CONF-9210071--27

BNL-NUREG-47971

"Level 1 Probabilistic Risk Assessment of Low Power and Shutdown Operations at a PWR: Phase II Results"

T-L. Chu, G. Bozoki, P. Kohut, Z. Musicki, S.M. Wong, B. Holmes[1]
J. Yang, C-J. Hsu, D.J. Diamond, N. Siu,[2] R-F. Su***
Brookhaven National Laboratory
Upton, New York

D. Bley, J. Lin
Pickard, Lowe and Garrick, Inc.

ABSTRACT

As a result of the Chernobyl accident and other precursor events (e.g., Diablo Canyon), the U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) initiated an extensive project during 1989 to carefully examine the potential risks during Low Power and Shutdown (LP&S) operations. Shortly after the program began, an event occurred at the Vogtle plant during shutdown, which further intensified the effort of the LP&S program. In the LP&S program, one pressurized water reactor (PWR), Surry, and one Boiling Water reactor (BWR), Grand Gulf, were selected, mainly because they were previously analyzed in the NUREG-1150 Study. The Level-1 Program is being performed in two phases. Phase 1 was dedicated to performing a coarse screening level-1 analysis including internal fire and flood. A draft report was completed was completed in November, 1991. In the phase 2 study, mid-loop operations at the Surry plant was analyzed in detail. The objective of this paper is to present the approach of the phase 2 study and the preliminary results and insights.

I. BACKGROUND

This paper presents the results of a level one probabilistic risk assessment (PRA)[1] of the Surry Nuclear Power Plant for accidents during low power and shutdown conditions. The work was performed by Brookhaven National Laboratory (BNL) for the Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES). This program was initiated in support of the NRC staff's follow-up actions to the March 20, 1990 Vogtle incident. In order to meet the RES commitment to the Office of Nuclear Reactor Regulation (NRR), a phased approach was used in the program. In phase 1, a coarse screening analysis,[2] which included internal fire and flood, was completed in November, 1991. This screening analysis produced a preliminary level one PRA for accidents during low power and shutdown. It also provided insights on potential accident scenarios and potential vulnerable configurations during low power and shutdown conditions. Mid-loop operation was found to be a potentially vulnerable plant condition. Phase 2 of the study was guided by the phase 1 results, and therefore it focused on a detailed analysis of mid-loop operation. This paper documents the preliminary results and findings of the phase 2 internal event analysis. The work on internal fire, internal flood, and seismic analysis is on-going, and will be reported at a later date.

---

[1] AEA Technology

[2] M.I.T., currently at Idaho National Engineering Laboratory

"Level 1 Probabilistic Risk Assessment of Low Power and Shutdown Operations at a PWR: Phase II Results"

T-L. Chu, G. Bozoki, P. Kohut, Z. Musicki, S.M. Wong, B. Holmes[1]
J. Yang, C-J. Hsu, D.J. Diamond, N. Siu,[2] R-F. Su***
Brookhaven National Laboratory
Upton, New York

D. Bley, J. Lin
Pickard, Lowe and Garrick, Inc.

ABSTRACT

As a result of the Chernobyl accident and other precursor events (e.g., Diablo Canyon), the U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) initiated an extensive project during 1989 to carefully examine the potential risks during Low Power and Shutdown (LP&S) operations. Shortly after the program began, an event occurred at the Vogtle plant during shutdown, which further intensified the effort of the LP&S program. In the LP&S program, one pressurized water reactor (PWR), Surry, and one Boiling Water reactor (BWR), Grand Gulf, were selected, mainly because they were previously analyzed in the NUREG-1150 Study. The Level-1 Program is being performed in two phases. Phase 1 was dedicated to performing a coarse screening level-1 analysis including internal fire and flood. A draft report was completed was completed in November, 1991. In the phase 2 study, mid-loop operations at the Surry plant was analyzed in detail. The objective of this paper is to present the approach of the phase 2 study and the preliminary results and insights.

I. BACKGROUND

This paper presents the results of a level one probabilistic risk assessment (PRA)[1] of the Surry Nuclear Power Plant for accidents during low power and shutdown conditions. The work was performed by Brookhaven National Laboratory (BNL) for the Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES). This program was initiated in support of the NRC staff's follow-up actions to the March 20, 1990 Vogtle incident. In order to meet the RES commitment to the Office of Nuclear Reactor Regulation (NRR), a phased approach was used in the program. In phase 1, a coarse screening analysis,[2] which included internal fire and flood, was completed in November, 1991. This screening analysis produced a preliminary level one PRA for accidents during low power and shutdown. It also provided insights on potential accident scenarios and potential vulnerable configurations during low power and shutdown conditions. Mid-loop operation was found to be a potentially vulnerable plant condition. Phase 2 of the study was guided by the phase 1 results, and therefore it focused on a detailed analysis of mid-loop operation. This paper documents the preliminary results and findings of the phase 2 internal event analysis. The work on internal fire, internal flood, and seismic analysis is on-going, and will be reported at a later date.

---

[1] AEA Technology

[2] M.I.T., currently at Idaho National Engineering Laboratory

Surry Unit 1 was chosen for this study in part because the Surry plant was previously analyzed in the Reactor Safety Study and NUREG-1150[3] and in part because Virginia Power offered their cooperation. The core damage frequency (or risk) during low power and shutdown calculated as part of this study will be compared with the core damage frequency calculated in NUREG-1150 for accidents during full power. The Surry Plant contains two Pressurized Water Reactors (PWRs) each rated at 788 megawatts (electrical) capacity and it is located near Surry in Virginia. Grand Gulf, a boiling water reactor, was selected as the plant to be analyzed in a parallel study[4,5] which is being performed by Sandia National Laboratories (SNL).

II. OBJECTIVES

The objectives of phase 2 of this program are:

1) Estimate the frequencies of severe accidents that might be initiated during mid-loop operation,

2) Compare the estimated core damage frequencies, important accident sequences, and other qualitative and quantitative results of this study with those of accidents initiated during full power operation (as assessed in NUREG-1150), and

3) Demonstrate methodologies for accident sequence analysis for plants in modes of operation other than full power.

III. APPROACH

Due to the changing plant configuration during low power and shutdown operation, it was necessary to define different outage types and different plant operational states (POSs) within each outage type. The approach used in performing the PRA for a POS in an outage type is similar to that used in the NUREG-1150 study. It includes the typical tasks such as identification of initiating events, development of fault trees and event trees, and quantification. Within each POS, the plant configuration continues to change with time, and the decay heat continues to decrease. Therefore, appropriate characterization of these changing conditions was necessary. Due to lack of existing detailed analysis of the plant response to different accident scenarios, it was found necessary to perform supporting thermal hydraulic analysis in order to successfully model the various accident scenarios. The following is a summary of the approach used in the key tasks of this study.

A. Outage Types and Plant Operational States

Outages were grouped into four different types: refueling, drained maintenance, non-drained maintenance with use of the residual heat removal(RHR) system, and non-drained maintenance without the use of the RHR system. Due to the continuously changing plant configuration in any outage, plant operational states (POSs) were defined and characterized within each outage type. For example, in a refueling outage up to 15 POSs were used. They represent the evolution of the plant throughout a refueling from low power back to low power. An extensive effort was made to collect Surry-specific data needed to characterize each POS. This included review of operating and abnormal procedures

for shutdown operations, review of shift supervisor's log books, review of monthly operating reports, and performing supporting thermal hydraulic calculations.

Three mid-loop POSs, in which the reactor coolant system (RCS) level is lowered to the mid-plane of the hot leg, were selected for detailed analysis. Two of them occur in a refueling outage, POSs R6 and R10, and one in a drained maintenance outage, POS D6. They are characterized by different decay heat levels, and different plant configurations such as the number of RCS loops that are isolated, and whether or not the RCS has a large vent. R6 represents a mid-loop operation that takes place early in a refueling outage. This mid-loop operation allows fast draining of the RCS loops to permit eddy current testing of the steam generator tubes. R10 takes place after refueling operation is completed to allow additional maintenance of equipment in the RCS loops. D6 represents mid-loop operation in which maintenance activities require the plant to go to mid-loop, and is characterized by the highest decay heat level among the three mid-loop POSs.

During the latest Surry Unit 1 refueling outage that started on February 28, 1992, the utility changed previous outage practice and avoided going to mid-loop operation. It is our understanding that the utility staff intend to continue this new practice. However, mid-loop operation can not be totally avoided in the future. With NRC concurrence, BNL developed the PRA model based on outages that included mid-loop operation prior to the February 1992 refueling.

B. Initiating Event Analysis

The approached used to identify initiating events, was to review existing studies, search licensee event reports (LERs), review published NRC documents, and review current Surry operating procedures. This approach should ensure that any incident that has occurred or any scenario that has been studied will be identified. However, a systematic approach, such as a failure mode and effect analysis (FMEA) or a hazard and operability study (HAZOP), was not employed to provide further assurance that all possible initiating events in all possible operating states have been identified.

C. Event Tree Analysis

In phase 1 of this study, accident scenarios were developed for all Low Power and Shutdown POSs. For those POSs that are similar to power operations, e,g, low power operations, the relevant NUREG-1150 event trees were reviewed and modified (if necessary) to reflect the current plant design and operation. For other POSs, event trees were developed in group discussions, involving typically four or more BNL staff members with expertise in PWR operations, PRA, human reliability analysis (HRA) and thermal hydraulics. Communications with staff at Virginia Power were established to clarify questions on the plant design and operations.

In phase 2, the event trees developed for the mid-loop POSs were reviewed and modified to incorporate additional information obtained in the system analysis and to reflect the current understanding of the expected operator responses to the accidents. A two-day meeting with Virginia Power operations personnel was held to discuss the potential accident scenarios, and the expected plant and operator responses.

D. System Analysis

The fault tree models developed as part of NUREG-1150 study were reviewed and modified, when necessary, to develop fault tree models for the plant at shutdown as well as during low power operation. Typically, two fault trees were developed for each system. One tree is applicable to power operations, and the other is applicable to shutdown conditions. The system configuration during shutdown was identified by reviewing the operating procedures used during shutdown, shift supervisor's log books, and the system training manual. Typically, the following changes were made to develop the fault trees applicable to shutdown conditions.

1) The position of valves during shutdown may be different from that during power operation. Therefore, the applicable failure modes of the valves are different from those of power operations.

2) Human error events associated with backup of automatic actuated systems or components which failed were modified to manual actuation with no automatic backup.

3) Maintenance unavailabilities relevant to the specific POS were estimated. For mid-loop POSs, the reduced inventory check list was used to determine whether or not the maintenance events are permitted. Those maintenance events prohibited by the check list, e. g. diesel generator maintenance, were not used in the quantification.

4) System success criteria were changed if necessary.

E. Supporting Thermal Hydraulic Analysis

The main purpose of the thermal hydraulic analysis was to support the event tree development and accident sequence quantification. In the phase one study, assumptions were made based on simple "back of the envelop" type calculations. It was found that more detailed calculations were needed to confirm the simple calculations, and support the assumptions made.

In the phase 2 study, a more detailed calculation was done to determine the timing of a feed and bleed operation while initially at mid-loop. The calculation also provided information on the amount of refueling water storage tank (RWST) water needed to sustain the feed and bleed operation, as well as the timing of core uncovery for different initial conditions.

The MELCOR code was also used to assess whether or not gravity feed from the refueling water storage tank (RWST) could be used to provide long term cooling (i.e. 24 hours, decay heat removal). It was found that gravity feed is sufficient only when the decay heat is relatively low, it can provide a few hours for restoring other means of decay heat removal when the decay heat is high.

In the case of reflux cooling, the results of the Idaho National Engineering Laboratory (INEL) study,[6] Westinghouse study,[7] and Virginia Power analysis[8] were reviewed and used to determine the success criteria.

F. Quantification

The initiating event frequencies were estimated using the Bayesian approach. The basic event data were based on the NUREG-1150 data base for Surry.[9] The quantification of fault trees and event trees was performed using point estimates only. No attempt was made to propagate uncertainty at this stage of the project. The IRRAS computer code,[10] Version 4.0, was used in the fault tree and event tree quantification.

G. Human Reliability Analysis

Two types of human error events were identified and modeled in this study, pre-accident errors and post-accident errors. For pre-accident errors, those identified in the NUREG/CR-4550 study for Surry[9] were adopted. Additional pre-accident errors were identified in the system analysis task and were added to the system fault trees.

The approach to evaluating dynamic human actions and recovery actions that follow an initiator is to first qualitatively define the event scenario, required action, important factors affecting operator performance, and the consequences of the action not being successful.

The qualitative evaluation of the actions and the important parameters that affect operator performance were used to derive the human error probabilities (HEPs) using an adaptation of the success likelihood index methodology. This methodology is based on the assumption that the likelihood of operator error in a particular situation depends on the combined effects of a small set of performance-shaping factors (PSFs) that influence the operator's ability to accomplish the action.

To quantify the HEPs, the PSFs were rated against a weight that relates the relative influence of each PSF on the likelihood of the success of the action and a score that relates whether the PSF helps or hinders the operator to perform the actions. With the rating for PSF, the numerical model was calibrated using well-defined actions obtained from analysis for other PRAs. The calibration procedure ensures that the error probabilities are realistic and consistent with available data, observed human behavior, and the results from comparable expert evaluations of similar activities.

H. Data Base Analysis

An extensive effort was made to collect data for use in characterizing the plant during shutdown and for quantification of the plant model.

1) A data base of initiating events was compiled and used in the initiating event analysis.

2) A review of the shift supervisor's log books, outage schedules, minimum equipment list, and monthly operating report was performed to identify the data needed to estimate the frequency of shutdown, duration of plant operational states, and maintenance unavailabilities.

3) Shift supervisor's log books were reviewed to determine the time period that the plant is in different configurations. For example, the reactor coolant loops were found to be isolated for a long period of time in a refueling.

IV. RESULTS AND INSIGHTS

This study found that the predicted core damage frequency during mid-loop operation is comparable to that of power operation. Due to the preliminary nature of the results, it was decided that no quantitative result will be presented. Operator failure to mitigate the accidents was found to be the most dominant contributor to the calculated core damage frequency. POS 6 of a drained maintenance outage (D6) is the most dominant POS. The characteristics of this POS are high decay heat level and a relatively short time available for operator action. In contrast, POS 10 of a refueling outage has a very low decay heat, and its core damage frequency is approximately 2 orders of magnitude lower.

The following were insights derived from in this study:

Operator Response: The dominant cause of core damage was found to be operator failure to mitigate the accidents. However, it should be mentioned that there is very large uncertainty in the human error probabilities currently used in this study. In general, it would be beneficial to have good training, procedures, and instrumentation to ensure that the utility staff are able to respond to accidents during shutdown.

Procedures for Shutdown Accidents: Very few procedures are currently available for accidents during shutdown. In most cases, the information in the procedures for power operation is helpful, if used for shutdown accidents. For example, the procedure for station blackout, ECA-0.0, provides instructions for dumping steam to the condenser. This procedure was taken credit for in this study. However, some procedures written with power operation in mind, can potentially mis-guide the operator if followed during shutdown. For example, the procedure for loss of offsite power, AP 10.00, states that "When the EDG is the only source of power to an emergency bus, the Component Cooling Pump should NOT be in service". During shutdown, CCW flow to the RHR heat exchanger is necessary for decay heat removal. Strictly following this procedure can have an adverse effect on the operator response.

Instrumentation: The level used during mid-loop operation, i.e., standpipe level instrumentation and ultra-sonic level instrumentation, have limited applicability during a shutdown accident. The standpipe system provides correct level indication only when there is no pressure build-up in the system. The ultra-sonic level instrumentation only provides level indication when the level is within the reactor coolant loops. This level instrumentation may not therefore be useful during a feed and bleed operation.

Supporting Thermal Hydraulic Analysis: The thermal hydraulic behavior of the reactor coolant system is rather complex. This is mainly due to the fact that the pressurizer is usually the relief path for coolant or steam, and the vessel head does not have a large vent. When performing thermal hydraulic analysis in support of the PRA effort, consideration has to be given to longer term system behavior, at least 24 hours into the accident. In this study, such calculations were done for feed-and-bleed operation using a charging pump, and with gravity feed from the RWST. It is believed that additional supporting calculations would be helpful for a better understanding of the effectiveness of reflux cooling, and feed and bleed using a low pressure injection pump. In this study, the results of the Virginia Power Technical Report # 865 were used to determine the number of steam generators needed as a function of time after shutdown. A conservative

assumption was made regarding the time when the initiating event occurs in each mid-loop POS, which determines the number of steam generators needed. It was conservatively assumed that if the number of steam generators was not enough, then no credit was given to reflux cooling. In this case, reflux cooling still would help. However, its benefit can not be determined without detailed analysis. In this study, it was assumed that hot leg injection using a low head injection pump is an adequate way of preventing core damage. Due to the low shut-off head of the pumps, approximately 150 psig, the concern is that if boiling takes place in the system the low head pump may not be able to inject.

Maintenance Unavailability: Based on a review of shift supervisor's log books and minimum equipment lists for 3 refueling outages, the maintenance unavailabilities of equipment that can be used to mitigate an accident were found to be very high. For example, 2 out of 3 charging pumps were found to be tagged out practically throughout the whole mid-loop period. The two low head injection pumps were also unavailable a large fraction of the time. As a result of the requirement of generic letter 88-17, the plant is required to have one high head pump and one low head pump available. In the quantification of this study, it was assumed that charging pump A, charging pump cooling water pump A, and low head injection pump A are available. Based on the check list used for reduced inventory conditions, it was also assumed that maintenance of diesel generators, 4 kv emergency buses, and stub buses is not allowed.

It was found in this study that maintenance unavailability is the dominant cause of equipment unavailability. In combination with human errors, maintenance of the charging pump cooling water pump, the charging pump, and the low head injection pump appear in the dominant cutsets for some of the core damage sequences.

Isolation of Reactor Coolant Loops: Review of the plant shutdown experience indicated that the reactor coolant loops are isolated for extended periods of time in a refueling outage. This practice makes the steam generators unavailable for decay heat removal upon loss of RHR. In a cold shutdown condition, the steam generators are usually maintained in the wet lay-up condition with the secondary side filled with water. During mid-loop operation, the availability of the SGs makes reflux cooling a possible method of mitigating a loss of RHR. This might be the only mitigation function available in a station blackout.

In this study, it was found that isolation of the RCS loops is an important contributor to core damage frequency.

Single Failures of the RHR System: The RHR system at Surry is not a safety related system (i.e., it does not perform safety injection function). As a result, many single component failures can cause loss of RHR. In the RHR system, a single suction line from the loop A hot leg and a single flow control valve HCV-1758 are used. During RHR operation, a single CCW header is used to provide cooling to both RHR pump seal coolers and the operating RHR heat exchanger, and a single CCW return line from the RHR system is used. As a result, a failure of the trip valve 109A or B in the CCW return line can cause loss of the system. These trip valves also fail closed on loss of instrument air, or vital bus. It was found in this study that closure of the TV-109 valves is a significant contributor to loss of RHR. It was assumed that the opening of the RHR flow control valve HCV-1758 as a result of loss of vital bus III will cause RHR pump run out. This was also found to be a significant contributor to loss of RHR.

Valve Arrangement of Low Pressure Injection System and Auxiliary Feedwater System During Shutdown: The low pressure injection system has a motor operated valve 1890C in the flow path to the cold legs which is normally closed during shutdown. Failure of this valve to open or loss of power to the valve motor is a single failure that can cause failure of low head injection to the cold legs and loss of the flow path for gravity feed from the RWST. This failure was found to be an important contributor to the unavailability of the system. Hot leg injection, an alternative to cold leg injection, was taken credit for in this study. It is understood that cold leg injection is more preferable, because it ensures that the injected flow would go through the core.

The auxiliary feedwater system has six MOVs (151A,B, C, D, E, and F) in the flow path to the steam generators, that are normally closed during shutdown. They would become difficult to locate during a station blackout.

IV. CONCLUSION

The results of this study show that the core damage frequency during mid-loop operation is comparable to that of power operation. The dominant contributor to the core damage frequency is operator failure to mitigate the accidents. It is recognized that very large uncertainty exists in the human error probabilities currently used in this study.

A comparison of the results for the three mid-loop POSs shows that it is preferable to enter mid-loop when the decay heat is relatively low. Entering mid-loop as early as one day after shutdown should probably be avoided if possible.

This study identified that only a few procedures are available for mitigating accidents that may occur during shutdown. Additional procedures written specifically to address potential accidents during shutdown would be useful.

This study assumed that the reduced inventory check list was followed, and found that the maintenance unavailability of equipment not on the list were dominant contributors to system unavailability. However, it is believed that the check list is sufficient for ensuring the availability of essential equipment.

REFERENCES:

1. Chu, T-L, et al., "PWR Low Power and Shutdown Accident Frequencies Program, Phase 2- Internal Events," Rough Draft Letter Report, August 31, 1992.

2. Chu, T-L., et al., "PWR Low Power and Shutdown Accident Frequencies Program, Phase 1A - Coarse Screening Analysis," Draft Letter Report, November 13, 1991.

3. NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants." Final Summary Report, December 1990.

4. Whitehead, D.W., et al., "BWR Low Power and Shutdown Accident Sequence Frequencies Project," Phase 1 - Coarse Screening Analysis, Vol. 1-3, Draft Letter Report, Sandia National Laboratories, September 21, 1991.

5. Whitehead, D.W., et al., "BWR Low Power and Shutdown Accident Sequence Frequencies Project, Phase 2- Detailed Analysis of POS 5," Volume 1: Part 1 -Internal Events Excluding Fire and Flood, August 31, 1992.

6. Naff, S., et al., "Thermal-Hydraulic Processes During Reduced Inventory Operations with Loss of Residual Heat Removal," Idaho National Engineering Laboratory.

7. Audreycheck, T.S., et al., "Loss of RHR Cooling While the RCS is partially Filled," WCAP-11916, Westinghouse Electric Corporation, July, 1988.

8. "Background and Guidance from Ensuing Adequate Decay Heat Removal when RCS Loop Stop Valves are Closed. Surry and North Anna Power Statioms," NE Technical Report No.865, Virginia Power, December 1991.

9. Fowler, R.D., "Surry Unit 1 Probabilistic Risk Assessment (PRA) Related Data Base," Letter Report, Revision 1, Idaho National Engineering Laboratory, April 11, 1991.

10. Russell, K.D., et al., "Integrated Reliability and Risk Analysis System (IRRAS), Version 4, Reference Manual" NUREG/CR-5813, EGG-2664, VOL. 1, January 1992.

DISCLAIMER

END

DATE
FILMED
6/30/93