Discussion Details Supporting Industry's Position on Design Features – June 2010

Industry is in Compliance

Industry has been asked the basis for their being deemed to be in compliance with 10 CFR 70, Subpart H. Industry believes that they are in full compliance with the requirements of 10 CFR 70 on the following outlined basis.

- The rule required each licensee to define, document and submit their Integrated Safety Analysis (ISA) methodology to the NRC for approval prior to performing the required ISA. The licensees each prepared their methodology documents conforming to the rule and the guidance that the NRC had provided at that point. The methodology documents were reviewed and approved by the NRC.
- Neither the regulations nor these approved methodology documents precluded the introduction of the concepts or use of design features or bounding assumptions as they were written. In fact, there are examples where certain items were designated as design features and not IROFS based on discussions between NRC and the licensee.
- Licensees then performed their ISA work at the facilities using internal procedures which incorporated the approved methodology, guidance from various well established industry hazards analysis techniques and other guidance considerations necessary to complete the work at each facility. From the results of this work, ISA Summaries were prepared in accordance with NRC instructions and submitted to the NRC for review and approval (FR 65-56228, SECY-06-0217, and SA-17).
- The NRC performed onsite oversight of the work, and reviewed and approved all of the ISA summary documents submitted, finding them acceptable (SECY-06-0217, SA-17). While most licensees included some discussion of bounding assumptions or design features in their summaries, we are not aware that the subject was raised by NRC during final rule implementation.
- The licensees therefore believe that it was and remains clear that their work was found to be compliant by the NRC. Therefore notwithstanding any rule change or specific safety issue, we believe the licensee's work continues to be in full compliance in all instances where it was completed in accordance with the approved methodology, internal procedures and as approved in the ISA summaries.

Adhere to Risk-Informed and Performance-Based Rule

In September 1996, NEI at the request of industry filled a petition for rule making (PRM-70-7) which recommended ways to improve the performance at fuel cycle facilities through a Part 70 rule change. The proposal included evolving from a historically deterministic assessment to, among other things, the concept of a risk-informed and performance-based rule. The reasoning being that

licensee and NRC attention should validate and focus on those items most important to safety so that the relevant accident sequences are assured to be unlikely or highly unlikely depending upon the consequence. The licensee's safety program was therefore to be focused on risk and performance. The NEI petition was accepted in part with the exceptions noted in the Federal Register Notice (FRN 64-41330). The risk-informed and performance-based concept was clearly adopted; therefore supporting the concept that the most important safety risks should receive relatively higher NRC and licensee attention, e.g., IROFS.

The licensees' approach to implementing the rule, including the use of design features and bounding assumptions, clearly supports the concepts envisioned in the changes to Part 70. The recent NRC draft guidance and position are inconsistent with this philosophy, in that, it is causing licensees to identify additional design features or bounding assumptions as IROFS which has the effect of diluting the overall importance of those true barriers to prevent or mitigate an event. We suggest that a more holistic view should be employed to identify workable definitions and application of design features/bounding assumptions. This was the approach industry used in defining their NRC-approved ISA methodology which resulted in the NRC-approved ISA Summaries. This background was summarized in the first NEI paper on bounding assumptions transmitted to the NRC January 22, 2010. The industry welcomes a substantive response to the January industry position paper since it would further inform industry's deliberations on this matter.

Meeting Existing Regulatory Requirements

Regulations require the limiting of risk of all credible high and intermediate consequence events or nuclear criticality with the use of IROFS and assurance that the IROFS are available and perform their function when required (10 CFR 70.61 (b), (c) and (d), and 70.62). Credibility of the event is therefore a crucial attribute that requires the use of IROFS and is a basic part of the NRC approved methodologies used by the industry. Events that are not credible due to the existence of design features remain outside the sphere of this requirement. This is consistent with NRC's position on Reactor Safety regarding defense-in-depth (SECY-06-0217, Enclosure 3, Part 1, Section 3 where Regulatory Guide 1.174 is cited as stating that relative to defense-in-depth the philosophy will be preserved by ensuring that: . . . "the intent of the fundamental design features is maintained".

It is clear that there has to be a means to distinguish facility design features and the process, and IROFS; for otherwise at the end of the alternative logic everything could become an IROFS. SECY-06-0217 and FR 65 -56211 both include wording that indicates that the ISA is conducted and IROFS identified for significant potential accidents at the facility. In addition, the documents indicate that the rule change was intended to improve the margin of safety while reducing the regulatory burden. This all speaks to gradation of elements of the safety program and supports the fact that not all controls or features associated with a facility or process are IROFS. In the conduct of the ISA work, the teams must be able to identify a specific starting point and conditions on which to base and perform the analysis, and accept certain features/characteristics as they debate the issue of safety. Otherwise, the teams would become entangled in an endless loop that could, in part, ignore the

safety contribution of baseline design criteria to reduce the likelihood of an accident or consequence and thus detract from the desired result. This approach has been utilized as acceptable team safety practice across many industries in Standard Hazards Analysis methods. NUREG 1520, in concept, supports this since it states that the list of IROFS is intended to identify the basis of safety such that items will not be degraded without an adequate safety review. Design features once installed are judged to meet the ISA requirements as documented and are not subject to being degraded without a justifying safety review (10 CFR 70.72).

NUREG 1520 includes a caution against *Circular Reasoning* to avoid declaring an item as an IROFS. Also NUREG 1510, in addressing circular reasoning, implies that there is something very closely allied to IROFS that does not fall into that same category and this supports the concept of ***design features*** – a facility or process feature that cannot credibly fail to function or be rendered ineffective as a result of a change to the system. As stated in NUREG 1520, if an event is not credible, IROFS are not required. Likewise a design feature cannot credibly be rendered ineffective as a result of a change to the system. It is important to place the word *change* in the proper context. Change as used in this context means an inherent or spontaneous change, e.g. one that occurs as a result of normal use, wear, environmental conditions, process conditions or reasonably anticipated operator error as opposed to a change brought about deliberately through malicious acts, intentional acts without malicious intent or unauthorized engineering change. Simply put, a feature should not be identified as an IROFS by the ISA team if it can not credibly be degraded except by engineering change. It is through this logic that the ISA methodologies approved by the NRC and in use by current licensees meet the holistic requirements of 10 CFR 70.61 and changes in those methodologies are not required.

It is important to note that 10 CFR 70.64 requires new facilities to include design criteria which imply a reference to design features in the context of these discussions. Current facilities were excluded because it was unclear how these design criteria might be substantiated. In the process of conducting the detailed ISA work, the design basis became much clearer and quite possibly 70.64 should have been written in such a way to accommodate the design features of existing plants. Since design features are recognized for new plants, there should be a consistent recognition of design features for currently operating plants and the results of the ISA work support this.

<u>Adherence to Change Process under 10 CFR 70.72</u>

In recent discussions between industry and NRC, the NRC has stated that the licensee could make certain facility changes without NRC approval, NRC would not be aware of such changes and, in general, without an extensive set of IROFS, safety at the facility might degrade over time. We disagree with this statement. 10 CFR 70.72 is quite clear on the licensee's obligation to evaluate every change at their facility that could affect safety. There are extensive discussions to this effect in FR 64-41348 and FR 65-56217. Industry believes that 70.72 is not limited to IROFS because IROFS are only mentioned in 70.72 (c) (2) & (3) where as the section is far more inclusive regarding the facility safety program.

The control of change under 70.72 is quite disciplined and adequate to maintain control of the safety program. In addition, 70.72 requires licensees to submit a list of all changes made where the licensee did not submit them to the NRC for prior approval. Also, in addition to configuration control and management of change, it is important to note that through the license, the licensee has commitments to programmatic elements for all the safety disciplines, including the requirement for meeting double contingency for criticality safety. Viewed as it was intended, 70.72 provides significant assurance to licensees and NRC that the safety program will be maintained and the program elements coupled with required management measures clearly provide defense in depth. In addition, NRC inspectors have full access to such information while on site at the facility.

Possible Additional Reporting Requirements

The NRC has raised the concern that there may be failures of some items categorized as design features/bounding assumptions that would be of interest and therefore a designation of these as IROFS is necessary to facilitate reports to NRC. Industry believes that NRC should consider a rule change to capture the reporting or notification of certain events or information that NRC believes it needs to fulfill its safety mission, in the absence of new guidance. The Bulletin 91-01 reporting requirements were superseded in part to risk inform reporting requirements and to incorporate the concept of IROFS, acknowledging that not all NCS controls need to be designated as IROFS. With these changes, it is possible certain items of interest to the NRC were not included. It should be noted that adding IROFS for this purpose is completely contrary to the concept of risk informed and performance based IROFS and carries with it the undesirable potential for diluting the importance of IROFS.

Current Draft Discussion Guidance

Industry is concerned with the April draft guidance information. Specifically, it is focused exclusively on a narrow interpretation of 10 CFR 70.61, does not consider the entire regulatory framework and intent of the rule, and is contrary to one of the basic tenants of the changes to Part 70 as discussed previously. In addition, it does not reflect consideration of the industry's January 2010 position paper. As such, detailed specific comments do not appear to be warranted on that document at this time. Industry generally believes that a ***design feature*** is distinguished from a passive engineered IROFS if the only identified failure mechanism for a specific passive engineered feature is loss of configuration control. In those cases the item, feature or attribute is a ***design feature*** and it is not necessary to declare it as an IROFS. In this definition, failure characteristics are used to distinguish between ***design features*** and IROFS. Inherent failure modes relate to passive engineered IROFS but never to ***design features***. While other terms may need to be defined and additional guidance and examples obviously need to be developed, the guidance should underscore these guiding principles.

In Summary

Given the lack of clarity regarding whether NRC intends to pursue rulemaking on this matter or modify its enforcement approach, industry recommends that findings arising during inspections and licensing actions questioning licensee practices that are consistent with NRC-approved methodologies and licensee implementing procedures should be used to inform the development of clarifying guidance or future rulemakings on these matters. But until such guidance or rulemakings are complete – including provision for public notice and comment – these findings should not be used as a basis for enforcement action or licensing decisions.

The NRC position stated in SA-17 is that the appropriate ISG or NUREG 1520 would be updated to address such issues as they arose. The licensees firmly believe they have been implementing an NRC-approved course of action for roughly ten years. It has not been until recent licensing actions and certain inspections occurred that these questions have arisen indicating the need for additional guidance and alignment with the inspection and enforcement programs to be consistent with NRC practice on this matter. Unnecessarily modifying guidance will force licensees to perform significant work with little or no safety benefit and oversight and approval efforts will consume significant NRC resources. Since facilities are currently compliant, we believe that the proper course of action is to issue guidance consistent with industry practice that has been found to be acceptable as generally described above so as not expend significant industry and NRC resources with little or no safety benefit in most cases. The NRC may identify the need to modify the Part 70 reporting criteria to include items deemed necessary from a safety perspective that do not currently bear the IROFS designation or the language of 70.61 to more clearly align the rule with current NRC approvals and practice.