Proceedings of the Korean Nuclear Spring Meeting
Gyeong ju, Korea, May 2003

# Defense-in-Depth Risk Evaluation Model Development Strategy for Plant Configuration Risk Management of Pressurized Heavy Water Reactor Low Power/Shutdown Operation

Huichang Yang, Chang Hyun Chung

Seoul National University
Sinlim-dong San 56-1, Kwanak-Gu
Seoul, Korea 151-742

Gi Yong Kim, Moon Hak Jee, Chang Kyoung Sung

Korea Electric Power Research Institute
Moonji-dong, Yusung-Gu
Taejun, Korea 305-380

## Abstract

Configurations in nuclear power plants are defined by the outage status of plant equipment such as components, trains and systems. Equipment outage can occur by the maintenance or the unplanned equipment failures during power operation or low power/shutdown operation. The Configuration risk management plans were not developed for the low power/shutdown operation of pressurized heavy water reactors in Korea. In this study, the development strategy for the defense-in-depth risk evaluation model was developed as the part of the configuration risk management program for the low power/shutdown operation of pressurized heavy water reactors.

## 1. Introduction

Configurations in nuclear power plants are defined by the outage status of plant equipment. Equipment outage can occur by the maintenance or the unplanned equipment failures during power operation or low power/shutdown operation. The risk management plans were not developed for the low power/shutdown operation of pressurized heavy water reactors in Korea yet. In this study, the development strategy for the defense-in-depth risk evaluation model was developed as the part of the configuration risk management program for the low power/shutdown operation of pressurized heavy water reactors.

In US, many nuclear power plant utilities use the risk evaluation models which consist of qualitative and quantitative risk evaluation models. The qualitative risk evaluation models were developed to assess the defense-in-depth level using the decision trees such as Safety Function Assessment Trees(SFAT) and Plant Transient Assessment Trees(PTAT). The quantitative risk evaluation model used the PSA models.

The risk evaluation tools for configuration risk management(CRM) had or are being developed to equip such qualitative and quantitative evaluation capacity. In general, Equipment Out-Of-Service(EOOS), ORAM-Sentinel and Safety Monitor were used for the CRM purpose. Currently in US, for full-power CRM, about 30% of the US plants use the EPRI-developed ORAM-Sentinel program, 30% use the EPRI-developed EOOS program, 30% use the SCIENTECH-developed Safety Monitor program, and about 10% use tools and methods developed by individual utilities. For shutdown, it was estimated that about 70% of the plants use the ORAM-Sentinel program, about 10% use EOOS, 10% use Safety Monitor, and about 20% use utility-developed programs. The shutdown usage totals to greater than 100% because some utilities use multiple tools simultaneously during shutdown, such as ORAM and Safety Monitor. CRM tools are compared in table 1.

Table 1. Current Status of CRM Tools.

| CRM Tools | Application Status | | Developer | Main Features | Development Plan |
|---|---|---|---|---|---|
| | At Power | Low Power /Shutdown | | | |
| Utility Independent | ~ 10% | ~ 20% | Each Utility | Simple Functions. Using Commercial Database and Spreadsheets. | Being changed into other risk monitors. |
| ORAM-Sentinel | ~ 30% | ~ 70% | EPRI | - At Power Qualitative Evaluation. PSA results are used as lookup table.<br>- LP/SD Qualitative Evaluation using SFATs | There is no further development by EPRI.<br><br>Exelon independent code, PARAGON is under development. |
| EOOS | ~ 30% | ~ 10% | EPRI | Quantitative Evaluation using PSA model for at-power and LP/SD. Qualitative Evaluation Features are being developed. | Unidentified |
| Safety Monitor | ~ 30% | ~ 10% | SCIENTECH | Both qualitative and quantitative evaluation possible<br><br>Using PSA model and SFATs | Qualitative Evaluation Capacity using SFATs were almost completed. |

For the CRM of PHWR in Korea, the appropriate CRM tool should be determined. The requirements for the CRM tool for this study are as below.

- Plant model availability
- Qualitative risk evaluation capability
- Quantitative risk evaluation capability
- Complementary qualitative risk evaluation capability
- Complementary quantitative risk evaluation capability

Beside these requirements, the current status of available resources in terms of risk evaluation for PHWR in Korea should be considered. For Wolsung nuclear units, the plant models for on-line risk evaluation are not developed yet while the CRM tools such as EOOS and Safety Monitor, which have capability of quantitative evaluation, utilize the plant model specified as risk monitoring model. In addition, the risk models for LP/SD operation of Korean PHWRs are not developed. Therefore the CRMP should be developed using rather qualitative methods than quantitative methods especially for LP/SP operation. From this point of view, ORAM-Sentinel and Safety Monitor can be used for the development of CRMP for Wolsung PHWRs. In this research, ORAM-Sentinel version 3.0 was chosen as the tool for PHWR CRMP development.

For Wolsung Nuclear Unit 2, the improved standard technical specifications are be developed and revised for years, and Wolsung 2 has almost same design features with Wolsung 3 and 4. Therefore, there will be much advantage to select the reference plant for this research as Wolsung 2.

## 2. ORAM-Sentinel Methodology

ORAM-Sentinel provides assessments of plant safety based on availability of equipment important to safety and the potential loss of equipment due to plant activities. These configurations are compared against the station procedures, policies, regulatory requirements, and engineering and operational personnel expertise. Plant configurations are defined by equipment availability and unavailability, and evolutions that can potentially lead to plant transient conditions or have the potential to degrade defense-in-depth. These configurations are evaluated using both quantitative and qualitative techniques to develop overall assessment of safety. The assessments performed by ORAM-Sentinel include Safety Function Assessment, Plant Transient Assessment, Integrated Safety Assessment, PSA and PSSA results and System Performance Criteria, and these elements of ORAM-Sentinel safety assessments are shown in figure 1.

The overall safety status of plant is expressed by colors in ORAM-Sentinel. The basis for establishing an SFAT “color” is often based upon the plant management philosophy. At some plants, the colors may be assigned based upon the number of available mitigating systems that are available. At other plants, a “green” level might mean that all Tech Spec-required equipment is available; “yellow” might mean that one LCO is in effect, and “orange” might mean that more than one LCO is in effect. At all plants, a “Red” color generally reflects a disallowed configuration. The levels of defense-in-depth expressed by colors can be determined by the number of the degraded safety systems or functions. General definition and basis for color statement is presented in table 2.

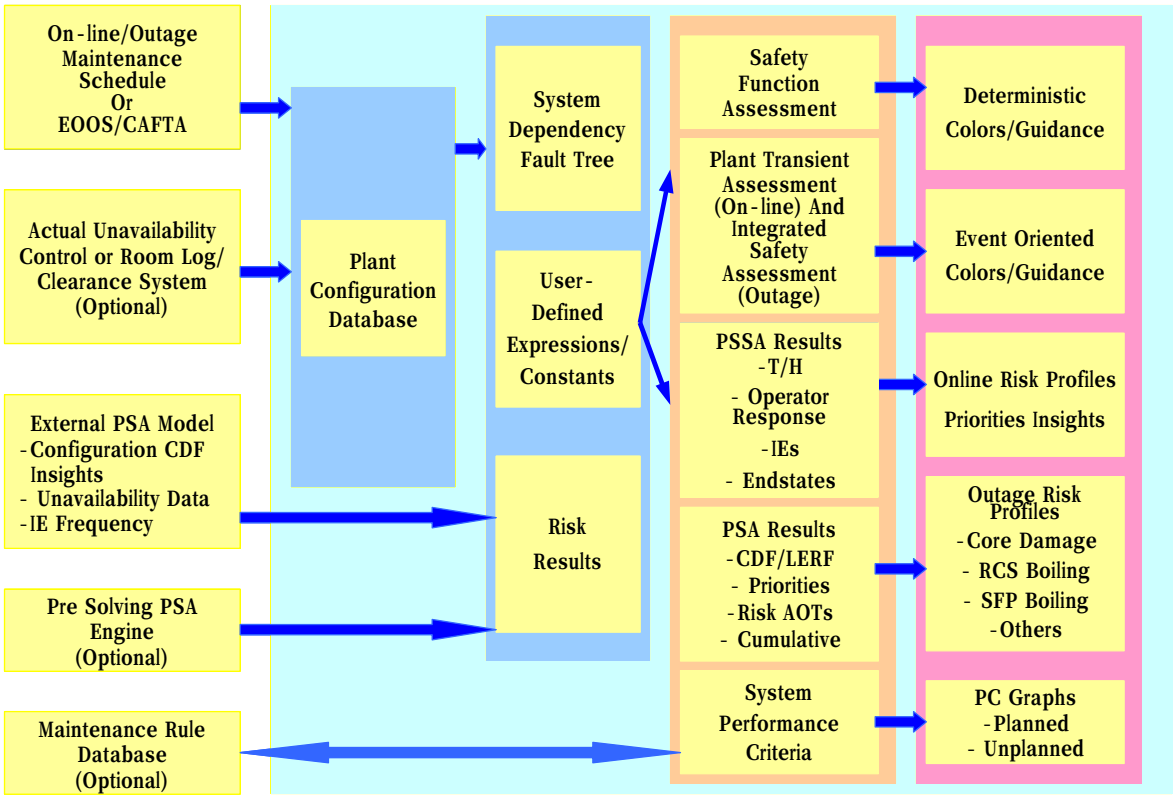


Figure 1. ORAM-Sentinel Overview

Table 2. General Definition of Overall Plant Safety Status

| Color | Definition and Basis |
|---|---|
| Red | Defense-in-depth is extremely challenged for restoration of the safety function under some or all accident events. This configuration should not be entered into voluntarily. Additionally, a Technical Specification Violation results in a RED result. |
| Orange | Defense-in-depth is marginal for the safety function. This color usually indicates multiple LCOs are in effect. |
| Yellow | Defense-in-depth is degraded, but is adequate for the safety function.<br>Usually the plant is in a technical specification LCO. |
| Green | Defense-in-depth is well maintained, or maximum, for the safety function. |

## 3. PHWR Configuration Risk Management Program Development Strategy

The typical plant elements that should be considered in a CRM program are as below:

- Removal of equipment from service and the restoration of the equipment to service.
- Changes in plant operating mode, including mode changes, important changes in operating temperature changes, water levels and pressures that could affect the plant response to various accidents and mitigating systems that might be available/unavailable.
- Changes in the operating alignment of risk-affecting systems, such as changes in status of running pumps, compressors, etc. Also, if the plant has components that could be aligned to different trains of the system, then the train that the component is aligned to can have a risk impact.
- The presence of environmental factors, such as severe weather, low temperatures, etc. that could change the likelihood of various accident and transient events.
- The performance of routine plant maintenance and testing activities that could affect the likelihood of a plant transient (such as a plant trip or a loss of power) if an error is made during the performance of the activity.

The strategy and procedures for the PHWR CRMP development was established through this study and those are as below.

(1) LP/SD Operation Analysis
    1) Operational modes
    2) Outage type
    3) Determination of POS classification factors
    4) Operation procedure analysis
    5) Plant Operational Status(POS) classification
    6) Estimation of average duration time for each POS
    7) Identification of safety function required for each POS
    8) Identification of systems and components which perform the safety functions need for each POS

(2) Plant Configuration Database(PCDB) Development
    1) Component/Train Variables
    2) Configuration Variables
    3) High risk evolution variables

(3) SFAT development
    1) Safety Function Definition
    2) Filter development
    3) SFAT logic development

(4) PTAT development
    1) Initiating event definition
    2) Filter development
    3) PTAT logic development

(5) Plant Safety Evaluation

(6) CRMP Development

## 4. Plant Configuration Database Development for Wolsung 2

From the analysis on the operational modes defined by the standard technical specifications those have been developed and revised by Korea Electric Power Corporation and Korea Electric Power Research Institute, critical safety functions were classified for each operational mode. By the safety functions required by technical specifications, components, trains and systems were identified which should be included plant configuration database as the variables which represents the plant safety status during low power/shutdown operation. For each plant configuration database variables, suitable status was assigned for the proper representation of equipment outage status. In addition to the analysis on the requirements in technical specifications, the plant startup and shutdown procedures were analyzed for the purpose of complement to the items derived from the previous analysis. Every item should be checked by the startup and shutdown procedures but excluded by the technical specifications were included as plant configuration variables. For selected components, trains and systems, it was decided that which item should be included in plant configuration database in component level or train or system level. For the effectiveness, plant configuration variable may not represent component. It can represent the component, or train or system or operational mode. Based on the plant configuration database and variables, plant safety status will be traced and assessed. The safety function assessment tree on the basis of developed database will be developed in future.

The objectives of risk monitoring system such as ORAM-Sentinel is to provide the information which include the actions to be taken to maintain the defense-in-depth of plants during online, and low power and shutdown operation. These risk monitoring systems can also provide the perspectives to minimize the overall risk level by controlling configurations of safe significant systems, trains and components during the maintenance scheduling processes. To perform these objectives, the safety functions those are necessary to maintain the plant within safe range of risk should be defined clearly and the criteria for this definition of safe function is the defense-in-depth concept of plant. To develop the logic to determine whether the safety function is successful or not, the plant configuration database should be developed, and the variables which consist of plant configuration database are selected in that manner the system, trains and components can represent the safety function of plant. The most important criteria in selecting the plant configuration database variables is such variables can represent the plant safety functions.

For this reason, the primary reference for selecting the plant configuration database variables in this study, was chosen as the technical specifications. The technical specifications contains the minimum requirements which should be followed during plant operations at any circumstances for the plant safety and such requirements were expressed as the limiting conditions for operation. In other words, the systems and components mentioned in the technical specifications are necessary for maintaining the plant in safe status. For this reason, the first category of plant configuration variables was chosen through the analysis of the technical specifications by listing the safety function and requirements presented in technical specifications.

The second reference for selecting the plant configuration database variable is the startup and shutdown operation procedures. In these procedures, the items should be checked during startup and shutdown operations to assure the plant safety are listed. Compared with the items derived from the analysis for the technical specifications, the items those should be included in plant configuration database were derived.

The third reference is the emergency operation procedures. In the procedures, the safety functions and the systems/components whose function should be kept online during abnormal

status of plant. These items should be included in plant configuration database.

Through the analysis, the PCDB was developed partly, and the configuration variables and high risk evolution variables will be selected soon. The analysis and the PCDB variable selection results was shown in table 3 as example. The level of modeling can be differ by which approach was adopted. Using the system dependency fault trees, the number of variables needed for the determination of plant configuration can be reduced. Otherwise, modeling the components in detailed level, the whole number of PCDB variables can be increased but the necessity of system fault tress will be reduced. By the type of the information sources those the model developer or plant operator can get, the modeling approach should be changed.

## 5. Safety Functions for Wolsung 2

Safety functions can be defined in terms of the plant operational status, or which safety function is required for a specific POS. Safety function definitions used by some US plants were presented in table 4. Among the assessment functions of ORAM-Sentinel, safety function assessment using SFAT is the largest portion of plant overall safety status assessment especially for LP/SD operation. Therefore the development of SFAT for PHWR was focused through study and the preliminary safety functions for Wolsung 2 were classified and presented in table 5. Main safety systems perform the multiple safety functions depending on the situation to which plant entered. Therefore the safety system classification in table 5 can be altered by the POS classification and such alteration cab be reflected by developing different filters and SFAT related to the appropriate filter.

## 6. Conclusion

The strategy and procedures for the PHWR CRMP development was established through this study, and the risk evaluation model for PHWR LP/SD operation in terms of defense-in-depth were developed partly. Considering the resources available for the risk assessment, the qualitative evaluation features of this strategy can contribute to the effective risk management and to the development of risk management program. The plant safety status assessment model which will be developed through this research can be utilized in the development of ISTS or RISTS also.

## 7. References


1. U.S. NRC, "An Approach for Plant Specific, Risk-Informed Decisionmaking: Technical Specifications," Regulatory Guide 1.177, 1998
2. P. K. Samanta et al., "Handbook of Methods for Risk-Based Anayses of Technical Specifications," NUREG-6141, 1994
3. T. L. Chu et al., “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1 : Analysis of Core Damage Frequency from Internal Events During Mid_Loop Operations," NUREG/CR-6144, 1994
4. OECD WG Risk and IAEA, "Risk Monitors, A Report on the State of the art," Draft 1, 2002
5. EPRI, "ORAM-Sentinel User's Manual Version 3.0," EPRI TR-107018, 1997
6. EPRI, "ORAM-Sentinel Development and ORAM Integration at Catawba and McGuire," EPRI TR-106802, 1998

Table 3. An Example of PCDB Variable for PHWR

| System | Component | Operational Mode | PCDB Variable | Description | Value | Safety Function |
|---|---|---|---|---|---|---|
| SDS1 | SOR | 1,2,3,4,5 | U2SDS1SOR | UNIT2 SDS1 SHUTOFF RODS | A, X | Reactivity Control |
| SDS2 | Poison Tank | 1,2,3,4,5 | U2SDS2_3471TK1<br>U2SDS2_3471TK2<br>U2SDS2_3471TK3<br>U2SDS2_3471TK4<br>U2SDS2_3471TK5<br>U2SDS2_3471TK6 | UNIT2 SDS2 LISS POISON INJECT. TK1<br>UNIT2 SDS2 LISS POISON INJECT. TK2<br>UNIT2 SDS2 LISS POISON INJECT. TK3<br>UNIT2 SDS2 LISS POISON INJECT. TK4<br>UNIT2 SDS2 LISS POISON INJECT. TK5<br>UNIT2 SDS2 LISS POISON INJECT. TK6 | A, X | Reactivity Control |

Table 4. General Safety Function Classifications

| **Catawba** | **Diablo Canyon** | **Surry (shutdown only)** |
|---|---|---|
| Reactivity Control | Sub Criticality | Reactivity Control |
| Containment Isolation | Core Cooling | Core Cooling |
| Containment Pressure | Heat Sink | Inventory Control |
| Cooling Water | RCS Integrity | Containment Status |
| ECCS Systems | Vital Power Sources | |
| AC Power Availablility | Component Cooling | |
| DC Power Availability | | |
| RCP Seals | | |
| Secondary Heat Removal | | |

Table 5. Safety Functions for PHWR

| Safety Function | Systems |
|---|---|
| 1. Reactivity Control | Shutdown System No. 1<br>Shutdown System No. 2<br>Moderator System<br>Moderator Cover Gas System<br>End Shield Cooling System |
| 2. Core Cooling | Emergency Core Cooling System<br>Shutdown Cooling System |
| 3. Primary Heat Transport System Pressure and Inventory Control | Heat Transport System<br>PORVs<br>Pressurizer System |
| 4. Secondary Heat Removal | Main Feedwater System<br>Auxiliary Feedwater System<br>Main Steam System |
| 5. AC Power | Standby Diesel Generator System<br>Standby Diesel Generator Fueling System<br>Off-site Power |
| 6. DC Power | DC battery System |
| 7. Cooling Water and Other Vital Support System | Service Water System<br>Instrument Air System<br>HVAC<br>Purification System<br>Condensate System<br>Dual Control Computer |
| 8. Containment Integrity and Cooling | Containment System<br>Dousing System<br>Local Air Cooler System |