A COMPARISON OF INTEGRATED SAFETY ANALYSIS AND PROBABILISTIC RISK ASSESSMENT

Dennis R. Damon
Nuclear Regulatory Commission, United States

Kevin S. Mattern
Nuclear Regulatory Commission, United States

Abstract – The U.S. Nuclear Regulatory Commission conducted a comparison of two standard tools for risk informing the regulatory process, namely, the Probabilistic Risk Assessment (PRA) and the Integrated Safety Analysis (ISA). PRA is a calculation of risk metrics, such as Large Early Release Frequency (LERF), and has been used to assess the safety of all commercial power reactors. ISA is an analysis required for fuel cycle facilities (FCFs) licensed to possess potentially critical quantities of special nuclear material. A PRA is usually more detailed and uses more refined models and data than an ISA, in order to obtain reasonable quantitative estimates of risk. PRA is considered fully quantitative, while most ISAs are typically only partially quantitative. The extension of PRA methodology to augment or supplant ISAs in FCFs has long been considered. However, fuel cycle facilities have a wide variety of possible accident consequences, rather than a few surrogates like LERF or core damage as used for reactors. It has been noted that a fuel cycle PRA could be used to better focus attention on the most risk-significant structures, systems, components, and operator actions.

ISA and PRA both identify accident sequences; however, their treatment is quite different. ISA's identify accidents that lead to high or intermediate consequences, as defined in 10 *Code of Federal Regulations* (CFR) 70, and develop a set of Items Relied on For Safety (IROFS) to assure adherence to performance criteria. PRAs identify potential accident scenarios and estimate their frequency and consequences to obtain risk metrics. It is acceptable for ISAs to provide bounding evaluations of accident consequences and likelihoods in order to establish acceptable safety; but PRA applications usually require a reasonable quantitative estimate, and often obtain metrics of uncertainty. This paper provides the background, features, and methodology associated with the PRA and ISA. The differences between the approaches are enumerated and their potential use in regulating fuel cycle safety is discussed. A critical evaluation of the application to FCFs including, hazards, completeness, adequacy, interactions, common causes, and personnel is performed. The application of both methodologies to various inspection and assessment tools is discussed. The regulatory advantages of the PRA, namely, the ability to quantify uncertainty and provide importance measures, are provided. The paper concludes that, while the ISA method is sufficient to establish an adequate safety basis, PRA is able to provide additional insights such as risk significance, uncertainty assessment, and prioritisation of safety features.

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[19] and NUREG-1513[20].

B. Regulatory uses of integrated safety analyses

1. Performance requirements

ISAs are directly used for compliance with the performance requirements in 10 CFR 70.61. The ISA is used 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)[1]. 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.

2. 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.

3. 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.

C. Technical features of an integrated safety analysis

1. 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. Most accident sequences that are identified in ISAs as exceeding these consequence thresholds involve consequences to the workers rather than the public. 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,

[19] 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.

[20] U.S. Nuclear Regulatory Commission, "Integrated Safety Analysis Guidance Document," NUREG-1513, May 2001.

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.

2. 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, 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.

3. 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[21] [22]. Human error probabilities might also be estimated based on plant experience. Human reliability modeling is typically not applied.

4. 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 a realistic estimate of 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.

5. 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. 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.

[21] Alber, T. G., et al., "Idaho Chemical Processing Plant Failure Rate Database", INEL-95/0422, August 1995.

[22] H.C. Benhardt, et al., "Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities," WSRC-TR-93-581, February 1994.

6. 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. In many cases releases are simply assumed to produce high-consequence doses as defined in 10 CFR 70.61.

7. 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[20]. Worker doses, if not calculated, are often 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 so, are acceptable for assurance of safety under 10 CFR Part 70, Subpart H.

8. 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.

9. 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.

II. Probabilistic 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.

B. 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. 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 aim 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.

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

C. Probabilistic risk assessment in fuel cycle facilities

No facility wide PRAs have been carried out for fuel cycle facilities in the United States; however, some limited analysis has been performed focusing on particular accidents that identified common-cause failures and human errors as 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.

III. Critical evaluation of integrated safety analysis and probabilistic risk assessment for safety under 10 CFR part 70

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. 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.

1. 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. For low-enriched uranium facilities, criticality can be controlled by independent controls on mass and moderation. Automatic controls are less common, as is dependence on power or other active support systems.

2. 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 programme required by 10 CFR Part 70.

3. 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. 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. 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. 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.

4. 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 phrase ISA.

5. 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[1]. 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[23]. A commitment to apply the double contingency principle is often part of a fuel facility license.

6. 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[24]. 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 in the context of whether a more PRA-like analysis would produce a better ISA result with respect to the ISA's function of assuring safety.

[23] American Nuclear Society, Nuclear, "Criticality Safety in Operations with Fissionable Materials Outside Reactors", ANSI/ANS 8.1, 1998.

[24] 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.

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	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 contingency[23] 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 ISA and PRA 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. 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 set of inspection findings, the effect on the likelihood and consequences of accident sequences could be evaluated in more detail.

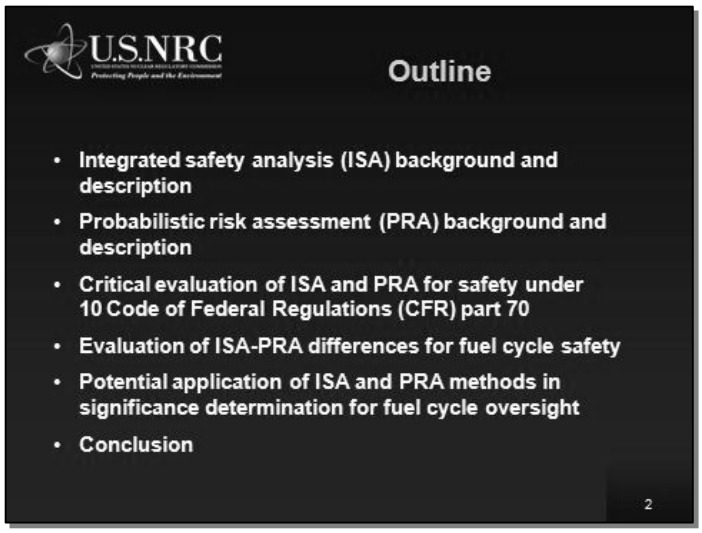
A quantitative (or more detailed qualitative) risk assessment would categorize the findings into broad categories based on its risk impact. Fuel cycle facility processes are capable of producing accidents with a variety of consequences, such as direct doses from nuclear criticality, doses from exposure to radioactive material, and various effects from exposure to toxic chemicals. Because worker safety plays a large role in the NRC's regulation of fuel cycle facilities, accidents at these facilities can affect multiple categories of receptors, the public outside the controlled area, as well as workers. Thus multiple risk significance metrics will, in principle, have to be used. In practice however, a single safety deficiency typically only affects one type of accident in one unit process. For example, a retention dike under a process containing fissile solution assures that a leak or overflow from the process assumes a sub-critical geometry, thus preventing a criticality accident. If such a dike were disabled for some period of time, an additional risk of large radiation dose from a criticality beyond that planned in the design would be imposed on nearby workers. One metric of risk significance would be this additional risk of large dose imposed on the nearest worker. The metric would be the increase in frequency of criticality with the dike disabled times the duration of the

disabled condition. This quantity is thus a probability of the accident that was incurred by the worker because of the disabled dike. Typically, such a deficiency only affects a few accident sequences, in this case those causing a leak or overflow of fissile solution into the dike. The limited scope of processes and accident sequences affected by a single deficiency may thus make it feasible for NRC staff to perform such risk significance evaluations for deficiencies on a case-by-case basis using realistic risk evaluations, even though the ISA for the process may not have been fully quantitative, or may have been very conservative. A full safety significance determination process and quantitative risk significance approach remains to be developed and tested. It could involve a mixture of qualitative and quantitative methods, depending on the situation to be analyzed and availability of information.

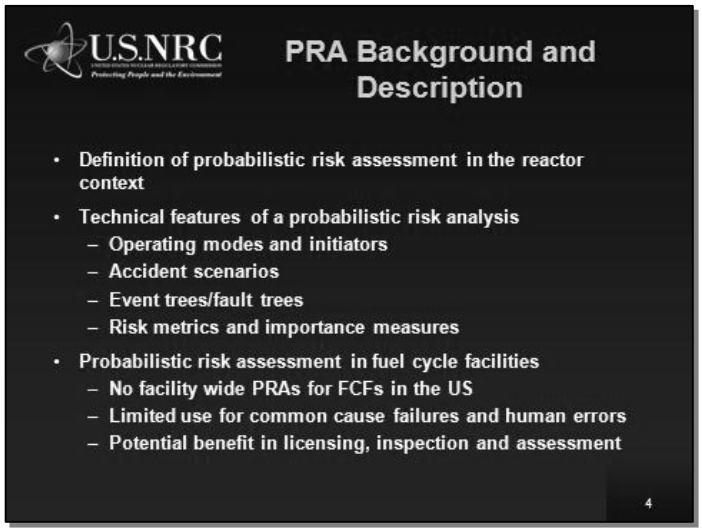
Conclusion

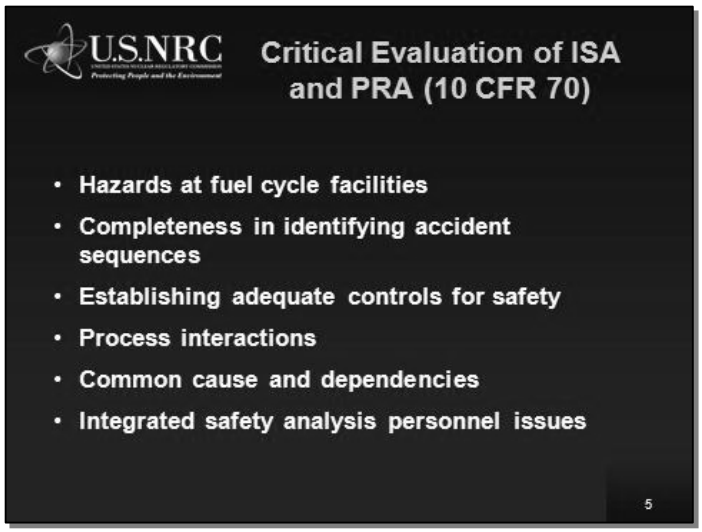
Fuel cycle ISAs and reactor PRAs are performed for different purposes. Some ISAs have used several PRA methods extensively, and other ISAs have used them selectively, as recommended in NRC guidance[20]. ISAs were not performed to estimate risk as PRAs do. ISAs were performed to identify potential accident 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, thus PRA methods should continue to be explored during future efforts in assessment of fuel cycle safety.

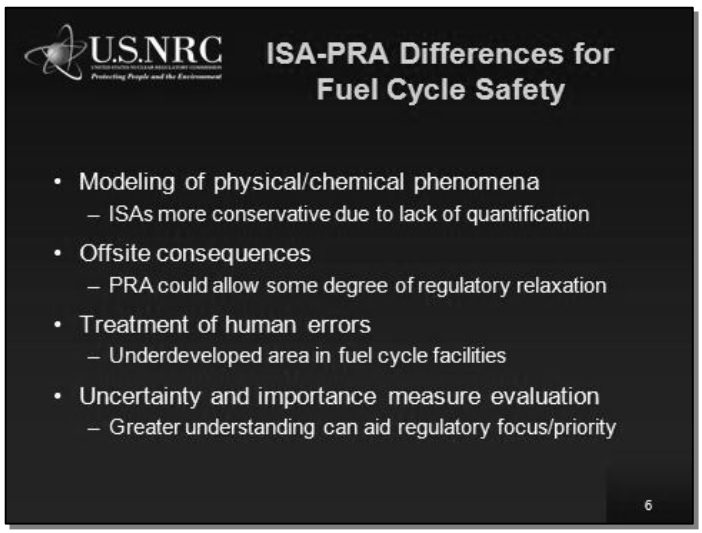

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment
A COMPARISON of INTEGRATED SAFETY ANALYSIS and PROBABILISTIC RISK ASSESSMENT
NEA/CSNI Workshop on
Safety Assessment of Fuel Cycle Facilities – Regulatory Approaches and Industry Perspectives
Dennis R. Damon and Kevin S. Mattern
Nuclear Regulatory Commission, United States
Toronto, Canada
September 27-29, 2011


U.S.NRC
Outline
• Integrated safety analysis (ISA) background and description
• Probabilistic risk assessment (PRA) background and description
• Critical evaluation of ISA and PRA for safety under 10 Code of Federal Regulations (CFR) part 70
• Evaluation of ISA-PRA differences for fuel cycle safety
• Potential application of ISA and PRA methods in significance determination for fuel cycle oversight
• Conclusion
2


U.S.NRC
ISA Background and Description
• Definition of integrated safety analysis
• Regulatory uses of integrated safety analyses
– 10 CFR 70.61
– Performance requirements
– Items relied on for safety (IROFS)
– Management Measures
• Technical features of an integrated safety analysis
– End states
– Accident sequences
– Credible events
3


U.S.NRC
Protecting People and the Environment
PRA Background and Description
• Definition of probabilistic risk assessment in the reactor context
• Technical features of a probabilistic risk analysis
– Operating modes and initiators
– Accident scenarios
– Event trees/fault trees
– Risk metrics and importance measures
• Probabilistic risk assessment in fuel cycle facilities
– No facility wide PRAs for FCFs in the US
– Limited use for common cause failures and human errors
– Potential benefit in licensing, inspection and assessment
4


U.S.NRC
Protecting People and the Environment
Critical Evaluation of ISA and PRA (10 CFR 70)
• Hazards at fuel cycle facilities
• Completeness in identifying accident sequences
• Establishing adequate controls for safety
• Process interactions
• Common cause and dependencies
• Integrated safety analysis personnel issues
5


U.S.NRC
Protecting People and the Environment
ISA-PRA Differences for Fuel Cycle Safety
• Modeling of physical/chemical phenomena
– ISAs more conservative due to lack of quantification
• Offsite consequences
– PRA could allow some degree of regulatory relaxation
• Treatment of human errors
– Underdeveloped area in fuel cycle facilities
• Uncertainty and importance measure evaluation
– Greater understanding can aid regulatory focus/priority
6

ISA and PRA in Significance Determination

- Realistic and predictable process for assessing the risk significance of inspection findings
- Use qualitative and quantitative risk insights to evaluate the significance of licensee performance deficiencies
- Risk significance evaluations for deficiencies on a case-by-case basis using realistic risk evaluations
- A mixture of qualitative and quantitative methods, depending on the situation to be analyzed and availability of information

7

Conclusion

- Fuel cycle ISAs and reactor PRAs are performed for different purposes
- ISAs were not performed to estimate risk as PRAs do
- ISAs identify potential accident sequences, designate IROFS to prevent or mitigate them, and describe management measures to be applied to assure IROFS reliability and availability
- ISA methods and processes have succeeded in meeting their objective and are acceptable for assuring safety under 10 CFR Part 70
- ISAs of specific processes may contain some potential deficiencies
- PRA methods should continue to be explored during future efforts in assessment of fuel cycle safety, including significance determination

8

Questions/Contact

Questions?

Contact:
Kevin S. Mattern
US Nuclear Regulatory Commission
Washington, DC 20555
kevin.mattern@nrc.gov
1-301-492-3221

9