Preliminary Description Paper

Risk-Informed Technical Specifications Initiative 4B

The purpose of this paper is to describe the general considerations in establishing a risk informed process to supplement the existing technical specification allowed outage times for systems/equipment with a configuration risk management approach.

Configuration risk management

One fundamental purpose of tech specs is to provide plant configuration control. Plants are designed with multiple redundant systems, and supporting systems to accomplish safety functions in accordance with the plant design basis and accident analysis as contained in the FSAR. Tech specs place limits on the times that systems, or supporting systems can be out of service, and establish actions that must be taken (often leading to plant shutdown) in the event these time limits are not met. Tech specs are not risk-informed, in that the allowed outage times do not typically have a risk basis, each out of service condition is considered independently, and few limits are imposed on the number of times an out of service condition can be entered.

The requirements of the maintenance rule impose additional constraints on equipment out of service times (unavailability). These requirements are more risk-informed, in that they address unavailability of a train or piece of equipment over a period of time. Plant maintenance generally involves temporary impacts on equipment availability that are balanced by increased reliability. The maintenance rule requires availability of risk-significant equipment to be balanced with reliability, through the use of PSA insights. This has the effect of establishing availability targets for important equipment in accordance with those values assumed in the PSA.

In November 2000, a risk-informed plant configuration control provision was added to the maintenance rule, 10 CFR 50.65, requiring assessment and consideration of risk prior to performance of both online and shutdown maintenance. Industry developed guidance to accompany this rulemaking through a revision to the maintenance rule implementation guideline. That document, NUMARC 93-01, revision 3, provides guidance on the use of quantitative probabilistic safety assessment (PSA), qualitative risk assessment, and plant operating experience to assess plant risk due to maintenance activities. It also provides guidance on actions that may be taken to manage the risk as determined by the assessment. The guidance also incorporates the shutdown risk management approach of NUMARC 91-06, which is based on preservation of key shutdown safety functions.

It is recognized that the configuration control requirements of technical specifications (deterministic) and the maintenance rule (risk informed) may be in conflict; however, the licensee is required to comply with both, resulting in limitations on configuration control flexibility that are unrelated to plant safety. The intent of this initiative is to address the incompatibilities between these methods, and provide a single, consistent approach for plant configuration control.

The scope of this initiative is limited to those action requirements and limiting conditions for operation that address configuration and operability of plant equipment, and are thus amenable to a risk assessment process. Existing technical specification actions and limiting conditions relative to plant parameters, such as fuel limits, pressure limits, or power-flow distribution maps, would not be affected. Further, this initiative applies to systems, components, and equipment that are explicitly addressed by technical specifications. Initiative 7 addresses the treatment of design features that are implicitly captured into technical specifications through the definition of OPERABILITY.

The intent of this initiative is to address situations where the train or system is unavailable, or the equipment's primary safety function is degraded (e.g. a HPSI injection valve is out of service, but the other active components of the system are available). Initiative 7 is intended to address situations where design features required for low probability initiating events are degraded, but the system's primary safety function is maintained. This would allow deferral of entrance into the Limiting Condition for Operation (LCO) for a specific time frame.

General guidelines of approach:

1. The existing AOTs and action requirements of tech specs would be retained.
2. An option will be added to use a configuration risk management approach to extend the AOT and undertake risk management actions as appropriate.
3. The risk assessment and management approach would be in accord with the guidelines of NUMARC 93-01, with additions as detailed below.
4. A backstop AOT will be developed, which cannot be exceeded regardless of the results of the risk analysis.

Explanation

Attachment 1 provides a draft tech spec page illustrating the format of the approach.

A planned maintenance condition may result in equipment either being removed from service, or rendered inoperable due to a degradation of the equipment's

function such that it no longer meets the tech spec operability definition. This results in entrance into the limiting condition for operation.

Following the determination of inoperability, the tech spec ACTIONS must be entered, and a risk assessment must be performed in accordance with the maintenance rule (a)(4) guidance. Risk management actions are also established in accordance with the (a)(4) guidance. These actions could include the need to perform a mode change prior to expiration of the Tech Spec AOT. The above combination of actions, which is the same as is currently in use, provides appropriate control of plant configuration risk up until the expiration of the AOT. The configuration risk management approach would optionally entered upon expiration of the existing AOT (frontstop).

Under the proposed approach, the licensee may make the decision to utilize the configuration risk management option to extend the AOT. This entails performance of an enhanced risk assessment in accordance with the description below. The risk assessment and determination of risk management actions must be completed prior to expiration of the existing AOT (frontstop). The risk management actions must be established prior to expiration of the frontstop.

A backstop AOT limit is implemented for all tech spec systems/equipment within the scope of this initiative. In no case can the AOT exceed the backstop limit. This is further explained below.

In the event of an emergent condition (as described in NUMARC 93-01), the enhanced risk assessment and associated risk management actions must be re-evaluated in a timely manner. Revised risk management actions must be in place within a timely manner.

Flexible AOT risk assessment and management

The flexible AOT assessment would include all provisions of the existing (a)(4) implementation guidance, with the following additions:

1. The assessment would require, as a minimum, a quantitative assessment using a level one internal events PSA and simplified LERF model for power operation.

2. All elements of the level one PSA must meet the minimum attributes for a risk-informed application when evaluated by a peer review team in accordance with NEI 00-02, industry peer review guidance document, or "conditional" grades must be resolved.

3. The PSA should be evaluated for update (model update and data update) on a minimum interval of two refueling cycles. Modifications to the plant resulting in non-minimal risk effects (changes to baseline risk, or changes to distribution of significant equipment or actions) must be reflected in the PSA, or otherwise accommodated in the risk assessment process, within X weeks.

4. The risk-informed decisionmaking process should have the capability to model the real time plant configuration, and calculate the configuration-specific CDF and LERF. That is, it should use the "zero maintenance" model, and be capable of timely requantification to address emergent conditions.

5. The assessment must consider instantaneous risk, integrated risk for a given configuration, and aggregate risk as discussed in NUMARC 93-01. The quantitative guidelines for each of these parameters are specified in NUMARC 93-01.

6. Explicit risk management actions (e.g., mode change, compensatory measure) based on the above quantitative guidelines, and other qualitative PSA and risk insights, may be developed and documented in advance for anticipated combinations of equipment with more significant risk impacts.

7. Regardless of the risk assessment outcome, planned maintenance activities must not be performed that would render both trains of a safety system inoperable at the same time. Emergent conditions may allow this situation for a limited time, based on the outcome of the assessment and management actions.

8. The assessment, results, and associated risk management actions must be documented and available for subsequent NRC audit or inspection.

Backstop AOT

A tech spec not-to-exceed value for each AOT subject to this initiative would be provided. This AOT would be referred to as the "backstop AOT", which could never be exceeded regardless of the risk evaluation results. For systems with very low risk impact, the backstop AOT provides for return to a configuration as described in the deterministic accident analysis, and obviates plant "modifications" involving very long allowed outage times.

The backstop is in place to address deterministic considerations. It is not necessary that the backstop AOT be derived from risk analyses. The risk assessment and management process required to utilize any portion or all of the backstop AOT is complete and self sufficient with regard to consideration of risk. Further, if a backstop value were to be derived from risk analyses (e.g., use of a Reg Guide 1.177

approach to calculate ICDP, etc) it would have to be based on specific assumptions with regard to the degree of degradation of the equipment. Typically a Reg Guide 1.177 evaluation assumes the equipment is out of service; however, for many anticipated conditions, the equipment could still be partially functional, and a backstop AOT calculated based on out of service equipment would preclude proper consideration of the actual equipment performance capability in the risk assessment and management process.

The backstop AOT would typically be 30 days. Individual exceptions may be identified.