Implementation of Risk Monitor at a U.S. Nuclear Power Plant

Aaron Moreno[a], Daniel Tirsun[a], Carroll Trull[b]
[a] Westinghouse Electric Company LLC, Glen Rose, TX, U.S.
[b] Westinghouse Electric Company LLC, Cranberry Twp., PA, U.S.

Abstract: This paper will cover an example of the implementation of risk monitor software at a nuclear power plant in the U.S. The site uses the risk monitor and results from the PSA to inform decisions made for work control, online risk management and outage risk, and emergent issues. How the insights translate to indicators used at the site on a daily basis and risk control measures put in place during heightened risk evolutions will be discussed. Specific examples of when the tools and insights are used, how results are communicated, as well as how this information has steered decisions will be included.

Keywords: Probabilistic risk assessment, probabilistic safety assessment, risk application, risk monitor, configuration risk.

1. BACKGROUND

In July of 1999, the U.S. Nuclear Regulatory Commission issued a final rulemaking, modifying the Maintenance Rule (10 CFR 50.65) to add paragraph (a)(4). With the following paragraph, the law requiring that all U.S. nuclear power plants assess and manage the risk associated with performing maintenance was established:

> *Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.*

This paper discusses the use of risk monitoring software at a U.S. nuclear power plant as a method to comply with paragraph (a)(4) of the Maintenance Rule that was implemented via guidance documents NUMARC 93-01 [1] and NRC Regulatory Guide 1.160 [2]. These software tools are referred to as Configuration Risk Monitor (CRM) models because they have been designed and built with the ability to assess the Core Damage Frequency and Large Early Release Frequency of the plant in variable configurations.

The site risk analysis personnel have installed and configured the Electric Power Research Institute (EPRI) Equipment Out of Service (EOOS) software for Online Configuration Risk Monitoring and the Outage Risk Assessment and Management (ORAM) software for Outage Risk Configuration Monitoring at this dual-unit U.S. nuclear power plant. These Configuration Risk Monitor applications are integrated into the daily operation of the site via plant procedures. They are supported or used by multiple groups including Risk Assessment and Applications, Online Work Control, Refueling Outage Work Control and Operations to assess configuration risk. The risk insights from the Configuration Risk Monitors are provided to Plant Management to aid in decision-making. Each of these roles and usages of the CRM tools will be discussed further in the following sections.

*morenora@westinghouse.com

2. CONFIGURATION RISK MONITOR SOFTWARE

The Configuration Risk Monitor tools are configured and maintained by the Risk Assessment and Applications group at the site. This group has the responsibility for maintaining the software, updating the software when Model of Record revisions are completed and providing subject matter expertise to the other software users on site.

2.1. Online Risk Monitor

The EOOS online risk monitor software integrates a model for each unit that is based on the PRA Model of Record, modified for use with the software. These models incorporate the plants internal events and a qualitative fire model, they do not have any external hazards such as high wind or flood. These models are editable and are used to define the plant specific parameters and relationships for the determination of relative plant risk. These two unit specific models do not communicate with each other, so a change to one model (e.g., taking out a shared system) will not automatically affect the other and therefore must be manually adjusted in the other unit model as needed.

There are several distinguishable features that differentiate a Configuration Risk Monitor from a Model of Record. The most significant differences between the two are the treatment of Test and Maintenance Basic Events and Alignment Basic Events. The Test and Maintenance Events are set to Zero because the user will specifically define the components that are out of service for the specific configuration of interest. Likewise, the alignments are set to Zero in the fault tree because they are set by the user to match the specific plant configuration for the intended analysis.

The user defines the configuration by adding components, alignments, environmental variances and tests/activities to the active items list. When the user sets the configuration in the active items list, the software will manipulate their associated basic event(s) in the fault tree. This interaction is dictated by the data in a mapping database. The mapping database is used to create relationships between basic events and their related components, alignments, environmental variances and tests/activities.

An additional feature of CRMs is the ability to account for situations that may increase initiating event frequencies. For example, severe weather may increase the likelihood of a weather induced Loss of Offsite Power and some maintenance activities have the potential to incidentally induce a reactor trip/turbine trip/main feedwater trip/etc. These factors can be included in the CRM as environmental variances.

The online CRM models are maintained to stay current with the Model of Record. Additionally, the risk analysis group reviews plant modifications, procedural changes and other plant change documentation that potentially could affect the models, which is documented in the site issue tracking system. Review aspects for inclusion in the CRM include:

- Workweek equipment configurations specified by Operations procedures that may alter mapping or defined alignments.
- Procedures establish threshold levels for risk and a matrix describing configurations for which analyses have been completed. Changes to these procedures may require a new PRA evaluation and/or procedure change.
- Communication of noteworthy changes and how they should be implemented, whether identified through routine screening or by Work Control.
- Review of existing changes that are documented in the risk group’s continuous update database.

The changes are documented and stored for future consideration. At the discretion of the Risk Analysis and Applications group, these changes may be incorporated into the models depending on

*morenora@westinghouse.com

their impact. The change may be implemented as a short-term (interim) change or a long-term change (i.e., during PRA periodic updates) depending on the impact to the model, and the potential to affect risk management actions.

Upon approval of a change/update by the risk group, the existing controlled models are replaced by the new updated model. The computers that have controlled models are carefully controlled via the site issue tracking system, which defines individuals who have access. Once installed for use as the current controlled model, the new updated model and documentation are procedurally controlled.

2.2. Outage Risk Monitor

Outage Risk Assessment and Management (ORAM) is a program used for qualitatively assessing the impact on plant safety for equipment out of service during shutdown conditions (Modes 5 & 6). The ORAM computer model is comprised of Safety Function Assessment Tree (SFAT) diagrams, event and fault trees and supporting databases. The ORAM model trees are built based on the NUMARC 93-01 [1] key safety functions (Decay Heat Removal, Inventory Control, Electric Power, Containment Closure and Reactivity Control) and also include Time to Boil calculations. Time to Boil considerations are used in the assessment trees in determining availability of equipment and defense in depth strategies. This model is editable and is used to define the plant specific parameters and relationships for the determination of relative plant risk.

The update schedule is similar to the online risk software. As a minimum, the model is reviewed/revised prior to each refueling outage. Review aspects include:

- Procedures establish defense-in-depth contingency plan (DIDCP) requirements. Changes to these procedures may require a new PRA evaluation and/or procedure change.
- Ensure changes to ORAM SFAT logic color determinations meet management expectations regarding outage risk management in accordance with plant procedures.
- Communication of noteworthy changes and how they should be implemented, whether identified through routine screening or by Work Control. If the change affects the ORAM SFAT logic, then the analyst will document it in the site issue tracking system and provide recommended changes.
- Review of existing changes that are documented in the risk group’s continuous update database.

During non-outage periods, there may be changes to the plant, outage procedures, and defense-in-depth (DID) strategies that do not require immediate evaluation. At the discretion of the Risk Assessment and Applications group, these changes may be incorporated into the ORAM model depending on their impact. If the change affects the DID requirements of the ORAM model, the risk analyst will ensure the change is reflected in the next outage evaluation cycle by entering the issue into the risk group’s continuous update database. Similarly, several months prior to the outage, the Assessment and Applications group reviews the outage plan to identify any new or non-standard plant configurations that maybe seen during the upcoming outage. The risk analyst will ensure the change is reflected in the next outage evaluation model prior to the start of the outage.

3. ONLINE RISK ASSESSMENT

An online risk assessment comprises an evaluation of the cumulative effect and/or instantaneous effect on core damage frequency (CDF) and large early release frequency (LERF) when systems and/or components are taken out of service to perform maintenance or testing activities during power operation. These assessments are performed in advance on a weekly basis by the Work Week Coordinators. They are reviewed at the beginning of each shift by the Operations personnel in the

*morenora@westinghouse.com

control room and can be modified by either the Operations or Work Week Coordinators to evaluate emergent component issues if they arise.

Risk is communicated by a series of colors (GREEN, YELLOW, ORANGE and RED). These colors are established by the Risk Assessment and Applications group with input from Operations and Plant Management. The purpose of the colors is to convey the plant risk in a way that is easy to comprehend by everyone at the plant. Increasing the color/risk should promote additional awareness about the critical activities taking place and based on procedure guidance may require the plant to develop risk mitigation actions to reduce the risk. The colors and their meanings used at this site are as follows:

- Risk Category 4 (GREEN) – Relatively **very low** level of risk posed by plant conditions.
- Risk Category 3 (YELLOW) – Relatively **low** level of risk posed by plant conditions. Time spent in these plant conditions should be minimized.
- Risk Category 2 (ORANGE) – Relatively **moderate** level of risk posed by plant conditions. This level of risk warrants Risk Management Actions that may include deferring the work until plant conditions are more favorable (e.g., power reduction or plant shutdown) or compensatory measures to reduce the level of risk. Time spent in these plant conditions should be minimized.
- Risk Category 1 (RED) – Relatively **high** level of risk posed by plant conditions. This level of risk warrants Risk Management Actions that may include deferring the work until plant conditions are more favorable (e.g., power reduction or plant shutdown) or compensatory measures to reduce the level of risk. Time spent in these plant conditions should be minimized and should not be scheduled or voluntarily entered.

Components are included in the weekly online risk assessment if they are within the scope of the Probabilistic Risk Assessment model and are Unavailable to perform their credited risk assessment function. It is worth noting that the online risk assessment can credit components that are Inoperable if they are still considered capable of performing their credited function or can be restored to Available status by an operator action. Based on guidance in NUMARC 93-01 [1], credit for restoration operator action can only be applied if the following criteria can be met:

- The function can be promptly restored either by an operator in the control room or by a dedicated operator stationed locally for that purpose.
- Restoration actions must be contained in a written procedure.
- Restoration must be uncomplicated (a single action or a few simple actions).
- Restoration must not require diagnosis or repair.

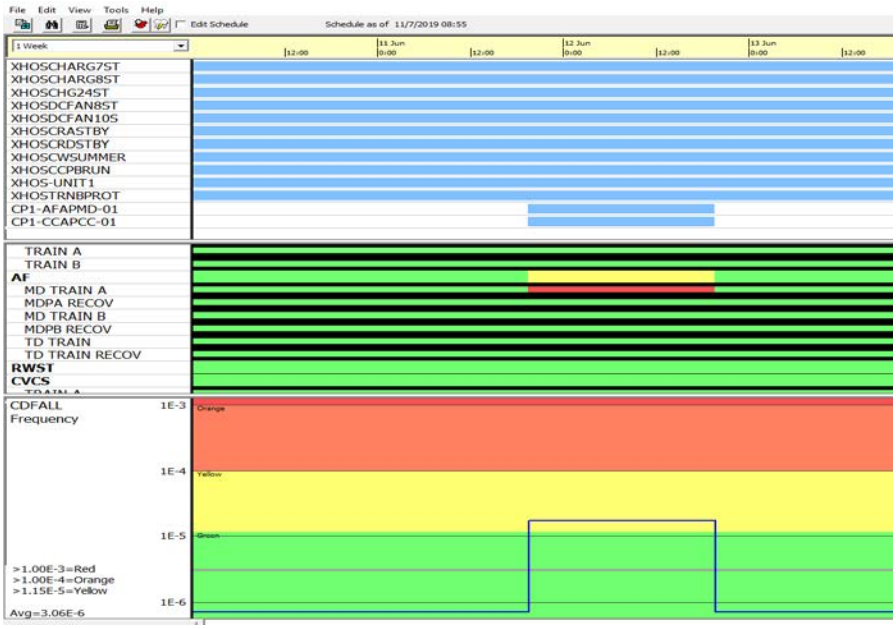
The scheduling process begins 8 weeks prior to the maintenance being performed at the plant. At the T-4 week (4 weeks prior to the work being performed) the schedule is provided to the Work Week Coordinators from the Scheduling group. The Work Week Coordinators begin their process of refining the schedule and they perform the initial risk assessment of the planned work. During their initial risk assessment, they identify high risk evolutions and will adjust the schedule to minimize the peak risk and duration of those activities. Additionally, they will look at the risk peaks to identify if concurrent maintenance activities are cumulatively contributing to the overall risk. If two concurrent activities can be scheduled to be worked in series rather than in parallel, the Work Week Coordinator will modify the planned schedule to transform a single elevated risk evolution into two low risk evolutions. In the example depicted by Figure 1, a motor driven Auxiliary Feedwater pump and a Component Cooling Water pump are initially scheduled to be Out of Service for maintenance at the same time. The resulting risk evaluation (Figure 1) indicates that this configuration results in a YELLOW risk category risk (this can be seen by the step function at the bottom which extends into the yellow region). While YELLOW configurations are permitted to be scheduled, they are avoided if possible. In this case, there is no logical reason these two activities must be worked in parallel so the

*morenora@westinghouse.com

Work Week Coordinator would modify the schedule to perform these activities in series in an effort to reduce the overall risk. The same two activities are shown in Figure 2; however, the schedule has been modified to perform these activities in series rather than concurrently. This modification effectively converts a single YELLOW risk category into two GREEN (low risk) categories as shown in Figure 2.

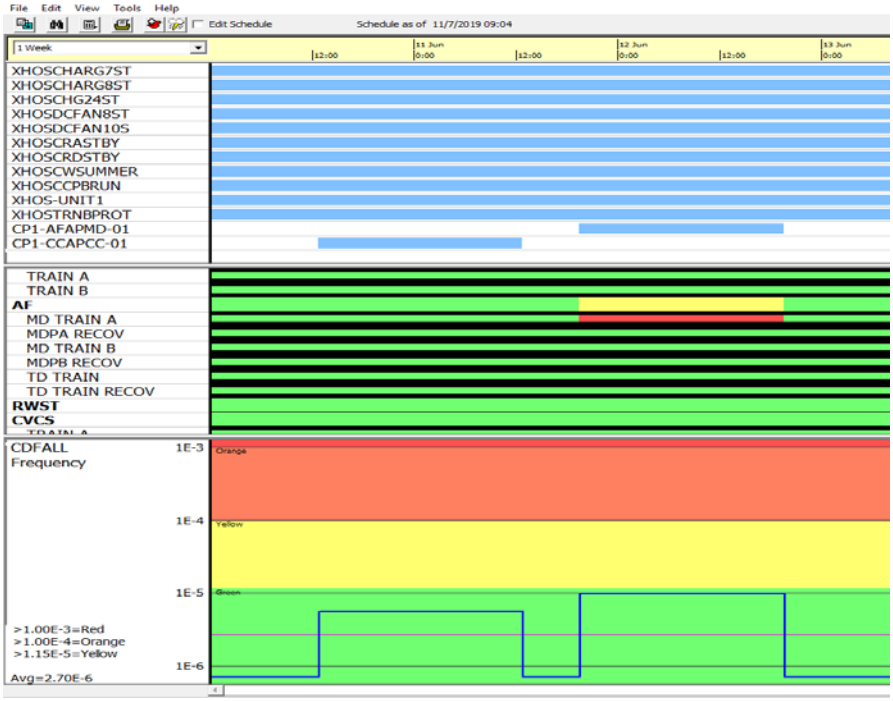
At the T-1 week (the week prior to the maintenance being performed), the schedule receives a risk evaluation by a risk analyst in the Risk Assessment and Applications group. During this risk evaluation, the risk analyst is attempting to identify scheduled activities that may have been inadvertently excluded from the Work Week Coordinator's risk evaluation. Additionally, the review focuses on identifying subtle impacts that may have been missed during prior risk evaluations. This review is also attempting to identify activities that have cross-unit implications or activities in the Switchyard that may increase the likelihood of inducing a Loss of Offsite Power. Additionally, these reviews offer the opportunity for the risk analyst to develop and communicate risk mitigation actions for activities that are greater than GREEN.

Figure 1: Example Initial Maintenance Schedule



*morenora@westinghouse.com

Figure 2: Example Modified Schedule



After the risk evaluation performed by the Risk Assessment and Applications group is completed, the schedule is presented to the Director of Work Management by the responsible Work Week Coordinator. During this presentation, the Director has the responsibility for challenging the schedule to ensure that the maintenance activities have been scheduled in the best sequence possible to minimize risk and that the risk impacts have been properly identified and are understood. Upon approval from the Work Management Director, the schedule is finalized and ready to be executed as planned in the following week.

4. OUTAGE RISK ASSESSMENT

An outage risk assessment comprises an evaluation of approved DID requirements related to each of the required SFATs. Resultant color codes are provided based on the level of DIDs available for that safety function. Time to boil calculations (reactor vessel and spent fuel pool) can modify the number and type of DIDs required for certain SFATs. In addition, ORAM consists of several simplified event trees that are used to gain risk insights for different plant configurations. The risk analysts assess if both adequate DID and appropriate plant configuration risk is maintained, and if determined to be inadequate, provide recommendations that can remedy the configuration.

Prior to the risk analyst performing any model changes or analysis, the analyst will perform baseline verification of the current ORAM model by copying the latest documented ORAM model (usually developed during the last unit refueling outage) and calculating the model with the outage schedule input file (DAT) that was used in its development. The analyst will then compare their results to those documented with the latest model, which validates that the model being used is current. The risk analyst works with Outage Management to ensure ORAM results provide adequate DID measures. The Outage Management and Operations groups determine if additional DID contingency plans (DIDCPs) are required and implement them in accordance with procedure. The risk analyst will incorporate all DIDCPs in effect into the ORAM model.

The Core Design Safety Analysis (CDSA) group performs the outage-specific time-to-boil (TTB) calculations and provides them to Outage Management and the Risk Assessment and Applications

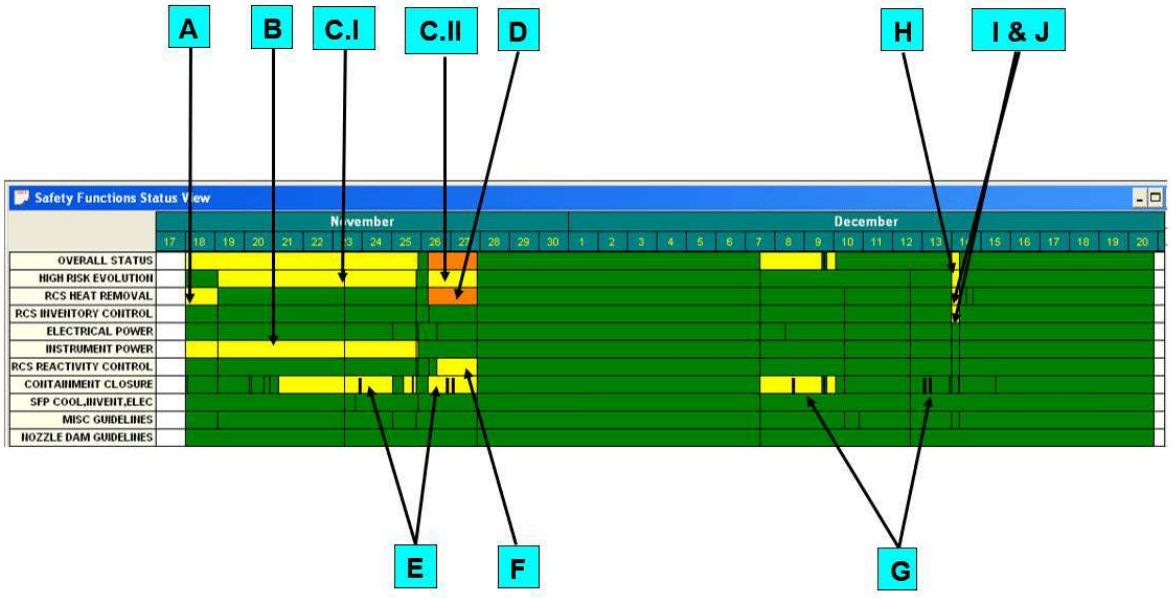
*morenora@westinghouse.com

group. The risk group determines a *best fit* curve that represents the decay heat of the outage unit as a function of time, as shown in the CDSA TTB calculation. This decay heat curve is then entered into the ORAM model along with the various RCS level heat capacities, the minimum time (to commence reactor fuel offload), the fuel ratio, and the spent fuel pool decay heat values. These are entered as user defined variables that are specific to the outage under evaluation.

During preparation for planned outages, Work Control/Outage Management will provide outage scheduling of activities, plant conditions, system availability, and DID contingencies that constitute each of the outage safety functions. The risk analyst performs an analysis, as required by plant management, to determine any ORAM model changes. Plant management will request outage risk determinations during this period to meet planning milestones, which are documented in the PRA evaluation process. The outage risk determinations are required, at a minimum, for schedules prepared four, three, two, and one month(s) ahead of the outage (T-4, T-3, T-2, T-1, etc.). The pre-outage reviews allow for schedule adjustments based on the risk analyses results. Potential changes to the schedule development of contingency plans and/or additional Management oversight are discussed and conclusions/changes documented.

A risk analyst from the Risk Assessment and Applications group will use the schedule provided by the Outage Scheduling group to generate ORAM Safety Function Assessment Tree (SFAT) results for the duration of the outage. An example of a typical outage schedule SFAT result is depicted in Figure 3. The risk analyst will evaluate each elevated risk configuration (denoted by the alpha numeric labels in Figure 3) and determine the specific cause of the risk escalation. The risk analysis documents their findings and presents their results in a series of pre-outage risk review meetings. During these meetings, the risk analyst explains the insights generated via the ORAM SFAT results and provides recommendations to mitigate risk either through schedule modification or risk mitigation actions.

Figure 3: Example ORAM Safety Function Assessment Tree (SFAT) Results



During the course of the outage, changes to the ORAM model may be needed on an emergent basis. These changes will be analyzed by the Risk Assessment and Applications group and approved as necessary. Subsequently, the changes will be communicated to the Work Management group for incorporation and monitored by the risk group to ensure adequate implementation. These emergent

*morenora@westinghouse.com

changes are documented by a revision to the outage specific PRA evaluation and the site issue tracking system.

During planned outages, the risk analyst will monitor and review the daily ORAM SFAT results (Figure 3) and risk profile provided by the Work Management group. The Work Control Center (WCC)/Outage Management will perform daily reviews. Similar to the on-line risk process, risk is communicated by a series of colors (GREEN, YELLOW, ORANGE and RED). These colors are established by the Risk Assessment and Applications group with input from Operations and Plant Management. The purpose of the colors is to convey the plant risk in a way that is easy to comprehend by everyone at the plant. Increasing the color/risk should promote additional awareness about the critical activities taking place and based on procedure guidance may require the plant to develop risk mitigation actions to reduce the risk. If significant changes to the schedule are implemented, the ORAM model is re-evaluated with the revised schedule and the results of that assessment are disseminated to the plant staff. This information includes actual plant conditions during the past 24 hours and the as-scheduled activities for the next 24 hours. The risk analyst will assess this information to ensure no significant impacts to SFAT results (i.e., color change) or risk management actions.

5. RISK COMMUNICATION

Plant Risk is communicated daily during “Plan of the Day” meetings that are held each morning. These meetings are attended by management staff from each of the working groups and are facilitated by the responsible Work Week Coordinator and Operations Shift Manager. During these meetings, the overall plant risk for the day is discussed including any activities that are greater than GREEN. The intent of these meetings is to ensure the management staff is aligned for the day and for them to be able to communicate the plant risk drivers to the working level staff during individual group briefings. This information is also provided to plant personnel via TV monitors located throughout the plants as well as daily newsletters during the outage.

When there are scheduled maintenance activities that put the plant into a YELLOW risk category, the Senior Reactor Operator (SRO) in the Main Control Room makes an announcement over the plant-wide Gaitronics system (integrated plant communication system) prior to the commencement of the activity. The SRO will announce that the plant is entering a YELLOW risk configuration due to maintenance activities on a specified component. This announcement makes the entire plant staff population aware that the plant is entering an increased risk configuration. This information is useful to the general population because it keeps them informed of the increased risk configuration and encourages them to consider how their actions can impact the elevated risk configuration of the plant. Once the maintenance is completed and the component returned to service, the SRO will make an additional site-wide announcement stating that the elevated risk configuration has been exited and that the current plant risk has returned to GREEN.

In the event an emergent component failure occurs, the SRO of the affected unit will evaluate the risk impact using the Online Configuration Risk Monitor in the Main Control Room. If the risk impact is greater than GREEN, the SRO will communicate the risk escalation to the plant management staff. The plant management will use the information as part of their decision-making process when they are developing a recovery strategy. As part of their recovery planning, they will consider the scheduled maintenance activities currently taking place and use the information to make priority decisions regarding resource allocation to reduce the risk and restore the plant as quickly as possible.

In addition, based on the level of expected risk increase and affected mitigating system components (those that are out of service), the plant will implement its “guarded equipment” program and post signs and barriers to protect remaining components.

*morenora@westinghouse.com

4. CONCLUSION

The inception of Maintenance Rule paragraph (a)(4) required nuclear power plants operating in the United States of America to evaluate the risk associated with performing surveillances, post-maintenance testing, corrective maintenance and preventive maintenance prior to performing maintenance activities. Utilities have largely adopted software tools that aid in performing these risk assessments for Online and Outage risk evaluations. At this specific dual-unit site, EPRI's Equipment Out of Service (EOOS) software is used for online risk and Outage Risk Assessment and Management (ORAM) software is used for outage risk configuration.

The software tools serve as an effective method to identify and minimize risk during all Modes of plant operation. The insights gained from these tools are used as an effective means for managing and communicating Core Damage and Large Early Release risk to personnel onsite via an intuitive color system and are critical for providing risk insights during management decision-making. These insights drive plant risk awareness through the use of guarded and protected equipment, the use of barriers and signage and effective plant communications via plant announcements and communications tools such as monitors, newsletters and during meetings. These tools and the results they provide are deeply ingrained in the processes and procedures onsite and are supported or relied upon by multiple work groups including Risk Assessment and Applications, Online Work Control, Refueling Outage Work Control, Operations and Management.

References

[1] NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", Revision 4a.
[2] NRC Regulatory Guide 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," Rev. 3, May 2012.

*morenora@westinghouse.com