DEVELOPMENT AND APPLICATION OF THE SAN ONOFRE SAFETY MONITOR

ABSTRACT

Halliburton NUS Corporation (NUS) has developed a risk-based configuration management software tool for use at Southern California Edison's San Onofre Nuclear Generating Station. The software, called the Safety Monitor, calculates an estimate of current plant core damage risk based upon the plant's current operating configuration (e.g., equipment operability, system operating alignments). All data is entered and displayed in a format easily understood by plant personnel.

The plant hopes to use this tool to ensure that risk is minimized during plant operations and to identify situations in which current Technical Specifications can be optimized. Plant configuration data and out-of-service time data is also automatically collected.

INTRODUCTION AND BACKGROUND

Southern California Edison (SCE) has been actively using its Probabilistic Risk Assessment (PRA) models to support operations and maintenance issues for many years at the San Onofre Nuclear Generating Station (SONGS), Units 2 and 3. This support generally involves the evaluation of specific plant operating conditions and strategies using various sensitivity studies. In many cases, the risk significance of various Technical Specifications and their Limiting Conditions for Operation (LCOs) and Allowable Outage Times (AOTs) were evaluated to address specific plant concerns. These Technical Specification studies indicated that some LCOs and AOTs might be too restrictive or did not consider that different plant operating conditions might alter the risk significance of each Technical Specification.

The U.S. Nuclear Regulatory Commission (NRC) has been conducting research into the risk implications of Technical Specifications and sought to create an industry working group to study these issues further. SCE agreed to join this working group in 1989, along with several other utilities. This group met periodically to discuss the various technical issues and to share the results of each organization's research into Technical Specification issues.

SCE recognized that it would be most useful to develop an on-line tool for operations and maintenance personnel that would allow easy access to risk information. In Great Britain, Nuclear Electric had developed a tool, called the Essential Systems Status Monitor (ESSM) for its Heysham station. ESSM is a computer-based tool that enables plant operators to directly determine the risk status of the plant based upon current equipment operability conditions. At Heysham, ESSM operation is an integral part of the plant's Technical Specifications and serves as the basis for acceptable plant operations. For example, if ESSM indicates that current plant risk is acceptable for the plant's current maintenance/operability state, then operations can continue in that state indefinitely.

SCE wished to develop a tool similar to ESSM for SONGS. However, whereas ESSM is a minicomputer-based application, SCE wished its tool (to be called the Safety Monitor) to be a personal computer-based application that would support multiple users on its Local Area Network. SCE also wished to make use of the Microsoft Windows' graphical user interface to make the tool easy to use by plant personnel.

A particular concern was the method by which the risk model solution would be obtained. In the past, PC-based risk tools would use the solution from the master PRA model (i.e., the cutset equation) and would requantify this pre-solved equation by changing the numerical values assumed in the equation. This method facilitates rapid calculation, but might not always give the correct results if unusual plant conditions make normally non-risk-significant equipment failures become risk dominant, the cutset equation could underestimate the importance of this equipment since its failure contributions might have been discarded from the model.

To reduce the likelihood of such model truncation errors, other plants that have used the cutset equation technique have either developed very extensive cutset equations or have...
developed libraries of cutset equations for each of the various plant operating states that might be experienced. While these approaches help to reduce the effects of truncation errors, the maintenance of these equation libraries can be very time consuming. If a change is needed to the risk model, significant labor effort could be required to regenerate the equation libraries since many calculation runs might need to be performed.

The last several years have seen the development of several ultra-fast fault tree solution algorithms. SCE desired that the SONGS Safety Monitor make use of these fast algorithms to allow the Safety Monitor to solve the entire risk model based upon unique plant conditions, rather than use pre-solved equations. Such an approach would not be possible without an extremely fast algorithm, since model re-solution typically takes many hours to perform using typical solution approaches. The use of a model re-solution approach, however, would ensure that the correct solution is obtained for each plant configuration. Maintenance of the model would also be simplified, since logic changes could be made directly to the model itself without the need to do numerous calculations.

SCE selected NUS to assist it in the development of the Safety Monitor code. NUS personnel had actively supported the PRA model development and its application to plant operating issues. Its personnel had also developed many of the computer codes used to maintain and quantify the SONGS models. NUS also had access to several of the modern ultra-fast solution algorithms that would need to be investigated for suitability of use in the Safety Monitor.

SOFTWARE DEVELOPMENT

SCE desired that the code be developed as Quality Affecting software using state of the art code development and Verification and Validation (V&V) standards. As a starting point, SCE and NUS defined a functional specification for the code. The specification considered such issues as expected users, display requirements, software constraints, and security requirements. Among the key functional requirements was the display of PRA information in a format that is readily understandable to non-PRA-familiar personnel and the ability to calculate an estimate of current plant risk using a complete Level 1 PRA plant fault tree within five minutes.

Based upon the completed functional specification, NUS developed a functional prototype of the code, using the Microsoft Visual Basic™ software development system. Visual Basic was selected for this purpose since it allowed for rapid development of highly functional software under Microsoft Windows. The prototype illustrated each of the main display screens and simulated the operation of each primary function through the use of sample data.

The prototype was reviewed with plant personnel to obtain comments regarding functionality, ease of use, and display format. A number of changes were made based upon the prototype's operation. Once comments were incorporated into the prototype, it was used as the basis for the development of the Software Design Document (SDD) for the actual code. Later, during software development, the prototype was used by the code designers to better understand what the completed software should do.

The development of the SDD was the next step in the software design process. The SDD forms the link between the functional specification developed at the beginning of the project and the final developed software. The SDD describes in text form the complete software design. Included are descriptions of each software module, module-to-module program flow, the detailed functions each module is to perform, descriptions of each data base and data file used by or created by the program, and example designs of each display screen (in this case, from the prototype code). The complete SDD describes over 80 software functions and 25 data bases and data files to support the program.

The SDD was reviewed by NUS personnel and SCE personnel to ensure it satisfied all requirements of the functional specification, and that the proposed code was feasible from a software design perspective. Various comments were received and incorporated into the SDD before actual software development began.

The software itself was developed using Borland C++ and various C++ toolkits. Data bases use the Raima Data Manager, a SQL-based multi-user Microsoft Windows-compatible data base system. The completed code consists of over 50,000 lines of code, plus hundreds of software objects to define various data structures, screen displays, and reports.

The heart of the program is the fault tree solution engine. In order to comply with the five minute solution requirement, a state of the art engine must be coupled with a very efficient, optimized fault tree model structure. NUS investigated several alternative solution engines and determined that the RELMCS algorithm would be best suited for this application. RELMCS is a product of RELCON AB of Sweden and is a proven high speed algorithm capable of solving very large fault tree models. The other options considered either lacked the ultra-fast solution speed or were largely unproved and contained known errors that would need to be corrected before the Safety Monitor could be considered operational.

The RELMCS algorithm computes a solution of the Level 1 core damage model in less than 5 minutes on a 486DX2-66 personal computer using a 1 x 10^-9 truncation level for cutsets. The use of an Intel Pentium™-based computer reduces the solution time to about two minutes. For comparison purposes, solution of the same model using a conventional code (e.g., FTAP, SETS, etc.) requires a computation time of at least one hour!

Using the SDD, the completed code was V&V'd for both stand-alone and multi-user network operation. The functional requirements list of the SDD served as a convenient basis for conducting the V&V and demonstrating that the code fulfilled all of its requirements.
RISK MODEL DEVELOPMENT

The development of the logic model used in the Safety Monitor involved three steps: the development of a fault tree top logic to represent the plant accident sequences; the development of consolidated fault tree models for each key system; the expansion of the fault tree models to include all plant operating configurations, and the mapping of plant components to the events in the logic model. The completion of this process resulted in a logically efficient model that is correlated to all plant components and captures all of the logic structure of the complete Level 1 PRA.

The Safety Monitor model is developed as a single fault tree whose top event is "core damage occurs due to an accident or transient". Each of the fifteen initiating events from the PRA are included in the model, as are all 92 core damage sequences from the event trees. However, in developing the Safety Monitor model, sequences can be combined and non-minimal sequences can be subsumed into other sequences. For example, a small LOCA sequence involving high pressure safety injection failure, RCS depressurization and low pressure safety injection success, and failure of auxiliary feedwater (AFW) can be subsumed into a sequence involving only failure of AFW, since the success of core cooling is irrelevant in terms of preventing core damage. Also, some sequences might involve early failures of a system, while other sequences involve late failures of the same system. These sequences might be able to be combined into a single sequence if both early and late system failures can be incorporated into the system fault trees. Using these methods, the 92 original sequences were reduced to about 45 sequences for evaluation in the Safety Monitor. The final step of the process involves grouping of similar sequences across initiating events wherever possible. For example, failure of AFW may lead to core damage for several initiating events. If the success criteria for AFW for these initiating events are similar, then the events can be analyzed as a group.

Following the development of the top fault tree logic, each of the system fault trees is examined to determine if it can be logically simplified. This process involves the elimination of duplicative logic gates, consolidation of events into "super" basic events (where possible), and restructuring of the fault tree to move support system fault tree linkages to as close to the top of the fault tree as possible. These actions help to reduce the number of logic gates and events in the model and reduce the number of inter-system linkages, while retaining the same cutset results as the original model. Using this approach, a system model that requires 20 pages of modeling in the original PRA can be reduced to 4 or 5 pages in the Safety Monitor model. It should be noted that this optimized model yields the same numerical results as the original model and that the information concerning basic events consolidated into "super" basic events is retained in the Safety Monitor data files so that full model fidelity is maintained.

Because the Safety Monitor will have to evaluate all of the possible system alignment states that can be used during power operation, the model had to be revised to properly support these alignments. At San Onofre, several key systems have "swing trains" and other alternate configurations. In the base Level 1 PRA, not all of these configurations are considered since they may be all logically equivalent. Six system models were identified for logic expansion to account for the various operating alignments.

The last step of the process is the correlation of the various plant components to the Safety Monitor model. One of the functional requirements of the software is that it must allow the plant operator to access any component in the plant, even if that component does not affect the safety model. As a result, over 55,000 components were loaded into the data bases for the Unit 2 Safety Monitor. Each of the basic events in the model were then reviewed to determine which components pertain to each basic event. This process was complicated by the fact that the equipment numbering scheme used by the operations and maintenance personnel differs somewhat from that used in the design drawings and system descriptions that were used to develop the Level 1 PRA models. As a result of this correlation effort, several thousand plant components were shown to directly affect the model's events. It is expected that several thousand additional components will be added to the correlation listings as the data bases are expanded to include various manual isolation and drain valves and other components not typically addressed in traditional PRAs.

SOFTWARE OPERATION

Figure 1 illustrates the main display screen of the Safety Monitor. Safety status is shown on the "gauge" display, along with a plot showing the risk level over the last seven days. A risk-based recommended AOT is provided to indicate how long the plant can remain in this configuration before SCE administrative risk limits are exceeded. From this main screen, the user can request the various functions of the monitor. The "administration" menu provides access to various administrative and PRA-specific functions that would not normally be accessed by plant operations personnel.

![Figure 1 - Main Display Screen](image)

Figure 2 shows the display of current plant status. The display shows the plant equipment currently out of service and the presence of environmental factors that might affect risk.
Examples of these factors might be severe weather or the performance of surveillance testing that might cause a plant scram. The "plant configuration" button is used to view the operating alignments of various plant systems that affect plant safety.

Figure 2 - View Status Screen

Figure 3 illustrates how the user removes equipment from service. The user selects the system and trains to display, then clicks on each component to remove from service. The user can also remove pre-selected groups of equipment from service simultaneously via the "select components via BAG (boundary area grouping) ID". BAGS are defined by San Onofre maintenance planning personnel for typical maintenance tag out boundaries for major pieces of equipment.

Changes in plant operating alignments, the presence (or absence) of environmental factors or special testing conditions, or the operability/inoperability status of plant equipment may be investigated using either "real" status changes or "hypothetical" status changes. "Real" status changes perform updates to the risk level display and record the changes to risk history and configuration history files. "Hypothetical" calculations allow the user to determine the effects of proposed actions in a "what if" fashion to investigate various maintenance strategies for the current plant operating configuration.

Figure 4 illustrates the display of currently important equipment. This display shows what currently operable equipment in the plant has the greatest risk significance given the plant's current operating configuration. Standby equipment that might be benefited by some form of functional testing is also indicated. The "testing advice" button provides an estimate of how much risk improvement might be realized if key equipment was operability tested at this time.

Figure 5 illustrates the advice provided to the user regarding what inoperable equipment should be restored. The display indicates the type of inoperability (equipment failure, routine maintenance, out of service for functional testing), as well as an estimate of how plant risk would be improved if each piece of equipment was restored. The user can also determine the effects of restoring a group of equipment simultaneously.

INTEGRATION INTO PLANT OPERATIONS

The Safety Monitor began use in an "off-line" capacity in December, 1993. Over a several month period, actual data from control room logs will be input to the code to check
software operation, to ensure that the Safety Model gives reasonable risk results over a variety of plant operating conditions, and to help establish appropriate administrative limits for the "green", "yellow", and "red" operating ranges. Following this pilot phase, operation of the Monitor will be introduced to the operations and maintenance staffs. In addition to its use by plant operations and maintenance planning personnel, it is expected that PRA personnel and plant management will use the Monitor to periodically assess plant performance. Several of the key data collection features of the Monitor may also be used to support compliance with the U.S. Nuclear Regulatory Commission's Maintenance Rule.

SCE hopes the information provided from the Monitor will be used to help establish a more risk-based approach to Technical Specification determination and compliance. For example, allowed outage times might be varied based upon the particular plant configuration that exists (e.g., a component might have a longer AOT if no other safety-affecting components are out of service, and a lesser AOT if other key equipment is already out of service). The Monitor might also be used as a basis for deferring routine Technical Specification required testing if the conduct of the test at a particular time might unduly increase the risk to the plant. Such tests would be rescheduled for performance during lower risk periods.

CONCLUSIONS AND FUTURE DEVELOPMENTS

The development of the Safety Monitor signals the beginning of a new phase of PRA applications activities that will directly benefit plant operations and maintenance personnel. The Safety Monitor provides a tool for operations personnel that allows them to easily access the insights of the plant's PRA model. The Monitor will offer operating advice to plant staff in a real-time capacity while collecting valuable configuration history data that will support PRA and Maintenance Rule activities.

The use of a tool such as the Safety Monitor makes it possible to develop risk-based Technical Specifications that would account for unique plant operating conditions and various environmental conditions that might influence the risk of a serious accident or transient. SCE believes that a more risk-based approach to Technical Specifications will allow greater flexibility to perform maintenance while the plant is operating while helping to ensure that overall operating risk is minimized.

The Safety Monitor may also be expanded in the future to address other aspects of plant operation. The Level 2 PRA model may be included to assess the impacts of various maintenance and operational activities upon the likelihood of a radioactive release following an accident. The consideration of such effects will allow evaluation of components such as containment isolation valves, containment pressure control systems and containment radioactivity cleanup systems.

Another area for future development is the incorporation of risk models to address shutdown conditions. The addition of this capability will allow operators and maintenance personnel to plan outage activities in a manner that will minimize risk. These models will also allow plant personnel to compare the risk impacts of performing various maintenance actions at power versus performing them during shutdown conditions (or during different shutdown modes).