

April 19, 2010

MEMORANDUM TO: Patricia Silva, Chief
Technical Support Branch
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

FROM: Michael Raddatz, Design Features Team Leader /**RA**/ P. Silva for
Technical Support Branch
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

SUBJECT: GUIDANCE TO STAFF REGARDING USE OF
BOUNDING ASSUMPTIONS AND DESIGN FEATURES
IN INTEGRATED SAFETY ANALYSES REVIEWS

The attached draft document was developed by staff as a foundation for talking points with industry at the April 27, 2010, public meeting. It provides our initial thoughts on the direction to inspectors and license reviewers on the consideration that should be given to licensees' use of bounding assumptions and design features in the implementation of their integrated safety analyses pursuant to Title 10 of the *Code of Federal Regulations*, Subpart H.

This document also fulfills our commitment made in an April 13, 2010, letter to the Nuclear Energy Institute (NEI) (ML100810193) to provide a discussion draft publicly available approximately 10 days prior to the next public meeting with industry officials, which is scheduled for April 27, 2010.

This document will be transmitted to NEI via e-mail and made available to the public as an attachment to the meeting notice (ML101020616) for the April 27, 2010, meeting.

Enclosure: as stated

CONTACT: Michael G. Raddatz, FCSS/NMSS
(301) 492-3108

MEMORANDUM TO: Patricia Silva, Chief
 Technical Support Branch
 Division of Fuel Cycle Safety
 and Safeguards
 Office of Nuclear Material Safety
 and Safeguards

FROM: Michael Raddatz, Design Features Team Leader **/RA/** P. Silva for
 Technical Support Branch
 Division of Fuel Cycle Safety
 and Safeguards
 Office of Nuclear Material Safety
 and Safeguards

SUBJECT: GUIDANCE TO STAFF REGARDING USE OF
 BOUNDING ASSUMPTIONS AND DESIGN FEATURES
 IN INTEGRATED SAFETY ANALYSES REVIEWS

The attached draft document was developed by staff as a foundation for talking points with industry at the April 27, 2010, public meeting. It provides our initial thoughts on the direction to inspectors and license reviewers on the consideration that should be given to licensees' use of bounding assumptions and design features in the implementation of their integrated safety analyses pursuant to Title 10 of the *Code of Federal Regulations*, Subpart H.

This document also fulfills our commitment made in an April 13, 2010, letter to the Nuclear Energy Institute (NEI) (ML100810193) to provide a discussion draft publicly available approximately 10 days prior to the next public meeting with industry officials, which is scheduled for April 27, 2010.

This document will be transmitted to NEI via e-mail and made available to the public as an attachment to the meeting notice (ML101020616) for the April 27, 2010, meeting.

Enclosure: as stated

CONTACT: Michael G. Raddatz, FCSS/NMSS
 (301) 492-3108

DISTRIBUTION:
 TSB r/f

ML101090518

OFC	FCSS/TSB	FCSS/TSB	FCSS/TSB
NAME	MRaddatz	PJenifer	PSilva
DATE	4/19/10	4/19/10	4/19/10

OFFICIAL RECORD COPY

Draft Staff Considerations on the use of Bounding Assumptions And Passive Engineered Features in Integrated Safety Analyses

Problem Statement

Lack of clear guidance to inspectors and license reviewers on licensees use of bounding assumptions and passive engineered features in the implementation of integrated safety analyses (ISA) pursuant to Title 10 of the *Code of Federal Regulation* (10 CFR) Part 70, Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material."

Regulatory Basis

70.61(b) *The 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.*

70.61(c) *The 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.*

70.61(d) *In addition to complying with paragraph (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, including use of an approved margin of subcriticality for safety. Preventive controls and measures must be the primary means of protection against nuclear criticality accidents.*

70.61(e) *Each 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 safety¹. The safety program... shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed² and in the context of the performance requirements of this section.*

70.62(1)(c)(vi) [Each licensee or applicant shall conduct and maintain an integrated safety analysis that is of appropriate detail for the complexity of the process, that identifies:] ... *Each item relied on for safety identified pursuant to 70.61(e) of this subpart, the characteristics of its preventive, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of 70.61.*

¹ "Items relied on for safety" mean structures, systems, equipment, components, and activities of personnel that are relied on to prevent potential accidents at a facility that could exceed the performance requirements in § 70.61 or to mitigate their potential consequences. This does not limit the licensee from identifying additional structures, systems, equipment, components, or activities of personnel (i.e., beyond those in the minimum set necessary for compliance with the performance requirements) as items relied on for safety.

² "Available and reliable to perform their function when needed" is defined as "based on the analyzed credible conditions in the integrated safety analysis, items relied on for safety will perform their intended safety function when needed, and management measures will be implemented that ensure compliance with the performance requirements of 70.61 of this part, considering factors such as necessary maintenance, operating limits, common-cause failures, and the likelihood and consequences of failure or degradation of the items and measures.

70.65 (b) *The integrated safety analysis summary must be submitted with the license or renewal application (and amendment application as necessary), but shall not be incorporated in the license. However, changes to the integrated safety analysis summary shall meet the conditions of § 70.72. The integrated safety analysis summary must contain:*

(1) A general description of the site with emphasis on those factors that could affect safety (i.e., meteorology, seismology);

(2) A general description of the facility with emphasis on those areas that could affect safety, including an identification of the controlled area boundaries;

(3) A description of each process (defined as a single reasonably simple integrated unit operation within an overall production line) analyzed in the integrated safety analysis in sufficient detail to understand the theory of operation; and, for each process, the hazards that were identified in the integrated safety analysis pursuant to § 70.62(c)(1)(i)-(iii) and a general description of the types of accident sequences;

(4) Information that demonstrates the licensee's compliance with the performance requirements of § 70.61, including a description of the management measures; the requirements for criticality monitoring and alarms in § 70.24; and, if applicable, the requirements of § 70.64;

(5) A description of the team, qualifications, and the methods used to perform the integrated safety analysis;

(6) A list briefly describing each item relied on for safety which is identified pursuant to § 70.61(e) in sufficient detail to understand their functions in relation to the performance requirements of § 70.61;

(7) A description of the proposed quantitative standards used to assess the consequences to an individual from acute chemical exposure to licensed material or chemicals produced from licensed materials which are on-site, or expected to be on-site as described in § 70.61(b)(4) and (c)(4);

(8) A descriptive list that identifies all items relied on for safety that are the sole item preventing or mitigating an accident sequence that exceeds the performance requirements of § 70.61; and

(9) A description of the definitions of unlikely, highly unlikely, and credible as used in the evaluations in the integrated safety analysis.

Definitions

Bounding Process Assumptions (BPA): Fundamental assumptions used in the safety analysis concerning properties of materials, operating parameters and conditions, the type of process and technology to be used, and physical laws. These assumptions are generally applicable to multiple processes throughout the facility.

Design Features: Passive attributes of physical structures, systems, equipment, and components used in the safety analysis which are designed into the process for either operational or safety purposes, and are therefore within the licensee's discretion to change (in accordance with regulatory requirements).

Generic Items Relied on for Safety (IROFS): An IROFS or systems of IROFS that applies to the entire facility, a process, or a whole spectrum of accident sequences in a process. Generic IROFS need not be listed separately for each accident sequence to which they are applicable as long as they are described in the Integrated Safety Analysis (ISA) Summary

Discussion

The aspects of bounding assumptions and passive engineered features discussed in this guidance include: what constitute bounding assumptions and design features, and when these are required to be IROFS; the use of generic IROFS; grading of quality assurance (QA) and management measures (including configuration management (CM) applied to IROFS; and what constitute sole IROFS.

Bounding Assumptions and Design Features

10 CFR 70.61 requires that the risk of credible events meeting specified consequence thresholds must be limited, that the risk of nuclear criticality accidents must be limited, and that the engineered or administrative controls or control systems that are necessary to meet the performance requirements be designated as IROFS. Performing an ISA involves identifying credible hazards that can lead to exceeding the performance requirements of 10 CFR 70.61(b), (c), or (d). Conduct of an ISA pre-supposes that there is a chemical or physical process (hereafter referred to as "the process") to analyze. The hazards postulated are specific to the process being analyzed, and depend on the types and quantities of material to be processed.

The unmitigated consequences associated with the identified hazards depend upon the technology and equipment to be used and other assumptions about the nature of the process. Information regarding the process that is intrinsic to the analysis used to determine the unmitigated consequences is sometimes referred to as "bounding assumptions" or "initial conditions". It defines the bounding parameters of the process being analyzed. It may be generic in the sense that it applies to all hazards analyzed in the facility (or major process area, such as dry conversion).

While the safety demonstration of the analyzed process relies on these bounding assumptions, there is no benefit or requirement to list them for every accident sequence to which they apply. Some of these items are so fundamental to the process design and safety analysis that it is not credible they would fail or deliberately be changed without altering the entire nature of the process. Many such bounding assumptions are so fundamental that they are captured as conditions of the license. As an example of this, chemical consequence or criticality calculations may be based on the maximum licensed

quantity of fissile material on-site. As another example, a low-enriched fuel fabrication facility may be limited to 5wt% ^{235}U , and does not process plutonium. Changing these license conditions would always require a license amendment. Bounding assumptions that are based on license conditions or commitments need not be identified as IROFS. However, other bounding assumptions that is subject to failure mechanisms and relied on to satisfy the performance requirements may be required to be designated as IROFS. Specific examples will be discussed later.

In addition to the bounding assumptions, engineered features of the design may be featured in the analysis and may play an important role in the management of risk of consequential events. These may include passive engineered features associated with the site, building, or entire process area, such as the building shell, roof, floor, piping systems and vessels. They may also include active systems such as a fire sprinkler system, a ventilation system, and some aspects of moderation controlled areas. Finally, human actions governed by administrative controls may sometimes be included within the analysis of consequences of credible events, although actions designed to prevent or mitigate the event should not be included in the assessment of unmitigated consequences. Many of these are generic in the sense that they apply to the entire facility, a process, or a whole spectrum of accident sequences in a process. If these items can credibly fail or be changed by the licensee, they should be evaluated as potential IROFS.

This guidance will refer to these two types of items as BPAs and design features.

Designation of Generic IROFS

10 CFR 70.61(e) states, in part, “Each 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 definition of an IROFS in 10 CFR 70.4 includes, “Structures, *systems*, equipment, components, and activities of personnel.” The regulations of Part 70 therefore, allow IROFS to be defined at the system level, i.e., by grouping multiple individual components, pieces of equipment, and/or operator actions together if they combine to perform a single well-defined safety function. An example of this would be the enrichment control system for an enrichment facility which may include in-line monitors and detectors, sampling, control flow valves, a programmable logic controller, control room computers, etc. It is not necessary that each of these components be listed as an individual IROFS because they work together to perform a single well-defined safety function. It is also not necessary that this IROFS be repeated in each and every sequence where a maximum bounding enrichment is assumed. It is, however, crucial that such a system of IROFS be clearly and completely defined, so that it is clear what is and what is not considered part of the IROFS (what is often referred to as the “boundary” of the IROFS) and what is necessary to perform the required safety function.³ The licensee’s CM Program must identify what individual components are part of this system of IROFS in plant working level documents (such as part and component drawings, piping and instrumentation diagrams, calibration and maintenance procedures, and procurement specifications) that are part of the process safety information maintained onsite. The flowdown from the ISA Summary into the CM Program documents should be clearly definable, so that the licensee staff can identify and manage the components or features of components that are part of the generic IROFS. This will also enhance the

³ Reference 10 CFR 70.62(1)(c)(vi)

efficiency of U.S. Nuclear Regulatory Commission (NRC) processes by facilitating vertical slice review of any selected IROFS.

Examples of Generic IROFS

The guidance that follows, draw a distinction between BPAs and design feature IROFS. Both of these are generic features of the facility or process, but the distinction between them is based on whether they are part of the enveloping definition of licensed activities or part of the design of facility process equipment or procedures.

Frequently, a BPA is so fundamental to the nature of licensed activities that it is very unlikely to fail and could not be changed without changing the entire nature of licensed activities. Failure would constitute a major process disruption and would almost certainly require reporting to the NRC. Changing it would almost certainly require a major license amendment. In the limited cases when a BPA is *credible* to fail in a manner that could cause a failure to meet the performance requirements of 70.61, then IROFS must be established to maintain the validity of the assumption.

On the other hand, a licensee can remove or change any design feature if allowed by the requirements of 10 CFR 70.72. The design feature may or may not have credible means of failure and changing it may or may not require a license amendment under 10 CFR 70.72. Common design features include structural components, geometry of equipment, configuration (spacing and arrangement) of equipment, and materials of construction. Since design features can credibly be changed, they should not be relied on to determine that an accident sequence is not credible. However they may be relied upon to prevent or mitigate the consequence of credible events. When a design feature is designated as an IROFS, it is recognized and controlled as safety significant in the facility's CM system and QA program.

The main distinction between a BPA and a design feature IROFS is that the former are not easily identifiable with specific systems, structures, or components within the facility. (Less important than distinguishing what category an item falls into is ensuring that all such generic items are identified and controlled as needed to meet the performance requirements.) A control used to maintain a bounding assumption, and an attribute of design features should be designated as an IROFS when it is relied on as part of the demonstration of compliance with the performance requirements and can credibly be changed.

Examples of such generic items, whether BPAs, design features, or other types of items, which may be designated as IROFS follow:

BPAs

- Bounding facility enrichment—If the maximum enrichment allowed under the license is used in all criticality calculations and is relied on to meet the performance requirement of 70.61(d), this is a generic IROFS that applies to all analyzed criticality accident sequences in the facility.
 - If the facility is not an enrichment facility, then there is no credible means of exceeding the maximum allowed enrichment because it would involve many unlikely human actions with reason or motive for this occur. Enrichment controls (e.g., assay verification upon receipt) are not IROFS.

- If the facility is an enrichment facility, then it may be credible to exceed the bounding enrichment and there should generally be an enrichment control system generic IROFS. An example of a credible enrichment upset is inadvertently connecting a product cylinder to a feed station.
- Reliance on fluorinating properties of dry conversion process - The lack of solutions in a dry conversion process means that a limiting quantity of moderator can be assumed in calculations and the process hazard analysis. The fluorinating nature of uranium hexafluoride (UF_6) can be assumed in several ways in a criticality analysis (limiting liquid water intrusion into process equipment and cylinders due to formation of self-sealing reaction products, reaction of liquid water to form hydrogen fluoride, limiting the H/X (hydrogen-to-fissile) ratio from wet air in-leakage, etc.). These are natural processes that should not be designated as IROFS.
- Physical and chemical form of material - Uranyl nitrate solutions may be assumed in a uranium recovery area, uranium dioxide powder with a bounding density in powder preparation areas, UF_6 in enrichment processes, etc.
 - If the process is analyzed safe for the most reactive fissile material that could credibly be present (such as optimally moderated uranium oxide in water), then IROFS are not needed to control the chemical form.
 - If the process is only analyzed for uranyl nitrate, and other forms of material are credible, then the controls necessary to ensure that more reactive materials are not present should be IROFS.

If the reactivity, volatility, toxicity, or other properties of concern are greater for one type of material than another, the fact that a process uses material of a certain physical and chemical form may be part of the safety basis of the process, in that it provides a safety function that supports meeting the performance requirements, and the associated control system should be an IROFS.

- Full water reflection - Assuming 12 inches of close-fitting water reflection around units is a common assumption used in nuclear criticality safety (NCS) analyses, since it provides the maximum possible reflection in most circumstances.
 - If there are no special moderators present or readily available on-site (such as graphite, heavy water, or beryllium; heavy concrete walls or floors are located away from fixed process equipment), or have shown to have been bounded by full water reflection (such as lube oil and organic solvents), then no IROFS are needed to prevent reflection conditions more reactive than twelve inches of water.
 - If measures must be taken to control special moderators, quantities of organic materials must be limited, or the process is mobile (such that it could be brought into close contact with heavy concrete walls or floors), then these controls should be designated as IROFS.

- Elevation above the flood plain/topographic features preventing flooding - These site features are part of the overall site characterization and prevent flooding in all parts of the facility. (Similar site characteristics that may be credited include the design basis earthquake, maximum rainfall, seasonal temperature ranges, size and shape of site boundary, etc.) Such characteristics may be able to be shown to be not credible to change, in which case they do not have to be IROFS.

Design Features

- Non-combustible construction of facility equipment - This may include the non-combustible construction of the fire sprinkler system (whereas other aspects of the sprinkler system may be part of an active IROFS), or other features of the building or fixed process equipment that limit the combustible loading.
- Use of plant-wide limits and controls - Examples include restrictions to limit all piping in a given area to less than 1 inch diameter, to maintain at least 12 inches between fissile-bearing equipment and portable containers, to maintain all accumulations to a depth of less than 4 inches, and to maintain individual gloveboxes to less than 350 grams ²³⁵U. These limits are generally based on “generic” (non-process specific) calculations, or on single-parameter limits as found in ANS-8 Series standards and are often incorporated into the license application. These specifications are generally relied upon to comply with 70.61(d) and may be characterized as a generic IROFS with sufficiently clear specification of applicable limits and locations (i.e., buildings, process areas, etc.) CM may be the necessary and sufficient management measure for this IROFS.
- Use of upstream controls for safety of downstream processes - Examples of these would be sampling and measurement to verify the characteristics of incoming feed material, flow controls in a downblending operation to limit downstream enrichment, and restrictions on lubricants added to powder to limit downstream moderation. If necessary for compliance with the performance requirements, these may need to be IROFS.
- Installation of fixed process equipment - The relative location and spacing of process vessels and equipment in the facility is often credited for neutron interaction control. A criticality safety interaction model implicitly assumes that different parts of the model are arranged as designed, and that everything that could increase reactivity in a statistically significant way has been included in the model. Moving process equipment around on the shop floor or installing new equipment could invalidate the assumed configuration of process equipment in the criticality calculations. If these features are relied on to comply with the performance requirements, then they should be designated as an IROFS.

Other Types of Generic IROFS

There may be some items that do not fall neatly into one of the preceding categories of generic IROFS, including systems of controls that may have active and/or administrative components. Some examples follow:

- Moderation controlled area - Moderation is often excluded from whole sections of a facility by means of an interlocking set of passive and administrative controls,

such as use of a double roof, double-sleeved pipes, a sloping floor, favorable geometry drains, the exclusion of liquid-bearing piping or solutions, prohibitions on bringing solutions into the area, restrictions on firefighting, etc. Exclusion of moderators would apply to every criticality sequence in the moderation controlled area. Failure is credible because the failure of any one part of the system could lead to a loss of moderation control. This system of controls is necessary to comply with the performance requirements of 70.61(d) and is therefore required to be an IROFS.

- Existence of fire sprinkler system - This provides mitigation for all fire events in the covered portion of the facility regardless of the initiating event. This would be an active engineered control that limits the spread of a fire. If credited to prevent or mitigate a consequence of concern (e.g., chemical release or radiological dose due to propagation of a fire), it would be required to be an IROFS.
- Process ventilation system - This system provides mitigation for chemical release scenarios (confinement), regardless of the specific reaction or event leading to a release. Passive portions of the system may be a design feature, but there may also be dynamic confinement. If it is necessary to comply with the performance requirements of 70.61(b) or (c), then it must be an IROFS.

Definition of the safety function of a generic IROFS

10 CFR 70.65(b) states, in part, that the ISA Summary must describe IROFS “in sufficient detail to understand their safety functions in relation to the performance requirements of §70.61,” and also that it must contain “information that demonstrates the licensee’s compliance with the performance requirements.” Taken together, this means that the IROFS must be described, that this description must identify the safety function of the IROFS, and that the information be sufficient to support the demonstration of compliance with the requirements of 10 CFR 70.61(b), (c), and (d). The amount of information needed to provide reasonable assurance that the IROFS will be available and reliable to perform its safety function when needed varies from one IROFS to another. It is not necessary to describe all physical attributes associated with the IROFS; it is only necessary to describe the attributes related to its safety function at the necessary level of detail to show that the performance requirements of 10 CFR 70.61(b), (c), and (d) are met.

IROFS (whether BPAs or design features) may be described generically. That is, they may be described as a whole system of components and/or operator actions that performs a single well-defined safety function. One example is that of “favorable geometry piping.” The description should be sufficiently detailed so that what falls within the system as well-defined: “favorable geometry piping in the uranium recovery area” or “in the XYZ Building.” It is not necessary that every section of piping be listed as a separate IROFS since the boundary has been unambiguously defined. All fissile solution piping in the facility would be subject to configuration management, so it is necessary that the pipes be included in the licensee’s facility management system and the linkage from the ISA Summary to lower-tiered documents be transparent.

With regard to the safety function, it may be sufficient to specify that a particular IROFS controls a specific parameter or parameters. Within the context of the facility’s NCS Program and the case of favorable geometry piping, this is taken to mean that it has

been accepted to be subcritical using an approved method, which may include performing a calculation of piping and surrounding equipment and showing that it is less than the licensed k_{eff} limit, comparing dimensions to single-parameter limits tabulated in the license application, or comparing dimensions to limits in industry-accepted handbooks and ANS-8 Series standards. Knowing that the piping is favorable geometry may be all the detail that the technical reviewer needs to know about it, in order to understand the safety function and to obtain reasonable assurance that the performance requirements will be met. (This assumes that it has no other safety-related attributes, such as the wall thickness, material of construction, or elevation.)

However, if the piping is close enough that neutron interaction is a concern, then additional detail on the system configuration may be appropriate. For example, it may be necessary to define the safety function as, "Piping is less than two inches in diameter" or, "Piping is less than the cylinder diameter in Table X and spaced at least 12 inches apart." Alternately, a whole array of piping or a complex piece of equipment may need to be evaluated to be shown subcritical, in which case it is not possible to describe the safety related attributes in such simple terms. One way of describing the safety related attributes at an appropriate level of detail would be to describe what is included in the criticality model at the system level and state that the entire piece of equipment is subcritical based on validated calculations. For example, a design features IROFS may be "geometrically safe sintering furnace FURN-123." The safety function would be "maintain subcriticality by limiting dimensions and system configuration based on criticality calculation." It is not necessary to list every component or to go into greater detail in the ISA Summary. An inspector or technical reviewer could retrieve the on-site documentation (the criticality safety analysis and/or calculation document) and see what dimensions are included in the model. Then as long as the model adequately bounds the as-built equipment, with approved margin, the performance requirement of 10 CFR 70.61(d) has been met.

Specifying the safety function at an appropriate level of detail is important to both the regulator and the licensee. Too sparse of a level of detail, and the information in the ISA will be insufficient to demonstrate compliance with the performance requirements. Too detailed, and it will constrain changes in a way that is unduly burdensome. For example, if the ISA Summary describes an IROFS as "vessel with diameter equal to two inches," then any increase or decrease in the diameter may need to be evaluated against the criteria of 10 CFR 70.72(c), especially if it is a sole IROFS. However, if it is described as "vessel with diameter less than two inches," then a decrease in diameter does not constitute a change to the IROFS, as it is described in the ISA Summary. Furthermore, if a bounding limit is used that provides for margin, a licensee may choose to describe it as "vessel with diameter less than four inches." Then, assuming the nominal diameter is two inches, a decrease, or an increase up to the analyzed subcritical limit of four inches, does not constitute a change to the IROFS, as described in the ISA Summary. The description of the IROFS, in terms of its safety-related attributes and the safety functions they perform (and in sufficient detail to provide reasonable assurance that the performance requirements are met) help define the safety envelope of the process. For those sequences that are reviewed as part of the NRC's horizontal and vertical slice reviews, it is this information that the reviewer sees and which form the basis for the approval. Therefore, it is the safety function of the IROFS, as described in the ISA, that is the basis for evaluating changes against in 10 CFR 70.72 and determining whether a failure has occurred that results in failure to meet the performance requirements (as in Part 70 Appendix A).

For the examples of generic IROFS listed above, here are examples of how they might be described in the ISA Summary at an appropriate level of detail:

BPA's

- Bounding facility enrichment: "Enrichment limited to less than 5wt% ²³⁵U plant-wide by license limit."
- Fluorinating properties of UF₆: "Solutions and liquid reagents not used in dry conversion area."
- Chemical form: "Reference fissile material is optimally moderated uranyl nitrate solution," (implicitly takes credit for neutron poisoning of nitrogen).
- Reflection: "No moderators more effective than water are allowed in the ABC process," or, "Lube oil limited to less than 1000 grams per pump in the ABC process."
- Building elevation: "Building constructed above the 100-year flood plain."

Design Features IROFS

- Non-combustible construction: "Vault storage racks will be composed of non-combustible materials."
- Portable container spacing: "All safe volume containers will be handled one-by-one and spaced at least 12 inches apart in the Uranium Recovery Area."
- Enrichment control: "UO₂ powder is limited to less than 4.25wt% ²³⁵U downstream of the large geometry blender by means of mass flow totalizers and in-line monitoring."
- Interaction control: "Process vessels are spaced no closer than 24 inches edge-to-edge," or, "Process equipment is arranged as described in area drawings."

Other Types of Generic IROFS

- Moderation controlled area: “Building XYZ is defined as a moderation controlled area,” (may be appropriate to list individual building features and procedural controls), or else define generally in the license application.
- Fire sprinkler system: “Room 123 in Building ABC is covered by a dry-pipe sprinkler system.”
- Process ventilation system: “Process off-gas system includes dual high efficiency particulate air filters and wet scrubber system to prevent radiological releases to the environment.”

Each description of the generic IROFS should include: (1) the system-level description, which includes information on what is included in the system (also known as the system boundary); (2) the safety significant attributes; (3) the safety function to be performed; and (4) sufficient information to understand its theory of operation and provide reasonable assurance that it will be sufficient to meet the performance requirements.

Many ISA Summaries contain tables of accident sequences similar to those in Appendix A of NUREG-1520. These typically include initiating events, IROFS, and risk-reduction (likelihood or consequence reduction) scores to demonstrate compliance with the performance requirements. While this is a useful format, this format is not required, and there is therefore, no requirement that generic IROFS be listed in every line of the tables to which they apply. One place that this information may be included is in the process description, in a header to the accident sequence table for the affected area (e.g., “all piping in this area is subcritical by geometry control”), or in a generic type of accident sequence (e.g., “loss of geometry control”). This may be included as part of the description of each process “in sufficient detail to understand the theory of operation” or “a general description of the types of accident sequences” as required in 10 CFR 70.65(b)(3).

Generic Design Features IROFS for Meeting 10 CFR 70.61(d)

The requirement that “each 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” has implications when performing calculations to demonstrate that “under normal and credible abnormal conditions, all nuclear processes are subcritical” (10 CFR 70.61(d)). There are a great many dimensions and compositions that go into modeling a fissile material process realistically. Not all of these variables are necessarily required to demonstrate subcriticality. It is part of the job of the analyst to determine which parameters need to be controlled to maintain subcriticality and meet the double contingency principle, based on the process configuration as modeled, and to select what controls and parameters are to be relied on to meet 10 CFR 70.61. The controls tend to be based on a subset of the variables that go into a calculation.

In general, if a criticality parameter is controlled for criticality safety purposes, it is controlled by means of a structure, system, equipment, component, or activity of personnel, to ensure that the parameter’s safety limit will not be exceeded. Pursuant to 10 CFR 70.61(e), that control should be identified as an IROFS. If a criticality parameter is not controlled, it will be assumed to be at its optimum or most reactive credible, value,

and no IROFS are necessary. The relationship between the subcriticality requirement in 10 CFR 70.61(d) and the remaining performance requirements of 10 CFR 70.61(b) and (c) is discussed in more detail in FCSS-ISG-03, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle."

As an example, consider an oxidation furnace in a low-enriched fuel fabrication facility. The licensee could choose to model the furnace as a horizontal cylinder filled with optimally moderated UO_2F_2 solution, and then determine the maximum permissible cylinder diameter. This would require a conservative model, generally somewhat larger than the actual furnace. If such a conservative model was not adequately subcritical, the licensee could choose to include the wall thickness and possibly the internal screw to displace material. If needed, the licensee could include the composition of the firebrick and steel internals, and may also need to model the discharge hopper, structural supports, and so on. Generally, the less margin there is, the more detailed the model will have to be. Including more system features in the model has the drawback that a larger number of dimensions and material compositions are relied on for safety. In each case, the IROFS is the geometry of the furnace. In the simple cylinder model, only the outer dimension of the furnace needs to be controlled. In the fully detailed model, the outer diameter, the wall thickness, the diameter of the screw shaft, and the hopper depth may be identified as geometry controls needed to ensure subcriticality. The licensee may determine that the firebrick thickness is not significant, because it chooses to conservatively model the furnace with full water reflection that bounds any external refractory material. The licensee would probably not model small steam piping, flanges, thermocouple penetrations, bolt heads, and structural supports, realizing that they have such a small effect on system reactivity that including or excluding them does not change its ultimate conclusion as to whether the system is subcritical. Only the minimum set of model parameters that is necessary to make a finding of subcriticality are being relied on to meet 10 CFR 70.61(d). (In fact, the licensee could choose to rely instead on mass control, if operationally feasible, and ignore the geometry of the furnace altogether.)

While the entire furnace would be controlled under the licensee's CM program, the criticality calculations are normally vastly simplified so as to reduce the amount of analytical work needed and the number of individual variables that need to be controlled. Generally, those factors that have a negligible effect on system reactivity are omitted from the calculation; otherwise they may be found to have a negligible effect in the course of doing sensitivity studies on the system. The licensee has the ultimate responsibility for deciding how detailed the modeling need be and deciding what parameters it is necessary to control.

Geometry is the preferred means of control, and passive engineered controls are preferred over active engineered or administrative controls. The safest design from the standpoint of criticality is the one that relies on passive geometry control. While favorable geometry is considered to mean dimensions that are safe when all other parameters are at their most reactive credible values, in reality geometry is almost never the only thing being relied on for safety. Implicit in saying that something is the assumption that the system is neutronically isolated, which implies interaction control. In addition, this is always for a given fissile material, usually with a distinct physical and chemical form and enrichment. Thus, spacing, physical and chemical form, and enrichment, are almost always implicitly relied on as BPAs or design features even for a favorable geometry IROFS.

Grading of QA and Management Measures

10 CFR Part 70 defines management measures as “the functions performed by the licensee, generally on a continuing basis that are applied to IROFS, to ensure the items are available and reliable to perform their functions when needed.” Management measures are applied to passive engineered, active engineered, and administrative IROFS to the extent needed to ensure that they will be sufficiently available and reliable to meet the performance requirements of 10 CFR 70.61(b), (c), and (d). As needed, “management measures include configuration management, maintenance, training and qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements” (10 CFR 70.4).

10 CFR 70.61(e) states, in part, that the function of the facility’s safety program is to “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.” The facility safety program consists of three elements: process safety information, integrated safety analysis, and management measures. 10 CFR 70.62(a) states that: “The safety program may be graded such that management measures applied are graded commensurate with the reduction of the risk attributable to that item” (the contribution of the IROFS to meeting the performance requirements). With regard specifically to management measures, 10 CFR 70.62(d) states that they “may be graded commensurate with the reduction of the risk attributable to that control or control system.” Only those management measures necessary to ensure that IROFS are sufficiently available and reliable to meet the performance requirements of 10 CFR 70.61(b), (c), and (d), as documented in the ISA Summary, need be implemented to comply with the above requirements.

A licensee’s methodology for determining the availability and reliability of IROFS is tied closely to its quality assurance program (QAP). Its ISA methodology frequently contains a table that describes what management measures will be applied to individual IROFS; this table is usually ‘graded’ only by the type of control (passive engineered, active engineered or administrative). A typical illustrative example follows:

Management Measure	Passive Engineered	Active Engineered	Enhanced Admin	Simple Admin
Configuration Management	✓	✓	✓	
Preventive Maintenance	✓	✓	✓	
Surveillance	✓	✓	✓	✓
Functional Testing		✓	✓	
Calibration		✓	✓	
Pre-operational Verification	✓	✓	✓	✓
Procurement Specification	✓	✓	✓	
Training and Qualification			✓	✓
Audits and Assessments	✓	✓	✓	✓
Procedures and Postings			✓	✓
Records Management	✓	✓	✓	✓
Other Quality Assurance (QA) Elements*	✓	✓	✓	✓

*As described in NUREG-1520 and 10 CFR Part 50 Appendix B

Another type of 'grading' may be based on defining different 'quality levels' (QLs). One common approach is to define QL-1 as applying to all IROFS, QL-2 as applying to other safety controls that are not IROFS (e.g., "defense-in-depth", double contingency items, or items that support the function of IROFS), and QL-3 as applying to non-safety items. A less preferred approach is applying QL-1 to sole IROFS and QL-2 to IROFS which are one of several items preventing or mitigating an accident. Generally, QL-1 items require that all management measures applicable to a certain type of control (as in the table above) be applied, whereas QL-2 items require only those measures deemed necessary by a specific safety evaluation, and QL-3 items do not require any management measures other than to be covered by the facility's CM Program.

Management measures applied to IROFS may be graded in ways other than these, as there is no set prescription for how IROFS may be graded. There is no regulatory requirement to apply the full set of management measures theoretically applicable to an engineered or administrative control to every IROFS of a given type. The management measures appropriate for any particular IROFS are rather determined by the way in which the IROFS contributes to the risk reduction in the ISA, which includes both the safety function that it performs and the degree to which it is relied on to prevent or mitigate an accident (i.e., "in the context of the performance requirements"). Factors that should be considered when grading an individual IROFS' management measures include the following:

1. The safety function of the IROFS (the specific attributes being relied on)
2. The specific failure mechanisms that could lead to exceeding the performance requirements
3. The amount of risk-reduction being credited for demonstrating compliance with the performance requirements

Two additional types of grading are permissible under the requirements of 10 CFR Part 70 besides those discussed above. First, there is no regulatory requirement or possible safety benefit to apply a particular management measure to an IROFS, regardless of its type or quality level, if the performance requirements can still be met without the management measure. Second, within each management measure, there is a gradation in the frequency or stringency with which it can be applied.

Several examples of how management measures may legitimately be graded follow:

- A pipe between two process vessels is frequently a passive engineered criticality control. Piping should be included as part of the facility's CM Program. The applicability of other management measures depends on the safety function of the pipe. For example, if only the outer diameter is credited for passive geometry control, and the pipe is not subject to bulging or corrosion, the only management measures necessary may be CM and certain supporting QA elements (such as procurement, pre-operational verification, and records management). However, if the inner diameter is credited, periodic surveillance of wall thickness may be necessary, depending on whether it is subject to a corrosive chemical environment. This periodic surveillance may also require calibration of test equipment, and procedures and training for its use. If the material of the pipe is credited as a neutron absorber control, additional management measures may be needed to ensure its composition prior to installation or continued efficacy.

- A robust passive geometry control with no identified credible means of failure may not require any management measures other than those associated with proper installation (procurement specification, pre-operational verification) and subsequent CM. However, if the geometry control is subject to corrosion, bulging, leaking, backflow, or has other credible failure mechanisms, periodic surveillance, maintenance, and other management measures may be needed to ensure that it remains available and reliable to perform its safety function when needed.
- The periodicity of surveillance of the above-mentioned pipe may depend on the amount of risk-reduction (e.g., likelihood or duration index assigned to its failure) afforded. For example, if the assumed likelihood of failure is $10^{-3}/\text{yr}$, then it is not necessary to subject the IROFS to surveillance as frequently as if its likelihood of failure is $10^{-1}/\text{yr}$. If duration is credited, the assumed duration of failure may be the basis for the surveillance period. For example, a duration index of -1 may imply surveillance should be performed on a monthly basis. The corrosion rate, taken together with the minimum permissible wall thickness, may also be the basis for the surveillance period. A control whose failure would be self revealing may need no formal surveillance, because its failure would be promptly detected and corrected.

One management measure in particular (CM) must be applied to all facility features, regardless of their safety significance or IROFS status, per 10 CFR 70.72(a). An important class of passive IROFS is the subset of facility design features for which no credible failure mechanism has been identified, other than failure of the CM program. For these items, the only mechanism that can lead to a consequence of concern is a design change, and in those cases, the minimal set of management measures is appropriate. The only management measure applicable to such passive design feature IROFS would be CM and associated measures needed to ensure its proper procurement, installation, periodic audits, and identification and correction of nonconforming items. Once it is installed, there would be no need to take further action, other than as part of periodic audits; there is simply no need to try to actively maintain facility features that cannot credibly change.

Grading of the management measures and quality assurance program commensurate with risk and in the context of the performance requirements may be done by grading, (1) what specific management measures are applied, and (2) the periodicity and stringency with which they are applied. Questions that may be asked in evaluating the appropriate amount of management measures to be applied include: *What is the safety function the IROFS performs? What are the possible ways in which it can fail? How reliable does it have to be? How does the application of management measures affect the reliability and availability?*

Applicability to Sole IROFS

For criticality safety there should almost never be items that are sole IROFS. Even for passive geometry control, there are always assumptions and additional controls (spacing, physical and chemical form, enrichment, etc.) upon which the designation as favorable geometry is based. In any case, process designs should ensure that at least two independent, unlikely, and concurrent changes in process conditions are necessary before criticality is possible. (For other disciplines, that are not required to meet double contingency, sole IROFS may occasionally be encountered.) In the few occasions

where there are sole IROFS, altering a sole IROFS should be understood as altering the safety function of the IROFS as described in the ISA Summary. Changes that do not alter the system boundary, safety significant attributes, safety function, or degree to which the item is relied on to prevent or mitigate an accident of concern (including, if relied on, the safety margin) do not alter the safety function of a sole IROFS as described in the ISA Summary. Describing the safety function at an appropriate level of detail (see discussion above on describing the safety function of a generic IROFS) therefore determine what physical changes may constitute altering a sole IROFS.

The fact that a design change, whether deliberate or inadvertent, could defeat the safety function of a geometrically safe item does not make that item a sole IROFS. 10 CFR 70.72 permits facility changes without prior NRC approval provided such a change: “does not alter any item relied on for safety, listed in the integrated safety analysis summary, that is the sole item preventing or mitigating an accident sequence...”. In the case of a favorable geometry component, the geometrically safe “item” has not failed in this particular sequence, and is therefore not preventing the event. The event being considered here is a design change, and what is preventing this event is the change control or configuration management program, not the safe geometry item. The item has not failed, nor, in the language of the rule, could it “prevent” the change. Thus the hardware item is not the “sole item preventing the accident sequence”; and the hardware “item” does not become a sole IROFS. (The geometrically safe item would only be a sole IROFS if there is some sequence in which a spontaneous failure - not the failure as the result of a design change - is credible, and is the only event that must occur before criticality is possible.)

The CM Program is a management measure, not an IROFS. The CM Program does not perform any identifiable safety function in and of itself, independent from the items that are in direct contact with the process. CM is applied *to* something, most significantly to the structures, systems, and components relied on to prevent or mitigate an accident (the IROFS). A failure of CM is therefore only significant in that it may impact the ability of an IROFS to perform its intended safety function when needed. It is important that items relied on for safety are designated as IROFS primarily so that they will receive special recognition prior to their being changed.

The spectrum of events that should be considered in performing the ISA includes design changes. To protect against such events, the items relied on to meet 10 CFR 70.61(b), (c), or (d) are designated IROFS, and the CM Program is a management measure that requires numerous approvals before an item can be changed. The possibility of design changes should be considered as part of the ISA process. Some changes would be extremely unlikely or even incredible, such as changing the thickness of the building foundation or replacing gas centrifuges with unfavorable geometry equipment. Some changes would be much more likely, such as connecting a flexible hose to the wrong tank, incorrectly installing (or failing to install) filter or trap media, or introducing larger portable containers than allowed into an area. If a massive failure of the configuration management system would be required, such that it would take many unlikely human actions or errors for which there is no reason or motive, then there is no credible hazard involving a design change, and a sequence does not need to be included in the ISA Summary. It would be expected that the evaluation would be included as part of the on-site ISA documentation. (Given the history of events involving deliberate or inadvertent configuration changes, proving this could be very difficult.) If a single event, or reasonably foreseeable series of events, for which there is reason or motive, can change

the configuration of the system, that should be evaluated to determine if there is an accident sequence that can result in exceeding the performance requirements.

In summary, items which rely on geometry to assure that they are subcritical for all normal or credible abnormal events are being used to demonstrate compliance with 70.61(d), and hence by 70.61(e) are IROFS. However, in general, they would not be sole IROFS. It is important for regulatory oversight to assure that all such items relied on to assure 70.61(b), (c), and (d) are designated IROFS. It is through this designation as IROFS that they become subject to the requirements assuring that the NRC has current information on the plant's safety basis; namely: 1) being included in the list of IROFS in the annual ISA Summary update, 2) subject to equivalent replacement (70.72(c)(2)), and 3) advanced approval of alteration of sole IROFS (70.72(c)(3)).