NOTICE

CERTAIN DATA CONTAINED IN THIS DOCUMENT MAY BE DIFFICULT TO READ IN MICROFICHE PRODUCTS.

Conf-890634--3

Presented at the EPRI Seminar on "Expert Systems for the Electric Power Industry," Orlando, FL, June 6-8, 1989.

CONF-890634--3

DE91 004518

SAFETY REVIEW ADVISOR

James A. Boshers
University of Tennessee

Israel E. Alguindigue
University of Tennessee

Catherine G. Burnett
Tennessee Valley Authority

Robert E. Uhrig
University of Tennessee

ABSTRACT

The University of Tennessee's Nuclear Engineering department, in cooperation with the Tennessee Valley Authority (TVA), is evaluating the feasibility of utilizing an expert system to aid in 10CFR50.59 evaluations. This paper discusses the history of 10CFR50.59 reviews, and details the development approach used in the construction of a prototype Safety Review Advisor (SRA).

The goals for this expert system prototype are to 1) aid the engineer in the evaluation process by directing his attention to the appropriate critical issues, 2) increase the efficiency, consistency, and thoroughness of the evaluation process, and 3) provide a foundation of appropriate Safety Analysis Report (SAR) references for the reviewer.

---

* Research sponsored by the U.S. Department of Energy

DISCLAIMER

INTRODUCTION AND BACKGROUND

In 1959, the Atomic Energy Commission (AEC), the predecessor to today's Nuclear Regulatory Commission (NRC), issued its first operating license, No. DPR-1, to the Vallecitos Boiling Water Reactor. As issued, the license required that General Electric (GE), the owners and operators, submit for AEC approval, every modification and test or experiment not explicitly approved in the Licensing Documents. These submittals would require AEC approval prior to their implementation. To support the experimental program of the Vallecitos project, GE had to submit several filings a month to the AEC. This arrangement was unacceptable to both the Atomic Energy Commission and General Electric [6].

In 1960, GE asked for, and received a reconsideration of these requirements. GE and the AEC then drafted a new agreement. After formal AEC review, the new agreement was issued as an amendment to DPR-1 on a memorandum and order dated 2 November, 1960. The amendment clearly stated that GE had complete freedom to make changes within the parameters of the technical specifications, provided that no unresolved safety question was involved.

Recognizing the widespread applicability of this approach to regulating changes to licensed facilities, the AEC issued proposed rule 10CFR50.59. The purpose of this new rule was to define the extent to which the licensee could make changes, and perform tests or experiments that were not specifically allowed for in the operating license. Four months after it was proposed, Title 10 of the Code of Federal Regulations part 50 section 59 (10CFR50.59) became effective on August 9, 1962.

Today, all licensed nuclear facilities are subject to 10CFR50.59. This regulation is valuable both to the licensees and to the NRC. For the owners/operators, it allows the freedom to operate and control their facility. The NRC finds the regulation valuable because it maintains the original licensing basis of the facility. Nevertheless, the implementation of this regulation has caused a great deal of confusion, both with the licensees and the NRC [6]. The difficulty comes in the interpretation of the document and the implementation of its requirements.

Specifically, 10CFR50.59 permits the licensee to make changes to the facility or procedures, and to conduct tests or experiments without prior NRC approval provided that the change, test, or experiment meets certain criteria. These criteria are:

1) The proposed activity must not involve a change in the technical specifications and,

2) The proposed activity must not involve an unreviewed safety question.

The first of these two criteria is rather straight forward and redundant since NRC approval is required for all technical specification changes. The difficulty comes in the interpretation of the second. The definition of an "unreviewed safety question" provided by the NRC in 10CFR50.59 is stated as follows:

10CFR50.59 (2)

A proposed change, test, or experiment shall be deemed to involve an unreviewed safety question if;

i) the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the Safety Analysis Report may be increased or,

ii) a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report may be created or,

iii) the margin of safety as defined in the basis for any technical specification is reduced [2].

An engineer attempting to evaluate a proposed modification, test or experiment must first determine several other issues. Questions like

1) What equipment is "important to safety"?

2) What is the Safety Analysis Report?

3) What is meant by "evaluated previously in the safety analysis report"?

4) What is a "margin of safety as defined in the basis for any technical specification"?

must be answered before the engineer may proceed [6]. The answers to these questions will differ depending on the facility and utility to which they are addressed. For example, the SAR is a broad term that can refer to an entire group of documents that were submitted to the NRC for approval. It usually includes the Final Safety Analysis Report (FSAR), the technical specifications, and the basis for the technical specifications, but it can also include design bases and design criteria documents. The SAR also includes all commitments documented in a Safety Evaluation Report (SER). The SER is a document written by the NRC to support the issuance of the operating license and is based on information provided in the SAR.

The determination of whether an unresolved safety question (USQ) is created by a proposed modification is probably the most difficult of all the issues to resolve. The first step is the appropriate application of the criteria. Only those changes and test or experiments that affect the licensing bases of the facility should be subjected to the USQ criteria. Regardless of the safety issues that may be raised by the proposed change, test or experiment, if that activity does not affect the licensing bases of the facility then it cannot be an USQ [6]. The difficulty is in determining if the change, test or experiment being evaluated impacts the scope of the SAR and thus the licensing bases.

A successful application of the 10CFR50.59 criteria to a proposed change, test or experiment requires that the individual performing the review be knowledgeable of the licensing documents associated with the particular facility, as well as the facility and all its safety related systems. This requires an amount of expertise that usually precludes any one individual from being knowledgeable in all areas. Thus in most cases, the engineer performing the review must interface with several other system engineers to properly evaluate the proposed activity.

If a 10CFR50.59 evaluation is done improperly, the results can be very serious. Aside from fines that could be imposed, there is a potential for the creation of a real threat to the safety and health of the public that could go undetected.

A case in point, occurred at the Sequoyah Nuclear Plant. An examination of the plant's design baseline identified a number of essential calculations that had been rendered invalid as a result of plant modifications. While reviews were

performed on the Engineering Change Notices (ECNs) associated with these changes, their potential impact upon certain calculations was not recognized. To prevent recurrence of this condition, a root cause analysis was performed. This analysis concluded that the large number and diversity of the calculations involved preclude any one engineer from being knowledgeable of the content of them all [1]. It was also concluded that, even if someone could be knowledgeable about the content of all calculations, there would still be a considerable variability to how engineering judgment would be exercised in safety reviews performed for similar modifications. This second finding expanded the task of defining corrective action from one of providing better maintenance of the calculations, to the broader purpose of providing a mechanism to help the engineer perform comprehensive and consistent safety reviews.

Analysis of the need in this broader context quickly revealed that possible plant modifications were so very diverse in nature and involved so many possible influences upon safety, that they exceeded the scope of knowledge of any single individual. For years, checklists were used to guide reviewers through their consideration of a proposed modification. Unfortunately, all determining factors cannot be meaningfully represented using a check list.

SOLUTION APPROACH

The nature of safety reviews requires that individuals performing these evaluations be knowledgeable in many areas of engineering. Evaluators must be familiar not only with licensing documents, but also with the facility, and specifically with safety related systems. Clearly, the amount of information to be processed is considerable. Hence, an expert system can significantly assist in the preparation of these reviews.

Expert Systems

An expert system is an application program that attempts to mimic human judgment by applying substantial knowledge of specific areas of expertise to solve finite, well-defined problems. By capturing in computer code the expertise of highly

qualified individuals, problems which reside in the same domain can be solved by repetitively applying the same knowledge.

An expert system typically consists of two components, an inference engine and a knowledge base. The inference engine gathers information, conducts searches, and draws inferences based on the strategy programmed into it. Once conclusions have been secured, recommendations are presented along with explanations on the bases for the conclusions.

The knowledge base of an expert system contains the expertise - collected from experts, books and publications - used in providing advice under a variety of conditions. This expertise describes a methodology for solving a problem as a human expert would solve it. The knowledge is encoded using rules, frames, or other techniques for knowledge representation and is manipulated by the inference engine to provide advice and recommendations.

There are some benefits to be obtained from the use of expert systems. One of the pressing and most significant problems in decision making is the fact that an expert cannot be available at all sites at all times. Expert systems make it possible to deliver expertise to remote locations where experts are not always available. It is also apparent that aside from providing advice, expert systems become repositories for undocumented knowledge which could otherwise be lost through retirement.

Another obvious advantage is that expert systems do not get tired or careless as the work load increases. In the environment of a nuclear power plant, people are sometimes affected by emotions, stress, and other factors which could influence the quality of their work. Expert systems can contribute to the enhancement of plant safety by eliminating some of the uncertainty and guess work from personnel decisions [3]. Expert systems can provide expert advice and rapid access to databases and other vital information.

Expert Systems and Conventional Computer Programs. The basic difference between expert systems and conventional computer programs is that expert systems manipulate knowledge while conventional programs manipulate data [5]. In a

conventional computer language, instructions to be executed are presented sequentially and are highly interconnected. There is an algorithm to be followed, and execution of the program implies a logic flow from one instruction to the next as presented in the code sequence. The expert system style of programming has fundamentally changed the way we give instructions to the computer and how the machine executes those instructions. Instructions are logically connected - not sequentially - and as long as there is a logical link between the input and the conclusions, the inference engine will eventually arrive at a result.

The separation of knowledge and inference techniques in an expert system simplifies greatly the task of updating knowledge bases. Since knowledge is structured independently, it remains distinct and legible and may be deleted, changed or included in a system without extensive logic redesign. In conventional computer programs, in contrast, the knowledge is interwoven with the program logic and structure, and changes are bound to disturb the behavior of the program.

An expert system contains a degree of self-awareness or self-knowledge that allows it to reason about its own operations. This self-knowledge gives an expert system the ability to provide explanations on its decisions and to generate status determination information.

Expert systems also have the ability to manipulate uncertain, or fuzzy data. When the data in the knowledge base is specific and precise, expert systems give results that are unambiguous. However, when information is not precise, incomplete, missing or conflicting, expert systems can still reach a rational conclusion or solution through the use of confidence factors. Under these conditions, an expert system will give the "most probable" solution or the "best" solution, but not necessarily the correct solution [3]. Experts are sometimes forced to make subjective evaluations. Such subjectivity may be easily incorporated into an expert system using confidence factors.

Applications of Expert Systems. The impact of the technology of expert systems has been felt in many areas of science, education, and industry. In the last ten

years, development efforts have resulted in the implementation of a great number of applications now operational, or in the prototype stage. In the nuclear industry, there are many areas in which expert systems could make significant contributions. Expert systems are foreseen as providing promising solutions for problems in personnel training, plant management and safety evaluation.

The ability of expert systems to generate status determination information and to provide explanations on the bases of their conclusions, can be used in the training of personnel [4]. Additional benefits are to be gained from the design and implementation of the system itself, which will force the development and documentation of decision making policies.

In the management and operation of nuclear power plants, expert systems can contribute as expert assistants to the operators, as monitoring and validating systems for sensor data, and as on-line access system for performance and safety data. Obviously, the robustness and completeness of the systems to be developed is of critical concern.

The Safety Review Advisor

The Safety Review Advisor is an expert system to aid in 10CFR50.59 evaluations. In building the SRA, we attempted to emulate the thought process of a reviewer. To accomplish this, the expert system must ask some questions that the engineer would address automatically. For example, the engineer evaluating the proposed activity must first determine whether the activity is a change, or a test or experiment and then apply the appropriate criteria.

Once this distinction has been made, the engineer begins to evaluate the proposed activity in greater detail. If the proposed activity is a change, the engineer must determine whether the change will affect only the facility or will also require a change to a procedure. However, both possibilities must be evaluated since either could require NRC approval prior to implementation.

Figure 1 shows the block diagram of the logic used in our approach to solving the problem. Since our efforts are presently directed towards the construction of a proof of principle prototype, the SRA deals exclusively with changes to the facility. Specifically, the prototype addresses changes directly affecting the Standby Power system of the Sequoyah Nuclear facility. Figure 2 shows the block diagram of the prototype under construction.

A full scale system, as depicted in figure 1, would address changes to both the facility and procedures, as well as the possible effects of proposed tests or experiments. Our choice of which branch to model was based on conversations with TVA personnel. They indicated that the majority of their evaluations, and the ones with the most potential impact on safety, were performed on proposed changes to the facility. The Standby Power system was chosen because it has very few interfaces with other systems. The few number of interfaces allowed for a more rapid development of the prototype.

To evaluate a proposed change to a facility, an engineer must determine which of the safety related system or systems would be directly affected by the change. The engineer must also determine the possible effects the change would have on other systems that interface with it.

Our prototype takes a similar approach. The SRA first determines the system on which the proposed change will be performed. The evaluator selects the appropriate system from a list of plant systems. A full scale version of this system would allow the engineer to choose more than one of the systems listed. Proposed modifications may directly affect several systems. The prototype on the other hand, only allows the selection of the Standby Power system.

The SRA then attempts to narrow the scope of attention by inquiring on the subsystem that the modification will affect. In the Standby Power system there are two major subsystems. These are the Emergency Standby AC Power Supply and the Vital DC Power Supply. The reviewer must then select one of the two. Once the appropriate subsystem is chosen, the SRA must determine which components or sets of components will be affected by the modification. Each inquiry presents a different list of choices based on the reviewer's input.

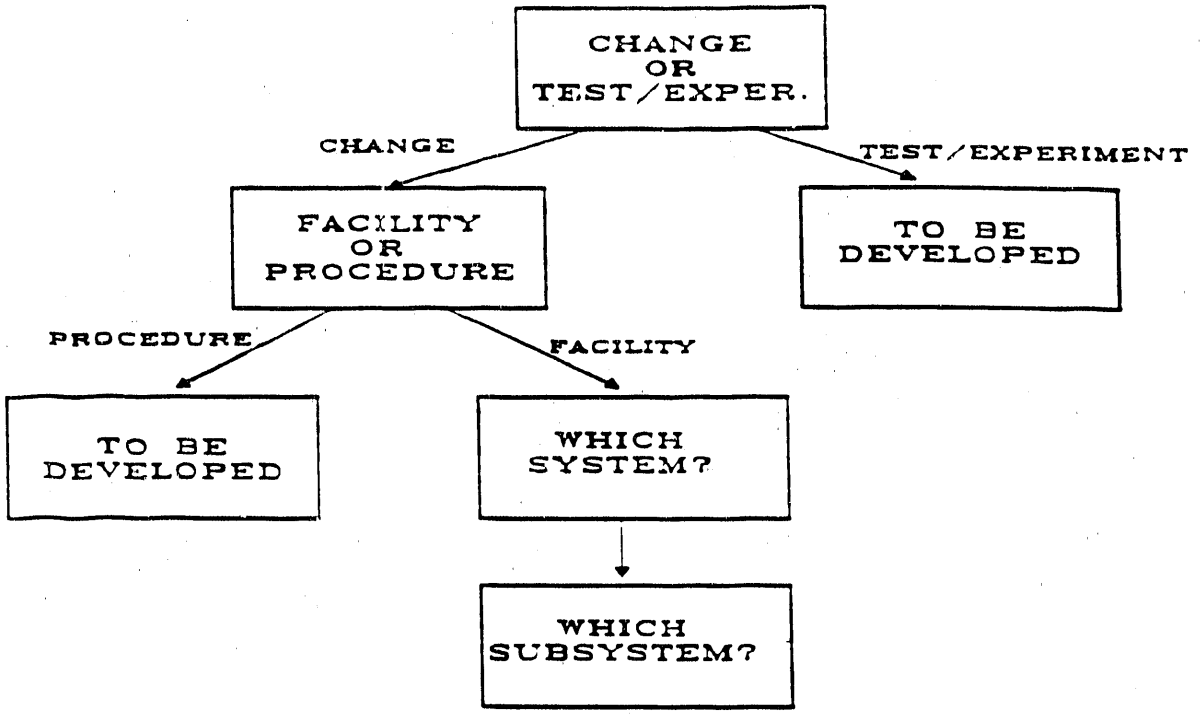

Figure 1. Full-Scale System Block Diagram.

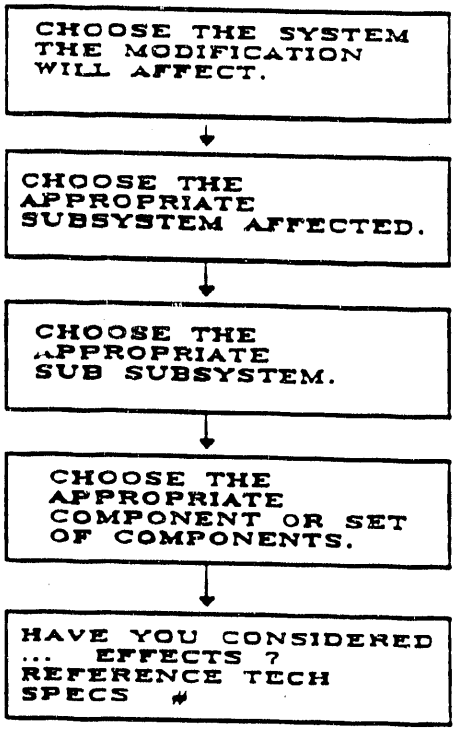

Figure 2. The SRA Block Diagram.

After the prototype sufficiently narrows the focus to a particular component or group of components, the system responds with the appropriate information. This information includes design criteria references, SAR references, and other critical information ("rules of thumb") relevant to the component. For instance, if the reviewer were evaluating the possible modification of the diesel generator's heat exchanger, the prototype would list all the appropriate SAR references that address the heat exchanger. The SRA would provide the appropriate requirements set forth in the design criteria and design basis documents, and it would also provide rules of thumb used by the diesel generator experts in evaluating the performance of the component (such as "only 15% of the tubes in the heat exchanger may be plugged without affecting its heat removal requirements"). The SRA would also make a recommendation regarding the necessity of performing a Safety Evaluation based on the reviewer's response.

Determining if a full scale safety evaluation is required is not the SRA's most important contribution. The biggest benefits are to be drawn from the collection of information presented to the evaluator. This information contains not only the expertise of several experts, but also licensing document references which could be very helpful in the documentation of the review.

TVA, like many other utilities, has designated engineers to perform Safety Evaluations. Easy access to information about each system and their major components, would significantly reduce the research time required to perform the evaluations. It would also help alleviate the concerns about inconsistency in the performance of safety evaluations.

PROJECT STATUS

Development of the SRA began in January 1989 and it is approximately one third complete. The current version of the system was coded in Texas Instruments' PC Plus following a modular design plan. Eventually each module of the SRA will address a different plant system. Interconnections among systems are also included in the design. Once completed, the SRA will be capable of addressing all modifications to Sequoyah's Standby Power system.

The feasibility of incorporating simplified plant system schematics into the prototype is being explored. Development to date has indicated that this capability will be a necessity for implementation of a large scale system.

RECOMMENDATIONS

If the system is to be expanded, it would be advisable to transport the system to a more powerful expert system environment or to code the SRA directly in a programming language. The size of a full-scale system is assured to cause a significant increase in the time required to run a consultation under PC Plus.

One of the major issues of a full sized expert system would be its ability to incorporate CAD drawings of plant systems and schematics. In a large system this capability will be almost mandatory. Comments from TVA personnel who reviewed the system indicate that there is a problem with consistent terminology. What the system engineer calls a 15 gpm pump, the engineer performing the review calls a fuel transfer pump. Both individuals are correct because on two different drawings different names are given to the same pump. Unless CAD drawings are incorporated in a full scale system, this problem will be aggravated.

CONCLUSIONS

The prototype Safety Review Advisor under development will address proposed modifications to the Standby Power system. The prototype is not a cure for all the woes that beset the engineer attempting to evaluate a proposed modification. It cannot address all possible changes, tests or experiments. The best that can be hoped for with the technology at hand is to develop an aid for the engineer to help him perform the evaluations more thoroughly, consistently and efficiently.

If the SRA were to be developed on a full scale, the issue of the engineer's dependency on the system would have to be addressed. The prototype is designed strictly as a tool to assist engineers in performing the evaluations. As with any other tool, the old adage " you need to be smarter than the machine you are trying to operate " still applies. There is concern that such a system would

create complacency in the engineer. An engineer using an expert system must always be aware of the boundaries and limits of such a system. The goal of the system is to direct the reviewer's attention to potential areas of concern, not to perform the evaluation.

REFERENCES

[1] Burnett, Catherine G., "Functional Specifications Safety Review Advisor (SRA)," Tennessee Valley Authority, Division of Nuclear Engineering, Engineering and Computer Methods Branch, Personal Communication.

[2] Title 10, U. S. Government, Code of Federal Regulations, Part 50, Section 59.

[3] Uhrig, Robert E., "Toward the Next Generation of Nuclear Power Plants," Forum for Applied Research and Public Policy, Fall 1986.

[4] Uhrig, Robert E., "Artificial Intelligence and Training of Nuclear Reactor Personnel," Proceedings of the CSNI Specialist Meeting on Training of Nuclear Reactor Personnel, Orlando, Florida, April 21-24, 1987.

[5] Waterman, Donald A., "How do Expert Systems Differ from Conventional Programs," Expert Systems, Vol. 3, No. 1, January 1986.

[6] Williams, Daniel H., "10CFR50.59: Why We Have it - What it Says," Personal Communication.

END

DATE FILMED

12/20/90