■
THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

SHUTDOWN RISK MANAGEMENT APPLIED AT PHILADELPHIA ELECTRIC COMPANY

William J. Dagan and Douglas E. True
ERIN Engineering and Research, Inc.
2175 N. California Blvd., Suite 625
Walnut Creek, California 94596
Fax: (510) 943-7087

Thomas Wilson and William Truax
Philadelphia Electric Company
955-965 Chesterbrook
Wayne, Pennsylvania 19087
Fax: (215) 640-6583

ABSTRACT

The development and implementation of an effective risk management program requires basic risk or safety knowledge and the conversion of such information into effective management tools. ERIN Engineering and Research, Inc., under contract to the Electric Power Research Institute, has developed an effective program, Outage Risk Assessment and Management (ORAM), to provide plant and management personnel with understandable results of shutdown risk studies. With this tool, the impact of plans and decision options can be readily determined and displayed for the decision maker. This paper describes these methods and their application to the Limerick Nuclear Station of Philadelphia Electric Company. It also sets forth a broader application of these methods to include support of management decisions at-power and following forced outages. The result is an integrated risk management framework which can allow management and technical personnel to utilize readily available and understandable risk insights to optimize each activity.

This paper addresses the resolution of several key issues in detail:

- How was the ORAM risk management method employed to represent the existing plant shutdown procedures and policies?
- How did the ORAM risk management method enhance the decision-making ability of the outage management staff?
- How was the ORAM software efficiently integrated with the outage scheduling software?
- How is quantitative risk information generated and used for outage planning and control?

The ORAM risk management philosophy utilizes a series of colors to depict various risk configurations. Each such configuration has associated with it clear guidance. By modifying the conditions existing in the plant it is possible to impact the type of risk being encountered as well as the guidance which is appropriate for that period. In addition, the duration of a particular configuration can be effectively managed to reduce the overall risk impact. These are achieved with minimal interactive reliance upon risk models but with clear, well founded analytical bases.

This methodology is being expanded to address both forced outage and at-power configurations. The result will provide a consistent framework which relies upon appropriate models for each configuration but presents consistent understandable information to management and decision makers. The use of such tools clearly represents an opportunity to improve the decision making process and enhance overall operational effectiveness. This paper includes examples of shutdown, at-power, and forced outage situations and presents management guidance appropriate for such cases. Several analytical methods currently being used are presented.

BACKGROUND

The Outage Risk Assessment and Management (ORAM) program was developed by the Electric Power Research Institute (EPRI) based on technical methods developed by ERIN Engineering and Research, Inc. (ERIN). It is a comprehensive program to assess the relative risk and safety for all evolutions throughout an outage. Thus far the technology has been applied effectively to refueling outages. The program is being further extended to encompass forced outages and power operations.

The ORAM program grew from shutdown safety studies originating in early 1991. EPRI recognized a need for heightened awareness in the area of shutdown risk as a result of various events and initiatives. The US Nuclear Regulatory Commission (NRC) announced a multi-faceted assessment to determine the need for additional regulations and controls at shutdown. Also, the Institute of Nuclear Power Operations (INPO) began a compilation of industry events at shutdown and commenced outage review visits. In addition, the US Nuclear Management and Resource Council (NUMARC) formed a working group on shutdown issues and issued a generic industry response in NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management".

There are two main features of the ORAM program: (1) a Probabilistic Shutdown Safety Assessment (PSSA) and (2) Risk Management Guidelines (RMGs). Both features can be used to achieve different objectives. They can be developed separately, but ultimately the two elements can be used most effectively to complement each other.

PROBABILISTIC SHUTDOWN SAFETY ASSESSMENT

The PSSA employs the basic principles of a Probabilistic Safety Assessment (PSA) to quantify endstate frequencies for various initiating events considering thermal hydraulic aspects, failed human actions, equipment unavailabilities, and safety function equipment failures. Endstates include not only core damage, but also bulk core boiling, fuel pool boiling, and others. Equipment unavailabilities and failure probabilities are quantified. Results include a timeline of endstate frequencies during an actual outage.

These safety assessments have several purposes, including (1) identifying insights for inclusion in the plant-specific risk management guidelines, (2) identifying insights of generic value for use by other utilities in their application of the risk management guideline's process, (3) identifying issues regarding shutdown risk that require further investigation, and (4) providing a plant model for evaluation of future outages.

The basic elements of PSSA include the following:

- The outage is represented as a series of plant states.
- Plant thermal hydraulic considerations are included in the model.
- System dependencies are captured in Fault Trees.
- Initiating events for each end state are developed.

During an outage, the thermal hydraulic analysis is a key input to the endstates under consideration. Decay heat is a function of time after shutdown. As decay heat decreases, it takes more time to progress from a initiating event to RCS boiling to excess fuel temperature. The thermal hydraulic analysis also provides insights such as the applicability of certain backup systems to remove decay heat.

An outage (or power evolution) is broken up into a Plant States Database (PSDB). The PSDB contains plant configurations and maintenance activities which are important to risk and safety. A common PSDB is employed in both the PSSA and RMG modules of ORAM. Figure 1 shows an example PSDB record representing a snapshot in time during the last Limerick Generating Station Unit 2 outage.

System dependencies are captured within fault trees in a similar but less complicated manner as those employed for full power PRA models. The initiating events considered in the PSSA reflect challenges to safety functions in the shutdown configurations. Decay heat removal and inventory control are the primary safety functions challenged which could result in the RCS Boiling and/or Core Damage end states. The following represents typical initiating events employed in PSSA models:

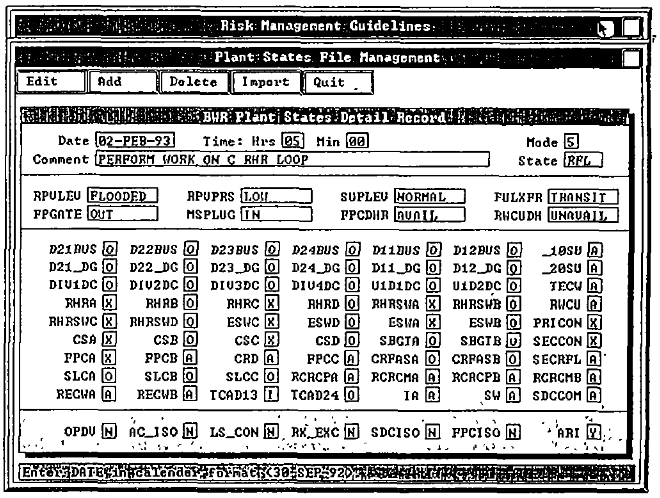
- DHR Pump Failure
- Loss of Offsite Power
- Loss of AC Power Bus
- RPV/SDC Isolation
- LOCAs
- RPV Draindown Events

In the PSSA, time-dependent analytical expressions rather than point estimates are used to model the initiating events. The use of analytical expressions allows more effective consideration of the unique plant states, thermal hydraulic considerations, human performance and hardware reliability.

RISK MANAGEMENT GUIDELINES

The Risk Management Guideline (RMG) framework of the ORAM program forms the basis for complete and consistent safety reviews of outages and activities at-power during the planning phase, the actual outage or plant evolution, and for post outage/evolution critiques. The RMG module provides a methodology to improve the technical basis for safety management decisions. It focuses on two important inputs: (i) a measure of defense in depth, given plant conditions, and (ii) safety enhancement actions commensurate with the degree of defense in depth. This methodology further provides discipline to the decision process and attempts to remove subjectivity from the process. The result is an approach to safety management which produces traceable and repeatable decisions.

Using RMGs for outage evaluation, each outage is divided into a series of discrete plant states defined by plant mode, availability of RCS inventory, and RCS configuration. Each plant state is reviewed relative to several key safety functions. The following reflect typical safety functions monitored which mimic those delineated in NUMARC 91-06:


Risk Management Guidelines
Plant States File Management
Edit
Add
Delete
Import
Quit
BWR Plant States Detail Record

Date 02-FEB-93 Time: Hrs 05 Min 00 Mode 5
Comment PERFORM WORK ON C RHR LOOP State RFL

RPVLEV	FLOODED	RPVPRS	LOW	SUPLEV	NORMAL	FULXFR	TRANSIT
FPGATE	OUT	MSPLUG	IN	FPCDHR	AVAIL	RWCUDH	UNAVAIL

D21BUS O	D22BUS O	D23BUS O	D24BUS O	D11BUS O	D12BUS O	_10SU A
D21_DG O	D22_DG O	D23_DG O	D24_DG O	D11_DG O	D12_DG O	_20SU A
DIV1DC O	DIV2DC O	DIV3DC O	DIV4DC O	U1D1DC O	U1D2DC O	TECW A
RHRA X	RHRB O	RHRC X	RHRD O	RHRSWA X	RHRSWB O	RWCU A
RHRSWC X	RHRSWD O	ESWC X	ESWD O	ESWA X	ESWB O	PRICON X
CSA X	CSB O	CSC X	CSD O	SBGTA O	SBGTB U	SECCON X
FPCA X	FPCB A	CRD A	FPCC A	CRFASA O	CRFASB O	SECRPL A
SLCA O	SLCB O	SLCC O	RCRCPA A	RCRCMA A	RCRCPB A	RCRCMB A
RECWA A	RECWB A	TCAD13 I	TCAD24 O	IA A	SW A	SDCCOM A
OPDV N	AC_ISO N	LS_CON N	RX_EXC N	SDCISO N	FPCISO N	ARI Y

Enter DATE in calendar format (30-SEP-92)

Figure 1 - LGS Plant States Editor Screen

- Decay Heat Removal
- Inventory Control
- Electric Power Control
- Reactivity Control
- Containment Control

The relative reliability of each safety function is determined by decision logic contained in shutdown safety function assessment trees. A "color" is assigned to the safety function indicating the relative degree to which the safety function is supported. Colors range from green through yellow, orange, and red. The color determines the defense in depth for a selected safety function in a given plant state, and how well the plant is managed in that condition determines the risk. Risk management guideline documents will exist for each color, for each safety function, and for each plant state. The risk management guidelines are a compendium of information of risk significance for the condition under review.

Within the ORAM software, plant personnel are given the opportunity to respond to each RMG with explanation for the particular action taken. Thus, permanent records of actions and justifications before, during and after an outage or power evolution can be kept.

AUTOMATING THE PROCESS

Both the PSSA and the RMGs can be automated by direct linkage of the common Plant States Database with outage scheduling programs, automated plant tagging systems, or potentially Safety Parameter Display Systems (SPDS). The advantage of this interface is the ability to rapidly assess a change or numerous changes to a schedule or equipment availability. The ORAM code requires a generic interface file which can be generated from a number of sources including those listed above. The ORAM models were automated with remarkable success during the last Limerick Generating Station (LGS) Unit 2 refueling outage. Other applications for forced outages and at-power evolutions are also being considered by Philadelphia Electric Company (PECo) management.

APPLICATIONS DURING A REFUELING OUTAGE

The ORAM program was used effectively during the LGS Unit 2 refueling outage which ended in March 1993. In fact, the use of ORAM played an important factor in enabling plant management to achieve a record outage of 53 days which was 15 days ahead of the original plan. Daily use of ORAM helped give plant personnel confidence that they were not overlooking safety as they accelerated the schedule. In addition, using the software to conduct "what-if" scenarios showed that they could do various activities in parallel with no decrease in their defense in depth requirements and little or no affect on plant risk.

Daily use was facilitated during the Limerick outage by linking the ORAM model to the outage scheduling software, PREMIS. Each day when the outage schedule was updated, a file containing information on specific activities and configuration changes was downloaded directly to the ORAM program. Reevaluation of the PSSA and RMG models then yielded changes in risk and safety directly resulting from the updated schedule. This enabled plant personnel to obtain a rapid assessment from a safety perspective and helped streamline the decision process regarding additional changes to the outage schedule.

Limerick outage management also manually changed system status within the ORAM model for those cases when equipment became unavailable and the outage scheduling software was not updated accordingly. This increased the effectiveness of the ORAM tool to evaluate defense in depth and relative risk based on actual plant conditions in addition to those that are planned.

A risk profile graph for the RCS Boiling endstate for the LGS outage is shown in Figure 2. The units are per hour rather than per year. At the start of the outage, the risk is highest with lower water level and decay heat at its highest. Here the risk of boiling roughly follows the decay heat curve. Upon floodup, the risk of boiling drops significantly. The small dip in risk around day 7 represents the time when the Fuel Pool gates were removed just prior to the Fuel Pool Cooling System being removed for maintenance. Therefore, for a short period, the Fuel Pool Cooling System also acted as a decay heat removal mechanism. The elevated plateau from day 10 to day 15 represents RHR Train A and C out of service. After approximately 15 days, the risk of boiling bottoms out. This is the point where thermal hydraulic analysis indicated that the time to boiling exceeded 24 hours in the flooded up configuration. The risk analysis assumed that external measures would be employed to prevent RCS boiling within a 24 hour period. Therefore, the only contribution to boiling after 15 days is from LOCA or draindown events. Around day 38, the water level was lowered for RPV reassembly. However, Division 4 DC power was also unavailable for a couple days at this time yielding a more elevated risk to boil. Finally, the last risk profile is the combination of the RPV hydro followed by a common RHR Shutdown Cooling outage.

The core damage risk profile for the LGS Unit 2 outage is given in Figure 3. Again the risk is highest at the start of the outage when the vessel head is removed and the cavity is not flooded. After floodup, risk of core damage drops significantly as would be expected. LOCA and draindown events dominate risk during the flooded up configuration. The elevated plateaus indicate periods when two of the four electrical divisions were removed from service in parallel. This rendered two RHR LPCI trains and one loop of Core Spray unavailability for injection.

Thus it can be seen that changes in the risk profiles for both RCS boiling and core damage can be directly attributed to ongoing outage activities or changes to outage configurations. Furthermore, changes in the outage which affected risk were shown on updated risk profiles through interface with the outage scheduling software.

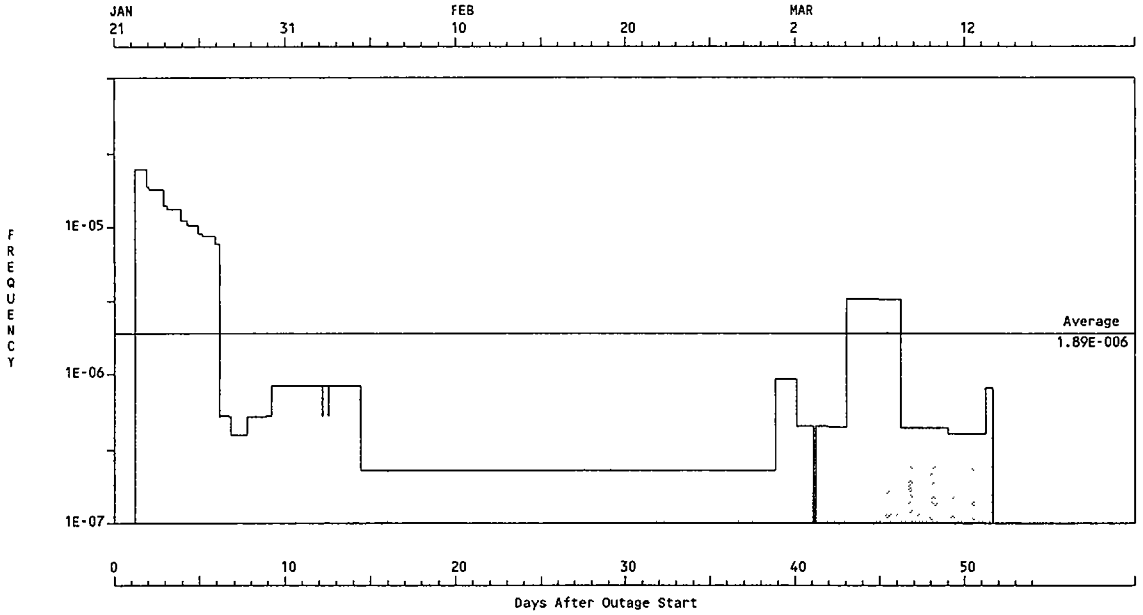


Figure 2 - LGS RCS Boiling Profile

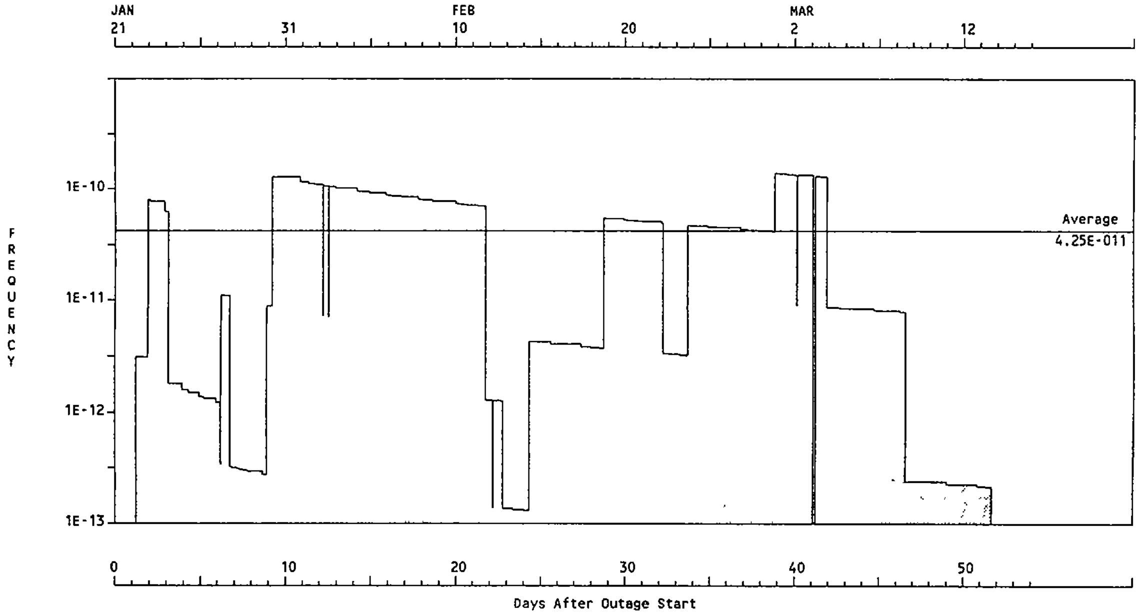
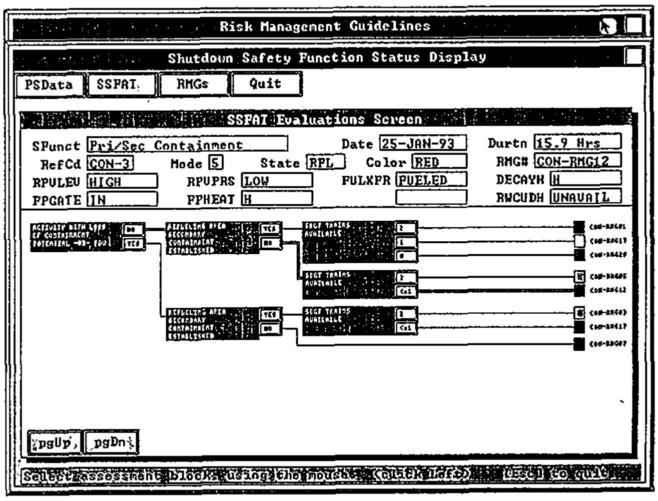


Figure 3 - LGS Core Damage Risk Profile

The overall outage RMG evaluation is illustrated in Figure 4. Here, the "green" indication in most safety functions throughout the outage reflects a relative safe outage philosophy. There are a number of "yellow" conditions in several safety functions which represent a change of defense in depth status to a slightly lower state, but still acceptable risk. The "orange" conditions which exist are categorized by Limerick management as higher risk, in which case, contingency plans should be in place prior to entering into an "orange" state.

The one "red" condition within Containment Control resulted from an unplanned evolution. Figure 5 shows the Shutdown Safety Function Assessment Tree (SSFAT) flowpath which processed that "red" state at that snapshot in time in the outage. Some information is given in the top portion of the SSFAT. In this case, the reactor was FUELED, the decay heat is High, the RPV Level is HIGH (at the flange as opposed to flooded up), and the Reactor Mode is 5 which indicates that the RPV head is removed. Therefore, this is early in the outage when the inventory is low, decay heat is high and the vessel has just been disassembled.

The first SSFAT decision box monitors if an activity directly affecting the containment or a potential for draining the vessel (PDV) is taking place. The presence of this decision block gives plant personnel the ability to highlight certain activities within the outage as having a detrimental affect on a particular safety function. In this case, no such activity was taking place. The next decision block checks for the availability of secondary containment. In this case, Secondary Containment was not available. The next block checks the number of Standby Gas Treatment (SBGT) trains available as a defense in depth mechanism. Here, one or less trains were available so a "red" condition was processed.


Risk Management Guidelines
Shutdown Safety Function Status Display
PSData
SSFAT
RMGs
Quit
SSFAT Evaluations Screen
pgUp
pgDn

SFunct Pri/Sec Containment
Date 25-JAN-93
Durtn 15.9 Hrs
RefCd CON-3
Mode 5
State RPL
Color RED
RMG# CON-RMG12
RPVLEV HIGH
RPVPRS LOW
FULXFR FUELED
DECAYH H
PPGATE IN
PPHEAT H
RWCUDH UNAVAIL

Select assessment block using the mouse (click left) [ESC] to quit

Figure 5 - SSFAT Flow Path Reflecting LGS "Red" Condition

Both trains were planned to be available in this configuration, but a damper failure rendered one train unavailable. This was a case where Limerick personnel manually updated the ORAM database to reflect actual plant conditions. The code then reflected this state showing the need for added caution and contingency planning. Specific cautionary measures could then be assessed by selecting the Risk Management Guidelines associated with this particular end condition.

It should be noted that the structure of the SSFAT decision logic is completely user-specified and can be established to suit each individual plants needs. In the above case, the resulting "red" condition did not reflect a Technical Specification requirement, but instead a requirement plant personnel administratively imposed to assure desired degrees

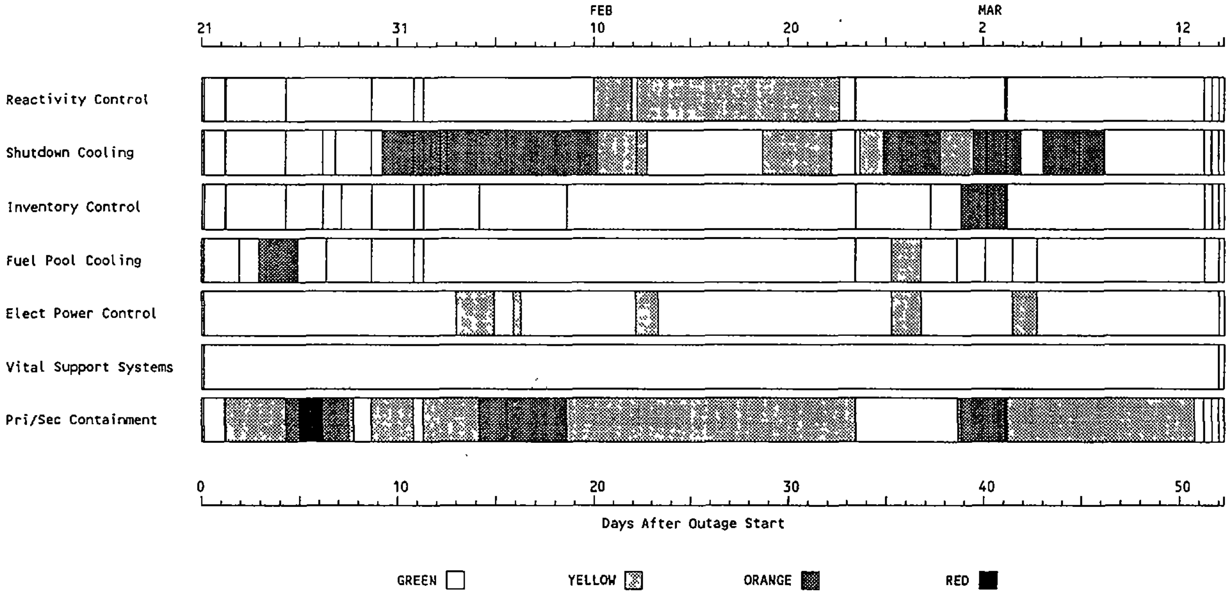


Figure 4 - LGS Safety Function Status Display

of defense in depth. Alternately, SSFAT logic could be developed for Technical Specification considerations, as may be the case if using this approach to evaluate at-power evolutions.

Therefore, the use of colors to indicate level of defense in depth or adherence to other administrative requirements gives plant personnel an overall view of where increased caution or contingencies are warranted throughout the outage. The ORAM code also provides traceability to allow personnel to determine how and why the defense in depth changed and to access applicable guidelines for the situation. Limerick plant personnel used this tool extensively to not only follow changes in defense in depth automatically through linkage with their outage scheduling software, but also to conduct numerous "what-if" test cases. This helped streamline the outage by indicating cases where activities could be conducted in parallel with no affect on defense in depth.

APPLICATIONS FOR FORCED OUTAGES

This methodology is being expanded to address forced outages and at-power evolutions. For forced outages, an ORAM model similar to that for refueling outages could be used to reflect considerations which are pertinent to the situation. This would yield a uniform and systematic practice for making decisions relative to plant safety and increased plant availability. Used in conjunction with an "at-power" model, decisions involving performing certain maintenance within the outage or allowing it to be done at-power could be weighed from a risk and safety perspective.

USE DURING AT-POWER EVOLUTIONS

Expanding this methodology to encompass at-power conditions will serve to analyze maintenance and testing activities from a total safety perspective no matter where it is being performed. These techniques could be used to justify performing additional activities at-power rather than within forced or refueling outages. The at-power tool could interface with power IPE models to create a real-time "risk indicator". The relative risk of performing an activity during shutdown could be compared to the affect on risk at-power. For instance, if a maintenance activity results in a peak in the outage risk, but has negligible affect on the power risk profile, then the activity is a candidate for consideration at-power.

The Risk Management Guideline tools could be expanded to encompass at-power considerations such as adherence to plant Technical Specifications. The effect of equipment unavailability could be weighed against requirements and systematically compared with other requirements on redundant or alternate systems for early warning of potential conflicts or to exercise increased caution. For instance, an instrument failure in itself may not be a problem with respect to plant operations or Technical Specifications. However, the failure of a related or backup instrument may put the plant in a LCO forcing shutdown. Appropriate guidance could be referenced which would direct personnel to increased caution and awareness for protecting the availability of the other instrument in this case. This would result in increased availability for the plant.

Similar philosophy could be used for evaluating planned maintenance windows with simultaneous out-of-service equipment at-power. Both the affect on plant risk and the effect on plant requirements can be systematically evaluated. The use of such tools clearly represents an opportunity to improve the decision making process and enhance overall operational effectiveness.