Preliminary paper for discussion

TS INITIATIVE 7

Impact of non technical specification design features on OPERABILITY requirements

Definition:

Provide for a deferral time, prior to entering limiting condition for operation, for equipment having technical specification OPERABILITY requirements, when the primary safety function of the equipment is maintained, but non technical specification design features in place solely to address low probability initiating events are degraded or not functional. During the time interval of deferred entry into the limiting condition for operation, the condition will be evaluated and managed under the maintenance rule plant configuration control requirement (10 FR 50.65(a)(4), and associated industry guidance (NUMARC 93-01, Revision 3).

Discussion:

In order to meet the definition of OPERABILITY, a system, subsystem, division, component, or device shall be capable of performing its specified safety function(s), and all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for performance of the safety function are also capable of performing their related support function(s). The "specified safety function" is that described in the basis for the technical specification, and which is necessary to address the conditions of the accident analysis contained in the updated final safety analysis report.

Important support systems, including instrumentation, normal and emergency electrical power, and cooling water, have specific technical specification requirements (including surveillance requirements, limiting conditions for operation and action requirements), with respect to their ability to support the frontline equipment in its performance under design basis accident conditions. This initiative would not replace the existing technical specification requirements for support equipment appearing in technical specifications (other than to the extent that the support equipment itself may also possess design features for low probability initiators that would fall under this initiative.) However, many equipment design features that do not directly appear in technical specifications have the potential to impact the OPERABILITY definition.

NRC generic letter 91-18 provides general guidance on the treatment of degraded conditions with respect to operability; and states that "…the fact that a system is not fully qualified does not, in all cases, render the system unable to perform its specified function if called upon". However, the guidance of generic letter 91-18 is primarily focused on degraded conditions that are discovered during the course of plant activities, and is less specific about the situations where equipment design features are temporarily altered to facilitate maintenance activities. Further the generic letter is not risk-informed, and predates the promulgation of the maintenance rule configuration assessment requirement, 10 CFR 50.65 (a)(4), which was specifically developed to address risk impact of maintenance activities. Implementation guidance for this section of the maintenance rule discusses the need to address temporary plant alterations through risk analysis and management, but the use of the (a)(4) approach does not relieve technical specification compliance issues. Thus, the intent of this initiative is to reduce existing inconsistency with the maintenance rule relative to design features not contained directly in the technical specifications

Certain support equipment, such as snubbers, containment penetration overcurrent protective devices, and motor thermal overload protection devices, were originally listed in the technical specifications, but were removed through the ITS conversion process. However, operability issues have continued to arise with respect to this equipment, and a new LCO, 3.0.8 has been proposed to link this specific category of support equipment to the supported system. For situations where the support equipment is not functional, this LCO will provide for a deferral period during which the limiting condition for operation for the supported system is not entered. Initiative 7 would not affect that equipment addressed by proposed LCO 3.0.8., but would provide a similar approach for other non technical specification design features, through a risk informed approach.

Typically non technical specification design features are in place to provide for equipment functionality during design basis accident conditions, such as high energy line breaks, large LOCAs, seismic events, internal floods, fires, and other infrequent events. Because of the very low initiator frequency, probabilistic safety analysis would generally show the functionality of these features to be of low risk significance. A simplified risk analysis approach is presented later in this paper.

Maintenance situations may arise where the frontline system remains capable of performing its major safety function (e.g., provide injection at design flowrate and pressure, provide negative reactivity insertion, etc.), but design features as described above are temporarily degraded or nonfunctional. An example would be a maintenance activity involving the removal of a high energy line break barrier, or a maintenance activity

involving the temporary opening of a door that normally provides protection against internal flood due to a LOCA. The technical specification equipment protected by the HELB barrier, or door, remains functional for plant transients or accidents other than those protected against by the door or barrier, but the technical specification equipment is INOPERABLE by the existing definition, as it does not meet all conditions of the accident analysis.

The configuration assessment provision of the maintenance rule requires risk assessment and management of temporary plant modifications to the above type design features, when their functionality is affected through temporary plant alterations or compensatory measures necessary to facilitate maintenance activities. This assessment involves the consideration of PSA insights, including initiator frequencies, dependencies, common cause failures, and other issues of potential risk impact. Further, the configuration management program defines risk management actions as appropriate based on the assessment results (e.g., control the duration of the degraded condition to a specific duration, limit work on redundant trains, etc.) However, the technical specification OPERABILITY requirements are independent of, and cannot presently be affected by, the conclusion of the risk assessment, or the use of risk management actions.

By providing an LCO entrance deferral time for the supported system, when design features are altered, technical specifications can be made more consistent with the configuration risk management approach of the maintenance rule. The proposed approach of this initiative is to provide a new LCO 3.0.9, describing the approach and any conditions on its use, and a new Bases table X.X.X which would list risk-informed deferral times due to non-functionality of listed design features. The risk-informed time limits are a function of the specific initiating events, and associated frequencies, that the features are designed to protect against. It is proposed that the following conditions would apply:

1. The new LCO 3.0.9 would reference the performance of the 10 CFR 50.65(a)(4) assessment, and note that, if the assessment and associated risk management actions suggest the need for a shorter duration than provided by the table (due to unique temporary plant configuration issues), the assessment result would be controlling.

2. The new LCO 3.0.9 would expand the applicability of the risk assessment from those situations involving temporary plant alterations or compensatory measures to facilitate maintenance activities, to any situation involving a degraded or nonfunctional design feature as described in the Bases table (thus providing a risk informed alternative to the generic letter 91-18 approach).

3. The new LCO 3.0.9 would limit the use of the provision, at a given time, and for specific initiating event(s), to one train of a multi-train safety system.

Proposed LCO 3.0.9

When a technical specification LCO is not met solely due to a degraded or nonfunctional design feature (identified in Bases table X.X.X), the technical specifications LCO is considered to be met unless the associated delay time (identified in Bases table X.X.X) for the non-technical specification design feature has expired. This is an exception to LCO 3.0.2 for the technical specifications supported system. The following conditions must be met to utilize this provision:

1. For a multi-train system designed to mitigate a specific initiating event or events (listed in Bases table X.X.X), the deferral time provision may be used for one train of the system at a single time, for a given initiating event or events.

2. For the interval of the deferral time, the degraded design feature will be evaluated and managed under the maintenance rule plant configuration control requirement (10 CFR 50.65(a)(4), and associated industry guidance (NUMARC 93-01, Revision 3.). Should the assessment and risk management actions for a specific plant configuration provide a deferral time that is shorter than that listed on the table, the (a)(4) risk management action shall be implemented.

3. This provision is applicable whether the design feature degradation is due to maintenance or due to a discovered condition.

4. Upon expiration of the non-technical specifications support system deferral time, the technical specification supported system shall be declared inoperable and the applicable conditions and required actions for the technical specifications supported system shall be entered in accordance with LCO 3.0.2.

Examples of these features are as follows: (note: The following table would be expanded to become Bases table X.X.X, as referenced below.)

Design features	**Initiators**	**Initiator Frequency**	**Deferral time**
Doors (system, component, train inside affected rooms)	Internal floods (MFLB) External floods HELB outside containment Fire	Need data Site specific 1E-02, per SDP small fires 1E-1 fire challenging barriers 1E-03)	
Barriers (system, component train protected by barrier)	Internal floods External floods HELB outside containment Fire	Need data Site specific 1E-02, per SDP small fires 1E-01 fire challenging barriers 1E-03)	
Seismic, other than snubbers (lead shielding, scaffolding)	Earthquake	Site specific – E-4?	
Automatic actuation capability not available, but restoration capability provided	LOCA, other DB events		
others			

Simplified risk analysis to support initiative 7 for design features impacting one train of a two train system

1. Assume the potential loss of a single train due to design feature outside tech specs [like door, barrier].

2. Single trains of emergency systems have a reliability of about 1E-2/demand or better. The 1E-2 number is mainly driven by major 'movers' in safety systems like EDGs and large pumps which have a failure to start of about 1/100 demands. This means that for a typical two-train safety system the loss of train should result in a increase in system unreliability of 1E-2 – but in practice

because of common cause effects on two train systems the increase is nearer 1E-1. This is equivalent to saying that the loss of a train will, on average, increase the CDF for sequences that the system is involved in by a factor of 10 [i.e., the train has a RAW of 10]. In practice a given system may not be required for some initiators so the actual overall RAW will be less than 10. A good range to assume for single trains [or components within train] is a RAW range of 2 to 10 for systems that feature as mitigators reasonably often in accident mitigation systems.

3. The initiators for the design features outside of tech specs are lower probability initiators. PRAs often classify initiators into a) probable during plant lifetime, 0.1 to 1/year – things like general transients, b) possible during plant lifetime, 0.01 to 0.1/year – things like a loss of offsite power, c) unlikely initiators less than .01/year like earthquakes, large LOCAs, floods for most plants.

4. Suppose that we are going to allow a 30-day deferral time for entry into AOT from known loss or removal of design feature. This is about 10% of a year, so a train loss for this time [assuming it has a RAW of 2 to 10] would increase CDF from 10% to nearly double. However, we would only be concerned about train loss if an initiating event of the right type occurred during the time the design feature, like an open door, was extant. In most cases the initiating event of concern is going to be an unlikely, initiator of 1E-2/year or less – which implies conservatively a 1E-3 probability or less [mostly a lot less] of occurring while the door is open.

5. Multiply the probability of the initiating event that could cause the loss of train by the potential increase in annual risk from the loss of the train. This gives 1E-3 x [1.1 to 2] or an 1.1E-3 to 2E-3 CDF multiplier. The current median CDF/year for US plants is 2.3E-5 [internal events] so the actual CDF increase based on a multiplier of 1.1E-3 to 2E-3 would be 2.5E-8 to 4.6E-8/year. These numbers are well within any noise factors for CDF increase. (need discussion of ICDP).

6. Exceptions might include items with RAWs well above 10 – could occur with some 2-train emergency power systems. Also plants where the normally low initiators are not low – perhaps some plant CDFs that are dominated by earthquakes or by internal floods. These plants might have to limit the total amount of time per year that the deferral time was exercised (but this should be covered by (a)(4))