Definitions to be added to the Glossary:

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

The only credible mechanism by which these features could be altered is through a formal design change performed under a configuration control program. Design features are subject to change control under configuration management, and are documented in the ISA.

Typical examples of Design Features include:

- Most installation dimensions, e.g., spacing between favorable-geometry tanks that prevents significant neutron interaction.
- Open-top cylindrical vessels whose outside diameter falls within the favorable-geometry requirement.
- A funnel break or break-tank between process vessels that protects against backflow, when it is designed so there exists no credible physical mechanism to force fluid in reverse through it, or to plug the atmospheric discontinuity in such a way as to allow backflow.

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

- License conditions or commitments, e.g. max 5% enrichment, max quantity of fissile material, site boundary, type of process and technology
- Physical Laws, e.g. the maximum density of water is 1 g/cc and occurs at 4º C.
- Material properties, e.g The maximum density of UOx pellets is 10.96 g/cc
- Full flooding of a vessel located above the second story of a building is not credible.
- Physical Location, e.g. elevation

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

- A facility process that is only operated on a 5-day a week two shifts a day.
- Internal building conditions such as lighting, noise level, escape routes, temperature, relative humidity, and maintenance of negative atmospheric pressure.
- Chemical state of as-received materials from suppliers, such as concentration and purity.

- The maximum temperature of a process effluent.
- The maximum design pressure of process vessel.
- Fluid pressure limits on atmospheric tanks established by maximum fluid depth and density.
- Fluid capacity limits established by tank size.
- Throughput limits established by equipment size.
- Equipment size, characteristics, and location, such as tank size and shape, pipe size and routing, pump capacity, fan capacity, filter configuration, enclosure integrity, fail-safe design, and roof integrity.

Consider adding changes to pg 3-24 and 3-25.
The above acceptance criteria are explained in greater detail below.

a. The primary function of the list describing each IROFS is to document the safety basis of all processes in the facility. This list assists in ensuring that the items (IROFS) are not degraded without a justifying safety review. Thus, the key feature of this list is that it includes all IROFS. To be acceptable, no item, control, or control system of a process that is needed to show compliance with the safety performance requirements of the regulation may be omitted from this list (see 10 CFR 70.61(e)). However, sets of hardware or procedures that perform the same safety function may be referred to as a single set of IROFS and do not need to be individually identified. The list of IROFS may erroneously be incomplete in a number of ways: (1) an ineffective method of identifying accident sequences may have been used, (2) in applying the method to identify accidents something was overlooked, (3) a whole area or process subject to accidents was improperly screened out or simply omitted from the ISA, (4) IROFS were not applied to an identified accident, or (5) the list of accidents was incomplete because of incompleteness in the process design itself. The reviewer should attempt, in the horizontal slice review, to determine if any of these errors has occurred.

b. IROFS may be composed of structures, systems, equipment, components or actions of personnel with a dedicated safety function. Structures, equipment and components with a property that is relied on for safety, if the credited safety function of these attributes can credibly fail during service must be designated as an IROFS. It is important in these cases to identify the critical safety characteristic(s) of the IROFS. The ISA Summary need not provide a breakdown of structures, systems, and equipment IROFS by component or identify all support systems. However, the ISA documentation maintained on site, such as system schematics and/or descriptive lists, should contain sufficient detail about items within a structure, system, or equipment IROFS, that it is clear to the reviewer and the applicant what structure, system, equipment, or component is included within the IROFS' boundary and would, therefore, be subject to management measures specified by the applicant. Some examples of items within a structure, system or equipment IROFS boundary are detectors, sensors, electronics, cables, valves, piping, tanks, and dikes. In addition, ISA documentation should also identify essential utilities and support systems on which the IROFS depends to perform its intended function. Some

examples of these are backup batteries, air supply, and steam supply. In some processes, the frequency of demands made on IROFS must be controlled or limited to comply with 10 CFR 70.61. In such processes, whatever features are needed to limit the frequency of demands are themselves IROFS.

Acceptance Criteria for the Definition of "Credible"

The regulation in 10 CFR 70.65 requires that the applicant define the term "credible." This term is used in 10 CFR 70.61, which requires that all credible accident sequences for which the consequences could exceed the performance requirements of 10 CFR 70.61 must be controlled to be unlikely or highly unlikely, as appropriate. If an event is not credible, IROFS are not required to prevent or mitigate the event. Thus, to be "not credible" could be used as a criterion for exemption from use of IROFS. This raises a danger of circular reasoning. In the safety program embodied in Subpart H to 10 CFR Part 70, the "not credible" nature of an event must not depend on any IROFS, i.e. any facility feature that could credibly fail to function or be rendered ineffective as a result of a change to the system other than being deliberately removed or altered. Each facility feature that can credibly fail, deliberate removal or alteration excepted, and that is needed to ensure that accident events are sufficiently unlikely is an IROFS. Management measures must offer high assurance, that such features are not removed or rendered ineffective during system changes. Also, one cannot claim that a process does not need IROFS because an accident sequence is "not credible" due to characteristics provided by some other controls or features of the plant that can credibly fail, that are not IROFS. Such an evaluation would be inconsistent with 10 CFR 70.61. However, although an accident sequence may not meet a definition of "not credible," it may meet the standards for "highly unlikely" or "unlikely" because of an infrequent external or internal initiating event, without the use of IROFS. In such a cases, IROFS are not necessary, but information is needed to show that the initiating event (deviation) does qualify as "highly unlikely" or "unlikely."

Any one of the following three independent acceptable sets of qualities could define an event as not credible:

(1) An external event has a frequency of occurrence that can conservatively be estimated as less than once in a million years.

(2) A process deviation consists of a sequence of many unlikely upsets, including human actions or errors for which there is no reason or motive. In determining that there is no reason for such errors, a wide range of possible motives, short of intent to cause harm, must be considered. Complete ignorance of safe procedures is possible for untrained personnel, which should be considered a credible possibility.
Obviously, no sequence of events should be categorized as not credible if it has actually occurred in any fuel cycle facility.

3) A convincing argument exists that, given physical laws, process deviations are not possible, or initiation of the accident sequence is extremely unlikely. The validity of the argument must not depend on any feature controlled by the facility's system of IROFS. Such a demonstration of "not credible" must be convincing despite the absence of designated IROFS.

Such a demonstration of "not credible" must be convincing despite the absence of designated IROFS. Typically, this can be achieved only for external events known to be extremely unlikely or passive aspects of facility design that have extremely unlikely failure frequencies short of being deliberately removed or altered (i.e. failure of configuration control practices).

Acceptance Criteria for Qualitative Definitions of Likelihood If the applicant's definitions are qualitative, they are acceptable if they meet all of the following criteria:

- They are reasonably clear and based on objective criteria.
- They can reasonably be expected to consistently distinguish accidents that are "highly unlikely" from those that are merely "unlikely."
- Their categorization of events as "highly unlikely" or "unlikely" yields results reasonably consistent with quantitative information and quantitative criteria such as those given in the example here.

The phrase "objective criteria" means the extent to which the method relies on specific identifiable characteristics of a process design, rather than subjective judgments of adequacy. Objective criteria are needed to achieve consistency. "Consistency" means the degree to which different analysts obtain the same results when they apply the method. This is important in maintaining an adequate standard of safety because the ISAs of future facility modifications may be performed by individuals not involved in conducting the initial ISA. An acceptable qualitative method of likelihood evaluation should yield results comparable to the examples of evaluation methods given in the appendices to this chapter.