

Industry October 14, 2010 – Markup of system scope discussion to address NRC writeup (comments previously provided to NRC indicated by user “CBC”, Oct 14<sup>th</sup> industry comments on October 14<sup>th</sup> indicated by user “Ind 1014”)

### 3.2.7 Event or Condition That Could Have Prevented Fulfillment of a Safety Function

. . . . .

#### Discussion

The level of judgment for reporting an event or condition under this criterion is a reasonable expectation of preventing fulfillment of a safety function. In the discussions which follow, many of which are taken from previous NUREG guidance, several different expressions such as "would have," "could have," "alone could have," and "reasonable doubt" are used to characterize this standard. In the staff's view, all of these should be judged on the basis of a reasonable expectation of preventing fulfillment of the safety function. Engineering judgment can be used to provide reasonable expectation that the safety function of the system would or would not be met. The staff considers that the use of engineering judgment implies a logical thought process that supports the judgment.

The intent of these criteria is to capture those events where there would have been a failure of a safety system to properly complete a safety function, regardless whether there was an actual demand. For example, if the high pressure safety injection system (both trains) failed, the event would be reportable even if there was no demand for the system's safety function.

If the event or condition could have prevented fulfillment of the safety function at the time of discovery an ENS notification is required. If it could have prevented fulfillment of the safety function at any time within three years of the date of discovery an LER is required.

These criteria cover an event or condition where structures, components, or trains of a safety system could have failed to perform their intended function because of: one or more personnel errors, including procedure violations; equipment failures; inadequate maintenance; or design, analysis, fabrication, equipment qualification, construction, or procedural deficiencies. The event must be reported regardless of whether or not an alternate safety system could have been used to perform the safety function. For example, if the onsite power system failed (if credited in the plant's accident analysis) the event would be reportable, even if the offsite power system remained available and capable of performing the required safety function.

The definition of the systems included in the scope of these criteria is provided in the rules. The applicable functions of these systems are those required to perform a safety function assumed in the plant's accident analysis as credited in chapters 6 or 15 of the FSAR or equivalent to perform one of the four functions (A) through (D) specified in the rule and are in TS. The applicable accident analyses are limited to events of moderate frequency, infrequent incidents, or limiting faults. It is not determined by the phrases "safety related," "important to safety," or "ESF." Support systems, including non-safety systems, are included within the scope of the reporting criteria to the extent that the condition would prevent the fulfillment of the safety function credited by the design basis accident analysis. This reporting criterion does not include systems included in the TS for reasons other than the system is assumed in the plant's accident analysis to perform one of the four functions (A) through (D) specified in the rule. These reporting criteria are applicable during plant modes, conditions, or accident situations as relied on in the plant safety analysis to meet regulatory requirements.

Comment [CBC1]: Operator Action / Engineering Judgment:

Previously discussed in section 2.1. Added here for consistency.

Comment [Ind 10142]: Change from systems to function per NRC writeup philosophy

Comment [CBC3]: The statement "The definition of the systems included in the scope of these criteria is provided in the rules." The sentence is only changed editorially by deleting the word "themselves."

Deleted: themselves

Deleted: se

Deleted: are

Deleted: it

Deleted: the

Deleted: includes

Deleted: by the TS to be operable to

Comment [CBC4]: The proposed wording adds clarity to the sentence to reflect that the systems/functions to be reported are those assumed in the accident analysis. This reporting requirement was based on the assumption that safety-related systems and structures are intended to mitigate the consequences of an accident. This clarification is to make it clear that one of the functions (a) through (D) must be impacted in such away that it invalidates an assumption of the plant's design basis accident analysis.

Deleted: typically

Deleted: .

Comment [CBC5]: The statement "Support systems not in TS, including non-safety systems, are included within the scope of the reporting criteria to the extent that they would prevent the safety function during design basis accident analysis conditions of a system required to be operable by TS" was added for consistency with other portions of NUREG 1022 Revision 2 and the stated intent of the requirement in 48FR33850, 48FR33854, and 48FR33858.

The following statement is added "This reporting criterion does not include systems included in the TS for reasons other than the system is assumed in the plant's accident analysis to perform one of the four functions (A) through (D) specified in the rule." Additionally, the answer to Example 2 is modified to reflect that the subject system must both have an affected safety function in the accident analysis and be included [... [1]

In determining the reportability of an event or condition that affects a system, it is not necessary to assume an additional random single failure in that system; however, it is necessary to consider other existing plant conditions. (See Example [4] below).

A system must operate long enough to complete its intended safety function as defined in the safety analysis report.

**Comment [CBC6]:** Moved to paragraph above for clarity and consistency

Appendix C, Section C.5, of Part 9900 addresses the use of manual action in place of automatic action in support of operability to ensure that the specified safety functions of systems, structures and components (SSC) can be accomplished.

**Deleted:** The term "safety function" refers to any of the four functions (A through D) listed in these reporting criteria that are required during any plant mode or accident situation as described or relied on in the plant safety analysis report or required by the regulations.

The extent to which manual actions may be credited is limited in the guidance. For instance, the guidance makes it clear that use of manual Operator actions in lieu of automatic actions to protect the plant's limiting safety system settings for nuclear reactors as defined in 10 CFR 50.36 is not considered acceptable.

**Deleted:** Generic Letter 91-18 provides guidance on determining whether a system is operable. ¶

**Deleted:** temporary

However, while it is recognized that the guidance does delineate specific restrictions, the guidance recognizes that there are conditions in which credit for manual operator action may be accepted as a means for ensuring the operability of a SSC and therefore its continued ability to satisfactorily complete its safety function. Similarly, manual actions can be used to provide reasonable assurance that the safety function required by the rule can be fulfilled.

Plant assessments, evaluations, and calculations may be used to support a reasonable expectation that a system, structure, or component is capable of performing its safety function as defined by the rule. Reasonable expectation is not considered absolute assurance that a system can perform its function.

**Comment [CBC7]:** Comes from 9900, sections. 3.9 and 4.8.

Required offsite circuits (circuits between the offsite transmission network and the onsite Class 1E AC Electrical Power Distribution System) and onsite emergency power (usually diesel generators) are considered to be separate functions by GDC 17. If all offsite circuits or onsite emergency power is unavailable to the plant when required by TSs to be operable, it is reportable regardless of whether the other system is available. GDC 17 defines the safety function of each system as providing sufficient capacity and capability, etc., assuming that the other system is not available. Loss of offsite power (loss of all offsite circuits) should be determined at the essential switchgear busses.

**Deleted:** Both

**Deleted:** electrical power (transmission lines) and onsite emergency power (usually diesel generators)

**Deleted:** either both

**Deleted:** power

**Deleted:** both

**Comment [CBC8]:** This change is consistent with revision to example 4 below

**Deleted:** .

The statement "Support systems not in TS, including non-safety systems, are included within the scope of the reporting criteria to the extent that they would prevent the safety function during design basis accident analysis conditions of a system required to be operable by TS" was added for consistency with other portions of NUREG 1022 Revision 2 and the stated intent of the requirement in 48FR33850, 48FR33854, and 48FR33858.

The following statement is added "This reporting criterion does not include systems included in the TS for reasons other than the system is assumed in the plant's accident analysis to perform one of the four functions (A) through (D) specified in the rule." Additionally, the answer to Example 2 is modified to reflect that the subject system must both have an affected safety function in the accident analysis and be included in the TS for a condition to be reportable under this criterion.

These changes are to insure that the intent of the reporting requirements are correctly reflected as discussed in NRC memorandum from Suzanne C. Black to Geoffrey E. Grant titled "Task Interface Agreement (TIA) 99-030 From Region III Regarding the Reportability Of Reactor Core Isolation Cooling (RCIC) System Failures" dated March 15, 2001 (Accession No. ML010740339) and RIS 2001-14 Position on Reportability Requirements for Reactor Core Isolation Cooling System Failure July 19, 2001.