being analyzed), including hazard and operability analysis, what-if checklists, fault trees, and event trees. Licensees list all of these sequences in the ISA summary submitted to the NRC and update them annually. Any credible event exceeding the consequence levels of the rule, whether hardware failure or human error, must be addressed in this accident identification task. All hazards, both internal and external to plant processes, must be considered. Event sequences may be screened out of the eventual list submitted to the NRC on the grounds that they cannot produce the consequences specified in the rule or are not credible. NUREG-1520 (Ref. 3) contains guidance on credibility.

### Hardware Failures and Human Errors

ISAs model both hardware failures and human errors. Hardware IROFS are usually identified at the subsystem rather than component level. For example, an IROFS could be defined as "an automatic control that stops a process given detection of a temperature out of range." ISAs

using the risk index method generally assign indices based on simple qualitative criteria, such as passive, active, or administrative control (human error). Quantitative ISAs use more specific hardware descriptions, such as internal valve leaks, to assign failure and error frequencies and probabilities of failure on demand. These values are typically taken from generic data sources (for example, see Refs. 6 and 7). Human error probabilities might also be estimated based on plant experience. Human reliability modeling is typically not applied.

Physical and Chemical Phenomena

All phenomena that could produce the consequences specified in 10 CFR 70.61 must be considered. However, except for calculating chemical and radiation exposures, physical and chemical phenomena involved in fuel cycle accidents usually do not require modeling or calculation to achieve the purposes of the ISA. For example, the magnitudes of criticality accidents can vary, depending on the initiating sequence of events. However, the ISA usually assumes that, if a criticality occurs, high consequences could result. Calculating total risk to individuals, as in a PRA, would require more detailed quantitative modeling of such phenomena, including estimating probabilistic variations in the magnitude and locations of the accidents.

Fires and External Hazards

Fires and external hazards are evaluated as accidents in ISAs as initiating events potentially leading to either a radiological or chemical release. Chapter 7 of the SRP (Ref. 3) specifically addresses fire safety. Fire safety is one of the technical disciplines normally represented on each ISA team. By rule, ISAs must consider external hazards as well as fire. The impact of fires, chemical releases, explosions, and similar events on the safety of processes other than those in which the event occurred must also be considered.

Plume Dispersion

For most scenarios, ISAs use worst-case dispersion to determine if the offsite radiological or chemical thresholds of 10 CFR 70.61 are exceeded. Typical assumptions include stability class F, low wind speed, no heavy gas model, and no plume rise. Consequently, the magnitude of the doses is not an average or typical case but a worst case. Probabilistic weather averaging, as in the MELCOR Accident Consequence Code System (MACCS) code used for PRAs, is not used. This conservatism would have to be removed in order to obtain realistic risk significance.

Guidance on determining worker doses from chemical or radiological releases in confined areas appears in NUREG/CR-6410, “Nuclear Fuel Cycle Facility Accident Analysis Handbook,” issued March 1998 (Ref. 8). However, in many cases such releases are simply assumed to produce high-consequence doses as defined in 10 CFR 70.61.

Quantification of Accident Sequences

Two of the approved ISAs quantify accident sequence frequencies. One ISA has no form of quantification but applies qualitative criteria to assure that IROFS are suitably reliable. The rest use a risk index method, which could be called semi-quantitative, similar to that described in Appendix A to Chapter 3 of the SRP (Ref. 3). Worker doses, if not calculated, are usually conservatively assumed to be high consequences. Offsite doses are often calculated conservatively using computer codes in order to determine if the regulatory thresholds are

exceeded. These calculations are not probabilistically averaged over weather conditions. They are typically for worst-case source terms and weather. Not all ISA assessments are conservative, but, if used are acceptable for assurance of safety under 10 CFR Part 70, Subpart H. On the other hand, for quantitative risk significance determination, ISA results with conservatisms might have to be adjusted if they would yield incorrect results in this application.

Uncertainties in Physical and Chemical Phenomena

ISAs usually handle uncertainties in accident phenomena by making conservative assumptions. These uncertainties are not modeled probabilistically to estimate known variations. Epistemic uncertainties, as opposed to variations, exist in the initiation of some types of chemical accidents, such as unanticipated chemical reactions, gas evolution, or precipitations. Thus, rare events of these types are difficult to assess.

Importance Measures

In an ISA, licensees do not routinely calculate importance measures, such as relative change in risk given that an IROFS failure probability is set to 1.0. Importance measures have been evaluated and used by NRC staff in a few applications, such as prioritizing which IROFS should receive more attention in inspections. A risk-significance metric has also been considered for use in determining the risk significance of inspection findings. (This significance metric is explained in the example in Section V.)

## II. PROBABILISTIC RISK ASSESSMENT BACKGROUND AND DESCRIPTION

### A. Definition of Probabilistic Risk Assessment in the Reactor Context

PRA is a systematic methodology to evaluate risks. Risk, in this context, refers to both probabilities and consequences of unintentional adverse events (i.e. accidents). In the NRC context, PRA has been applied to some NRC regulated nuclear activities, including all nuclear power reactors. PRA involves identifying potential accidents and quantifying the magnitude of their consequences and their probability or frequency of occurrence. Consequences are expressed numerically (e.g., the number of early fatalities or dollar cost impacts of the accident), and likelihoods of occurrence are usually expressed as frequencies. Collective risk metrics, such as the expected value of cost impacts, are calculated by summing the products of each accident's consequences (dollars) and its frequency. Large early release frequency (LERF) is another risk metric often used in reactor PRA applications. LERF is a metric, of frequency; but it is associated with the understood consequences of a large early release. To obtain the LERF, the PRA must sum the frequencies of all sequences of initiating events and mitigating system failures that lead to a large early release. Each type of risk metric is useful for different types of applications and gives different insights.

For NRC-regulated reactors, three levels of PRA are defined based on the attributes of the accident progression:

(1) Level 1 evaluates the sum of all the accident sequences that can lead to irreversible damage to the reactor core. Its output is expressed as the frequency of core damage.

(2) Level 2 focuses on the accident sequences that, following core damage, can lead to failure or bypass of the reactor containment. Its output is the frequency of radiological release from reactor containment to the environment (of which LERF is a subset).

(3) Level 3 assesses the transport of the released radiation through the atmosphere and its impact on the offsite population and the environment. Its results are expressed through the frequency of total population dose (person-rem) and the offsite health and economic consequences. The level of detail, complexity, and quantification in a PRA can vary depending on the purposes to which its results are applied, and the complexity of the phenomena that must be modeled.

## B. Regulatory Status

In the United States, PRA use is guided by the PRA policy statement of 1995 (Ref. 9) and various regulatory guides that describe the use of PRA results for risk management (e.g., Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," (Ref. 10) and Regulatory Guide 1.200 (Ref. 2)). Although PRA is not required by regulation in the licensing and oversight of current light-water reactors, decisions are often informed by the results of PRAs. Licensing technical reviewers review licensee risk analyses submitted in support of license amendment requests. For fire protection, licensees have the option of using PRA technology or a more conventional deterministic and prescriptive approach to meet the current requirements. The entire current fleet of nuclear power plants (NPP) carried out PRAs under the NRC's Individual Plant Examination (IPE) for Severe Accident Vulnerabilities Program. For future reactors licensed under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," a description and results of the PRA are required. Overall, the uses of PRA have increased and matured over the past 35 years, not only in the United States but also worldwide. Professional organizations have developed standards of requirements for PRAs, and the NRC has endorsed these standards. PRAs are used for various purposes in NRC regulatory activities, including risk-informing licensing actions, assessing the risk significance of inspection findings, and severe accident mitigation alternatives analysis performed under 10 CFR 51.53, "Post-construction Environmental Reports," as part of applications for license renewal.

## C. Development of Probabilistic Risk Assessment by the NRC

Over the past four decades, the NRC and the nuclear industry have made a large investment in PRA development and application. In 1975, the landmark "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" (WASH-1400, NUREG-75/014 (Ref. 11)), established the fundamental paradigm for all subsequent PRAs. Over the years, the NRC and its contractors performed a series of studies (the Reactor Safety Study Methodology Application Program, the Integrated Reliability Evaluation Program, and NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," issued December 1990 (Ref. 12)) and guided the industry to perform studies as well, notably IPEs for internal events and the equivalent for external events. The industry also performed major PRAs in the aftermath of the Three Mile Island Unit 2 accident (such as for the Zion, Indian Point, Limerick, and Seabrook plants).

More recently, the NRC developed (and currently maintains) a set of PRA models for all operating U.S. commercial nuclear power plants. The staff uses these standardized plant analysis risk (SPAR) models—most of which are Level 1 models addressing internal events that may occur during at-power operation—to support risk-informed decision making. For example, the accident sequence precursor program uses the SPAR models to help provide a comprehensive, risk-based view of NPP operating experience and a measure for trending core damage risk. The reactor oversight program uses PRA results to support the agency's SDP. In addition to performing PRAs, the NRC has supported substantial work on developing the many

elements of a PRA. This development work included major programs on severe accident analysis, human reliability, database development, seismic behavior, uncertainty analysis, internal fires and floods, data analysis, and initiating event analysis.

### D. Technical Features of a Probabilistic Risk Analysis

The end states and scope of PRAs vary, depending on the application of the results. The scope of a particular PRA application requires analysis of all operating modes and initiators that significantly affect the required risk metric. Section II.A of this document described two of these risk metrics (and hence end states). PRAs model accident sequences leading to the end states within the scope of the particular application that is using the PRA results. Within a particular scope, reactor PRAs aims to be complete in terms of the spectrum of potential initiating events and accident scenarios. This includes consideration of hardware failure rates and human error probabilities at a level of detail sufficient for quantification. Human reliability methods developed under NRC auspices have been applied to estimate operator error probabilities in scenarios requiring operator action.

Certain physical phenomena in reactor accident sequences need to be modeled in PRA sufficient to allow quantification of outcomes. For example, pressure and temperature challenges that accidents pose to containment must be quantified. For example, if releases from containment occur in a hypothetical sequence, the timing and amounts of isotopes released need to be quantified in order to determine offsite doses.

Fires and other external challenges to safety systems are typically modeled in complete reactor PRAs.

Plume dispersion is modeled realistically, considering probabilistic variations of weather in Level 3 PRAs.

PRAs quantify frequencies of accident sequences using computer codes that incorporate a variety of probabilistic models, such as event trees, fault trees, and reliability equations. Event trees and fault trees will later be referred to as they are used in some ISAs. This is not to equate event tree/fault tree modeling with PRA, but these are one pair of PRA techniques that can be useful for ISA. Applicable input for quantifying these modes is available from the extensive database of hardware failures for the existing reactor fleet. More recently, quantitative probability models other than the standard event tree/fault tree approach have been applied.

Uncertainty analyses have been performed for PRAs, but not universally. Importance measures have been developed and applied in some cases to facilitate such insights as identifying dominant risks or vulnerabilities.

Typically, PRAs search for potential dependencies, common-cause failures, and systems interactions. Explicit methods and data for modeling dependencies in hardware have been developed and applied in PRAs. Similarly, human error models developed for reactor applications have explicit consideration of dependency between human errors.

In sum, PRAs of reactors strive to provide a realistic quantitative calculation of risk metrics appropriate to their application and scope.

## E. Probabilistic Risk Assessment in Fuel Cycle Facilities

No facility wide PRAs have been carried out for fuel cycle facilities in the United States. Some recent, limited work focused on particular accidents, such as the risk of red oil excursions in the mixed-oxide facility under construction at the Savannah River Site. This limited analysis identified common-cause failures and human errors as the major contributors. Compared to nuclear power plants, a wider range of hazards is posed by fuel cycle plants, including toxic chemicals, explosions, hazardous chemical reactions, radiological releases, and inadvertent nuclear criticality accidents. In most fuel cycle accident scenarios, facility workers are the receptors. The fuel cycle facility geometry of multiple sources and multiple receptors differs from the reactor geometry.

Dedicated standby safety systems, as in reactors, are not the most common type of controls. Instead, process safety designs rely more on normal operating systems, operator actions, and passive features to cope with abnormal conditions. This is more analogous to nuclear power plants in low-power shutdown mode. Individual processes are characterized by many unique process and operations aspects, especially with respect to the diversity of human actions that are involved. Since PRA has not been performed for these plants, it remains to be seen what difficulties might arise in attempting to represent the system's processes and functions in sufficient detail to quantify end states realistically.

While PRA methodology can be used to estimate the overall likelihood of undesirable consequences (as defined in the PRA model), an additional important strength of PRA is the ability to better understand and rank the relative importance of each modeled component, system, or event. Such understanding can aid in several regulatory processes, including prioritizing licensing reviews, focusing inspection and routine oversight, and evaluating the significance of equipment failures or other events. It should also be noted that the traditional use in PRA of event trees and fault trees can present challenges to modeling process systems like those that exist at fuel cycle facilities. However, other PRA methods may be more suitable for such systems and are also available.

# III. CRITICAL EVALUATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT FOR SAFETY UNDER 10 CFR PART 70

This section discusses and evaluates current ISA methods and how they relate to methods used in PRA, with respect to the objectives of ISA under 10 CFR Part 70, Subpart H, to assure acceptable safety.

As previously indicated, some licensees use some PRA techniques in the ISAs. In principle, the desired results of the first phase of ISA or PRA are the same: identifying all relevant accident sequences. Therefore, methods should be used that are effective for this purpose. The NRC has provided guidance (Refs. 3 and 4) that includes recommended uses of the PRA techniques of fault trees and event trees for this purpose where appropriate. Generally, fuel cycle licensees have followed this recommendation.

Once the first phase (accident identification) is complete, ISAs must evaluate compliance with the performance criteria of 10 CFR 70.61. The objective is to attain reasonable assurance that the set of IROFS limiting the likelihood or consequence of each accident sequence is adequate. To provide this assurance, a quantification of sequence frequencies may or may not be used. Some PRA methods are useful for quantification of accident frequencies and consequences in

the ISA context. The extent to which application of such PRA techniques is needed or useful for the safety function of ISAs is discussed below.

The first ISAs were initiated in the early 1990s for plants that had already been operating for two decades. ISAs were not mandatory until Subpart H of 10 CFR Part 70 became final in 2000, but, in several cases, they had been started before this date. Consequently, the industry and the NRC have some years of experience with this process. A draft SRP and ISA guidance document were available when the rule was promulgated. The NRC staff and affected licensees had extensive interaction concerning these documents, and the agency issued them shortly after the rule. Over the next four years, all of the existing licensees subject to subpart H to Part 70 completed their initial ISAs for the purpose of compliance.

During the performance of the ISAs, issues and questions of interpretation arose. The NRC held workshops and produced ISG documents addressing the issues. Specifically, the NRC developed guidance on the treatment of initiating events, external events, dependencies, and quantification of accident frequencies. This guidance has been incorporated into Revision 1 to the SRP (Ref. 3, Chapter 3).

By late 2004, ISAs of existing facilities were complete. These initial ISAs were reviewed by teams of NRC staff knowledgeable in the relevant technical disciplines, including ISA techniques. As a result of these reviews, some new issues arose, usually specific to a particular licensee or process analysis. These issues were resolved, and the initial ISAs were approved as acceptable for safety, with the last approval issued in late 2008. Subsequently, ISAs have been updated annually by licensees and are subject to inspection. Thus there is a continuing process of learning and improvement to ISAs that addresses many of the theoretical weaknesses of some ISA methods relative to PRA.

Hazards at Fuel Cycle Facilities

The nature and magnitude of hazards at fuel cycle facilities governed by the ISA requirement differ markedly from nuclear reactors. The designs of some types of safety controls are also quite different both from reactors and among processes within a facility. Principal hazards include toxic chemicals and fissile materials with the potential for inadvertent criticality. Radiological sources are, except for plutonium facilities, of very low magnitude. Thus, except for a few large chemical sources, most hazards do not pose a significant risk to members of the public offsite. Toxic chemicals are typically controlled through careful and robust containment. Criticality is often controlled by use of passive safe geometry equipment, such as that described in the example in Section V below. For low-enriched uranium facilities, criticality can be controlled by independent controls on mass and moderation. Automatic controls are relatively uncommon, as is dependence on power or other active support systems.

Completeness in Identifying Accident Sequences

One potential problem in ISA or PRA is overlooking a potential accident. Instances of this have occurred in fuel cycle ISAs because the analysts either had not thought of a particular scenario or had incorrectly screened it out as not credible. However, these instances have not usually been a result of methodological differences between ISAs and PRAs.

Under 10 CFR Part 70, the objective is to identify sequences and apply IROFS sufficient to limit risk, not to estimate risk per se. NRC staff reviews and oversight of ISAs have, so far,

concluded that the ISAs have accomplished this objective overall and so have performed their function in the safety regulatory program required by 10 CFR Part 70.

Establishing Adequate Controls for Safety

Although ISAs do not necessarily provide quantitative estimates of IROFS failure rates and probabilities, the regulation does state that likelihoods of consequential events are to be made appropriately unlikely, hence acceptably safe. The ways that accidents and IROFS identified in ISAs are managed under the requirements of the rule provide this assurance of safety. The reasons why ISAs are sufficient for this purpose are discussed here. In 10 CFR Part 70, the NRC requires that accident sequences be evaluated and shown to comply with the performance requirements of 10 CFR 70.61. For example, high-consequence events must be highly unlikely. Typically, this evaluation has been done using either quantitative frequency assessment or the risk index method. The SRP contains guidance on performing such likelihood evaluations, including those that are purely qualitative. A rigorous and realistic application of this guidance will usually be sufficient to assure that the basic safety design of a process is capable of being sufficiently reliable. More importantly, 10 CFR 70.62, "Safety Program and Integrated Safety Analysis," requires that "management measures" be applied to each IROFS to ensure that it is sufficiently reliable and available. Thus, in addition to a capable design, safety is assured by the practices required under 10 CFR Part 70. Required practices beyond management measures are listed as "baseline design criteria" in 10 CFR 70.64, "Requirements for New Facilities or New Processes at Existing Facilities," which are made mandatory for safety designs of new facilities or processes.

Another practice that contributes to the assurance that process designs provide acceptable safety is the use of conservatism in assessing both the consequences and the likelihoods of accidents in ISAs. For example, chemical releases and criticality accidents are usually assumed to result in high consequences, even though this would not be so in many cases. Some licensees apply safety controls beyond the minimum number required to demonstrate compliance with 10 CFR 70.61. ISA assessments of accident sequences, if conservative, support assurance that safety designs are acceptable and robust. However, it should be remembered that other features of licensee safety programs, such as the management measures and baseline design criteria of 10 CFR Part 70, also help ensure that controls are adequately reliable.

The following paragraphs discuss some specific technical differences between ISAs and PRAs that might affect the complete identification of accidents or the adequacy of controls.

Process Interactions

One challenge to assuring safety is to identify interactions between processes that may cause problems. This may happen when an upset in one process impacts other processes, or when safety features that address different hazards interact. The classic cases are: (1) fire suppression that uses water providing moderator that could facilitate a criticality accident; and (2) chemical accidents affecting adjacent processes. The regulations explicitly require that ISAs analyze these types of interactions. In fact, this is what is meant by "integrated" in the term ISA. Another type of interaction is the erroneous transfer of undesired material between processes. This challenge requires communication of the results of one process ISA to others.

However, in practice, many fuel cycle processes are reasonably isolated from one another because plants are operated in batch mode.

Common Cause and Dependencies

For redundant hardware safety controls, the risk index method described in the original SRP had not explicitly recommended a method of common-cause correction like the beta factor method used in PRAs. However, the issue of the independence of controls arose early during performance of the ISAs, and NRC staff provided guidance in ISG-1, which has now been incorporated into Chapter 3 of the revised SRP (Ref. 3). Facility methods of modeling identical redundancy vary, from taking no credit for the second control to applying a dependency factor, as in the beta factor method. Licensees are very aware of common-cause and dependency issues because of the prominence of the "double contingency principle" in the basic American National Standards Institute/American Nuclear Society (ANSI/ANS) criticality safety standard, ANSI/ANS 8.1 (Ref. 13). A commitment to apply the double contingency principle is often part of a fuel facility license.

Independence of human actions was another area of NRC-industry discussion. Appendix B to Chapter 3 of NUREG-1520 (Ref. 3) provides some guidance on this issue. As ISAs do not model human error in detail, there is a potential for dependencies to be overlooked.

Integrated Safety Analysis Personnel Issues

One licensee who applied PRA techniques to ISAs discussed this process in a paper, "Applying Nuclear PRA to a Nuclear Fuel Cycle Facility Integrated Safety Analysis," presented at Probabilistic Safety Assessment and Management Conference 10 in June 2010 (Ref. 14). The NRC staff concurs with many of the evaluative statements in this paper. In particular, the paper points out the challenge that plant staff familiar with the safety design of processes are usually not familiar with PRA or ISA techniques. On the other hand, it takes time for PRA experts to become familiar with fuel facility hazards and processes because of their large number and diversity. This dichotomy of personnel experience may have more influence on ISA results than purely methodological ISA and PRA issues.

Table 1, summarizes each of the ISA and PRA technical features mentioned in the SRM in the context of whether a more PRA-like analysis would produce a better ISA result with respect to the ISA's regulatory function of assuring safety.

**Table 1 Evaluation of ISA-PRA Differences for Fuel Cycle Safety**

| Technical Features or Topics | ISA | Hypothetical PRA for Fuel Cycle | Implication for Safety or Compliance |
|---|---|---|---|
| End states | high or intermediate consequences (see 10 CFR 70.61) | could use more refined consequences than found in the ISA | 10 CFR Section 70.61 acceptable for current facilities, may need to be supplemented for risk significance determinations |
| Completeness of accident sequences | uses various systematic methods | uses various systematic methods | In principle no difference. |
| Quantification of accident sequences | a few ISAs are quantified, most use risk index method of Ref. 3, chap. 3 | Quantified accident sequences frequencies | ISAs generally acceptable. Quantification might be helpful in marginal cases. |
| Modeling of physical/chemical phenomena | ISAs often use conservative assumptions | PRA could quantify some phenomena | ISAs generally conservative, which is acceptable. Some accidents may be mis-categorized due to lack of quantitative understanding of a phenomenon. |
| Offsite consequences | ISAs use bounding weather assumptions | Level 3 PRAs use realistic statistical consequences | conservative approach is adequate for safety, PRA might allow relaxations in some cases |
| Internal fire modeling | ISAs always consider fire scenarios and interactions | PRA not necessarily different | in principle no difference, except ISA assessment is usually not quantitative. |
| Level of detail in modeling | ISAs often use simplified models | PRA could have more detail | detail is not usually needed for safety; but detail may lead to better understanding. |
| Treatment of hardware failures | hardware failures are addressed at subsystem level. | often more detail in models | detail may provide better understanding of failure likelihood. |
| Treatment of human errors | some ISAs are simplistic and have only one value for human error | PRA could attempt modeling, but basis may not exist for many scenarios | this is an undeveloped area for some situations that occur at fuel facilities. |
| Completeness of safety control systems analyzed | some ISAs do not take credit for all safety controls as IROFS | PRA would credit additional controls besides those credited as IROFS | not crediting all controls is acceptable for assuring at least minimal safety under 70.61, but other safety principles may apply. |

| Technical Features or Topics | ISA | Hypothetical PRA for Fuel Cycle | Implication for Safety or Compliance |
|---|---|---|---|
| Treatment of dependency and system interactions | dependencies considered in double[1] contingency analysis, sometimes quantitatively | PRA explicitly model dependencies across multiple systems. | in principle, no difference, but risk index method does not have dependency analysis built-in, but must be added via double contingency or other analysis. |
| Risk metrics | ISAs assess individual accident sequences, not risk to individuals | PRA could sum risk to individuals | avoids problem of number of sequences, but excessive numbers not a common problem with ISAs |
| Uncertainty and importance measure evaluation | ISAs do not quantify uncertainty or importance, but ISA results have been used for importance evaluation | PRAs often include uncertainty analysis and can produce several types of importance measures for modeled events. | Uncertainty assessment might be important for cases where safety is marginal, or there is very large uncertainty. Understanding the relative importance of plant systems, components, and events can aid regulatory focus and priority. |

## IV. POTENTIAL APPLICATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT METHODS IN SIGNIFICANCE DETERMINATION FOR FUEL CYCLE OVERSIGHT

If the NRC were to revise the oversight process for fuel cycle facilities to be risk-informed and systematic, one required element would be a realistic and predictable process for assessing the risk significance of inspection findings. This process could use qualitative and quantitative risk insights to evaluate the significance of licensee performance deficiencies. The determination of risk significance within the process could be conducted in phases. The initial phase would be a screening review, based on qualitative criteria, to identify those findings that would clearly not result in a significant increase in risk (a “green” finding). Based on a test analysis of past inspection findings, the NRC staff anticipates that a majority of findings would be screened out by this initial qualitative process. For the remaining smaller set of inspection findings, the effect on the likelihood and consequences of accident sequences could be evaluated in more detail.

A hypothetical example of a quantitative risk significance evaluation is described in Section V of this paper. Such a quantitative (or more detailed qualitative) risk assessment would categorize the findings into broad categories—such as green, white, yellow, or red—based on its risk impact. Because worker safety plays a large role in the NRC’s regulation of fuel cycle facilities, there would likely be at least two significance metrics—one for the risk impact on workers and one for the impact on the public. The following section contains an example of such a quantitative risk significance evaluation using different methods. A full significance

[1] ANSI/ANS 8.1 (Ref. 13): Double Contingency Principle. Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes to process conditions before a criticality accident is possible.

determination process and risk significance approach remains to be developed and could involve a mixture of methods, dependent on the situation to be analyzed and availability of information.

## V. EVALUATION OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT FOR USE IN RISK SIGNIFICANCE DETERMINATION

This section describes an example fuel cycle inspection finding and evaluates the relative merits of using ISA or PRA methods to determine the risk significance of the finding. The evaluation first demonstrates the use of ISA risk index results versus PRA-like quantitative accident sequence frequency results in obtaining risk significance metrics for a hypothetical fuel cycle process. The characteristics illustrated by this example can then be used to evaluate the ISA-PRA differences for this application. A purpose of this example is to illustrate how a quantitative significance evaluation could be done for a fuel cycle design of typical complexity. The example intentionally lacks any of the potential defects of ISAs, such as safety controls not being credited, because this is not the purpose of this demonstration.

The length of the narrative necessary to explain the example may distort the message into an undue emphasis on the relative accuracy of quantitative versus risk index method quantification. This difference in quantitative accuracy, while possibly important in specific cases, is not necessarily the most important message of this section. Important messages include that: (1) whatever methods are used, supplements or modifications may be necessary because the ISAs were not done to produce risk estimates; and (2) risk significance evaluations for fuel facility inspection findings could often be relatively simple because scenarios are often simple.

All ISAs must include some form of evaluation of the likelihood of each accident sequence. In practice, some of these evaluations have been quantitative, using the PRA methods of fault trees or event trees. These quantitative ISAs produce accident sequence frequencies, but these frequencies are not summed to obtain total risk to an individual. Other ISAs use the risk index method described in Appendix A to Chapter 3 of NUREG-1520 (Ref. 3).

The results of either of these types of ISA evaluations—quantitative or risk index—can be used to evaluate the risk significance of fuel cycle inspection findings in a manner similar to the use of PRA in the reactor oversight program. However, it can be difficult to do this in a way that accurately and realistically reflects the risk significance of the finding, because ISAs are not risk assessments. Some of these potential difficulties will be discussed following the example.

The example process design relies on passive safe geometries to prevent a criticality accident. There are many other types of safety designs encountered in ISAs. For example, when geometry control is not feasible, mass may be limited by batch sizes controlled by equipment and operator monitoring. Alternatively, for low-enriched uranium, sources of moderation may be rigorously excluded from areas where mass or geometry is not controlled. Another common control scheme is to limit fissile powder mass by batch control, and to monitor moderation by both automatic and manual measurement. Fires in areas that might cause radiological or chemical release are typically prevented by excluding flammable materials, plus provisions for firefighting. Radiological or chemical hazardous materials are often isolated in actively ventilated cells. Thus the example chosen, although common, is only one of many types that would require analysis.

Description of a Hypothetical Example Process

This section analyzes an example process using information from two different techniques that might have been used in the ISA: (1) the risk index method (ISA-like); and (2) full quantification of frequencies (PRA-like). These example analyses are then critically evaluated against various factors in the context of this specific purpose of risk significance determination. The purpose of this example is to illustrate how quantitative risk would be used in risk significance evaluation for a typical fuel cycle process. However, it should be noted that this is only one example; and it does not illustrate the circumstance where there are additional controls not included in the analysis.

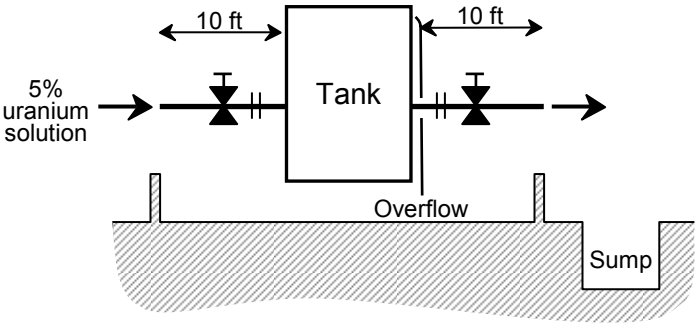


Figure 1 Hypothetical system

This example analysis postulates a process consisting of a tank, two 10-foot sections of piping, two flange connections, and two manual valves (Figure 1). An enriched uranium solution flows through the system. The process is protected by a floor dike to retain any solution that may escape the system. The dike has a surveillance inspection for leaks once every 2 years. The diked area has a subcritical geometry and is capable of holding the entire contents of the system. The floor area outside the dike contains a sump having an unsafe geometry; that is, a criticality accident would occur if the sump were filled with solution from the tank.

One challenge to the dike would be a solution leak from one of the components of the process. Another possible challenge would be an overflow that occurs during a transfer of solution into the process. Thus the two events that can initiate a challenge (i.e., initiating events) are a process leak and a process overflow.

Every 2 years, surveillance is to be done to determine if the dike is intact and will not leak if solution is spilled into it. If solution were to enter the diked area when a leak path existed in the dike, the solution could flow to the unsafe geometry sump, and a criticality accident would result. Such a criticality would produce an acutely fatal radiation dose to any workers nearby, and hence would be a high consequence event under 10 CFR 70.61.

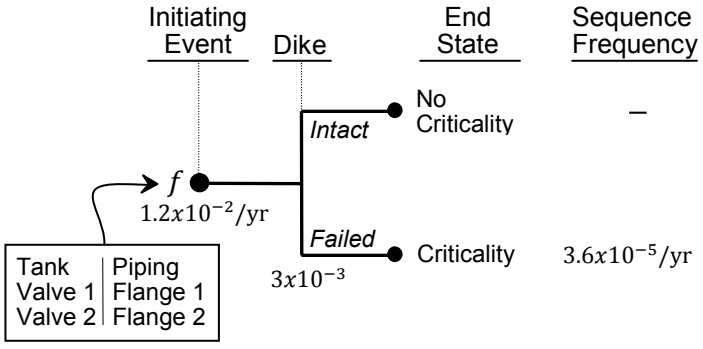


Figure 2 Event tree model

Evaluation Using a PRA-Like Model

The example process consists of six components: one tank, two valves, two flanges, and 20 feet of pipe. In the PRA model, there are two initiating events, a process leak and an overflow during a transfer of solution into the process. Each of the six components in the process is a potential source of a leak contributing to the initiating event process leak. Values for leak frequencies of each of these types of components were obtained from a generic component failure database for facilities similar to fuel cycle plants. The process leak initiating event frequency, $1.2 \times 10^{-2}$ per year, is the sum of the leak frequencies of these six components. The criticality sequence frequency is the product of the initiating event frequency and the probability that the dike is in a failed state when the leak occurs. This probability is the "unavailability" of the dike, which equals the downtime divided by the sum of downtime plus uptime. The dike could develop a leak at any time during the 2 years between surveillances, so the average time spent in the down, or failed, state is one-half the 2-year surveillance interval: 1 year. The average time spent in the up state is the mean time to failure, which is the reciprocal of the failure rate of the dike, 0.003 per year (/yr). Thus, the probability of the dike being in the failed state is (1 yr)/(1 yr + 1/(0.003/yr)) = 0.003, the value in the event tree above in Figure 2. The dike failure frequency estimate of 0.003/yr is postulated to have been based on plant experience with diked areas. Thus, the criticality accident resulting from the sequence process leak–dike leak is $(1.2 \times 10^{-2}/\text{yr})(0.003) = 3.6 \times 10^{-5}/\text{yr}$.

There is a second event tree for the overflow initiating event. This initiator is assigned a frequency of 0.005, again based on plant experience. For this initiator, the probability that the dike is leaking is the same as above, namely 0.003. Thus this sequence leading to a criticality has a frequency of $(0.005\ \text{yr})(0.003) = 1.5 \times 10^{-5}/\text{yr}$.

The sum of the sequence frequencies for process leak plus overflow yields a total frequency of a criticality accident of $5.1 \times 10^{-5}/\text{yr}$.

Mathematics of the ISA Risk Index Method of Likelihood Evaluation

The system in Figure 1 could be modeled quantitatively as a process with four states corresponding to the combinations of the two conditions: (1) the process leaking or not and (2) the dike leaking or not. $U_p$ is the probability that the process is leaking at any given point in time, and $U_d$ is the probability that the dike is leaking. The dominant way that one could enter the state where both are leaking is to be in the state in which the dike has developed a leak and then the process leaks before this is corrected. The probability of being in the state in which the dike has failed but the process is not leaking is $U_d(1 - U_p)$.

Thus, the frequency of transfer into the state where both are leaking is the following:

$$\lambda_p U_d \left(1 - U_p\right) \approx \lambda_p U_d$$

where $\lambda_p$ = frequency of the process leaking
$U_d$ = unavailability of the dike = probability that it is in a leaking condition
$1 - U_p$ = probability that the process initially is not leaking

The unavailability of the dike is a function of the time that the dike is unavailable, $\tau_d$, and the frequency, $\lambda_d$, that the dike fails:

$$U_d = \frac{\tau_d}{\tau_d + {}^{1}/_{\lambda_d}}$$

Because ${}^{1}/_{\lambda_d}$ is usually much greater than $\tau_d$, the denominator can be simplified to ${}^{1}/_{\lambda_d}$. Thus,

$$U_d = \lambda_d \tau_d$$

A risk index model is obtained by substituting for $U_d$.

$$\lambda_p U_d \approx \lambda_p \lambda_d \tau_d$$

Index values are considered to be the logarithm of frequencies, probabilities, or durations of failed conditions. Taking the logarithms, the risk index model for the hypothetical system is the following:

$$I_{process\ leak} = \overbrace{I_p}^{\lambda_p} + \overbrace{I_d}^{\lambda_d} + \overbrace{I_{dur}}^{\tau_d}$$

A similar sequence exists in which the solution enters the dike because of an overflow during transfer.

Evaluation by the ISA Risk Index Method

In practice, an ISA model using the risk index method is much simpler than a PRA model. Instead of individual components, controls are simply identified as active, passive, or administrative, and each type has an index value. In this example, both the process equipment and the dike are regarded as "passive engineered controls" and are each assigned a frequency index value of $I_p = I_d = -3$.

Because surveillance examinations of the dike occur every 2 years, the average length of time that the dike would be in a failed condition before it is discovered would be 1 year. Because the logarithm of the 1-year interval is zero, the duration index is assigned a value of zero. The index value for the accident sequence is the sum of the two frequency indices and the duration index:

$$I_{process\ leak} = \overbrace{(-3)}^{I_p} + \overbrace{(-3)}^{I_d} + \overbrace{(0)}^{I_{dur}} = -6$$

For the overflow–dike leaks sequence, the same equation, except the initiating event, is the overflow:

$$I_{overflow} = \overbrace{(-1)}^{I_o} + \overbrace{(-3)}^{I_d} + \overbrace{(0)}^{I_{dur}} = -4$$

As this is an administrative control, it is assigned a frequency index of -1. In this example, plant experience was not applied as it was to obtain the 0.005/yr overflow frequency in the PRA example. Instead the risk index method identified an overflow as an administrative control carried out by operators, and hence assigned a tabulated index of -1 for an administrative control to this event. The ISA likelihood evaluations are often, but not always, conservative, which is acceptable for the purposes of determining compliance with the requirement that high-

consequence events be highly unlikely. As a result, these likelihood evaluations for ISA are often not realistic estimates of risk.

Comparison of Results

Table 2 compares the results from the two accident frequency evaluation methods.

**Table 2 Comparison of Results from PRA and ISA**

| | PRA | | ISA | | |
|---|---|---|---|---|---|
| | initiating event | failure on demand event | passive control initiator | passive control failure on demand | |
| Level of Assessment | Tank<br>Valve 1<br>Valve 2<br>Flange 1<br>Flange 2<br>Pipes | Dike | Process | Dike | |
| Model | $\sum_{i=1}^{n} f_i Pr(i) = f_{total}$ | | $I_p + I_d + I_{dur} = I_{total}$ | | |
| Sequence Inputs | *frequency* | *probability* | *SSC index* | *SSC index* | *duration index* |
| Leak | $1.2x10^{-2}$/yr | $3.0x10^{-3}$ | $-3$ | $-3$ | 0 |
| Overflow | $5.0x10^{-3}$/yr | $3.0x10^{-3}$ | $-1$ | $-3$ | 0 |
| Leak | $3.6x10^{-5}$/yr | | $-6$ | | |
| Overflow | $1.5x10^{-5}$/yr | | $-4$ | | |
| Total | $5.1x10^{-5}/yr$ | | n/a | | |

In ISAs, sequence risk indices always remain separate; they are never summed as is the common practice with the sequence frequencies of a PRA. Thus, to make use of risk index ISA results for risk significance, the sequence indices need to be converted to frequencies so that they can be summed (see the example below).

Table 3 compares the results of the PRA method and the risk index methods. The table shows the risk indices with their exponential equivalents. The results show that the PRA and risk index methods can give different numerical results. This is expected, given that the index method has broad groups of SSCs, such as passive engineered controls. Passive controls can have a wide range of failure rates. In contrast, the groups of SSCs in the compiled failure rate information that is typically used for a PRA can have more narrowly defined groups. Although NUREG-1520 (Ref. 3) encourages a licensee to consider plant failure data instead of indices of broad SSC groups, the indices remain less specific than the failure rates in compiled rate references. For example, the typical index assignments are, for passive controls, -3, for active controls, -2, and for administrative control, -1.

**Table 3 Comparison of Results from the PRA and the Risk Index Methods**

| Sequence | | Method: PRA | Method: Risk Index |
|---|---|---|---|
| | Leak | $3.6\text{x}10^{-5}$/yr | $\text{RI}(-6) \equiv 1\text{x}10^{-6}$ |
| | Overflow | $1.5\text{x}10^{-5}$/yr | $\text{RI}(-4) \equiv 1\text{x}10^{-4}$ |
| | Total | $5.1x10^{-5}$/yr | $1.01x10^{-4}$ |

For certain types of SSCs in fuel cycle facilities, such as the dike in this example, failure rate data are often lacking, even in compiled references, increasing the reliance on plant experience.

It should also be noted that the quantitative failure frequency information taken from compiled databases such as Ref. 6 is considered generic for processing facilities, and hence highly uncertain. On the other hand, for the purposes of the risk significance evaluation described in the following section, order-of-magnitude accuracy is all that is needed.

Risk Significance Evaluation Using Results from the Two Methods

The risk significance metric for a specific deficiency is illustrated using the results from Table 3 and a postulated deficiency. The postulated deficiency is some action that inadvertently left the dike in a leaking condition. This compromised condition was not detected because of a failure to conduct surveillance for 4 years. Given that the dike was compromised, either a process leak or an overflow would result in a criticality accident because the leaking fissile solution would flow into the unsafe geometry sump. The accident frequency has increased from its original value of $\lambda_b = 3.6\text{x}10^{-5}/\text{yr} + 1.5\text{x}10^{-5}/\text{yr} = 5.1\text{x}10^{-5}/\text{yr}$ to the sum of the frequencies of the initiating events, $\lambda_d = 1.2\text{x}10^{-2}/\text{yr} + 5\text{x}10^{-3}/\text{yr} = 1.7\text{x}10^{-2}/\text{yr}$. Originally, the baseline probability that the high-consequence accident would happen during the time $t$ = 4 years was supposed to be—

$$\Pr(\text{high consequence} \mid \text{baseline}) = 1 - \exp(-\lambda_b t) = 2\text{x}10^{-4}$$

Because of the deficiency, the probability is,

$$\Pr(\text{high consequence} \mid \text{deficiency}) = 1 - \exp(-\lambda_d t) = 0.066$$

The metric used to determine the risk significance of deficiencies for fuel cycle facilities is the increase in the probability of a high-consequence event that was incurred because of a deficiency. This metric is analogous to the metric used in the Reactor Oversight Process.

Using the quantitative (PRA) accident frequencies, this increase is as follows:

$$\Delta\Pr(\text{high consequence}) = \Pr(\text{hc} \mid \text{deficiency}) - \Pr(\text{hc} \mid \text{baseline}) = 0.066 - 2\text{x}10^{-4} \approx 0.066$$

Alternatively, using the results from the risk index ISA from Table 3, the sequence indices in the case of the deficiency are -3 for the process leak and -1 for the overflow, which are equivalent to an annual process leak frequency of $10^{-3}$/yr and an overflow frequency of $10^{-1}$/yr, for a total accident frequency of 0.101/yr during $t$ = 4 years, given the deficiency. The baseline (no deficiency) accident frequency would be the sum of the frequencies in Table 2,

$10^{-4}$/yr + $10^{-6}$/yr = 1.01x$10^{-4}$/yr. Substituting these results into the equation for the delta probability yields a change in probability of—

ΔPr (high consequence) = Pr (hc | deficiency) - Pr(hc | baseline) = 0.3324 - 0.0004 = 0.332

(Four-digit results are used here to illustrate that the baseline probability is very much lower than that with the deficiency. This does not imply that the accuracy of the estimates is four digits. Rather, it illustrates that the baseline risk subtraction can usually be ignored.)

In this example, the risk index method yields a risk significance metric that is a factor of 5 higher than the PRA method. This is not surprising, as the risk index method is more of a qualitative ranking method than an attempt to be accurate.

To complete the significance determination, the probability change value (e.g., 0.066 or 0.332) would be compared to threshold values that define the boundaries between significance categories. For example, suppose that the threshold of high significance is 0.1, the threshold of moderate significance is 0.001 and the threshold between low significance and very low is 0.0001. With these thresholds, the risk index method would categorize the example deficiency as high significance (0.332 > 0.1), while the quantitative frequency method would yield moderate significance (.001 < .066 < 0.1).

Note that these example risk significance determinations did not need to use the total risk to an individual worker. This is because the significance metric is the change in probability and so does not involve the total. Typical deficiencies involve only one control in one process and a few accident sequences, as in the example here. This applies whether one uses results from a risk index evaluation or a PRA. Note also that it would be inefficient to evaluate the risk from all accidents in all facilities before implementing a significance determination process as was done to support the reactor oversight program. Based on a review of recent inspection findings, there would be only about two significant safety findings per plant per year. Thus most accident scenarios in a facility would never be used in a significance evaluation.

Aspects of Integrated Safety Analysis Influencing a Significance Determination

Some ISAs of some processes evaluate accident frequencies and consequences using conservative practices. This is not to say that ISAs as a whole are always conservative; in fact, nonconservatisms also exist. Use of a conservative ISA result could exaggerate the risk significance of a particular deficiency compared to an analysis that was based on more realistic information. Many of these conservatisms, such as not crediting all safety features, are present in ISAs, even if they use quantitative, PRA-like methods. Conservatisms are acceptable for compliance purposes because the purpose of ISAs is not to estimate risk but to limit the likelihood of each accident sequence separately in order to assure safety. Some of the practices that cause ISA results to be significantly inaccurate estimators of risk are discussed below.

Radiological and chemical exposures of persons in ISAs are often estimated conservatively. Sometimes, chemical releases are simply assumed to cause high consequences in terms of 10 CFR 70.61, or a very conservative dispersion calculation and source term are used. In particular, for chemical and radiological releases potentially reaching individuals off site, it is common to use a single Gaussian dispersion calculation with the wind blowing directly at the individual at low wind speed with stability class F. Each of these is an unlikely condition. The probabilities that the wind could be blowing in a different direction or that the stability could be

other than class F are not credited. Each of these is at least a factor of 0.1. Thus the actual frequency of high consequences to an individual could be two or more orders of magnitude lower than would be the case if an adjustment for these factors was not made. Such conservatisms, even when large, are not a defect when using the ISA for compliance purposes. For realistic assessment of risk significance, however, such deviations are too large.

ISA analyses of some processes do not take credit for all safety controls as IROFS, so ISA documentation does not mention these controls. Consequently, when a deficiency occurs in a particular process, the NRC staff will have to find out from the licensee whether such additional controls exist and model them. This applies regardless of whether the risk index method or quantitative methods are used. Again, the deviation from realism for this type of conservatism is usually very large; which means that it needs to be corrected in the significance evaluation in order to obtain a reasonable value.

In some instances, ISAs of a particular process were nonconservative. Generic nonconservatisms in ISA methods are usually corrected during NRC staff review of the ISA. However, a non-conservative analysis of an individual fuel process may occur; for example, overlooking a specific sequence. Another type of nonconservatism is improperly screening out an event on the grounds of low frequency or consequences. These improperly screened events may not be identified during an ISA review because these reviews only examine a selected subset of plant processes in detail, as described in NUREG-1520 (Ref. 3). Furthermore, the ISA summary typically does not list all events that have been screened out. In cases in which the inspection itself has discovered the omitted accident sequence, its omission in the ISA is not a problem for significance determination because the process can be designed to take it into account. Screening out events inappropriately might, to a certain extent, have been remedied by detailed peer review, as has been done for PRAs. However, detailed peer review of ISA's has not been done and is inhibited by the proprietary nature of fuel process designs. Annual updates of ISAs may not revisit previously analyzed designs unless there have been changes. For these reasons overlooked sequences may continue to be discovered by licensees and NRC inspectors.

ISA methods and criteria vary more than PRAs, and hence use of ISA results for risk significance must be careful to avoid inconsistency. The proprietary nature of ISA, the flexibilities in the regulation and the lack of detailed ISA standards endorsed by NRC (other than references 1 and 4) make these inconsistencies difficult to remedy via licensee action.

The risk index method has inherent uncertainty, so that, if used to estimate accident frequency for risk significance, results may differ from a quantitative evaluation by a substantial amount.

The simple process used in the example significance determination above does not illustrate another possible difference between ISAs and reactor-like PRAs; namely, analysis of complex control systems with dependencies. NUREG-1513 (Ref. 4) recommends use of fault tree and event tree modeling in such cases. On the other hand, many of the controls in fuel facilities are quite simple, like the example. One particular type of dependency, loss of power, is not a safety issue for most processes in most fuel facilities, because power is not required for most safety functions. Processes are often rendered safe by simply ceasing operation or by passive features. Plants do have backup power on site, but this is typically provided to permit orderly process shutdown, not for safety. Exceptions are negative pressure confinement systems, which require continuous operation of fans, and some cooling systems.

## SUMMARY

Fuel cycle ISAs and reactor PRAs are performed for different purposes. But some ISAs have used some PRA methods extensively, and other ISAs have used them selectively, as recommended in NRC guidance (Ref. 4). ISAs were not performed to estimate risk as PRAs do. ISAs were performed to identify potential accident sequences, designate IROFS to prevent or mitigate them, and describe management measures to be applied to assure IROFS reliability and availability. As a result of substantial reviews of ISAs which have been approved, NRC staff has concluded that the ISA methods and processes have succeeded in meeting this objective and are acceptable for assuring safety under 10 CFR Part 70. This does not preclude that ISAs of specific processes may contain one of the potential deficiencies previously mentioned.

Caution should be exercised in using ISA results for risk significance determination. ISAs were not performed to produce risk results for this application. In some cases, ISA results provide a reasonable risk estimate of sequence frequencies and consequences; in other cases, they do not. However, it should be remembered that, for the purposes of the oversight program, order-of-magnitude significance is sufficient. Because ISAs are not performed to support risk significance, the staff expects that modifications would be needed in some cases to obtain reasonable and consistent evaluations.

As illustrated in the example in Section V, the simplicity of many fuel cycle process and associated accident scenarios will often make it feasible for NRC staff to perform quantitative risk significance evaluations for an inspection finding on a case-by-case basis. This, of course, depends on the availability of applicable failure data and consequence evaluation tools for the particular scenario. Thus, such quantitative evaluations will not always be possible. Based on review of recent inspection findings, few such quantitative evaluations are likely to be needed each year, so it would be inefficient to pre-evaluate all accident sequences in all fuel cycle facilities to support a risk significance process.

## REFERENCES


1. U. S. Nuclear Regulatory Commission, “Staff Requirement Memoranda - Briefing on the Fuel Cycle Oversight Process Revisions,” May 2010.

2. U. S. Nuclear Regulatory Commission, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk Informed Activities,” Regulatory Guide 1.200, March 2009.

3. U.S. Nuclear Regulatory Commission, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” NUREG-1520, Rev. 1, May 2010.

4. US. Nuclear Regulatory Commission, “Integrated Safety Analysis Guidance Document,” NUREG-1513, May 2001.

5. U. S. Nuclear Regulatory Commission, “Proposed Rule 10 CFR 70 Section 70.61 Performance Requirements,” Federal Register Vol. 64 No. 146 page 41341, July 30, 1999.

6. Alber, T. G., et al., “Idaho Chemical Processing Plant Failure Rate Database”, INEL-95/0422, August 1995.

7. H.C. Benhardt, et al., “Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities,” WSRC-TR-93-581, February 1994.

8. U. S. Nuclear Regulatory Commission, “Nuclear Fuel Cycle Facility Accident Analysis Handbook,” NUREG/CR-6410, March 1998.

9. U. S. Nuclear Regulatory Commission, “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement;” Federal Register, 50 FR42622, August 16, 1995.

10. U. S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, November 2002.

11. U. S. Nuclear Regulatory Commission, “The Reactor Safety Study,” WASH-1400, 1975.

12. U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG-1150, 1991.

13. American Nuclear Society, Nuclear, “Criticality Safety in Operations with Fissionable Materials Outside Reactors”, ANSI/ANS 8.1, 1998.

14. Matthew Warner and Jim Young, “Applying Nuclear PRA to a Nuclear Fuel Cycle Facility Integrated Safety Analysis,” presented at Probabilistic Safety Assessment and Management Conference 10, June 2010.