NRC Staff Considerations on a Comparison of Integrated Safety Analysis to Probabilistic Risk Assessment

The Staff Requirements Memorandum (SRM) to the Commission briefing of April 29, 2010, on revising the fuel cycle oversight program directed staff to produce a concise paper that was a critical evaluation and comparison of Integrated Safety Analyses (ISA) and Probabilistic Risk Assessment (PRA). The SRM to SECY-10-0031 stated that the Commission expects the paper "to better inform proposed enhancements to the oversight process." The following are NRC staff considerations for conducting such a comparison.

EXECUTIVE SUMMARY

ISA Description

ISA is a systematic analysis required by 10 CFR 70 Subpart H for major fuel cycle facilities to identify all accident sequences leading to high or intermediate consequences, and Items Relied On For Safety (IROFS) to prevent or mitigate these accidents. Section 70.61 explicitly defines high and intermediate consequences. For example, a high-consequence event for a worker is a life threatening chemical exposure or a dose greater than 100 rem. An intermediate-consequence event for a worker is a chemical exposure that produces serious health effects, or a dose from 25 to 100 rem. Accidental criticality, radiological, and chemical exposures are to be considered. ISAs are to identify sufficient IROFS to demonstrate that high-consequence events are "highly unlikely" and intermediate are "unlikely", as defined by the licensee. There is no requirement that accident sequence likelihoods be quantified as frequencies; nor that they be multiplied by consequences and summed to obtain an estimate of risk to individuals.

Definition of the terms "unlikely" and "highly unlikely" is left to the licensee to propose, subject to the U.S. Nuclear Regulatory Commission's (NRC) approval. The NRC provided guidance (References 1 and 4) as to some acceptable ways to comply with these requirements. Although the NRC produced these guidance documents, NRC did not develop the basic methods, such as HAZOP or fault trees. They describe, nor perform tests of ISAs, but endorsed techniques already in use for compliance with OSHA regulations. What NRC provided in the Standard Review Plan, Revision 1 of 2010 (Ref. 1) is extensive and detailed guidance on how to execute these methods in practice, based on experience with the actual ISAs over the last 10 years. In particular, likelihood evaluation guidance is provided in Reference 1, Chapter 3 and its appendices for quantitative, qualitative, and risk index methods.

Some PRAs may limit the scope of their analysis, for example, to internal events only, because this is sufficient for some particular applications. ISAs are intentionally not limited in scope, except as specified in the regulation. They are required to be comprehensive in considering hardware failures, human errors, fires, and external events. ISAs are also to consider interactions between fire, criticality, chemical, and other events. This is what is meant by "integrated" in ISA.

Physical and chemical phenomena resulting from an event identified in the ISA are usually not modeled in detail to support a risk estimate. Instead, usually either a conservative outcome is assumed or a bounding evaluation of consequences is made. In particular, this applies to source terms and offsite plume dispersion for chemical or radiological releases.

ISAs are not performed to estimate risk, but to identify IROFS so that they may be subject to the safety management program required by 10 CFR 70 Subpart H. A few ISAs do estimate accident frequencies quantitatively; but most use the risk index method, which has some relation to frequencies.

PRA Description

PRA is a systematic method of estimating frequencies and consequences of accidents, and combining these into various risk metrics. To be useful for most applications, risk metrics are estimated quantitatively. These risk estimates must be best estimate or average, as opposed to a bounding or conservative analysis as is used in design analysis. To estimate risk accurately PRAs must quantify risk-significant phenomena. If the phenomena vary probabilistically, like weather, this must be modeled and an average determined. Similarly, the amount of radioactive material released from containment during an accident must be estimated realistically.

Reactor PRAs use event trees to delineate sequences of events leading to adverse consequences of concern, such as core damage or large release from containment. The frequencies and probabilities of events that appear in these trees are obtained either directly from failure data on these events or by further breaking down the event into components using fault trees until a level of events is reached for which failure data does exist. Dose consequences to individuals at locations around the reactor are calculated for each category of accidental radiological release. The frequencies and consequences are then summed for each individual to obtain a total risk metric. As a surrogate for risk of acute fatality to individual members of the public, large early release frequency may be calculated. In other applications, collective health risk and cost risk impacts summed over the whole population.

Unlike ISAs, PRAs are not used directly to demonstrate compliance with safety performance requirements in the regulations. However, there are many regulatory applications of PRA, including risk significance determination in the reactor oversight program, safety design optimization in Severe Accident Mitigation Alternatives (SAMA) analysis, and backfit or regulatory analysis to justify imposing new safety requirements. When PRAs are a reasonably accurate estimate of risk, they can be used to gain insights into the risk significance of plant features and safety challenges. ISAs were not done to estimate risk and so may, for certain processes, not provide results that are useful for risk insights without correction.

The NRC and industry have devoted large resources to develop PRA technology, tools, and industry standards. In contrast, only modest guidance development has supported ISA technology. Reactor PRAs have been peer reviewed, and industry standards developed. Much of the content of ISAs are proprietary or sensitive; hence not normally available in detail for peer or public review.

No comprehensive PRA has been performed for any of the currently licensed fuel cycle facilities; although a few facilities have quantified the frequencies of accident sequences.

Evaluation of ISA PRA Differences for Compliance with 10 CFR 70

ISAs for fuel cycle facilities have a direct regulatory role of identifying all accident sequences and evaluating their likelihood for compliance with 10 CFR 70.61 performance requirements. The rule does not require any particular systematic technique for identifying accidents.

However, NRC guidance (NUREG-1513, ISA Guidance Document, May 2001) recommends use of event tree/fault tree methods for complex systems. Thus it is possible that, for a particular complex process, failure to use these methods might result in failure to identify all accident sequences and IROFS necessary for compliance. In this case, NRC staff might find that use of these PRA techniques is necessary for compliance in order to identify all accidents.

A similar argument is difficult to make for compliance with the likelihood requirements of 70.61, since the definitions are left to the licensee. However, NRC has provided guidance as to quantitative definitions of “highly unlikely” and “unlikely.” In addition, there is the existing set of approved licensee definitions. The most common alternative to quantification, the risk index method, is a relative ranking of sequence frequencies that is only roughly quantitative. A quantification of accident sequences might well be desirable, especially in cases where the evaluation results in just meeting the performance requirements; but it is not required.

In practice, NRC staff and industry have participated in a continuous process of developing and reviewing the ISAs starting in the late 1990s. This process has resulted in correcting various deficiencies and in overall improvement of the ISAs. As a result of substantial reviews of each ISA, for those which have been approved, NRC staff has concluded that the ISAs are acceptable for compliance.

Evaluation of ISA-PRA Differences for Risk Significance Determination

If the Fuel Cycle Oversight Program (FCOP) were revised to be more like the reactor oversight program, a risk-informed FCOP in safety areas addressed in the ISAs typically would have a process of determining the risk significance of deficiencies found by the licensee or NRC inspectors. Risk significance is usually quantified as the increase in accident frequency caused by a deficiency times the duration of this increased frequency. In principle, the metric could be the increase in the integrated product of frequencies times consequences over all affected sequences, rather than just the frequency. In the reactor oversight program, for findings which do not screen based on qualitative criteria, quantitative risk significance evaluations are performed. Information to assist in these quantitative evaluations has been developed based on pre-processed risk information from PRAs. Areas of oversight not related to ISA, such as 10 CFR 20 radiological protection or safeguards, may use deterministic significance criteria, rather than criteria involving quantitative risk.

Two of the ISAs have quantified accident frequencies which could be used for such quantitative determinations. Most of the others have used risk index evaluations (see Chapter 3, Appendix A of NUREG-1520, Standard Review Plan for Review of a License Application for a Fuel Cycle Facility, May 2010), which can also be used for significance; although this method is only roughly quantitative. When a safety deficiency is found in a typical fuel facility process, it typically relates to a single piece of process equipment. Thus, for a typical fuel facility deficiency, only the few accident sequences in that process need be considered in determining risk significance. Because of this, it is usually feasible to evaluate the risk significance of the deficiency at the time it occurs without having pre-processed information available. Sequence frequency information from the facility ISA can often be used in such determinations, though with caution as explained below. Naturally, an ISA with PRA-like quantitative frequencies produces more refined information for this purpose than one using risk indices.

Caution should be exercised in using ISA results for risk significance determination. ISAs were not performed to produce complete and accurate estimates of risk. In some cases ISA results do provide a reasonable risk estimate of sequence frequencies and consequences—in other cases not. Similarly, the definition of “high consequences” in the ISA rule (10 CFR 70.61) encompasses a wide range of severity and numbers of affected individuals; and so is not ideal for making risk significance distinctions.

Three situations where ISA results would have to be modified in order to provide even approximately correct risk significance will be described here. The first is where an accident sequence has been overlooked, or where there is a sub-sequence of an identified accident that is of higher frequency or consequences than that assessed in the ISA. In such cases, if there is a deficiency disabling an IROFS in the identified sequence, the resulting frequency of high consequences (which is what determines risk significance) will be underestimated because there will be additional risk from the unidentified sequence. The second situation is where the licensee does not declare an existing safety control as an IROFS because it is not needed to make a sequence “highly unlikely.” In such a case, the frequency of an accident given the deficiency will be overestimated, if one only uses information in the ISA. This is because the ISA has taken no credit in its accident frequency evaluation for the undeclared control. The third situation is a large release, either chemical or radiological, exposing persons offsite. ISAs in such cases usually calculate exposures to individuals nearest the site using worst-case weather and source terms. Thus, if a deficiency increased the frequency of such a release, one would be over-estimating the likelihood that the event would cause high consequences offsite because the weather would not normally be worst case. Realistically, high consequences might only occur for only a small fraction of weather conditions. In performing risk significance evaluations of inspection findings, each of these types of large deviations from realistic impacts would need to be corrected. Risk significance determinations typically need only be accurate to an order-of-magnitude, but deviations such as these typically exceed this rough standard.

Introduction and Summary of Structure

Background and Introduction

In the SRM, the Commission directed staff to consider specific technical features of ISA/PRA such as end states and accident sequence quantification. These are addressed, primarily in Section I, Table 3 (at the end of the paper). In addition to technical features, Sections I and II discuss regulatory uses, development, and background of ISAs and PRAs—since these are quite different.

The SRM directed that the paper include a “critical evaluation of how ISAs differ from PRAs.” Sections I and II describe how ISAs and PRAs differ; but a critical evaluation implies a determination of adequacy, or which is superior for some specific purpose. Adequacy or superiority of a method depends on the purpose or application of the analysis. Thus Sections IV and V contain critical evaluations of ISA and PRA, specifically with respect to their use for two particular applications, namely:

1) compliance with 10 CFR 70 and acceptable safety (Section IV), and

2) performing risk significance determination to support a risk-informed FCOP (see Sections IV and V).

One difficulty in characterizing ISAs is that they vary widely, both in methods and in the nature of the processes being analyzed. Ten CFR 70 leaves choice of ISA methods to the licensee. A few licensees have chosen to use PRA methods. That is, accident sequences are quantified using event trees or fault trees. Other licensees use fault trees occasionally. Thus the ISA versus PRA dichotomy is not as clean as it may sound. Section V attempts to create a clean dichotomy by comparing, (a) use of an ISA with quantified fault trees or event trees as in PRA to (b) use of an ISA with the risk index method (see Reference 1, Chapter 3, Appendix A). The potential effects of all ISA/PRA differences, not just the issue of quantification, are discussed in Sections IV and V.

The principle conclusion of Section III is that, although PRA methods are recommended by NRC and have been applied by licensees for specific situations in ISAs, the ISAs that have been approved are acceptable for compliance with Part 70 and for safety. One conclusion of Section V is that, in principle, it appears feasible to use ISA results supplemented in specific cases by additional information to estimate quantitative risk significance of inspection findings. In practice, desired information may not be available, as an ISA was not developed as a risk-significance tool. Thus, ISA results must be used with caution, for this application. The significance evaluations would be done by NRC staff for each finding when it occurs. There would be no need to assign quantitative frequencies to all facility accident sequences in advance since each deficiency would typically affect only a few sequences.

Basis for Evaluation of ISAs

Fuel cycle facilities tend to have a large number of processes with diverse safety features. ISAs for these facilities have been reviewed by multi-disciplinary teams. Due to the large number of processes, the teams review only a select subset of them in detail. The staff ISA reviews produced Technical Evaluation Reports (TER) that made findings on compliance with the regulations. However, these TERs typically do not address the kinds of evaluations this paper is undertaking. Consequently, in order to make evaluations of the ISAs for this paper, it has been necessary to consult with a substantial number of ISA reviewers. Thus, the basis for the statements regarding ISAs in this paper is the experience of these reviewers.

I. ISA Background and Description

A. ISA Definition

ISA is defined in 10 CFR 70.62(c) 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 is provided in References 1 and 4.

B. Regulatory Uses of ISAs

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 rule. High-consequence events must be highly unlikely, and that intermediate-consequence events must be unlikely as defined by the analysts. Processes must be subcritical for all normal and credible abnormal conditions, with preventive controls being the primary means of protection. This differs from PRAs, which are used to inform decisions, but not directly used for compliance.

Identification of IROFS

Through the ISA process, a set of IROFS is identified. When a structure, system, or component (SSC) is designated as an IROFS, regulatory requirements become applicable. These requirements include that the IROFS be sufficient to meet the likelihood/consequence requirements of 10 CFR 70.61. Changes to IROFS must be reported to the NRC annually. The exception is when the IROFS is the only such SSC in an accident sequence (e.g., sole IROFS), in which case prior NRC approval is required.

Other Applications of ISA Results

Another application of ISA results has been prioritization of IROFS to be inspected during the operational readiness reviews of the Gaseous Centrifuge Enrichment Plants. In addition, ISAs produce annual IROFS lists and failure logs that are useful in guiding regular inspections. Revision of inspection and enforcement guidance to make use of ISA information is in progress.

C. Origin of ISAs

After two serious incidents in 1988 and 1991 at fuel cycle facilities, one of them a fatality caused by chemical effects, NRC staff considered various possible regulatory reforms. It was decided to produce a new rule, 10 CFR 70 Subpart H, which brought chemical effects under NRC jurisdiction and required ISAs. The Statements of Consideration for this rule included the following statement regarding 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, NRC issued References 1 and 4 which provided guidance on ISA methods, including likelihood evaluation, and choosing systematic methods for identifying accidents based on the type of process to be analyzed. Reference 4 recommended use of the PRA methods of event trees and fault trees for complex control systems, or when a quantitative evaluation of accident frequencies is to be done. Two out of the nine ISAs performed to date made extensive use of such quantitative methods.

D. ISA Development by NRC

The NRC development of ISA methods was minimal. References 1 and 4 were adapted from the chemical and nuclear reactor industries. The techniques recommended in NUREG -1513 (Reference 4) are largely based on methods developed for compliance with the Occupational Safety and Health Act (OSHA) chemical safety requirements. In part, this was done to “complement and be consistent with the parallel OSHA and Environmental Protection Agency requirements”, as stated in the statements of consideration for Subpart H. As the ISAs were being performed by fuel cycle facilities, questions arose on ISA methods, including likelihood evaluation. These questions were discussed in workshops; and NRC staff developed interim staff guidance documents that are now incorporated as appendices to Chapter 3 of Reference 1. Although limited example analyses were provided in Standard Review Plans, no extensive ISAs were performed by NRC staff or contractors as models, as was done for PRA of reactors.

E. Technical Features of an ISA

It is difficult to generalize about technical features of ISAs because each plant is different, and a variety of ISA methods were used. It should be noted that plant process designs are proprietary, hence ISA documentation is generally not shared with other licensees.

End States

End states of accident sequences are defined in 10 CFR 70.61 as radiation doses or chemical health effects to workers and/or persons outside the controlled area. Most accidents sequences result in health effects to workers. Relatively few accidents exceed the consequence levels defined in the rule for persons offsite due to the distances involved. Occurrence of a criticality accident, the most common type of accident, could easily result in fatality to a worker if close enough to the accident location. Total frequencies of fatality to individuals are not summed over all accidents.

Quantification of Accident Sequences

Accident sequence frequencies are quantified in two of the approved ISAs. Reference 2 is one source of failure rate inputs. 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 similar to that described in Appendix A of Chapter 3 of Reference 1; which could be called semi-quantitative. Offsite doses are often calculated conservatively using computer codes in order to determine if thresholds of the rule are exceeded. These calculations are not probabilistically averaged over weather conditions. They are for worst-case source terms and weather. This conservatism is acceptable for compliance with 10 CFR 70 Subpart H, but would have to be adjusted in order to obtain reasonable quantitative risk significance results.

Hardware Failures and Human Errors

Both hardware failures and human errors are modeled in ISAs. Hardware IROFS are usually identified at the sub-system level, for example, 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/error frequencies and probabilities of failure on demand. These values are typically taken from generic data sources like References 2 and 3.

Physical and Chemical Phenomena

Except for calculating chemical and radiation exposures, physical and chemical phenomena involved in fuel cycle accidents do not require modeling or calculation to achieve the purposes of the ISA. Accidental criticalities are considered to be high-consequence events, since they can produce acute fatalities, as shown by the record of actual accidents. Calculating total risk to individuals would require such calculations, including probabilistic variations in magnitude and locations of the accidents.

Fires and External Events

Fires are evaluated as accidents in ISAs as potentially causing either a radiological or chemical release. Chapter 7 of the Standard Review Plan (Reference 1) specifically addresses fire safety. Fire safety is one of the technical disciplines normally represented on each ISA team. ISAs, by rule, must consider external events as well. Different operating modes, such as shutdown for maintenance, should, in principle be analyzed.

Plume Dispersion

Worst-case dispersion is used to determine if offsite radiological or chemical thresholds of 10 CFR 70.61 are exceeded. Typical assumptions are: stability class F, low wind speed, no heavy gas model, and no plume rise. Thus the magnitude of the doses is not an average or typical case, but worst case. Probabilistic weather averaging, as in the 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 is provided in NUREG/CR-6410, Nuclear Fuel Cycle Facility Accident Analysis Handbook. However, in many cases, such releases are simply assumed to produce “high-consequence” doses as defined in 10 CFR 70.61.

Uncertainties in Physical and Chemical Phenomena

Uncertainties in accident phenomena are usually handled in ISAs by making conservative assumptions. They are not modeled probabilistically to estimate known variations. Estimating variation in criticality magnitudes would require technology development. Uncertainties, as opposed to variations, exist in 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

Importance measures, such as relative change in risk given that each IROFS failure probability is set to 1.0 one at a time, are not routinely calculated in an ISA. Such importance measures have been used in certain applications, including prioritizing IROFS for inspections. A risk significance metric has been considered for use in determining risk significance of inspection findings. This will be explained in the example in Section V of this paper.

II. PRA Background and Description:

A. PRA Definition in the Reactor Context

PRA is a systematic methodology to evaluate risks associated with complex technologies. In the nuclear power industry, the major application has been to light water reactors (LWRs). Risk is characterized by the magnitude of the possible consequences and the likelihood (probability/frequency) of occurrence of each consequence. Consequences are expressed numerically (e.g., the number of early fatalities, latent cancers or collective dose in person-rem); and their likelihoods of occurrence are usually expressed as frequencies. The total risk is the sum of the products of the consequences multiplied by their frequencies.

A PRA usually answers three basic questions: what can go wrong, how severe are the consequences, and what are their probabilities or frequencies? For LWRs, three levels of PRAs are defined based on important 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 and its output is the frequency of radiological release from reactor containment to the environment (of which large early release frequency is a subset); and 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 consequent offsite health and economic consequences.

B. Regulatory Status

In the U.S., PRA use is guided by the PRA Policy Statement of 1995 and various regulatory guides that describe the use of PRA results for risk management (e.g., Regulatory Guide 1.174, and Regulatory Guide 1.200). While PRA is not a formal requirement in the licensing and regulation of current LWRs, decisions are often informed by results of PRAs. 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 NRC's Individual Plant Examination program and has opted to continue using the PRA approach. For future reactors, licensed under 10 CFR 52, a PRA is required as part of the license application. Overall, the use of PRA, have increased and matured over the past 35 years, not only in the U.S. but worldwide. Standards have been developed by professional organizations on requirements for PRAs, and NRC participates in these activities to help develop guidance useful for its regulatory applications. PRAs are used in the Reactor Oversight Program (ROP) to assess the risk significance of inspection findings in the significance determination process and in the SAMA analysis performed under 10 CFR 51.53 as part of an application for license renewal.

C. PRA Development by NRC

Over the past four decades, NRC (and the nuclear industry) has made a large investment in PRA development and application. The landmark Reactor Safety Study (WASH-1400) established the fundamental paradigm for all subsequent PRAs. The NRC and its contractors performed a series of studies (Reactor Safety Study Methodology Application Program (RSSMAP), Integrated Reliability Evaluation Program (IREP), and NUREG-1150) over the years and guided the industry to perform studies as well, notably IPEs and Individual Plant Examination of External Events. The industry also performed major PRAs in the aftermath of the TMI-2 accident (such as Zion, Indian Point, Limerick, Seabrook). More recently, the NRC developed (and currently maintains) a set of PRA models for all operating U.S. commercial NPPs. 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 in analyses to help identify potential precursors to support the agency's Significance Determination Process (SDP) and to confirm licensee risk analyses submitted in support of license amendment requests. In addition to performing PRAs, much work has been done on methods development of virtually all elements of a PRA. This included major programs on severe accident analysis, human reliability, data base development, and seismic behavior of plants.

D. Technical Features of a PRA

The scope of a particular PRA application may not require analysis of all operating modes and initiators. But, within the scope of the analysis, reactor PRAs are aimed at being systematic and complete in terms of the spectrum of potential initiating events and accident scenarios. Typically, PRAs search for potential dependencies, common cause failures, and systems interactions. The likelihoods of events are quantified based on appropriate data. Uncertainties in the likelihoods and associated consequences are usually estimated. The well-developed human reliability methods are applied to scenarios involving human error. Accident initiators both internal and external to the plant are considered. Typical tools used in a PRA are failure modes and effects analysis, event trees, fault trees, codes for calculating physical and chemical behavior during severe accidents, and codes for evaluating offsite consequences. More recently, quantitative probability models other than the standard event tree/fault tree approach have be applied. In sum, PRAs strive to provide a realistic depiction of the risks of nuclear energy systems, including the identification of major contributors to risk and the sensitivities and uncertainties of the results to key input data and assumptions.

E. PRA in Fuel Cycle Facilities and FCOP

No facility-wide PRAs have been carried out for fuel cycle (FC) facilities in the U.S. Some recent, limited work focused on particular accidents, such as the risk of red oil excursions (ROE) in the MOX facility under construction at Department of Energy's Savannah River site in South Carolina, which identified common cause failures and human errors as the major contributors to the risk of ROEs. In contrast to NPPs, the hazards posed by FC plants include toxic chemical and explosion hazards, in addition to radiological hazards. The recipients of the predominant risks are facility workers. FC facility processes usually have few standby safety systems and mainly rely on normally operating systems and operator actions to cope with abnormal conditions. This is more analogous to NPPs in low power shutdown mode. Individual FC processes are characterized by many unique aspects with regard to processes and operations, especially with respect to the diversity of human actions that are involved. The issue of ISA versus PRA relates to the complexity of the facility being analyzed and whether the underlying logic model of the facility is able to represent the system's processes and functions in sufficient detail to capture its vulnerabilities realistically.

If the FCOP is to be revised to make use of the risk significance of a deficiency that is uncovered in the inspection process, there is a need for metrics and criteria for risk significance that can address the variety of accidents. The significance determination of inspection findings may have to be based directly on the delta probability of a high or intermediate consequence accident that was caused by the deficiency. Separate significance determinations would be needed for workers and public because they differ, even for the same event.

III. Critical Evaluation of ISA-PRA for Compliance with 10 CFR 70

The theme of this section is to explain how, despite the fact that some of the more simple ISAs are less rigorous compared to a full PRA. ISAs can produce results that are acceptable for compliance with 10 CFR 70 and for safety.

The first ISAs were initiated in the early 1990s for plants that had already been operating for two decades. Today, the year 2010, the industry and NRC have almost 20 years of experience with this process. ISAs were not actually mandatory until 10 CFR 70 Subpart H became final in year

2000. A draft SRP and an ISA Guidance Document were already in existence at that time, had been thoroughly discussed with the affected licensees, and were issued shortly after the rule. Over the next four years, all the existing licensees completed their initial ISAs for the purpose of compliance. During this time licensees encountered many problems and questions of interpretation. Workshops were held and Interim Staff Guidance documents were produced addressing the issues. This guidance is now part of Revision 1 of the SRP. By late 2004, ISAs of all affected 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, new issues and problems were discovered—both generic and specific. Due to the size of the ISAs, correction of these problems took some time. These original ISAs were all approved as acceptable for compliance with the rule by late 2008. This long and fairly intensive process resulted in improvements to ISAs that addressed many of the potential weaknesses of ISAs. Specifically, guidance was developed on treatment of initiating events, external events, dependencies, and quantification of accident frequencies. This guidance has been incorporated as Appendices to Chapter 3 of Reference 1. This process of improvements to ISAs continues today, supported by the NRC inspection program. Some of these issues that relate to ISA-PRA differences will be discussed below.

Process Interactions

Correctly addressing interactions between processes, where an upset in one process affects another, was one of these issues. One reason it arises is that processes are usually analyzed separately in ISAs. However, impacts of accidents in one process on another are analyzed in ISAs. In fact, this is what is meant by “integrated” in the term ISA. In some cases, processes are reasonably isolated because outputs are tested before being input to the next process. Fire, chemical, and criticality interactions are always considered. Some types of chemical process upsets are difficult to anticipate, and hence the effect on subsequent processes may be overlooked.

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 independence of controls arose early during performance of the ISAs; and NRC staff provided guidance in ISG-1, which has now been incorporated in Chapter 3 of the revised SRP (Reference 1). Facility methods of correcting for common cause vary from taking no credit for the second control to applying a dependence factor, as in the beta factor method. Licensees are very aware of issues of common cause and dependency due to the prominence of the “double contingency principle” from the basic ANSI/ANS 8.1 criticality safety standard. The double contingency principle is often part of a commitment in fuel facility licenses. Independence of human actions was another area of discussion between NRC and industry. Appendix B to Chapter 3 of Reference 1 provides some guidance on this issue.

Conservatism

It is not possible to say whether ISAs as a whole are conservative or not. However, the fact that certain sequences, as presented in the ISAs, contain conservatisms—if regarded as a risk estimate—is not a defect for the purposes of compliance purposes of Part 70. The major non-conservatism, based on events and findings subsequent to the ISAs, appears to be due to screening out of sequences that are actually plausible. Under Part 70, the objective is to identify sequences and IROFS, not to estimate risk. In the end, NRC staff evaluations of ISAs have, so far, concluded that the ISAs are acceptable for the purposes of the safety program of 10 CFR 70. This state was reached only after a long process of development and review.

ISA Team Issues

Reference 5 is a paper discussing application of PRA techniques to ISAs by a licensee who has done this. 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 PRA experts considerable time to become familiar with plant processes, due to the large number and diversity of such processes. This personnel experience situation may have more influence on ISA results than purely methodological issues.

IV. Context of Significance Determination in the Fuel Cycle Oversight Program

If the oversight process for FC facilities was revised to be risk-informed and systemtic, similar to the reactor oversight program, one element of the process would be a SDP. This SDP would use risk insights to evaluate the significance of identified licensee performance deficiency against defined thresholds. The determination of risk significance within the SDP would be conducted in phases. The initial phase would be a screening review, based on qualitative criteria, to identify whether an inspection finding would clearly not result in a significant increase in risk, and thus need not be analyzed further (a ‘green’ finding. Based on analysis of past inspection findings, 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/or consequences of accident sequences would be quantified.

A hypothetical example of such a quantitative risk impact evaluation is described in Section V below. This quantitative (or more detailed qualitative) risk assessment would categorize the findings into categories; such as green, white, yellow, or red—based on its risk impact. Since worker safety plays a large role in NRC’s regulation of FC 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 quantitative risk significance evaluation using different methods. A full SDP 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. Critical Evaluation of ISA-PRA for Use in the FCOP SDP

This section provides a critical evaluation of ISA and PRA results as used for risk significance determination of inspection findings (deficiencies) as might be done in a revised FCOP. This is done by first demonstrating the use of ISA risk index results versus PRA-like quantitative accident sequence frequency results in obtaining risk significance metric for a hypothetical, but typical, fuel cycle process. The characteristics illustrated by this example can then be used to evaluate the ISA-PRA differences for this application. The length of the narrative necessary to explain the example may distort the messages of this section into an undue emphasis on the accuracy of quantitative versus risk index method based quantification of risk significance. This difference in quantitative accuracy, while possibly important in specific cases, is not necessarily the most important message here. Rather, the important messages are 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 can be done for each deficiency when it occurs and do not require evaluation of all accident sequences in a facility.

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

The results of either of these types of ISA evaluations, quantitative or risk index can be used to evaluate risk significance of FC inspection findings in very much the same way as in the ROP. However, there are difficulties in doing this in a way that accurately reflects the risk significance of the finding because ISAs were not done to obtain risk estimates.

<u>Description of a Hypothetical Example Process</u>

An example process will be analyzed here 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 will then be critically evaluated against various factors in the context of this specific purpose of risk significance determination.

For this example analysis, we postulate a process consisting of a tank, two 10-foot sections of piping, two flange connections, and two manual valves. An enriched uranium solution flows through the system. The process is protected by a floor dike to retain solution that may escape the system. The dike has a surveillance inspection for leaks once every two years. The diked area has a sub-critical 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.

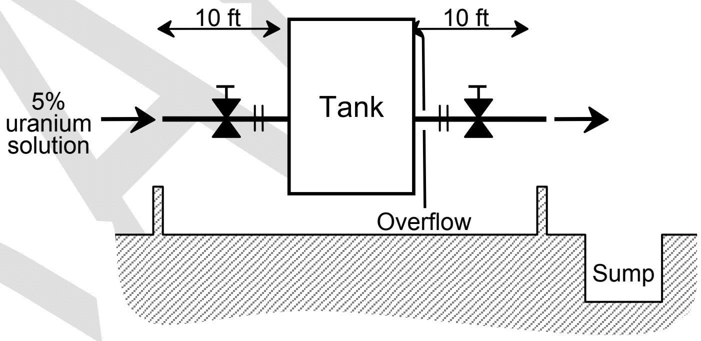

Figure 1 Hypothetical system

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 event) are a process leak and a process overflow.

Every two years a surveillance is to be done to determine if the dike is intact, that is, it 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 in terms of 10 CFR 70.61.

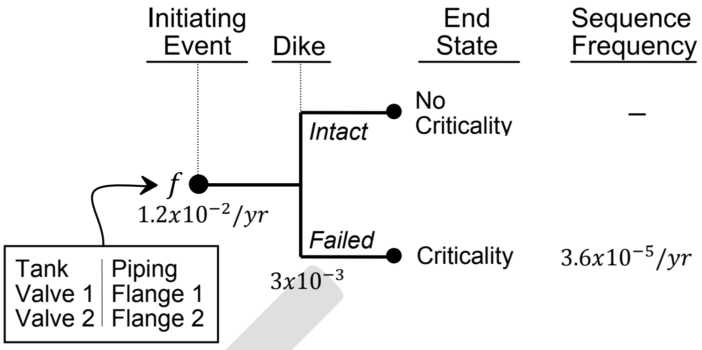

Figure 2 Event tree model.

PRA 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 Reference 2, which is a database of generic component failure data for facilities similar to FC plants. The "process leak" initiating event frequency, 1.2x10^{-2} /yr, is the sum of 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 two years between surveillances, so the average time spent in the "down," or failed, state is one-half the two-year surveillance interval, that is, one 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 /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. The dike failure frequency estimate of 0.003 /yr is postulated here to have been based on plant experience with diked areas. Thus the criticality accident resulting from the sequence process leak - dike leak is (1.2x10^{-2} /yr)(0.003) = 3.6x10^{-5} /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. The probability that the dike is in a leaking, given this initiator, is the same as above, namely 0.003. Thus this sequence leading to a criticality has a frequency of (0.005 yr)(0.003) = 1.5x10^{-5} /yr.

The sum of the sequence frequencies for process leak plus overflow yields a total frequency of a criticality accident of 5.1 x10^{-5} /yr.

Relation Between Quantitative (PRA) and Risk Index Methods of Frequency 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) process leaking or not, and 2) dike leaking or not. We write U_p as the probability that the process is leaking at any given point in time, and U_d as the probability that the dike is leaking. Then the dominant way that one could enter the state where both are leaking is to be in the state where the dike has developed a leak, and then the process leaks before this is corrected. The probability of being in the given state is: $U_d(1 – U_p)$.

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

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

where λ_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, τ_d, and the frequency, λ_d, that the dike fails.

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

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

$$U_d = \lambda_d \tau_d$$

To obtain a risk index model,

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

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

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

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 would be regarded as “passive engineered controls,” and are each assigned a frequency index value of $I_p = I_d = -3$.

Since surveillance examinations of the dike occur every two years, the average length of time that the dike would be in a failed condition before it is discovered would be one year. Since 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; that is

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

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

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

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 “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 conservative, which is acceptable for the purposes of determining compliance with the requirement that “high-consequence” events be “highly unlikely.” Thus these likelihood evaluations for ISA are often not realistic estimates of risk.

Critical Evaluation of the Accuracy of Risk Index ISA versus PRA

The results from the two accident frequency evaluation methods are compared in Table 1.

Table 1

	PRA		ISA		
	initiating event	failure on demand event	passive control initiator	passive control failure on demand	
Level Of Assessment	Tank Valve 1 Valve 2 Flange 1 Flange 2 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	$3.6x10^{-5}/yr$		-1		
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; as will be shown in the example below.

The results of the PRA method and the risk index methods are compared in Table 2. The risk indices have been shown their exponential equivalent. 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 compiled failure rate information that is typically used for a PRA can have more narrowly defined groups. While Reference 1 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: passive controls = -3, active controls = -2, and administrative control = -1.

Table 2 Comparison of results from the PRA and the Risk Index Methods

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

For certain types of SSCs in FC facilities, such as the dike in this example, failure rate data is 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 Reference 2 is considered “generic” for processing facilities, and hence highly uncertain. Reference 2 gives an error factor (95th percentile / median) of 10 for the component leak frequencies used for the “process leak” initiator. 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

A risk significance metric for a specific deficiency is illustrated using the results in Table 2 and a postulated deficiency. The postulated deficiency is some action that inadvertently left the dike in a leaking condition. Furthermore, this compromised condition was not detected due to failure to conduct surveillance for four years. Given that the dike was compromised, either a process leak or an overflow would result in a criticality accident, since the leaking fissile solution would flow into the unsafe geometry sump. The accident frequency has increased from its original value of λ_b = 3.6E-5 /yr + 1.5E-5 /yr = $5.1\text{x}10^{-5}$ /yr to the sum of the frequencies of the initiating events, λ_d = $1.2\text{x}10^{-2}$ /yr + $5\text{x}10^{-3}$ /yr = 1.7 $\text{x}10^{-2}$ /yr. Originally the baseline probability that the high-consequence accident would happen during the time t = 4 years was supposed to be
Pr(high consequence | baseline) = 1 – exp(-λ_b t) = $2\text{x}10^{-4}$

Due to the deficiency the probability was actually

Pr(high consequence | deficiency) = 1 – exp(-λ_d t) = 0.066

The metric used here to determine risk significance of deficiencies for FC 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 ROP.

Using the quantitative (PRA) accident frequencies this increase is just
delta Pr(high consequence) = Pr(hc | deficiency) - Pr(hc | baseline) = 0.066 - $2\text{x}10^{-4}$ ≈ 0.066

Alternatively, using the results from the risk index ISA from Table 2, the sequence indices in the case of the deficiency are -3 for the process leak and -1 for the overflow, which are equivalent to a 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 = 1.01×10^{-4} /yr. Substituting into the equation for the delta probability yields a change in probability of

delta Pr(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. Furthermore, a factor of 5, or even 10, as an estimate of 95th/50th percentile uncertainty in quantitative PRA frequencies is not uncommon.

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 0.01, the threshold of moderate significance 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 > .01), while the quantitative frequency method would yield “moderate” (.001 < .066 < .01).

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 <u>change</u> 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. It is not necessary to pre-evaluate the risk to all individuals from all accidents. Such pre-evaluation, even just of all individual accident sequence frequencies in the ISA without summation, would involve numerous controls and sequences; yet, very few of these evaluations would ever be used. For example, there are only about two significant criticality violations per plant per year; yet, there could be hundreds of safety controls in the facility.

<u>Aspects of ISA Influencing a Significance Determination</u>

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, non-conservatisms 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 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. Some of the practices which cause ISA results to be significant inaccurate estimators of risk will be 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 offsite, 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 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 is not made. Such conservatisms, even when large, are not a defect when using the ISA for compliance purposes; but for risk significance such deviations are too large.

ISA analyses of some processes do not take credit for all safety controls as IROFS; so these controls are not mentioned in ISA documentation. Thus, 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.

There have been some instances where ISAs of a particular process were non-conservative. Generic non-conservatisms with ISA methods are usually corrected during NRC staff review of the ISA; but individual sequences overlooked in one particular process are difficult to detect. For example, one type of non-conservatism is improperly screening an event out 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 Reference 1. Furthermore, the ISA Summary typically does not list all events which have been screened out. In cases where the inspection itself has discovered the omitted accident sequence, its omission in the ISA is not a problem for the SDP since the significance determination can simply take it into account.

The risk index method itself, if regarded as an estimate of accident frequency for use in risk significance evaluations, is so uncertain that such results may differ from a PRA-like evaluation in either direction by a substantial amount.

The simple process used in the example evaluations above does not illustrate one difference between ISAs and reactor-like PRAs that could exist, namely analysis of complex control systems with dependencies. NUREG-1513 recommends use of fault tree/event tree modeling in such cases. However, many of the controls in FC facilities are quite simple, as in the example above. One particular type of dependency, loss of power, is not a safety issue for most processes in most FC 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 onsite, but this is to permit orderly process shutdown, not usually for safety. One exception is the negative pressure confinement system in the MOX plant.

Table 3 below summarizes the critical ISA-PRA evaluations discussed in this paper, in the context of risk-significance evaluation in an FCOP.

Table 3. Critical Evaluation of ISA-PRA Differences for Fuel Cycle Risk-Significance Determination

Issues in Assessing Risk Significance	**ISA**	**PRA**	**Implication for FCOP Applications**
end states	high or intermediate consequences (see 70.61)	LERF[1], CDF[2], etc.	Can use probability of high or intermediate consequences for SDP[3]
completeness of accident sequences	Instances of improper screening out of sequences have been observed.	Experienced fault tree practitioners usually avoid improper screening.	The possibility of incompleteness should be considered in SDP.
Quantification of accident sequences	A few ISAs are quantified, most use risk index method of Ref. 1 Chap. 3	PRAs are always quantified and common cause considered.	Inadequacies of ISA quantification will have to be corrected for each SDP evaluation, if needed.
Modeling of physical/chemical phenomena	ISAs often use conservative assumptions	PRAs typically use realistic calculations	Very large conservatisms will require correction in SDP.
offsite consequences	ISAs use bounding weather assumptions.	Level 3 PRAs use realistic statistical consequences	Needs to be corrected in individual SDP evaluations.
Internal fire modeling	ISAs always consider fire scenarios and interactions.	PRAs include detailed fire analysis if in-scope	Guidance may be needed for consistency among facilities
Inconsistency due to differing modeling assumptions	ISAs of fuel cycle facilities vary significantly from one another.	PRA modeling of Fuel Cycle Facilities would need development.	Significance determination needs guidance to make evaluations consistent across licensees.
Level of detail of modeling	ISAs often use simplified models	PRAs usually have more detail, especially in human actions and dependencies.	For SDP more detail may be needed in certain cases, but most designs are simple.
Treatment of hardware failures	Hardware failures are addressed at sub-system level.	Individual components are modeled.	In specific cases, sub-system level may be too inaccurate.
Treatment of human errors (HEs)	Some ISAs are simplistic and have only one value for human error.	PRAs use a systematic human reliability assessment (HRA).	Human error analysis applicable to fuel cycle may need development.
Completeness of safety control systems analyzed.	Some ISAs do not take credit for all safety controls as IROFS.	PRAs typically will address all applicable controls.	Existence of additional controls will need to be assessed in each SDP case.

Issues in Assessing Risk Significance	**ISA**	**PRA**	**Implication for FCOP Applications**
input data for assessment	Many ISAs use single failure probability based on active, passive, or administrative control	PRAs use quantitative data for hardware and human reliability.	Rough ISA results may sometimes be good enough, sometimes not.
treatment of dependency and system interactions	Dependencies considered in double contingency analysis; sometimes quantitatively.	PRAs attempt to systematically treat dependency and system interactions.	Occasionally important.
risk metrics	ISAs assess individual accident sequences; not risk to individuals.	PRAs traditionally calculate risk to individuals.	The summation necessary for risk significance would have to be done for each evaluated inspection finding.
uncertainty and importance measure evaluation	ISAs do not quantify uncertainty or importance; but ISA results have been used for importance evaluation.	PRAs typically include uncertainty analysis.	For FCOP applications, uncertainty analyses may not be needed.

1. Large Early Release Frequency 2. Core Damage Frequency 3. Significance Determination Process

<u>Conclusions</u>

The numerous ISA-PRA differences listed in Table 3 above may give the impression that ISAs are deficient. But some ISAs have used PRA methods extensively; and other ISAs have used them selectively, as recommended in NRC guidance (Reference 4). ISAs were performed to identify accidents and IROFS, not estimate risk, as PRAs do. As a result of substantial reviews of each ISA, for those which have been approved, NRC staff has concluded that the ISAs have succeeded in this objective and are acceptable for compliance.

On the other hand, for risk significance determination, caution should be exercised in using ISA results. ISAs were not performed to produce complete and accurate estimates of risk. In some cases ISA results provide a reasonable risk estimate of sequence frequencies and consequences; in other cases not. Thus, modifications may need to be made in using these results for risk significance evaluation in a FC oversight process.

As illustrated in the example in Section V, it appears to be feasible for NRC staff to perform quantitative risk significance evaluation for each inspection finding that is a safety deficiency at the time the deficiency is found. This is because, typically only a few accident sequences in one process will be affected by the deficiency. It is not necessary to pre-evaluate the frequencies of all accident sequences in all processes. Based on analysis of previous inspection findings, only a few of them would require such quantitative significance evaluations each year

References

1. USNRC, NUREG-1520 Rev. 1, Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility, May 2010.
2. Westinghouse Savannah River Co., WSRC-TR-93-262, Savannah River Site Generic Database Development, June 1993.
3. Benhardt, H. C. et al., WSRC-TR-93-581, Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities, Feb 1994.
4. USNRC, NUREG-1513, Integrated Safety Analysis Guidance Document, May 2001.
5. 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.