JENSEN HUGHES

158 W. Gay Street, Suite 400
West Chester, PA 19380 USA
jensenhughes.com
O: +1 610-431-8260

WHITE PAPER ON ASPECTS OF THE REACTOR OVERSIGHT PROCESS FOR THE AP1000 REACTOR DESIGN

Prepared For

AP1000 Owner's Group (APOG, LLC)
through
Southern Nuclear Operating Co., Inc.
42 Inverness Center Parkway
Birmingham, AL 35242

Revision: 0a

Project #: 1DAD2F001.000
Project Name: AP1000 Reactor Design
Report #: 02F001-RPT-01

	Name and Date
Preparer:	Donald A. Dube
Reviewer:	Pat W. Baranowsky
Review Method	Design Review ☒ Alternate Calculation ☐
Approver:	

REVISION RECORD SUMMARY

Revision	Revision Summary
0a	Initial issue addressing APOG comments

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1
1.0 TECHNICAL BASIS FOR THE MITIGATING SYSTEMS PERFORMANCE INDEX 3
1.1 Overview of the MSPI 3
1.2 Applicability to New Reactors 5
1.3 Applicability to Passive Systems 6
1.4 Issues with Phasing-in the MSPI for AP1000 8
1.4.1 Technical Basis for the Three-Year Monitoring Period 8
1.4.2 Technical Basis of the Risk Cap 8
1.4.3 Technical Basis of the Performance Limit 9
1.4.4 The Need for a Three-Year Monitoring Period 10
2.0 THE ROLE OF RTNSS IN ROP 11
2.1 Overview of RTNSS 11
2.2 Technical Basis for Performance Indicators and Inspection 12
2.3 PIs and MSPI for RTNSS 13
2.3.1 Appropriateness of RNS for MSPI 15
2.3.2 Appropriateness of CCS for MSPI 15
2.3.3 Appropriateness of SWS for MSPI 16
2.3.4 Appropriateness of Standby DGs for MSPI 16
2.3.5 Summary of Appropriateness of MSPI 16
2.4 Inspection Activities for RTNSS 16
3.0 CONCLUSIONS 18
4.0 REFERENCES 19

LIST OF TABLES

Table 1-1 Systems Included in MSPI 4
Table 1-2 Component Types Included in MSPI for Unreliability Monitoring 4
Table 1-3 Key Passive Systems in the AP1000 6

LIST OF FIGURES

Figure 1-1 Variable Backstop 9
Figure 1-2 1Q/2015 Performance Indicators - Fort Calhoun 10
Figure 2-1 Historical Performance Indicator with Unintended Consequences 14

EXECUTIVE SUMMARY

This paper assesses the implementation of certain aspects of the Reactor Oversight Process (ROP) to the AP1000 reactor design. Specifically, the technical basis for the ROP in general and the mitigating systems performance index (MSPI) in particular are evaluated. The applicability to passive safety systems as well as systems under the regulatory treatment of non-safety systems (RTNSS) is considered. Counting type indicators analogous to unplanned scrams per 7000 critical hours and safety system functional failures are found to meet the attributes for a good performance indicator (PI).

However, practical implementation considerations arise with the MSPI if applied to passive structures, systems and components (SSC) in the AP1000. For one, there are insufficient performance data on passive systems and components to develop meaningful industry-averaged performance baselines that are a key aspect of the MSPI formulation. Robust data for passive system unavailability baselines will not be obtained from the projected fleet of AP1000 reactors for a decade or more. Plant-specific reliability data over a three-year monitoring period for risk-significant passive components may never be sufficient to give a meaningful and robust MSPI value. A single failure in high risk-importance systems would likely invoke the risk cap for most if not all monitored component types in passive systems because of this lack of reliability data.

A second issue arises with the phasing-in of the MSPI for a new reactor that is starting commercial operation. Historical documents such as NUREG-1753 and NUREG-1816 founded the MSPI based on a three-year monitoring period. The three-year observation period was found to balance the need for good statistics against the need to detect performance changes within a reasonable time. The verification of the MSPI and numerical simulation that led to confidence in the robustness of the MSPI were both based on a three-year monitoring period. Both the risk cap and the performance limit are formulated on a three-year rolling indicator.

Any option that phases in the MSPI at a newly operating plant before three years of plant-specific performance data have been obtained compromises the original basis of the MSPI. Large volatility could be exhibited by the indicator.

Given the above discussion, alternatives to the MSPI should be pursued for the passive systems of interest.

The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions to back up the passive systems. Recognizing this, the U.S. Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI) developed a process to identify important active systems and to maintain appropriate regulatory oversight of those systems.

Source documents such as WCAP-15985, Revision 2 provide the basis for the selection of systems under RTNSS for the AP1000 design. Administrative controls are formatted similar to the Technical Specifications (TS) with operability requirements, applicability, actions and completion times (if operability requirements are not met), surveillance requirements, and bases for the availability controls. There are no limiting conditions for operation (i.e., there is no requirement to bring the plant to a safe-shutdown condition when operability requirements are not fulfilled) if the completion times for required actions are not met. This is a key distinction from standard TS and could, theoretically, impact the average unavailabilities of RTNSS systems and cause divergence from the industry-averaged values for similar (safety-related) systems in the MSPI.

Either because of the lack of relevant industry performance data to serve as baselines, lack of robustness of the performance data being measured, or investment controls that are irrelevant

during power operation, an MSPI-type performance indicator is found to be inappropriate for all systems included under RTNSS. In the absence of good candidate PIs for RTNSS, inspection using risk assessment to determine significance would seem to be the most appropriate activity to undertake until sufficient AP1000 operating experience becomes available.

1.0 TECHNICAL BASIS FOR THE MITIGATING SYSTEMS PERFORMANCE INDEX

This paper assesses the implementation of certain aspects of the Reactor Oversight Process (ROP) to the AP1000 reactor design. Specifically, the technical basis for the ROP in general and the mitigating systems performance index (MSPI) in particular are evaluated. The applicability to passive safety systems as well as systems under the regulatory treatment of non-safety systems (RTNSS) is considered in Section 2.

1.1 Overview of the MSPI

The purpose of the MSPI is to monitor the performance of selected nuclear power plant systems based on their ability to perform risk-significant functions [1]. It is comprised of three elements - system unavailability, system unreliability and system component performance limits. The index is used to determine the cumulative significance of failures and unavailability over the monitored time period.

The MSPI of a given system is a simplified linear approximation of the change in core damage frequency (CDF) attributable to changes in the reliability and availability of risk-significant elements of the system during internal events with the reactor operating at power. Thus, the calculation focuses on key components, and quantifies the change in CDF using a simple formula based on the sum of changes in the unavailability index (UAI) and the unreliability index (URI), as follows:

$$MSPI = UAI + URI$$

The MSPI evolved following the conceptual development of risk-based performance indicators in NUREG-1753 and after several public workshops and meetings [2]. The MSPI replaced the Safety System Unavailability (SSU) performance indicators because of known deficiencies with the SSU. Specifically, these deficiencies included the use of fault exposure hours and short-term unavailability to approximate unreliability, the omission of certain unreliability elements, the use of generic ("one-size-fits-all") performance thresholds irrespective of the risk significance of the system, and potential double-counting as a result of support system failures cascading onto front line systems. Moreover, the way the SSU indicators measured unavailability was inconsistent with the definition in the NRC's Maintenance Rule, as well as the indicators promulgated by the World Association of Nuclear Operators and the Institute of Nuclear Power Operations.

Reference 3 provides an overview of the MSPI formulation, its characteristics, benefits and limitations, and key issues needed to be addressed at that time. In NUREG-1816 [4], the NRC staff and its contractors extensively tested and improved the MSPI methodology during the twelve-month pilot plant application phase, and evaluated technical issues related to the new indicator's sensitivity to probabilistic risk assessment (PRA) modeling detail. The MSPI went into effect after the first quarter of 2006 and was implemented at all operating U.S. boiling water reactor (BWR) power plants and all pressurized water reactors (PWR) power plants.

The risk significance of mitigating systems was originally determined through analysis of NRC's SPAR models supplemented by quantification results found in the Individual Plant Examination (IPE) submittals and the associated IPE Database. Specific equipment (i.e., mitigating systems and component classes) was identified as risk-significant based on combinations of importance measure values calculated from these sources. In addition to being risk-significant, the mitigating system must be capable of detecting performance changes in a timely manner. As noted in Reference 2, "the associated monitoring period must be long enough to reduce the probabilities of false negatives and false positives to acceptable levels, but no longer."

After detailed analysis of candidate systems for consideration in the MSPI, the final set of systems chosen for monitoring was narrowed to those listed in Table 1-1 below. All of these systems, by design, are systems employing active devices such as pumps and electrical generators.

The evaluation of risk-significance in Reference 2 also identified several component classes that were important. These were chosen because they can provide plant-wide performance attributes that would potentially reflect performance changes due to "cross-cutting" issues before individual system or train indicators. Unreliability was selected to be the risk-informed performance indicator for each of these component classes. The final list of monitored components chosen for the MSPI is provided in Table 1-2. It is important to note that these are all “active components” in that “passive components” such as check valves and manual valves that do not require external sources of power or motive force are deliberately excluded from the URI. Such passive components as well as water tanks and other structures may be included in the MSPI through their impact on train or system unavailability (UAI), but are not included for unreliability.

Table 1-1 Systems Included in MSPI

BWR Systems	PWR Systems
Emergency AC power	Emergency AC Power
High-Pressure Injection (High Pressure Coolant Injection, High Pressure Core Spray, Feedwater Coolant Injection)	High-Pressure Injection (may include charging pumps and associated valves)
High-Pressure Heat Removal Systems (Reactor Core Isolation Cooling or Isolation Condenser)	High-Pressure Heat Removal Systems (Auxiliary or Emergency Feedwater)
Residual Heat Removal	Residual Heat Removal (may include containment spray recirculation system for CE plants)
Cooling Water Support Systems (safety related service water or raw water, safety related component cooling water)	Cooling Water Support Systems (safety related service water or raw water, safety related component cooling water)

Table 1-2 Component Types Included in MSPI for Unreliability Monitoring

Circuit breaker
Hydraulic-operated valve
Motor-operated valve
Solenoid-operated valve
Air-operated valve
Motor-driven pump
Turbine-driven pump
Diesel-driven pump
Emergency diesel generator
Hydroelectric unit (Oconee)

Finally, as follow-on to the previous SSU performance indicators that were the predecessors of the MSPI, only safety-related systems were chosen for inclusion in the MSPI [4]. Thus,

alternate AC power (or Station Blackout) generators, non-safety standby feedwater pumps, and non-safety component cooling water and raw water systems were deliberately excluded from the MSPI.

1.2 Applicability to New Reactors

In this report, a review of the principal source documents has been performed to identify the applicability of the MSPI to passive safety systems as well as the traditional active systems for new reactor types other than the BWRs and PWRs in operation at the time of the original publication of those studies [1, 2, 3, 4]. No specific reference is made in those studies to new or advanced reactor designs including designs that have been certified, are undergoing certification, or may be considered for certification in the future such as:

- Those designs with mostly active safety features, e.g. System 80+, Advanced Boiling Water Reactor, and others
- Those designs with mostly passive safety features, e.g. AP1000, ESBWR, and others
- Small modular reactors (SMRs)
- Non-light water reactors

However, it is important to note that the possibility of applying the concepts of the MSPI to other reactor types (other than the currently operating BWR and PWR fleet) has not been explicitly excluded, either.

In response to the Commission's Staff Requirements Memorandum (SRM) on SECY-10-0121, "Modifying the Risk-Informed Regulatory Guidance for New Reactors," a series of tabletop exercises was conducted by the staff and external stakeholders in 2011 [5]. The purpose of the tabletops was to test various realistic performance deficiencies, events, modifications, and licensing bases changes against current NRC policy, regulations, guidance and all other requirements (e.g., Technical Specifications, license conditions, code requirements) that are or will be relevant to the licensing bases of new reactors. The exercises assessed the applicability of current risk metrics to new reactor types. These included such risk-informed applications as risk-informed in-service inspection (RI-ISI) of piping, risk-informed technical specifications (RITS) initiative 4b (completion times), and RITS 5b (surveillance frequency program). The final series of exercises considered the ROP, including the MSPI.

The MSPI exercises considered several actual equipment performance events in the operating fleet and applied them to the ABWR (Toshiba), and the US-APWR (Mitsubishi) [6]. The AP1000 was not considered. Several observations from the exercises included:

- The MSPI case studies seemed to reasonably represent situations applicable to new reactors with active safety systems.
- The cases were limited to active designs; passive designs are too different to evaluate at that time and a meaningful MSPI may not be possible for passive systems.
- The cases indicated that it would be rare and unlikely to cross greater-than-green thresholds for active new reactor designs (assuming the numerical thresholds for new reactors remained unchanged from present performance indicators (PI)). The performance limit (backstop) would play a more significant role and could be emphasized for the new reactor MSPI.
- Given the anticipated low utility of this indicator for new reactor designs, it may be impractical for licensees to create an MSPI basis document and track and report MSPI data.

- Alternatives to the MSPI for new reactors could include the development of alternate mitigating system performance indicators and/or additional inspection to supplement/offset insights currently gained through MSPI.

The participants also briefly discussed some of the passive systems and degradation modes for the AP1000 and other passive designs that could impact their performance and may need to be considered in the future.

This author is not aware of any further exercises or analyses in the nearly five years since the issuance of the tabletop summary results that change the above observations.

1.3 Applicability to Passive Systems

The second bullet regarding the tabletop exercises for new reactor ROP in Section 1.2 is particularly noteworthy: *"a meaningful MSPI may not be possible for passive systems."*

There are several desirable attributes for a robust MSPI:

- The system should have relatively high risk importance as measured by the PRA
- Baseline or industry-averaged performance should be available for system/train unplanned unavailability performance comparison, and component reliability comparison
- There must be sufficient plant-specific system and component performance data generated over the three-year monitoring period to preclude a volatile indicator

System-level importance measures that were calculated as part of the construction ROP effort (cROP) identified a number of passive systems in the AP1000 with high PRA importance as measured by system-level risk achievement worth (RAW) [7]. For example, the safety related DC and vital AC power (IDS) for instrumentation and controls as well as some functions of the passive decay heat removal system (PXS) are noted as having High risk importance for the cROP significance determination process (SDP). A number of other systems such as the core makeup tanks are also found with Intermediate importance. A list of the key passive systems in the AP1000 is provided in Table 1-3.

While considered to be "passive" in nature, even the passive safety systems include a limited set of components such as air-operated valves and DC-powered motor-operated valves that traditionally are considered to be "active." However, many of the valves do not need to change state for an accident, are "fail-safe", or are not normally testable during power operation. This limits the availability of performance data for a robust indicator as discussed below.

Table 1-3 Key Passive Systems in the AP1000

Depressurization System (ADS)
Core Makeup Tanks (PXS)
In-Containment RWST, Injection and Recirculation Modes (PXS)
Passive Containment Cooling System (PCS)
DC-1E (IDS)
Passive RHR (PXS)
In Vessel Retention of molten core (PXS - IVR)
Containment Hydrogen Control System, Passive Autocatalytic Recombiners (VLS - PARs)

With no currently operating AP1000 reactors in the U.S., and none worldwide for that matter, there are insufficient performance data on passive systems and components to develop meaningful unavailability baselines. For example, there are no system/train planned unavailability baselines for core make-up tanks, passive residual heat removal, or DC power systems. In comparison, the data for the industry-averaged baselines and prior distributions in the MSPI for the current operating fleet were generated from several hundred reactor-years of operating experience [1, 4]. Robust data for passive system unavailability baselines will not be obtained from the projected fleet of AP1000 reactors for a decade or more.

While some basic failure rates for explosive valves are available [8], these have been obtained solely from this type of valve in BWR standby liquid control systems and are of questionable applicability to the AP1000. Likewise, equipment performance data for DC power systems including batteries, chargers, and static switches would need to be tabulated and evaluated.

A second limitation when it comes to implementing the MSPI on passive systems and components, particularly for the URI portion of the MSPI, is the low frequency of testing and hence the low number of plant-specific component demands and run-hours which make up critical inputs to the unreliability algorithm. For example, in the current reactor fleet, the typical number of start demands over a three-year monitoring period for emergency diesel generators often exceeds 100 (when pooled). Similarly, standby motor-driven pumps typically have 100 or more start demands, and several hundred hours of operation. Running or alternating pumps may have tens of thousands of operating hours during the monitoring period. Such large demand and operating-hours data, which comprise the denominator portion of the failure rate determination, make for a robust indicator. The MSPI for most current systems can tolerate one or more failures without exhibiting volatile swings in the indicator. It is this author's experience that the most volatile behavior of the MSPI is for standby systems with components that have high risk importance but low demands or low run hours.

In contrast, some of the AP1000 systems, such as PXS, cannot be tested during normal operation, and hence reliability data can be obtained only during outages. Even when pooled, the number of demands on some components such as explosive valves will be insufficient to demonstrate a robust indicator. The URI will be driven by the prior distribution if a Bayesian approach is utilized as is the case with current MSPI monitored components. This is contrary to one of the basic principles of the MSPI – that it is measuring plant-specific performance. It may be possible to utilize alternate prior distributions than are currently used in the MSPI, but this would require a significant developmental effort. Since many of the "active" components such as the ADS motor-operated valves are not testable during power operation, the derived unreliability from a component failure could be significant. A failed component will result in high risk implications for the observation period and may even imply that significant safety function degradation was present for a long period of time, e.g. operating cycle. The SDP is a better way to measure operational risk under these circumstances.

In summary, it is anticipated that it will be a decade or more before meaningful baseline unavailability data are obtained for the most risk-important passive systems in the AP1000. Plant-specific reliability data over a three-year monitoring period for risk-significant passive components may never be sufficient to give a meaningful and robust MSPI value. A single failure on high risk-importance systems would likely invoke the risk cap for most if not all monitored component types in passive systems because of this lack of reliability data. Given this situation, alternatives to the MSPI should be pursued for the passive systems of interest.

1.4 Issues with Phasing-in the MSPI for AP1000

1.4.1 Technical Basis for the Three-Year Monitoring Period

The MSPI was always intended to use a three-year monitoring period. When the MSPI was first implemented in 2006, the 100+ reactor units all had significant operating experience. This allowed for a "cold start" of the MSPI using the three prior years of plant-specific performance data. Because of the importance of the three-year monitoring period, it was decided not to use the MSPI following the restart of Browns Ferry Unit 1 in 2007 after a prolonged shutdown until three years of operating experience were obtained.

One to five year monitoring periods were considered in the feasibility study in NUREG-1753 [2]. Based on statistical analyses as documented in Appendix F, the authors recommended one year for the unavailability and three years for the unreliability indices as shown in Table F-8 of that report. However, this recommendation did not have the benefit of piloting. For practical data collection and reporting purposes, and since the unavailability index was found to be less sensitive to the monitoring period than unreliability, the MSPI pilot was implemented in 2002 with a three-year rolling monitoring period for both unreliability and unavailability.

In NUREG-1816 [4], the NRC staff extensively tested and improved the MSPI methodology during the twelve-month pilot plant application phase, and evaluated technical issues related to the new indicator's sensitivity to probabilistic risk assessment (PRA) modeling detail. A rolling three-year data collection period for the MSPI is central to the validity of the verification effort.

1.4.2 Technical Basis of the Risk Cap

NUREG-1816 found some system indicators associated with the MSPI had significant "false positive" issues. That is, for statistical reasons, there was (in the early formulation of the MSPI) a significant probability that a plant system at baseline performance would cross over the Green/White threshold. As discussed in detail in Appendix D of that report, random failures that occur at a rate consistent with the industry performance are not indicative of a performance issue. That is, one failure over a three-year performance monitoring period, or one failure above the normal expectation, can be argued not to constitute a significant trend.

The risk cap of $5x10^{-7}$ is a fundamental aspect of the MSPI and was chosen with great deliberation. Given baseline system performance (MSPI ~ 0) just prior to the failure, the risk cap of $5x10^{-7}$ from a single failure combined with incremental unavailability (i.e., UAI) due to corrective maintenance should normally result in an MSPI under the Green/White threshold of $1x10^{-6}$. In effect, the risk cap allowed up to an incremental $5x10^{-7}$ for UAI. As discussed in NUREG-1816 Appendix D, the incremental UAI of $5x10^{-7}$ was itself consistent with Regulatory Guide 1.177 at that time [9].

The three-year monitoring period is a key element of the risk cap formulation. As discussed above, given a risk cap of $5x10^{-7}$ allows up to an incremental $5x10^{-7}$ for the UAI contribution before $1x10^{-6}$ is reached. The incremental UAI comes about from the product of the Birnbaum for unavailability of the train or segment and incremental unavailability from the corrective (unplanned) maintenance. The unplanned unavailability is the unplanned maintenance hours divided by the critical hours of the three-year monitoring period.

$$\text{Incremental UAI} = B_i * [\text{incremental unplanned maintenance/critical hrs in 12 qtrs.}]$$

What if a monitoring period other than three years was used, for example, one year? The incremental train or segment unplanned unavailability would be about three times higher because of fewer critical hours in the one-year period, and the incremental UAI would also be about three times higher. In effect, substantial margin to the Green/White threshold would be

lost, negating the full benefit of the risk cap as currently formulated, and increasing the probability of false positives.

In effect, a monitoring period other than three years would be inconsistent with the basic formulation of the risk cap. This means that, if it were decided to implement the MSPI for the AP1000 reactors, it should not take effect until a full three years of plant-specific operating experience are available at a given unit, at a minimum.

1.4.3 Technical Basis of the Performance Limit

If the risk cap was formulated to address *false positives* in the MSPI, the *backstop* (or what has come to be called the *component performance limit*) was instituted to address, to some degree, *false negatives*. The concern was that during the MSPI pilot, large numbers of component failures were observed to be needed for some components in some systems in certain pilot plants before the MSPI turned White at $1x10^{-6}$.

Conceptually, the performance limit is a limit on the total number of failures, of all failure modes and of all components of one type in one system of a single nuclear power plant unit. If the number of failures seen in the three-year performance period exceeds the performance limit, the system MSPI is denoted as White. The criterion is based on statistical significance of the observed number of failures, relative to prior expectations.

The performance limit given in Section F.4 of NEI 99-02 [1] is derived from a linear regression as shown in Figure E.3 of NUREG-1816 and is reproduced below as Figure 1-1.

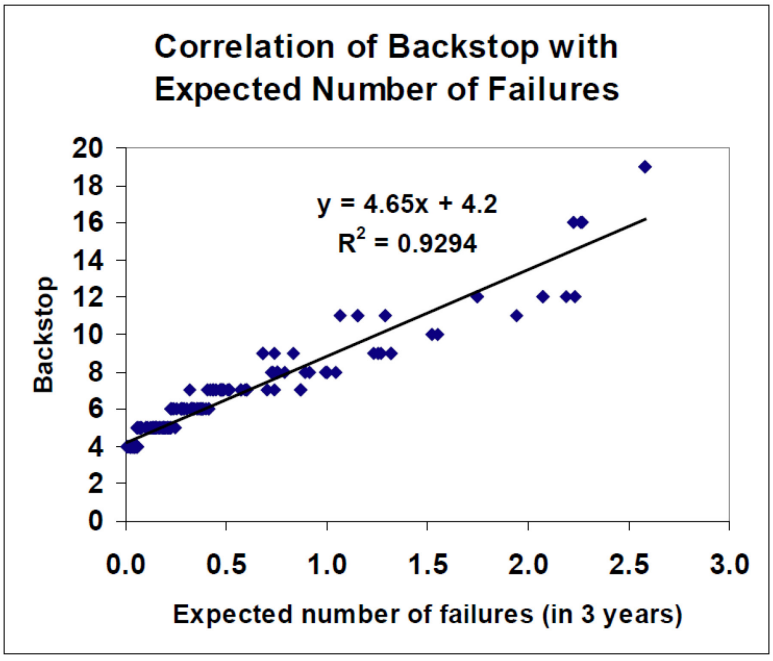

Figure 1-1
Variable Backstop

The correlation in Figure 1-1 shows the backstop, or number of allowable component failures of a given component type within a system, as a function of the expected number of failures. The expected number of failures, in turn, depends on the number of demands (and run hours if applicable) as well as industry-averaged component failure rates. The component performance limit clearly relied on three years' worth of performance data from the pilot plants.

In effect, a monitoring period other than three years is inconsistent with the basic formulation of the performance limit. Again, the same conclusion is reached as in Section 1.4.2. If it were decided to implement the MSPI for the AP1000 reactors, it should not take effect until a full three years of plant-specific operating experience are available at a given unit, at a minimum.

1.4.4 The Need for a Three-Year Monitoring Period

The basic formulation of the MSPI requires three years of performance data before being implemented. While it would be theoretically possible to use a shorter monitoring period than three years during initial AP1000 operation, the MSPI values would be volatile and subject to large fluctuations as component failures and uncharacteristic high train/segment unavailabilities roll into the monitored period. One need only look at the one indicator for Fort Calhoun when it returned to service after an extended outage (2Q/11 to 4Q/13) to realize that a volatile indicator is not in any of the stakeholders' best interest (see Figure 1-2). The volatility in the Emergency AC Power indicator arose because the denominators in the UAI and URI formulations were not sufficiently large to buffer small deviations in diesel generator maintenance and an historic failure in the first quarter of 2012.

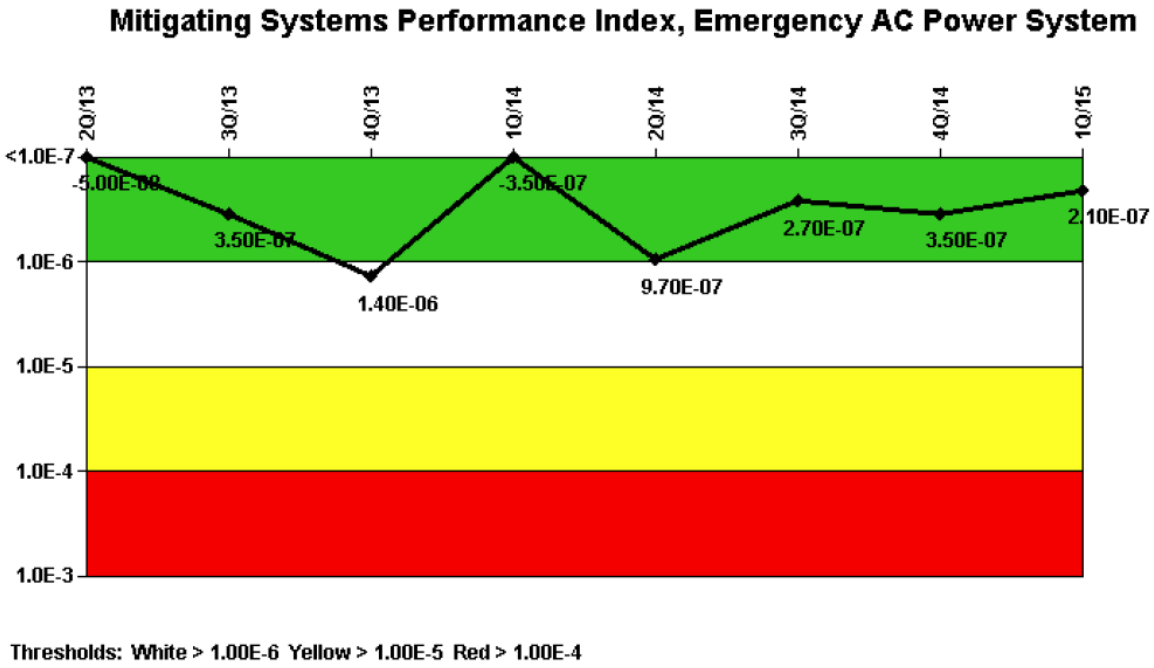

Figure 1-2
1Q/2015 Performance Indicators - Fort Calhoun

2.0 THE ROLE OF RTNSS IN ROP

2.1 Overview of RTNSS

A brief overview of RTNSS sufficient to outline its potential role in the ROP for the AP1000 is provided in this section. It is beyond the scope of this paper to fully describe RTNSS. Source documents include the EPRI Advanced Light-Water Reactor Utility Requirements Document (URD) for passive plants [10]; several Commission papers including SECY-93-087, SECY-94-084, SECY-95-132 (and associated staff requirements memoranda); the NRC's Final Safety Evaluation Report (and supplements) on the AP1000 [11]; and WCAP-15985, Revision 2 [12].

The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions to back up the passive systems. Recognizing this, the NRC and EPRI developed a process to identify important active systems and to maintain appropriate regulatory oversight of those systems. This process does not require that the active systems brought under regulatory oversight meet all safety-related criteria, but rather that these controls provide a high level of confidence that active systems having a significant safety role are available when they are challenged.

The RTNSS process applies broadly to those non-safety-related structures, systems and components (SSCs) that perform risk significant functions, and therefore, are candidates for regulatory oversight. The RTNSS process uses the following five criteria to determine those SSC functions:

1. SSC functions relied upon to meet deterministic NRC performance requirements such as Part 50.62 of Title 10 of the Code of Federal Regulations (10 CFR 50.62) for mitigating anticipated transients without scram (ATWS) and 10 CFR 50.63 for station blackout (SBO)
2. SSC functions relied upon to ensure long-term safety (beyond 72 hours) and to address seismic events
3. SSC functions relied upon under power-operating and shutdown conditions to meet the Commission's safety goal guidelines of a core damage frequency (CDF) of less than $1x10^{-4}$ each reactor year, and a large release frequency (LRF) of less than $1x10^{-6}$ each reactor year
4. SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents. This issue was discussed in detail in SECY-93-087. For the AP1000, this criterion for assessing containment performance is the degree to which the design comports with the Commission's probabilistic containment performance goal of 0.1 conditional containment failure probability (CCFP) when no credit is provided for the performance of the non-safety-related, defense-in-depth systems.
5. SSC functions relied upon to prevent significant adverse systems interactions

If a non-safety-related SSC mitigation function is relied upon in the focused PRA sensitivity studies to allow the calculated CDF and LRF to meet the safety goal guidelines, it is designated risk important and will be subject to regulatory oversight.

The focused PRA uncertainty evaluation determines which non-safety-related SSCs should be identified as RTNSS-important to add margin to compensate for the PRA uncertainties. In certain situations, no non-safety-related SSCs can directly compensate for the PRA uncertainties. In these cases, margin is provided in the PRA by adding regulatory oversight on those non-safety related SSCs that have been identified as being able to improve the results of the PRA sensitivity studies for other sequences. Quality requirements for RTNSS are specified

in Table 17-1 of the AP1000 Design Control Document (DCD). Section 10.2 of WCAP-15985, Revision 2, provides mission statements of the important nonsafety-related SSCs.

Section 10.3 of WCAP-15985, Revision 2, proposed a means for implementing RTNSS controls in the form of short-term administrative availability controls for the SSCs, except for the diverse actuation system (DAS) manual controls which are incorporated in the TS. The regulatory oversight of these RTNSS-important SSCs, as described in Table 10-2, "Investment Protection Short-Term Availability Controls," of WCAP-15985, Revision 2, is incorporated in DCD Tier 2, Table 16.3-2 of the same title.

The administrative controls are formatted similar to the TS with operability requirements, applicability, actions and completion times (if operability requirements are not met), surveillance requirements, and bases for the availability controls. There are no limiting conditions for operation (i.e., there is no requirement to bring the plant to a safe-shutdown condition when operability requirements are not fulfilled) if the completion times for required actions are not met. *This is a key distinction from standard TS and could, theoretically, impact the average unavailabilities of RTNSS systems and cause divergence from the industry-averaged values for similar (safety-related) systems in the MSPI.*

2.2 Technical Basis for Performance Indicators and Inspection

Inspection Manual Chapter (IMC) 0305 describes NRC's Operating Reactor Assessment Program [13]. The ROP integrates NRC's inspection, performance indicator, assessment, and enforcement programs applicable to operating reactors. The Operating Reactor Assessment Program evaluates the overall performance of operating commercial nuclear reactors and communicates this information to licensee management, members of the public, and other stakeholders. The Operating Reactor Assessment Program collects information from inspections and PIs to enable the NRC to develop objective conclusions about a licensee's safety performance.

To measure plant performance, the oversight program focuses on seven specific "cornerstones" which support the safety of plant operations in the three broad strategic areas. These include such focus areas as initiating events, mitigating systems, barrier integrity, and others. Additionally, there are cross-cutting elements such as human performance.

Within each cornerstone, a broad sample of data on which to assess licensee performance in risk-significant areas is gathered from PI data submitted by licensees and from the NRC's risk informed baseline inspections. The PIs are not intended to provide complete coverage of every aspect of plant design and operation, but they are intended to be indicative of performance within the related cornerstone.

PIs are a means of obtaining information related to licensee performance in certain attributes of each cornerstone. They provide indication of problems that, if uncorrected, may increase the probability and/or the consequences of an off-normal event. *Because not all aspects of licensee performance can be monitored by PIs, safety and security significant areas not covered by PIs are assessed using the ROP Inspection Program.* This is a key premise of SECY-99-007 that laid the foundation for the ROP.

The power reactor inspection program is composed of several elements to provide indication of licensee performance [14]. The key feature of the program is the baseline inspection program, which defines the minimum level of inspection that all plants will receive regardless of performance. The supplemental inspection program is performed to independently evaluate the root causes of performance deficiencies when indications of declining licensee performance are obtained through either the PIs or other inspections (principally the baseline inspection

program). Plant events are inspected to determine their significance and to determine the agency's necessary response.

The baseline inspection program was developed using a risk-informed approach to determine a comprehensive list of areas to inspect (inspectable areas) within each cornerstone of safety. These inspectable areas were selected based on their risk significance (i.e., they are needed to meet a cornerstone objective as derived from a combination of probabilistic risk analyses insights, operational experience, deterministic analyses insights, and regulatory requirements).

Risk has been factored into the baseline inspection program in four ways: (1) inspectable areas are based on their risk importance in measuring a cornerstone objective, (2) the inspection frequency, how many activities to inspect, and how much time to spend inspecting activities in each inspectable area is based on risk information, (3) the selection of activities to inspect in each inspectable area is based on plant-specific risk information, and (4) inspectors are trained in the use of risk information. Furthermore, determining the risk significance of inspection findings is important in establishing the urgency of corrective actions.

All the important aspects of a cornerstone area are inspected where a PI has not been established (e.g., design). In cornerstone areas where the PIs provide only limited indication of performance, the inspectable areas provide indication of the aspects not measured (e.g., operator performance during an event). If performance of the cornerstone objective in a cornerstone area is sufficiently measured by a PI, the inspection effort in the baseline program only verifies that the PI is providing the intended data.

2.3 PIs and MSPI for RTNSS

Given the above discussion in Section 2.1 regarding the RTNSS process, and Section 2.2 regarding the purpose of PIs in general and the MSPI in particular, what role should PIs take on for RTNSS?

The general literature provides ample discussions of what makes a good performance indicator. From the decades-long experience with PIs in the nuclear industry, what comes to mind for risk-informed performance indicators includes the following attributes:

1. There is a strong nexus with reactor safety and public safety
2. The performance is measurable
3. There are sufficient data so that the indicator is robust: small changes in input data do not cause large gyrations (or volatility) in indicator response
4. The PI should not result in unintended consequences
5. The PI is not overly burdensome

As discussed in Section 2.1, five criteria were used for inclusion under RTNSS. By definition, all of the systems in RTNSS have some nexus with safety. However, only the third and fourth criteria directly relate to quantitative measures of risk obtained from the plant PRA model.

Counting type indicators analogous to unplanned scrams per 7000 critical hours and safety system functional failures generally meet the five attributes above for a good PI.

Past indicators such as the SSU which tabulated all causes of system train unavailability, both unplanned (e.g., corrective maintenance) and planned (e.g., preventive) have been shown to have unintended consequences. Figure 2-1 below taken from a historical performance indicator illustrates how the licensee significantly reduced planned maintenance on an important system in order to avoid the indicator turning White. Indicators should not be designed that incentivize

such behavior. The MSPI was formulated so as not to penalize the use of planned maintenance hours up to the pre-planned baseline.

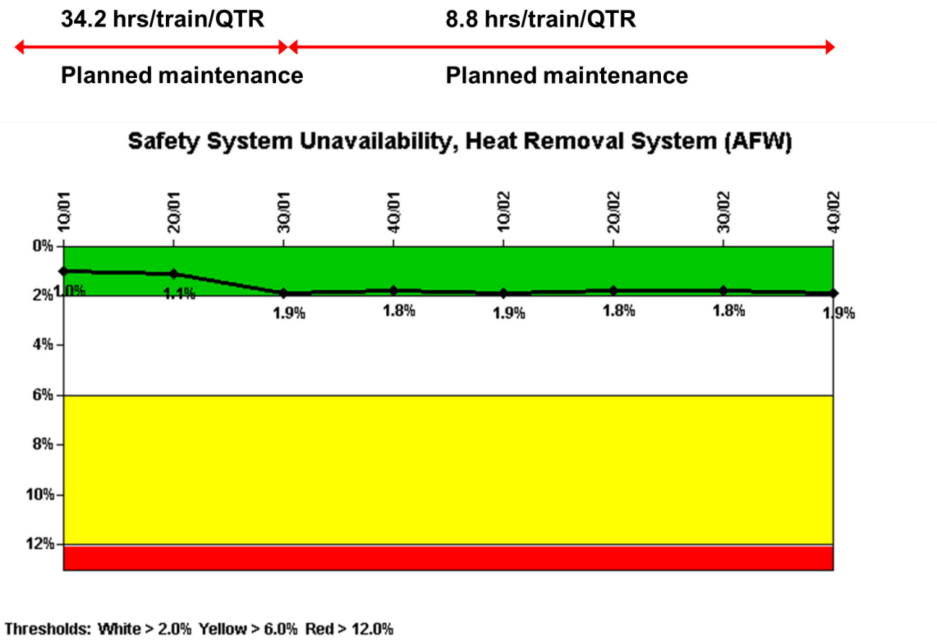

Figure 2-1
Historical Performance Indicator with Unintended Consequences

Table 2-1 of WCAP-15985, Revision 2, lists the non-safety systems that initially failed the focused PRA (i.e., Commission goals may not be met without the system in question), and hence are systems that may be covered by RTNSS:

- Chemical and Volume Control System (CVS)
- Normal Residual Heat Removal System (RNS)
- Startup Feedwater System (SFWS or simply FWS)
- Main AC Power System (ECS) (diesel only)
- Diverse Actuation System (DAS)
- Hydrogen ignitors

The offsite power function can be considered part of Main AC power but, by itself, has low risk importance. Moreover, it is better suited for treatment as an initiator-type indicator rather than a mitigating system PI. Thus, ECS consists primarily of the investment protection standby diesel generators. Non-safety DC power primarily supports DAS. CVS was later screened out in WCAP-15985 based on more detailed consideration and low impact on reactor coolant system leakage and LOCA frequency. Likewise, SFWS was later screened out based on low impact on CDF and LRF.

Some systems have been added to RTNSS to support safety functions 72 hours after an initiating event. However, systems such as Main Control Room Cooling and Instrumentation Room Cooling (mainly fans) are not traditional systems that lend themselves to robust indicators since they are generally low risk-importance support systems in the PRA and have too few components to monitor. Neither would it seem appropriate to include long-term make-up to water storage tanks and the spent fuel pool since there are generally long times available for

such action and numerous pathways.Additional RTNSS systems that may be appropriate for PI include:

- Component Cooling Water System (CCS)
- Service Water System (SWS)

Of the final list of systems in RTNSS for the AP1000, several lack historical industry performance data that could be readily used to establish baselines in an MSPI-type formulation. Still other systems can be expected to have so little in the way of plant-specific performance data in the monitoring period that the PI would not be robust, e.g., a single battery or DC bus failure could cause a large step increase in the indicator, essentially making it binary in nature. There are better assessment tools such as inspection, event response, or the significance determination process for these sorts of failures. DAS, hydrogen igniters, and Non-Class 1E dc (and uninterruptible power supply system) are examples of systems that would not be appropriate for an MSPI-type formulation.

In summary, after assessing all of the systems under RTNSS, the following are finalists for consideration as potential PIs (or MSPIs):

1. Normal Residual Heat Removal System (RNS)
2. Component Cooling Water System (CCS)
3. Service Water System (SWS)
4. Standby Diesel Generators (ECS)

Similar systems to these four, although safety-related, are currently in the MSPI. Further evaluation of the appropriateness of establishing PIs (or MSPIs) for these systems is discussed below.

2.3.1 Appropriateness of RNS for MSPI

RNS consists primarily of two major pumps and associated valves, heat exchangers, instrumentation and controls. Investment protection controls are provided in Table 16.3-2 of the DCD. In operating modes 1 to 3, only 1-of-2 trains needs to be operable. In effect, during full-power operation one train may be inoperable/unavailable for an indefinite period of time. Moreover, the ACTION for the one required train is 72 hr for notification of the chief nuclear officer (or alternate), and 14 days to restore to operable. Should that not be met, additional actions such as interim compensatory measures are required, with a full one month completion time. There is no provision for plant shutdown if these actions are not met.

Hence, these actions would skew the average train unavailabilities compared to the current RHR systems in the MSPI. Industry-averaged train unavailabilities currently used in the MSPI per Reference 1 would not be applicable, and so new baselines would need to be obtained for the AP1000 RNS before implementing the MSPI. Moreover, system performance only has meaning during reactor shutdowns, which may not occur on a consistent yearly or three-year monitoring basis. A system performance indicator during shutdown would be inconsistent with the MSPI, which is an at-power indicator.

Secondly, RNS SSCs individually, and as a system, have very low risk achievement worth (RAW) for power operation (RAW< 2). In an MSPI sort of treatment, these RAWs would result in less than the current 1E-6/yr Green/White threshold given indefinite system unavailability. For the reasons stated above, an MSPI for power operation would not be appropriate.

2.3.2 Appropriateness of CCS for MSPI

While CCS has investment protection controls only during modes 5 and 6, because of potential single-point vulnerability for reactor coolant pump (RCP) cooling, operation with one train at-

power would be minimized to preclude reactor shutdown. However, CCS SSCs individually, and as a system, have very low risk achievement worth (RAW) for power operation (RAW< 2). In an MSPI treatment these RAWs would result in less than the current 1E-6/yr Green/White threshold given indefinite system unavailability. For this reason, the MSPI in its current format, an at-power indicator, would not be appropriate.

2.3.3 Appropriateness of SWS for MSPI

While SWS has investment protection controls only during modes 5 and 6, because of potential single-point vulnerability for RCP cooling, operation with one train at-power would be minimized to preclude reactor shutdown. However, SWS SSCs individually, and as a system, have very low risk achievement worth (RAW) for power operation (RAW< 2). In an MSPI treatment these RAWs would result in less than the current 1E-6/yr Green/White threshold given indefinite system unavailability. For this reason, the MSPI in its current format, an at-power indicator, would not be appropriate.

2.3.4 Appropriateness of Standby DGs for MSPI

Standby DGs have investment protection controls during modes 1 to 5. However, only 1-of-2 DGs need to be operable.

There is no provision for plant shutdown if these actions are not met. Both individually, and collectively as a 2-train “system”, the standby DGs have low risk importance in the full-power PRA (RAW<2). In an MSPI sort of treatment, these RAWs would result in less than the current 1E-6/yr Green/White threshold given indefinite system unavailability. For the reasons stated above, an MSPI for power operation would not be appropriate.

2.3.5 Summary of Appropriateness of MSPI

A systematic review of the systems in RTNSS has been performed. Either because of the lack of relevant industry performance data to serve as baselines, lack of robustness of the performance data being measured, low PRA risk importance, or investment controls that are irrelevant during power operation, an MSPI-type performance indicator is inappropriate for all systems included under RTNSS. As discussed above, an indicator measuring only system or train unavailability could be problematic with regard to the establishment of appropriate performance thresholds given that investment controls allow for one if not both trains of systems to be INOPERABLE indefinitely during various modes of operation.

2.4 Inspection Activities for RTNSS

As discussed in Section 2.2 above, all the important aspects of a cornerstone area are to be inspected where a PI has not been established. In cornerstone areas where the PIs provide only limited indication of performance the inspectable areas should provide indication of the aspects not measured.

The conclusion of Section 2.3 is that an MSPI-type performance indicator is inappropriate for all systems included under RTNSS. However, one cannot rule out the possibility of establishing other sorts of PIs that measure some aspect of SSC performance such as failures or unplanned unavailability, particularly for those systems important during reactor shutdown.

In the absence of good candidate PIs for RTNSS, inspection using risk assessment to determine significance would seem to be the most appropriate activity to undertake until sufficient AP1000 operating experience becomes available. Such activities might include, for example:

- Adherence to investment protection controls per DCD Table 16.3-2
  - Surveillances

    - Completion times
    - Implementation of interim compensatory measures, as necessary
- Implementation of investment protection controls in concert with (a)(4) of the Maintenance Rule, 10 CFR 50.65

3.0 CONCLUSIONS

This report assesses the application of PIs in general and the MSPI in particular to advanced passive designs, such as the AP1000. Counting type indicators analogous to unplanned scrams per 7000 critical hours and safety system functional failures generally meet the attributes for a good PI.

However, practical implementation considerations have been identified with the MSPI if applied to passive SSCs in the AP1000. For one, there are insufficient performance data on passive systems and components to develop meaningful industry-averaged performance baselines that are a key aspect of the MSPI formulation. Robust data for passive system unavailability baselines will not be obtained from the projected fleet of AP1000 reactors for a decade or more. Plant-specific reliability data over a three-year monitoring period for risk-significant passive components may never be sufficient to give a meaningful and robust MSPI value.

A second issue arises with the phasing-in of the MSPI for a new reactor that is starting commercial operation. Historical documents such as NUREG-1753 and NUREG-1816 founded the MSPI based on a three-year monitoring period. The three-year observation period was found to balance the need for good statistics against the need to detect performance changes within a reasonable time. Any option that phases in the MSPI at a newly operating plant before three years of plant-specific performance data have been obtained compromises the original basis of the MSPI.

Given the above discussion, alternatives to the MSPI should be pursued for the passive systems of interest.

Source documents such as WCAP-15985, Revision 2 provide the basis for the selection of systems under the RTNSS process for the AP1000 design. Administrative controls are formatted similar to the TS with operability requirements, applicability, actions and completion times (if operability requirements are not met), surveillance requirements, and bases for the availability controls. There are no limiting conditions for operation if the completion times for required actions are not met. This is a key distinction from standard TS and could, theoretically, impact the average unavailabilities of RTNSS systems and cause divergence from the industry-averaged values for similar (safety-related) systems in the MSPI.

Most RTNSS systems that mimic the traditional active systems in the MSPI (e.g., residual heat removal) have extremely low risk achievement worth. In combination with low CDF for the AP1000, risk-based PIs such as the MSPI would remain Green under virtually all circumstances.

An MSPI-type performance indicator is found to be inappropriate for all systems included under RTNSS. In the absence of good candidate PIs for RTNSS, inspection using risk assessment to determine significance would seem to be the most appropriate activity to undertake until sufficient AP1000 operating experience becomes available.

4.0 REFERENCES

1. NEI 99-02, “Regulatory Assessment Performance Indicator Guideline,” Rev. 7, Nuclear Energy Institute, 2013.
2. NUREG-1753, “Risk-Based Performance Indicators: Results of Phase 1 Development,” U.S. Nuclear Regulatory Commission, April 2002.
3. U.S. Nuclear Regulatory Commission, Interoffice Memorandum from Scott F. Newberry (RES/DRAA) to John A. Zwolinksi (NRR), “Request for Review of Mitigating Systems Performance Indices White Paper,” May 12, 2003. (Adams Accession No. ML031350208 and ML031360121).
4. NUREG-1816, “Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for the Pilot Plants, Final Report,” U.S. Nuclear Regulatory Commission, February 2005.
5. SECY-10-0121,”Modifying the Risk-Informed Regulatory Guidance for New Reactors,” and associated Staff Requirements Memorandum, U.S. Nuclear Regulatory Commission (Adams Accession No. ML102230076 and ML110610166), 2010 and 2011, respectively.
6. U.S. Nuclear Regulatory Commission, “Summary of Public Meeting Held on October 26, 2011, to Further Discuss Key Points from Tabletop Exercises for New Reactor Risk Applications in the Reactor Oversight Process (ROP),” (Adams Accession No. ML11308A310, ML11308A354, and ML11308A379), 2011.
7. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter (IMC) 2519, “Construction Significance Determination Process,” Appendix A, p. 10, 2013.
8. NUREG/CR-6928, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, 2007.
9. Regulatory Guide 1.177, “An Approach for Plant-Specific, Risk Informed Decisionmaking: Technical Specifications,” U.S. Nuclear Regulatory Commission, August 1998.
10. “Advanced Light Water Reactor Utility Requirements Document, Volume 3, Revision 8: ALWR Passive Plant,” TR-016780-V3R8, Electric Power Research Institute, Palo Alto, CA, 1999.
11. NUREG-1793, Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design (NUREG-1793, Initial Report), U.S. Nuclear Regulatory Commission, 2004.
12. WCAP-15985, Revision 2, “AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process,” Westinghouse Electric Co., August 2003.
13. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter (IMC) 0305, “Operating Reactor Assessment Program,” 2015.
14. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter (IMC) 0308 Attachment 2, “Technical Basis for Inspection Program,” 2006.