CONF-880464--1

DE88 005437

Use of probabilistic risk assessment (PRA) in expert systems to advise nuclear plant operators and managers

Robert E. Uhrig

Instrumentation and Controls Division, Oak Ridge National Laboratory,*
P.O. Box X, Oak Ridge, Tennessee 37831-6009
and Department of Nuclear Engineering, University of Tennessee
Knoxville, Tennessee 37996-2300

ABSTRACT

The use of expert systems in nuclear power plants to provide advice to managers, supervisors and/or operators is a concept that is rapidly gaining acceptance.[1,2] Generally, expert systems rely on the expertise of human experts or knowledge that has been codified in publications, books, or regulations to provide advice under a wide variety of conditions. In this work, a probabilistic risk assessment (PRA)[3] of a nuclear power plant performed previously is used to assess the safety status of nuclear power plants and to make recommendations to the plant personnel.

Nuclear power plants have many redundant systems and can continue to operate when one or more of these systems is disabled or removed from service for maintenance or testing. PRAs provide a means of evaluating the risk to the public associated with the operation of nuclear power plants with components or systems out of service. While the choice of the "source term" and methodology in a PRA may influence the absolute probability and consequences of a core melt, the ratio of two PRA calculations for two configurations of the same plant, carried out on a consistent basis, can readily identify the increase in risk associated with going from one configuration to the other. PRISIM,[4] a personal computer program to calculate the ratio of core melt probabilities described above (based on previously performed PRAs), has been developed under the sponsorship of the U.S. Nuclear Regulatory Commission (NRC). When one or several components are removed from service, PRISIM then calculates the ratio of the core melt probabilities. The inference engine of the expert system then uses this ratio and a constant risk criterion,[5] along with information from its knowledge base (which includes information from the PRA), to advise plant personnel as to what action, if any, should be taken.

1. INTRODUCTION

The original purpose of the system described here was to monitor the status of a nuclear power plant in order to identify situations which, if not mitigated, would lead to an unsafe condition or a plant trip. Indeed, the objective was to identify a problem early in a potential scenario and be able to take timely action to avoid a trip. As the project developed, it became evident that information in the knowledge base of the expert system, which came from a previously performed PRA, was valuable to plant managers and supervisors as well as operators. The expert system can be used either in an on-line mode in which information on component and system failures is monitored, or in a "what if" mode in which plant personnel may query the system to evaluate the plant status. Information from the PRA can provide a basis for decisions on priorities and resource and manpower allocations that can minimize the risk to both the public and the plant.

2. USE OF PRA IN NUCLEAR PLANT CONTROL AND MANAGEMENT

It is a well-known fact that nuclear power plants have many redundant systems and can continue to operate with one or more of these systems disabled. Indeed, it is standard procedure to remove systems from service in order to maintain or test them to meet regulatory requirements. Often there is a time limit for any particular redundant plant component or system to be out of service, set by the NRC as part of the technical specifications (TSs) or the limiting conditions of operation (LCOs) on the basis of perceived risk to the public. Since risk, particularly perceived risk to the public, is a difficult quantity to evaluate, most time limits in TSs and LCOs are judgment calls by the NRC staff and the operating utility.

The application of probability risk assessment (PRA) to nuclear power plants[3] provides a means of evaluating the risk to the public associated with the operation of nuclear power plants, at least on a relative basis. While the choice of the "source term" and

*Operated by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under Contract No. DE-AC05-84OR21400.

methodology in a PRA may influence the absolute probability and the consequences of core melt, comparison of two PRA calculations for two configurations of the same plant, carried out on a consistent basis, can readily identify the increase in risk associated with going from one configuration of a plant to another (e.g., by removing components or systems from service). This ratio (called "risk factor," R) of core melt probabilities (assuming no recovery of failed or disabled systems) obtained from two PRA calculations for different configurations was the principal numerical input to the expert system that recommends what mitigating action, if any, would be taken to prevent an unsafe situation from developing. Although the risk factor obtained from a PRA is not the only (or necessarily the best) basis for making such recommendations, the rationale for this choice was that

1. it involves PRAs that most plant managers and reactor operators understand (at least conceptually), and PRAs are available (or will be available) for most plants;

2. core melt probabilities (or their reciprocals) are arguably related to nuclear safety, and hence constitute reasonable criteria on which to base decisions involving nuclear safety; and

3. PRISIM,[4] a computer program that readily gives the desired ratio of core melt probabilities (i.e., the risk factor, R) on a personal computer using the results of a PRA performed previously, had already been developed for the NRC under a contract supervised by ORNL.

3. PRISIM: PLANT RISK STATUS INFORMATION MANAGEMENT SYSTEM

Under the sponsorship of the NRC, PRISIM was developed by JBF Associates of Knoxville, Tennessee, to provide resident inspectors at nuclear power plants with the relative safety status of the plant under all configurations. PRISIM calculates the risk factor R using an algorithm that emulates the results of the original PRA. It also presents additional information about the current status of the plant.

PRISIM supplies two types of information: an interactive response that reflects the status of the plant at that moment, and preprocessed (or "canned") information from the PRA that is independent of the plant's status. As various plant components or systems fail or are removed from service for testing or maintenance, the core melt probability changes. For each configuration, PRISIM quickly provides the following situation-specific information:

- the factor by which the instantaneous core melt probability increases when the specified set of components is out of service. This is the quantity called the risk factor, R, which is discussed above.

- the most important failure scenarios for core melt, ranked according to their expected probabilities of occurrence. This provides a priority listing of plant failure modes.

- a ranking of the safety-related equipment "not known to be out of service" according to their relative contributions to the instantaneous core melt probabilities. This provides a list of equipment that is important in avoiding core melt.

- a ranking of the specified out-of-service equipment according to the benefit of restoring each to service.

PRISIM considers the removal from service of about 90 components or subsystems in 11 major systems and calculates the values of the risk factor if they are removed from service. Multiple failures are considered, but the risk factors for individual components or systems do not combine in any logical way. For instance, the battery & switch gear emergency cooling system has six components that have risk factors of 10. However, when any two of them are removed from service simultaneously, the combined risk factors range from 19 to 73. If three of these systems are removed simultaneously, the combined risk factors range from 28 to 130.

To demonstrate the kind of information available under multifaulted conditions, Table 1 shows the output from PRISIM as displayed on the PC monitor when four important systems are taken out of service. The particular four systems removed from service are listed in Table 1 and give a risk factor of 430--a very large value. Table 1 also presents the ranking of the importance of equipment "not known to be out of service" and presumably functioning properly. These pieces of equipment represent the various systems yet available to prevent core melt, without restoration of any systems.

More importantly, Table 1 presents the equipment ranked according to the benefit of restoration: returning the 125-V dc Bus D02 or diesel generator 1 to service is at least five times more important than getting the BWST (borated water storage tank) outlet block

Table 1. Risk Implications Of The Current Plant Status

430 Is The Risk Factor With The Following Equipment Out Of Service

Battery and switchgear room cooling system chilled water train A fails
125-V dc Bus D02 fails to provide power
Diesel generator 1 fails
BWST Outlet block valve BW1X plugs

Ranking of equipment not known to be out of service:

1. SRV fails to reclose (EFW available)
2. SRV fails to reclose (EFW unavailable)
3. ICWS isolation valve CV3820 fails to close
4. Auxiliary cooling water systems isolation valve CV3643 fails to close
5. EFW pump P7A turbine steam relief valve PSW-6602 fails open
6. Diesel generator 1 HX service water valve CV 3806 fails to open
7. SRV fails to reclose (loss of offsite power and EFW available)
8. Battery and switchgear room cooling system--chilled water train B fails
9. Diesel generator 2 fails
10. Independent failure of the power conversion system
11. Service water pump P4B fails to start
12. Emergency feedwater pump P7A fails

Equipment ranked according to the benefit of restoration

Equipment	Risk factor reduction
125-V dc Bus D02 fails to provide power	6
Diesel generator 1 fails	5
BWST outlet block valve BW1X plugs	1
Battery and switchgear room cooling system train A fails	1

valve BW1X plugs or the battery and switchgear room cooling system back into service. It is clear that information of this sort is useful to the plant manager and supervisors in determining which systems warrant priority attention.

PRISIM also contains 981 core melt scenarios, and it presents them in rank order for the particular faulted configuration. Usually, only the first five or six scenarios are meaningful, but all 981 are available in the event the plant configuration changes.

The preprocessed information from the PRA that PRISIM provides is grouped into the following categories, which are described briefly:

Dominant accident sequences. Table 2 presents the dominant accident sequences ranked by percent of core melt probability (without recovery of any failed systems or components). The initiating event is presented, as well as the safety-related system whose failure caused the event.

Safety-related systems, subsystems and components. The information available on plant safety-related systems, subsystems, and components includes the risk reduction importance (the fractional decrease in risk when equipment is perfectly reliable), the risk sensitivity importance (the approximate increase in risk when equipment fails), and the risk significance importance (a combination of the first two importances). Risk reduction and risk sensitivity importances are ranked numerically with values presented.

Support system interfaces. Support system interfaces provide information on the support services required by safety system components. Only functions that alone can fail either a component of a front-line system or another support function are considered. The support system development presented takes into account the specific role(s) that the component or function must play in mitigating the accident scenarios of interest.

Component failure data. Component failure data available for the plant include summaries of licensee event reports (LERs) by component type, and comparisons of plant-specific failure data with industry-averaged failure data for plant equipment.

Table 2. Dominant Accident Sequence Selection List

Rank	Initiating event	Safety-related system failures	% Of core melt probability (w/o recovery)	% Of core melt probability (w/recovery)
1	Loss of power conversion system	SRVR-HPRS	21.0	7.4
2	Small LOCA (eq. diam ≤1.2 in.)	HPIS	16.0	17.0
3	Loss of offsite power longer than 8 hours	HPIS	14.0	27.3
4	Loss of offsite power	SRVR-HPRS	12.0	3.8
5	Transient requiring scram (all front-line systems avail.)	PCS-SRVR-HPRS	7.9	2.8
6	Small LOCA (eq. diam ≤4 in.)	HPRS	7.1	2.6
7	Small LOCA (eq. diam ≤1.66 in.)	HPRS	6.0	2.1
8	Loss of offsite power	EFS-HPIS	4.1	5.1
9	Small-small LOCA (eq. diam ≤1.2 in.)	EFS-HPRS	3.1	2.0
10	Loss of service water system	SRVR	2.4	14.5
11	Loss of power conversion system	SRVR-HPIS	0.83	0.78
12	Loss of offsite power	SRVR-HPIS	0.79	1.2
13	Loss of offsite power	EFS-SRVR-HPIS	0.71	1.0
14	Transient requiring scram (all front-LINE systems avail.)	RPS-HPIS	0.67	0.04
15	Loss of service water system	EFS	0.52	2.5

Testing/surveillance requirements. The PRISIM data base provides information associated with periodic testing/surveillance requirements for safety-related systems. Descriptions of integral tests and of component tests associated with the selected safety-related systems are presented.

Operator actions. Information available for operator actions includes planned operator responses and operator recovery actions. Both can be presented in rank order by risk reduction importance, risk sensitivity importance, and/or risk significance importance. Numerical values are presented.

4. IIR: INCREMENTAL INCREASE IN RISK

In order to utilize information from PRISIM in an expert system, it was necessary to select one specific quantity that broadly represents the safety status of the plant, and hence could serve as a criterion for decision making. The quantity selected was the product of the increase in core melt probability for a particular faulted configuration and the time that it exists. This dimensionless quantity, called the "incremental increase in risk" (IIR), is shown as the cross-hatched area in Figure 1, which is a plot of the probability of core melt vs time that a faulted condition exists. If A, the probability of core melt for normal operations, is increased to B due to one or more faulty components (or components removed from service for maintenance) for a period of time, T, then the value of IIR is [(B - A)T]. Since, by definition, B is the product of the risk factor R and the normal core melt probability A, IIR is equal to [A(R - 1)T]. The concept adopted in this study was that the limiting value for IIR would be the <u>same</u> for all situations.[5] (Although this approach is not consistent with current NRC practice, it provides a philosophical basis for setting time limits on LCOs and TSs.)

Since the PRISIM prototype used the PRA for Arkansas Nuclear One (ANO), a B&W pressurized light-water reactor, this study adopted a B&W plant of that vintage and size for demonstration purposes. An early PRA on ANO indicated that it had a core melt probability of 3.79×10^{-4} per year or 4.33×10^{-8} per hour with all systems operational. In order to select a limiting value of IIR, the LCOs and TSs for ANO were reviewed. The reference situation chosen for the decision criterion was the LCO associated with all components of one train of the auxiliary feedwater system being out of service. It allowed the system to be out of service (for which PRISIM gave an R value of 18.2) for up to 36 hours. Hence,the core melt probability for this faulted configuration is $(18.2 \times 4.33 \times 10^{-8})$ per hour, and the corresponding limiting value of IIR is $[4.33 \times 10^{-8} \times (18.2 - 1) \times 36] = 2.68 \times 10^{-5}$. The concept envisioned here is that the plant would be shut down (either automatically or by the operator upon the advice of the expert system) when the IIR reached this value. It is interesting to note that most, but not all, of the incremental integrated risks for the various limitations imposed by LCOs and TSs are less than this limiting value.

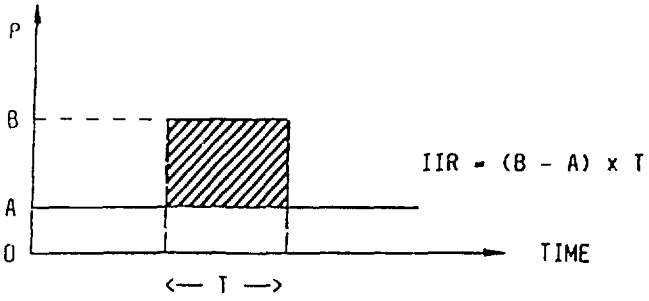

Figure 1. Plot of core melt probability vs time out of service.

5. USE OF PRISIM IN AN EXPERT SYSTEM

The original PRISIM program was modified to provide a "live" display that calculates the risk factor for a particular configuration and presents a bar chart showing how long the plant could continue to operate before our chosen limiting value of IIR (2.68×10^{-5}) is exceeaed. Plant personnel can choose the component or combination of components to be taken out of service, and this modified PRISIM program will calculate how long the plant can continue to operate before regulations require that either some of the components be returned to service or the plant be shut down. Some configurations with low risk factors can operate for days or weeks without exceeding the limiting IIR value, while others with large risk factors can operate for only a few hours. For instance, use of the risk factor of 430 found in Table 1 would require the plant to be shut down within 86 minutes unless one or more of the systems could be brought back into service within that time.

The principal virtue of this approach is its simplicity. It gives plant personnel a good indication of the time available to get components back into service and avoid a shutdown. It also gives them a clear picture of the components that must be maintained to avoid core melt, assuming that none of the inoperative components are returned to service.

One difficulty with this system is the situation in which a component or system out of service produces a <u>deminimus</u> value of IIR. Although the true risk to the plant and the public is insignificant, the value of IIR continues to grow over time toward the limiting value. For a faulty component that has a risk factor of 1.5 (a 50% increase in a very small risk), the limiting value of IIR would be reached in 1238 hours or 51.6 days, requiring the plant to be shut down. The solution to this problem is to use a type of "forgiving" system that ignores or deemphasizes the influence of problems in the past. One method is to use a negative exponential weighting with passing time (a form of convolution). This can be readily implemented with an appropriate exponential decay constant and a newly defined limiting parameter (which would be different from the IIR used above). Another alternative, which was actually implemented, is to use a 72-hour "moving window" in which the influence of any configuration that existed more than 72 hours (or some other appropriate time period) in the past does not contribute to the calculation of IIR.

The expert system "shell" chosen for this program was Texas Instruments' PERSONAL CONSULTANT PLUS. Rules involving risk factors, IIR, and the time before shutdown given by PRISIM were incorporated into the knowledge base as well as rules associated with the list of components presented by PRISIM that stood between the present configuration and core melt. The PRISIM program was modified to calculate the increase in core melt probability on a continuous basis and then to calculate the corresponding IIR value using a three-day moving window. These values were entered into the expert system, which then presented its recommendations for consideration by plant personnel.

Since both PRISIM and PERSONAL CONSULTANT PLUS are large computer programs, they were implemented on separate AT class personal computers (PCs). For "proof of principle testing," data and plant information were transferred manually between the two programs. With the advent of extended and expanded memories and multi-tasking operating systems, it is expected that both programs can be put on the same PC, with direct communication between the two programs. Much work remains to be done to make this approach "user friendly."

6. CONCLUSION

This program has demonstrated the feasibility of using a probabilistic risk assessment as a basis for decisions in an expert system to advise plant personnel regarding the status of a nuclear power plant. The system utilizes information from the PRA and presents it in an intelligent form, along with its recommendations and the rationale behind them. Indeed, this type of system, had one been available, could have warned the plant operators at Chernobyl that they were getting into a serious situation as they systematically disabled the various safety systems.

7. REFERENCES

1. Proceedings of ANS Topical Meeting, "Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry," Snowbird, Utah (August 31-September 2, 1987).

2. Seminar Notebook, "Expert Systems Applications in Power Plants," Electric Power Research Institute, Palo Alto, California, Boston, Massachusetts (May 27-29, 1987).

3. "PRA Procedures Guide," NUREG/CR-2300, U.S. Nuclear Regulatory Commission (1983).

4. D. J. Campbell et al., "Operational Phase of Inspection Prioritization," Trans. Thirteenth Water Reactor Research Information Meeting, NUREG/CP-0072, U.S. Nuclear Regulatory Commission (October 1985).

5. R. E. Uhrig et al., "Basis for Setting Technical Specifications and Limiting Conditions of Operation," Trans. Am. Nucl. Soc. 53 (1986).

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.