NRC Staff White Paper
Mitigating Systems Performance Indicators for New Reactor

ROP Working Group

Executive Summary

The purpose of this white paper is to explore viable options for the selection and monitoring of the mitigating systems for the Westinghouse AP1000 simplified advanced light water reactor plant design.

The passive safety system design of the AP1000 is significantly different from the active safety systems of the current fleet. As such, direct application of the active and mechanical-equipment-focused MSPI framework to the AP1000 design is not practical without changes to its scope and formulation. This paper uses the available NEI and NRC Commissioners' guidance and AP1000 design information to identify options for the scope and methods to monitor the mitigating systems.

This paper proposes to maintain the current MSPI risk thresholds for the AP1000 monitored systems consistent with the NRC Commissioners' direction. It also recognizes that the current statistically-based performance limits may be more valuable due to the expected increase in risk margin associated with the AP1000 design and includes as options the tightening of the performance limits and the consideration of the use of a short-term performance limit. As the current performance-based limits were originally designed to limit false positives, it is recognized that any limit tightening would require careful analysis of both the benefits and potential adverse consequences of this action. Although options to change the performance-based limits are included, such changes do not achieve the desired risk-informed focus of the indicators.

Monitoring of the active safety-related valves associated with the Refueling Water Storage Tank, Recirculation Sump, Passive Residual Heat Removal System and the Automatic Depressurization System is proposed as an option. However, test indicators developed in this paper show that the high reliability of these valves and relatively low Birnbaums point to the need to re-evaluate the constrained non-informative prior (CNIP) update process that is currently used by the MSPI program. The seven test indicators developed for this paper include consideration of the CNIP and an alternate data processing approach known as the Maximum Likelihood Estimation (MLE). Of the seven test indicators, when the MLE is used, five were sensitive enough to cross thresholds as the number of failures are increased.

The test indicators were developed to address a single component type with no system boundary limitations. This variation from the current functional-based approach is believed to maximize the data population and helps to address the limited demands associated with many of the candidate components.

Two primary approaches for establishing the monitoring scope are investigated: Plant Risk-Informed Scope and MSPI Functional-Based Scope.

The Plant Risk-Informed Scope approach focuses on identifying AP1000 safety and non-safety systems that are significant risk contributors. It risk-informs the system selection as opposed to the deterministic system selection process used for the current fleet. This approach also included consideration of systems and/or functions included within the scope of the regulatory

treatment of non-safety systems (RTNSS). However, for the AP1000, no RTNSS functions were found to have a high enough risk significance to result in sensitive indicators.

In support of this white paper, an audit of the Westinghouse AP1000 PRA basic event importance ranking was performed. Insights gained from this audit were used in the function selection process and to test various indicator options.

The paper shows that the use of a risk-informed scope could result in the addition of functions that have not been previously monitored and the inclusion of some non-safety related systems and components is possible.

The second approach considered, the MSPI Functional-Based Scope approach, focuses on identifying AP1000 systems consistent, to the extent possible, with the NEI 99-02 guidance. This approach would likely require some modifications to the current MSPI guidance due to the safety system configurations of the AP1000.

A limited assessment of potential guidance changes was performed and additional changes to those currently identified will be needed as the final set of options for MSPI implementation is selected.

A total of 12 options associated with the implementation of AP1000 mitigation system monitoring were identified including two associated with the approach for identifying the system scope, four associated with the deterministic performance limits, four associated with the monitoring of non-safety-related equipment, and two associated with the processing of data (i.e., the use of MLE instead of the CNIP, and component focused indicators). Although some insights were gained from the test indicators, this paper does not make any final recommendations as to the preference of these options.

Two areas requiring additional analysis were also identified: an assessment of the benefits and impact of tightening the performance-based limits, and a comprehensive assessment of the effectiveness of MLE. Other assessments may be required as the identified options are refined.

Table of Contents

1. Purpose

The purpose of this white paper is to explore options for a framework for the AP1000 Mitigating System Performance Index (MSPI) indicators. This paper addresses the approach for risk limits, identifies the candidate AP1000 systems and components for inclusion into the MSPI, develops several test indicators and identifies potential changes to the MSPI guidance document, NEI 99-02 [Reference 1]. It also includes a summary of NRC Commissioners' guidance associated with the implementation of a MSPI for new reactors and associated discussion demonstrating consistency with this guidance.

2. AP1000 Design

The AP1000 Design Control Document (DCD) states that the AP1000 safety systems are designed to maximize the use of natural driving forces such as pressurized nitrogen, gravity flow and natural circulation flow and do not rely on active components such as pumps, fans or diesel generators. It also states that a minimum number of valves are used for the purpose of initially aligning the safety systems. [Reference 2]

It further states that the safety systems are designed to function without safety-related support systems such as alternating current, component cooling water, services water, heating, ventilation and air conditioning. Safety-related direct current (dc) power is provided to support reactor trip and engineered safeguards actuation. Batteries are sized to provide the necessary dc power and uninterruptible as power for items such as the protection and safety monitoring system actuation, the control room functions including habitability, dc-powered valves in the passive safety-related systems and containment isolation. [Reference 2]

It is the use of these passive safety systems that makes the direct application of the existing MSPI framework difficult and for this reason a modified approach is required. Several options are presented for the identification and monitoring of the AP1000 mitigating systems.

3. Commission Guidance

3.1. SECY-10-0121, Modifying the Risk-Informed Regulatory Guidance for New Reactors

In the Staff Requirement Memorandum (SRM) on SECY-10-0121, dated March 2, 2011 [References 3 and 4], the Commission reaffirmed that the existing safety goals, safety performance expectations, subsidiary risk goals and associated risk guidance (such as the Commission's 2008 Advanced Reactor Policy Statement and Regulatory Guide 1.174), and key principles and quantitative metrics for implementing risk-informed decision making, are sufficient for new plants. The SRM also stated that the Commission expects that the advanced technologies incorporated in new reactors will result in enhanced margins of safety and that new reactors with these enhanced margins and safety features should have greater operational flexibility than current reactors. This flexibility will provide for a more efficient use of NRC resources and allow a fuller focus on issues of true safety significance.

3.2. SECY-12-0081, Risk-Informed Regulatory Framework for New Reactors

SECY-12-0081 [Reference 5] states that the existing MSPI would not be adequate and would be largely ineffective in providing meaningful input to the risk-informed regulatory decision-making process for new reactor designs. The SECY documents numerous case studies that demonstrated this shortfall. The case studies demonstrated that it would be extremely rare to cross greater-than-green MSPI thresholds that would result in an increased regulatory response for active new reactor designs, and a meaningful MSPI may not even be possible for passive systems using the current formulation of the indicator. The existing performance limit approach, which incorporates a backstop that indicates when the performance of a monitored component in an MSPI system is significantly lower than expected industry performance, would play a more significant role and could potentially be emphasized and modified for the active new reactor designs.

The SECY states that it would take greater than 25 emergency diesel generator (EDG) start failures or greater than 25 EDG run failures for the U.S. Evolutionary Power Reactor (U. S. EPR) to exceed the green-white risk threshold, and 12 failures to reach the performance limit. In another case, it would take 14 or more turbine-driven emergency feedwater pump failures or greater than 25 motor-driven pump failures for the US-APWR to exceed the green-white threshold using the licensee’s PRA model, and the performance limit would not be exceeded until 6 or more pump failures in a 3-year timeframe occurred. Taken as a whole, it would be highly improbable to have a greater-than-green indicator for any MSPI system at any of the new reactor facilities, even taking into account the performance limit (backstop) as it is currently formulated. Therefore, the existing MSPI would provide little if any insight into plant performance for new reactors and would not trigger an appropriate regulatory response to address performance issues. The staff determined that alternate performance indicators (PIs) in the mitigating systems cornerstone could potentially be developed and/or additional inspection could be used to supplement insights currently gained through MSPI.

SECY-12-0081 states that as the result of tabletop exercises, the staff developed three options for applying the risk-informed regulatory framework of the ROP to new reactors. These options were:

- 3A Use as is (status quo)
- 3B Augment Existing Processes with deterministic backstops
- 3C Develop deterministic tools

The staff recommended Option 3B. In the SRM on SECY-12-0081 [Reference 6], the Commission directed the staff to give consideration to the use of relative risk metrics, or other options, that would provide a more risk-informed approach to the determination of the significance of inspection findings for new reactors. The Commission also requested:

1. A technical basis for the staff’s proposal for the use of deterministic backstops, including examples;

2. A technical evaluation of the use of relative risk measures, including a reexamination of the pros and cons listed in the staff's 2009 white paper;
3. A discussion of the appropriateness of the existing performance indicators and the related thresholds for new reactors.

3.3. SECY-13-0137, Recommendations for Risk-Informing the Reactor Oversight Process for New Reactors

SECY-13-0137 [Reference 7] addresses the requested information contained in the SRM on SECY 12-0081. SECY 13-0137: clarified the staff's proposal for use of deterministic backstops replacing the "deterministic backstop" term with "qualitative measures," concluded that the relative risk approach's short comings outweigh its benefits, and noted that a risk-informed alternative would need to be developed for new reactors.

In SRM on SECY-13-0137 [Reference 8] dated June 30, 2014, the Commission stated:

- The staff should develop appropriate Performance Indicators (PIs) and thresholds for new reactors, specifically those PIs in the Initiating Events and Mitigating Systems cornerstones, or develop additional inspection guidance to address identified shortfalls to ensure that all cornerstone objectives are adequately met.
- The staff should develop, with appropriate stakeholder input, the necessary updates to the PIs, including any new PIs or changes to thresholds, and submit them to the Commission for approval prior to power operation for the first new reactor units.
- The Commission noted that the overall structure of the existing ROP should be preserved. The staff should notify the Commission through the annual report on the ROP self-assessment if they identify any further changes that are necessary, once the staff has gained operating experience with the new Generation III+ plants.

This SRM is the latest Commission guidance to the staff on the ROP for new reactors.

4. MSPI Risk Thresholds

NEI 99-02 defines the MSPI risk-informed decision rules for assigning a performance color as:

MSPI $\leq$ 1.0e-06	Green
MSPI > 1.0e-06 AND $\leq$ 1.0e-05	White
MSPI > 1.0e-05 AND $\leq$ 1.0e-04	Yellow
MSPI > 1.0e-04	Red

As stated in the Commission's SRM on SECY-10-0121, the Commission expects that the advanced technologies incorporated in new reactors will result in enhanced margins of safety and that new reactors with these enhanced margins and safety features should have greater operational flexibility than current reactors. This flexibility will provide for a more efficient use of NRC resources and allow a fuller focus on issues of true safety significance.

Therefore, this white paper proposes to maintain the current MSPI risk thresholds for the systems monitored by the MSPI program for the AP1000. As such it is expected that a larger risk margin will likely be available to the AP1000 due to its low calculated core damage frequency. Consistent with the Commission's direction, this added margin will provide increased operational flexibility.

Also, as found in case studies summarized in SECY-12-081, it is anticipated that component failures or train unavailability will challenge greater than green thresholds for new design plants much less frequently than the current operating designs. This should not be seen as a weakness of the indicator but as a strength of the low risk profile of the AP1000 design.

5. MSPI Performance-Based Limits

The MSPI Performance-Based Limits are described in Section F.4 of NEI 99-02 which states that these limits are for MSPI-monitored components with low Birnbaum values where significant degradation in performance could occur before the risk significance reaches a point where the MSPI would cross the white boundary.

NUREG 1816 [Reference 9] states that those components for which a large number of failures would be needed to produce a change in the MSPI that is greater than 1x10-6/yr have come to be called "insensitive indicators." However, what constitutes a "large" number of failures can be subjective. For the sole purpose of performing sensitivity studies to identify possible solutions to the insensitive indicator issue, the NRC staff used a condition of "more than 20 failures" in the original definition.

Although this limit is rarely tripped for current reactors, it may become the primary mechanism for exceeding an MSPI limit for the AP1000 as the Birnbaums for the identified components will generally be low. Therefore, it is anticipated that the MSPI performance-based limits could play a more significant role in the monitoring program for the AP1000.

5.1. MSPI Performance-Based Limits Bases

As stated in NUREG 1816 Appendix E [Reference 9], the performance-based limit or backstop is a limit on the total number of failures on the monitored components. It was formulated to have the following properties:

- Probability of false positive is less than or equal to 0.01
- The fraction of positives that are false is less than or equal to 5%

The backstop is designed to ensure that false positives are very rare, and if a positive occurs it is very probably a true positive.

The process used to develop these limits as documented in NUREG 1816 is described as follows:

For each system/component/failure-mode/data-period, the empirical Bayes (EB) distribution was found, modeling between-plant variation in either p (for failure to start, failure to load and run, or failure to open or close) or λ (for failure to run). The plant-specific means were tabulated. Each pilot plant-specific mean represents a "best estimate" of the parameter at the plant during the 3-year period.

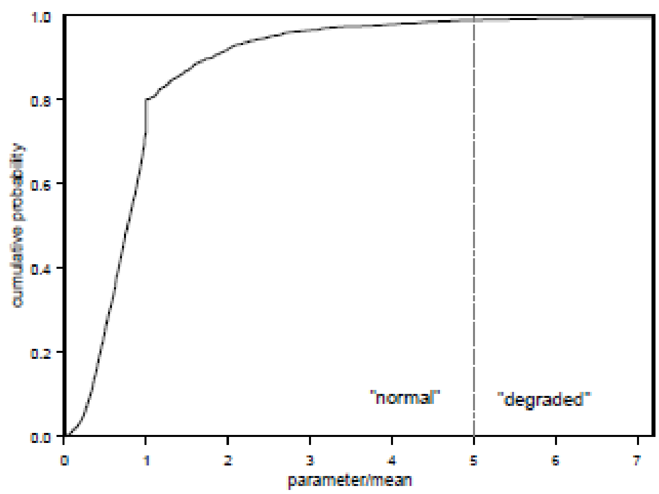
For each system/component/failure-mode/data-period, the EB means were rescaled by dividing them by the industry mean. This put all the parameters on the same scale, with mean 1. For two system/component/failure-mode/data-periods, the EB distribution was degenerate, showing no "between-plant" variability. For these two cases, every plant-specific parameter was assigned a rescaled value of 1.

The rescaled plant-specific means were pooled into a single data set, with 2388 values associated with the 20 pilot plants. The smallest value was 0.016 and the largest value was 24.05.

The values were ordered from smallest to largest, and the empirical cumulative distribution was plotted. This is shown in Figure E.2.

Empirical Distribution of Rescaled Plant-Specific Parameters

(from NUREG 1816 Figure E.2)



Parameter values less than 5 times the industry mean were considered "normal." Values that are more than 5 times the industry mean were considered "degraded." This resulted in the following formulation:

Backstop = 4.65 (Expected Number of Failures) + 4.2

Based on this formulation, if zero failures are expected over a three-year period, then the backstop is 4 failures; if one failure is expected then the backstop is 9 failures. Any reduction in this formulation would require a reassessment of the governing properties.

5.2. Short-term Backstop

As stated in NUREG 1816, a short-term backstop was investigated. The definition of this backstop is the same as the performance-based limit backstop discussed above except the time period for collecting data is only six months. An assessment of the pilot plant data was performed and documented in NUREG 1816 and it was found that the expected number of failures had a very short range, from 0.0 to 0.4 and the resulting backstop was 4 or 5 for nearly all systems at nearly all plants.

5.3. Backstop Options

As the backstop by definition is not risk-informed, any adjustment would not create a risk-informed indicator; it would only compensate for the insensitive risk-informed indicators. Therefore, the first option is to make no adjustments **[OPTION PLE-1]**. The backstop can be adjusted through the addition of the short-term backstop **[OPTION PLE-2**] or by reducing the margin on the current backstop **[OPTION PLE-3**] or by doing both **[OPTION PLE-4]**. Implementing a short-term backstop would enable a shorter implementation period (from plant startup to valid indicator) as the current backstop uses a three year rolling data window. If a reduction in the three-year or six-month performance indicator is desired in order to enhance its ability to detect degraded performance, then additional analysis will be required to determine the change in false positives that could result.

6. MSPI Applicable Plant Modes

The current MSPI scope addresses internal at-power events. Although this scope is not stated clearly in the NEI 99-02 guidance, it can be inferred from the guidance on unavailability monitoring in Section F 1.2.1 which states that train/segment unavailability is the ratio of hours in test and maintenance to the number of critical hours; the guidance on the calculation of core damage frequency (CDF) in Section F 1.3.2 which defines the CDF used in the formulation of MSPI as being the internal events, average maintenance, at-power value; and the guidance on PRA requirements in Section G 2 which states that the MSPI is an index that is based on internal initiating events, full-power PRA.

To maintain consistency with the current MSPI guidance, risk-significant systems that support functions other than those mitigating at-power internal events are excluded in this paper from consideration as MSPI-monitored functions.

7. Regulatory Treatment of Non-Safety Systems (RTNSS)

The RTNSS process applies broadly to those non-safety-related SSCs of advance reactors that perform risk-significant functions and, therefore, are candidates for regulatory oversight. See SECY 94-084 [References 10 and 11] and SECY 95-132 [References 12 and 13] for a detailed discussion on RTNSS. The RTNSS process is included in this paper as a potential source of systems that should be considered for MSPI.

RG 1.206 Section C.IV.9.3.6, Regulatory Oversight Evaluation, states that following the identification of RTNSS, the Combined License (COL) applicant should conduct the following activities to determine the means of appropriate regulatory oversight for the RTNSS-important non-safety systems:

• review the FSAR, the PRA, and audit plant performance calculations to determine whether the design of the risk-significant, non-safety-related SSCs satisfies the performance capabilities and reliability / availability missions

• review the FSAR information to determine whether it includes the proper design information for the reliability assurance program, including the design information for implementing the Maintenance Rule

• review the FSAR information to determine whether it includes proper short-term availability control mechanisms if required for safety and determined by risk significance.

SECY 94-084 recommended an operational reliability assurance program (O-RAP) for plant SSCs that are risk-significant (or significant contributors to plant safety). The scope of proposed O-RAP included RTNSS SSCs. In the SRM on SECY 94-084, the Commissioners disapproved the recommendation to require an O-RAP and stated that the objectives of the O-RAP should be incorporated into existing programs for maintenance or quality assurance. Therefore, RTNSS SSCs are included in the maintenance rule methodology for performance monitoring and the quality assurance program for design and operational errors through a COL action item.

As risk-significant non-safety systems within the scope of the RTNSS process require regulatory treatment including monitoring within the scope of the Maintenance Rule, this white paper includes the consideration of these risk-significant non-safety systems within the scope of the MSPI program for the AP1000. The identification of AP1000 RTNSS systems is discussed later in this paper.

8. MSPI System Scope

As stated in NEI 99-02 and NUREG-1816, the purpose of the MSPI is to "monitor the performance of selected systems based on their ability to perform risk-significant functions."

For current reactors, the MSPI covers six mitigating systems and five indicators: emergency ac power (EAC), high pressure injection (HPI), heat removal system (HRS), residual heat removal (RHR), and service water system/component cooling water (SRW/CCW). These systems are consistent with the previous Safety System Unavailability (SSU) indications with the exception of the cooling water indicator. The SRW/CCW systems were added to explicitly address this important contributor to plant safety for MSPI-supported components. The selected systems for current BWRs and PWRs are summarized in the following table.

MSPI Monitored Systems

Description	BWR	PWR
Emergency AC Power	EAC	EAC
High Pressure Injection	HPCI/HPCS/FCI	HPSI
Heat Removal System	RCIC/IC	AFW/EFW
Residual Heat Removal	RHR	RHR
Cooling Water	SRW/CCW	SRW/CCW

9. Monitored Functions Guidance

Section F5 of NEI 99-02 identifies the potential monitored functions for each system included within the scope of the MSPI. The NEI guidance is summarized below:

System	Guidance
Emergency AC Power System	Power to Class 1E Systems
High Pressure Injection	Maintains reactor coolant inventory at high pressure
Heat Removal	For PWRs, to provide decay heat removal via the steam generators.
Residual Heat Removal System	For long-term decay heat removal function
Cooling Water Support System	Support function for the four front-line monitored systems. Includes direct cooling functions provided by service water and component cooling water or their cooling water.

10. MPSI Function - Emergency AC Power

The AP1000 does not have safety-related emergency ac diesel generators as these are not needed for the operation of the passive safety-related mitigation systems. However, the AP1000 does include on-site diesel generators for defense-in depth.

This paper investigates an option to monitor the two defense-in-depth onsite standby diesel generators.

10.1. Onsite Standby Diesel Generators

The AP1000 has two onsite standby diesel generator units, each furnished with its own support subsystems, in order to provide power to selected plant non-safety-related ac loads. Power supplies to each diesel generator subsystem components are provided from separate sources to maintain reliability and operability of the onsite standby power system. These onsite standby diesel generator units and their associated support systems are classified as AP1000 Class D, defense-in-depth systems. [Reference 15]

The onsite standby diesel generator function to provide a backup source of electrical power to onsite equipment needed to support decay heat removal operation during reduced reactor coolant system inventory and midloop operation. The diesels are identified as performing an important non-safety-related function and are included in the Investment Protection Short-Term Availability Controls. [Reference 15]

10.2. Ancillary AC Diesel Generators

The AP1000 has two ancillary ac diesel generators located in the annex building that provide power for Class 1E post-accident monitoring, MCR lighting, MCR and divisions B and C I&C room ventilation and for refilling the PCS water storage tank and the spent fuel pool when no other sources of power are available. The ancillary generators are not needed for refilling the PCS water storage tank, spent fuel pool makeup, post-accident monitoring or lighting for the first 72 hours following a loss of all other ac sources. [Reference 15]

The generators are classified as AP1000 Class D. The generators are commercial, skid-mounted, packaged units and can be easily replaced in the event of a failure. Generator control is manual from a control integral with the diesel skid package. These generators are located in the portion of the Annex Building that is a Seismic Category II structure. Features of this structure which protect the function of the ancillary generators are analyzed and designed for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles. [Reference 15] The inclusion of the ancillary generators is not recommended by this paper as they provide no contribution to reducing the calculated core damage frequency.

11. MSPI Function - High Pressure Injection

The AP1000 does not use high pressure injection. Its alternate approach is to depressurize the RCS and to maintain RCS inventory through Its passive core cooling system consisting of accumulators, an in-containment refueling water storage tank and associated valves.

For purposes of MSPI, the passive core cooling system has been divided into two functional categories: Heat Removal and High Pressure Injection.

Heat Removal:	Core Makeup Tanks, Passive Residual Heat Removal Exchangers
High Pressure Injection:	Automatic Depressurization System (ADS), In-containment Refueling Water Tank, Accumulators

Although the MSPI monitored function is high pressure injection, this paper uses the combination of the ADS and the in-containment tanks and valves of the passive core-cooling system as the systems to be monitored for the MSPI injection function in its example of functional-based scoping described later in this paper. If this functional mapping is adopted, the high pressure MSPI function as described in NEI 99-02 would need to be broadened.

This white paper identified the active components associated with the Automatic Depressurization System and In-containment Refueling Water Storage Tank as potential MSPI monitored components. The Accumulators are excluded as there are no active components associated with their safety function.

11.1. Automatic Depressurization System

The automatic depressurization system consists of four different stages of valves. The first three stages each have two lines and each line has two valves in series; both normally closed. The fourth stage has four lines with each line having two valves in series; one normally open and one normally closed. The four stages, therefore, include a total of 20 valves. The four valve stages open sequentially. [Reference 16]

The first stage, second-stage and third-stage valves have dc motor operators. The stage 1/2/3 control valves are normally closed globe valves; the isolation valves are normally closed gate valves. The fourth-stage valves are interlocked so that they cannot open until reactor coolant system pressure has been substantially reduced. The fourth stage control valves are squib valves. There is a normally open motor-operated gate valve in series with each squib valve. [Reference 16]

The first three stages have a common inlet header connected to the top of the pressurizer. The outlet of the first to third stages then combine to a common discharge line to one of the spargers in the in-containment refueling water storage tank. There is a second identical group of first- to third-stage valves with its own inlet and outlet line and sparger. [Reference 16]

The fourth-stage valves connect directly to the top of the reactor coolant hot leg and vent directly to the steam generator compartment. There are also two groups of fourth stage valves, with one group in each steam generator compartment. [Reference 16]

The automatic depressurization valves are designed to automatically open when actuated and to remain open for the duration of an automatic depressurization event. Valve stages 1 and 4 actuate at discrete core makeup tank levels, as either tank's level decreases during injection or from spilling out a broken injection line. Valve stages 2 and 3 actuate based upon a timed delay after actuation of the preceding stage. This opening sequence provides a controlled depressurization of the reactor coolant system. The valve opening sequence prevents simultaneous opening of more than one stage, to allow the valves to sequentially open. The valve actuation logic is based on two-of-four level detectors, in either core makeup tank for automatic depressurization system stages 1 and 4. [Reference 16]

The stage 1/2/3 automatic depressurization control valves are designed to open relatively slowly. During the actuation of each stage, the isolation valve is sequenced open before the control valve. Therefore, there is some time delay between stage actuation and control valve actuation. [Reference 16]

11.2. Accumulators

The two accumulators contain borated water and a compressed nitrogen cover gas to provide rapid injection. They are located inside the reactor containment and the discharge from each tank is connected to one of the direct vessel injection lines. These lines connect to the reactor vessel downcomer. [Reference 16]

11.3. In-containment Refueling Water Storage Tank

The in-containment refueling water storage tank is located in the containment at an elevation slightly above the reactor coolant system loop piping. Reactor coolant system injection is possible only after the reactor coolant system has been depressurized by the automatic depressurization system or by a loss of coolant accident. Squib valves in the in-containment refueling water storage tank injection lines open automatically on a 4th stage automatic depressurization signal. Check valves, arranged in series with the squib valves, open when the reactor pressure decreases to below the in-containment refueling water storage tank injection head. [Reference 16]

12. MSPI Function – Heat Removal

The AP1000 uses a passive core cooling system that provides a means for depressurizing the RCS and passive inventory control. Also included within this system is the capability to remove both heat immediately following a trip and long-term residual heat.

The AP1000 safety function for heat removal is addressed in this paper by residual heat removal section as the same AP1000 passive cooling systems perform both functions.

The AP1000 also includes two motor-driven startup feedwater pump trains. These pump trains are non-safety grade for the function of providing heat removal. This white paper investigated the inclusion of these pumps into the MSPI scope.

12.1. Startup Feedwater

The startup feedwater system supplies feedwater to the steam generators during plant startup, hot standby and shutdown conditions, and during transients in the event of main feedwater system unavailability. The startup feedwater system is composed of components from the AP1000 main and startup feedwater system (FWS) and steam generator system (SGS). [Reference 17]

In the event of loss of the main feedwater system, the startup feedwater pumps automatically supply feedwater to the steam generators for heat removal from the reactor coolant system. The heat removal function of the startup feedwater system is non-safety-related. The startup feedwater system avoids the need for actuation of the safety-related passive core cooling system. Following the transient, the system refills the steam generators and supports reactor coolant system cooldown. [Reference 17]

The inclusion of the startup feedwater system is not recommended as the pumps provide no contribution to reducing the calculated core damage frequency.

13. MSPI Function - Residual Heat Removal

This white paper proposes an option to include the active components associated with the Passive Residual Heat Removal Heat Exchanger and Core Makeup Tanks as part of the MSPI monitored components.

13.1. Passive Residual Heat Removal Heat Exchanger

The passive residual heat removal heat exchanger is designed to remove sufficient heat so that its operation, in conjunction with available inventory in the steam generators, provide reactor coolant system cooling and prevents water relief through the pressurizer safety valves during loss of main feedwater or main feedline break events. [Reference 16]

Passive residual heat removal heat exchanger flow and inlet and outlet line temperatures are monitored by indicators and alarms. The operator can take action, as required, to meet the technical specification requirements or follow emergency operating procedures for control of the passive residual heat removal heat exchanger operation. [Reference 16]

13.2. Core Makeup Tanks

The core makeup tanks automatically provide injection to the reactor coolant system as the temperature decreases and pressurizer level decreases, actuating the core makeup tanks. The passive core cooling system can maintain stable plant conditions for a long time in this mode of operation, depending on the reactor coolant leakage and the availability of ac power sources. For example, with a technical specification leak rate of 10 gpm, stable plant conditions can be maintained for at least 10 hours. With a smaller leak a longer time is available. However, in scenarios when ac power sources are unavailable for as long as 24 hours, the automatic depressurization system will automatically actuate. [Reference 16]

13.3. Normal Residual Heat Removal System

The AP1000 contains a normal Residual Heat Removal System (RNS) with its heat removal function stated as non-safety-related and is not required to operate to mitigate design basis events. However, the RNS does perform the following safety-related functions:

- containment isolation of RNS lines penetrating containment using containment isolation valves according to the criteria specified in DCD Tier 2, Section 6.2.3

- preservation of the RCS pressure boundary integrity using pressure isolation valves according to the criteria specified in DCD Tier 2, Section 5.4.8
- provide a flow path for long-term, post-accident makeup to the containment inventory

The normal residual heat removal system also provides low pressure makeup from the cask loading pit to the reactor coolant system. The system is manually initiated by the operator following receipt of an automatic depressurization signal. If the system is available, it provides reactor coolant system makeup once the pressure in the reactor coolant system falls below the shutoff head of the normal residual heat removal system pumps. The system provides makeup from the cask loading pit to the reactor coolant system and provides additional margin for core cooling. [Reference 18]

The injection function described above was determined to be RTNSS by WCAP-15985 [Reference 13].

14. MSPI Function – Cooling Water

As stated in Section F.5 of NEI 99-02, the functions monitored for the cooling water support system are those that are necessary to provide for direct cooling of the components in MSPI monitored trains or segments of systems supported by the cooling water system.

The AP1000 non-safety-related service water system supplies cooling water to remove heat from the non-safety-related components cooling water system. The component cooling water system provides cooling to the following components: RCPs, Letdown Heat exchanger, Reactor coolant Drain Tank Heat Exchanger, RHR Pumps, RHR Heat Exchangers, SFP Heat Exchangers, Chillers, Sample Heat Exchanger, CVS Miniflow heat exchanger, air compressors, condensate pump oil coolers. [Reference 19]

Cooling functions typically performed by cooling water that are excluded from the AP1000 design are diesel generator cooling (diesels are non-safety-related and air cooled), high pressure injection pump cooling (RCS is depressurized by ADS and inventory control is passive), RCP seal cooling (pumps are sealless with all rotating components inside a pressure vessel), and residual heat removal (passive core cooling system).

The inclusion of the AP1000 non-safety-related component cooling water is only for the support of the non-safety-related normal residual heat removal system. Based on the Westinghouse RTNSS assessment, normal residual heat removal is included only for low pressure RCS injection of cask loading pit water into the RCS following ADS actuation. Although cooling is required for pump operation, cooling water systems are not identified as RTNSS for at-power operation.

This paper investigates an option to monitor the component cooling and service water systems.

15. AP1000 Passive Safety System Valves

The proposed components to be monitored for the AP1000 include the active valves contained within the passive cooling system.

There are four types of remote operated valves within the AP1000 passive cooling system that could be potentially included within the AP1000 scope of MSPI. These are categorized as follows:

- Squib Valves — Explosively Opening
- MOV Active — Motor Operated Valves that change state to perform safety function
- MOV Passive — Motor Operated Valves that do not change state to perform safety function
- AOV Active — Air Operated Valves that change state to perform safety function

The following table summarizes the type and number of valves contained within the passive cooling systems.

System	Squib Valves	MOVs Active	MOVs Passive	AOVs Active	Total
CMT			2	4	6
Accumulators[1]			2		2
RWST	4		2		6
Recirc Sump	4		2		6
PRHRHX			1	4	5
ADS	4	12	4		20
TOTAL	**12**	**12**	**13**	**8**	**45**

Note 1: Accumulators are screened due to lack of active components.

The above table shows a total of 45 valves with 13 being passive and therefore excluded from monitoring. This results in a total of 32 valves as potential components to be monitored within the scope of the MSPI program.

Table 6.3-1, reproduced from the AP1000 DCD [Reference 16] lists the remote actuation valves contained in the passive core cooling system.

Table 6.3-1 **PASSIVE CORE COOLING SYSTEM - REMOTE ACTUATION VALVES**				
	Normal Position	**Actuation Position**	**Failed Position**	**Notes**
Core Makeup Tanks CMT inlet isolation MOV (V002A/B) CMT outlet isolation AOV (V014A/B,V015A/B)	Open Closed	Open Open	As is Open	(1,4)
Accumulators Accumulator discharge MOV (V027A/B)	Open	Open	As is	(2,4)
In-Containment Refueling Water Storage Tank IRWST injection line MOV (V121A/B) IRWST injection line squib (V123A/B, V125A/B)	Open Closed	Open Open	As is As is	(2,4)
Containment Recirculation Sump Valves Recirculation line MOVs (V117A/B) Recirculation line squib valves (V118A/B, 120A/B)	Open Closed	Open Open	As is As is	(2,4)
Passive Residual Heat Removal Heat Exchanger PRHR HX inlet MOV (V101) PRHR HX outlet AOVs (V108A/B) IRWST gutter isolation AOVs (V130A/B)	Open Closed Open	Open Open Closed	As is Open Closed	(2,4)
Automatic Depressurization System Valves ADS Stage 1 MOVs (V001A/B, V011A/B) ADS Stage 2 MOVs (V002A/B, V012A/B) ADS Stage 3 MOVs (V003A/B, V013A/B) ADS Stage 4 MOVs (V014A/B/C/D) ADS Stage 4 squib valves (V004A/B/C/D)	Closed Closed Closed Open Closed	Open Open Open Open Open	As is As is As is As is As is	(3)

<u>Notes</u>:
(1) These valves are normally in the correct post-accident position, but receive confirmatory actuation signals to redundant controllers.
(2) These valves are normally in the correct post-accident position with their power locked out. They also receive confirmatory actuation signals.
(3) These valves are normally in the correct post-accident position, but receive confirmatory actuation signals.
(4) The operation of these valves is not safety-related.

16. Valve Test Frequency

16.1. Squib Valves

It is anticipated that the 12 squib valves identified as potential components to be monitored will be tested very infrequently and therefore will have limited demands during a given three-year window.

ASME Operation and Maintenance of Nuclear Power [Reference 20] states that squid valves are Category D valves and are excluded from the in-service test requirements of once every 92 days (3 months). Section ISTC-5260 states that 20% of the charges of explosively actuated valves are to be tested every 2 years.

In addition, a squib continuity test for each valve every two years is included as a license condition for the new plants.

It is assumed that these tests (explosive charge test and continuity test) will be performed during outage periods. For the 12 squib valves per unit, it is estimated that there would be 12 continuity tests and 3 explosive charge tests every two years. Therefore, a three-year period will either have 15 demands (one outage) or 30 demands (two outages) depending on the start and stop date of the moving reporting window and the timing of the outages.

This demand frequency is significantly less than that of other components such as the emergency diesel generators of the current fleet which average approximately 50 demands per year or 150 demands per three-year period.

The impact of this low demand frequency would need to be assessed to ensure that the monitoring of the squib valves will produce a viable indicator.

16.2. Motor Operator Valves

According to the AP1000 technical specifications, the in-service testing (IST) program should followed. ASME Table ISTC-3500-1 states that Category A and B valves should be tested every 3 months. A Category A valves are valves for which seat leakage is limited to a specified maximum amount in the closed position for fulfillment of their required function(s). For Category B valves, the seat leakage in the closed position is inconsequential.

For the 12 active MOVs associated with the ADS, it is estimated that there will be approximately 144 demands in 12 quarters / 3 years.

16.3. Air Operated Valves

Similar to the testing for MOVs, the 8 active AOVs associated with the passive cooling systems are estimated to have approximately 96 demands in 12 quarters or 3 years.

17. AP1000 RTNSS

The identification of AP1000 systems and associated functions subject to the RTNSS process is documented in WCAP-15985 [Reference 14] and is based on SECY 95-132. The selection process considers both probabilistic and deterministic criteria. The resulting list of systems and associated functions for the AP1000 is shown in the following table.

System	Mode	Description
Instrumentation Systems		
DAS ATWS mitigation	1	Diverse Actuation System mitigation functions of reactor trip, turbine trip, and PRHR HX actuation.
DAS ESF actuation	1,2,3,4,5,6	DAS initiate ESF functions of PRHR actuation, CMT actuation on RCP trip, and passive containment cooling and selected containment isolation actuation.
Plant Systems		
RNS - Injection	1,2,3	RNS injection capability provides margin for ADS stage 4 squib valves, IRWST injection/containment recirculation check and squib valve reliability uncertainty, and long-term cooling thermal/hydraulic uncertainty.
RNS - RCS open	5,6 (2,3)	Portions of RNS needed to provide shutdown decay heat removal during RCS open conditions.
CCS - RCS open	5,6 (2,3)	Portions of CCS needed to support RNS shutdown decay heat removal during RCS open conditions
SRW - RCS open	5,6 (2,3)	Portions of SRW needed to support CCS system shutdown decay heat removal during RCS open conditions.
PCS water makeup - long-term shutdown	1,2,3,4,5,6	The PCS recirculation pumps provide the capability to transfer water from the PCS water storage tank and spent fuel pool to support post-72hour operation of passive safety-related SSCs. This capability is required when the decay heat of the core is sufficient to require PCS water evaporative cooling.
MCR cooling - long-term shutdown	1,2,3,4,5,6	The MCR ancillary room fans provide cooling of the MCR to support post-72 MCR habitability during all modes of plant operation.
I&C room cooling - long-term shutdown	1,2,3,4,5,6	Instrumentation room fans provide cooling of the Class 1E instrumentation rooms to support post-72hour post-accident monitoring during all modes of plant operation.
Hydrogen Ignitors	1,2,5,6 (2,3)	Provides margin for uncertainty in hydrogen burn consequences.
Electrical Power Systems		
AC power supplies	1,2,3,4,5	Onsite ac power supplies (provide margin for ADS/IRWST injection/containment recirculation valve reliability certainty, and long-term cooling thermal/hydraulic uncertainty.
AC power supplies -	5,6 (2,3)	Diesel generators as a backup source of electrical power to support decay

System	Mode	Description
RCS open		heat removal operation during RCS open conditions.
AC power supplies - long-term shutdown	1,2,3,4,5,6	The ancillary diesel generators provide power to support post-72hour operation following at-power and shutdown events.
DC power supplies - DAS	1,2,3,4,5,6 (3)	Non-class 1E DC and UPS system provides electrical power to the DAS and actuation components to actuate reactor and turbine trip and initiate PRHR under conditions indicative of an ATWS during power operation

Systems that are identified as being RTNSS for modes other than Mode 1,2 or 3 are excluded from consideration in order to be consistent with the current internal events, at-power focus of the MSPI program.

18. AP1000 Westinghouse Importance Ranking

An audit of the AP1000 importance ranking was performed on by the NRC Staff on July 25, 2016 at Westinghouse's Rockville offices in order to establish realistic Birnbaum values for this white paper.

18.1. AP1000 Passive Safety System Valves

The following squib, motor-operated and air operated valve data associated with components of the AP1000 passive safety systems are consistent with that found in the Westinghouse data.

18.1.1. Squib Valves

The following table shows squib importance data consistent with that contained in the Westinghouse PRA.

Probability	Birnbaum	Description
8.88E-04	3.24E-07	PMS Squib Valve Termination Unit Fail to Operate
8.88E-04	3.24E-07	PMS Squib Valve Termination Unit Fail to Operate
5.80E-04	2.32E-07	PXS Explosive Operated Valve APP-RCS-PL-V004B Fail to Open
5.80E-04	2.32E-07	PXS Explosive Operated Valve APP-RCS-PL-V004D Fail to Open
5.80E-04	5.06E-09	PXS Explosive Operated Valve APP-RCS-PL-V004A Fail to Open
5.80E-04	5.06E-09	PXS Explosive Operated Valve APP-RCS-PL-V004C Fail to Open
5.80E-04	6.09E-10	PXS EOV APP-PXS-PL-V123A Fail to Open
5.80E-04	6.09E-10	PXS EOV APP-PXS-PL-V125A Fail to Open

Probability	Birnbaum	Description
8.88E-04	5.51E-10	PMS Squib Valve Termination Unit Fail to Operate
8.88E-04	5.51E-10	PMS Squib Valve Termination Unit Fail to Operate
5.80E-04	4.35E-10	PXS EOV APP-PXS-PL-V123B Fail to Open
5.80E-04	4.35E-10	PXS EOV APP-PXS-PL-V125B Fail to Open
5.80E-04	4.75E-11	PXS EOV APP-PXS-PL-V120A Fail to Open
5.80E-04	4.75E-11	PXS EOV APP-PXS-PL-V120B Fail to Open
TOTAL	1.13E-06	

The ADS function and its associated squib valves and the Passive Core Cooling System injection and recirculation squib valves have a total Birnbaum importance contribution of 1.13E-06.

18.1.2. ADS Active MOVs

The following ADS motor-operated valve data are consistent with that found in the Westinghouse data.

Probability	Birnbaum	Description
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V002A Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V002B Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V003A Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V003B Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V012A Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V012B Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V013A Fail to Open
1.07E-03	1.02E-06	RCS MOV APP-RCS-PL-V013B Fail to Open
TOTAL	8.13E-06	

The ADS function and its associated MOVs have a total Birnbaum importance contribution of 8.13E-06.

18.1.3. Passive Core Cooling AOVs

The following Passive Core Cooling air-operated valve data are consistent with that found in the Westinghouse data.

Probability	Birnbaum	Description
1.11E-03	6.16E-08	PXS-AOV-V108B Fails to Open – PRHR HX outlet
1.11E-03	5.62E-08	PXS-AOV-V130A Fails to Close – IRWST Gutter Isolation
1.11E-03	5.31E-08	PXS-AOV-V108A Fails to Open – PRHR HX Outlet
1.11E-03	5.29E-08	PXS-AOV-V130B Fails to Close – IRWST Gutter Isolation

Probability	Birnbaum	Description
1.11E-03	4.03E-09	PXS-AOV-V014A Fails to Open – CMT Outlet Isolation
1.11E-03	4.02E-09	PXS-AOV-V014B Fails to Open – CMT Outlet Isolation
TOTAL	2.32E-07	

The Passive Core Cooling Core Makeup Tanks and Residual Heat Removal heat exchanger functions and its associated AOVs have a total Birnbaum importance contribution of 2.32E-07.

18.1.4. Passive Core Cooling SOVs

The Westinghouse data were found to include specific events for solenoid valves associated with the Passive Residual Heat Exchanger Gutter Isolation AOV (V130A) and Core Makeup Tank Outlet Isolation AOV (V014A). These valves automatically open on a Core Makeup Tank actuation signal from the Plant Protection and Monitoring System (PMS), which actuates an air solenoid valve associated with each valve. They can also be opened through a CMT actuation signal from the Diverse Actuation System (DAS) which actuates a separate common air solenoid valve in the compressed and instrument air system (CAS). Opening of the valves is an active safety-related function because they initiate CMT injection to mitigate design basis accidents. Closing is not an active safety-related function. The reliability of these valves is important in the AP1000 PRA and they are captured in the D-RAP.

Probability	Birnbaum	Description
9.54E-04	1.24E-06	PXS SOV APP-PXS-PL-V130A-S2 Fail on Demand
9.54E-04	5.71E-07	PXS SOV APP-PXS-PL-V014A-S2 Fail on Demand
TOTAL	1.81E-06	

The gutter isolation SOVs for Passive Core Cooling and the outlet isolation SOVs for the Core Makeup Tanks have a combined Birnbaum of 1.81E-06. Note that it is unclear as to why these two SOVs were explicitly modeled as opposed to be incorporated into the component boundary of the AOVs and why only two of the six AOVs were found on the Westinghouse importance ranking.

18.2. Other Important Mechanical Components

One objective of the review of the Westinghouse importance data was to determine if there were other important events that could be candidates for monitoring within the MSPI program. The following two mechanical components were noted as having importance ranking values greater than 5E-07.

Probability	Birnbaum	Description
6.76E-05	2.35E-06	SGS Safety Valve APP-SGS-PL-V030A Fail to Close
6.76E-05	2.35E-06	SGS Safety Valve APP-SGS-PL-V030B Fail to Close
TOTAL	4.70E-06	

The steam generator relief function and its associated relief valves have a total Birnbaum importance contribution of 4.7E-06.

18.3. Important Electrical Components

Although electrical components have not been the historical focus of MSPI, several electrical related events show as being significant within the Westinghouse data.

Probability	Birnbaum	Description
4.32E-04	2.04E-06	VCS Sensor/Transmitter (Temperature) APP-VCS-JE-TE053A Fail to Operate
4.32E-04	2.04E-06	VCS Sensor/Transmitter (Temperature) APP-VCS-JE-TE053B Fail to Operate
2.15E-04	1.97E-06	ECS-EK-23 Unavailable due to Unplanned T&M
1.04E-05	1.94E-06	IDS Bus APP-IDSB-DS-1 Fail to Operate
1.04E-05	1.92E-06	IDS Bus APP-IDSC-DS-1 Fail to Operate
1.04E-05	1.92E-06	IDS Bus APP-IDSD-DS-1 Fail to Operate
1.04E-05	1.36E-06	ECS BUS APP-ECS-ES-2 Fails to Operate
1.04E-05	1.36E-06	ECS BUS APP-ECS-EK-23 Fails to Operate
1.04E-05	1.34E-06	IDS Bus APP-IDSC-DK-1 Fail to Operate
4.46E-05	1.21E-06	IDS Battery (DC) APP-IDSD-DB-1A Fail to Operate
4.46E-05	1.21E-06	IDS Battery (DC) APP-IDSD-DB-1B Fail to Operate
4.46E-05	1.15E-06	IDS Battery (DC) APP-IDSC-DB-1A Fail to Operate
4.46E-05	1.15E-06	IDS Battery (DC) APP-IDSC-DB-1B Fail to Operate
4.46E-05	1.12E-06	IDS Battery (DC) APP-IDSB-DB-1A Fail to Operate
4.46E-05	1.12E-06	IDS Battery (DC) APP-IDSB-DB-1B Fail to Operate
1.04E-05	1.08E-06	EDS Bus APP-EDS4-EA-1 Fail to Operate
2.15E-04	1.06E-06	ECS-EK-11 Unavailable due to Unplanned T&M
4.10E-06	1.05E-06	ECS Circuit BKR Spurious Operation
4.10E-06	1.05E-06	ECS Circuit BKR Spurious Operation
4.46E-05	9.50E-07	IDS Battery (DC) APP-IDSA-DB-1B Fail to Operate
1.04E-05	6.14E-07	EDS Bus APP-EDS3-EA-1 Fail to Operate
1.04E-05	5.77E-07	IDS Bus APP-IDSC-DD-1 Fail to Operate

The two temperature sensors identified above (TE053A and TE053B) are used in the Diverse Actuation System (DAS), actuation logic for passive containment cooling system (PCS) initiation and isolation of critical containment penetrations. The containment temperature monitoring function and its associated sensors have a total Birnbaum importance contribution of 4.08E-06.

The other electrical components are not further evaluated for the MSPI framework due to their high reliability.

18.4. Significant Low Birnbaum Components

A review of the AP1000 importance list found several basic events for components similar to those currently monitored and also included RTNSS scoped components. The components found during the Westinghouse review include:

Function	Component	Current MSPI Monitored Function	RTNSS (Mode 1)	Birnbaum
Onsite AC Power	Standby DG	No – not Class 1E	Yes	<1E-07
Onsite AC Power	Ancillary DG	No – not Class 1E	Yes	<1E-07
Residual Heat Removal	Normal Residual Heat Removal Pumps	No – not Class 1E	Yes – RNS Injection only	<1E-07
Cooling Water	Component Cooling Water Pumps	No – not Class 1E	No*	<1E-10
Cooling Water	Service Water Pumps	No – not Class 1E	No*	<1E-09

*Although not explicitly stated in Reference 14, cooling water is required to support pump operation for RNS injection

As shown above, these components have Birnbaums less than 1E-07 and are expected to be insensitive to the formulation used by MSPI.

19. AP1000 System Selection

As stated in NUREG 1816, the purpose of the MSPI is to monitor the performance of selected systems based on their ability to perform risk-significant functions. Due to the passive nature of the AP1000, there is not a direct match between the systems typically monitored in the current fleet with the systems utilized by the AP1000.

Two primary approaches are investigated in this paper for selecting the scope of functions to be monitored.

1. Plant Risk-Informed Scope **[OPTION SCOPE-1]**
2. MSPI Functional-Based Scope **[OPTION SCOPE-2]**

These methods are developed in the following sections.

19.1. Plant Risk-Informed Approach [OPTION SCOPE-1]

This approach focuses on identifying AP1000 safety and non-safety systems that are significant risk contributors as the primary means for identifying the monitored systems. This approach risk-informs the system selection as opposed to the deterministic system selection process used for the current operating reactors.

Generally, when the sum of the Birnbaum importance values for active failures, and/or test and maintenance associated with a function or component type is 5E-07 or greater, then those functions or component types are considered to be good candidates for inclusion into a risk-informed MSPI scope. A few additional basic events were evaluated that did not meet this criterion in order to fully address RTNSS contributors and to ensure systems that had been historically included within the MSPI program have a firm basis for exclusion. Components associated with the electrical distribution system were excluded due both to their high reliability and in order to be consistent with the current MSPI scope.

A review of the available AP1000 Westinghouse information yields the following candidate systems:

Risk Informed Approach
Candidate AP1000 Functions and Components

Classification	System	Function	Components
SR	ADS	Automatic Depressurization System	4 squib valves, 12 MOVs
SR	PXS	Passive Core Cooling System – Injection	4 squib valves
SR	PXS	Passive Core Cooling System - Recirculation	4 squib valves 2 AOVs (gutter Isolation)
SR	PXS	Passive Core Cooling System – Core Makeup Tanks	4 AOVs (low Birnbaum - included to evaluate scope criteria) 4 SOVs
SR	PXS	Passive Core Cooling System – Residual Heat Removal HX	4 AOVs (low Birnbaum - included to evaluate scope criteria) 4 SOVs
SR	SGS	Main Steam Safety Valves	10 relief valves
SR	VCS	Containment Temperature	2 temp elements
NSR	ZOS	Standby Diesel Generators - RTNSS (low Birnbaum)	2 diesel generators

Classification	System	Function	Components
NSR	ZRS	Ancillary Diesel Generators - RTNSS (low Birnbaum)	2 diesel generators
NSR	RNS	Normal Residual Heat Removal (low Birnbaum)	2 pumps
NSR	CCS	Component Cooling Water (low Birnbaum)	2 pumps
NSR	SRW	Service Water (low Birnbaum)	2 pumps

Test indicators were developed as an initial assessment of the effectiveness of a risk-informed performance indicator.

Aligning the above identified functions with the current MSPI-monitored functions yields the following table.

Candidate AP1000 Risk-Informed MSPI Scope

System	Guidance	Risk-Informed AP1000 Scope
Emergency AC Power System	Power to 1E Systems	NSR Onsite Standby Diesel Generators
High Pressure Injection	Maintains reactor coolant inventory at high pressure	Automatic Depressurization System. Passive Core Cooling System – Injection Passive Core Cooling System - Recirculation ADS reduces RCS pressure to allow for passive injection.
Heat Removal	For PWRs, to provide decay heat removal via the steam generators.	Passive Residual Heat Removal. Core Makeup Tanks Adequate to remove initial and long-term residual heat.
Residual Heat Removal System	For long-term decay heat removal function	Normal Residual Heat Removal
Cooling Water Support System	Functions that are necessary for direct cooling of components in monitored trains or segments	Component Cooling Water / Service Water System
New Function	Prevent uncontrolled steam generator blowdown	Main Steam Safety Valves
New Function	Indicator for containment environment	Containment Temperature Sensors

The result of this approach would be to monitor several non-safety-related systems that are subject to the RTNSS process and monitor two new safety-related functions not currently in the scope of MSPI monitored functions.

19.2. MSPI Functional-Based Scope [OPTION SCOPE-2]

This approach focuses on identifying AP1000 systems consistent with NEI 99-02 guidance to the extent possible. The following table summarizes the results of this approach. To accomplish this mapping, the safety design of the AP1000 was assessed to find functions and components that perform similar functions to that contained in the current MSPI program. Although this approach is limited to the current MSPI functions, mapping the equivalent AP1000 function was performed broadly.

One significant difference between the current fleet and the AP1000 is that all active systems are non-safety-related. Therefore, a key question is whether important non-safety-related systems should be monitored **[OPTION NSR-1]**.

Candidate AP1000 Functional-Based MSPI Scope

Description	BWR	PWR	AP1000
Emergency AC Power	EAC	EAC	**Option NSR-2a**: No safety-related EDGs are required by plant design. Not monitored **Option NSR-2b**: Onsite Standby DGs DGs provide important non safety defense-in-depth capability
High Pressure Injection	HPCI/HPCS/FWCI	HPSI	Automatic Depressurization System. Passive Core Cooling System – Injection Passive Core Cooling System - Recirculation ADS reduces RCS pressure to allow for passive injection.
Heat Removal System	RCIC/IC	AFW/EFW	Passive Residual Heat Removal. Core Makeup Tanks For the AP1000, the passive heat removal system is capable of addressing both short term and residual heat removal.

Description	BWR	PWR	AP1000
Residual Heat Removal	RHR	RHR	**Option NSR-3a**: Function is not applicable as Passive Residual Heat Removal is adequate to remove initial and long-term residual heat and is addressed above. **Option NSR-3b**: Normal Residual Heat Removal – heat removal function
Cooling Water	SRW/CCW	SRW/CW	**Option NSR-4a**: CCW and SRW are not required for ECCS, RCP Seals, RHR or DGs. **Option NSR-4b**: CCW and SRW required to support the normal heat removal system.

The result of this approach would be to monitor similar functions to those currently monitored for operating reactors. However, in order to address the uncertainties associated with passive systems, several non-safety-related systems could be monitored. The table shows the options of monitoring the on-site diesel generators and the normal residual heat removal, component cooling water and service water systems.

20. Test Indicators

This section explores several potential indicators based on the available data. Due to data limitation (i.e., small component type populations and limited demands), all test indicators were developed to address only a single component type with many indicators crossing system boundaries. This approach is labelled in this white paper as **OPTION Data-2**. It is believed that this approach maximizes the data population as many candidate components have limited demands.

20.1. Indicator Data Processing

The current MSPI indicators used a Bayesian analysis method that includes the use of a constrained non-informative prior (CNIP) as described in Appendix J of NUREG-1816 and Appendix F of NUREG-1753 (Reference 21). This technique sets the prior distribution to the industry mean and treats other characteristics of the of the prior as non-informative.

Other data analysis techniques that were considered in NUREG-1753 include:

Updated the "Industry" Prior	The industry prior reflects variability across the industry of the long-term average value
Maximum-Likelihood Estimate (MLE)	Makes no use of historical information; derives an estimate entirely from current failure and demand information. NUREG-1753 refers to the MLE as being based on a "zero" prior because it is like having previously observed zero failures in zero demands, which is updated with current data by adding current failures to the (zero)) numerator and current demands to the (Zero) denominator.

NUREG-1753 compared the behavior of the CNIP with the MLE and the "industry prior." The CNIP was found to be the best of the alternatives considered at that time. NUREG-1816 summarizes the findings. It states that the MLE has a false-positive problem: it uses the number of failures directly, and is a noisy signal. The "industry prior" has the opposite problem: it gives less prior density to large excursions, creating a false negative potential. The CNIP falls between these extremes and provides the best combination of minimizing both false positive and false negative. It also states that "a low value of the CNIP density for high failure probability requires the accumulation of a significant number of failures before the posterior density becomes significant in that region. Because of the form of the CNIP, if the baseline failure probability is a very small number (the case for many of the candidate AP1000 components), the CNIP accords a very low prior probability to significantly degraded performance, and it takes a certain amount of data to overcome this.

In the current MSPI indicators, the key components that are being monitored are pumps and EDGs. These components have a moderate failure probability and perform reasonably well with the CNIP. However, the primary AP1000 candidate components for monitoring are valves which have a significantly lower failure probability. In addition, the original analysis of false positives did not include the benefit of the front-stop, a feature introduced during the development of NUREG-1816. This feature restricts the worth of the one single failure to 5E-07 thus preventing a key false positive concern. For a pure unreliability indicator (no unavailability contribution) it requires a minimum of two failures in order for an indicator to cross the Green-White threshold.

In order to fully investigate the effectiveness of the test indicators, failure rates were calculated using both the CNIP and the MLE. The approach of using the MLE is a key option to be considered in order to successfully implement MSPI for the AP1000 design. **[OPTION Data-1]**

20.2. Squib Valve Indicator

The Squib Valve indicator monitors all twelve AP1000 squib valves across multiple systems. It includes the four IRWST injection line squib valves, four Containment Recirculation Sump squib valves, and the four ADS Stage 4 squib valves.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with the squib-related systems during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all squib valve related Birnbaums and the common cause correction factor is assumed to be two. Two failure rate calculation methods were examined: the CNIP consistent with the current MSPI formulation and the MLE. Fifteen demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 15.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	5.00E-01	NEI 99-02 Section F 2.3.7
b	8.62E+02	Calculated based on AP1000 failure rate of 5.80E-04
B	1.13E-06	Sum of all AP1000 Squib-related Birnbaums
CCF	2.00E+00	Estimate - requires development
B (CCF)	2.26E-06	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0	5.80E-04	5.80E-04	-2.90E-07	2.26E-06	-6.55E-13	-1.31E-09
1	15	0.07	1.71E-03	5.80E-04	1.13E-03	2.26E-06	2.55E-09	1.49E-07
2	15	0.13	2.85E-03	5.80E-04	2.27E-03	2.26E-06	5.13E-09	3.00E-07
3	15	0.20	3.99E-03	5.80E-04	3.41E-03	2.26E-06	7.70E-09	4.51E-07
4	15	0.27	5.13E-03	5.80E-04	4.55E-03	2.26E-06	1.03E-08	6.01E-07
5	15	0.33	6.27E-03	5.80E-04	5.69E-03	2.26E-06	1.29E-08	7.52E-07
6	15	0.40	7.41E-03	5.80E-04	6.83E-03	2.26E-06	1.54E-08	9.03E-07
7	15	0.47	8.55E-03	5.80E-04	7.97E-03	2.26E-06	1.80E-08	1.05E-06
8	15	0.53	9.69E-03	5.80E-04	9.11E-03	2.26E-06	2.06E-08	1.20E-06
9	15	0.60	1.08E-02	5.80E-04	1.02E-02	2.26E-06	2.32E-08	1.35E-06
10	15	0.67	1.20E-02	5.80E-04	1.14E-02	2.26E-06	2.57E-08	1.51E-06
11	15	0.73	1.31E-02	5.80E-04	1.25E-02	2.26E-06	2.83E-08	1.66E-06
12	15	0.80	1.42E-02	5.80E-04	1.37E-02	2.26E-06	3.09E-08	1.81E-06
13	15	0.87	1.54E-02	5.80E-04	1.48E-02	2.26E-06	3.35E-08	1.96E-06
14	15	0.93	1.65E-02	5.80E-04	1.59E-02	2.26E-06	3.60E-08	2.11E-06
15	15	1.00	1.77E-02	5.80E-04	1.71E-02	2.26E-06	3.86E-08	2.26E-06

Due to that very low base-line squib valve failure rate, additional failures result in small failure rate changes when using the CNIP. The combination of these small changes and the low Birnbaum value make the indicator insensitive to changes in reliability. In other words, every valve could fail when tested without crossing a threshold.

The MLE approach results in a larger change in failure rate and will result challenges to the current thresholds as failures are increased. The following table summarizes the failure impacts:

Squib Valve MLE Indicator

Failures	Status
0	Green
1	Green
2	Green
3	Green
4	Green
5	Green
6	Green
7	White
>7	White

20.3. ADS MOV Indicator

The ADS MOV indicator monitors twelve AP1000 passive safety system MOVs that are required to change state in order to perform their safety function.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with the active MOV-related passive safety-systems during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all active MOV related Birnbaums and the common cause correction factor is assumed to be two consistent with the NEI 99-02 guidance. Two failure rate calculation methods were examined: CNIP consistent with the current MSPI formulation and the MLE. 144 demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 144.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.99E-01	NEI 99-02 Section F 2.3.7
b	4.66E+02	Calculated based on AP1000 failure rate of 1.07E-03
B	8.10E-06	Sum of all passive system active MOV Birnbaums
CCF	2.00E+00	from NEI 99-02 Table 7
B (CCF)	1.62E-05	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	1.07E-03	1.07E-03	-3.30E-07	1.62E-05	-5.35E-12	-1.73E-08
8	144	0.06	1.39E-02	1.07E-03	1.29E-02	1.62E-05	2.08E-07	8.83E-07
9	144	0.06	1.56E-02	1.07E-03	1.45E-02	1.62E-05	2.35E-07	9.95E-07
10	144	0.07	1.72E-02	1.07E-03	1.61E-02	1.62E-05	2.61E-07	1.11E-06
20	144	0.14	3.36E-02	1.07E-03	3.25E-02	1.62E-05	5.27E-07	2.23E-06
30	144	0.21	5.00E-02	1.07E-03	4.89E-02	1.62E-05	7.92E-07	3.36E-06
40	144	0.28	6.63E-02	1.07E-03	6.53E-02	1.62E-05	1.06E-06	4.48E-06
50	144	0.35	8.27E-02	1.07E-03	8.16E-02	1.62E-05	1.32E-06	5.61E-06
60	144	0.42	9.91E-02	1.07E-03	9.80E-02	1.62E-05	1.59E-06	6.73E-06
70	144	0.49	1.15E-01	1.07E-03	1.14E-01	1.62E-05	1.85E-06	7.86E-06
80	144	0.56	1.32E-01	1.07E-03	1.31E-01	1.62E-05	2.12E-06	8.98E-06
89	144	0.62	1.47E-01	1.07E-03	1.46E-01	1.62E-05	2.36E-06	1.00E-05
90	144	0.63	1.48E-01	1.07E-03	1.47E-01	1.62E-05	2.38E-06	1.01E-05
144	144	1.00	2.37E-01	1.07E-03	2.36E-01	1.62E-05	3.82E-06	1.62E-05

A sensitivity analysis was performed to determine the impact of reduced demands. When the demands were reduced by a factor of 2 (from 144 to 72), the number of failures to cross a threshold was also reduced by a factor of 2 (from 10 failures to cross the Green/White threshold to 5 failures to cross the Green/White threshold).

Passive System MOV MLE Indicator

Failures	Status
0 - 9	Green
10	White
10 - 88	White
89	White
90 - 144	White

20.4. Passive System AOV Indicator

The Passive System AOV indicator monitors eight AP1000 passive safety system AOVs that are required to change state in order to perform their safety function. The AOVs are associated with the CMT and the Passive Residual Heat Removal Heat Exchanger.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with the active AOV-related passive safety-systems during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all active AOV related Birnbaums and the common cause correction factor is assumed to be two consistent with the NEI 99-02 guidance. Two failure rate calculation methods were examined: CNIP consistent with the current MSPI formulation and the MLE. 96 demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 96.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.99E-01	NEI 99-02 Section F 2.3.7
b	4.50E+02	Calculated based on AP1000 failure rate of 1.1E-03
B	2.32E-07	Sum of all passive system active AOV Birnbaums from NEI 99-02
CCF	1.50E+00	Table 7
B (CCF)	3.48E-07	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	1.11E-03	1.10E-03	7.66E-06	2.32E-07	1.78E-12	-2.55E-10
1	96	0.01	2.74E-03	1.10E-03	1.64E-03	2.32E-07	3.81E-10	2.16E-09
20	96	0.21	3.75E-02	1.10E-03	3.64E-02	2.32E-07	8.45E-09	4.81E-08
40	96	0.42	7.41E-02	1.10E-03	7.30E-02	2.32E-07	1.69E-08	9.64E-08
50	96	0.52	9.24E-02	1.10E-03	9.13E-02	2.32E-07	2.12E-08	1.21E-07
60	96	0.63	1.11E-01	1.10E-03	1.10E-01	2.32E-07	2.54E-08	1.45E-07
94	96	0.98	1.73E-01	1.10E-03	1.72E-01	2.32E-07	3.99E-08	2.27E-07
95	96	0.99	1.75E-01	1.10E-03	1.74E-01	2.32E-07	4.03E-08	2.29E-07
96	96	1.00	1.77E-01	1.10E-03	1.75E-01	2.32E-07	4.07E-08	2.32E-07

A review of the above data finds that due to the low Birnbaum value the indicator will not cross a performance threshold even if every demand resulted in a failure. Therefore, this indicator would be an ineffective performance index.

20.5. Passive System SOV Indicator

The Passive System SOV indicator monitors eight AP1000 passive safety system SOVs that are required to change state in order to perform their safety function. The SOVs are associated with the CMT and the Passive Residual Heat Removal Heat Exchanger. It should be noted that only two of the eight SOV Birnbaums were identified during the Westinghouse review.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with the active SOV-related passive safety-systems during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all active SOV related Birnbaums and the common cause correction factor is assumed to be 1.5 consistent with the NEI 99-02 guidance. Two failure rate calculation methods were examined: CNIP consistent with the current MSPI formulation and the MLE. 96 demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 96.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.98E-01	NEI 99-02 Section F 2.3.7
b	5.23E+02	Calculated based on AP1000 failure rate of 9.54E-04
B	1.81E-06	Sum of all passive system active SOV Birnbaums from NEI 99-02
CCF	1.50E+00	Table 7
B (CCF)	2.72E-06	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	9.52E-04	9.54E-04	-1.80E-06	2.72E-06	-4.88E-12	-2.59E-09
1	96	0.01	2.42E-03	9.54E-04	1.47E-03	2.72E-06	3.98E-09	2.57E-08
35	96	0.36	5.73E-02	9.54E-04	5.64E-02	2.72E-06	1.53E-07	9.87E-07
36	96	0.38	5.90E-02	9.54E-04	5.80E-02	2.72E-06	1.57E-07	1.02E-06
50	96	0.52	8.16E-02	9.54E-04	8.06E-02	2.72E-06	2.19E-07	1.41E-06
60	96	0.63	9.77E-02	9.54E-04	9.68E-02	2.72E-06	2.63E-07	1.69E-06
94	96	0.98	1.53E-01	9.54E-04	1.52E-01	2.72E-06	4.12E-07	2.66E-06
95	96	0.99	1.54E-01	9.54E-04	1.53E-01	2.72E-06	4.16E-07	2.68E-06
96	96	1.00	1.56E-01	9.54E-04	1.55E-01	2.72E-06	4.21E-07	2.71E-06

Solenoid Valve MLE Indicator

Failures	Status
0	Green
1	Green
2-35	Green
36	White
>37	White

20.6. Steam Generator Safety Valve Indicator

The Steam Generator Safety Valve indicator monitors ten AP1000 relief valves.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with the valves during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all active relief valve related Birnbaums and the common cause correction factor is assumed to be two. Two failure rate calculation methods were examined: CNIP consistent with the current MSPI formulation and the MLE. Ten demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 10.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.99E-01	NEI 99-02 Section F 2.3.7
b	4.66E+02	Calculated based on AP1000 failure rate of 1.07E-03
B	4.70E-06	Sum of all SG Safety Birnbaums
CCF	2.00E+00	Assumed for test case
B (CCF)	9.40E-06	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	1.07E-03	6.76E-05	1.00E-03	9.40E-06	9.42E-09	-6.35E-10
1	10	0.10	3.15E-03	6.76E-05	3.08E-03	9.40E-06	2.89E-08	9.39E-07
2	10	0.20	5.24E-03	6.76E-05	5.18E-03	9.40E-06	4.87E-08	1.88E-06
3	10	0.30	7.34E-03	6.76E-05	7.28E-03	9.40E-06	6.84E-08	2.82E-06
4	10	0.40	9.44E-03	6.76E-05	9.37E-03	9.40E-06	8.81E-08	3.76E-06
5	10	0.50	1.15E-02	6.76E-05	1.15E-02	9.40E-06	1.08E-07	4.70E-06
6	10	0.60	1.36E-02	6.76E-05	1.36E-02	9.40E-06	1.28E-07	5.64E-06
7	10	0.70	1.57E-02	6.76E-05	1.57E-02	9.40E-06	1.47E-07	6.58E-06
8	10	0.80	1.78E-02	6.76E-05	1.78E-02	9.40E-06	1.67E-07	7.52E-06
9	10	0.90	1.99E-02	6.76E-05	1.99E-02	9.40E-06	1.87E-07	8.46E-06
10	10	1.00	2.20E-02	6.76E-05	2.20E-02	9.40E-06	2.06E-07	9.40E-06

Due to that very low base-line safety valve failure rate, additional failures result in small failure rate changes when using the CNIP. The combination of these small changes and the low Birnbaum value make the indicator insensitive to changes in reliability. In other words, every valve could fail when tested without crossing a threshold.

The MLE approach results in a larger change in failure rate and will result challenges to the current thresholds as failures are increased. The following table summarizes the failure impacts:

Steam Generator Safety Valve MLE Indicator

Failures	Status
0	Green
1	Green
2	White
>2	White

The front-stop is not required for this indicator and due to the low Birnbaum value, the Yellow and Red threshold cannot be crossed.

20.7. Containment Temperature Element Indicator

The Containment Temperature Element indicator monitors the two Temperature sensors (TE053A and TE053B) that are used in the Diverse Actuation System (DAS), actuation logic for passive containment cooling system (PCS) initiation and isolation of critical containment penetrations. These temperature elements were noted as having high Birnbaum values.

The indicator only addresses reliability as it is anticipated that no unavailability will be associated with these elements during at-power operation.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all temperature element related Birnbaums and the common cause correction factor is assumed to be two. Two failure rate calculation methods were examined: CNIP consistent with the current MSPI formulation and the MLE. Twenty-four demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 24.

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	5.00E-01	NEI 99-02 Section F 2.3.7
b	1.16E+03	Calculated based on AP1000 failure rate of 4.32E-04
B	4.08E-06	Sum of all containment temperature element Birnbaums estimated for test
CCF	2.00E+00	case
B (CCF)	8.16E-06	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	4.32E-04	4.32E-04	-3.46E-08	8.16E-06	-2.82E-13	-3.53E-09
1	24	0.04	1.27E-03	4.32E-04	8.38E-04	8.16E-06	6.83E-09	3.36E-07
2	24	0.08	2.12E-03	4.32E-04	1.68E-03	8.16E-06	1.37E-08	6.76E-07
3	24	0.13	2.96E-03	4.32E-04	2.53E-03	8.16E-06	2.06E-08	1.02E-06
4	24	0.17	3.81E-03	4.32E-04	3.38E-03	8.16E-06	2.76E-08	1.36E-06
5	24	0.21	4.66E-03	4.32E-04	4.22E-03	8.16E-06	3.45E-08	1.70E-06
6	24	0.25	5.50E-03	4.32E-04	5.07E-03	8.16E-06	4.14E-08	2.04E-06
7	24	0.29	6.35E-03	4.32E-04	5.92E-03	8.16E-06	4.83E-08	2.38E-06
24	24	1.00	2.07E-02	4.32E-04	2.03E-02	8.16E-06	1.66E-07	8.16E-06

Due to that very low base-line temperature element failure rate, additional failures result in small failure rate changes when using the CNIP. The combination of these small changes and the low Birnbaum value make the indicator insensitive to changes in reliability.

The MLE approach results in a larger change in failure rate and will result challenges to the current thresholds as failures are increased. The following table summarizes the failure impacts:

Steam Generator Safety Valve MLE Indicator

Failures	Status
0	Green
1	Green
2	Green
3	White
>3	White

The front-stop is not required for this indicator and due to the low Birnbaum value, the Yellow and Red threshold cannot be crossed.

20.8. Standby Diesel Generator Indicator

Unlike the three previous valve indicators, the standby diesel generator indicator addresses both unavailability and unreliability.

20.8.1. Unavailability

This unavailability indicator monitors the two AP1000 standby diesel generators. Although these generators are non-safety-related, they do contribute to the reducing the risk of the AP1000 by providing a backup source of electrical power to onsite equipment that can be used to support decay heat removal.

The indicator only addresses unavailability and will be combined with unreliability portion of the indicator at the end of Section 21.5.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of the two unavailability. The percent unavailability was varied from 0 to 100% to determine the sensitivity of this indicator.

UA-Baseline	1.70E-03	Section F.1.2.3 Table 1
UA-AP1000	1.34E-02	DG UA assumed in PRA

UA-P	**UA-BL**	**Delta UR**	**MaxB**	**URI**
10%	1.34E-02	8.66E-02	7.87E-08	6.82E-09
20%	1.34E-02	1.87E-01	7.87E-08	1.47E-08
30%	1.34E-02	2.87E-01	7.87E-08	2.26E-08
40%	1.34E-02	3.87E-01	7.87E-08	3.04E-08
50%	1.34E-02	4.87E-01	7.87E-08	3.83E-08
60%	1.34E-02	5.87E-01	7.87E-08	4.62E-08
70%	1.34E-02	6.87E-01	7.87E-08	5.40E-08
80%	1.34E-02	7.87E-01	7.87E-08	6.19E-08
90%	1.34E-02	8.87E-01	7.87E-08	6.98E-08
100%	1.34E-02	9.87E-01	7.87E-08	7.76E-08

20.8.2. Unreliability

This unavailability indicator monitors the two AP1000 standby diesel generators.

The indicator only addresses unreliability and will be combined with unavailability portion of the indicator at the end of Section 21.5.

The indicator is formulated using data consistent with the Westinghouse PRA. The Birnbaum value is the summation of all like standby diesel Birnbaums for each failure mode and the common cause correction factor is estimated to be 1.25 consistent with the NEI 99-02 guidance. Two failure rate calculation methods were examined: the CNIP consistent with the current MSPI formulation and the MLE. Twenty-four demands were assumed to occur over a three-year period and the number of failures was varied from 1 to 24.

a. STANDBY DIESEL FAILRE TO START

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.92E-01	Based on NEI 99-02 Section F 2.3.7 Table 8
b	9.79E+01	Based on NEI 99-02 Section F 2.3.7 Table 8
B	7.51E-08	Sum of all diesel start Birnbaums from NEI 99-02 Table
CCF	1.25E+00	7
B (CCF)	9.39E-08	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	5.00E-03	5.00E-03	4.07E-07	9.39E-08	3.82E-14	-4.69E-10
1	24	0.04	1.22E-02	5.00E-03	7.19E-03	9.39E-08	6.75E-10	3.44E-09
2	24	0.08	2.04E-02	5.00E-03	1.54E-02	9.39E-08	1.44E-09	7.35E-09
3	24	0.13	2.85E-02	5.00E-03	2.35E-02	9.39E-08	2.21E-09	1.13E-08
4	24	0.17	3.67E-02	5.00E-03	3.17E-02	9.39E-08	2.98E-09	1.52E-08
5	24	0.21	4.49E-02	5.00E-03	3.99E-02	9.39E-08	3.74E-09	1.91E-08
6	24	0.25	5.30E-02	5.00E-03	4.80E-02	9.39E-08	4.51E-09	2.30E-08
7	24	0.29	6.12E-02	5.00E-03	5.62E-02	9.39E-08	5.28E-09	2.69E-08
24	24	1.00	2.00E-01	5.00E-03	1.95E-01	9.39E-08	1.83E-08	9.34E-08

b. STANDBY DIESEL FAILURE TO LOAD-RUN

Nd	total number of failures on demand during the previous 12 quarters	
D	total number of demands during the previous 12 quarters	
a	4.95E-01	Based on NEI 99-02 Section F 2.3.7 Table 8
b	1.64E+02	Based on NEI 99-02 Section F 2.3.7 Table 8
B	7.31E-08	Sum of all diesel load -run Birnbaums from NEI 99-02 Table
CCF	1.25E+00	7
B (CCF)	9.14E-08	Calculated CCF *B

Nd	D	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	3.01E-03	3.00E-03	9.21E-06	9.14E-08	8.42E-13	-2.74E-10
1	24	0.04	7.93E-03	3.00E-03	4.93E-03	9.14E-08	4.51E-10	3.53E-09
2	24	0.08	1.32E-02	3.00E-03	1.02E-02	9.14E-08	9.35E-10	7.34E-09
3	24	0.13	1.85E-02	3.00E-03	1.55E-02	9.14E-08	1.42E-09	1.11E-08
4	24	0.17	2.38E-02	3.00E-03	2.08E-02	9.14E-08	1.90E-09	1.50E-08

5	24	0.21	2.92E-02	3.00E-03	2.62E-02	9.14E-08	2.39E-09	1.88E-08
6	24	0.25	3.45E-02	3.00E-03	3.15E-02	9.14E-08	2.87E-09	2.26E-08
7	24	0.29	3.98E-02	3.00E-03	3.68E-02	9.14E-08	3.36E-09	2.64E-08
24	24	1.00	1.30E-01	3.00E-03	1.27E-01	9.14E-08	1.16E-08	9.11E-08

c. STANDBY DIESEL FAILURE TO RUN

Nd	total number of failures on demand during the previous 12 quarters	
Run-Hrs	total number of run hours during the previous 12 quarters	
TM	24	mission time
a	5.00E-01	Based on NEI 99-02 Section F 2.3.7 Table 8
b	6.25E+02	Based on NEI 99-02 Section F 2.3.7 Table 8
B	7.97E-08	Sum of all diesel run Birnbaums from NEI 99-02
CCF	1.25E+00	Table 7
B (CCF)	9.96E-08	Calculated CCF *B

Nd	Run-Hrs	MLE	UR-BC	UR-BL	Delta UR	Birnbaum	URI	URI-MLE
0	0	0.00	1.92E-02	8.00E-04	1.84E-02	9.96E-08	1.83E-09	-7.97E-11
1	24	0.04	5.54E-02	8.00E-04	5.46E-02	9.96E-08	5.44E-09	4.07E-09
2	24	0.08	9.24E-02	8.00E-04	9.16E-02	9.96E-08	9.12E-09	8.22E-09
3	24	0.13	1.29E-01	8.00E-04	1.29E-01	9.96E-08	1.28E-08	1.24E-08
4	24	0.17	1.66E-01	8.00E-04	1.65E-01	9.96E-08	1.65E-08	1.65E-08
5	24	0.21	2.03E-01	8.00E-04	2.02E-01	9.96E-08	2.02E-08	2.07E-08
6	24	0.25	2.40E-01	8.00E-04	2.39E-01	9.96E-08	2.38E-08	2.48E-08
7	24	0.29	2.77E-01	8.00E-04	2.76E-01	9.96E-08	2.75E-08	2.90E-08
24	24	1.00	9.05E-01	8.00E-04	9.05E-01	9.96E-08	9.01E-08	9.95E-08

20.8.3. Combined Unavailability and Unreliability

In order to determine the viability of the Standby Diesel Indicator, the maximum values for the unavailability and unreliability test indicators were combined.

Parameter	Performance	Index
DG Unavailability	100%	7.76E-08
DG Failure to Start	24 of 24	9.34E-08
DG Failure to Load-Run	24 of 24	9.11E-08
DG Failure to Run	24 of 24	9.95E-08
TOTAL		**3.62E-07**

The above values are below the 1E-06 threshold even when all parameters are set to the maximum degraded state. As such, the standby diesel generators would be an ineffective indicator.

20.9. Other RTNSS Indicators

The Birnbaum importance of other RTNSS components such as the ancillary diesel generators, service water pumps, residual heat removal pumps and component cooling water pumps was found to be lower than that of the standby diesel generators. As an indicator for the standby diesel generators was found to be risk insensitive, it is therefore postulated that the identified other RTNSS systems will also be insensitive. No additional assessment was performed for these systems.

21. Initiation of Monitoring

As stated in NEI 99-02, MSPI monitors the performance of selected systems over a rolling 12-quarter time frame. On initial plant operation, there will be insufficient data to calculate the performance indicators. Therefore, a phase in process will be required. The use of the short-term backstop may be one approach to reduce the phase-in period.

22. Options

This paper explores several options for the application of the MSPI program to the AP1000. These can be broadly grouped into the following categories:

Approach
Performance Limit
Monitoring of Non-Safety-Related Systems
Data Processing

22.1. Approach

The paper explores the results associated with two difference approaches to determining the scope of monitored systems as shown below:

Option	Description
Scope-1	Plant Risk-Informed Scope
Scope-2	MSPI Functional-Based Scope

The risk-informed approach has the potential to identify functions and associated components that have not previously been considered for monitoring such as the steam generator safety valves. Although this approach ensures that the developed indicator would be effective, it results in a customized approach to the MSPI scope.

The functional-based approach results in the identification of several RTNSS systems that have been found to be insensitive as risk informed indicators. If these systems are included (e.g., standby diesel generators, normal heat removal, component cooling water and service water) then the use of a performance-based limit would be required.

22.2. Performance Limit

The paper explores changes to the performance limits as shown below.

Option	Description
PLE-1	No performance limit change
PLE-2	Implement short-term Limits
PLE-3	Tighten current performance limits
PLE-4	Implement both short-term limits and tighten current limits

The performance limits are very important if a functional-based scope is used for the AP1000 MSPI program as many of the candidate indicators would have insensitive risk indicators. However, such an approach requires additional research and would distance the program from its risk-informed roots.

22.3. Monitoring of Non-Safety-Related Systems

There are several non-safety-related AP1000 systems that provide important risk-significant and /or defense-in-depth functions. The monitoring of these systems could provide additional assurance and augment the limited active safety-related AP1000 components.

Option	Description
NSR-1	Monitor important non-safety-related systems
NSR-2	Monitor the non-safety-related diesel generators (AP1000 only)
NSR-3	Monitor the non-safety-related residual heat removal systems heat removal function
NSR-4	Monitor the non-safety-related CCW and SRW systems

Based on the test indicators, the development of risk-informed indicators for RTNSS systems using the current risk thresholds does not appear to be feasible. Indicators for these systems would need to be performance based.

In addition, based on the test indicators, no risk significant non-safety-related systems were identified (i.e., all non-safety-related candidate indicators were found to be insensitive). Therefore, the use of the risk-informed approach does not require the inclusion of non-safety-related systems.

22.4. Data Processing

Two options to the processing of unreliability data was explored in an attempt to address insensitive indicators.

Option	Description
Data-1	Implement MLE method for updating data
Data 2	Implement component-type specific cross system indicators

Based on the test indicators, all test indicators proved to be insensitive when the current CNIP approach to processing unreliability data was used. However, several indicators appear to behave reasonably in that they do not appear to be overly sensitive when MLE was employed. A more comprehensive assessment of this method should be performed prior to implementation.

In addition, all test indicators were developed to address a single component type with several indicators crossing system boundaries. It is believed that this approach maximizes the data population as many candidate components have limited demands.

23. Changes to MSPI Guidance

This section identifies a few initial changes that will be required to NEI 99-02.

23.1. MSPI Scoping Changes

Depending on the options selected, it will be necessary to reflect the final AP1000 selection criteria into the NEI 99-02 guidance. The below table reflects changes that will be necessary to reflect the inclusion of the AP1000 safety-significant systems. Additional changes will be necessary if one or more of the proposed options are selected.

System	Guidance	Proposal
Emergency AC Power System	Power to 1E Systems	Broaden guidance to include power for Defense-in Depth.
High Pressure Injection	Maintains reactor coolant inventory at high pressure	Broaden guidance to include maintaining adequate inventory (as opposed to high pressure) to support core heat removal. The AP1000 lowers pressure to allow for passive injection.
Heat Removal	For PWRs, to provide decay heat removal via the steam generators.	No change necessary.
Residual Heat Removal System	For long-term decay heat removal function	Broaden guidance to state that RHR can support near-term and long-term heat removal
Cooling Water Support System	Functions that are necessary for direct cooling of components in monitored trains or segments	No change necessary. There are no direct cooling requirements for AP1000 monitored trains or segments.

23.2. Deviation from Exclusion of Low-Risk Valves

NEI 99-02 Section F.2.1.2 provides guidance to allow the exclusion of low risk valves whose Birnbaum importance is less than 1.0E-06. The guidance states:

"This rule is applied at the discretion of the individual plant. A balance should be considered in applying this rule between the goal to minimize the number of components monitored and having a large enough set of components to have an adequate data pool. If a decision is made to exclude some valves based on low Birnbaum values, but not all, to ensure an adequate data pool, then the valves eliminated from monitoring shall be those with the smallest Birnbaum values. Symmetric valves in different trains should be all eliminated or all retained."

In the case of AP1000, for several functions there will be no other components monitored except active valves and as such the 32 valves identified by the white paper should not be screened out by the guidance contained in Section F.2.1.2.

24. Summary

This white paper proposes to maintain the MSPI risk thresholds consistent with the NRC Commissioners' direction and proposes to maintain the at-power focus of the current MSPI framework.

Monitoring of the active safety-related valves associate with the RWST, Recirculation Sump, Passive Residual Heat Removal System and the Automatic Depressurization System is proposed. An option evaluating the resulting indicators as component-type focused (i.e., one component type per indicator) as opposed to function focused was tested. It was found that the CNIP data update process used in the current indicators would result in insensitive indicators. The use of the MLE proved to be more effective and appears to address the limitation of the CNIP associated with high reliability components.

The paper documents the need to investigate two alternatives for determining the scope of monitored functions: a risk-informed approach and a MSPI functional-based approach. The risk-informed approach provides for a stronger scope bases but results in larger differences between the identified functions and the current MSPI program. The MSPI functional-based approach represents an attempt to map the appropriate AP1000 systems into the MSPI's system scope identified by NEI 99-02 in order to maintain consistency with the current MSPI framework. This approach identifies system functions that are insensitive and would require many functions to be screened out of scope or would require the monitoring to be performance-based.

Options were also investigated for the monitoring of risk-significant non-safety-related systems. The inclusion of these systems would broaden the monitoring program by monitoring key defense-in-depth functions. However, test indicators found that for AP1000 these systems would be risk insensitive.

This paper also recognizes that the AP1000 systems are less likely to challenge the risk thresholds due to the low calculated core damage frequency of this plant. Therefore, the performance-based limits will likely play a more significant role. The importance of performance-based limits increases if low risk RTNSS systems are monitored. Options for improving the performance-based limit are addressed. These include incorporation of a short-term backstop and the option of tightening the current backstop limit. Additional analysis and a reassessment of the backstop governing properties would be required.

25. References

1. NEI 99-02, Regulatory Assessment Performance Indicator Guideline, Revision 7, August 31, 2013.
2. Westinghouse AP1000 Design Control Document, Chapter 1, Introduction and General Description of the Plant, Revision 19
3. NRC SECY-10-0121, Modifying the Risk-Informed Regulatory Guidance for New Reactors, September 14, 2010 (ML102230076).
4. NRC SRM, Staff Requirements – SECY-10-0121 – Modifying the Risk-Informed Regulatory Guidance for New Reactors, March 2, 2011 (ML110610166).
5. NRC SECY-12-0081, Risk-Informed Regulatory Framework for New Reactors, June 6, 2012 (ML102230076).
6. NRC SRM, Staff Requirements – SECY-12-0081 – Risk Informed Regulatory Framework for New Reactors, October 22, 2012 (ML12296A158).
7. NRC SECY-13-0137, Recommendations for Risk-Informing the Reactor Oversight Process for New Reactors, December 17, 2013.
8. NRC SRM, Staff Requirements – SECY-13-0137 – Recommendations for Risk-Informing the Reactor Oversight Process for New Reactors, June 30, 2014.
9. NUREG 1816, Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for the Pilot Plants, February, 2005.
10. NRC SECY-94-084, Policy and technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs, March 28, 1994 (ML003708068).
11. NRC SRM, SECY-94-084 – Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems and COMSECY-94-024 – Implementation of Design Certification and Light-Water Reactor Design Issues, June 20, 1994 (ML003708098).
12. NRC SECY 95-132, Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084), May 22, 1995 (ML003708005).
13. NRC SRM, SECY-95-132, Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084), June 28,1995 (ML003708005).
14. Westinghouse, AP1000 Implementation of the Regulatory Treatment of Non Safety-Relate Systems Process, WCAP-15985, Revision 2, dated August 2003
15. Westinghouse AP1000 Design Control Document, Chapter 8, Electric Power, Revision 19
16. Westinghouse AP1000 Design Control Document, Chapter 6, Engineered Safety Features, Revision 19
17. Westinghouse AP1000 Design Control Document, Chapter 10, Steam Conversion, Revision 19
18. Westinghouse AP1000 Design Control Document, Chapter 5, Reactor Coolant System and Connected Systems, Revision 19
19. Westinghouse AP1000 Design Control Document, Chapter 9, Auxiliary Systems, Revision 19

20. ASME Operation and Maintenance of Nuclear Power Plants, ASME OM-2015
21. NUREG 1753, Risk-Based Performance Indicators: Results of Phase 1 Development, April 2002 (ML021140453 and ML021140531)

26. Acronyms and Abbreviations

1E	IEEE designation for components and systems essential for the safe shutdown of a reactor and preventing the escape of radioactive material to the environment.
ADS	Automatic Depressurization System (AP1000 designation)
AFW	Auxiliary Feedwater
AOV	Air Operated Valve
BWR	Boiling Water Reactor
CAS	Compressed and Instrument Air System (AP1000 Designation)
CCF	Common Cause Failure
CCS	Component Cooling Water (AP1000 designation)
CCW	Component Cooling Water
CDF	Core Damage Frequency
CMT	Core Makeup Tank
CNIP	Constrained Non-Informative Prior
CVS	Chemical Volume Control System
DAS	Diverse Actuation System (AP1000 designation)
DCD	Design Control Document
DG	Diesel Generator
D-RAP	Design Reliability Assurance Program
EAC	Emergency AC Power
EB	Empirical Bayes
ECS	Main AC Power System (AP1000 designation)
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
ESF	Engineered Safety Features
FWCI	Feedwater Coolant Injection
FWS	Feedwater System
HPCI	High Pressure Coolant Injection
HPCS	High Pressure Core Spray
HPI	High Pressure Injection
HPSI	High Pressure Safety Injection
HRS	Heat Removal System

IDS	Class 1E DC and UPS System (AP1000 designation)
MCR	Main Control Room
MLE	Maximum Likelihood Estimation
MOV	Motor Operated Valve
MSPI	Mitigating System Performance Index
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
O-RAP	Operational Reliability Assurance Program
PCS	Passive Containment Cooling System (AP1000 designation)
PMS	Plant Protection and Monitoring System (AP1000 designation)
PRA	Probabilistic Risk Assessment
PRHRHX	Passive RHR Heat Exchanger (AP1000 designation)
PWR	Pressurized Water Reactor
PXS	Passive Core Cooling System (AP1000 designation)
RCIC	Reactor Core Isolation Cooling System
RCP	Reactor Coolant Pump
RHR	Residual Heat Removal
RNS	Residual Heat Removal System (AP1000 designation)
RTNSS	Regulatory Treatment for Non-Safety Systems
RWST	Refueling Water Storage Tank
SECY	Commission Paper
SFP	Spent Fuel Pool
SGS	Steam Generator System (AP1000 designation)
SRM	Staff Requirement Memorandum
SRW	Service Water
SSCs	Structures, Systems and Components
SSU	Safety System Unavailability
SWS	Service Water System (AP1000 designation)
UPS	Uninterruptable Power Supply
U.S. APWR	U.S. Advanced Pressurized Water Reactor
U.S. EPR	U.S. Evolutionary Power Reactor
VCS	Containment Recirculation Cooling System (AP1000 designation)