Proceedings
of the
International Topical Meeting
on
Advanced Reactors Safety

Volume II

Orlando, Florida
June 1-5, 1997

Sponsored by the American Nuclear Society's
Nuclear Installations Safety Division

Cosponsored by the

Atomic Energy Society of Japan
Canadian Nuclear Society
Korea Nuclear Society
European Nuclear Society
U.S. Department of Energy
Organization for Economic Cooperation and Development
International Atomic Energy Agency

Published by the
American Nuclear Society, Inc.
La Grange Park, Illinois 60526 USA

THE IMPORTANCE OF PROPERLY TREATING HUMAN PERFORMANCE IN PROBABILISTIC RISK ASSESSMENTS

C. A. Kukielka
Pennsylvania Power & Light Co.
Two North Ninth Street
Allentown, PA 18101
(610) 774-7526

F. G. Butler
Pennsylvania Power & Light Co.
Two North Ninth Street
Allentown, PA 18101
(610) 774-7712

M. A. Chaiko,
Pennsylvania Power & Light Co.
Two North Ninth Street
Allentown, PA 18101
(610) 774-7755

A. S. Fitch
Pennsylvania Power & Light Co.
P.O. Box 467
Berwick, PA 18603
(717) 542-3510

E. R. Jebsen
Pennsylvania Power & Light Co.
Two North Ninth Street
Allentown, PA 18101
(610) 774-7729

R. M. Peal
Pennsylvania Power & Light Co.
P.O. Box 467
Berwick, PA 18603
(717) 542-3889

INTRODUCTION

A critical issue to consider when developing Advanced Reactor Systems (ARS) is the operators' ability to reliably execute Emergency Operating Procedures (EOPs) during accidents. This issue is generally investigated using Probabilistic Risk Assessment (PRA) and the associated Human Reliability Analysis (HRA). Reviewing the results of a number of PRA studies on existing plants shows that the core melt and containment failure frequency are typically dominated by operator error. This implies that the installed equipment is far more reliable than the operator using it. The proper response to this result, presuming it is a proper reflection of actual plant risk, is to modify the plant, improve the operator training program, and upgrade procedures to the point where the operator is at least as reliable as the equipment being operated.

Current HRA methods, however, tend to generate high probabilities of operator error relative to the equipment failure probabilities. While it is true that assuming large operator error rates is conservative when attempting to establish the core damage frequency, it is also true that it is non-conservative when trying to identify severe accident vulnerabilities associated with plant design and operation. Assuming large operator error rates, relative to other failure modes, predetermines that operator error will dominate the PRA insights and may, therefore, mask true severe accident vulnerabilities, which, due to the high assumed operator error rates, have less significant contribution to the core damage frequency. The ramifications of this approach are particularly troublesome in that while responding to an actual plant event, a highly proficient operator may be hindered by mis-guided plant design features, installed because of assumed high error rates. In fact, many of the design changes necessary to satisfy Defense in Depth at Susquehanna have been made to allow the operator to reliably implement EOPs. Therefore, assuming inappropriately high error operator rates when developing advanced reactor designs may result in improper design assumptions and contribute to a less safe plant.

PP&L recognized this trap and has developed a method for evaluating operator performance which is consistent with the goal of identifying important operator actions without compromising the ability of the PRA model to identify significant severe accident design vulnerabilities. This method, which has evolved over the last 14 years of risk analysis, melds the strengths of both probabilistic and deterministic analyses to addresses the central questions associated with operator reliability:

1. Does the operator understand the status of the plant?

2. Given that the plant status is understood, does he know what to do?

3. Given 1 & 2, what are the odds of successful EOP execution?

Questions 1&2 concern the non-algorithmic mental process of understanding. HRA methods, which presume an algorithm, should not be used to address these questions. Therefore, PP&L relies on deterministic methods to evaluate them. Question 3

is amenable to statistical analysis. Therefore, simulator exercises are used to develop probability of response as a function of time curves for time limited operator actions. This method has been used to identify and resolve deficiencies in the plant operating procedures and the operator interface. A description of this method is provided along with an application to Anticipated Transient without Scram (ATWS) sequences. Additionally, the results PP&L's HRA analysis are compared with the result of similar BWR analyses.

PP&L'S HUMAN RELIABILITY EVALUATION PROCEDURE

Over the past 14 years PP&L has been applying PRA methods to investigate severe accident issues and, when necessary, finding cost effective ways of reducing risk associated with these issues. Therefore, the PRA methods, including HRA, used by PP&L are targeted at identifying and resolving design and operator performance vulnerabilities, not at bounding the probability of failure. This target is fully consistent with the NRC goal for human reliability analysis as stated in NUREG-1335, *"The object of doing the analysis is not to establish the process of doing human reliability analysis, but to make the plant safer through the human reliability analysis and subsequent accident management program."* PP&L endorses this objective and has interwoven this objective in its HRA method.

This method consists of the following steps:

1. Incorporate proceduralized operator actions into event tree/fault tree models.

2. Determine the Risk Achievement Worth (RAW) and Risk Reduction Worth (RRW) of the operator actions credited in step 1.

3. For those procedural steps having a significant RAW or RRW, determine if the Severe Accident Defense in Depth (D in D) criteria are satisfied. These criteria are listed in Table 1.

4. If Defense in Depth is not satisfied, modify equipment, procedures, or training to establish Defense in Depth and incorporate changes into the plant model. Repeat steps 2 through 4 until Defense in Depth is established.

The goal of this evaluation is to ensure that the operator is at least as reliable as the equipment being operated. Achieving this goal represents the optimal level of plant safety because the operator is capable of fully utilizing the equipment installed in the plant.

The first step in this method involves incorporating the proceduralized operator actions into the event tree/fault tree models. No credit is taken for operator actions not specified in the EOPs or the procedures referenced from the EOPs.

The RAW and the RRW of each EOP step are computed next. The RAW is used to identify operator actions significant to maintaining the present level of risk, while the RRW is used to identify which operator actions, if improved, will result in a significant risk reduction. RAW is defined to be the increase in risk if the Operator Error Probability (OEP) is set equal to one for the step of interest, while RRW is defined to be the reduction in risk if the OEP is set equal to zero. Mathematically these are defined to be:

$$RAW_i = \{R_i(1)-R_o\}/R_o \qquad (1)$$

$$RRWi = \{R_o-R_i(0)\}/R_o \qquad (2)$$

Here,

RAW_i = the RAW for step I,
RRWi = the RRW for step I,
$R_i(1)$ = the risk with the OEP for step i =1,
$R_i(0)$ = the risk with the OEP for step I=0,
R_o = the baseline risk computed using Susquehanna method.

Based upon equations 1 & 2, large values of RAW and values of RRW approaching 1 are important operator actions.

EOP steps with significant RAW or RRW are subjected to a Defense in Depth evaluation. This evaluation is a critical step when evaluating operator performance. It ensures:

1. that the EOPs represent a set of instructions that can be reliably executed;

2. that the information necessary to implement the procedures is available to the operator in a timely and unambiguous manner;

3. that the EOPs are written in a clear and unambiguous manner;

4. that sufficient time exists for the operator to observe plant symptoms, read the procedure step and reliably execute the required action; and

5. that the facility necessary to reliably implement the EOPs is available to the operator.

Given that the above conditions are satisfied, it is reasonable to expect that a well trained operator will reliably execute the EOPs with a failure rate that is small relative to the failure rate of the equipment operated. Establishing Defense in Depth is the objective of the PP&L HRA method. The outcome of this method is a set of operating procedures that can be executed reliably by the operator. Therefore, establishing Defense in Depth assures reliable operator performance.

Establishing Defense in Depth is a multi-discipline activity, which involves representatives from Operations, Training, and Risk Analysis. The risk analysis engineer first determines if the procedures satisfy the Procedural Defense in Depth criteria identified in Table 1. The procedures are evaluated against these criteria using the plant logic model and plant transient analysis. These criteria are designed to maximize the chance of operator success by: avoiding procedures that, given an additional equipment failure, will have an adverse impact on the plant; taking action to protect equipment being used to mitigate the accident; and performing actions to allow for success should subsequent equipment failure occur. With the procedural criteria satisfied, the procedures are next evaluated against the Interface Criterion.

This evaluation is performed by all three disciplines and consists of several activities. Reactor transient calculations and simulator exercises are used: to establish the time available to execute the procedures; to determine if the information required to implement the procedures is available to the operator in a clear and unambiguous manner; and, in part, to determine if the facility exists to reliably implement the procedures in a timely manner.

Operator interviews are carried out immediately after the simulator scenario. During the interview the recorded scenario is played to aid the operator in remembering the actions taken. These interviews are used to establish that the procedures are well written, convey the intended action, and are unambiguous with respect to the desired action and expected outcome. Additionally, the operators are questioned about their ability to implement the procedures given the available instrumentation and controls.

Statistical analysis is performed on time limited operator actions to ensure that sufficient time exists to reliably execute each step. Response time data is collected during simulator exercises and fit to a distribution function. This function is then used to compute the probability of not executing the procedure within the available time. The goal of this analysis is to determine if it is reasonable to expect the non-response probability to be on the order of, or less than, the equipment failure probability.

Modifications to equipment, procedures, or training occur, as needed, to establish Defense in Depth. The process is repeated until Defense in Depth is established. Procedures, equipment, and training have all been modified at Susquehanna to establish Defense in Depth.

ATWS EXAMPLE

This HRA method was used when developing the EOPs for Susquehanna. The Susquehanna ATWS EOPs are somewhat unique and have been endorsed by the ACRS and USNRC[a]. These ATWS procedures are used to illustrate the PP&L HRA method.

The operator actions included in the plant ATWS logic model are identified in Table 2. These steps appear on the ATWS EOP flow chart in three parallel paths: one for reactor power control, one for reactor water level control, and one for reactor pressure control. These paths are implemented in parallel, by the operating crew with the Unit Supervisor directing the crew response. Each step number is proceeded by a letter denoting the path: Q for reactor power control, L for reactor level control, and P for reactor pressure control. Prior to executing these steps, the operator must first enter and follow the EOPs. Therefore, entering and following procedures appears first in the Table. Finally, the operator must initiate heat removal from the containment by Suppression Pool Cooling (SPC). This step appears on the primary containment control procedure. Approximately 20 hours are available to perform this action if Standby Liquid Control (SLC) has been successful. Therefore, this step appears last in the Table.

[a] Letter from D. E. Matthews USNRC to K. P. Donovan, BWROG, Acceptance of Proposed Modifications to the BWR Emergency Procedures Guidelines (TAC Nos. M89489 & M89629), 6/6/96.

Based upon the value of RAW, following written procedures is the operator's single most important responsibility. This fact should be understood independent of the value of RAW. It is a standard PP&L assumption that the operator follows the procedures without error. While some may view this assumption as unrealistic and non-conservative, it is entirely reasonable and necessary to bound the analysis. Arbitrarily assigning a "reasonable OEP" to procedural error is, in fact, non-conservative, if the goal is "*to make the plant safer through human reliability analysis,*" since it will tend to dominate the risk profile and mask opportunities for safety improvement. The PP&L assumption is not arbitrary but is based upon thorough evaluations of the EOP steps required, the time required to perform them, and the equipment relied upon. The PP&L Defense in Depth process provides the data and the confidence necessary to allow this assumption to be valid for PRA analysis. PP&L fully expects this assumption to be factual in any real plant event requiring entry to the EOPs. Additionally, if the operator fails to follow procedures, then the analysis becomes unbounded and cannot be modeled as part of the Individual Plant Examination (IPE). If the operator fails to follow procedures, then the reason for this failure must be developed as part of an accident sequence. There are a multitude of reasons , perhaps an infinite number, why the operator would fail to follow procedures. However unlikely, each of these sequences must be developed resulting in an overwhelming task. Therefore, assuming the operator follows procedures is not only an appropriate assumption, but necessary to bound the analysis.

Entering and following procedures applies, generally, to all the procedures in the EOPs. Therefore, Defense in Depth is established for this action by demonstrating that Defense in Depth exists for each steps.

EOP Step 2, Initiate SPC, Step Q1, Initiate SLCS, and Step L5, Initiate ADS if RPV water Level cannot be maintained above TAF all have RAW values greater than 100. Step Q1, additionally, has a very high value of RRW. Therefore, each of these steps is evaluated for Defense in Depth.

The operator is instructed to initiate SPC whenever the suppression pool temperature exceeds 90°F. The suppression pool temperature is clearly displayed in the control room. About 20 hours are available to complete the action, if SLCS has been successful. Initiating SPC is a routine action, having been performed well over 1000 times at Susquehanna. Initiating SPC will not result in an adverse consequence should additional failures occur. Actions have been incorporated into the Residual Heat Removal (RHR) system operating procedures to protect the RHR equipment. These actions include instructions on how to initiate RHR without water hammer in the absence of fill and vent capability. Should the RHR system fail, actions are specified to re-establish the main condenser as the heat sink or to prepare the reactor building for containment venting or failure. These preparations include aligning equipment and the necessary support equipment to support vessel injection, even if the equipment in the reactor building were destroyed. Therefore, Defense in Depth is established for initiation of SPC.

The SLCS is a diverse method of shutting down the reactor. Therefore, its importance is obvious during ATWS events. Since SLCS is diverse to the Reactor Protection System (RPS), its importance is stressed during operator training, with special emphasis directed at eliminating any reluctance to its initiation. Initiating SLCS has no adverse impact, should additional failure occur. No actions are required to protect SLCS, since the ATWS event does not impact it. Should the SLCS system fail, Manual Rod Insertion (MRI) is capable of shutting down the reactor without challenging the primary containment integrity. The MRI step directly follows SLCS initiation. SLCS is initiated early, as a diverse means of suppressing reactivity excursions, should the reactor operate in regimes of high subcooling or low reactor pressure. Therefore, initiation of SLCS satisfies Procedural Defense in Depth.

The current SLCS initiation step is the result of a number of revisions motivated by the above Defense in Depth criteria. Initial placement of the SLCS initiation step was consistent with the generic procedural guidance, which allows initiation any time before the suppression pool temperature reaches 110°F with the reactor power greater than 5%. However, during simulator exercise, two distinct SLCS initiation strategies emerged, each with a distinct probability of response as a function of time curve. Both strategies were allowed by procedures. In one strategy the operators initiated SLCS immediately any time an ATWS occurred and the reactor power was greater than 5%. In the second strategy, the operators waited until the suppression pool approached 110°F, before starting SLCS.

After reviewing this situation, it was decided that this instruction was ambiguous. Additionally, since delayed SLCS initiation could impact the success of ATWS sequences with HPCI failure. This step was changed to require SLCS initiation any time a valid scram signal is present and the reactor power exceeds 5% or cannot be determined. This change eliminated ambiguity in the EOP step and provides guidance when reactor power cannot be determined. This change resulted in consistent initiation of SLCS.

During procedure validation, however, it was observed that SLCS initiation was delayed as the operators worked through the EOP flow charts. While response time was more than adequate to protect the reactor and containment with High Pressure Coolant Injection (HPCI) successful, it was too close to the time to reach the 110°F initiation set point. Additionally, early boron is preferable when considering ATWS stability issues. Therefore, the SLCS initiation step was moved so that it occurs immediately after determining that the power is greater than 5% and that Alternate Rod Insertion (ARI) initiation has been ineffectual.

The impact of this change on the response curves is presented in Figures 1 & 2. The data from simulator exercises was fit to a two parameter Cumulative Weibull distribution, P(t).

$$P(t) = 1-\exp\{-(t/\alpha)^{\beta}\} \qquad (3)$$

Here

t = the time to perform the action, and the other parameters are provided in the following Table.

Weibull Parameters for Operator Response Curves

Parameter/Location	Old	New
Shape Parameter β	2.43	3.71
Characteristic Life α (sec)	169.8	69.9

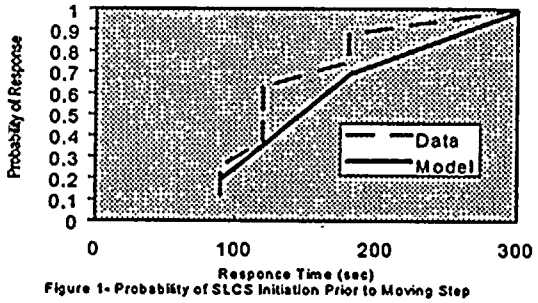

Figure 1- Probability of SLCS Initiation Prior to Moving Step

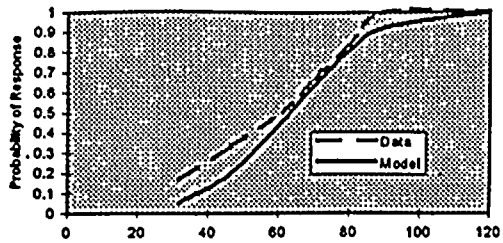

Figure 2 Probability of SLCS Initiation After Moving Step

Using these distributions, the probability of non-response can be computed for each case. As an example, initiation of SLCS within 120 seconds prevents power excursions, should depressurizaton be required, as in the case of ATWS with HPCI failure. Prior to changing this step, the probability of not initiating SLCS within 120 seconds is estimated to be 0.65. Therefore, ATWS with HPCI failure would likely result in core damage from power excursions. Changing the step to a more prominent location results in much earlier execution. The probability of non-response after changing the step is estimated to be on the order of 10^{-3}. This probability of failure is on the order of the equipment failure rate, which is the goal of this HRA method. This significant improvement is the result of establishing Defense in Depth. When Defense in Depth is established, reliable operator performance can be expected.

Step L5, Initiate the Automatic Depressurization System (ADS) if RPV water level cannot be maintained above TAF, also has a significant value of RAW once the IPE modifications to plant and procedures are incorporated. Depressurization is necessary to allow low pressure injection from either condensate or RHR should high pressure sources be unavailable. Given this set of failures, the operator responsible for reactor power will initiate SLCS and the operator responsible for reactor level will initiate ADS and attempt to control injection flow.

Core damage from unstable operation at low pressure is expected if the core is un-borated[b]. Additionally, uncontrolled injection from the RHR system could sweep boron from the RPV and cause a power excursion. Therefore, manual depressurization is of value only if boron is injected promptly and the RHR system can be controlled. Due to the changes to

[b] Mitigation of BWR Core Thermal-Hydraulic Instabilities GE NEDO-32164. BWROG EPG Rev 4 NEDO -31331 & BWROG EPG & AMG Rev 0 p B-14-8, SABRE Internal PP&L calculation EC-ATWS-0505.

the SLCS initiation step, prompt initiation of SLCS can be expected.

The RHR control circuit, however, was designed to prevent throttling RHR injection flow for 5 minutes after a Loss of Coolant Accident (LOCA) signal[c]. This lockout ensures that injection flow will not be throttled during LOCA, an appropriate design if one assumes that the operator is likely to inappropriately control flow. As discussed above, ATWS events generate a LOCA signal, but require RHR flow control. Given this design, the operator must control flow by starting and stopping RHR pumps. This method of flow control is not conducive to successful operation; thus, violating the Interface Criterion. The 5 minute lockout was removed from the control circuit. After modification the RHR system provides a viable system to provide controlled low pressure injection. With these changes to the procedures and plant design, it is reasonable to expect the operator to reliably execute the EOP steps.

ATWS, with SLCS failure, also represents a challenge to the operator. With SLCS failed, MRI represents an alternate method of shutting down the reactor. Insertion of less than 40 control rods is sufficient to place the reactor in hot shut down. Each rod requires about 45 seconds to insert. Therefore, if SLCS fails, the operator can avoid core damage or containment failure, if regimes of unstable operation can be avoided and the rods can be inserted, prior to exceeding the containment ultimate strength.

However the Rod Sequence Control System (RSCS) prevents driving out of sequence rods once the reactor power drops below 25% power. The RSCS must be bypassed before MRI can be used to shut down the reactor. The RSCS can be bypassed in the relay room using jumpers. This evolution would typically requires up to 30 minutes to accomplish from the time of scram failure. The probability that the operator will successfully insert 30 control rods, given the delay to bypass RSCS, prior to exceeding the containment ultimate strength, is much greater than the failure probability of the equipment used for MRI. Therefore, Defense in Depth was not satisfied.

This deviation from Defense in Depth was addressed by installing a RSCS bypass switch at the RSCS panel in the control room. With the RSCS bypass switch installed, the operator can initiate MRI immediately after SLCS initiation, independent of the status of SLCS. The peak containment pressure following installation of the RSCS bypass switch is calculated to be only 30 psig. This peak pressure was estimated assuming the operator initiated MRI at 10 minutes and a 90 second insertion time for each rod. The peak pressure using more realistic operator response data was limited to 12 psig. The operator is provided unambiguous instruction, the necessary facility to complete the action, and the amount of time available to complete the action far exceeds the time required to complete the action. Therefore, it is reasonable to expect the operator to perform at least as reliably as the equipment being operated.

In addition to bypassing the RSCS, the RPV must remain pressurized if MRI is to be used to shutdown the reactor without core damage. Operation of an unborated reactor at power and low pressure is postulated to result in core damage caused by a reactivity excursion. RPV depressurization can be expected during ATWS with SLCS failure for two reasons: loss of high pressure injection and suppression pool temperature exceeding the Heat Capacity Temperature Limit (HCTL). Both of these events are expected during ATWS with SLCS failure.

The HPCI pump is cooled by the pumped water. The water temperature for continuous operation should not exceed 140°F, however, temperatures up to 170°F are allowed for short periods of time. HPCI initially takes suction from the CST, but transfers to the suppression pool on high suppression pool level shortly after the ATWS. This transfer assures assumptions in the containment hydrodynamic loads analysis are not violated by HPCI operation. Again, this is an appropriate design if one presumes that the operator is likely to be unaware of the suppression pool level. However, successful response during ATWS requires the operator to bypass the suction transfer. This bypass takes place in the relay room and could require up to 30 minutes. The suppression pool temperature would exceed 170°F about 10 minutes following the ATWS. Since it is unreasonable to expect the action to be reliably completed, Defense in Depth was not established.

This violation was rectified by removing the automatic suction swap. Therefore, the HPCI suction remains from the CST and HPCI is not challenged.

The generic procedural guidance also requires emergency depressurization prior to exceeding the HCTL. The rationale for this guidance does not

[c] This lockout is not required to meet the plant licensing basis.

appear to consider the potential for core damage, when an unborated reactor is operated at low pressure. Additionally, the depressurization is performed as a precaution to ensure the availability of the containment vent. Venting is not required with success of MRI. Therefore, this guidance was eliminated from the ATWS EOP.

Prior to establishing Defense in Depth, the operator was hindered by plant features designed to inhibit operator action for other scenarios. While these features prevent inappropriate action during LOCA events, they hinder a proficient operator at responding to ATWS events. Establishing Defense in Depth required modifications to both equipment and procedures. These changes have resulted in a set of procedures that can be reliably implemented and the necessary facility to allow reliable execution.

EASE OF PROCEDURE IMPLEMENTATION

A number of actions identified in Table 2 have RAW and RRW values ~0. This implies that the plant risk is insensitive to the operators' proficiency at implementing these steps during ATWS events. Of particular interest are: steps L1, ADS Inhibit, and L3, Maintain water level in target.... The requirement to bypass the HPCI suction transfer has been eliminated from the Susquehanna design. The risk significances of these remaining actions has been reduced or eliminated in the process of establishing Defense in Depth.

Consider step L1, ADS Inhibit. This step prevents automatic depressurization during ATWS, which given the potential for core damage at low pressure, should be significant. However, in establishing Defense in Depth, the water level target band was raised above the ADS set point by 1.5 to 4 feet. Water level fluctuations may result in the level momentarily falling below the ADS initiation set point. However, transient calculations demonstrate when such fluctuations occur, the level rises above the setpoint prior to exceeding the ADS timer timing out. Therefore, failure to inhibit ADS has no impact on the calculated risk. The step is maintained in the procedures to satisfy the first Procedural Defense in Depth Criteria.

As with step L1, step L3, maintain water level in target band is also perceived to be important. Current generic guidance instruct the operator to maintain the RPV water level in a band from TAF to Minimum Steam Cooling Water Level (MSCWL), which is 30 inches below Top of Active Fuel (TAF) at Susquehanna. Therefore, to be successful, the operator must maintain the water level in a 30 inch band by controlling the pump flow rate. Additionally, the same operator must control reactor pressure using Safety Relief Valves (SRVs), since the RPV water level is extremely sensitive to their opening and closing. Operation below the MSCWL may result in core damage from insufficient cooling. Therefore, this step should have a very high RAW value.

This step is not risk significant at Susquehanna because the water level control band, which was designed to satisfy Defense in Depth, is used to protect the core and promote boron mixing. Two phenomena challenge core integrity during ATWS: thermal-hydraulic instabilities initiated by high core inlet subcooling and overheat from lack of cooling. Maintaining the RPV water level about 2 feet below the feedwater sparger, -60 inches below instrument zero, eliminates core challenges from thermal-hydraulic instabilities. Maintaining the RPV water level above TAF, -161 inches below instrument zero, ensures two phase core cooling. Therefore, a level control band of -60 to -161 provides the necessary protection for core cooling, while allowing the operator a 101 inch control band. Additionally, higher water levels promote boron mixing and suppress water level fluctuations due to the greater free area when the water level is above the upper plenium. Therefore, the operator is instructed to keep the level above -110 inches when possible.

This water level strategy has the added advantage, that during the challenging MSIV closure ATWS, the operator need only verify HPCI initiation and operation. The water level for full HPCI flow is about -110 inches below instrument zero, which is within the water level control band. The water level will drift up as liquid boron reduces the reactor power, however, by the time the water level reaches -60 inches, sufficient boron has been injected to shutdown the reactor. Therefore, during the challenging MSIV closure ATWS, operator intervention is not required for water level control.

OPPORTUNITIES LOST

This paper has demonstrated that reliable operator performance can be expected, when Defense in Depth is satisfied. Additionally, it has been shown that taking credit for reliable operator performance allows the IPE to be used to investigate opportunities

for safety improvement. This section addresses the converse; that is, assuming unreliable operator performance results in less reliable operator performance and lost opportunities for safety improvement.

This hypothesis was investigated by using typical OEP in the Susquehanna event and fault trees and then computing the RRW for each EOP step. These operator error probabilities were obtained from NUREG-1150 and NSAC-152 and are presented in Table 2, along with the RRW for each step. Using these OEPs, the re-calculated core damage probability for ATWS sequences at Susquehanna was computed to be 1.4×10^{-6}. This number is comparable to the values reported in NUREG 1150 of 1.9×10^{-6} and an industry performed IPE of 1.0×10^{-6}. This comparison implies that the calculated core damage frequency for ATWS is determined by the values assumed for operator error.

As discussed earlier, the RRW is used to determine what EOP steps, if improved, are likely to result in a safety improvement. Reviewing the RRW values in Table 2, one sees that only SLCS initiation represents the potential for safety improvement. When credit is taken for the improvement discussed in this paper, the calculated core damage probability is reduced from 1.4×10^{-6} to 1.6×10^{-8}.

If the actual operator performance is consistent with the typical values generated using traditional HRA models, then the significant risk reduction from the safety improvements identified using Defense in Depth may never be realized during an actual plant event because the operator may not perform the procedural steps. However a set of optimized EOPs that can be implemented within the available time and the facility to implement them exist for those operators who do implement them. The only "downside" of using Defense in Depth to evaluate operator performance is the potential to underestimate the calculated risk.

However, if operator performance exceeds the expectations of those employing typical OEP, then those employing typical OEPs may never realize the safety improvements identified using the Defense in Depth approach. EOPs will not be optimized nor do incentive exist to improve equipment interfaces. Good operators will not have the opportunities for implementing mitigating actions, since these actions will not be available through the plant design and procedures. One gains a "conservative" estimate of the core damage probability, but looses potential success paths that all operator can implement.

CONCLUSION

As described above, numerous changes to the Susquehanna design, procedures, and operator training program have occurred. These changes were made to establish defense as defined in Table 1. The result of these changes are:

- a set of Emergency Operating Procedures that are unambiguous in intent and expected outcome, and have a high likelihood of successful implementation,
- a control room that presents the information necessary to implement the procedures in a unambiguous and timely manner and the controls necessary to reliably execute the EOPs, and
- an operating crew that is well trained, practiced and tested on observing symptoms, entering appropriate procedures and executing the necessary steps.

These changes were made as result of satisfying Defense in Depth and represent a real safety improvement.

It has been shown that the current HRA methods yields estimates of the core damage and containment failure frequency, which some find more believable, but could fail to generate opportunities for safety improvement. Applying the Defense in Depth approach yields core melt and containment failure frequencies that are unbelievable to some, but has provided the opportunity for real safety improvement. PP&L has chosen to focus attention on identifying severe accident vulnerabilities and opportunities for safety improvement. To this end the Defense in Depth approach bore much fruit.

TABLE 1
SEVERE ACCIDENT DEFENSE IN DEPTH CRITERIA

A. Accident sequences with high calculated frequencies are unacceptable.

B. Accident sequences having low calculated frequencies must also have Defense in Depth. Defense in Depth is defined for equipment and procedures as follows.

Equipment

1. Core damage or containment damage shall not occur without multiple failures of redundant or diverse equipment.

2. Vessel failure shall not occur following core damage unless an additional independent equipment failure occurs.

3. Containment failure shall not occur following core damage unless an additional independent failure occurs.

4. Containment failure shall not occur following vessel failure unless an additional independent equipment failure occurs.

Procedures

1. No procedures shall have adverse consequences in the case of additional equipment failures beyond those occurring initially.

2. The necessary anticipatory actions shall be performed to avoid loss of additional equipment, but shall not degrade the existing situation.

3. The necessary anticipatory actions shall be performed to permit successful response to potential failure, but shall not degrade the existing situation.

Interface

The nature and timing of information to the operator shall be sufficient to assure timely execution of all appropriate procedural steps.

TABLE 2
OPERATOR ACTIONS EVALUATED IN ATWS ANALYSIS

Step #	Action	Purpose	RAW	RRW	Typical OEP
1	Entry & follow ATWS EOP	Directs operator actions when power > 5%	3,038	0	0.0003
Q1	Initiate SLCS	Injects liquid poison into core	126	0.904	0.02
Q2	Manual Control Rod Insertion (MRI)	Diverse method of reactivity control	5.4	.052	1.0
L1	Inhibit ADS	Prevents undesired ADS initiation should water level oscillations trigger ADS	~0	~0	na
L2	Throttle flow until RPV level<-60	Manual action required, when MSIVs are open, to prevent density wave oscillations. Not required if MSIVs close	18	~0	0.27
L3	Maintain water level in target band of -80 to -110 with allowable range of -60 to -161	Prevents density wave oscillations, ensures two phase core cooling and promotes boron mixing	~0	~0	na
L4	Bypass HPCI suction transfer	Prevents HPCI failure on high suction temperature	~0	~0	0.02
L5	Initiate ADS if RPV water level cannot be maintained above -161 (TAF)	Rapidly reduces RPV pressure to allow low pressure makeup to inject	119	0.059	0.02
L6	Control Low Pressure Makeup (LPM)	Manual control of LPM required to prevent boron flushing and reactivity excursions	6.6	0.06	0.64
2	Initiate Suppression Pool Cooling (SPC)	Removes energy from the containment	760	0.07	0.00001