HITACHI

GE Hitachi Nuclear Energy

Jerald G. Head
Senior Vice President
Regulatory Affairs

P.O. Box 780
3901 Castle Hayne Road
MC A09
Wilmington, NC 28402
USA

T 910 819 5692
F 910 362 5692

June 4, 2010

MFN 10-174

Daniel H. Dorman, Director
Division of Fuel Cycle Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Transmittal of Paper Presented at Industry Conference: "Applying Nuclear PRA to a Nuclear Fuel Facility Integrated Safety Analysis"

Dear Mr. Dorman,

On April 29, 2010, the U.S. Nuclear Regulatory Commission ("NRC") Staff briefed the Commission on Fuel Cycle Oversight Process revisions. In a May 12, 2010, Commission Staff Requirements Memorandum ("SRM") related to the briefing, the Commission requested of the Staff a "concise paper comparing Integrated Safety Analyses (ISAs) for fuel cycle facilities and Probabilistic Risk Assessments (PRAs) for reactors, including a critical evaluation of how ISAs differ from PRAs." The SRM indicated that the Staff should submit the paper to the Commission by October 29, 2010.

GEH has been interested in applying risk information to fuel cycle operation and assessments of safety and is participating in the 10th International Probabilistic Safety Assessment and Management Conference, June 7 - 11, 2010 (*see* http://www.psam10.org/). As part of the conference, a GEH attendee will be presenting a paper on applying nuclear PRA methodology to a fuel facility ISA. The paper will be published as part of the conference proceedings. GEH has obtained approval to submit the paper to the NRC for your use in addressing the Commission's SRM. Accordingly, a copy of the paper is enclosed.

While the paper asserts that nuclear PRA can be adopted by an ISA to "help narrow this gap between an ISA's ambition and its comprehensiveness," the paper does not represent application of PRA techniques for any specific fuel cycle facilities. It is submitted for information only and is not, at this time, related to any ongoing action with the NRC.

NMSS01

Please contact me if you have any questions regarding the paper.

Sincerely,

Jerald G. Head

Enclosure

Cc: Document Control Desk, NRC

(Via E-Mail w/enclosure):
Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
R. W. Borchardt, NRC EDO

Reference:

1. Memorandum, A. Vietti-Cook to R. W. Borchardt, "Staff Requirements – Briefing on the Fuel Cycle Oversight Process Revisions" (May 12, 2010).
2. eDRF 0000-0118-4850.

Enclosure:

1. M. Warner, J. Young, "Applying Nuclear PRA to a Nuclear Fuel Facility Integrated Safety Analysis" (June 2010).

Applying Nuclear PRA to a Nuclear Fuel Facility Integrated Safety Analysis

Matthew Warner[a*], **Jim Young**[a*]
[a]GE Hitachi Nuclear Energy, Wilmington, NC, USA

Abstract: Nuclear fuel processing facilities are required to conduct an integrated safety analysis (ISA) as part of the licensing process. An ISA identifies potential accident sequences, designates items relied on for safety (IROFS), and describes management measures to provide reasonable assurance of IROFS availability and reliability. IROFS are intended to either prevent initiating events or mitigate accident consequences to an acceptable level. The ISA process also identifies and evaluates all internal initiating events (e.g., explosions, spills, and fires); and external initiating events (flooding, high winds, earthquakes, and external fires) that could result in facility-induced consequences to workers, the public, or the environment.

Nuclear PRA methodology can be utilized for an ISA at a nuclear fuel processing facility. Applying the knowledge base that exists in the nuclear PRA industry to a fuel facility ISA can improve the quality and efficiency of the ISA. To do this, the training and oversight of the non-risk professionals on the ISA team is vital. Key areas to emphasize are precise definitions of initiators and IROFS, the multiple manifestations of dependency, and the use of quantitatively based data.

Keywords: PRA, IROFS, Integrated Safety Analysis, Fuel Fabrication Facility.

1. INTRODUCTION

Nuclear power plant Probabilistic Risk Assessment (referred to hereafter as PRA) has grown in popularity since the Individual Plant Examinations of the early 1990s. The growth can be attributed to more than just the assurance that the risk to the public from operating plants is acceptable. More practically, the insights gained from these exhaustive analyses have helped the industry and its regulator better focus resources through a risk informed culture.

The use of risk insights in the nuclear industry is not confined to nuclear power plants. Nuclear fuel facilities use risk information to identify the systems, components and operator actions most important to chemical, radiological and criticality safety. To discover and/or confirm these features, fuel facilities in the United States are required to develop an Integrated Safety Analysis (ISA)—mandated by the U.S. Nuclear Regulatory Commission (NRC) rule 10 CFR Part 70, Subpart H [1]. A nuclear fuel facility ISA does not typically receive the same resources as a PRA both in the initial construction and in the continuing maintenance. Therefore, ISAs tend to be less comprehensive and less detailed resulting in a more qualitatively based analysis. Yet, they are very ambitious in that they established the safety controls the facility will rely upon and become commitments to the NRC.

The assertion of this paper is that the advancements made in nuclear PRA can be carefully adopted by an ISA to help narrow this gap between an ISA's ambition and its comprehensiveness. The evolution of PRA has led to the development of standards—the ASME/ANS level 1 PRA standard [2] will be discussed in this paper—which provide a substantial set (hundreds) of requirements that a PRA can be viewed against. Each of these requirements has been vetted by top industry experts making these PRA standards one of the most complete and practical resources on the topic of risk available today inside or outside of nuclear PRA. Additionally, the collection of guidance documents referred to in the standards can supply the commonly chosen methods that fulfill the requirements. A subset of the

numerous requirements and guidance material can be adapted by a risk professional to significantly improve the quality and efficiency of an ISA.

If such an adoption of PRA practices is attempted, a need to balance the wealth of information with the realities of a limited budget will likely be recognized. Also quickly recognized is the stark difference in the makeup of the ISA team as compared to a PRA team. An ISA team is typically weighted heavily with facility experts that, although highly talented in their field, are typically inexperienced in risk. The minority representation by risk professionals necessitates the training of facility experts in fundamental risk concepts and the ownership of the more advanced risk tasks by the risk experts.

How to choose the PRA practices and impart them to the ISA team while not becoming critical path is the focus of this paper. The most vital PRA practices that can be adapted to produce a sound and more quantitatively based ISA are presented.

A familiarization, though, is first needed with what an ISA is and how it differs from a PRA.

2. SUMMARY OF A FUEL FACILITY ISA AND COMPARISON TO A PRA

The NRC's key reference on the topic, NUREG-1520 [3], describes the purpose of an ISA:

> An integrated safety analysis (ISA) identifies potential accident sequences in the facility's operations, designates items relied on for safety (IROFS) to either prevent such accidents or mitigate their consequences to an acceptable level, and describes management measures to provide reasonable assurance of the availability and reliability of IROFS.

This definition shows how aggressive an ISA is in its ambition in that it, "...designates items relied on for safety...". It is this definition that necessitates a quality analysis rooted in sound risk principles.

The NRC has developed two key references on the topic. The previously mentioned NUREG-1520 lays out acceptance criteria while NUREG-1513 [4] provides general guidance on preparing and documenting one. The pertinent areas in NUREG-1520 relating to ISA are Chapters 3 and 11. Although part of the Standard Review Plan (SRP) for a fuel facility's license application, the ISA and its summary are not part of the facility's license.

To identify the potential accident sequences, all credible initiating events (IEs) both internal and external are to be included. External events include floods, high winds, earthquakes, transportation accidents, and accidents at nearby industrial facilities among others. In the identification of initiating events, an ISA and a PRA are similar. Both employ inductive and/or deductive methods such as Failure Modes and Effects Analysis (FMEA) and Master Logic Diagram. An ISA, however, does not usually group initiators to the degree seen in typical PRAs. This leads to a proportionally greater number of IEs in an ISA. This is understandable since a fuel facility tends to have more distinct, stand-alone processes than a nuclear plant.

A hazard can be screened, but only when its unmitigated consequences do not exceed certain levels or, as stated above, when it is considered not credible. Before IROFS are determined, the unscreened hazards must have their unmitigated consequences determined. NUREG-1520, Table A-1, shown on the next page, presents the 10 CFR 70.61 chemical and radiological consequence severity limits:

Table 1: NUREG-1520 Table A-1: Consequence Severity Categories Based on 10 CFR 70.61

	Workers	Offsite Public	Environment
Category 3 High Consequence	*RD> 1 Sievert (Sv) (100 rem) **CD = endanger life	RD> 0.25 Sv (25 rem) 30 mg sol U intake CD = long-lasting health effects	
Category 2 Intermediate Consequence	0.25 Sv (25 rem) <RD ≤ 1 Sv (100 rem) CD = long-lasting health effects	0.05 Sv (5 rem) <RD ≤ 0.25 Sv (25 rem) CD = mild transient health effects	Radioactive release >5000 x Table 2 of 10 CFR Part 20 Appendix B
Category 1 Low Consequence	Accidents of lower radiological and chemical exposures than those above in this column	Accidents of lower radiological and chemical exposures than those above in this column	Radioactive releases producing lower effects than those referenced above in this column

* RD = Radiological Dose
** CD = Chemical Dose

For those accidents judged to have intermediate or high consequences, IROFS must be developed to mitigate. IROFS are similar to safety related components in a nuclear plant. When credited with mitigating a certain accident, the ISA definition states that, "management measures to provide reasonable assurance of the availability and reliability of IROFS," must be maintained.

The mitigated likelihood of high consequence accident sequences must be considered 'highly unlikely', while those of intermediate consequences must be 'unlikely'. NUREG-1520 provides assistance with these terms by presenting acceptance criteria, shown in Table 2 below, for an applicant's quantitative definitions.

Table 2: NUREG-1520 quantitative guidelines for likelihood terms

Likelihood term of 10 CFR 70.61	Guideline
Unlikely	Less than 10^{-4} per-event per-year
Highly Unlikely	Less than 10^{-5} per-event per-year

The units in the above guideline introduce a key distinction in an ISA. The consequence likelihood is judged on a per event[1] basis only. Unlike a PRA, where accident sequences leading to an undesired end state (such as CDF and LERF) are combined, an ISA can isolate and focus on one accident sequence at a time against the guidance. The NUREG advises that since the focus is on a per event basis, "the likelihood of each individual sequence must be quite low." This emphasizes the need for a facility to have IROFS in place that keep accident sequences more than just narrowly below a limit. Rather, they should aim for likelihoods consistently well below the threshold to ensure the cumulative risk is kept as low as possible even though the accident sequences are judged individually.

It is important to note that a quantitative evaluation of a facility is not required in an ISA (indeed it can be completely qualitative in which the criteria for likelihood presented above do not apply). In reality, an ISA may have a mix of quantitative, qualitative, and quasi quantitative analysis for its IEs, IROFS, and accident sequences. This is a great benefit of translating PRA technology to an ISA in that excess

[1] NUREG-1520 defines event here as "occurrences of consequences". Therefore, each undesirable accident sequence is to be separately judged against the quantitative guidelines.

and needless subjectivity can be removed taking the basis towards the quantitative direction. A discussion on data analysis is provided later to highlight this benefit.

As mentioned earlier, an ISA is less comprehensive when compared to a PRA which allows it to be completed with fewer resources. While a PRA will maintain significant bases for its many interlocking and overlapping analyses, an ISA contains more abbreviated ones for a smaller set of tasks. For instance, a PRA will generally perform detailed fault tree modeling of systems that mitigate initiating events. This detailed modeling will ensure the numerous dependencies (such as component common cause failure) are recognized in the system failure probability for a given accident sequence. An ISA generally does not perform any detailed modeling of its IROFS, opting instead for estimates based on historical data or on qualitative definitions like the risk-indexing method presented in NUREG-1520 Appendix A.

To summarize, an ISA identifies credible IEs, determines their unmitigated consequences, and designates IROFS to reduce a given accident sequence frequency below a certain threshold. With this basic understanding of an ISA established, the remainder of this paper focuses on areas where PRA expertise can benefit an ISA.

3. A TRAINING FRAMEWORK FOR NON-RISK PERSONNEL

A fuel facility is a collection of complex systems and operations much like a nuclear plant, albeit less interrelated. To perform an ISA, the team requires expertise in the design and operation of the facility. These facility experts are vital in identifying potential hazards, determining their consequences, and choosing the mitigative or preventive IROFS. Because their experience is not in risk, however, foundational errors in estimating the per accident sequence likelihood might be made resulting in significant rework during the ISA.

Risk experts involved in an ISA may decide to first establish a framework to prevent errors. Presented in formal or informal training, key risk concepts can be established before hazards are even identified at the beginning of the ISA. One of these key concepts, the avoidance of double counting, is presented below. Also presented in this section is the definition of the word 'credible'. The quality and efficiency of the ISA depends on the precise definition of this word and the establishment of key risk concepts.

Double counting of IROFS as both preventive and mitigative features for an IE is a common error that can underestimate the likelihood of a given scenario. A generic example of a poorly defined IE causing double counting is:

Car Crash on Icy Road (IE) → Anti-lock brakes (IROFS) → Airbag (IROFS) → End State

The IE here is really a description of the entire accident sequence—there is an icy road, the car needs to brake, the anti-lock brakes need to work and if they fail to stop the car safely, the airbag must work. Misunderstanding the IE as the accident sequence, its frequency may be estimated based on how often a car crashed on this icy road over a certain period of time. The IE, therefore, includes the anti-lock brakes IROFS implicitly applied as a preventive feature. Double counting then emerges when the mitigative anti-lock brakes IROFS is explicitly applied to the sequence.

A clear remedy to this situation is presented below. By refining the IE definition to be confined to only an icy road condition existing, the double counting is removed:

Road Icy (IE) → Anti-lock brakes (IROFS) → Airbag (IROFS) → End State

This simple risk concept understood by the team at the beginning of the ISA will prevent this most common error (double counting) which results in the most rework later on.

Likely the second most common source of rework is the lack of clarity in the word 'credible'. NUREG-1520 specifies that all credible events need to be analyzed. A frequent mistake takes something very credible (an icy road) and considers it not credible by confusing the context of credible to be against the whole accident sequence instead of the IE. This could cut a credible event from further analysis. Thus, setting a ground-rule that the judgment of credible applies only to the IE is vital.

With the understanding that credible is confined to the IE, the interpretation of what that word means is usually inconsistent. NUREG-1520 provides mostly qualitative acceptance criteria and emphasizes that to be not credible, the frequency must be negligible in light of the overall risk. Without a precise definition of credible, the unmitigated frequencies for some events may be viewed as not credible based on vague justification such as, "this has never happened in the industry" without ever quantitatively estimating the event. This is the first instance where a specific PRA requirement from the level 1 standard can assist an ISA.

Requirement IE-C6 provides the screening criteria for nuclear power plant IEs. For example, an event could be screened if, "the frequency of the event is less than 1E-7 per reactor year (/ry), and the event does not involve either an ISLOCA, containment bypass, or reactor pressure vessel rupture". Although this precise frequency is not transferrable to an ISA, the meaning behind this requirement is. The criteria for screening must be low enough to make the addition to total risk by the IE negligible (1E-07 per year is negligible in view of a CDF of 1E-05 per year for example). The criteria must also make exceptions for unique events that could significantly bypass the engineered safety features of the facility.

The above discussion illustrates the need for basic training for facility experts by risk experts and continuing oversight from a risk perspective. Carefully defining the word credible at the start will avoid missing truly credible IEs. Training on foundational risk concepts such as the avoidance of double counting will reduce considerable rework in the later stages of an ISA.

4. DEPENDENCY

Even with the fundamental logic of an ISA's accident sequences being sound, more advanced topics in risk must be applied and understood by the team to ensure a quality ISA. One of these general topics, dependency, is usually a high contributor to a nuclear plant's core damage frequency (CDF) and large early release frequency (LERF). Recognizing this, the Level 1 standard devotes a significant amount of its requirements to the subject of dependency and its many manifestations. Although the importance of independence between ISA IROFS is emphasized in ISA references, how to identify and handle dependent relationships is generally not and is an area PRA can provide great contributions to.

4.1 IROFS dependency on the IE

Requirement AS-B1 of the standard states:

> For each modeled initiating event, IDENTIFY mitigating systems impacted by the occurrence of the initiator and the extent of the impact. INCLUDE the impact of initiating events on mitigating systems in the accident progression either in the accident sequence models or in the system models.

Adapting this requirement to an ISA will cause the team to carefully inspect IE/IROFS relationships. An IE postulated might be the release of hazardous gas in a certain room. A mitigating IROFS may involve a remote operator isolating the source of the gas assuming a person in the leak location notifies (also an IROFS). The probability of this notification must not be viewed independent of the leak, but should recognize how the gas leaking nearby can impact the local worker's performance of a seemingly simple task.

4.2 Dependency between IROFS

Another key area to focus on is the dependency that sometimes exists between IROFS. An ISA team will need to look at both the dependence an IROFS may have on a preceding IROFS success or failure and the more subtle dependence due to insufficient diversity between IROFS or common cause failure (CCF).

Dependence on preceding IROFS success or failure can be adapted from requirement AS-B2. The standard gives the example of the dependence of low pressure injection on RPV depressurization in a reactor. Applied to the gas leak example, failure of the local worker to notify the remote operator nullifies any assessment of leak isolation probability by the remote operator.

This dependency is an obvious logical requirement, however if the team does not employ an event tree (ET) or other visual representation of accident sequences, these obvious logic missteps may go unnoticed. It is often a temptation to sparingly use event trees because more general purpose software (e.g. a spreadsheet program) may be used for drawing event trees. Because of the labor intensive process for creating visual representations of logic in these general purpose programs, the team may avoid constructing ETs until a finished product is neared. At this time the illogical sequences may be noticed leading to more rework. Although the initial expense is high in comparison to general purpose software, applications capable of quickly drawing and modifying a logical structure, such as an event tree, should be promoted.

4.3 Common Cause Failure

In addition to the interaction between IROFS based on success or failure, facility experts should understand that multiple IROFS lacking significant diversity cannot be viewed independently. SY-B contains many of the CCF requirements in the standard. Because an ISA does not typically use detailed system modeling for its IROFS, the CCF investigation for an ISA can be much less resource intensive. Using screening values for a method such as Multiple Greek Letter (NUREG/CR-4780 [7]) can simplify the process, especially for fuel facility unique equipment that has not had its common cause data developed.

4.4 Human failure event dependency

The final dependency area to focus on is the significant impact the failure of a human action can have on subsequent human actions. To rapidly reduce a sequence likelihood, there may be a temptation to use a chain of human actions alone. Consider a mass measurement that is key to preventing criticality concerns down the line. The team may elect for numerous verifiers of this measurement as individual IROFS to lower the sequence frequency below the threshold. The impact of the first failed measurement is not normally addressed on each subsequent verifier and the human event probabilities are viewed as completely independent. HR-G7 is a requirement that can help reinforce to the team the need for human dependency analysis and NUREG/CR-1278 [5] can be utilized to properly adjust each human event. Often, after the diminishing returns from a chain of operator actions are realized, a mix of more appropriate operator and engineered IROFS is usually selected.

5. DATA

Moving on from dependency, PRA resources in data is an area that can help make a more quantitatively based ISA. As discussed previously, an ISA is typically a quasi-quantitative analysis. Such a simplified analysis may match qualitative criteria to a quantitative range. Guidance often used is found in NUREG-1520 Appendix A which presents the risk indexing method. For example, Table A-10 in this appendix presents failure probabilities and their qualitative criteria.

Table 3: NUREG-1520 Table A-10: Failure Probability Index Numbers

Probability Index No.	Probability of Failure on Demand	Based on Type of IROFS	Comments
-6*	10^{-6}		If initiating event, no IROFS needed.
-4 or -5*	$10^{-4} - 10^{-5}$	Exceptionally robust passive engineered IROFS (PEC), or an inherently safe process, or two redundant IROFS more robust than simple admin. IROFS (AEC, PEC, or enhanced admin.)	Can rarely be justified by evidence. Most types of singe IROFS have been observed to fail.
-3 or -4*	$10^{-3} - 10^{-4}$	A single passive engineered IROFS (PEC) or an active engineered IROFS (AEC) with high availability	
-2 or -3*	$10^{-2} - 10^{-3}$	A single active engineered IROFS, or an enhanced admin. IROFS, or an admin. IROFS for routine planned operations	
-1 or -2	$10^{-1} - 10^{-2}$	An admin. IROFS that must be performed in response to a rare unplanned demand	

For a certain IROFS involving an active engineered control, the failure on demand range is provided at 1E-02 to 1E-03. For conservatism, an ISA analyst may choose 1E-02 for the control, however little objective basis supports the choice. The team may produce overly conservative or perhaps even optimistic IROFS probabilities when compared with actual data from PRA references (this also applies to IE frequencies which NUREG-1520 qualitatively presents in a similar fashion in table A-9).

A possible reason a typical ISA relies on a qualitative basis may be due to the lack of up to date data resources for fuel facilities. NUREG/CR-6928 [6], for instance, provides nuclear power plant generic data for IEs and components. At times, a data source like this can be confidently applied to certain IEs or component failures in an ISA. Of course, much of this data would not be directly applied due to inherent differences between a fuel facility and a nuclear power plant. Other references exist outside the nuclear industry that can be applied to an ISA as well. The establishment of data sources at the beginning of an ISA will avoid defaulting to data based in qualitative criteria.

6. THE USE OF FAULT TREES

The topics already covered are the major areas where PRA best practices can be vital to a high quality and efficient ISA. The final item presented by this paper is the use of fault trees. This item may not be worth the resource investment during an ISA especially if general purpose software is used. It is an option, however, that an ISA team should consider.

As mentioned previously, event trees are eventually used in ISAs to present the accident sequences, especially for those IEs which have high unmitigated consequences. In contrast to a PRA, values for the IROFS presented are rarely the result of detailed fault tree modeling and are usually based in qualitative judgment as just discussed in the previous section.

A simple fault tree for certain IROFS may be desirable, especially when the IROFS being credited is not merely a component, but rather a subsystem whose intra-system dependencies need to be accounted for. Fault tree modeling of these more complex IROFS can also allow for more accurate system failure probabilities when only component level data is available. This again emphasizes the need for risk specific software. Even simple fault tree construction would likely prove impractical without dedicated software.

7. CONCLUSION

The nuclear power plant PRA industry has built an impressive knowledge base (in its standards, guidance material, generic data references, etc.) that can be carefully utilized to produce more efficient and robust risk analysis at a nuclear fuel facility in support of NRC ISA requirements. This wealth of knowledge certainly cannot be applied blindly or without careful examination. But, in the case of fuel facility ISA, the appropriate application of PRA experience will catch logic errors, capture missed dependent relationships, provide more up to date data, and avoid the use of more uncertain qualitatively based data.

References

[1] U.S. Code of Federal Regulations, Title 10, Part 70, Subpart H, "*Domestic Licensing of Special Nuclear Material*," U.S. Government Printing Office, Washington, DC.

[2] ASME / ANS, "*Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*," 2009.

[3] U.S. Nuclear Regulatory Commission, "*Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility*," NUREG-1520, 2002.

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

[5] U.S. Nuclear Regulatory Commission, "*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*," NUREG/CR-1278, 1983.

[6] U.S. Nuclear Regulatory Commission, "*Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*," NUREG/CR-6928, 2007.

[7] U.S. Nuclear Regulatory Commission, "*Procedures for Treating Common Cause Failures in Safety and Reliability Studies*," NUREG/CR-4780, 1989.