RAS 11459

DOCKETED
USNRC

2006 APR -3 PM 3:45

OFFICE OF THE SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Interim Staff Guidance-03, Revision 0
Nuclear Criticality Safety Performance Requirements and Double Contingency Principle

Prepared by
Division of Fuel Cycle Safety and Safeguards
Office of Nuclear Material Safety and Safeguards

Issue

This guidance describes the relationships between Title 10 of the Code of Federal Regulations (10 CFR) Part 70, Subpart H nuclear criticality safety requirements (i.e., the 10 CFR 70.61 performance requirements and the double contingency principle of 10 CFR 70.64).

Introduction

Part 70 of 10 CFR, Subpart H contains three separate requirements to ensure nuclear criticality safety. One requirement, 10 CFR 70.64(a)(9), requires that the design of new facilities and processes provide for criticality control including adherence to the double contingency principle. A second requirement, 10 CFR 70.61(b), requires that high consequence events (which typically will include criticality accidents) be highly unlikely. A third requirement, 10 CFR 70.61(d), requires that nuclear criticality accidents be limited by assuring that under normal and abnormal conditions all nuclear processes are subcritical, including use of an approved margin of subcriticality, and also requires that the primary means of criticality protection be prevention.

The purpose of this Interim Staff Guidance (ISG) is to clarify the relationship between these three requirements.

Discussion

There are three separate requirements in 10 CFR Part 70 for ensuring nuclear criticality safety. The first requirement of 10 CFR 70.64(a)(9) is more prescriptive and deterministic than the performance requirements of 10 CFR 70.61. Section 70.64 establishes baseline design criteria for new facilities and processes, similar to general design criteria in 10 CFR Part 50. One of these baseline design criteria applies directly to criticality safety. Specifically, 10 CFR 70.64(a)(9) requires that the design "provide for criticality control including adherence to the double contingency principle." Section 70.64(b) further specifies that new facilities or processes must incorporate defense-in-depth practices, which is defined as a "design philosophy, applied from the outset and through completion of the design, that is based on providing successive levels of protection such that health and safety will not be wholly dependent upon any single element of the design, construction, maintenance, or operation of the facility." Section 70.64(b)(1) specifically mentions preference for the selection of engineered controls over administrative controls to increase overall system reliability.

Another more risk-informed and performance-based requirement is contained in 10 CFR 70.61. In short, this regulation stipulates that credible high consequence events shall be made "highly unlikely" or be mitigated (10 CFR 70.61(b)) and that intermediate consequences shall be made "unlikely" or be mitigated (10 CFR 70.61(c)). High and intermediate consequence thresholds

U.S. NUCLEAR REGULATORY COMMISSION
In the Matter of Louisiana Energy Services, LP
Docket No. 70-3103-ML Official Exhibit No. Staff 59-M
OFFERED by: Applicant/Licensee Intervenor
NRC Staff Other
IDENTIFIED on 3/6/06 Witness/Panel Staff Criticality
Action Taken: ADMITTED REJECTED WITHDRAWN
Reporter/Clerk Bethany Engel

February 17, 2005

Template=SECY-027

SECY-02

for workers and members of the public are established for both chemical and radiological events. Under this risk-informed and performance-based regulation a criticality accident would typically be considered a high consequence event to the worker since the worker could receive a dose in excess of 100 rem TEDE (total effective dose equivalent).

In addition, there is a separate provision within 10 CFR 70.61 that specifically addresses criticality safety. Section 70.61(d) states that, in addition to meeting the requirements above for high and intermediate consequence events, 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." The purpose of this is to preclude a situation where nuclear criticality would be permitted as long as the dose thresholds of § 70.61(b) and § 70.61(c) are not exceeded.

Thus, 10 CFR Part 70 contains three separate and distinct requirements related to precluding nuclear criticality (10 CFR 70.64(a)(9), 10 CFR 70.61(b), and 10 CFR 70.61(d)), besides provisions in § 70.24 and § 70.52, which pertain to mitigating the consequences of a criticality accident and reporting its occurrence.

Section 70.61(d) of 10 CFR Part 70

Section 70.61(d) requires that under normal and credible abnormal conditions all nuclear processes are subcritical including use of an approved margin of subcriticality for safety. In addition, preventive controls and measures must be the primary means of protection against criticality. Meeting this performance requirement entails a number of factors. First, all normal and credible abnormal conditions must be identified. There are many different methods that may be employed to do this, but a systematic methodology should be used to provide reasonable assurance that the complete spectrum of credible conditions has been identified.

Normal conditions are those specifically allowed for as part of the normal modes of operation in the facility design (i.e., conditions that may occur without the failure of any items relied on for safety (IROFS)). Abnormal conditions are those events not planned for as a regular occurrence in the facility or operation design. They include those undesirable conditions that are the result of external events and process deviations, including those resulting from the failure of identified IROFS. Credible abnormal events include both credible single events (e.g., an external event or failure of a single IROFS) and credible sequences of events. Credible sequences of events include, but may not be limited to, chains of independent but not unlikely process deviations (i.e., not precluded by IROFS) and chains of related failures of IROFS (i.e., failures that are not independent). Some judgment must be employed in determining what constitutes a credible abnormal condition. It is not necessary to include multiple independent failures of IROFS within the spectrum of credible abnormal conditions. Additional guidance on what is considered not credible is contained in NUREG-1520, Section 3.4.3.2:

a. "An external event for which the frequency of occurrence can conservatively be estimated as less than once in a million years."

b. "A process deviation that consists of a sequence of many unlikely human actions or errors for which there is no reason or motive...."

c. "Process deviations for which there is a convincing argument, given physical laws, that they are not possible, or are unquestionably extremely unlikely...."

The requirement that nuclear processes be subcritical is satisfied if the licensee or applicant demonstrates that the most reactive credible conditions are subcritical. To provide adequate assurance of subcriticality, this must include margin. There are several different ways to demonstrate subcritcality, as discussed below:

- If subcriticality is demonstrated using an appropriately validated calculational method, then k_{eff} (K effective) (including calculational uncertainties) must be less than the approved upper subcritical limit (USL), as specified in the license. Meeting this requires that models bound actual anticipated conditions (e.g., tolerances and uncertainties appropriately taken into account, most reactive credible system parameters allowed are assumed), as specified in the license. Additional guidance is provided in the criticality chapter of NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility," (Sections 5.4.3.4.1, 5.4.3.4.2, and 5.4.3.4.4).

- Subcritical margin may also be expressed in terms of system parameters rather than system k_{eff}. An example would be where the licensee or applicant has committed to use mass or dimensional limits that are some specified fraction of the critical values of those parameters. In such cases, the approach used must be approved by the NRC.

- Subcriticality may be demonstrated on the basis of subcritical limits included in the license, U.S. Nuclear Regulatory Commission (NRC) endorsed American National Standards Institute (ANSI) standards, or other documents that have been approved or endorsed by NRC. Approval or endorsement by the NRC implies that the Agency has found these references to include an acceptable margin of subcriticality for safety.

- Industry handbooks of criticality data may also be used if widely accepted in the nuclear industry and if used in accordance with any limitations of that data. The NRC, however, reserves the right to evaluate the use of such handbooks on a case-by-case basis.

The requirement that preventive controls and measures be the primary means of protection against criticality is satisfied if engineered or administrative controls relied on to meet § 70.61(d) are designed to prevent occurrence of the critical excursion rather than mitigate its consequences. By stating that prevention should be the *primary* means of protection, it is recognized that there may be extraordinarily rare occasions when prevention alone is not sufficient to meet § 70.61(d). Such cases require convincing demonstration that there is no practicable way to meet § 70.61(d) with solely preventive measures.

Some examples where the § 70.61(d) requirement has not been met:

- A process in which the most reactive credible conditions have not been modeled and have not been shown to have k_{eff} less than the approved USL.

- A process in which subcriticality is based on criticality calculations, but the model is outside the area of applicability of the calculational method.

- A process for which there is an unanalyzed or unanticipated credible abnormal condition (e.g., unanticipated failure of an IROFS or unanticipated external event).

- A process for which there is a credible common-mode event that can result in the failure of all criticality controls such that it can lead to a critical configuration.

- A process in which the designated IROFS are not sufficient to limit the system to a subcritical configuration.

Relationship of 10 CFR 70.61(b) to 10 CFR 70.61(d)

Section 70.61(b) states ". . . the risk of each credible high consequence event must be limited. . . . Controls . . . shall be applied to the extent needed to reduce the likelihood of occurrence of the event so that . . . the event is highly unlikely . . . ."

Section 70.61(d) states ". . . the risk of nuclear criticality accidents must be limited by assuring that under normal and credible abnormal conditions, all nuclear processes are subcritical, *including an approved margin of subcriticality* . . . ."

As written, the rule language requires both provisions (i.e., § 70.61(b) and § 70.61(d)) be met, since § 70.61(d) states "In addition to complying with paragraphs (b) and (c) of this section . . . ." However, during the 10 CFR Part 70 rulemaking, regulated industry representatives met with NRC and submitted letters in which they expressed their desire that NRC not consider criticality accidents high consequence events and not associate quantitative likelihoods with double contingency. As discussed in the release notes issued with the 10 CFR Part 70 rulemaking, in response to industry arguments accidental criticality was explicitly removed from the high consequence (§ 70.61(b)) category and a separate performance requirement for criticality (§ 70.61(d)) was created. The staff felt that in so doing, both the industry's desires as well as the staff's needs would be met. Further, the staff felt that the § 70.61(d) requirement required the same information as that required by § 70.61(b). Saying all nuclear processes must be subcritical in § 70.61(d) implies that criticality events must be prevented. Moreover, since likelihood is never zero, some non-zero likelihood must be assumed; the highly unlikely requirement in § 70.61(b) is appropriate for this. Therefore, the staff felt that by removing criticality explicitly from § 70.61(b) and creating § 70.61(d) during the rulemaking, the staff still retained its desired outcome–to prevent criticality accidents from occurring. The final rule Statement of Considerations (SOC) stated that "...the NRC believes that a separate performance requirement for nuclear criticality prevention is appropriate. The staff recognizes that many (but not all) nuclear criticality accidents would reasonably be expected to result in worker doses that exceed the high- and intermediate-consequence standards in 10 CFR 70.61(b) or (c). However, regardless of the dose directly resulting from the accident, an inadvertent nuclear criticality should be avoided. This is consistent with the Commission's goal to prevent inadvertent criticalities, as reflected in the NRC Strategic Plan (NUREG-1614) . . . ." However, there remained ambiguity regarding the relationship between

§ 70.61(b) and § 70.61(d). While the staff's intent was to have a single performance requirement for criticality accidents, this cannot be substantiated by a literal examination of the final rule.

Comparing the language in § 70.61(b) and (d), one concludes that § 70.61(d) is actually more restrictive than § 70.61(b). Section 70.61(d) essentially requires that there be no criticality accidents, with a high degree of assurance. Section 70.61(b) essentially requires that deaths and injuries (as implemented through a dose limit) be precluded (i.e., be made to be highly unlikely). If criticality accidents are prevented, then deaths and injuries are also prevented. However, the converse is not necessarily true; if deaths and injuries are prevented, criticality accidents are not necessarily prevented. Therefore, if one meets § 70.61(d), then one also automatically meets § 70.61(b); and if one meets § 70.61(b) through preventive means, and also meets the additional requirements specified in § 70.61(d), then one also meets § 70.61(d) in full. Thus, if a licensee chooses to address criticality event sequences under 10 CFR 70.61(b) with a preventive strategy and has an approved margin of subcriticality for safety, then the licensee will have also met the requirements under 10 CFR 70.61(d). However, if the licensee chooses to address criticality event sequences under 10 CFR 70.61(b) with a mitigative strategy, then the licensee will <u>not</u> have met the requirements under 10 CFR 70.61(d) and additional controls will have to be identified to ensure subcriticality.

Another consideration is that both § 70.61(b) and § 70.61(d) set the standard that must be met (i.e., the performance requirements), but not the methodology. Methodology requirements are contained in § 70.62. One cannot look at § 70.61 in a vacuum. All other 10 CFR Part 70 provisions must also be met, including the § 70.62(c) provision that requires the integrated safety analysis (ISA) to include radiological hazards, facility hazards, potential accident sequences, and identification of IROFS as well as the assumptions and conditions under which the IROFS are relied upon to support compliance with § 70.61 performance requirements. It also requires that the ISA team include a person with experience in criticality safety. These requirements must be met regardless of whether the licensee attempts to meet the performance requirements starting from § 70.61(b) or § 70.61(d). The three options below can be seen to be equivalent when one considers that § 70.62 must also be met for all cases.

To meet the regulations and prevent criticalities, an applicant/licensee may use one of the three approaches below (in conjunction with other 10 CFR Part 70 requirements, including those in § 70.62):

1. Demonstrate compliance with § 70.61(d); or
2. Demonstrate compliance with § 70.61(b), considering only preventive controls and including an approved margin of subcriticality; or
3. Separately demonstrate compliance with both § 70.61(d) and § 70.61(b).

Use of any of the above three approaches will satisfy the regulations.

That both § 70.61(b) and § 70.61(d) apply to criticality is supported by NUREG-1520. NUREG-1520, Section 5.4.3.4.4, addresses meeting the requirements of § 70.61(d). In addition, there are several references to the requirement to make criticality highly unlikely.

Double Contingency Principle § 70.64(a)(9)

In addition to complying with the performance requirement in § 70.61, new facilities and processes are required to comply with the baseline design criteria in § 70.64. Section 70.64(a)(9) requires that the design provide for criticality control, including adherence to the double contingency principle (DCP). In addition to this requirement for new facilities and processes, many existing facilities and processes have license commitments to meet the DCP for licensed activities. Although Subpart H of 10 CFR Part 70 is relatively new, this conceptual framework is not new. Licensees have historically committed to ANSI/American Nuclear Society -8.1 (ANSI/ANS-8.1). This standard also requires that nuclear processes be ensured to be subcritical under normal and credible abnormal conditions. By contrast, the DCP is stated as a recommendation of ANSI/ANS-8.1. Therefore, the standard recognizes that adherence to the DCP can be one means, but is not necessarily the only means of meeting the underlying subcriticality requirement. The conditions under which compliance with the DCP ensures that § 70.61(d) is met are discussed below.

The double contingency principle is a design principle intended to be used in designing a facility that meets the performance requirements of § 70.61. The definition in § 70.4 ("...process designs *should* incorporate sufficient factors of safety...") implicitly recognizes that there may be some cases in which a strict adherence to the double contingency principle is not practicable. This should be an exceedingly rare situation and should be accompanied by a convincing demonstration that a strict adherence to the double contingency principle is not practicable. Section 70.64(a) allows for this in stating that licensees must maintain the application of this criterion unless the integrated safety analysis (ISA) demonstrates that it is not relied on for safety or otherwise does not require adherence.

The presence of two controls may not be necessary, or may not be sufficient, to meet the DCP. The DCP does not necessarily require two controls; it requires "at least two...changes in process conditions" be needed before criticality is possible. Meeting this may necessitate one, two, or more than two controls depending on the possible conditions that can lead to criticality. In general, there will be many pathways to criticality and, therefore, more than two controls required to meet the DCP for an entire process.

In addition, § 70.64(b)(1) requires that the design must incorporate, whenever practicable, preference for the selection of engineered over administrative controls to increase overall system reliability. Passive engineered controls are generally preferable to active engineered controls, and engineered to administrative controls. In addition, process design should rely on geometry control as opposed to control of other parameters whenever practicable, and on diverse means of control (e.g., reliance on two different criticality parameters or different means of controlling one parameter) whenever practicable, to minimize the potential for common-mode failure. Cases in which these preferences cannot be complied with will generally require more justification to show adherence with the DCP. For example, one cannot claim that the double contingency principle is met with only two controls (regardless of type) if the resulting configuration fails to protect against all credible pathways to criticality or limit the risk of inadvertent criticality as required in 10 CFR 70.61(d).

Relationship between § 70.61 and § 70.64(a)(9)

As stated above, adherence to the DCP can be one means of meeting the performance requirements of § 70.61(d) (and, therefore, also § 70.61(b)). Historically, a number of different approaches to double contingency have been used. Some cases that have been used in the past may not be sufficiently robust to satisfy the performance requirements of § 70.61. Typically, this has been due to a reliance on controls that were not sufficiently robust (e.g., weak administrative controls). The purpose of this guidance is not to promote a new standard for all applications but rather to clarify when adherence to the DCP will establish a sufficient basis for meeting the performance requirements. To facilitate this, the following guidance is provided on the various terms in the definition of the DCP:

Unlikely changes in process conditions should be expected to occur rarely, or not at all, during the lifetime of the facility. Operational events that occur regularly should not be credited as a contingency relied on to meet the DCP (although they may constitute part of a contingency if a combination of events may be considered unlikely). Therefore, the occurrence of any such event generally reveals a deficiency in the design that should result in corrective action. Determination that a contingency is unlikely should be based on objective attributes of the criticality controls, rather than on subjective judgment alone. Examples of such attributes are environmental factors that can degrade the reliability and availability of controls, margin, and redundancy and diversity of controls. (Guidance on some of the availability and reliability qualities that should be considered is provided in NUREG-1520, Section 3.4.3.2(9) and NUREG-1718, "Standard Review Plan for the Review of a License Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," Section 5.4.3.2(B)(vii).) Management measures must be provided, as needed, to ensure that the failure of the criticality controls is an unlikely contingency. (NOTE: Usage of the term "unlikely" in the DCP is not equivalent to the term as used in § 70.61(c) for intermediate consequence events.)

Independent changes in process conditions are such that one contingency neither causes another contingency nor increases its likelihood of occurrence. The existence of any credible common-mode failure of both contingencies means that it is not valid to consider them independent. For example, related actions performed by the same individual or using the same equipment will not generally be sufficiently independent to meet the DCP.

Concurrent does not mean that the two changes in process conditions must occur simultaneously, but that the effect of the first contingency persists until the second contingency occurs. Prompt detection and correction of abnormal conditions should thus be provided to restore double contingency protection. The time required to detect and correct failures should be significantly shorter than the anticipated time between failures in order for there to be significant risk reduction provided from failure detection.

Changes in process conditions does not imply that reliance on two different parameters is mandatory to meet the DCP. Reliance on two different parameters is preferable to reliance on two controls on a single parameter, however, because of the difficulty in achieving complete independence when controlling one parameter. In those cases in which single parameter control is unavoidable, great care should be taken to ensure that no common-mode failures exist.

In addition to meeting the above, the following guidance is provided to illustrate the conditions under which adherence to the double contingency principle (in terms of the guidance above) is sufficient to meet the performance requirement of 10 CFR 70.61:

- Controls are established on system parameters to preclude changes in process conditions, and these controls are designated as IROFS in accordance with § 70.61(e). (Reliance should be based on items that are designated as IROFS in the ISA Summary and not on random factors that may or may not be maintained.)

- The condition resulting from the failure of a leg of double contingency has been shown to be subcritical with an acceptable margin (e.g., k_{eff} is less than USL, parameters are within subcritical limits specified in the license or endorsed standards).

- Controls are sufficiently reliable to ensure that each change in process conditions necessary for criticality is "unlikely." Management measures are established to ensure that they are available and reliable to perform their safety function.

Because the DCP is only one means of meeting the performance requirements, it is possible to meet the DCP without meeting the conditions above (including designating criticality controls as IROFS in the ISA Summary). In this case, however, another method must be relied on to meet the § 70.61 performance requirements. However, in order to use compliance with the DCP as part of the demonstration of meeting the § 70.61 performance requirements, these conditions should be met.

Some specific examples of control systems that meet § 70.61(d) through use of the DCP follow:

A passive geometry control in which no credible failure mode (e.g., bulging, corrosion, or leakage) exists and which has been placed under configuration management:

- A favorable geometry vessel in a benign environment in which corrosion or other material degradation is not credible. In addition, the vessel is of such robust construction (e.g., thick stainless steel, steel surrounded by concrete) that it is unquestionably not going to leak, and there is no credible mechanism for the material to accumulate in an unfavorable configuration.

- A tank that is not authorized to contain fissile material is located far outside the fissile material handling areas and is physically isolated from fissile liquid processes by a blank flange or siphon break, such that backflow is not credible.

Two passive controls in which there is a credible failure mode, and there are sufficient management measures to ensure the controls continue to perform their safety functions (e.g., periodic surveillance to detect corrosion/bulging):

- A favorable geometry solution column, in which leakage of the tank is a credible upset. In addition, the column is in an area in which the solution would leak into a favorable geometry

dike, and the leakage would be self-revealing (i.e., column is in a continually manned area) or the column and dike would be subject to periodic surveillance.

- A double-sleeved solution line in which leakage of the inner pipe would be quickly detected (e.g., by conductivity probe between the pipes or by transparent baffling).

- A storage array in which fissile material is stored in fixed geometry containers, and the spacing between containers is fixed by birdcages or other fixed devices, and geometry and spacing controls are ensured by configuration management and periodic walkthroughs.

One passive control under configuration management and one active engineered control whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure:

- A calciner relying on geometry and moderation control in which geometry control is provided by limiting the calciner interior to the height of a single layer of pellet boats, and moderation control is provided by monitoring of the calciner temperature. Temperature control is ensured by thermocouples that alarm if the temperature drops below a minimum setpoint.

- A downblending tank that is subcritical for uranium solutions with less than a limiting enrichment in which volume control is provided by the design of the tank and enrichment control is provided using mass flow totalizers and a mechanical stirrer. The failure of these active devices automatically stops the transfer of solution and actuates an alarm.

- A large geometry tank relying on raschig rings for criticality control in which the raschig rings are only approved up to a limiting concentration, and the concentration is controlled by an in-line sodium iodide detector that closes an isolation valve when actuated.

One engineered and one enhanced administrative control in which the instrumentation and devices included in the administrative control are subject to periodic functional testing and maintenance, and the operator action is performed routinely or reinforced by periodic drills and training:

- A powder handling glovebox relying on moderator and mass control in which moderator control is provided by the glovebox design (e.g., airtight, dry nitrogen atmosphere, sloped ventilation ductwork) and mass is procedurally controlled by limiting batch size. In addition, mass transfers must be logged into a computer tracking system that alarms if mass limits are exceeded.

- A vessel in which the volume of fissile solution is controlled by the diameter of the tank and by procedurally limiting the solution height. In addition, operator actions are backed up with a high-level switch equipped with an alarm.

One engineered control and one simple administrative control in which the reliability of the administrative control is subject to a high degree of redundancy:

- Solution transfer from favorable to unfavorable geometry relying on two controls on concentration. Two different operators are required to draw separate samples which are then analyzed in the laboratory by two different methods and shown to be within concentration limits before transfer is authorized. In addition, the area supervisor maintains control of a key to the transfer pump so that the procedure may not be inadvertently bypassed. This is backed up with an in-line sodium iodide detector that automatically closes an isolation valve if concentration limits are exceeded.

  (NOTE: Use of two independent samples is generally not considered adequate for both legs of double contingency because of the difficulty in ensuring complete independence between the samples.)

Two administrative controls that are independent (e.g., performed by different individuals or verified by a supervisor), for which human factors have been considered in the design of the process such that the operation is not prone to error, and there is sufficient margin to require multiple failures before the criticality control limit can be exceeded:

- A glovebox relying on dual mass control in which two operators or an operator and a supervisor must confirm that placing material into the glovebox will not result in the mass limit being exceeded. In addition, criticality would require the mass limit to be exceeded multiple times, which would be difficult to achieve and would be readily apparent.

- A drum storage array limited to a vertical stack of four drums in which there are no forklifts in the area capable of raising a drum above this height. In addition, the drums are very heavy and violating the stack height limit would require an immense physical effort.

- A planar storage array in which mass-controlled containers are procedurally limited to not less than 24 inches center-to-center, and in which criticality would require assembling a very large number of containers into a spherical heap and reflecting them intimately with water.

Other considerations ensuring that there is no credible event leading to criticality:

- A facility handling uranium enriched to no more than 1 weight percent (wt%) uranium-235 (^{235}U).

- A facility in which the site-wide limit is less than a minimum critical mass.

- A facility storing contaminated soil or equipment with a very low uranium concentration in which there is no known concentration mechanism that can lead to a critical configuration.

Some examples of control systems that would not meet § 70.61(d) through use of the DCP:

Double contingency consisting of two single operator actions without any supervisor verification or redundancy:

- Solution transfers that rely only on two operators drawing separate samples or in which a single procedural deviation could cause an unauthorized transfer.

- A mass controlled system in which triple batching (i.e., two successive batching errors) could result in criticality when the mass transfers are done by a single operator.

- A storage array in which two violations on administrative spacing requirements could credibly lead to criticality.

A leg of double contingency consisting of an administrative control for which correct performance of the action cannot be readily confirmed or is subjective:

- A solution vessel in which the operator is required to confirm concentration or chemical form by visually observing a color change in the solution.

- A tank in which the operator is required to verify prior to operation that the tank is "essentially empty."

A leg of double contingency consisting of complex administrative tasks composed of multiple steps that are susceptible to error:

- A glovebox in which the operator is required to calculate the mass of plastic, paper, and other miscellaneous materials in order to comply with moderator control.

- A solution transfer operation in which one leg consists solely on a single sample being correctly drawn, labeled, analyzed, recorded, and read.

- Maintenance on a dissolution process in which criticality safety relies on the correct performance of a procedure to replace an in-line filter. The procedure requires that the filter be removed, flushed, and re-installed in a multi-step process that has several opportunities for failure.

A leg of double contingency consisting of an administrative control with insufficient margin to ensure that the safety limit will not be exceeded:

- A glovebox in which mass is controlled administratively, and in which the normal mass limit is almost equal to the minimum critical mass.

- A planar storage array in which spacing between containers is administratively limited to be less than 24 inches center-to-center, and in which criticality will result if a few containers are placed 23 inches apart.

A leg of double contingency consisting of an engineered control in which there is no reasonable means to detect and correct the failure within a given time.

- A solution process in which it is plausible for concentrated solution to be allowed to accumulate undetected over a long period of time in an unfavorable geometry.

- A vessel in which geometry control is provided by a double wall, but there is no means of detecting leakage between the walls. In addition, the vessel is of a type known to have a history of leakage (e.g., heat exchanger).

A leg of double contingency consisting of a control in an environment where its safety function is degraded.

- A solution vessel relied on for geometry control, but which is subject to pressure fluctuations that can cause the vessel to bulge beyond a favorable diameter.

- Instrumentation whose performance is degraded under conditions that can be reasonably expected during normal operations (e.g., temperature, pressure, presence of corrosive gases, or loss of essential utilities such as electricity, plant air, or water).

A leg of double contingency consisting of a control where its behavior under adverse conditions is uncertain.

- An unfavorable geometry pump in which mass control relies on the presumption that the pump will malfunction before an unsafe volume of uranium accumulates in the pump oil, and for which no failures of this type have been observed.

A leg of double contingency consisting of undeclared design features or process conditions that are not precluded by being explicitly controlled.

- A powder blending operation in which uranium oxide density that is less than the theoretical density is assumed, but the process variables affecting density (e.g., calcinations temperature, mechanical pressure of the pellet press) are not specifically controlled and there is no confirmatory sampling.

- A solvent extraction process in which nominal concentration of uranyl nitrate is assumed, but there is no in-line monitoring or confirmatory sampling.

- A vault in which the mass limit is not controlled by procedure or license limit, but is merely based on current inventory.

- A process relying on the favorable geometry of passive equipment, but for which the dimensions and/or material composition are not specifically identified as criticality controls.

This list is merely illustrative and not meant to be exhaustive. However, these examples demonstrate that double contingency that satisfies the performance requirements can be based on one, two, or more than two passive engineered, active engineered, or administrative controls, and that reliability and availability of those controls depends on management measures, safety margins, environmental conditions, human factors, and other process and control characteristics. Not every application similar to these examples will be found acceptable—determination must be made on the totality of the information available, and an analyst should consider all factors that may degrade the robustness of the controls.

Regulatory Basis: 10 CFR 70.64(a)(9), 10 CFR 70.61(b), and 10 CFR 70.61(d)

Technical Review Guidance

Relationship of 10 CFR 70.61(b) and 10 CFR 70.61(d)

The reviewer needs to assure that all applicable 10 CFR Part 70 criticality provisions (including § 70.62(c)) are met. To meet the regulations and prevent criticalities an applicant/licensee may use one of the three approaches below (in conjunction with other 10 CFR Part 70 requirements, including those in § 70.62):

1. Demonstrate compliance with § 70.61(d); or
1. Demonstrate compliance with § 70.61(b), considering only preventive controls and including an approved margin of subcriticality; or
2. Separately demonstrate compliance with both § 70.61(d) and § 70.61(b).

Use of any of the above three approaches will satisfy the regulations.

Staff should not dictate which of the above three options must be met; rather, staff should assure that the applicant/licensee has met one of these options.

Double Contingency Principle

One way, but not the only way, of meeting 10 CFR 70.61 is by applying the double contingency principle (defined in 10 CFR 70.4) to accident sequences leading to criticality that are required to be developed per § 70.62. Adherence to the DCP will satisfy the performance requirement of § 70.61(d) (and therefore also § 70.61(b)) provided the following conditions are met:

- Controls are established on system parameters to preclude changes in process conditions, and these controls are designated as IROFS in accordance with § 70.61(e). (Reliance should be based on items that are designated as IROFS in the ISA Summary and not on random factors that may or may not be maintained.)

- The condition resulting from the failure of a leg of double contingency has been shown to be subcritical with an acceptable margin (e.g., k_{eff} is less than USL, parameters are within subcritical limits specified in the license or endorsed standards).

- Controls are sufficiently reliable to ensure that each change in process conditions necessary for criticality is "unlikely." Management measures are established to ensure that they are available and reliable to perform their safety function.

In the absence of meeting these conditions, an alternate demonstration of compliance with the performance requirements should be provided.

Recommendations

This guidance should be used to supplement Chapter 5, "Nuclear Criticality Safety," of NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility" and Chapter 6, "Nuclear Criticality Safety," of NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility".

References

U.S. Code of Federal Regulations, *Title 10, Energy,* Part 70, "Domestic Licensing of Special Nuclear Material."

U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility." NRC: Washington, D.C. March 2002.

U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility." NRC: Washington, D.C. August 2000.

Approved: /RA/ Date: 02/17/2005
Director, Division of Fuel Cycle Safety
and Safeguards, NMSS

February 17, 2005