Division of Fuel Cycle Safety and Safeguards
Interim Staff Guidance - 01

Methods for Qualitative Evaluation of Likelihood

Issue:

Use of a method for qualitative evaluation of likelihood in the context of a review of a license application or amendment request under 10 CFR Part 70, Subpart H.

Introduction:

The purpose of this document is to provide guidance to the NRC staff for the qualitative evaluation of likelihood during review of a license application or amendment request under 10 CFR Part 70, Subpart H. An illustrative example of one acceptable method of evaluating the likelihood of one type of accident sequence is presented in subsequent sections. Note that this guidance is limited to an evaluation of sequences in which the overall likelihood can be expressed solely in terms of systems of preventive IROFS, and does not discuss situations in which credit is taken for the initiating event frequency, but instead assumes the initiating event occurs. Credit for initiating event frequency will be considered in a separate guidance document. Although this method would be acceptable for use by an applicant in performing an Integrated Safety Analysis (ISA), this guidance is intended for use by the staff in performing vertical- and horizontal-slice reviews of specific processes.

The vertical-slice review of a particular process should find that the process complies with the performance requirements (including likelihood) of 10 CFR 70.61, but the more important goal of the vertical-slice review is to verify the adequacy of the applicant's ISA process. NUREG-1520, Section 3.6, states that the reviewer should make a general finding as to whether the items relied on for safety (IROFS), management measures, and programmatic commitments will, if properly implemented, meet the performance requirements of 10 CFR 70.61. In order to support this overall finding, the reviewer should make evaluations with regard to each of these three elements. There are certain reliability and availability qualities of controls and systems of controls that make accidents unlikely or highly unlikely. This guidance provides an example of one method for determining whether the reliability and availability qualities of the controls in a particular process are adequate to support compliance with the likelihood requirements in 10 CFR 70.61(b) and (c). This evaluation method relies on qualitative characteristics of systems of IROFS, rather than partly quantitative methods such as the index method used in Appendix A to Chapter 3 of NUREG-1520.

Note that it is difficult for any qualitative likelihood determination method to be comprehensive in that it is difficult to cover all possible situations. The method presented herein should thus be viewed as a rough screening method–that is, a guide to the kind of thorough process that should be employed. The crucial role of expert judgement in the final determination of likelihood thus cannot be overstated.

Discussion:

10 CFR 70.61 requires that all events that can result in high consequences be shown to be highly unlikely, and those that can result in intermediate consequences be unlikely. Likelihood

determination may be based on either quantitative or qualitative methods. This document provides guidance on an acceptable qualitative method for determining likelihood.

A quantitative evaluation method is one that seeks to assign a numerical frequency to the accident sequence as a whole, based on objective failure data. By contrast, a qualitative evaluation method relies on the application of objective criteria to categorize the accident sequence into one of a number of qualitative likelihood categories. The index method as described in Appendix A of NUREG-1520 lies between these two approaches in that it categorizes the failure likelihood of individual IROFS based on qualitative criteria, but then combines individual likelihood indices mathematically into an overall accident sequence likelihood index. It should be recognized that there is an implicit relationship between these various approaches in that they merely provide different descriptions of the same attribute (e.g., an index of -1 is roughly analogous to a likelihood on the order of 10^{-1}/yr). All of these approaches are valid and all have some degree of subjectivity; none of these approaches is preferred by the staff.

A qualitative evaluation method should rely on a qualitative assessment of the reliability and availability characteristics of IROFS or systems of IROFS relied on to prevent or mitigate a particular event. In this document, the terms “controls” and “IROFS” are synonymous. The likelihood of any particular accident sequence relies on the totality of the system of IROFS. The evaluation against the 10 CFR 70.61 likelihood requirements should thus consider the entire set of IROFS, and should only consider IROFS. As stated in 10 CFR 70.62(d), the likelihood under 10 CFR 70.61 must be supported by a “management measures” program. These management measures are needed to ensure the reliability and availability of the system of IROFS. Thus, a judgement of compliance must consider the applicant’s programs and management measures in addition to the individual characteristics of a given process.

The guidance in this document applies to an evaluation of the key reliability and availability qualities of an IROFS or system of IROFS. If these characteristics meet certain qualitative criteria, the IROFS or system of IROFS can be presumed capable of making the accident sequences highly unlikely. As stated in NUREG-1520, Section 3.4.3.2(9), the key reliability and availability qualities of **individual** IROFS include:

1) The safety margin in the controlled parameter, compared to process variation and uncertainties
2) The type of control (e.g., passive and active engineered, administrative)
3) Type and grading of management measures (e.g., surveillance, training)
4) Detection of failure (e.g., fail-safe, self-announcing, or subject to periodic surveillance)

The key reliability and availability qualities of **systems** of IROFS include:

1) Defense-in-depth
2) Redundancy
3) Independence

It is assumed here that adequate management measures are applied to IROFS–that is, it is assumed that the IROFS are supported by configuration management, training, procedures,

maintenance, etc., as needed. The reviewer should look at both the applicant's programs and practices for management measures and the specific application of management measures in the system being evaluated.

The method described below categorizes accident sequences based on the characteristics of redundancy, independence, safety margin, and reliability and availability of individual controls. For a determination of highly unlikely, the sequence must be put into the category of "highly unlikely" or "not highly unlikely." The actual determination of whether a given system of IROFS makes a high-consequence event "highly unlikely" should be left to the individual reviewer, based on a consideration of the total relevant information available on the specific system. The applicant must ensure that the sequence remains highly unlikely in its future performance.

Regulatory Basis: 10 CFR 70.61(b), (c), (d), and (e); 10 CFR 70.62(c)(v)

METHOD (Technical Review Guidance)
This section describes a step-by-step procedure for determining in which likelihood category a particular system of IROFS belongs. The first step is to determine whether the whole spectrum of accident sequences have been considered in performance of the ISA.

Completeness

Before attempting to evaluate individual accident sequences to determine their likelihood, the reviewer should evaluate whether the list of accident sequences is complete. There are several formal methods that have historically been used to identify potential accident sequences (e.g., What If, HazOp, Failure Modes and Effects Analysis (FMEA), Event Tree, Fault Tree). Systematic methods suitable to the process being considered should be employed, consistent with industry guidelines and considering the nature and complexity of the operations. Not all methods may be suitable in all applications. The SRP has guidance for this review. At this point, a Request for Additional Information (RAI) may be submitted.

Consequences

The consequences of the accident need to be evaluated in terms of the radiological dose or chemical exposure, to determine whether the event must be "highly unlikely" or "unlikely" in accordance with 10 CFR 70.61(b) or (c). For radiological events, conservative assumptions should be made with regard to time, distance, and shielding. It is noted that distance to the receptor can have a large effect on the consequence. In particular, criticality events will generally be categorized as high-consequence events. For chemical events, standard industry exposure limits (such as Emergency Response Planning Guidelines (ERPGs) and Acute Exposure Guideline Levels (AEGLs)) should be employed. In general, chemical events that could result in ERPG-3 exposures will be categorized as high-consequence events.

> Note: Controls used in assumptions of initial conditions in consequence calculations such as geometry, fire loadings, or fire wall ratings may be IROFS.

Accident Sequence Categories

Once the consequences (and thus required likelihood) have been determined, the reviewer should look at the overall accident sequence. Four different categories of accident sequences are provided in the list below. In this approach, a system of IROFS belonging to one of the categories generally has the potential to make the sequence "highly unlikely."

> Note: For the purpose of this method, the "event" is the failure of the IROFS and not the *initiating event*. The likelihood of initiating events is part of another discussion.

Criticality Accident Sequences

Criticality accident sequences must also meet 70.61(d) and, for new processes and facilities, the double contingency principle in 70.64(a)(9). Guidance on how to meet these requirements will be contained in a separate guidance document.

Category 1. Highly reliable and available multiple, independent controls.
Category 2. Single failure with very large safety margin
Category 3. Single rare event with backup administrative control
Category 4. More than two redundant controls

Guidance for identifying the category in which a given system of IROFS belongs is given below, along with illustrative examples:

(1) Highly reliable and available multiple, independent and diverse controls

Systems of IROFS belonging to this category typically consist of two or more IROFS that have to fail before the accident can occur. These IROFS should be diverse (i.e., perform different safety functions, such as controlling two different parameters or one parameter two different ways) in order to minimize the potential for common-mode failure. A sample procedure for assigning a likelihood to this event is provided below:

(a) First identify whether the IROFS are sufficiently reliable and available, considering all relevant reliability and availability qualities. If not, then this event does not belong to Category 1 as defined above.

(b) Determine whether the controlled parameters are independent. If any single event can cause all parameters to exceed safe values, then the parameters are not independent.

(c) If the parameters are not independent, determine whether the IROFS are diverse. If the IROFS function in the same manner (i.e., they can fail by the same failure modes), then they are not diverse. The reviewer should then determine whether these diverse IROFS are independent; diverse IROFS generally provide greater assurance of independence. If any single event can cause all IROFS to fail, then the IROFS are not independent.

If the IROFS are sufficiently available and reliable, and the controlled parameters are independent, or the controls are independent and diverse (i.e., meet (a) and either (b) or (c) above), then this sequence belongs to Category 1.

Examples of systems falling under Category 1 include:

Independent parameters

- Independent passive engineered geometry and neutron absorber controls in a solution processing system.
- Geometry controls combined with process limits on chemical form (acidity or temperature) in a uranium-recovery process.

Single parameter with diverse controls

- Confinement composed of primary containment (such as a glovebox), a high efficiency particulate air (HEPA) filters, and a scrubber.

(2) Single failure with very large safety margin

Since there is only one IROFS failure in such cases, it must be made highly unlikely. Cases in which there is clearly a very large safety margin should be regarded as presumptively "highly unlikely."

One example of this kind of event would be a very robust passive structure in which there is a large *safety factor* in those parameters that relate to the safety function of the structure (e.g., structural strength, including resistance to external events). Massive rupture of strong vessels or pipes may qualify as highly unlikely, whereas simple leakage would not.

Often, use of very large safety margins make accidents highly unlikely by a combination of an administrative control, a very sound human factors design, and a *process parameter margin* so large that even failure to comply with the formal control is very unlikely to lead to an accident. A common example is administrative control of material additions to a process. If the amount normally added is much less than an amount that could produce an accident, such an addition might be considered highly unlikely. Addition of unsafe amounts should be made unlikely even with an untrained operator. Large margins to criticality are used such that the system will remain subcritical even under double batching.

Examples of systems falling under Category 2 include:

- Mass control in a powder handling area, in which normal mass limits are much less than the minimum critical mass.

- Concentration control for a waste-water treatment facility, in which release limits are much less than the infinite medium critical concentration.

(3) Single rare event with backup control

This situation differs from the use of multiple highly reliable controls (Category 1) in that only one of the controls may be considered highly reliable. Thus, there is primary reliance on the rarity of a single event. The backup control (which is frequently

administrative) usually cannot be considered to be very reliable, but may still be necessary to make the accident sequence highly unlikely. The review of likelihood should focus on whether the rarity of the single event can be justified.

Examples of systems falling under Category 3 include:

- Restrictions on the use of water in manual firefighting, in the event of a large fire in a uranium powder processing facility.

- A requirement to valve out gas lines to a furnace in the event of an earthquake.

(4) Multiple (more than two) independent and redundant controls

If a system of IROFS is redundant (i.e., perform the same safety function, such as maintaining a single parameter within a given range), but does not have at least two highly reliable controls, it may still make occurrence of the sequence highly unlikely by providing additional controls. These multiple controls should be independent in order to ensure that the full benefit of multiple layers of protection is realized. Systems of IROFS belonging to this category are distinguished from those in Category 1 by the fact that more than two controls are required to either: (1) provide the necessary accident sequence likelihood; or (2) provide greater assurance that there is no common-mode failure. This typically occurs when individual controls are less reliable than those needed for Category 1, or non-diverse means of control are employed.

Examples of systems falling under Category 4 include:

- Multiple supervisor overchecks of administrative actions on a fissile material transfer operation.

- Dual independent sampling credited as one leg of double contingency.

- Confinement composed of multiple identical ventilation zones with HEPA filters.

IROFS Reliability

Once the accident sequence has been categorized, and a preliminary assessment of likelihood has been made, it is necessary to evaluate whether the controls are, in fact, sufficiently reliable and available to make the sequence “highly unlikely.”

Each of the combinations of qualitative control categories and surveillance categories listed below may be regarded initially as sufficiently reliable to meet the likelihood requirements, subject to the final likelihood determination discussed below. The types of controls and surveillance categories are addressed in the sections below.

Table 1. Control and Surveillance Categories

Control Category	Surveillance Category
Robust passive controls	Biannual or better (i.e., twice/yr)
Less robust passive controls	Monthly or better
Continuously active controls	Weekly or better
Standby automatic controls	Weekly or better
Administrative controls (see Note 1)	(see Note 2)

Many controls are either fail-safe or fail-evident. Such controls may not need formal surveillance at planned intervals, although operators may need procedures and training in rendering the system safe if failure does occur.

NOTE 1: Administrative controls that are used routinely and have reliable hardware, trained operators, and written procedures may be considered reliable controls. This may require multiple measurements and overchecks.

NOTE 2: Failure of the administrative control discussed here occurs when the controlled parameter exceeds its safety limit, not when the administrative (operating) limit is exceeded. Often the existence of an administrative control means that operators are routinely present during operations. This makes it likely that the surveillance situation is failure-evident, which is generally sufficient. The need for formal surveillance therefore arises when the result of the failure would be hidden.

Examples of controls in each category in Table 1 above are provided below:

Robust Passive Controls: Strong passive structures (e.g., critically safe fluid-retention dikes, columns, and tanks; welded thick piping; short piping; glued piping).

Less Robust Passive Controls: Drain or overflow orifices or tubes, filters, thin piping, large arrays of piping, screwed piping.

Continuously Active Controls: Fan, pump, stirrer, heater, and active coolers.

Standby Automatic Controls: Interlocks, switches, active detectors.

Standby automatic controls are generally characterized by having multiple active components, such as detection, logic, transmission, and actuation circuits. In addition, they must normally rely on utilities such as electric power, air, or hydraulics. Failure of the power source is one way such a system can fail. A key consideration in enhancing the reliability of such systems is to design them to be fail-safe or failure-evident on loss of essential utilities.

Administrative Controls: Any control that relies on human action, or restraint from action, is an administrative control. Such controls often involve the use of hardware (e.g., active devices and moving machinery) to function. Thus, an administrative control

can always fail as the result of human error and may be capable of failing as the result of hardware malfunction.

Enhanced Administrative Controls: Active monitoring of a parameter along with an alarm, to which an operator will respond is often referred to as an "enhanced" or "augmented administrative control."

Surveillance Categories:

Fail-safe

Fail-safe means that either: (1) the control always fails into a safe condition; or (2) when the control enters a failed state, action occurs immediately to render the system safe. Active controls should be designed to be fail-safe. For the control to be fail-safe, all components of the system must be fail-safe with respect to all mechanisms of failure.

Failure-evident

Leaks and structural failures of passive controls that are normally in the view of operators are examples of self-evident failures. Another category is active monitoring of a parameter along with an alarm, to which an operator will respond (i.e., an enhanced administrative control).

Weekly (or monthly) or better surveillance

For the remaining categories, the failure of controls is neither self-evident nor alarmed, and so there must be formal surveillance. The unsafe condition resulting from failure must also be capable of being rendered safe within a short period of time relative to the surveillance period (e.g., weekly surveillance should generally result in repair within a few hours, whereas monthly surveillance should generally result in repair within a couple days).

At least biannual (twice/yr) surveillance

This type of surveillance may be satisfied by a safety staff or configuration control staff audit to verify that the installed control or structure is still functional and conditions are still safe.

Final Assessment of Likelihood

The final assessment of likelihood should be done by considering all the available information about the reliability of the system of IROFS. A preliminary assessment may be done based on the type of accident sequence, and then the type and quality of controls, surveillance, duration of failure, and the effect of other management measures should be considered.

Additional Considerations

Some additional considerations that should be taken into account in assessing likelihood are presented below:

Independence: Independent parameters or controls are those in which no credible single event can cause the failure of both parameters or controls to produce an accident. Typically, for parameters this means that if either of two parameters is kept within its safety limits, the accident cannot occur even with all other parameters in their most hazardous states.

An example of two parameters that are difficult to make independent are pressure and temperature. Generally, an event that introduces energy into the system will cause both pressure and temperature to increase. When independent parameters are used, it is relatively easy to construct a set of two independent controls simply by establishing separate controls on each of the two parameters. Administrative controls are generally difficult to make completely independent due to reliance on common individuals and/or hardware.

It should be recognized that what is meant by an administrative control is often a whole set of hardware items, procedural tasks, and prohibitions applied to ensure a controlled parameter does not exceed its safety limit. Such administrative controls may include multiple human actions, redundant measurements, or supervisor overchecks in order to achieve a certain level of reliability. Use of independent parameters has the virtue that it is easier to eliminate single actions or mistakes that could cause both parameters to exceed their safety limits than when using a single parameter.

Any of the following events or conditions that could lead to both controls being disabled at the same time would make the controls not independent:

1) The two controls share a common hardware component, whose failure would disable both.

2) Loss of a utility function (e.g., electricity, compressed air, hydraulic pressure, heating, cooling, humidity control)

3) Failure of support structures, surrounding structures, or dropping of large items

4) Credible actions of workers (e.g., vehicle collision, forklift accidents, maintenance actions)

5) Violent internal events (e.g., explosions, fires, ruptures)

6) External events (e.g., aircraft crashes, earthquakes, windstorms, floods, natural fires)

7) Common environmental conditions (e.g., unusual heat, cold, rainfall, snow, ice, humidity, vibration, corrosive atmosphere, unusual conditions in a process fluid or material that is being controlled)

8) Common-cause failure from a common source of plugging material in the process fluid (e.g., plugging of supposedly redundant overflow lines, drain orifices, and filters)

9) Other common-cause failures that could negate otherwise independent controls (e.g., adverse chemistry, temperature, flow, or other conditions in processed fluids or materials)

> Note: The performance requirements of 10 CFR 70.61 do not require strict independence of controls. However, independence is highly desirable due to the amount of risk reduction it affords. Moreover, this is a requirement for criticality scenarios covered under 10 CFR 70.64.

If controls are not independent (as discussed above), then the likelihood methodology must accommodate this (i.e., it must contain an allowance for common-cause failure).

Safety Margin: By safety margin, we mean the quantitative difference between the value of a parameter that is likely to be encountered during normal or credible abnormal conditions and the value of that parameter that would cause a controlled parameter to reach a value at which an accident is possible.

Mitigative IROFS: Examples of Mitigative IROFS include fire detection or suppression equipment and shielding, which do not prevent the accident, but may reduce the consequences. High consequence events are to be highly unlikely, or the consequences must be less severe than those discussed in 10CFR70.61(b)(1)-(4). Intermediate consequence events are to be unlikely, or the consequences must be less severe than those discussed in 10CFR70.61(c)(1)-(4).

IROFS Boundaries: Evaluate all of the necessary attendant instrumentation, controls, normal or emergency power, cooling and seal water, lubrication, and auxiliary equipment required by the IROFS to perform its specific safety function. The basis for establishing the boundaries for IROFS is taken from the definition of *operable/operability* used for power reactors.

Industry Experience: When using industry experience to determine the reliability of controls, consider the source of the data. Give more weight to process industry, nuclear industry, or facility-specific data than generic manufacturers' data. Application-specific factors (e.g., operating environment, demand frequency, and impact of management measures) can either increase or decrease control reliability and should be considered. Give less weight to other statements, such as "...no documented failures..."

Sole IROFS: An item relied on for safety that is the sole item preventing or mitigating an accident sequence that exceeds the performance requirements of 10CFR70.61.

Quality Assurance Elements: Certain management measures such as Maintenance, Procedures, Training and Qualifications, and Records are quality assurance elements. Documentation of surveillance and test activities required to ensure that the IROFS remain operable and available are QA records.

Uncertainties: Uncertainties include variations in a process parameter as well as an instrument's ability to detect variations. This may affect the performance of an IROFS in a number of ways. See "Safety Margin" above, which refers only to process parameters.

- Key Types of Processes and Controls to Review

As stated in Chapter 3 of NUREG-1520, findings concerning the compliance of the overall safety program should be based on review of several elements, including: programs and methods, the ISA summary, and a more detailed review (vertical slice) for a selected set of individual processes. The Standard Review Plan contains guidance on the selection of processes for this detailed review. Listed below are some types of processes with the potential for high risk. The risk importance should be one factor considered in selecting those processes for which a detailed review will be done.

1) Transfers from favorable to unfavorable geometry (fluids, powders, or solids)

2) Fissile solution systems

3) Systems possessing only administrative controls, without large safety margins.

4) Systems containing unusually toxic, flammable, explosive, or otherwise hazardous chemicals.

5) Systems with chemical reactions that are potentially highly exothermic.

6) Systems in which hazardous interactions between chemicals that may be present can occur.

- Recommendation:

This guidance should be used to supplement Chapter 3, Integrated Safety Analysis (ISA) and ISA Summary, and Appendix A, Example Procedure for Accident Sequence Evaluation, of NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility."

- References:

U.S. Code of Federal Regulations, Title 10, Part 70, "Domestic Licensing of Special Nuclear Material," U.S. Government Printing Office, Washington, D.C.

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

Approved:_____Date:_____
DIRECTOR, NMSS/FCSS