

May 7, 2012

Ms. Janet R. Schlueter, Director  
Fuel and Material Safety  
Nuclear Generation Division  
Nuclear Energy Institute  
1776 I Street, NW, Suite 400  
Washington, DC 20006-3708

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION RESPONSE ON USE OF DESIGN FEATURES TO MEET REQUIREMENTS IN TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* (10 CFR) PART 70, "DOMESTIC LICENSING OF SPECIAL NUCLEAR MATERIAL"

Dear Ms. Schlueter:

This letter and its enclosure provide the U.S. Nuclear Regulatory Commission (NRC) staff response to your letter dated June 7, 2011 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML111930051), and industry positions presented at a public meeting on August 17, 2011 (ADAMS Accession No. ML11236A149). This response deals with the reliance on design features in conducting integrated safety analyses (ISAs) required under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 70, "Domestic Licensing of Special Nuclear Material." The NRC staff appreciates the Nuclear Energy Institute's (NEI's) time and effort spent in presenting its perspective and providing the NRC staff with supporting materials. The NRC staff has carefully considered the information presented by NEI on the proposed use of design features with respect to ensuring compliance with 10 CFR Part 70, maintaining an adequate level of safety at fuel cycle facilities, and considering currently accepted practices regarding ISA methodologies.

Based on its consideration of the information that NEI and the industry provided, the NRC staff concludes that the methodology the industry proposes does not meet the requirements of 10 CFR Part 70. Specifically, 10 CFR 70.4, "Definitions," defines items relied on for safety (IROFS) as "structures, systems, equipment, components...that are relied on to prevent potential accidents at a facility that could exceed the performance requirements in [10 CFR] 70.61 ["Performance Requirements"] or to mitigate their potential consequences." 10 CFR 70.61(e) requires that each engineered control or control system necessary to demonstrate compliance with the performance requirements in 10 CFR 70.61(b), (c), or (d) (i.e., to reduce the likelihood or consequences of externally or internally initiated events and limit the risk of nuclear criticality accidents) must be designated as an item relied on for safety.

The NRC staff recognizes that 10 CFR Part 70 covers different licensed activities; therefore, the designation of structures, systems, and equipment may differ among facility types. However, the determining factor is if an item is relied on to prevent or mitigate events and their consequences. The staff sees no distinction between a passive engineered control and a design feature in terms of their functions to prevent or mitigate events and accidents. Therefore, if a design feature is used to meet the requirements of 10 CFR 70.61, the design feature must be included among the designated IROFS. Additionally, Chapter 3, "Integrated

Safety Analysis (ISA) and ISA Summary,” of NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” issued May 2010, states that it is not acceptable to conclude that a process does not need to be included in the IROFS because an event is “‘not credible’ due to characteristics provided by some other controls or features of the plant that are not IROFS.” A further discussion on the use of passive engineered controls or features is provided in the enclosure to this letter.

The NRC staff also considered NEI’s proposed definitions of “bounding assumptions” and “initial conditions.” As noted in the enclosure, the use of these broadly defined terms could improperly render certain events or accident sequences not credible, and thus preclude safety analyses consistent with 10 CFR Part 70 requirements. The NRC staff is also concerned that licensees provide a sufficient level of detail on these subjects in the ISA summary to ensure that the staff can make necessary regulatory findings. The NRC staff recognizes that most of the process information (e.g., initial conditions and bounding assumptions) will be maintained in a facility’s ISA; however, sufficient information should be submitted with the license application to enable the staff to determine if the facility, equipment, and procedures are adequate to protect health and minimize danger to life and property in accordance with 10 CFR 70.23(a)(3) and (4).

The NRC staff recognizes that additional guidance on the use of passive design features, bounding assumptions, and initial conditions is needed. Therefore, the staff is planning to revise guidance in NUREG-1520 to clarify acceptable methods for achieving regulatory compliance. The revised guidance will address the use of passive engineered controls to meet the 10 CFR 70.61 requirements and provide clarification on the completeness of the ISA summaries to ensure that license applicants appropriately consider credible events when developing an ISA. The staff also will consider if any conforming changes to NUREG-1513, “Integrated Safety Analysis Guidance Document,” issued May 2001, are needed. The planned changes in guidance reflect current requirements and do not represent a new staff position. The staff plans to publish a *Federal Register* notice that describes the proposed changes to these guidance documents and provides an opportunity for public comment before any draft guidance is made final.

In the interim, the staff will consider if additional, more formal, communication with our licensees is appropriate to: 1) ensure a common understanding of the application of this position by the fuel cycle industry, and 2) better understand the scope and impact of the consistent application of the NRC’s position on “design features.”

If you have any questions, please contact Cinthya Román of my staff at 301-492-3224 or via e-mail at [Cinthya.Roman@nrc.gov](mailto:Cinthya.Roman@nrc.gov).

Sincerely,

**/RA/**

John D. Kinneman, Director  
Division of Fuel Cycle Safety  
and Safeguards  
Office of Nuclear Material Safety  
and Safeguards

Enclosure:  
As stated

If you have any questions, please contact Cinthya Román of my staff at 301-492-3224 or via e-mail at [Cinthya.Roman@nrc.gov](mailto:Cinthya.Roman@nrc.gov).

Sincerely,

**/RA/**

John D. Kinneman, Director  
Division of Fuel Cycle Safety  
and Safeguards  
Office of Nuclear Material Safety  
and Safeguards

Enclosure:  
As stated

**DISTRIBUTION:**

PMNS            FCSS r/f                            RidsNMSSOd                            JHull, OGC

**ML113420462**

OFFICE:	FCSS/MODB	OGC	QTE	FCSS/MODB	FCSS	FCSS
NAME:	CRomán	MYoung	KAzariah-Kribbs	JBowen	MBailey	JKinneman
DATE:	2/15/12	3/15/12	3/16/2012	3/20/12	3/22/12	5/07/12

**OFFICIAL RECORD COPY**

## Industry Mailing List

### E-mail

[anm@nei.org](mailto:anm@nei.org) (Andrew Mauer)  
[jrs@nei.org](mailto:jrs@nei.org) (Janet Schlueter)  
[Vcm3@earthlink.net](mailto:Vcm3@earthlink.net) (Charlie Vaughan)  
[dlspangler@babcock.com](mailto:dlspangler@babcock.com) (Dave Spangler)  
[blcole@babcock.com](mailto:blcole@babcock.com) (Barry Cole)  
[Robert.sharkey@areva.com](mailto:Robert.sharkey@areva.com) (Robert Sharkey)  
[Robert.link@areva.com](mailto:Robert.link@areva.com) (Robert Link)  
[Calvin.manning@areva.com](mailto:Calvin.manning@areva.com) (Calvin Manning)  
[Scott.murray@ge.com](mailto:Scott.murray@ge.com) (Scott Murray)  
[Albert.kennedy@ge.com](mailto:Albert.kennedy@ge.com) (Albert Kennedy)  
[Julius.Bryant@ge.com](mailto:Julius.Bryant@ge.com) (Julius Bryant)  
[Larry.parscale@honeywell.com](mailto:Larry.parscale@honeywell.com) (Larry Parscale)  
[Michael.greeno@honeywell.com](mailto:Michael.greeno@honeywell.com) (Michael Greeno)  
[Dallas.gardner@honeywell.com](mailto:Dallas.gardner@honeywell.com) (Dallas Gardner)  
[gsanford@nefnm.com](mailto:gsanford@nefnm.com) (Gary Sanford)  
[wpadgett@nefnm.com](mailto:wpadgett@nefnm.com) (Wyatt Padgett)  
[jwnagy@nuclearfuelservices.com](mailto:jwnagy@nuclearfuelservices.com) (John Nagy)  
[wrshackelford@nuclearfuelservices.com](mailto:wrshackelford@nuclearfuelservices.com) (Randy Shackelford)  
[jkwheeler@nuclearfuelservices.com](mailto:jkwheeler@nuclearfuelservices.com) (Jennifer Wheeler)  
[shanksvj@pgdp.usec.com](mailto:shanksvj@pgdp.usec.com) (Vernon Shanks)  
[borenml@pgdp.usec.com](mailto:borenml@pgdp.usec.com) (Michael Boren)  
[fogeld@ports.usec.com](mailto:fogeld@ports.usec.com) (Doug Fogel)  
[stoneaa@ports.usec.com](mailto:stoneaa@ports.usec.com) (Al Stone)  
[minerp@usec.com](mailto:minerp@usec.com) (Pete Miner)  
[sensuet@usec.com](mailto:sensuet@usec.com) (Terry Sensue)  
[alstadcd@westinghouse.com](mailto:alstadcd@westinghouse.com) (Cary Alstadt)  
[couturgf@westinghouse.com](mailto:couturgf@westinghouse.com) (Gerald Couture)  
[dwgwyn@moxproject.com](mailto:dwgwyn@moxproject.com) (Dealís Gwyn)  
[dayates@moxproject.com](mailto:dayates@moxproject.com) (Doug Yates)  
[jjmiller@intisoid.com](mailto:jjmiller@intisoid.com) (John Miller)  
[Jim.kay@areva.com](mailto:Jim.kay@areva.com) (Jim Kay)  
[Scott.horton@areva.com](mailto:Scott.horton@areva.com) (Scott Horton)  
[Julie.olivier@ge.com](mailto:Julie.olivier@ge.com) (Julie Olivier)  
[Patricia.campbell@ge.com](mailto:Patricia.campbell@ge.com) (Patricia Campbell)

## **NRC Staff Position on the Use of Design Features to Meet Requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 70, “Domestic Licensing of Special Nuclear Material”**

### Summary of Regulatory Requirements

Title 10 of the *Code of Federal Regulations* (10 CFR) 70.61, “Performance Requirements,” identifies the requirements for preventing accidents or mitigating their consequences. Specifically, 10 CFR 70.61(b) requires that “[t]he risk of each credible high-consequence event must be limited. Engineered controls, administrative controls, or both, shall be applied to the extent needed to reduce the likelihood of occurrence of the event so that, upon implementation of such controls, the event is highly unlikely or its consequences are less severe than those in paragraphs (b)(1)–(4) of this section.” 10 CFR 70.61(c) similarly requires that “[t]he risk of each credible intermediate-consequence event must be limited. Engineered controls, administrative controls, or both, shall be applied to the extent needed so that, upon implementation of such controls, the event is unlikely or its consequences are less than those in paragraphs (c)(1)–(4) of this section.” 10 CFR 70.6(d) states that “[i]n addition to complying with paragraphs (b) and (c) of this section, the risk of nuclear criticality accidents must be limited by assuring that under normal and credible abnormal conditions, all nuclear processes are subcritical.”

10 CFR 70.61(e) provides that “[e]ach engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of this section shall be designated as an item relied on for safety. The safety program, established and maintained pursuant to § 70.62 of this subpart, shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of this section.”

Management measures are an important part of 10 CFR 70.62, “Safety Program and Integrated Safety Analysis.” As stated in 10 CFR 70.62(d), management measures “ensure compliance” with the 10 CFR 70.61 performance requirements. The 10 CFR 70.62(d) management measures provision provides some flexibility in further stating that such measures “may be graded commensurate with the risk reduction attributable to” the 10 CFR 70.61 engineered or administrative controls. In accordance with 10 CFR 70.62(d), management measures must ensure that any 10 CFR 70.61 control identified as an item relied on for safety is “designed, implemented, and maintained, as necessary, to ensure” the item’s availability and reliability.

### Engineered Controls and Design Features

The terms “engineered control,” “administrative control,” and “control system” are not defined in 10 CFR Part 70, “Domestic Licensing of Special Nuclear Material.” However, “active engineered control,” “administrative control,” and “passive engineered control” are among the relevant terms defined in NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” issued May 2010.

The NRC staff recognizes that the word “control” is used in multiple contexts throughout 10 CFR Part 70. Since the meaning of this word depends on its context (e.g., the licensee’s controlled area, beyond the control of the licensee, engineered control, administrative control, control systems, criticality control), it is difficult to provide a single, overarching definition. For

example, when used with respect to process safety, control may mean equipment, instruments, components, human actions, or mechanisms designed to prevent the causes or mitigate the consequences of process deviations. Or, when used with respect to criticality safety, control may mean equipment, instruments, components, system design, human actions, or mechanisms designed to ensure that under normal and credible abnormal conditions, all nuclear processes are subcritical. Therefore, the NRC staff plans to revise NUREG-1520 to clarify how the term “control” is used in different contexts.

In its letter dated June 7, 2011 (ADAMS Accession No. ML111930051), NEI defined design features as:

Passive engineered features of the facility/process configuration that have insignificant probability of failure, the safety aspect is not easily altered, is not subject to routine replacement, is not subject to degradation, and do not require periodic testing or verification to ensure they remain available and reliable to perform their intended function. ...

The NRC staff concludes that design features—as the industry defined them at an August 17, 2011, public meeting (ADAMS Accession No. ML11236A149), and in the letter dated June 7, 2011—perform the same safety function as passive engineered controls. NUREG-1520 indicates that a passive engineered control is a device that uses only fixed physical design features to maintain safe process conditions without any required human action. For example, passive engineered controls or design features refer to items such as vessels, containers, barriers, and structures that perform a safety function. The safety function of passive engineered controls depends solely on their fixed physical design properties. If the item is properly designed and maintained, and it has no defects, the safety function should be available even if there is a process deviation. IROFS, as stated in 10 CFR 70.4, “Definitions,” are “structures, systems, equipments, components...that are relied on to prevent potential accident sequences at a facility that could exceed the performance requirements in [10 CFR] 70.61 or to mitigate their potential consequences.” Therefore, any structure, system, equipment, or component that uses fixed physical design properties (e.g., passive engineered control or design feature) that is relied upon to prevent or mitigate an accident and that is used to comply with the performance requirements of 10 CFR 70.61, must be designated as an IROFS. In addition, such design features are subject to the 10 CFR 70.62(d) management measures.

The NRC staff recognizes that passive engineered controls normally have a lower likelihood of failure than active engineered controls. Some potential causes of active systems failure, such as lack of human action or power failure, do not exist when passive safety is provided. However, passive systems are subject to other failure mechanisms that need to be addressed to ensure that they are not significant. The applicant or the licensee should assess the reliability and availability of the passive engineered control (or design feature) in the short term, long term, and under adverse conditions. Appropriate testing and demonstration or other applications of management measures may be needed to determine if the design is free of errors that can lead to design or manufacturing defects. These defects can adversely affect the availability and reliability of the safety function to be performed.

Because passive engineered controls generally are more reliable than active engineered controls, the NRC staff concludes, consistent with 10 CFR 70.62(d), that graded management measures can be applied to passive engineered controls to ensure they are available and reliable to perform their safety function. The NRC staff recognizes that passive engineered controls might not need as much maintenance or surveillance as active engineered controls, but

passive engineered controls must be subject to management measures to meet 10 CFR 70.62(d) requirements. The NRC staff plans to revise NUREG-1520, Chapter 11, "Management Measures," to clarify the application of graded management measures to passive engineered features.

### Bounding Assumptions and Initial Conditions

In its letter dated June 7, 2011, NEI provided the following definitions:

#### Bounding Assumptions:

Identified assumptions about a process or material characteristics that bound the credible conditions of the process. These assumptions are based on the process chemistry, applicable scientific principles, facility-specific experimental data, operational history, and/or facility construction requirements. In determining the bounding assumptions for process parameters or material characteristics, no credit may be taken for controls placed on those parameters, with the exception of upstream process controls that have been specified as IROFS...

#### Initial Conditions:

Important aspects of a process and associated equipment, process operating parameters (e.g., temperature, pressure, flow rate), material throughput, and characteristics of the facility in which the process resides (e.g., design features) that establish the normal operating conditions from which the process hazard analysis is performed...

During the August 17, 2011, public meeting and in its letter dated June 7, 2011, NEI indicated that bounding assumptions and initial conditions would be maintained in the integrated safety analysis (ISA) records and included in the configuration management system for the facility, but not in the ISA summary. The staff recognizes that 10 CFR 70.62(c)(vi) requires each licensee or applicant to conduct and maintain an ISA that identifies the assumptions and conditions under which the items that are relied upon to support compliance with the performance requirements of 10 CFR 70.61. Although licensees are not required to submit all of their process safety information for the NRC's review, 10 CFR 70.65, "Additional Content of Applications," requires licensees to provide detailed information in the ISA summary about the site, the facility, and processes. For example, 10 CFR 70.65(b)(4) requires licensees to provide information in the ISA summary that demonstrates the licensee's compliance with 10 CFR 70.61 performance requirements; 10 CFR 70.65(b)(3) requires a description of each process analyzed in the ISA in sufficient detail to understand the theory of operation; and 10 CFR 70.65(b)(6) requires a list briefly describing each item relied upon for safety that is identified pursuant to 10 CFR 70.61(e) in sufficient detail to understand its functions in relation to the performance requirements of 10 CFR 70.61. Therefore, the ISA summary should include assumptions and conditions necessary to understand the theory of operation of a process, or to understand the function of IROFS in relation to the performance requirements of 10 CFR 70.61.

In addition, 10 CFR 70.22(a)(7) states that each application for a license shall include a description of equipment and facilities that the applicant will use to protect health and minimize danger to life or property. As stated in 10 CFR 70.23(a)(3) and (4), an application for a license will be approved if the Commission determines that the applicant's proposed equipment, facilities, and procedures are adequate to protect health and minimize danger to life and

property. NUREG-1520 states, “the description in the ISA summary is considered acceptable if it provides a list of materials or conditions that could result in hazardous situations, including the maximum inventory amounts and locations of the hazardous materials at the facility.” Therefore, the licensee’s ISA summary should include any bounding assumptions or initial conditions necessary to understand how the process, equipment, facility, and procedures are used to protect health and minimize danger to life and property.

Incorrect assumptions can lead to errors in the design, construction, and operation of a facility. Incorrect assumptions can also lead to nonconservatism and inadequate evaluation of risk. In addition, incorrect assumptions could improperly render certain events or accident sequences not credible and thus preclude safety analyses consistent with 10 CFR Part 70 requirements. NUREG-1520 states that a determination that an event is “not credible” could be used as a criterion for exemption from the use of IROFS. As indicated in NUREG-1520, if assumptions are used to classify an event as “not credible,” a convincing argument should exist that given physical laws, process deviations are not possible or are extremely unlikely.

Licenses can use initial conditions to conduct the safety analysis and identify credible accident sequences. The ISA summary must contain a general description of the accident sequences, as required by 10 CFR 70.65(b)(3). NUREG-1520 states that an ISA summary description of an accident sequence “is acceptable if it permits the reviewer to determine how each accident sequence for which the consequences could exceed the performance requirements of [10 CFR] 70.61 is protected against by IROFS or a system of IROFS.” Therefore, the ISA summary should describe any initial conditions necessary to understand how each credible accident sequence is protected against by an IROFS.

The NEI definition indicates that initial conditions include characteristics of the facility in which the process resides (e.g., design features). Those characteristics can be used to classify a particular event as not credible. However, the staff view is that a determination that an event is “not credible” must not depend on any design feature or characteristic of the facility that could be rendered ineffective as a result of a change that the licensee made. As indicated in NUREG-1520, “[e]ach facility feature that is needed to ensure that accident events are sufficiently unlikely is an [i]tem relied on for safety.”

The NRC staff plans to revise NUREG-1520 to provide guidance on acceptable uses and documentation of bounding assumptions and initial conditions to support safety analyses. The guidance, which will be published in draft for public comment, will address what information should be contained in the ISA summary and what information can be maintained in an ISA.

### Conclusion

The NRC staff concludes that given the 10 CFR 70.4 definition of IROFS, the 10 CFR 70.61 performance requirements, and the 10 CFR 70.62 safety program, passive engineered controls (including design features) performing a safety function, and which are relied upon to meet the performance requirements, must be designated as IROFS. Such IROFS also must be subject to management measures, as required by 10 CFR 70.62(d). Graded management measures may be applied to certain design features in accordance with 10 CFR 70.62(d) to provide sufficient assurance that these IROFS will be reliable and available when needed to perform their safety function. It is not acceptable, however, to conclude that a process does not need IROFS because an event is “not credible” due to the characteristic provided by some other controls or features of the plant that are not IROFS.

The NRC staff also concludes that although licensees and applicants are not required to submit all of their process safety information for NRC review, the ISA summary should contain a description of any bounding assumptions and initial conditions necessary to understand how the process, equipment, facility, and procedures are used to protect health and minimize danger to life and property to comply with 10 CFR 70.23(a)(3) and (4).

The NRC staff anticipates revising NUREG-1520 to: 1) clarify the different meanings of the term “control,” 2) clarify guidance on graded management measures, 3) clarify the acceptance criteria in Chapter 3 for the facility-specific definition of “credible” that licensees must provide, and 4) clarify the acceptable level of detail provided in the ISA summary, including any bounding assumptions and initial conditions relied upon. Additional changes to NUREG-1520 may be considered as part of this effort. Changes will be discussed in a *Federal Register* notice, and the public will have the opportunity to provide comments before the changes are finalized.