Final Report

Department of Energy Award No. DE-FG03-86SF16610

**Joint Application of AI Techniques, PRA and Disturbance Analysis Methodology
to Problems in the Maintenance and Design of Nuclear Power Plants**

David Okrent, Principal Investigator
Mechanical, Aerospace and Nuclear Engineering Department
University of California
Los Angeles, CA 90024-1597

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Final Report

Department of Energy Award No. DE-FG03-86SF16610

**"Joint Application of AI Techniques, PRA and Disturbance
Analysis Methodology to Problems in the Maintenance
and Design of Nuclear Power Plants"**

David Okrent
Principal Investigator

Mechanical, Aerospace and Nuclear Engineering Department
5532 Boelter Hall
University of California
Los Angeles, CA 90024-1597

1 March 1989

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.

MASTER

OKS
DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

TABLE OF CONTENTS

Executive Summary.....	i
1. Introduction.....	i
2. PROLGRAF-B: A Knowledge-Based System for the Automated Construction of Nuclear Plant Diagnostic Models.....	iii
3. A Prototype Knowledge Based System for Preventive Maintenance Optimization.....	ix
4. An Expert System for Finding Fragility Curves of Building Structural Systems at the Preliminary Design Stages.....	xi
5. A Probabilistic-Based Expert System to Optimize the Economics of Spare Parts Inventory Control for a Nuclear Power Plant.....	xiii
6. An Expert System to Estimate Time, Rate and Magnitude of Important Radioactive Isotopes, Given a Loss of Containment Integrity.....	xiv
7. An Operator Response Aid in Severe Earthquakes.....	xvi
 1. INTRODUCTION	 1
2. PROLGRAF-B: A KNOWLEDGE BASED SYSTEM FOR THE AUTOMATED CONSTRUCTION OF NUCLEAR PLANT DIAGNOSTIC MODELS, <i>S.B. Guarro</i>	3
1. Motivation and Objectives of the Research.....	3
2. LFM Feature Summary and Example.....	6
3. User's of LFM and Comparison with AI Expert Systems.....	7
4. Identification of Desirable LFM Extensions.....	10
5. Object Oriented Database Representation of LFM Models.....	18
6. PROLGRAF-B Model-Building Procedures.....	20
6.1. Process and Model Primary Object Identification.....	22
6.2. Causality Flow Identification.....	27
6.3. Causality Transfer Function and Interaction Specification.....	30
6.4. Fault and Causality Conditioning Specification.....	33

7.	PROLGRAF-B Procedural Extensions.....	49
7.1.	Causality-Link Check Procedure.....	50
8.	PROLGRAF-B Prototype Software.....	51
8.1.	Design of the PROLGRAF-B Workstation Interface.....	53
8.2.	PROLGRAF-B Software Prototype Demonstration.....	55
9.	Conclusions and Possible Further Developments of this Research.....	61
	References.....	62
3.	A PROTOTYPE KNOWLEDGE-BASED SYSTEM FOR PREVENTATIVE MAINTENANCE OPTIMIZATION, <i>S. Arueti</i>	64
1.	Background.....	64
2.	Objectives.....	66
3.	Terminology and Some Key Assumptions.....	67
4.	Methodology.....	68
4.1.	Cost Optimization.....	68
4.2.	Bayesian Data Analysis.....	70
4.3.	Knowledge Representation.....	75
5.	Implementation and Results.....	78
6.	Conclusions.....	79
	References.....	79
4.	AN EXPERT SYSTEM FOR FINDING FRAGILITY CURVES OF BUILDING STRUCTURAL SYSTEMS IN THE PRELIMINARY DESIGN STAGE, <i>L.-Y. Lee</i>	81
1.	Introduction.....	81
2.	Background.....	82
3.	An Overview of the Knowledge Base Expert Systems.....	84
4.	Problem Analysis.....	85
5.	Methodology and Assumptions.....	90
6.	Knowledge Acquisition and Representation.....	93
7.	Inference Network and Control Strategy.....	99

8. Discussion.....	104
9 Conclusions.....	107
10. Acknowledgments.....	107
References.....	198
 5. A PROBABILISTIC-BASED EXPERT SYSTEM TO OPTIMIZE THE ECONOMICS OF SPARE PARTS INVENTORY CONTROL FOR A NUCLEAR POWER PLANT, <i>K.-Y. Kim</i>	112
1. Introduction.....	112
2. Methodology.....	113
2.1. Function of Expert System.....	113
2.2. Cost-Effectiveness Calculation.....	119
3. Structure of the Expert System.....	122
References.....	122
 6. AN EXPERT SYSTEM TO ESTIMATE TIME, RATE AND MAGNITUDE OF RELEASE OF IMPORTANT RADIOACTIVE ISOTOPES, GIVEN A LOSS OF CONTAINMENT INTEGRITY, <i>K.-Y. Kim</i>	123
1. Introduction.....	123
2. Instrumentation.....	123
3. Physical Approach to Estimating Release Rate.....	125
3.1. Magnitude of Release.....	125
3.2. Thermodynamic Properties.....	127
3.3. Resuspension.....	127
3.4. Location of Leakage from Containment.....	127
4. Basic Scheme of the Expert System.....	127
4.1. Knowledge Representation and Inference.....	128
5. Summary.....	131
6. Acknowledgements.....	131
References.....	132
 7. AN EXPERT SYSTEM TO ASSIST DIAGNOSIS FOLLOWING SEVERE EARTHQUAKES, <i>S.-H. Lee</i>	133

1. Background.....	133
2. Objective.....	134
3. Approach.....	134
4. PRA/Event Trees.....	135
5. EPG/Functional Restoration Guidelines.....	135
6. Confusions and Remedies - Case Study.....	138
7. Likelihood Estimation.....	140
8. Conclusions and Recommendations.....	140
References.....	140

Appendix A. List of Publications

Appendix B. List of Theses (Completed and In Progress)

Appendix C. List of Software and Manuals Available

EXECUTIVE SUMMARY

1. Introduction

This final report summarizes the accomplishments of a two year research project entitled "Joint Application of Artificial Intelligence Techniques, Probabilistic Risk Analysis, and Disturbance Analysis Methodology to Problems in the Maintenance and Design of Nuclear Power Plants," D. Okrent, Principal Investigator, a project funded by Department of Energy Award No. DE-FG03-86SF-16610. The objective of this project is to develop and apply appropriate combinations of techniques from artificial intelligence (AI), reliability and risk analysis, and disturbance analysis to well-defined programmatic problems of nuclear power plants. Reactor operations issues were added to those of design and maintenance as the project progressed.

While expert systems are likely to play an increasing role in nuclear power, it is becoming clear that AI rule-based or frame-based knowledge structures cannot be considered a universal panacea. This is especially true for complex diagnostic problems in which "heuristic knowledge" is mixed with a deeper physical knowledge. There is likely to be a need for a marriage of techniques, that is, for "model-based" or hybrid expert systems, in which "conventional" algorithms are coupled with AI inference engines.

This project consisted of six primarily pragmatic tasks, each aimed at the development of an expert system, as follows:

1. A knowledge-based system for the automatic construction of nuclear plant diagnostic models (a marriage of AI and the logic flowgraph disturbance analysis methodology);

2. A probabilistic, prototype expert system to aid decision-making on the scheduling of preventive maintenance based on a comparison between expected costs and benefits;
3. A hybrid expert system to estimate the principal seismic failure modes and the seismic fragilities of a building at the preliminary design stage, to enable more balanced design by an engineer with only moderate experience;
4. A probabilistic-based expert system to optimize the economics of spare parts inventory control;
5. An expert system to aid emergency measures off-site, given a core melt accident, by estimating the time, amount, rate, and type of radioactive material release in the event of a loss of containment integrity; and
6. A methodology, and hopefully an expert system, to identify those severe-earthquake-caused, accident scenarios likely to lead to operator confusion and a potential failure of recovery actions as a result of spurious information to the operator.

This research has led to the granting of three Ph.D. degrees and one M.S. degree. One more Ph.D. thesis is in its final stages. A considerable number of conference papers and journal articles are resulting from these efforts.

The results of the research tasks listed above are summarized in the six sections which follow.

2. PROLGRAF-B: A Knowledge-Based System for the Automated Construction of Nuclear Plant Diagnostic Models

The PROLGRAF-B research has been aimed at the development of a computer based model-builder for the semi-automated construction of Logic Flowgraph Methodology (LFM) models of plant and engineering processes.

The complexity of many modern engineering systems, such as nuclear power plants or large spacecraft, requires the development of system models to analyze and monitor their performance. LFM has been under development as a "qualitative process modeling" technique which produces process models that are both closer to the physics of the modeled process and contain more useful information than the well known binary-tree models used in traditional reliability and safety analysis. LFM produces process models in a digraph-network form; an associated "inference engine" implemented in the form of computer software, is then capable of automatically analyzing the LFM process-model and deriving from it either of the following:

- fault trees for any "top event" that could be of interest in terms of analyzing off-line the expected reliability performance of the process; standard fault-tree analysis codes can then be used to identify the basic combinations of faults (called "cut-sets" in fault-tree specialists' language) which can produce that top event;
- success trees for any process subfunction of interest (also for off-line analysis);
- diagnostic mini-trees for the identification of the root-causes of operational problems in the given process; this analysis can be executed on-line and in "real time" if instrumentation readings can be directly fed into the

LFM inference engine; these readings are used to confirm which of the events and parameter excursions that may potentially occur within the process are actually been observed by the instrumentation and should be reflected in the LFM-executed diagnosis. The LFM-deduced diagnostic mini-tree can then easily be translated into natural language diagnostic messages to be displayed to the process operators;

- recovery mini-trees which, after a diagnostic analysis has identified the root causes for an undesired process state, identify possible counteractions to neutralize the effects of these and bring the process back under acceptable conditions; recovery mini-trees can also be straightforwardly translated into natural language messages to be displayed to process operators.

The PROLGRAF-B development project pursues the goal of making the LFM technique accessible to non-specialists, for applications to practical process design and operations problems. This general goal translates into the more specific objective of deriving an "intelligent LFM model builder", that is, a procedure (implemented in a software package) which contains knowledge concerning the desired syntactical and semantic form of a *generic* LFM model and which uses this generic knowledge to guide the steps of a user through the process of building a valid and robust LFM model of a *specific* given process of interest.

In the first part of the PROLGRAF-B research we have defined a set of procedures for the definition of a substantially complete version of the LFM model for a given system and have applied these procedures to a simple test case (manually first, and then in a prototype version of the PROLGRAF-B software). The steps corresponding to these procedures are summarized below:

1. identify basic devices and components (e.g., pumps, valves, heat exchangers, etc.) in the piping and instrumentation diagram (P&ID) of the process to be modeled;
2. identify device and component "connectors" (e.g., pipes, wires, pneumatic lines, etc.) in P&ID;
3. identify essential parameters characterizing the functionality of each component (e.g., pressure, flowrate, temperature, etc.);
4. recognize and identify direct cause and effect relations among parameters within each P&ID-represented component;
5. recognize and identify direct cause and effect relations among parameters across separate P&ID-represented components;
6. recognize and identify multiple interactions among "input" parameters which determine the state of "output" parameters (process feedback and feedforward effects can be treated as subcases of such interactions).

The second part of the research called for the development of a framework and of specific PROLOGRAF-B procedures for the modeling of process faults and their inclusion in the LFM process model; it was anticipated that this may require modifications and functional improvements of the LFM modeling schemas to achieve the most natural fault representation, on top of which efficient model building procedures could be derived and implemented; due to budget and schedule constraints this activity had not been planned to proceed beyond the procedure-definition stage into an actual prototype software-development stage.

In the original LFM modeling environment, faults were expressed either as events conditioning and modifying a cause-and-effect relation in a particular

abnormal fashion, or as basic binary events representable as LFM "binary variable nodes" (BVNs) (not unlike "binary events" in fault-trees, or "component blocks" in reliability block diagrams). As part of our effort aimed at identifying orderly procedures for LFM model construction, we have refined this fault representation framework into a classification which includes:

Internal Parameter State Change Faults (IPSCF), i.e. device/component internal faults which can manifest themselves as undesired spontaneous changes of state of a process parameter or variable;

Internal Relation Change Faults (IRCF): i.e. device/component internal faults which manifest themselves as changes in the cause-and-effect relation between two or more process parameters or variables;

External Relation Change Faults (ERCF): i.e. process faults which manifest themselves as either a failure by a process component to maintain its state in the range "requested" by the normal cause-and-effect relationship(s) linking its characterizing parameters to parameters in other components, or a failure by that component to respond as intended by design to an external command (that is a command or input proceeding from a parameter in another component) which requires a change of state in one or more of its characterizing parameters.

The above classification responds to the desire of reflecting two types of distinctions among faults: the first being the one between undesired changes of state and undesired changes of state correspondences (i.e., cause and effect relationships), the second being the one between faults internal to individual components and fault affecting more than one component as a block.

The three classes of faults identified above are represented differently in the LFM environment. More specifically, IPSCFs are represented as basic binary

events forcing a specific state in the directly affected LFM variable, whereas IRCFs and ERCFs correspond to conditions affecting the relations of cause-and-effect between LFM variables. These latter types of fault are represented in LFM by mapping the basic binary events or the off-normal states of multi-valued LFM variables representing the condition themselves to changes in the expressions of the transfer functions representing the cause-and-effect relations among LFM variables.

The reality of fault identification and representation in an engineering system or process is that there exists no substitute for the analyst's experience in such a task, except of course for the capability offered by the use of computer databases to store reference lists of faults that have been observed in the past as being typically associated with the operational behavior of certain process components. The analyst will, however, still be called to judge on the applicability of each item on such generic lists to the specific component and situation which is being modeled. The fundamental procedural steps that the PROLOGRAF-B model builder will execute offer the advantage of uniformity and systematic rigor in the execution of the fault representation phase of the LFM model building over the less formal "manual" approach which was used in the past. These identified procedures can be summarized as follows:

1. From a database of known P&ID component types, call up and complete pre-compiled lists of basic "within-component" fault-generating events (e.g., for a pump: rotor freeze, seal leak, housing perforation, etc.);
2. Divide the basic fault-generating events identified per Step 1 into the three basic categories: IPSCF basic events, IRCF conditions, ERCF conditions;

3. Identify ERCF conditions which may result from identified component connector fault-generating events (by definition these should not produce IPSCFs nor IRCFs);
4. Systematically examine all the cause-and-effect relationships expressed in the LFM model and identify which changes in these relationships appear to be possible in correspondence of specific process events;
5. Identify and represent as cause-and-effect conditioning events all the events that may produce the cause-and-effect relationship changes identified per Step 4.

The execution of steps summarized above concludes the PROLGRAF-B model-building and fault-representation procedures.

The results that have been achieved show that a full process analysis package, composed of a PROLGRAF-B-like model-builder and of an LFM model-analyzer like the one already demonstrated during previous research at UCLA, can be practically designed and developed, for the benefit of both engineering analysts charged with the off-line execution of process reliability and optimization studies and of process operators responsible for on-line process diagnosis and management. Based on the experience gained in our research, we believe that the development of a software package of "production level quality" (i.e., having satisfactory features of versatility and robustness) should become possible with a reasonable level of effort. This remains conditional upon the anticipated availability of more flexible computer programming shells and software development environments at the inexpensive end of the spectrum of PC and Engineering Workstation application development tools. Specifically, it would be very useful to have available "object oriented" programming tools designed to

facilitate an intensive and effortless link-up between databases, graphic representations and definition of procedures and programming steps, as well as an easy, interactive switching among these separate but related dimensions of the programming environment.

3. A Prototype Knowledge Based System for Preventive Maintenance Optimization

The objective of this study was to design and build a prototype knowledge-based system for demonstrating preventive maintenance (PM) scheduling. The PM schedule is optimized based on probabilistic inferences, with some deterministic input imposed as constraints. Using probabilistic data on failure rates, repair times, repair costs and indirect economic costs, and within the imposed deterministic constraints, the program develops an optimum (minimum expected) cost maintenance schedule for the various pieces of equipment described by the model. The resultant schedule is stored separately as a slot value in the unit representing each component, subsystem or system, and can be accessed independently for each equipment.

The prototype knowledge-based system, the "Maintenance Advisor" is a frame-based, object-oriented program. Equipment and other objects are represented as complex units, each of which contains in its own frame a complete set of characteristics (e.g. function, driver, operating environment), data (e.g., failure rate, repair time and cost, etc.) and functional capabilities (e.g. update and plot distributions). These are all represented as unit-slots.

The main decision rules are based on probabilistic data. These data as developed by using the "Advisor"'s Bayesian data analysis tools, and are stored in the appropriate slots of each equipment's unit in the form of prior and

posterior distributions. The program contains the basic tools for creating prior distributions, updating and plotting them.

The program also has the capability of using generic distributions as prior distributions, by utilizing the TYPE-OF hierarchical structure, a specialization and generalization of the data analysis methodology and probabilistic inheritance role. The underlying principle of this method is that each component type can be described as a special case of a more general superclass. The distributions of the generic classes, or their combination, can be used as a prior distribution which is updated by subclass specific data. The user is free to use any combination of parent (generic) distributions and a locally created distribution as the prior distribution of a component.

The "Maintenance-Advisor" was constructed with the Kee shell, utilizing additional Lisp functions. The inherent KEE frame and object-oriented programming orientations are broadly used in the program, but in many cases they have been found insufficient for our purposes, mainly because the use of distributions for data analysis and the need for specific logical relations in the form of logic block diagrams. Several generalizations and specific developments have been accomplished for that purpose, two of which are:

1. a "probabilistic inheritance" wherein the basic parent-child inheritance relations have been generalized such that a child-unit can inherit a combination of probability distributions from all its parent-units and from a local value. The simple "Override-Values" inheritance-role becomes a special case of the "Probabilistic Inheritance" role. This role can be further generalized by making it bi-directional, such that information from all child units will be available for developing the prior distribution of a parent unit; and

2. an additional propagation network, which has been developed for inheritance of knowledge along the PART-OF hierarchy. Its application is similar to that of the regular inheritance roles in the TYPE-OF hierarchy, except that it used the block diagrams as a means for combining information to be inherited along the PART-OF hierarchy.
4. **An Expert System for Finding Fragility Curves of Building Structural Systems at the Preliminary Design Stage**

Seismic fragility is one of the most important factors for identifying the safety of civil structures, especially structures in the nuclear power plant industry. Not only is seismic fragility required for probabilistic risk assessment investigations, but also it may have an impact on the design, because parts of the constructed structure found to have inadequate seismic capacity may be very difficult to modify. Seismic fragility is therefore one of the key constraints in the structural design process. In the past decade, a number of probabilistic risk assessment studies have been conducted, however, the seismic fragility function had not been considered in designing the building structural system, especially during the preliminary design stage.

This research is a starting point for the development of an expert system for determining seismic fragility curves of structural systems in a nuclear power plant or conventional building at the preliminary design stage. The resulting system should assist an engineer with moderate engineering background and limited reliability knowledge to analyze the failure functions of building structures. It simulates the performance of human experts in identifying the potential failure modes and their variabilities for a structure of interest. Then, by combining the stress results of crude analyses, the method of linear

statistical modelling, the current conceptions of seismic fragility evaluation and damage evaluation, and the intuition and experience of human experts, the seismic fragility functions of the structure are estimated.

The induction technique is used for knowledge acquisition. Thus, the characteristics of structural system performance during earthquake excitations are described by attributes and their values. The rules for the selection of the components for seismic fragility evaluations may be deduced from the results of expert diagnosis of a pattern space configured from the attributes. Because the set of attributes and their values is generally incomplete, the deduced results often contain uncertainties and imprecisions. Also, the local responses estimated by crude analyses, approximations of analytical modelling, empirical formulas and tricks result in the other sources of uncertainties.

A procedure to combine the implementation techniques of a knowledge base expert system and traditional programming has been developed in order to build an expert system for solving a semi-ill-formed problem like seismic fragility evaluation of building structural systems in the preliminary design stage. Based on this implementation technique, the major sequential order associated with the reduced subproblem have been written in terms of a knowledge-based expert system. This design strategy decomposes a complicated problem into a series of simpler subproblems, fires the associated rule sets, fact bases, empirical formulas and tricks to solve the subproblems, and combines the results of these subproblems to estimate the solution. In this way the domain of search space and the required computer time is significantly reduced.

The prototype expert system can estimate the seismic fragility functions of steel structures, reinforced concrete structures and combinations thereof. Both

nuclear power plant structures and conventional buildings have been considered; however, some special types of structural systems, such as the containment structure, coolant-tower structure, water tank, high-rise building, and underground structure of the embedded part of a building system are not included. However, it should be possible to extend the system to cover these special types of structures based on the techniques developed by this research.

Knowledge related to the material properties, the ratio of actual strength to theoretical value, the levels of damping appropriate for structures close to collapse, the inelastic effects (by using ductility modified response spectrum techniques), the radiation of energy from the structure into soil and the sources of both inherent randomness and uncertainties which result from a lack of knowledge, approximations in analytical modelling, empirical formulas and tricks, were considered in developing this expert system. About 220 functions and 400 rules have been implemented in the system.

5. A Probabilistic-Based Expert system to Optimize the Economics of Spare Parts Inventory Control for a Nuclear Power Plant

Spare parts inventory control is an important and complicated problem for nuclear power plants. It is not easy to decide which parts to stock and in what quantity. Excess inventory means a waste of money and warehouse storage, while a lack of spare parts can lead to expensive power replacement costs (say \$500,000 per day).

The maintenance manager has an important impact on the spare parts inventory. However, even if the maintenance manager is an expert on ways to manage the spare parts inventory, he will need a great deal of information concerning the parts and components, as well as good guidelines for this complicated problem.

To help initiate a quantitative approach to the optimization of spare parts inventory control, a prototype expert system was built using the *Intelligence Compiler* shell on an IBM PC/AT. The code distinguishes among corrective maintenance (CM), preventive maintenance (PM) and predictive maintenance (PM). The code performs a cost-effectiveness calculation for the optimal stocking level of each component which is queued. It also gains a measure of optimal stocking level as determined by the user's experience and judgment and the vendor recommendations.

The cost-effectiveness calculation balances the costs of purchasing stocking the spare parts against the cost of increased down-time and of increased risk, if operation continues with a component unavailable. The component failure rates are established generically, and then are updated with plant experience, including allowance for increased failure rates near end of life. The SARA code is used to evaluate the increment in risk associated with component unavailability. The code allows for lead time to acquire spare parts and any fractional reduction in power resulting from spare part unavailability.

6. An Expert System to Estimate Time, Rate and Magnitude of Release of Important Radioactive Isotopes, Given a Loss of Containment Integrity

In the unlikely event that an accident involving large scale core melt occurred in a light-water-cooled, nuclear power reactor, various preparations have been made to gather information to help guide any offsite evacuation steps, should they be necessary. These include measurement of radioactivity exterior to the reactor plant as well as a group of measurements inside the containment. However, the existing measurement capability is inadequate to give quantitative information on the rate of escape of radioactive material, isotope by isotope,

should a significant loss of containment integrity occur. Such information, together with continuing meteorological data, could place evacuation or sheltering measures on a much more certain foundation than is possible with the radioactivity measurements now provided.

This study is intended to explore the practicality of devising a simple expert system, which, together with the relevant instrumentation, could provide detailed information on rate of escape of radioactive isotopes from containment, at least approximately. A pressurized water reactor (PWR) with a large dry containment is used as the model for study.

Basic to the method is the anticipated availability of instruments to measure concentration of significant individual radioisotopes in containment about once a minute. The escape of radioisotopes is assumed to be proportional to that of non-condensable gases, which are monitored and/or predicted in part.

The expert system assumes the availability of the following parameters on an essentially continuous basis (all triply redundant):

- containment atmospheric temperature (five locations)
- containment pressure (five locations)
- containment sump level
- water level about containment floor
- refueling water storage tank level
- containment sump temperature
- hydrogen concentration
- carbon dioxide concentration
- radioisotope concentrations

It is assumed that the fission products in the containment atmosphere at any time are well mixed with the nitrogen and oxygen gas (and hydrogen and carbon dioxide, if any) and the steam, which, prior to occurrence of a loss of containment integrity, is ordinarily saturated and in equilibrium with the water in the sump or on the containment floor.

The leakage rate determination involves the calculation of gas loss during the leakage period by direct observation of containment pressure and temperature. The steam pressure is assumed to continue to correspond to saturation at sump water temperature.

The prototype expert system is implemented with KEE on a Symbolics LISP machine. The expert system is named *RELEASE*.

If temperature or pressure inside containment suddenly changes, the inference process of the expert system starts to check whether containment has failed or not. If it has failed, the expert system shows the released amount of radionuclides during each time interval (and the rate of release) and the leak location.

The system differentiates between pressure drop due to containment spray or due to a loss of containment integrity. It also includes analytic and auctioneering methods for validation.

7. On Operator Response Aid in Severe Earthquakes

Recent PRA studies indicate that potential accidents initiated by large earthquakes are among the major contributors to public risk. During a severe earthquake, any component, system or structure may fail; the plant may be driven

into a very complex situation in which instrumentation and control systems may also fail and provide operators with unreliable information about the processing parameters crucial to plant safety. Symptom-oriented procedures depend on indicators, and faulty indicators may cause the operator not to act in time, or incorrectly.

The objective of the present study is to improve the operator capability of responding to seismic damage through the use of EPGs (emergency procedure guidelines). The fact that the symptoms presented to operators may be unreliable in the case of severe earthquakes endangers the validity of actions in EPGs. It is the purpose of this study to deterministically identify possible weakness of EPGs given a severe earthquake as well as to probabilistically evaluate those identified weaknesses. It is expected the study results will provide valuable information for further studies on plant safety during severe earthquakes, e.g., the development of an expert system, the refinement of symptom-oriented guidelines, etc.

Three major steps are taken in this study, they are:

Step I: Review PRA reports to identify critical operator action sets (COAS) which contains those operator actions whose combined failure will lead the reactor to a core melt condition.

Step II: Identify possible confusions given some postulated structural, systems or component (SSC) or instrumentation and control (I&C) the identified critical operator action set when it is performed according to the instructions in the EPGs, and discuss possible remedies for identified confusions.

Step III: Estimate the likelihood of those postulated SSC or I&C failure.

Review and simplification of event trees in an existing PRA report yields 47 safe sequences and 169 core melt sequences, some of which may contain COAS and provide the basis for our case study.

Review of the 47 identified safe sequences reveals that they do prevent the reactor core from melting by protecting the first four critical safety functions: maintenance of subcriticality, maintenance of core cooling, maintenance of heat sink, and maintenance of reactor coolant system integrity. Review of the 169 identified core melt sequences reveals that any of them fails at least one of the four functions. Based on the review results, it was found that the COAS is contained in the following four Function Restoration Guidelines:

- FR-S.1: Response to Nuclear Power Generation - ATWS
- FR-C.1: Response to Inadequate Core Cooling
- FR-H.1: Response to Loss of Secondary Heat Sink
- FR-P.1: Response to Imminent Pressurized Thermal Shock Condition

Several cases were examined and possible remedies for identified confusions discussed. For instance, the failure of the refueling water storage tank level indicator in a COCA may prevent the operator from performing the sump recirculation mode in time, allowing the pumps to get damaged due to running without water and to fail to perform the recirculation mode later. If this occurs, core melt should result because there is no water to cool the core in the long term. A possible remedy for this case is that the sump level (or floor level) indicator is used to verify the RWST level indicator, that is if the building has a high enough water level, the operator may go to the recirculation mode without waiting until RWST low low level alarm sounds (or at least the operator is given a specific warning).

As another instance, the failure of the normal charging path may prevent the operator from performing other rapid boration means, which are required for the ATWS situations. Given an ATWS, the operator is guided to perform high pressure injection due to the high temperature in the core. Any of the found high pressure injection paths may achieve the cooling purpose in the guideline. If the seismic class injection charging path is used, the reactor get cooling and go subcritical. However, if non-seismic-class, high head safety injection path is used and it has failed, the ATWS situation remains an core melt may occur if the operator does not recognize the problem in time. A possible remedy for this case is that the required core cooling paths for ATWS situations should be the safety injection charging paths, with the high head safety injection path as a supplement.

The likelihood of seismic-induced failure of a given set of SSCs or I&Cs, will be estimated for an illustrative hazard curve. The conditional risk of combinations of failures lead to operation confusion, given an earthquake, will also be estimated.

1. INTRODUCTION

This is the final report for a two year research project entitled "Joint Application of Artificial Intelligence Techniques, Probabilistic Risk Analysis, and Disturbance Analysis Methodology to Problems in the Maintenance and Design of Nuclear Power Plants," D. Okrent, Principal Investigator, a project funded by Department of Energy Award No. DE-FG03-86SF-16610. The objective of this project is to develop and apply appropriate combinations of techniques from artificial intelligence (AI), reliability and risk analysis, and disturbance analysis to well-defined programmatic problems of nuclear power plants. Reactor operations issues were added to those of design and maintenance as the project progressed. The first annual report for the project was issued in December 1987 as Report UCLA-ENG-8745 [1].

While expert systems are likely to play an increasing role in nuclear power, it is becoming clear that AI rule-based or frame-based knowledge structures cannot be considered a universal panacea. This is especially true for complex diagnostic problems in which "heuristic knowledge" is mixed with a deeper physical knowledge. There is likely to be a need for a marriage of techniques, that is, for "model-based" or hybrid expert systems, in which "conventional" algorithms are coupled with AI inference engines.

This project consisted of six primarily pragmatic tasks, each aimed at the development of an expert system, as follows:

1. A knowledge-based system for the automatic construction of nuclear plant diagnostic models (a marriage of AI and the logic flowgraph disturbance analysis methodology);

2. A probabilistic, prototype expert system to aid decision-making on the scheduling of preventive maintenance based on a comparison between expected costs and benefits;
3. A hybrid expert system to estimate the principal seismic failure modes and the seismic fragilities of a building at the preliminary design stage, to enable more balanced design by an engineer with only moderate experience;
4. A probabilistic-based expert system to optimize the economics of spare parts inventory control;
5. An expert system to aid emergency measures off-site, given a core melt accident, by estimating the time, amount, rate, and type of radioactive material release in the event of a loss of containment integrity; and
6. A methodology, and hopefully an expert system, to identify those severe-earthquake-caused, accident scenarios likely to lead to operator confusion and a potential failure of recovery actions as a result of spurious information to the operator.

This research has lead to the completion of three Ph.D. theses and one M.S. thesis. One more Ph.D. thesis is in its final stages. The three Ph.D. theses have been published as reports, UCLA-ENG-8942, 8943, and 8944 [2-4]. A considerable number of conference papers and journal articles have resulted from these efforts. They are listed in Appendix A.

The results of the research tasks listed above are summarized in the following six sections of this report.

2. PROLGRAF-B: A KNOWLEDGE-BASED SYSTEM FOR THE AUTOMATED CONSTRUCTION OF NUCLEAR PLANT DIAGNOSTIC MODELS

Sergio B. Guarro

1. Motivation and Objectives of the Research

The PROGRAF-B research is focused on the development of a computer-based model-builder for the semi-automated construction of Logic Flowgraph Methodology (LFM) models of plant and engineering processes. In the progress report [1] for the period September 1987 - March 1988 of this project we have discussed at some length the motivations for conceiving and executing this research. We repeat here the essence of that discussion as it provides some useful background information to the reader. The early results of this research have also been documented in the first annual project progress report and in several publications (please see the list of PROLGRAF-B project related publications provided at the end of this section).

The complexity of many modern engineering systems, such as nuclear power plants or large spacecraft, requires the development of system models to analyze and monitor their performance. Automated diagnosis of undesired operational transients in a nuclear power plant process has been an active subject of research for the last ten years. Examples of different approaches to the solution of this problem are the early research on Disturbance Analysis Systems (DASs) and the more recent developments in the area of Automated Emergency Operating Procedures (AEOPs).

The early efforts in the field of automated plant process analysis were hindered by the scarcity of efficient modeling tools suited for self-contained representation of typical target processes. For example, the "cause-consequence

tree" methodology used in the DAS prototypes produced "event-oriented" models [2]. This type of representation required a separate model development effort for each individual event sequence for which a diagnostic capability was desired. The resulting models often lacked flexibility, in that even relatively small deviations of an actual occurrence from a modeled event sequence could compromise the capability by the model and the associated diagnostic software to match and recognize the sequence. The outcome of this scarcity of appropriate tools was a reduction of research efforts in this area, and a re-direction of research by major organizations, like the Electric Power Research Institute, towards the development of computer based models for a "symptomatic", rather than diagnosis-based, treatment of plant operational transients [3].

A discrete modeling approach, called the Logic Flowgraph Methodology (LFM) and designed to overcome some of these difficulties, has been developed and tested at the University of California, Los Angeles [4-6]. This approach is neither "event-" nor "symptom-oriented", but can rather be defined as "process-oriented". LFM has been under development as a "qualitative process modeling" technique which produces process models that are both closer to the physics of the modeled process and contain more useful information than the well known binary tree models used in traditional reliability and safety analysis. LFM produces process models in a digraph-network form; an associated "inference engine" implemented in the form of computer software is then capable of automatically analyzing the LFM process-model and deriving from it any of the following:

- fault trees for any "top event" that could be of interest in terms of analyzing off-line the expected reliability performance of the process;
- success trees for any process subfunction of interest (also for off-line analysis);

- diagnostic mini-trees for the identification of the root-causes of operational problems in the given process; this analysis can be executed on-line and in "real-time", if instrumentation readings can be directly fed into the LFM inference engine to confirm which of the events and parameter excursions that are allowed within the set of physical constraints reflected in the LFM model are actually observed by the instrumentation, and should be accounted for in the LFM-executed diagnosis; the ultimately deduced diagnostic mini-tree can also be translated into natural language diagnostic messages in a straightforward way;
- recovery mini-trees which, after a diagnostic analysis has identified the root causes for an undesired process state, identify possible counteractions to neutralize the effects of these and bring the process back under acceptable conditions; recovery mini-trees can also be straightforwardly translated into natural language messages to be displaced to process operators.

In essence, then, the LFM models can be used in conjunction with the LFM "inference engine" to perform automated reliability analysis of a plant process [4,5], or to derive in real time both process diagnostic and process recovery recommendations for plant operators [4-6].

The essential features of the LFM discrete simulation environment are described in Section 2. With the description of the environment as background, the discussion then focuses in the following sections on the PROLGRAF-B (PROcess Logic flowGRAPH Builder) "intelligent interface" program which has been the specific subject of the research activities carried out in this project. The PROLGRAF-B development project goal has been that of making the LFM technique accessible to non-specialists, for applications to practical process design and

operations problems. This general goal has been pursued by seeking the definition and prototype demonstration of an "intelligent LFM model builder," that is, a software package which contains knowledge concerning the desired syntactical and semantic form of a *generic* LFM model and which uses this generic knowledge to guide the steps of a user through the process of building a valid and robust LFM model of a *specific* given process of interest. The LFM model produced by the PROLGRAF-B model builder for a given plant or process is contained in an "intelligent database" output structure containing and representing all the LFM "objects" necessary to describe the modeled process.

2. LFM Feature Summary and Example

The Logic Flowgraph Methodology (LFM) was developed as a means of constructing computer implementable models of complex plant processes, such as those taking place in nuclear power or chemical plants. The LFM models take the form of directed graphs, with relations of causality and conditional switching actions represented respectively by "causality edges" and "conditional edges" that connect network nodes and special operators. Of these, the first represent important process variables and parameters, and the latter represent the different types of possible causal or sequential interactions among them.

The specific usefulness of LFM as a discrete simulation tool derives from its direct and intuitive applicability to the modeling of causality driven processes, and from the capabilities offered by the LFM computer-based "inference engine". This was developed as an integral part of the methodology, and allows a user to analyze the synthetic LFM models on-line, e.g. for the direct real-time monitoring and automatic diagnosis of a process, or off-line, e.g. for the construction of reliability or risk models.

The reader interested in the details and the applications of the LFM simulation framework will find detailed explanations and discussions in [4-6]. For the purpose of illustrating some of the fundamental concepts and modeling "primitives", or "objects" used in LFM we can refer to the simple LFM graph depicted in Figure 2.1. The graph shows that between variable 1 (V1) and variable 2 (V2) there normally exists a causal relation of direct proportionality in terms of possible deviations from rated steady-state values. This is indicated by the "default" (i.e., shown as unconditioned) +1 gain value in the directed "multiple gain box" (MGB) between V1 and V2. However, when a condition of moderate positive variation from steady-state occurs for variable 3, that is, $V3 = +1$, the causal link between V1 and V2 is no longer valid, as shown by the 0 gain value that is pointed at in the same MGB by the "true" outcome of the condition test "is $V3 = +1$?". This test is in turn represented by the diamond box ("test box" or TB in the LFM denomination conventions) along the conditional edge from V3 to the gain box.

Figure 2.1: Example of LFM Model

3. Uses of LFM and Comparison with AI Expert Systems

As explained above, the computer executable interpretation of the LFM models makes them especially well suited for the analysis of complex processes and the

diagnosis of unexpected situations that may occur in such processes. The LFM inference engine is capable of automatically developing from the LFM graph models, without help from the user, complete logic tree analyses of a condition occurring in the modeled process. The only input needed by the LFM inference engine is the specification of a "top event", i.e. the event for which an analysis or explanation is required. If any other conditions and events existing in the process are observable (i.e., can be detected), they can also be fed as input to the inference engine. The analytical procedure will use these recorded observations to appropriately restrict the "search space" in the search for the "root cause" events and conditions that can be logically deduced as the ones determining the event. To work with a simple example of these concepts we can refer again to Fig. 2.1. If we ask the LFM code to determine for what conditions we can have the top event "V2 = 0" (meaning that the variable is at its unperturbed steady-state) and we do not provide any further information, the code will give us back the following answer:

"V1 = 0" .or. ("V1 = <any value>" .and. "V3 = +1")

However, if we have observed that V3 has not changed from its steady state value (i.e., V3 = 0) and we provide this information to the analytical inference engine, or if the code itself receives direct input to that effect from a sensor measuring the variable V3, then the deduced root event will simply be:

"V1 = 0"

The LFM models and software perform functions analogous to those typically expected from diagnostic "expert systems" developed in the AI (artificial intelligence) domain, but are also suited for the off-line development of full fault and success trees for system reliability and risk analysis applications.

With respect to most expert system "shells" and frameworks LFM presents some notable differences. The LFM representation paradigm is based on synthetic graphic models which contain in *implicit* form a combination of "semantic networks" and "if-then rule" knowledge representations, whereas most expert systems utilize plainly stated "IF-THEN" rules which are analytic in nature, and usually expressed by means of verbal statements. To provide an example of this, we must explain first that in the LFM models any continuous variation range of a variable or parameter is discretized as follows:

<parameter value> = +10	for large positive variations,
<parameter value> = +1	for small positive variations,
<parameter value> = 0	for the unperturbed steady state,
<parameter value> = -1	for small negative variations,
<parameter value> = -10	for large negative variations,

Thus, it can be easily seen that the fully explicit IF-THEN equivalent of the simple LFM model in Fig. 2.1 can be given by the following statement list:

- 1) "IF V1 IS AT STEADY STATE THEN V2 IS AT STEADY STATE"
- 2) "IF V1 IS NOT AT STEADY STATE AND V3 HAS A SMALL POSITIVE VARIATION THEN V2 IS AT STEADY STATE"
- 3) "IF V1 HAS A SMALL POSITIVE VARIATION AND V3 DOES NOT HAVE A SMALL POSITIVE VARIATION THEN V2 HAS A SMALL POSITIVE VARIATION"
- 4) IF V1 HAS A SMALL NEGATIVE VARIATION AND V3 DOES NOT HAVE A SMALL POSITIVE VARIATION THEN V2 HAS A SMALL NEGATIVE VARIATION"

- 5) "IF V1 HAS A LARGE POSITIVE VARIATION AND V3 DOES NOT HAVE SMALL POSITIVE VARIATION THEN V2 HAS A LARGE POSITIVE VARIATION"
- 6) "IF V1 HAS A LARGE NEGATIVE VARIATION AND V3 DOES NOT HAVE A SMALL POSITIVE VARIATION THEN V2 HAS A LARGE NEGATIVE VARIATION"

Another important feature of the LFM software is its ability to automatically handle feedback and feedforward loops. This feature allows the construction of logic trees that have already been checked and adapted to satisfy all the logic consistency rules that must be obeyed in the presence of process loops.

It should also be noted that, unlike many AI expert systems, which are developed from "heuristic" or empirical knowledge of the application domain, LFM is best suited for the modeling of a given process based on knowledge that, although qualitatively expressed, is "deep", that is, rooted in the "cause - effect" reasoning principle.

4. Identification of Desirable LFM Extensions

The LFM modelling scheme, i.e. the "grammar" and "syntax" rules providing the general modeling environment and structure within which the LFM models of a given physical process can be derived were originally developed to provide a combination of modeling potential and relative simplicity for the representation of certain classes of object processes, such as nuclear plant and other thermal-hydraulic plant processes. Since the primary objective of this research is to define procedures and rules to be implemented in interactive software to allow a

semi-automatic construction of LFM models, it was found useful to examine whether any modifications to the syntactic structure of these models may be beneficial. An identification of useful improvements in the LFM modeling environment can at this stage be directly reflected in the definition of PROLGRAF-B, avoiding later changes and retrofits, which would probably be more difficult to implement. A brief investigation in this direction, supported by the experience gained through the use of LFM in several specific applications, allowed us to conclude that certain extensions of the LFM modelling environment are desirable to ensure greater flexibility and to facilitate its application to a broader range of "target" processes. The desirable extensions that we have been able to identify are mostly meant to offer the LFM user the capability of a more generalized and flexible framework for the definition and correlation of parameter and variable state definitions, replacing the fixed scheme based on two binary and five "continuous-discretized" states originally used in LFM. The details of the added modelling features are discussed below.

The LFM syntax, as described in [4] and [5], allows the analyst to represent the propagation of causality and the correspondence of linked parameter states by means of "multiple gain boxes" (MGBs). These LFM model constituents show what relations (e.g.: direct proportionality, inverse proportionality, amplification etc.) exist between the deviations from steady state of any pair of causality-linked parameters. Within the same conceptual framework, we have developed a more general form of parameter state definition and causal linkage for a more effective LFM-based representation of deep process-knowledge. A few modifications to the basic LFM modeling conventions have been defined to create this more generalized modeling framework. As a result of the first modification, the modeled parameters are no longer represented across the board by two

binary and five continuous "discretized" states. Instead of the previous values +1, -1, +10, -10 (indicating, respectively, for a given parameter, a small deviation in the positive direction, a small deviation in the negative direction and large deviation in the positive or the negative direction, all deviations being "measured" from the assigned 0, i.e., "normal" state), any number of states can now be defined, with each state being represented by an integer increased by unity (in a positive or negative direction, depending on whether the intent is to represent an increasing deviation in the steady positive or negative direction from the original reference steady state) over the previous state. Thus, each LFM parameter or variable, V , will be now represented by a vector V_i with a user defined, rather than fixed, number of states, as shown below:

$$V_i = [-N, -N+1, \dots, 0, \dots, M-1, M]$$

Each parameter vector will thus contain $M+N+1$ states (including the 0 reference steady state), of which N are "negative deviate states" and M are "positive deviate states". Strictly binary variables are not affected by these new conventions and are represented in the same way as in the original LFM, that is, by using the value 1 to indicate the "true" or "on" state and the value 0 to indicate the "false" or "off" state.

A second modification of LFM generalizes multiple gain boxes (MGBs) into "multiple transfer functions (MTFs)", capable of more effectively representing the mapping of the states of a parameter which is upstream in a causality linked pair, into the states of the downstream parameter. In short mathematical notation, given that U is the state vector of the upstream parameter and D is the state vector of the downstream one, the transfer function of the causality link

between the two is a multiplier vector TF, such that for each allowed mapping $U \rightarrow D$:

$$D_j = TF(1,j) * U_i$$

This generalization allows a straightforward representation of process non-linearities, by allowing the gain multiplier to be a function of the upstream parameter state value. The previously used MGB representation was strictly linear and the gain values used to map upstream parameter states into downstream ones could not change as a function of the upstream state. To illustrate the MTF concept further, consider the example given in Table 4.I in which variable U (the upstream variable) is linked to variable D (the downstream variable). The table shows the state vectors U and D arbitrarily defined in this example to represent the two variables, the allowed mapping from the U variable states into the D variable states, and the values of the corresponding transfer function elements. Note that the -1 state for variable U is shown to map into either the state 0 or the state -1 of variable D. A situation like this may occur in practice when the analyst does not have sure knowledge on the nature of the cause-effect relation in an upstream/downstream variable pair in correspondence of one or more of the states of the upstream variable or parameter (e.g. state -1 of variable U in the given example).

It should be noted that when no non-linearities are present in the causal link between two given process parameters, the vector TF becomes a constant and the associated MTF can be represented essentially in the same way as an MGB would have been in the earlier version of LFM.

Table 4.1: Example of Parameter State Transfer Function

Parameter State Vectors				Allowed Mappings	Transfer Function Vector
U		D			
1	U ₁	j	D _j	1 → j	TF(1,j)
5	2	4	2	5 → 4	1
4	1	3	1	4 → 3	1
3	0	2	0	3 → 2	1
2	-1	1	-1	2 → 2	0/(-1)
1	-2			2 → 1	1
				1 → 1	1/2

Just like the previous version, the generalized LFM allows the "conditioning" of transfer functions. This means that the normal mapping between two variables, TF^1 can be modified into a different mapping, TF^2 , in the presence of a certain condition (or set of conditions). A one to one correspondence, identified by the superscript order-index affixed to the mapping vector, is thus established. Another way of explaining this is by noting that an MTF with multiple conditioned mappings is a two dimensional matrix, with one dimension identified by the set of conditions which determine which transfer function vector is to be applied, and the other dimension identified by the state of the input parameter in the linked pair. Conditions are expressed in the LFM "conditioning network" by means of test boxes (TBs; see Fig. 2.1) and can be combined into condition-sets by boolean logic operators expressed in graphic form by means of appropriate combinations of OR, AND and M-out-N gates.

The definition and use of a generalized framework for representation of parameter states and process non-linearities, as it was just described in this section, has also led us to identify an accordingly defined scheme for the representation of multiple interactions among process variables. A special operator called the Special Input Box (SIB) had been identified in the original

LFM concept as the means of describing a non-linear interaction of two or more process parameters, the combination of whose actual states would determine the state of another dependent parameter. For example, if two gaseous substances are pumped into a tank where they mix before being piped out, the output volume flowrate of the mixture will depend linearly on both input volume flowrates. However, if the two input gases can react chemically and form another compound once their relative concentrations have exceeded a certain ratio, then the output volume flowrate will exhibit a non-linear dependence on the two input flowrates. This type of situation can be handled in a relatively straightforward fashion in the LFM modeling environment. Because of the extension of the LFM parameter representation scheme in the fashion that we have just described, the SIB has been re-molded into a standardized LFM operator, which is now called the "Non-linear Input Interaction Operator" (NIIO).

The concept and use of an NIIO is relatively simple. Figure 4.1 and Table 4.II give a hypothetical example of the basic underlying idea by showing the model of a physical situation like the one just envisioned above, involving the non-linear interaction of two gaseous flowrates, FG1 and FG2, which enter a tank and produce a gas mixture output flowrate FG3.

Figure 4.1: Example of Non-linear Input Interaction Operator

Figure 4.1 shows that a NII interaction takes place between variables FG1 and FG2 at the input of variable FG3, whereas Table 4.II shows the nature of the interaction in the form in which it is represented by the NII. The NII is in essence a matrix which shows the state, or states, of FG3 which may result when a certain state of FG1 combines with a certain state of FG2. Because there are two input parameters, the NII matrix is two-dimensional. A situation in which N input variables into another LFM node were to exist would be represented by an N-dimensional NII matrix.

The physical reality represented by Table 4.II is one in which the two gases pumped into the tank start a chemical reaction whenever the concentration of the second gas (whose volume flowrate is represented by the LFM variable FG2) substantially exceeds that of the first gas (volume flowrate FG1). It is also assumed that the specific volume of the gas produced by the reaction (which contributes to the output gas mixture flowrate FG3) is substantially greater than the specific volume of the unreacted mixture of the two gases. This explains why state 0 (normal) of the first gas flowrate, "combining" with state 1 (high) of second gas flowrate can produce a state 1 (high) or state 2 (very high) for flowrate FG3 of the gas mixture (and also why the FG1= -1 FG2= 1 combination can produce FG3= 0 or =1, and the FG1= -1 FG2=0 combination FG3= -1 or =0).

TABLE 4.II: Example of Non-linear Interaction State Matrix

FG3		FG2		
		-1	0	1
FG1	1	0	1	1
	0	-1	0	2 / / 1
	-1	-1	0	1 / / 0
	-1	-1	-1	

The above matrix representation of NIIs has a direct implication in terms of the LFM inference backtracing. In the presence of an NII the LFM inference simply relates back the states of the output variable (FG3 in the example just given) to the states of the input variables (i.e. FG1 and FG2). Thus if one is interested in understanding the possible causes of a state 1 (high) for FG3, the inference backtracing will produce the logic-tree shown in Fig. 4.2.

Figure 4.2: Example of NII Driven Backtracing

In order for the LFM extensions discussed in this section to be made fully operative, they would have to be implemented in the software package that allows

the automated application of the LFM inference engine. This task is conceptually straightforward, although it requires in practice a certain level of effort in terms of software encoding and debugging.

5. Object Oriented Database Representation of LFM Models

The LFM inference engine uses synthetic LFM process models as input and generates analytic logic trees as output. These trees explain how specific events, defined by the analyst as the focus of his/her analysis, or actually occurring in the plant process and thus the subjects of a diagnostic real-time analysis, have been produced by basic process conditions. The LFM input models constitute the knowledge base upon which the inference engine operates to generate its deductions. This knowledge base must be made available to the inference engine in a form suitable for analysis and deduction by the latter. The objective of the PROLGRAF-B model builder is thus to generate a database containing process-related deep knowledge in the LFM process-model format.

A natural form of representing LFM models is by "object oriented" database generation. In this type of representation the individual elements appearing in an LFM model are categorized as belonging to one of a finite set of LFM object classes. For example, LFM continuous variable nodes (CVNs) constitute a class of objects, whereas multiple gain boxes (MGBs) constitute another class. Each class is characterized by a set of "attributes" or "dimensions" which in turn take on specific "values" in the instantiation of a specific object within a certain class. This concept is illustrated by Table 5.I. The table shows the CVN objects which appear in the LFM model of Fig. 2.1, their dimensions, and the values taken by these for that specific instance of inter-object relations. The

end product of the PROLGRAF-B model building procedures is thus an object data-base constructed in format similar to that shown in Table 5.I. This constitutes a convenient means of making available to the LFM inference engine the deep-knowledge base required for its cause-effect back-tracing and reasoning.

TABLE 5.I: Continuous Variable Nodes in Test-case Example

<i>DIMENSIONS</i>	<i>VALUES</i>		
Identifier	V1	V2	V3
Causal inputs	none	1 from MGB	none
Causal outputs	1 into MGB	none	none
Condtnl. outputs	none	none	1 into TB

Process-related knowledge is usually available in forms that are not directly usable by a system analyst. For many industrial processes, piping and instrumentation diagrams (P&IDs) describe the functional layout of components and systems, as well as other elements of basic engineering data regarding the specific process of interest (e.g., pipe sizes, presence of instrumentation and controls, etc.).

P&IDs can give the analyst a reasonable idea of how a process is supposed to work by showing its principal constituting components and their physical process connections (e.g., by piping, wiring, etc.). In essence P&IDs show the principal "objects" that populate the process space and some of their functionally relevant attributes. However, other attributes, most notably the ones linked to operational logic and control modes, which are equally if not more important than the layout-related ones for the purpose of representing and analyzing system functionality, are not directly contained nor implicitly expressed by P&IDs. Despite the incompleteness of the information that they carry, P&IDs constitute a good starting point to operate a transformation of process

knowledge into LFM format. Such a transformation can be thought of as a translation or mapping from a certain type of object space (i.e., the object space which obeys the P&ID process representation conventions) into another (i.e., the one which obeys the LFM representation conventions).

Because constructing a knowledge base in the "target" LFM object space requires the specification of object attributes which are not described in the "source" P&ID object space, the translation process implies a "knowledge added value". This consists in additional elements of knowledge and information regarding the functional characteristics of the represented process or system, which have to be added by the system engineer or analyst. The obvious implication is that the translation process can be designed to be largely computer assisted but cannot be entirely automatic. The PROLGRAF-B model-building procedures attempt to formalize the P&ID - LFM knowledge translation in a series of user augmented steps. The ultimate objective is to allow the development of a flexible model-builder software tool implementable in an "intelligent workstation" interactive environment for the construction of LFM process models. For greater flexibility and adaptability of the model-builder software the choice of priority is likely to ultimately contemplate the use of second generation "expert system" shells that can be applied in a PC workstation hardware environment, although early prototyping may be realized in more sophisticated LISP-machine environments.

6. PROLGRAF-B Model-Building Procedures

The PROLGRAF-B model building procedures consist essentially of a series of user-guided transformations by which the process knowledge "contained" in the

process piping and instrumentation diagrams (P&IDs), functional design specifications, and in the analyst's own understanding, is eventually synthesized and molded into the desired LFM object database form. The codification of these procedures in the PROLGRAF-B intelligent interface program will greatly facilitate the task of a user who wants to construct an LFM process model and wants to reduce the amount of effort required to become familiar with the detailed application of the LFM modeling rules and syntax.

The prototype version of the procedures which are being developed to demonstrate the feasibility of the concept uses piping and instrumentation diagrams (P&IDs) as the starting point of its "reasoning", and queries the user through an organized series of question and answer interactions. Four main stages of program/ user interaction are required to operate the knowledge transformation from the assumed sources of process knowledge to the LFM object oriented database. These stages are:

- Process and Model Primary Object Identification
- Causality Flow Identification
- Causality Transfer Function and Interaction Specification
- Fault and Causality Conditioning Specification

The PROLGRAF-B interaction with the user follows the reasoning procedures outlined in the following sections, which illustrate each of the knowledge transformation stages listed above. Each step in the procedure is consecutively numbered. Individual steps and/or major blocks of steps are illustrated by examples that make reference to a simple "test case" system with feedback control, depicted in P&ID format in the upper portion of Figure 6.1.

Figure 6.1: Identification of Plant System Elements from P&ID

6.1 Process and Model Primary Object Identification

The identification of the primary "objects" in a given process requires the user of PROLOGRAF-B to recognize and list the fundamental elements appearing in the P&ID representation of that process. PROLOGRAF-B will invite the user to complete the following steps:

Step 1- Identify principal components in P&ID.

(Form "super components" if necessary).

From examination of the system P&ID the user will identify the principal system components. Some degree of judgment and insight will have to be applied by the analyst in deciding which of the many components that typically appear in a detailed P&ID should be considered as the fundamental ones for modeling purposes.

Importance in process functionality is the main criterion to be applied here. In the analysis of complex systems it will be necessary to condense blocks of components into conceptually defined "supercomponents". For example,

These objects will not appear in the LFM model itself, but are used as guidance to identify the LFM model primary objects -- that is, the LFM variable nodes (VNs) -- as explained in the next procedural step which the user will be asked to complete by the model builder program:

**Step 3- Identify essential parameters characterizing
functionality of components identified in Step 1.**

For each component a list of parameters that can be used to characterize its performance is provided. The user is invited to identify in the list those parameters that in his opinion are the best minimal set that can be used to model the target process at the desired level of detail. The "minimal set" should be chosen in such a way as to minimize the number of parameters used to characterize a given component. This process of synthesis, however, should be applied with special attention directed at avoiding the suppression of representation of those process elements and relations through which potentially important faults and disturbances may manifest themselves.

A "library" of parameters usable to characterize components that may typically appear in a plant process will be eventually made part of a "user-orientation database" accessible via the PROLOGRAF-B software. Lists of typical parameters for each one of the component types which appear in the test-case example are presented below. From these a user would be invited to select his/her best choice of characterizing parameters. The user would also be invited to add parameters to the list of chosen parameters for each component, if he/she thought that this list were incomplete or inadequate for his modeling purposes.

Pump parameter list

- a. speed
- b. input pressure
- c. output pressure
- d. Dp (head)
- e. flowrate

Control valve parameter list

- a. stem position command
- b. stem position
- c. input pressure
- d. output pressure
- e. Dp
- f. flowrate

Flow sensor parameter list

- a. actual flowrate
- b. measured flowrate

Controller parameter list

- a. set point (specify for which variable)
- b. input signal (" " " ")
- c. output command (" " " ")

Test-case : A possible set of parameter selections for the
example system used in the example could be as follows:

Pump : speed (Ps), flowrate (Pf);

Control Valve: [stem position] command (CVc),
[stem] position (CVp), flowrate
(CVf)

Flow Sensor: flowrate (FSf), [flow] measure (FSm)

Controller: input [signal] (Ci), output [signal]
(Co)

Once chosen by the analyst, component parameters are considered by PROLOGRAF-B as newly defined LFM "variable node" objects. At the end of this step the knowledge transformation process has thus progressed to the stage depicted in Figure 6.2. This figure illustrates grafically the parameter selection that could have been theoretically identified as the one best suited to describe the "test case" system. The picture shown in the figure is a hybrid representation in which the principal P&ID objects (i.e., components and connectors) appear together with the LFM variable node objects that have been chosen to represent them. Note that in this example only some of the possible characterizing variables for each component have been selected; e.g., for the pump component, the pump speed (Ps) and the pump flowrate (Pf) are judged sufficient to describe the component functions.

Figure 6.2: Identification of Essential Process Parameters

6.2 Causality Flow Identification

Once the primary objects which exist in a given process -- i.e. components and component-connectors -- are recognized and associated with a set of basic LFM objects -- i.e. the parameters that are chosen to characterize the process components -- the next task that needs to be undertaken in the LFM model building sequence concerns the identification of the *relations* which exist among identified objects, and the representation of these relations in the appropriate LFM format. The relations of interest to the analyst in the LFM modeling environment are relations of cause and effect among parameters. These relations are shown in the LFM graphic representation conventions by directed edges joining the flowgraph node pairs which correspond to the parameters affected by the cause effect relation. To facilitate the process, PROLGRAF-B requests the user to complete this identification of cause-effect relations in two steps. In each of these steps the identification process is guided by the object-related knowledge that has been gathered in the previously executed model-building procedures. More specifically, it is recognized that in a plant process causality is transmitted by physical means, that is, cause-effect

influences may propagate either from one parameter to another within individual components, or they may propagate across component boundaries through the causality-conducting medium provided by the component connectors that physically link specific sets of component in a particular system configuration. The following practical steps should thus be executed by a user interacting with the PROLGRAF-B software for the purpose of identifying process causality flow:

Step 4- Recognize and identify the direct cause-effect relations between parameters within each component.

Limiting his attention to direct influences of cause and effect within individual components, the user identifies which variables drive and which variables are driven in all the identifiable parameter-to-parameter causal relations.

Test-case : "pump speed Ps drives pump flowrate Pf";
example "control valve command CVc drives control valve position CVp"; etc.

Step 5- Recognize and identify the cause-effect relations between parameters linked by connectors across component boundaries.

To guide the user through this step, the model-builder program utilizes the component connectors identified in Step 2 as a means for pre-identification of possible cause-effect links between pairs of variable nodes (i.e., parameters) associated with separate components.

Test-case : Pipe 1 (p1) connects "pump" to "control valve", thus cause-effect links are possible between the parameters Ps (pump speed) and Pf (pump flowrate) on one side, and CVf (control valve

flowrate), CVp (control valve position) and CVc (control valve command) on the other. The user can then readily determine that the p1 connector establishes a mutual (i.e., bi-directional) causal influence between Pf and CVf.

With reference to the test case example, Figures 6.3 and 6.4 illustrate the corresponding Steps 4 and 5 respectively, whereas Figure 6.5 shows the incomplete LFM model that is obtained at the end of Step 5.

Figure 6.3: Within-component Causal Relations

Figure 6.4: Inter-component Causal Relations

Figure 6.5: Incomplete LFM Model

6.3 Causality Transfer Function and Interaction Specification

The system model that is obtained at the end of Step 5 is not a "complete" LFM model, in that it only shows which cause-and-effect mechanisms exist in a given process, but does not describe their actual nature. For example, it shows that in the test-case system the pump speed influences the pump flowrate, but it doesn't specify how. It also fails to show if, for those variable nodes that are influenced by more than one input parameter, any special non-linear interaction effect takes place among the input variables, so that the influenced "output" parameter is determined by other than just a simple linear superposition effect. For example, by looking at the model in Fig. 6.5 one cannot tell (except by guess) how the combined action of the causal inputs from both the pump flowrate (Pf) and control valve position (CVp) variable nodes determine the state of the control valve flowrate CVf. In order to complete the model a few additional model building steps have to be executed, as described hereinafter.

Step 6- For each variable node in the model, define a vector of discrete values sufficient to completely characterize the state of the associated variable.

In Section 4, we have introduced a form of variable state representation and causal linkage that has been developed as an improvement and a generalization of the previously adopted LFM modeling conventions. In the generalized LFM, process variable value ranges can be represented by an ad-hoc number of states, each state being represented by an integer increased by unity over the previous state (for deviations increasing in the positive direction from the "0", i.e. normal, state), or decreased by unity (for deviations increasing in the negative direction from the "0" state). Thus, to complete the definition of the object attributes of an LFM variable node V, the user must be asked by PROLGRAF-B to define a vector

$$V_i = \{ -N, -(N - 1), \dots, 0, \dots, M-1, M \}$$

containing $M + N + 1$ states (N "negative deviate states", the " 0 " reference steady state and M "positive deviate states").

Test Case : A possible definition of states for the variables
example appearing in the test-case system may be:

$CVf_i = \{ -1, 0, 1 \}$ (low, normal, high);

$Cvp_i = \{ -1, 0, 1 \}$ (close more, hold steady,
open more);

etc.

Step 7- For all the causal relations identified in Steps 4 and 5 define

"multiple transfer functions" (MTFs) to determine how mutual influences among process variable states can propagate in the system that is being modeled.

MTFs are a generalization of the earlier mentioned MGB (multiple gain box) LFM "objects". As it was previously discussed in Section 4, they represent the

mapping of the states of an upstream variable into those of a downstream variable. This implies that the user be asked by PROLGRAF-B to define, for each pair of causality-linked variables U and V, a mapping vector such that

$$D_j = TF(ij) * U_i$$

In Step 7 the user also decides if the number of variable nodes in the model may be reduced by merging into one node those variables that may not be necessary to represent separately.

Step 8- Identify "multiple interaction nodes" (MINs), that is, LFM variables directly influenced by more than one other variable, and select or define an appropriate "input interaction operator" (IIO) to describe the interaction.

When more than one causal input into a node exists, the analyst has to determine if the causal effects merging into the node influence the corresponding variable in a linearly independent way (e.g., by superposition of effects), or if a particular non linear interaction may exist there. The LFM modeling primitives include standard non-linear input operators such as the "causative-corrective input operator" (CCIO), which can be used to show corrective actions taking place at the controlled variable nodes of feedback and feedforward loops. Non standard interactions are described by "non-linear input interaction operators (NIIOs). These are multi-dimensional matrices (the number of dimensions depending on the number of interacting node inputs) which allow the states of the vector representing a downstream variable which is influenced by the non linear interaction of a set of upstream variables, to be defined as a function of the combination of the vector states of the influencing variables. This subject has also been discussed in greater detail in Section 4.

Test-case : Completion of Steps 6, 7 and 8 transforms the example incomplete example LFM model of Fig. 6.5 into the more complete representation shown in Fig. 6.6. Note that in this simple model it was sufficient to represent transfer functions with constant "gains" : +1 for direct proportionality between variations of causally linked variables, -1 for inverse proportionality (as required in the feedback relation between the measured flowrate, FSm, and the controller output, Co). Note also that a standard LFM CCIO was used at the input of CVf to show that the control valve position can exert a corrective action on the causal effects produced by pump speed and flowrate. Finally, note that two variable pairs were "reduced" into one variable, namely FSm - Ci (into FSm) and CVc - CVp (into CVp).

Figure 6.6: Completed LFM Model

6.4 Fault and Causality Conditioning Specification

The definition of PROLGRAF-B building steps for the procedurally-aided inclusion of process faults in an LFM model has required some research effort to

identify and characterize the nature of the problem at a basic conceptual level. This Section has been divided in subsections which closely reflect and summarize the steps along which our research in this area has progressed.

6.4.1 Definition of Engineering Process Faults

Engineering process faults can generally be referred to either components or component connectors which directly appear in the piping and instrumentation diagram representing the process (P&ID). The concepts of "P&ID component" and "P&ID component connector" constitute one of the starting points for the execution of the PROLOGRAF-B model building procedures and have been discussed in Section 6.1. A topological distinction between "faults in P&ID component" and "faults in P&ID component connection" would thus appear to be a natural one. However, from the point of view of defining faults in a way that facilitates their representation in the LFM object representation space it is preferable to work with a slightly different type of distinction, which classifies faults by the type of functional manifestation rather than topologically. Such a "functional classification" characterizes faults according to one of the following two definitions:

A) Internal Change-Of-Behavior Fault (ICBF)

An internally produced and spontaneous change of state of a process component (from the desired to an undesired state);

B) External Relation Change Fault (ERCF)

A failure by a process component to: a) maintain its state in the range intended by design as the one consistent with its external connections with other components, or: b) to respond, as intended by design, to an external command which requires a change of component state.

We note that the ICOBF and ERCF "functional" definitions almost exactly map into the topological classes "fault in P&ID component" and "fault in P&ID component connector". More specifically it can be observed that the ICOBF functional class can always be seen as being entirely contained within the topological class "fault in P&ID component" and that the mapping can be interpreted as a complete one-to-one mapping if the boundaries between "components" and "component connectors" are seen from a functional, rather than physical, point of view. To clarify this point further, we note first that an ERCF is a fault which manifests itself as a drastic modification of the flow of causality along a connector between two directly linked P&ID components and that such a fault can be produced in any of the following three ways:

- B1: a fault at the "output port" of the component from which the causality connection is maintained or the change of state command is issued;
- B2: a fault in the "connector" between the "commanding" and "receiving" components (a "connector" is typically a pipe, an electrical connection, or a pneumatic line);
- B3: a fault at the "input port" of the "receiving" component.

It becomes then clear that the topological class "fault in component connector" and the functional class "ERC Fault" could generally be interpreted as been the same class if the "functional boundaries" of the physical entities "component connectors" are extended to include component input and output ports through which causality flow links with other components are maintained. Examples of component "input" and "output ports" in hydraulic systems are pump and valve flanges; in mechanical systems, the physical boundaries (sometimes corresponding to the presence of specific motion-interface devices such as

mechanical joints, sometimes only identifiable as geometrical boundaries) where a motion generating device (e.g., an electrical motor rotor) is connected to a motion-transmitting device (e.g., the motor shaft).

It should be noted that the distinction between the ERC subtypes B1, B2 and B3 has been made here only for the purpose of clarifying the relation between the topological fault classification scheme suggested by the nature of the P&ID representation and the functional classification which is most natural and easy to implement in LFM. This should become more clear to the reader with the illustrations and discussions given in Sections 6.4.3 and 6.4.4 on the subject of LFM fault representation and PROLOGRAF-B related procedures. It will be seen there that for the representation of faults in the LFM modeling environment no practical distinction between the three above ERCF subtypes needs to be made. In LFM we shall adopt the convention of assigning all three subtypes to the LFM "multiple transfer function boxes" (MTFs), which model the causality flow function(s) expressed (implicitly in the P&ID representation scheme) by component connectors. As will be also become apparent in Section 6.4.4, however, the different basic origination points of the three subtypes can be properly represented in an LFM model by defining different basic binary events acting as conditioning events on the MTF, one for each different originating fault. At this level of detail it is possible to make clear to which of the three above listed fault subtypes a specific basic fault, represented by a basic binary LFM variable node (BVN), actually belongs.

6.4.2 Classification of Faults in P&ID and LFM Object Spaces

The construction of an LFM model requires a transposition of engineering knowledge from a device- and component-oriented object space, such as a piping

and instrumentation diagram (P&ID), to the parameter- and causality-flow-oriented space of the LFM representation itself. In such a transposition a P&ID device or component (such as "pump", or "valve") typically is expanded into an LFM "mini-model", consisting of a few nodes representing key parameters or variables (in LFM we recall that such nodes are called CVNs, for "continuous variable nodes", or BVNs, for "binary variable nodes") and of the causal edges representing the appropriate cause-and-effect relations among these (this part of the transposition process is accomplished in the first four steps of the PROLOGRAF-B model building process).

The immediate consequence of this in terms of LFM fault representation is that ICOBFs have to be distinguished further into the two following subclasses:

a) Internal Parameter State Change Faults (IPSCFs):

those device/component internal faults which can be thought of as an undesired spontaneous change of state of one of the parameters/variables which appear in the device/component LFM mini-model;

b) Internal Relation Change Faults (IRCFs):

those device/component internal faults which can be thought of as a change in the cause-and-effect relation between two or more of the parameters/variables which make up the device/component LFM mini-model

It is important to note that IRCFs manifest themselves as a failure by an internal component variable to respond as expected to the change of state of another internal component variable to which it is causally linked by a direct connection. In this sense their form of manifestation is similar to that of the ERCFs (External Relation Change Faults). The difference is in that the latter

always correspond to a change in the cause-and-effect relation between parameters or variables which are part of the representation of separate devices and components (i.e., devices and components which appear as separate and distinct objects in the P&ID representation used as the reference knowledge base for the construction of the LFM system-model and the source of the "transposition" process).

It is useful to illustrate these concepts with an example before discussing how the different types of fault classes defined above can be handled in the execution of the transposition from P&ID to LFM representation of an engineering process or system knowledge base.

A P&ID subsystem, made up of the components "Pump", "Control Valve", "Flow Sensor" and "Controller", has been discussed heretofore in terms of the procedures to be automated to allow the construction of an LFM model by means of the PROLOGRAF-B model builder software. The pump component of this relatively simple subsystem is, in its LFM representation, modelled by means of two CVN variables, namely "pump speed" (Ps) and "pump flowrate" (Pf), while the control valve is modelled by means of three CVNs, namely "control valve command" (CVc), "control valve position" (CVp) and "control valve flowrate" (CVf). Fig. 6.5 shows one causality relation (proceeding from Ps to Pf) within the device "Pump", two causality relations (from CVc to CVp, and from CVp to CVf, respectively) within the device "Control Valve", and one causality relation (from Pf to CVf) bridging across the two just named devices.

Let us consider now the following basic faults which may potentially affect these two devices, either individually or when considered as a whole functional block:

- 1) pump motor shaft seizure
- 2) pump housing perforation (by corrosion or by mechanical damage)
- 3) control valve actuator freeze
- 4) pipe break in between pump and control valve

According to the definitions of fault types given in the preceding discussion, and to the LFM parameter representation of the "Pump" and "Control Valve" devices, the faults listed would have to be classified as follows (explanation of the classification is given under each heading):

1) pump motor shaft seizure → IPSC Fault:

the whole motor/pump device is modeled as one component and no causality flow from motor to pump via the shaft connector is explicitly modeled in the LFM representation of Fig. 6.5; therefore a motor seizure is to be considered an "internal" fault which directly causes a change of state in the LFM variable "pump speed" (Ps);

2) pump housing perforation → IRC Fault :

the effect of this fault would be to cause a massive leak through the housing breach, which in turn would drastically weaken the relation of direct proportionality between the pump variables Ps and Pf (speed and [discharge] flowrate);

3) control valve actuator freeze → IRC Fault :

the effect of this fault is to prevent response by the valve stem position (LFM variable CVp) to state change requests from the valve command signal (LFM variable CVc); in other words the fault manifests itself as a change in the causal relation between CVc and CVp;

4) *pipe break between pump and valve → ERC Fault :*

the effect of this fault is to cause a massive leak in the connection between the pump and the valve components, which would drastically weaken the relation of direct proportionality between the pump and the valve flowrates (LFM variables P_f and CV_f).

Referring back to what was stated in the definition of fault types as well as to the example given above, we note the following:

- A. In the P&ID object-space a natural classification of faults can be based on whether a fault has its origin within the device or component where its effect become manifest, or whether it is rooted in the connections or couplings between separate devices or components. This is essentially the distinction between ICOB vs. ERC faults.
- B. In the LFM object-space a classification of faults can be based on whether a fault can be represented as a basic event (i.e., an event without any other cause explicitly represented or modelled upstream of itself in the cause-and-effect flow representation which is at the base of the LFM modelling concept), or as an undesired change in one of the causal relationships between variables that characterize the behavior of an individual component or of a block of components seen as a whole. This is essentially the distinction between IPSC vs. IRC and ERC faults.
- C. In the framework of representing how they affect causal relations between process parameters, IRC and ERC faults can be represented essentially in the same way. The only distinction is that IRC faults concern changes in causal relationships that exist within the boundaries of one individual device or component LFM mini-model, whereas ERC faults concern changes in causal relationships which exist across such boundaries.

6.4.3 LFM Representation of Faults

In the original LFM modeling environment, faults were expressed either as events conditioning and modifying a cause-and-effect relations in a specific, off-normal way, or as basic binary events expressed just as any other LFM "binary variable nodes" (BVNs) (see Refs. [4,5]). As part of our effort of identifying orderly procedures for LFM model construction, we have better defined, although not drastically changed, this fault representation framework, based on the classification of fault types discussed in Sections 6.4.1 and 6.4.2, which we repeat and summarize below:

IPSC (Internal Parameter State Change) Faults:

those device/component internal faults which can manifest themselves as undesired spontaneous changes of state in anyone of the component parameters/variables which appear in the device/component LFM "mini-model";

IRC (Internal Relation Change) Faults:

those device/component internal faults which manifest themselves as changes in the cause-and-effect relation between two or more of the parameters/variables which make up the device/component LFM "mini-model";

ERC (External Relation Change) Faults:

those process faults which manifest themselves as: a) a failure by a process device/component to maintain its state in the range "requested" by the normal direct cause-and-effect relationship(s) linking its characterizing parameters to other component parameters (as intended by design and implied by its physical connections with other components), or: b) to respond as intended by design to an external command which requires a change of state in one or more of its characterizing parameters.

We note again that the above classification corresponds to the desire of reflecting two types of distinctions: the first distinction is between undesired changes of state in process parameters and undesired changes in state correspondences (i.e., cause and effect relationships) between process parameters, the second is between faults originating internally to individual components and faults originating in connections between components. It may also be noted that IRCFs manifest themselves in a manner similar to that of the ERCFs (External Relation Change Faults). The difference is in that the latter always correspond to a change in the cause-and-effect relation between parameters or variables which are part of the representation of separate devices and components (i.e., devices and components which appear as separate and distinct objects in the P&ID which appear as separate and distinct objects in the P&ID representation used as the reference knowledge base for the construction of the LFM system-model), whereas in IRCs the same phenomenon affects directly only parameters which are defined within the boundaries of one individual component. The categorization just presented above reflects the distinctions that are more important from a modeling point of view in the LFM object-space (i.e., faults which directly force a spontaneous change in the state of an LFM variable node vs. faults which modify the nature of the causal relations between LFM variables), while retaining also the distinction between intra- and inter-component fault origination mechanisms which is inherited from the P&ID object representation space.

The three classes of faults identified above are represented differently in the LFM environment. More specifically, IPSCFs are represented as basic binary events forcing a specific value in the directly affected LFM variable, whereas

IRCs and ERCs correspond to conditions affecting the cause effect relations between LFM variables. Both fault types may be represented either by basic binary LFM variables or by an LFM variable entering an off-normal state in its range of discrete states. In either case these conditions are implicitly "logically-anded", through the LFM device of MGB/MTF conditioning, with a particular value (or set of values) of the LFM variable which is upstream in the causality flow expressed by the MGB or MTF "conditioned" by the fault (please refer to Sections 2 and 4, and to Refs. 4 and 5 for details on the meaning and use of these LFM devices).

One exception to this general rule is the particular situation in which the outcome of an ERC is to indicate a new point of "diverging causality flow" in the process, in correspondence of a component connector. This is the case, for example, when a pipe obstruction in a fluid flow from Point A to Point B of a piping system causes the flowrate at Point B to be driven to nil (by the course of the originally followed causality flowpath), but also causes the flowrate an instant feedback in the reverse causality flow direction which drives the flowrate at Point A also to nil.

Section 6.4.4 provides examples and clarifications (based on the simple test-case system that we have adopted to illustrate the results of this research) of all the various types of LFM process fault representations that have been discussed here.

6.4.4 PROLOGRAF-B Procedures for Fault Identification and Representation

The reality of fault identification and representation in an engineering system or process is that there exists no substitute for the analyst's experience in such a task, except of course for the capability offered by the

use of computer databases to store reference lists of faults that have been observed in the past as being typically associated with the operational behavior of certain process components. The analyst will, however, still be called to judge on the applicability of each item on such generic lists to the specific component and situation which is being modeled. The fundamental procedural steps that the PROLGRAF-B model builder can directly perform offer, in the execution of the fault representation phase of the LFM model building, the advantage of uniformity and systematic rigor over less formalized approaches which have been standard in similar analytical activities performed within the scope of typical fault-tree or reliability block diagram manual derivations.

If we resume the definition of the model-building steps where we had left it at the end of Section 6.3, the fault identification and causality conditioning procedures that we have identified can be summarized as reported below. Please note that the test-case examples presented to illustrate the various steps listed in the following are representations of the types of situations which may be encountered in a typical LFM model-building session, but are not meant to be an exhaustive set for the system used here as the test-case.

Step 9- Identify basic fault-generating events associated with individual P&ID components.

From a pre-compiled database of known P&ID component types, call up and complete (or generate from ground up for component types not included in the database) lists of basic fault-generating events (e.g., for a pump: rotor freeze, seal leak, housing perforation, etc.);

Test-case : a) Within the control-valve component the following basic faults
example may occur: "fail open", "fail closed", "seal leakage"; b) within

the controller component the following basic faults may occur:
"DC power loss", "gain reversal", "gain too high", "gain too low"; etc.

Step 10- Categorize fault types and generate appropriate LFM model representations of component faults.

Divide the basic fault-generating events identified per Step 9 into the three basic categories: IPSCF basic events, IRCF conditions, ERCF conditions; the first of the three categories produces LFM binary nodes forcing the state of a variable node into a particular abnormal "value", the second and third categories are represented as LFM condition events activating specific non-default MTF transfer functions or MGB gains (see Section 4 and Refs. [4,5]);

Test-case : Limiting our attention to the control valve, "fail open" and
example "fail closed" are classified as IPSCFs, respectively expressed by LFM binary variable nodes (BVNs) CVfo and CVfc, which directly drive the variable CVp (control valve position) to open or close; "seal leakage" is classified as an IRCF expressed by an LFM condition CVsl "weakening" the gain between the internal variables CVp (control valve position) and CVf (control valve flowrate).

The same classification steps should be completed for all the other P&ID components.

Step 11- Identify basic fault-generating events associated with individual P&ID component-connectors.

Repeat Step 1 for P&ID component connectors.

Test-case : a) In "pipe 1" (connector between pump and control example valve)
example the following basic faults may occur: "pipe leakage", "pipe rupture", "pipe obstruction"; for "wire 1" (connector between flow sensor and controller) the following basic faults may occur: "open circuit", "ground short"; c) etc.

Step 12- Generate appropriate LFM model representations of component faults.

Create appropriate ERCF conditions in correspondence of identified component connector fault-generating events (by definition these should not produce IPSCFs nor IRCFs);

Test-case : Limiting our attention to the "pipe 1" component connector, "pipe example leak" is an ERCF which is expressed as an LFM condition P11, weakening the gain between the pump variable Pf (pump flowrate) and the control valve variable CVf (control valve flowrate); "pipe rupture" is an ERCF which is expressed as an LFM condition P1r, nullifying the gain between the pump variable Pf (pump flowrate) and the control valve variable CVf (control valve flowrate). The third basic fault identified in Step 11, i.e. "pipe obstruction", presents the interesting situation in which an ERC fault creates a "diverging causality flow" at the LFM MGB/MTF which is affected by it. This case has been brought to the reader's attention and briefly discussed at the end of Section 6.4.3. In this case the ERC condition P1o activates in the MGB/MTF between the variables Pf and CVf a transfer function selection which acts both in the direction from pump to control valve and in the opposite direction (from control valve to pump),

and which forces both variable Pf (pump flowrate) and CVf (control flowrate) to decrease to their nil value.

At the end of Step 12 the LFM model of the test-case system would look like the one laid down in Fig. 6.7 (except that the model presented in the figure contains the representation of only those fault conditions that we have discussed in the "test-case examples" given above in correspondence with the description of Steps 9 through 12). The PROLGRAF-B procedures could be considered completed at this point, except for the inclusion of the representation of process changes of mode, be they intrinsic to the physics of the process (e.g., the activation of different causal relations between process variables at certain "trigger values" reached by certain specific process parameters), or designed into its operational controls (e.g., the switch of a process parameter control from automatic to manual, or viceversa, according to a control option chosen by the process operators). These instances are addressed in the last two PROLGRAF-B procedural steps which are described below.

Figure 6.7: LFM Model Including Representation of Faults

Step 13- Identify possible process "change-of-mode" conditions. Systematically examine all LFM-model MTFs/MGBs (in other words all the cause-and-effect relationships expressed in the model and identify which changes in these relationships, if any, appear to be possible in correspondence of specific process events;

Test-case : Assuming that the feedback control system of the test-case
example system can be deactivated manually by opening a switch on the electrical connection between the controller and the control valve, the MGB/MTF affected by this action is clearly the one between the LFM variables Co (controller output) and CVp (control valve position), which represents the cause-and-effect action physically carried out through the component connector "wire 2".

Step 14- Introduce process "change-of-mode" conditions in LFM model.

Represent all the events that may produce the cause-and-effect relationship changes identified per Step 13 as MTF/MGB-conditioning events.

Test-case : The LFM representation of the "change-of-mode" condition
example identified in Step 13 is very similar to that of an ERC fault; here, however, the basic event representing the MGB/MTF conditioning, expressed by LFM binary condition CVdo (control valve disactivation option) which brings to nil the gain between the variables Co and CVp, corresponds to a deliberate option chosen by the process operators rather than to a fault spontaneously occurring in the process. The section of the LFM model related to the representation of this change-of-mode option is depicted in Fig. 6.8.

Figure 6.8: LFM Model Section Representing Process Change-of-Mode

Step 14, when completed, concludes the PROLOGRAF-B fault representation and model building procedures. We note again that the generation of LFM conditioning events associated with Steps 13 and 14 should normally be applied to identify and represent process "mode changes", that is, changes in cause-and-effect process relationships triggered by physical non-linearities (such as the change of slope in the relation between temperature and pressure in a gaseous medium) and/or the effect of "logic switches" designed into the process control logic (such as the possible switching from a low gain to a high gain control action in a feedback loop). We have included these steps in the procedural series related to fault identification as a matter of convenience and because of the close analogy of the associated conditioning event identification with the identification of IRCF and ERCF conditions.

7. PROLOGRAF-B Procedural Extensions

The concepts and procedures that have been described in the preceding sections have been verified and matured to a stage sufficient to allow the development of a prototype software demonstration package, which has been designed and partially developed (see Section 8). Other features of the LFM model builder

that could be developed to make it more complete and error-proof have been defined at a more preliminary level and would need to be better refined and verified before a translation into actual software may be attempted.

One such extension, beyond the stage of development of the LFM model-building procedures described heretofore, which has been envisioned but not fully specified and designed regards the implementation of an automatic check procedure for the elimination of possible modeling redundancies that the PROLOGRAF-B user could involuntarily introduce in the representation of process cause-effect paths in the LFM graph models. A brief discussion of this possible extension is given in the following subsection.

7.1 Causality-Link Check Procedure

The purpose of the causality-link check procedure is to identify if any of the cause-effect relations identified in Steps 4 and 5 (Section 6.2) are logically redundant and/or do not satisfy the requirement of having to hold as "direct" relations (i.e., without any intermediate parameter link). This redundancy-checking function can be based on an automatic algorithm that "opens" the direct existing links between parameters and verifies if another link, proceeding in the same cause-effect direction, exists between the same parameter pairs. This can be done by application of a heuristic search technique, or, more rigorously, by modifying the "reachability theorem", widely known and used in graph theory, to account for those cases in which multiple causality paths between two parameters may exist legally in the context of a specific LFM model. Examples of "legal" multiple causality links are parallel physical causality paths, alternative-direction causality paths (i.e, from B to A as well as from A to B), feedback and feedforward effects, or other cases in which the additional

causality links combine into the receiving end of the parameter pair through a multiple parameter input interaction represented in the LFM model by an NIIO.

For all those cases in which a redundant link is identified the PROLGRAF-B user should be presented with the question of whether: a) the redundant path should be eliminated, or b) the existence of the parallel causality path(s) is legal "as-is" because of physical link redundancy, or c) a feedforward effect exists and an IIO (input interaction operator) was overlooked in the construction of the LFM model and has to be added. In the last of the three cases depicted here the (cause-effect) redundancy is only apparent and would be eliminated by correcting the model with the introduction of the previously missed IIO. The model builder program should ask the user the necessary directions to perform this correction. These directions would consist essentially in verifying that in fact an IIO is needed at the input of the parameter which is on the "downstream" side of the cause-effect merging paths, and in carefully checking which cause-effect paths are in fact interacting to produce the possible states of the downstream parameter. After the model has been corrected the redundancy checking procedure will be re-initialized.

8. PROLGRAF-B Prototype Software

The PROLGRAF-B model builder has been designed to allow computer-assisted generation of logic-flowgraph models of plant processes.

The degree of success achievable in pursuit of this objective has been evaluated in our research by verifying that the envisioned model building procedures can in effect be implemented in a workable software (and hardware) environment. A software development and demonstration plan has been executed for this purpose, although with realistic objectives, given the budget adjust-

ments that had to be absorbed by the project within its execution period. These objectives essentially consisted in the implementation of the procedures defined in Section 6, up to Step 8 included, into a prototype software package which has been developed within an "expert system" shell of suitable characteristics. The initial orientation for the development of the model-builder workstation demo was to develop a first prototype in a LISP machine running under the KEE expert system shell. Because of the low portability and high cost of such an environment we have strived to accomplish essentially the same objectives by use of a PC/AT based expert system shell, although we obviously had to adjust our development activities to the constraints imposed by the considerably less flexible and less sophisticated user interface offered by this PC-based shell.

An ideal workstation environment would allow the PROLGRAF-B software user to shift back and forth between a graphic representation of the object spaces that he/she is operating on -- e.g. the P&ID space and the LFM space -- as well as that of some of the intermediate stepping stones of the knowledge transposition procedures which execute the mapping from one object space to the other. Since programming such a graphic-oriented environment is very costly in manpower we have been seeking a compromise in which most of the executable procedures were guided by a programmed sequence of item lists and activity menus based on which the user is requested to make choices to complement the knowledge transposition rules programmed into the model-builder software. Our objective was also that of presenting a graphic display of the "source" and "target" object spaces, to allow the realization by the user of the spatial relationships of the object that populate both spaces.

8.1 Design of the PROLOGRAF-B Workstation Interface

In parallel with the definition of model-builder procedures and rules, an attempt has been made to define some of the desirable functional features that could be implemented in a PROLOGRAF-B workstation environment beyond the initial demonstration level discussed in the previous subsection. The objective of this activity has been both to assess the feasibility of designing such a workstation and to explore the features that it should contain. The design of an "intelligent diagram editor" to facilitate the construction of both source and target object space models has been developed.

The diagram editing interface should provide four primary functions. The first is the ability to construct an object, i.e. an icon with user defined features. The icon is comprised of a bit map within a closed geometric object having active connections (i.e. "pins") on its perimeter. In addition, a knowledge base may be assigned to the object, so that there exists both a rule structure and a data base for each particular icon. The second capability of the diagram editor is the ability to lay down an instance of the icon in a workspace. This instance represents a specific entity. The third capability is that of interconnecting the entities to create a diagram. These connections can only be made between pins; the system recognizes which entities are interconnected and through which specific pins. The pins themselves have the capacity to represent information. The final capability is the ability to create and populate a knowledge base associated with the icon specifically assigned to a component. These knowledge bases can perform the function of an expert system or a method (procedure) when activated so that a person using the diagram editor can be guided through the correct sequence of model building steps.

The P&ID of a system is created by connecting specific instances of standard component and connector types provided in the diagram editor icon library. Consistently with the procedures already discussed, within which the workstation interface is to be operated, two distinct menus are assigned to each icon. The first is a process variable list. As was already discussed in the section dedicated to the description of the PROLOGRAF-B model-building procedures, a pump may be assigned flow rate or discharge pressure; an electric motor may be assigned voltage, current or rpm; and a sensor may read level, flow rate, temperature etc. In addition, this menu may describe the steady-state condition for the component, e.g. valve 20% or 70% open, or valve closed. The second menu can be used to list "standard" component faults, in accordance with the general procedural definitions discussed in Section 6.4.4. For a valve actuator, a fault menu may include failure to open on demand, failure to close on demand, inadvertent opening, and inadvertent closure. A valve controller would have an analogous set of failure modes.

According to the principles also expressed in Sections 6.4.4, the fault menu would also apply to component connectors. For an electric line connector, the fault menu list could include "short" or "open" and for a pipe it could include small or large leak, small or large break, or obstruction.

Once the physical model is constructed, a rule based system enforcing the procedures described in Sections 6 and the information input by the user, can translate the P&ID diagram into an LFM representation. To each physical icon, a set of LFM "node icons" would be assignable, since the LFM process variables can be seen as attributes of the P&ID objects. The model-builder program performs the transformation in a mathematical sheet, according to the encoded model-building procedures and to user-input information, and lays down and draws

LFM objects and interconnection edges on the screen. This is essentially done at each intermediate step of the physical-model-to-LFM-model transformation, to allow the user to have a direct synthetic view and feedback on the effect of his/her interaction with the model builder code. The LFM model eventually obtained from this interaction depicts the cause-effect constraint propagation mechanism of the process or the system being analyzed, which in turn can be analytically interpreted by the LFM inference software which has been presented and discussed in Refs. [4-6].

8.2. PROLGRAF-B Software Prototype Demonstration

The PROLGRAF-B software prototype implements and demonstrates the LFM model building procedures described in Section 6, up to the point of generating in a graphic page the realization of an LFM model for a given process system (not inclusive of fault representation). The implemented steps (1 through 9) are :

1. identify basic devices and components (e.g., pumps, valves, heat exchangers, etc.) in the piping and instrumentation diagram (P&ID) of the process to be modeled;
2. identify device and component "connectors" (e.g., pipes, wires, pneumatic lines, etc.) in P&ID;
3. identify essential parameters characterizing the functionality of each component (e.g., pressure, flowrate, temperature, etc.);
4. recognize and identify direct cause and effect relations among parameters within each P&ID-represented component;
5. recognize and identify direct cause and effect relations among parameters across separate P&ID-represented components;

6. define state representation vectors for all variable nodes identified in the model;
7. define transfer functions corresponding to all causal relations identified in the model and representing how mutual influences among modeled process variable can propagate along the LFM model;
8. recognize and identify multiple interactions among "input" parameters which determine the state of "output" parameters (process feedback and feedforward effects can be treated as subcases of such interactions).

Figure 8.1 shows the computer realization of the P&ID of the simple "pump and valve" subsystem used as the test case of our research. This realization is not as trivial as it may appear on paper, as it derives from the following knowledge base which has explicitly been incorporated in the model building software environment:

- a. a library of P&ID component/device icons, tagged according to function as either "primary components", "control components", or "sensors";
- b.- a color-coded identification of component connectors as either "power connectors" (i.e., connectors whose primary function is to allow the transmission of energy and or mass from component to component), or "control connectors" (i.e., connectors whose primary function is to allow the transmission of sensor/control signals from component to component).

Figure 8.1: PROLOGRAF-B Software Realization of Subsystem P&ID

P&ID knowledge base elements a and b are useful because they allow the identification of process feedback and feedforward function that have to be later transposed into the LFM object representation space.

From a P&ID representation like the one shown in Fig. 8.1 the user can proceed to "mouse" on each represented component to initiate the transposition of that component into the LFM representation space. This can be done by following optionally either of two different routes:

- the first one allows a "custom" definition of an LFM mini-model for the selected P&ID component, by executing the PROLOGRAF-B model building Steps 3 and 4 listed above and following very closely the procedures described in full detail in Section 6;
- the second one allows the automatic (i.e., software executed) "expansion" of the P&ID component into an LFM mini-model which has been previously defined

and stored as a "standard definition" for that component; Fig. 8.2 and Fig. 8.3 show respectively the PROLOGRAF-B menu where either alternative route can be selected (DM and EX menu items in Fig. 8.2) and the result of the automated expansion of the component "Control Valve" into the three causally linked parameters "Control Valve command" (CVc), "Control Valve (stem) position" (CVp) and "Control Valve flowrate" (CVf).

Figure 8.2: PROLOGRAF-B Menu for PI&D - LFM Translation Activities

Figure 8.3: PROLGRAF-B Expansion of P&ID Control Valve Component into LFM Mini-model

The remaining steps of the PROLGRAF-B model building procedures listed above are executed by the prototype software almost exactly as they have been defined in Section 6. Once an LFM model has been laid down in the PROLGRAF-B LFM graphic page, essential data that need to be attached to the various LFM graphic elements in order to make the model complete can be entered by selecting a data entering "activity" from a menu and then "mousing" on the graphic element of interest. Figure 8.4, for instance, shows a menu where the activity to enter data regarding LFM "multiple transfer functions" (MTFs; see Section 4 for discussion of this type of LFM element) can be selected. After choosing that activity the "clicking" of the mouse on any of the MTFs laid down in the LFM graphic model page will bring up on the screen a predesigned data-form (or series of data-forms) where the data applicable to the selected MTF may be entered. Figure 8.5 shows the data-form for the MTF, in this case expressed

more simply as a "multiple gain box" (MGB), which expresses the causality flow and mapping of states from the pump flowrate (Pf) to the valve flowrate (CVf) LFM variables. Similar forms can be called up to define the LFM variable states themselves and the "non-linear input interaction operator" (NIIO) matrices (again, refer to Section 4 for discussion of NNIOs).

Figure 8.4: PROLOGRAF-B Menu for Execution of MTF Definition and Data Input Activities

<<< MTF / MGB Form >>>

ID:	A_120	DESCRIPTION	Causality link from pump to control valve
TYPE:	MGB1		
LABEL:	Pf-CVf		
INPUT VARIABLE: Pf		NO. OF GAINS: 1	
OUTPUT VARIABLE(S): CVf			
DEFAULT GAIN (# 0):	+1	CONDITION:	n/a
GAIN (# 1):		CONDITION:	
GAIN (# 2):		CONDITION:	
GAIN (# 3):		CONDITION:	
GAIN (# 4):		CONDITION:	

Figure 8.5: PROLGRAF-B Form for MTF/MGB Data Input

9. Conclusions and Possible Future Developments of this Research

The development of the PROLGRAF model builder has progressed satisfactorily well beyond its initial conceptual definition stage. The indications collected in our research have been positive, showing that most of the research objectives have been reached at the realistically achievable demonstration level.

We have successfully completed the software implementation of the procedural steps that were outlined and discussed above in Sections 6, and a prototype software demonstration of the fundamental model-builder functions implemented in those procedures (up to Step 8 included). The development and verification of this "stage one" PROLGRAF-B prototype concept, applied to the simple valve and pump system with feedback discussed above, has essentially allowed us to ascertain the feasibility of a semiautomated construction of process models in LFM format, which effectively express the functional cause-effect and physical relationships in a plant process of interest.

If research activities can be in the near future continued in this area, the software "stage one" prototype could be extended in a reasonably straightforward fashion into a second stage demo.

In this second stage of development the PROLGRAF-B prototype software could be developed to include the model building procedures designed and discussed in Section 6, Steps 9 through 14, covering the effect of process faults and mode-changes on the normal process parameter states and causality relations. This would correspond to the last model building stage (Fault and Causality Conditioning Specification) of the four which were earlier identified and listed in Section 6 of this report. A family of codes, including the "stage one" and "stage two" PROLGRAF-B software as well as the LFM inference engine discussed in Refs. [4-6], could form the embryo of future production-level software packages which would make possible the computer-aided reliability and process operation analysis of complex engineering systems. We believe that the research that we have just completed represents an important step forward along the difficult path leading to the achievement of that objective.

References

1. S. Guarro: "PROLGRAF-B: A Knowledge-based System for the Automated Construction of Nuclear Plant Diagnostic Models", in Technical Progress Report for period Sep. 1987 - March 1988 (by D. Okrent and G. Apostolakis) for DOE Award No. DE-FG03-UCLA, March 1988
2. A.B. Long: "Technical Assessment of Disturbance Analysis Systems", Nuclear Safety, Vol. 21, No. 1, 1980
3. D.G. Cain: "Review of Trends in Computerized Systems for Operator Support", Nuclear Safety, Vol. 27, No. 4, 1986
4. S. Guarro, D. Okrent: "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", UCLA-ENG 8507, Jan. 1986
5. S.B. Guarro, D. Okrent: "The Logic Flowgraph: a New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", Nuclear Technology, Vol. 67, Dec. 1984

6. S.B. Guarro, D. Okrent: "Use of Logic Flowgraph Models in a Computer Aided Process Analysis and Management System", Proc. of the 1985 International Topical Meeting on Computer Applications for Nuclear Power Plant Operation and Control, Tri-Cities (Pasco), WA, Sep. 8-12, 1985

3. A KNOWLEDGE-BASED MAINTENANCE-ADVISOR PROTOTYPE

Shimshon Arueti

1. Background

The decision making process as it relates to a nuclear power plant is complex and of considerable impact on the quality and cost of plant operation. Factors that contribute to the nature of this process are inherent complexity of plant technology and the high cost of either plant shutdown for maintenance or failure to perform a necessary maintenance. Direct maintenance cost, indirect costs such as power replacement and, more importantly, safety implications must all be taken into account.

The process is complicated by the existence of a set of deterministic constraints such as plant technical specifications, operating and maintenance procedures, and initial conditions such as refueling outages, LCOs, and peaks in electricity demand. Within these constraints plant management has to decide whether or not to perform a maintenance activity, based on considerations of best timing and optimal benefit. Of particular interest is preventive maintenance (PM) scheduling, since a good PM program can not only minimize maintenance cost, but also have a significant effect on plant operations as a whole.

Despite the importance and the complexity of the maintenance task, it is currently carried out, in most cases, with insufficient methods and tools. Based on private communications and on references such as Morgenstern et al. (1986) and Jeffries (1986) it seems that most maintenance programs have the following characteristics:

- a. PM programs are based mainly on deterministic time constraints such as manufacturer recommendations, technical specifications, etc.
- b. In some specific cases vibration monitors are used for prediction of problems.
- c. The decision process very often contains ad-hoc decisions.

Morgenstern et al (1986) stresses that "Vendor-generated information provides the technical basis for most maintenance activities and is the primary source of technical information for writing and updating detailed maintenance procedures on safety-related and balance-of-plant equipment", and that "Discussion with maintenance supervisors revealed that the unavailability and poor quality of vendor information is widespread and not limited to one or few vendors."

Jeffries (1986) reports, among other topics, on the consequences of such practices. He states that "While measured plant performance has improved overall since 1980, the maintenance related contribution to reportable events and challenges to safety systems remains high and is increasing by some measures."

Two methods for PM optimization have been developed in the recent years under EPRI sponsorship. The first method [Perla et al. (1984), Walker (1987)] performs cost/benefit analysis of each analyzed equipment. It is based on identifying important plant equipment and predicting its future performance with and without changes in the regularly scheduled maintenance program.

The second approach is the Reliability-Centered Maintenance (RCM) [Hook et al. (1987), Vasudevan et al. (1985), Crelin et al. (1986)]. The methodology was

adopted from the commercial air transport industry. It is based on a series of orderly steps, including identification of system/subsystem functions and failure modes, prioritization of failures and failure modes (using a decision logic tree), and finally selection of PM tasks that are both applicable (i.e. have the potential of reducing failure rate) and effective (i.e. economically worth doing).

2. Objectives

The objective of the current study was to develop methodology and design and implement a prototype tool, the Maintenance Advisor, based on this methodology which would assist the scheduling and decision making for performance of PM activities in a nuclear plant, based on probabilistic judgment and probabilistic inference rules. Using probabilistic data on failure rates, repair times, repair costs and indirect economic costs, and within the imposed deterministic constraints, the program develops an optimum (minimum expected cost) maintenance schedule for the various pieces of equipment described by the model.

Included in the decision making are plant and system level probabilistic and deterministic data such as core damage frequency, expected core damage cost, probability of plant shutdown due to limited conditions for operation (LCO), planned refueling shutdown, etc.

The data base for the prototype consists of the auxiliary feedwater system (AFWS) of a pressurized water reactor and is designed to be easily expandable to the whole plant, as well as transferable to other types of plants, e.g. other nuclear plants, chemical facilities, etc.

The decision tool utilizes modern programming techniques, mainly artificial intelligence (AI) techniques, and a built in structure of the related systems and components.

The tool is designed to optimize preventive maintenance activities based on minimum expected cost analysis.

3. Terminology and Some Key Assumptions

- a. For the purpose of this study PM consists of all those maintenance jobs that are scheduled prior to any failure detection, which are not minor and are not regularly performed by the operational staff (such as daily inspections, equipment lubrication, etc.).
- b. The strategy of the program is to minimize "cycle specific cost" (cost per unit-time) in which both scheduled PM and unscheduled expected corrective maintenance (CM) are accounted for, as well as indirect costs such as economic cost of plant shutdown and safety related expected cost due to a potential accident.
- c. The main parameter that makes PM cost beneficial is parts aging, which results in increasing failure rate over time. On the other hand, both the potential for human error during maintenance and direct and indirect maintenance costs make it undesirable to perform unnecessary PM. These two effects are represented in the form of a "bathtub" time dependence distribution, with the first peak representing the increased failure rate at the beginning of a cycle due to maintenance errors, while the second peak represents aging.

- d. The benefit of performing PM during outages (as opposed to PM during operation) is represented by two major factors: reduced direct costs and reduced system unavailability which is reflected in lower indirect costs.
- e. Corrective repair costs, unavailability, and other probabilistic parameters are computed in terms of their expected values.

4. Methodology

The study developed methodology for optimizing PM in order to achieve minimum plant operating cost. The parameters involved in the optimization are not only those related directly to PM (such as cost and repair time), but rather a variety of operating parameters such as refueling outages schedule, component failure rates and repair times, cost and probability of an accident involving core damage, economic cost of a shutdown, LCO requirements, and many others. The PM schedule is considered, therefore, as one variable in a much broader problem of optimizing operational costs.

The methodology involved research and some unique developments in three distinct areas: cost optimization, probabilistic data analysis and knowledge representation.

4.1 Cost Optimization

The approach taken in the current study is an automatic one-step analysis, which is based on selection of PM intervals for each analyzed equipment, as opposed to selection of equipment to be maintained at a given time. The method can be titled "minimizing system cycle specific cost", and some of its main characteristics are:

- The variable to be minimized is expected cost per unit-time (specific cost).
- The parameters for the optimization process are mostly probabilistic.
- The method accounts for operational cost parameters in their most generic sense, and not only for variables that are directly attributable to PM cost.
- Systems, subsystems and components are not analyzed individually, but rather in the context of a complete system. Their interrelations are vital parameters for the optimization process.
- The computation is performed recursively, such that the system specific cost is minimized based on minimum subsystem specific costs, which themselves are based on minimized component specific costs.

The block diagram in Figure 1 describes the process of optimizing the PM scenario of any equipment. It is first applied to the top level equipment, which is in our case the AFWS. During the computation it is then applied recursively to the various subsystems and components of that system.

First (block [5]) the specific cost $C_{m=1}$ of the AFWS is computed for exactly one PM per cycle (during outage) and $C_{m=2}$ for an alternative cycle with one PM every two cycles. The cost is computed in each case by using the function described in the block diagram of Figure 2. This function, in turn (in block [8]) optimizes the scenario of the AFWS subsystems using again the function described in Figure 1. This recursive process continues until the components' scenarios are optimized, and their optimum costs are used for the optimization of the subsystems and the system.

If $C_{m=1} > C_{m=2}$, $C_{m=2}$ becomes the optimal specific cost, m is increased and new alternative specific cost is computed. This process continues until $C_{m+1} > C_m$ or until $m = \text{maximum number of cycles}$. C_m is then returned as the optimum specific cost (in block [13]).

If $C_{m=1} \leq C_{m=2}$ it is assumed that further increase of m will not bring any cost reduction. $C_{m=1}$ is then compared with $C_{n=2}$, the specific cost with two PMs per cycle. If again $C_{m=1} < C_{n=2}$, $C_{m=1}$ is declared the optimum cost, and $m=1$ is the optimum scenario. If, on the other hand, $C_{n=2} < C_{m=1}$, $C_{n=2}$ becomes the optimum specific cost, and n is increased until a point is reached when $C_{n+1} \geq C_n$ and C_n is returned as the value of the optimum specific cost (in block [18]).

When a component PM scenario is computed, there is no more recursive branching to lower level equipment. The cost is computed by block [5] in Figure 2. This computation is described by the function tree in Figure 3.

4.2. Bayesian Data Analysis

Data analysis for the probabilistic parameters, including failure rates, repair times and costs are based on Bayesian probability theory. Some modifications and generalization [Arueti and Apostolakis (1987)] added to the process more flexibility, less dependence on subjective prior probabilities, and in our opinion, more reliable interpretation of the available data. The process is based on having layers of objects, each layer containing cases of objects in the previous (higher level) layer. With this arrangement data can be attributed to any layer, depending on the details available on the data, and results can be obtained from each layer, depending on the specific application. Information is propagated between various layers, such that high level object variability distributions serve as a generic prior distributions for lower levels, while data from all lower levels are combined to create high level variability distributions.

Figure 1 Flow Diagram of the Cost Optimization

Figure 2 Function Tree for Computing Component Total Specific Cost

Figure 3 Hierarchical Structure for Valves

As an example, assume the valve hierarchy in Figure 4 below. Motor operated valve (MOV) becomes a special case of "Valves" when the operator of the valve is specified as "electric motor". In terms of the data analysis, the default option for the prior distribution of "MOV" failure rates, for example, is the "valves" failure rate distribution. If no other distribution is supplied by the user, the "valves" distribution is updated with "MOV" specific data (using Bayes' Theorem) to obtain "MOV"'s posterior distribution.

If the "MOV" had more than one parent (e.g.) "valves" and "motor operated equipment" for this example), the user would be able to choose any linear combination of the parent distribution as a prior distribution for "MOV", or to supply a new one.

Figure 4 Flow Diagram of Equipment Specific Cost Computation

Although not applied in the Maintenance Advisor prototype, the formulation allows development of high level object variability distributions from a combination of the lower level distributions.

4.3. Knowledge Representation

The Maintenance Advisor is a frame-based [Minsky (1985), Fikes and Kehler (1985)] object-oriented [Stefic and Bobrow (1986)] program. Equipment and other objects are represented as complex units, each of which contains in its own frame a complete set of characteristics (e.g. function, driver, operating environment), data (e.g. failure rate, repair time and cost, etc.) and functional capabilities (e.g. update and plot distributions). These are all represented as unit-slots.

4.3.1. Equipment Hierarchical Relations

The plant equipment are organized in two hierarchies: The TYPE-OF hierarchy in which each instance in a lower level is a special case of an instance in an upper level, and the PART-OF hierarchy in which each instance in the upper level contains instances in the lower level. The logical relations between lower and upper level equipment in the PART-OF hierarchy are defined via logic block diagrams attached to the various pieces of equipment.

Each equipment can identify its descendants in the PART-OF hierarchy via pointers to the descendant units which are attached to its &CONTAINS slot. The pointer references are preceded by an operator that defines the relations between the descendants. Similarly the &CONTAINED-IN slot of each equipment-unit contains a pointer to its ancestor unit.

Figure 5 below is an example of the &CONTAINED-IN slots of the unit AFWS-A-8 in the MAINTENANCE-ADVISOR knowledge base. The ancestor-unit of AFWS-A-8 is AFWS-TRAIN-A2. AFWS-A-8 has three descendants in the PART-OF hierarchy, which are: PIPE-A-8, AFW-PUMP-#-11, and AFW-PUMP-#-11-MOTOR. The descendants are contained in AFWS-A-8 as logically serial units. This relation is imposed by the operator SER that precedes them in the &CONTAINS slot value.

Figure 5 The &CONTAINS and &CONTAINED-IN Slots of AFWS-A-8

Figure 6 is an example of the TYPE-OF hierarchy of pumps in the Maintenance Advisor.

The only system included in the current implementation of the Maintenance Advisor prototype is the auxiliary feedwater system (AFWS) of a pressurized water reactor. The program is flexible enough to allow for future extension by adding both systems to the plant model and components to the current simplified system model.

Figure 6 The Maintenance Advisor's Pumps TYPE-OF Hierarchy

4.3.2 Enhancements to Knowledge Representation

The "Maintenance-Advisor" is constructed with the KEE [Intellicorp (1986)] utilizing additional LISP functions. The inherent KEE frame and object oriented programming orientations are broadly used in the program, but in many cases they have been found insufficient for our purposes. In order to be able to deal with the variety of parameters involved in the decision process it was necessary to add reasoning power to the underlining KEE shell, mainly because of the use of distributions for data analysis and the need for specific logical relations in the form of logic block diagrams. Several generalizations and specific developments have been accomplished for that purpose, two of which are:

- a. a "probabilistic inheritance" wherein the basic parent-child inheritance relations have been generalized such that a child-unit can inherit a combination of probability distributions from all its parent-units and from a local value. The simple "Override-Values" inheritance-role becomes a special case of the "Probabilistic Inheritance" role. Although not implemented in the prototype, the formulation allows for further generalization of this

role by making it bi-directional, such that information from all child units will be available for developing the prior distribution of a parent unit; and

- b. an additional propagation network, which has been developed for propagation of knowledge along the PART-OF hierarchy. Its application is similar to that of the regular inheritance roles in the TYPE-OF hierarchy, except that it uses the block diagrams as a means for combining information to be inherited along the PART-OF hierarchy.

5. Implementation and Results

The concepts described above have been implemented in the Maintenance-Advisor knowledge based prototype, whose goal is to prove the concept and to test the sensitivity to various parameters.

A set of parametric runs were executed on the Maintenance Advisor. The results of these runs demonstrate that the method is effective in modeling a variety of operational variables, including safety related and economical variables, and that it can be tuned such that one variable (e.g. safety) will be emphasized versus the others. The method can also be used to check, and if necessary modify, the appropriateness of regulatory requirements. One of the findings of the parameter study was that in certain conditions the current LCO requirements compete with the maximum availability requirement, rather than enhancing it.

And finally, the current implementation is just a subset of a full scope operational tool. Many parameters have not been included, or have been included in part, and the data used is a mixture of generic data, data adopted from various unrelated sources, and simple "intelligent guesses".

6. Conclusions

The Maintenance-Advisor is a prototype knowledge-based system using probabilistic inferences to optimize preventive maintenance scheduling of a (nuclear) plant. The Advisor uses a Bayesian approach for data analysis and object oriented programming as its underlying programming method.

Among the methodological foundations developed around the program are:

1. A "minimal expected specific cost" approach to cost/benefit analysis for maintenance scheduling.
2. A hierarchical approach to data analysis based on Bayes Theorem and on Generalization and Specialization of distributions.
3. Generalization of KEE-based knowledge propagation, inheritance and storage techniques, among which are "probabilistic inheritance" and "block diagram based inheritance".

The way in which the Maintenance-Advisor analyzes probabilistic data and performs systems analysis makes it an example of probabilistic safety analysis (PSA) application for plant operation.

7. References

Arueti, S. and G. Apostolakis (1987), "PRA-Based Data Analysis for Use in Computerized Decision Aids," presented at The American Nuclear Society Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, UT, August 31 - September 2.

Crellin, G.L. et al. (1986), "Use of Reliability-Centered Maintenance for the McGuire Nuclear Station Feedwater System," EPRI NP-4795, prepared by Los Alamos Technical Associates, Inc. and Saratoga Engineering Consultants, Inc.

Hook, T.G. et al. (1987), "Application of Reliability-Centered Maintenance to San Onofre Units 2 & 3 Auxiliary Feedwater System," EPRI NP-5430, prepared by ERIN Engineering and Research Inc.

IntelliCorp (1986), "KEE) Software Development System User's Manual."

Jeffries, A.J. (1986), "Status of Maintenance in the Nuclear Industry - NUREG-1212," Memorandum to G.A. Reed, ACRS Subcommittee Chairman on Maintenance Practices, August 7.

Minsky, M. (1985), "A Framework for Representing Knowledge," in Readings in Knowledge Representation, R.J. Brachman and H.J. Levesque, editors, Morgan Kaufmann.

Morgenstern, M.H. et al. (1986), "Improving the Development, Use, and Control of Maintenance Procedures," Proceedings of the ANS International Meeting on Nuclear Power Plant Maintenance, Salt Lake City, UT, March 23-27.

Perla, H.F. et al. (1984), "A Guide for Developing Preventive Maintenance Programs in Electric Power Plants," EPRI NP-3416, prepared by Pickard, Lowe and Garrick, Inc.

Vasudevan, R. et al. (1985), "Application of Reliability-Centered Maintenance to Component Cooling-Water System at Turkey Point Units 3 and 4," EPRI NP-4271, prepared by Los Alamos Technical Associates, Inc.

Walker, I. (1987), "Development of a Maintenance Program," Proceedings of the 14th Inte-ram Conference, Toronto, Ontario, Canada, May 26-29.

4. AN EXPERT SYSTEM FOR FINDING FRAGILITY CURVES OF BUILDING STRUCTURAL SYSTEMS IN THE PRELIMINARY DESIGN STAGE

Lone-Yee Yee

1. Introduction

Seismic fragility is one of the most important factors for identifying the safety of civil structures, especially structures in the nuclear power plant industry. Not only is seismic fragility required for probabilistic risk assessment investigations, but also it may have an impact on the design, because unsatisfactory parts of a completed structure may be very difficult or expensive to modify. Seismic fragility is therefore one of the key constraints in the structural design process. In the past decade, a number of probabilistic risk assessment studies have been conducted [1-6]; however, the seismic fragility function had not been considered in designing the building structural system, especially in the preliminary design stage.

This research is a starting point for the development of an expert system for determining seismic fragility curves of structural systems in a nuclear power plant or conventional building at the preliminary design stage. The resulting system will assist an engineer with moderate engineering background and limited reliability knowledge to analyze the failure functions of building structures. It simulates the performance of an expert in identifying the potential failure modes and their variabilities for a structure of interest. Then, by combining the stress results of crude analyses, the method of linear statistical model, and the methodology developed by Kennedy [Kennedy et al., 1980, 1984], the fragility curves of the structure will be estimated.

2. Background

The seismic fragility function is the distribution function of capacity or conditional failure probability associated with a specified limit state. In addition, the capacity is generally represented as a function of loading parameters such as effective peak ground acceleration or local response factors. Therefore, the probability of failure for a specified limit state may be given by Eq. (1)

$$P_f = \int_{-\infty}^{\infty} F_R(s) f_s(s) ds \quad (1)$$

where P_f = the probability of failure for a limit state

$F_R(s)$ = the fragility function represented to loading parameter, s

$f_s(s)$ = the density function of loading parameter, s

However, due to the unexact nature of the data, the incomplete knowledge of the problem and approximations in development of the analytic model, the exact fragility function associated with a limit state is unknown. In other words, uncertainty [7] exists for the estimated fragility function; therefore, the rational way to represent it is a family of fragility curves.

Currently, there are two approaches to estimate the seismic fragility functions of complex engineering systems. One approach is to use a combination of the opinions of many experts to estimate the fragility functions without performing any sophisticated analysis [8-11]. The other is to use one or two expert judgments plus the help of detailed structural analyses to estimate the seismic fragility functions [1-6]. Depending on the purpose of, financial resources, available information and knowledge related to the target problem,

Loading Factor or Response Parameter S

Figure 1. A Simplified Representation of Fragility Curves

either one of these two approaches can be chosen. However, the former is usually selected to estimate a family of generic fragility curves related to a whole industry or a subgroup in an industry. On the other hand, to evaluate the plant specific fragility curves, the latter is often employed.

Although the generic fragility curves will provide valuable information to the emergency management agency or building code authority to perform risk assessment or to improve the current practice in an industry or a subgroup of an industry, they will be too broad to be useful in seismic probabilistic risk assessment associated with a specific nuclear power plant or a conventional building. Knowledge of the specific fragility function associated with a building structural system is necessary in order to assist an engineer or designer in removing potentially poor design aspect at the preliminary design stage. It could also be useful if one were attempting to design a structure or plant to have a balance or fairly uniform seismic capability.

3. An Overview of the Knowledge Base Expert Systems

The essential feature of a knowledge base expert system is that it consists of two parts: the knowledge base and the inference engine. The knowledge base contains all the available expertise and facts related to the target problem. On the other hand, the inference engine provides the tools to solve the problem by firing the expertise and facts implemented in the knowledge base. The success of this manipulated programming technique provides a way to computerize the human expert judgment and experience used for solving a problem which is incompletely designed [12-21].

Because the knowledge related to the ill-formed problem is generally incomplete, there will be no way to deduce the conclusion precisely. Most of

the existing knowledge base expert systems have developed a specific method to handle the inexact reasoning inference process. Depending on the purpose and specific features of the target problem, the uncertainty may be treated as a possibility or probability. In this research, the certainty factor will be treated as a weighting factor to estimate the average value of the inexact data or the coherence of the results estimated by empirical formulas. High accuracy of the certainty factor is unnecessary when one treats it as a weighting factor.

4. Problem Analysis

On reviewing the methodology of seismic fragility evaluation for existing building structural systems in the nuclear power plant industry, one finds that the investigation process starts with the identification of critical components or substructures, whose failure will result in the functional failure of safety related equipment or the failure of structural integrity itself, and follows with complicated numerical analyses to estimate the capacity functions associated with the limit states of these selected components or substructures [1-6]. The identification of the critical component or substructures is conducted by a complex decision process in the expert's head with the help of plant specific data and detailed stress results. The estimation of the quantitative value of the fragility often relies on expert judgment of the analysis result in order to get a meaningful answer. However, to estimate the fragility curves of building structural system at the preliminary design stage, some modifications of this investigation procedure are necessary because none of the plant specific data, detailed stress results, and complicated structural analyses are available.

Although each building structure is a complex and unique system, it generally is designed inside the design envelop. In other words, the behavior

of a building structure under earthquakes is predictable with some uncertainties. Hence, some common aspects will exist for buildings designed with the same structural conceptions. Based on these common aspects, the attributes to describe the characteristics of the structural behavior under seismic conditions may be deduced. Once a set of values to describe each attribute has been defined, a building structure may be represented as the hierarchy of pattern spaces configured from these attributes and their values. Under this representation, the complex decision-making process for the identification of critical components or substructures can be decomposed into several simpler hierarchical subproblems; for this reason, they may be identified by diagnosing the values of attributes without performing any numerical analysis.

The local responses, however, are needed in order to estimate the quantitative value of the capacity function for the selected components or substructures. For getting these local responses, some crude stress analysis schemes will be employed. These crude schemes are the same as the tools used in the preliminary design stage by senior engineers for their everyday job. However, there are some limitations of these methods; therefore, obtaining reasonable results for the local responses will rely on engineer's judgment. In fact, the median values and variabilities of the response factor and its subfactors [Kennedy et al., 1980, 1984] cannot be evaluated by these methods. Fortunately, some common aspects exist because these factors or subfactors describe the global behavior of a structural system under seismic conditions. Therefore, meaningful results of these parameters may be found based on expert diagnosis of the attributes and their values, corresponding to these common aspects.

Figure 2 depicts a hierarchical diagram for seismic fragility investigation of building structural systems. Based on this hierarchical representation, not

only the related attributes could be defined but also the procedure of a systematic way to represent the knowledge would be developed. The procedure associated with critical components identifications may be written as a sequence of nine steps:

- (1) Classify the potential structural configurations into different structural system categories.
- (2) Define the attributes and their values to describe the essential features of structural configurations.
- (3) Use expert opinions to develop rules to assign buildings into the corresponding structural system categories.
- (4) Define the attributes and their values for each structural system to describe the dynamic characteristics of this system.
- (5) Use expert opinions to develop rules to describe the dynamic behavior of each structural system.
- (6) Use expert opinions to develop rules to identify the critical stick or sticks and weak link or links between sticks.
- (7) Define the attributes and their values to describe the capacity distribution per each stick or each link.
- (8) Use expert opinions to develop rules to identify the weakest component associated with critical stick or link.
- (9) Use expert opinions to develop rules to identify the potential failure modes associated with soil-foundation system.

where

UBC: Uniform Building Code;	TB : Turbine Building
M : Magnitude;	S : Symmetry
RC : Reinforced Concrete;	SF : Soil Foundation System
H : Horizontal Subsystem;	V : Vertical Subsystem
MF : Mat Foundation;	R : Rigid
SW : Shear Wall	

Figure 2. A Hierarchical Diagram for Seismic Fragility Investigation

Similarly, the procedure for estimating these parameters associated with fragility evaluation may be written as follows:

- (1) Collect the generic statistical data for material properties, size variability and model uncertainty.
- (2) Use expert opinions to develop rules to translate the generic data into a plant specific data.
- (3) Review the literature and reports; for example, the existing reports for probabilistic risk assessments.
- (4) Use expert opinions to develop rules for using the results in items (1) and (3) to estimate the uncertainty or randomness of these factors or their sub-factors.
- (5) Use expert opinions to define the potential loading distribution under seismic conditions.
- (6) Use expert opinions to choose crude numerical schemes to estimate the local response of a selected component.
- (7) Use expert opinions and information of design criteria and the result in (f) to estimate the possible configuration of the selected component.
- (8) Use expert opinions to estimate the mean values and variabilities of these parameters.
- (9) Apply Kennedy's model to estimate the capacity function.

According to references [1-6], the mathematical model used to estimate the quantitative result of seismic fragility associated with a selected element is written as Eq. (2)

$$A = A_D F_S F_\mu F_R \quad (2)$$

where

A = the seismic fragility function with respect to (effective) peak ground acceleration.

A_D = design peak ground acceleration

F_S = factor accounting for the ratio of actual strength to design (or reference) load effect

F_μ = factor accounting for the inelastic energy absorption capacity

F_R = factor accounting for the ratio of design (or reference) load effect to true load effect

5. Methodology and Assumptions

According to past experience [22-27], the damage of building systems caused by earthquakes will usually be concentrated on the weakest story or stories. Hence, identification of the critical stories will be the first step for seismic fragility evaluation. In this identification process, knowledge of the relative capacity-demand ratio for each story will be essential. The attributes or parameters to describe this ratio may be deduced as the cross sectional area of the vertical subsystem, the cross sectional area second moment inertia of the vertical subsystem, the material properties, the weight at each floor, the cut-out percentage of each floor, and the assumed or possible shape of the seismic load distribution [28-31] for each story. Although the relative capacity-demand ratio for each story may not be fully determined by these attributes, a

plausible result for critical story identification can be achieved, using engineering judgment. Also, the values of these attributes are available or predictable without performing any structural analysis; for this reason, it will be possible to identify the critical stories in the preliminary design stage.

Because a building structure is, generally, a highly redundant system, how to estimate the seismic fragility functions of the weakest stories will be the other critical point for developing this expert system. Without performing any detailed and complicated numerical analysis, it would be a very difficult task to estimate the seismic fragility functions because they are derived from the combination of the conditional failure probabilities of the corresponding potential failure modes associated with the critical story. To remove this difficulty, the following methodologies and assumptions are introduced in the development of this expert system.

Elements at each story, especially at the critical story, will be categorized into several groups. All elements inside the group will be assumed to exhibit the same failure characteristics under seismic conditions. In other words, if the failure mode of one element is shear failure, then the other elements inside the group will also fail by shear. Consequently, the differences of the conditional failure probabilities between the elements inside the group can be assumed to be insignificant, especially for estimating the seismic fragility at the preliminary design stage. Hence, the seismic fragility function of the weakest group will be inferred from the fragility function of the element inside it. Moreover, it is assumed that the failure of any group will result in serious damage at the corresponding story. Therefore, the seismic fragility function of the critical story or the whole building will be derived from the fragility of the weakest group related to that story.

The essential task in developing this expert system will be to deduce the attributes which describe the failure characteristics related to each group without the use of structural analysis or detailed response. For example, in considering the failure characteristics of reinforced concrete columns, the limit states could be evaluated as shear failure, bending failure, bending-shear failure, tension shear failure and buckling. All of the limit states are a function of column clear height, condition of connections, material properties, column depth, location of the inflection point, reinforcement configuration and so on. However, if the ratio of column height to column depth is small, then bending failure and buckling would be deduced as the most improbable limit states. Therefore, the ratio of column clear height to column depth or the ratio of column clear height to inter-store height will be deduced as the attribute to describe the failure characteristics of the reinforced concrete column.

The local responses, however, are needed in order to estimate the quantitative values of the fragility functions for the selected elements, groups or substructures. Based on the current methodologies [1-6] for seismic fragility evaluation of an existing building, the fragility function is represented as the multiplication of the strength factor, the inelastic energy absorption factor, and the structural response factor. By considering the statistical behavior of structural material properties and the ratio of actual strength to theoretical value [1-6,32-46], the median value and the corresponding inherent randomness and uncertainties related to the strength factor will be evaluated. To account for inelastic effects, the ductility-modified response spectrum techniques [23,47] were employed based on the system ductility ratio or the ductility ratio of the critical element [1-6,23,26,48,49] (dependent on which one is smaller) for the structural system near the collapse situation. Response spectra techniques [23,44-45,40] were used to estimate the structural response effects.

Damping [23,44,48] expected at failure, the median centered spectra [47-49,51-52] for soil sites from multiple seismic events, the soil-structure interaction effects [52-59], model combinations [1-6,44,45,52], combinations of earthquakes components [1-6,23], and the engineering judgment for the sources of both inherent randomness and uncertainties due to lack of knowledge or approximations were also accounted for in developing this expert system.

6. Knowledge Acquisition and Representation

In this research, there are two different types of knowledge involved. One is the intuition and experience of human experts and the other lies in existing methodologies and empirical formulas. For the former, communication with human experts is essential in order to elicit the knowledge inside their heads. On the other hand, reviewing the literature, reports and papers is a suitable way to collect the existing methodologies and formulas. However, the data types of the elicited or collected knowledge may not in a computer compatible form; for this reason, the task of knowledge representation is necessary. In this task, the knowledge will be represented as a particular data type in order to satisfy the format for implementation of the computer program.

Most of the knowledge related to seismic fragility evaluation is of a functional type. For example, one empirical formula states that the fundamental period of a moment-resisting frame system is proportional to the number of the building stories. In order to rewrite this formula in terms of rules, one would need about ten to twenty rules for covering the range from low to mid-high types or buildings. Thus, the advantage of the functional representation is that a considerable number of data or rules has been replaced by a single formula. On

the other hand, the disadvantage of the functional representation is that the algorithm associated with it will highly correlate and maintain sequential order. Thus, separation of the inference network from the knowledge base and updating the knowledge base will be difficult tasks in developing a functional-type knowledge base expert system.

However, it is almost impossible to estimate the seismic fragility function without performing any functional evaluation, regardless of how complicated or simple the evaluation is. Moreover, most of the parameters, attributes or functions related to fragility evaluation are continuous variables and highly correlated; for this reason, the corresponding rule type knowledge base expert system would be a huge system. Based on the above considerations, a function type knowledge base expert system has been built.

A function consists of three parts: name, arguments and body code. The difficult part in expressing a function in an explicit form is its body code but not its name and arguments. In programming, it is no problem to leave the body code alone after a function has been defined. For example, in FORTRAN programming, a function can be called anywhere inside the program after it has been defined. For the firing of a function correctly, work must be done to correctly match the function name and its arguments. Consequently, the methodology to build a functional type knowledge base expert system involves deducing an auxiliary rule which is made up of the function name and its arguments, and implementing this auxiliary rule in the knowledge base.

Each auxiliary rule is represented in terms of an associated list, which is the data structure related to the frame-like knowledge base expert system. The first element of the list is the value of the name slot, which describes the

name of a variable. The second element of the index slot and the value of this slot will denote the data type of the variable. If the variable is numerical or verbal data, the third element will denote its meaning. The third element will be the arguments or formulas corresponding to the functional type or goal type variable, respectively. In addition, descriptions and cardinalities may be included in the list to make the definition of the variable clearer.

The data related to this research has been classified into four categories. The first category is numerical data, which is represented in term of fuzzy subsets [60,65]. In other words, to each numerical value there has been attached a certainty factor or possibility. The second category is verbal data, which describes the terminologies related to this research. The function will be the third type of data, which may be a rule set or formula. Last is the goal type data which presents the generic name of the associated rules or formulas, and which makes the system capable of deriving the outcome in multiple ways and of updating the functional type of knowledge.

Some auxiliary rules related to this research are shown as follows:

1) Numerical Data

- (ldpf d (live and dead load of each floor for seismic
load evaluation: ksf))
- (papf d (plan area of each floor: sq ft))
- (pocf d (percentage of cut-out per floor area: %))

2) Verbal Data

- (plan-shape s
((R ("rectangular shape.")))

```

(T ("T shape.))
(L ("L shape.))
(I ("I shape.))
(U ("U shape.))
(else ("anything else.)))

```

soil-profile s

```

((S1 ("rock of any characteristics (either shale-like or
      crystalline in nature) or stiff soil conditions
      where the soil depth is less than 200 feet and the
      soil types overlying rock are stable deposits of
      sands, gravels, or stiff clays.))
(S2 ("a profile with deep cohesionless or stiff clay con-
      ditions, including sites where the soil depth exceeds
      200 feet and the soil types overlying rock are
      stable deposits of sands, gravels, or stiff
      clays.))
(S3 ("a profile with soft-stiff to medium-stiff clays and
      sands, characterized by 30 feet or more soft-stiff
      to medium-stiff clays with or without intervening
      layers of sands or other cohesionless soil.))
(V1 ("a profile with shear wave velocity not less than
      500 feet per second.))
(V2 ("a soil layer with shear wave velocity between 1000
      feet per second to 2000 feet per second overlies
      on a bedrock with shear wave velocity not less than
      5000 feet per second.))

```


(unknown ("no knowledge of the soil profile."))

(other ("anything not belonging to the combination of
them."))))

3) Functional Data

- (fwt f (ldpf papf) (floor weight: kips))
- (geomf f (pocf) (floor rigidity effects))

4) Goal Data

- (period1 g (periodg periods1 periods2)
(fixed-base fundamental period estimations of
steel frame))
- (period f g (periodg periodo)
(fixed-base fundamental period estimations of
reinforced concrete wall system))

It is anticipated that updating of knowledge will be easy according to the developed techniques. For example, the procedure to add some new formulas for deriving the associated goal may be written as follows:

1. Rewrite the third element including the names of the new formulas associated with the auxiliary rule of the goal.
2. Write auxiliary rules corresponding to the new formulas and arguments.
3. Put these new auxiliary rules into the knowledge base (anywhere).
4. Define the new formulas and arguments.

Similarly, the same procedure will be used to update any kind of data type related to this study. Figure 3 illustrates the procedure in updating function type of knowledge.

G : Generic Name of Functions F's.

A's : Arguments of Function F2.

Auxiliary Rule : (G g (F1 F2)) Old Rule for G;

: (G g (F2 F3)) New Rule for G;

: (F2 f (A1 A2 A3)) Rule for F2.

Figure 3. A Simplified Diagram for Updating Functional Type of Knowledge

7. Inference Network and Control Strategy

The expertise of seismic fragility evaluation is made up of three parts: expert opinion, analytical modelling, and empirical formulas. The direct coupling of these three parts leads to great difficulty in separating the inference mechanism and the knowledge base. As shown in Figure 4, the procedure to solve the problem is almost rigid, although engineering judgment is essential. To relax the rigidity of the investigation process, the following concept will be introduced:

1. Maintain the sequential order of the investigation process.
2. Assign a 'generic name' to each investigation step.
3. Consider each 'generic name' is a goal statement.
4. Build a knowledge base expert system to derive the outcome associated with each 'generic name'.
5. Apply traditional programming techniques to link all the outcomes associated with each 'generic name'.

Figure 5 presents the hierarchical diagram related to this concept. Based on this concept, the knowledge base, inference mechanism, and control strategy have been successfully separated. Utilization of expertise has been enhanced because functions or empirical formulas can be added to or deleted from the knowledge base.

According to the above statement, the expert system related to seismic fragility evaluation is made up of a series of sub-expert-systems associated with the major steps of the investigation process. Depending on the data type of knowledge to derive the corresponding sub-goal, each associated sub-expert-system may need a different mechanism to accomplish its particular task efficiently. The logic steps related to the investigation process may be too

Figure 4. A Typical Investigation Process Related to Seismic Fragility Evaluation

Figure 5. A Hierarchical Diagram to Present the Concept for Relaxing the Rigidity of Investigation Process

complex to be implemented in the knowledge base. Therefore, it was decided to separate the control strategy and the inference mechanism in developing an expert system related to this research.

In this research, the complicated problem has been decomposed into eight subproblems such as system identification, critical story identification, critical direction identification, critical group identification, critical element (it is a fictitious element to represent the failure mode associated with a group) identification, fixed-based fundamental mode estimation, fundamental mode estimation accounting for soil-structure interaction, and seismic fragility evaluation for the selected element. However, it is important to recognize that most of the sequential order related to this decomposed problem must be maintained. For example, substructure approach is used to estimate the soil-structure interaction effects; consequently, the fixed-based fundamental mode must have been known before the soil-structure interaction effects will be accounted for.

Although the sequential order must be maintained, this decomposed problem presents a general procedure to estimate the seismic fragility functions of building systems. In other words, this sequential order may not need to be updated later if the problem domain does not change. Moreover, the hierarchy of this decomposition presents a clear picture to describe the investigation process for seismic fragility evaluation. Besides, the representation of this investigation process for seismic fragility evaluation of potential building types is analogous to an event tree representation for identifying the potential consequences associated with an accident in a complex engineering system. Also,

the backward chaining process to derive the outcomes of each subproblem is analogous to the fault tree technique to evaluate the top event failure probability resulting from the potential failure modes associated with it. Based on this analogy, the way to expand this investigation process for seismic fragility evaluation of the other types of structural systems will be figured out.

The building system related to seismic fragility evaluation is the same as the initial event in an event tree representation. The consequence resulting from the initial event will depend on the success or failure of the top events associated with the event tree. Similarly, the seismic fragility function of a particular building system will depend on the outcomes of the reduced subproblems which are estimated by the specific knowledge related to this building type. For example, the developed expert system in this research does not contain the knowledge to estimate the seismic fragility function of a cooling-tower structure; therefore, the system will respond that the system is unable to estimate the seismic fragility of this type of structure after the structural type has been identified as a cooling-tower.

A procedure to combine the implementation techniques of a knowledge base expert system and traditional programming has been developed in order to build an expert system for seismic fragility evaluation. Based on this implementation technique, the major sequential order associated with the reduced subproblems was maintained; however, the expertise and facts related to each subproblem have been written in terms of a knowledge base expert system. This design strategy decomposes this complicated problem into a series of simpler subproblems, fires the associated rule sets, fact bases, empirical formulas and tricks to solve the subproblems, and combines the results of these subproblems to estimate the solution. Hence, the domain of search space and the computer time will significantly be reduced.

Figure 6 depicts a schematic view of the expert system for seismic fragility evaluation of building structural systems. This expert system consists of seven components such as control strategy, inference engine, auxiliary rule bases, functions, supporting mechanism for fuzzy set operation, reasoning engine and user interface. The control strategy contains the main logic flow path of the investigation process related to seismic fragility evaluation. It sequentially loads the auxiliary rule bases into the inference engine to explain how to get the result.

After the inference engine is loaded, it will control the whole system until the assigned task is finished. For accomplishing the given task, the inference engine will continuously search, query and execute the right formulas and data. To achieve this inference process, the abstract representation of the functions has been implemented in the auxiliary rule bases. All of the expertise, such as the rules of thumb, engineering judgments and empirical formulas, was represented in terms of functions. The supporting mechanism provides the tools for numerical calculations related to the fuzzy data. Finally, based on the request of the user, the reasoning engine will be fired to explore the reasoning of the outcome.

8. Discussion

In this research, building system identification is an ill-formed part because the expertise to perform this task can not use any analytical modelling or empirical formulas. In other words, the corresponding expert system to do the job of building system identification will be a diagnosis system. Therefore, the knowledge related to this task can be represented in terms of rules. Consequently, we may use a different inference mechanism and different data

Figure 6. A Schematic View of the Expert System for Seismic Fragility Evaluations

structure representation of the knowledge base related to each major investigation step to develop the whole system, if this design strategy is feasible.

Numerical calculation with fuzzy data will, however, create some problems. The first problem is that the computer time will grow exponentially. For example, if a function has five arguments and each of term has five possible (fuzzy) values, the function will be evaluated 3125 times in order to cover all the possible combinations. To remove this difficulty, an ad hoc procedure is introduced in this system. Based on this procedure, the number of possible values of any fuzzy variable will be no more than two, and the number of combinations will be linearly proportional to the number of arguments. One of the two possible values is the value of the fuzzy variable, in which the certainty factor is considered as a weighting factor in order to evaluate the average value.

Another problem arises from the comparison of the values of fuzzy data. For example, comparison of the relative capacity-demand ratio of each story is essential in order to identify the critical story. For this comparison, another ad hoc procedure is introduced. In this procedure, it is assumed that fuzzy data will be a uniform distribution within a range from the minimum possible value to the maximum possible value, in which the minimum value and the maximum value may be equal to the product of the value and its certainty factor and the ratio of the value to its certainty factor, respectively. Finally, if conventional or existing operations are applicable to handle the fuzzy data related to this system, they will also be implemented in the system.

9. Conclusions

A prototype expert system to estimate the seismic fragility functions of steel structures, reinforced concrete structures and their combining structural systems has been built. About 220 functions and 400 rules have been implemented in the system. In this expert system, both nuclear power plant structures and conventional buildings have been considered; however, some special types of structural systems, such as containment structure, cooling-tower structure, underground structure or embedded part of a building system, water tank and high-rise building, are not included. But, it would be no problem to extend the system to cover these special types of structures based on the techniques developed in this research.

The system, which is called SFE (Seismic Fragility Evaluation), was written in the Golden Common Lisp language. However, it would be no problem to run this expert system on other Common Lisp Interpreters because the format used to build this system is compatible with all of them. Moreover, every sentence or statement implemented in this system is in English style; therefore, there should be no problem in understanding it. Following these implemented step by step instructions, a user can use this system without significant training, although some basic knowledge of personal computers and fundamental structural engineering background is essential. Further details can be found in reference [66]. The procedure to estimate the membership function of a function will need further research work.

10. Acknowledgments

The authors wish to acknowledge the expert advice of Dr. R.P. Kennedy. This work was supported in part by the U.S. Department of Energy award No. DE-FG03-86SF-16610.

References

1. Kennedy, R.P., et al., Probabilistic Seismic Safety Study of the Existing Nuclear Power Plant. *Nuc. Engrg. & Des.*, Vol. 59, pp. 315-338, 1980.
2. Kennedy, R.P. and Ravindra, M.K., Seismic Fragilities for Nuclear Power Plant Risk Studies. *Nuc. Engrg. & Des.*, Vol. 79, pp. 49-68, 1984.
3. PG&E Long Term Seismic Program, Methods and Procedures for the Phase IIIA Seismic Fragilities of Structures and Components at the Diablo Canyon Power Plant. 1987.
4. Wesley, D.A., et al., Conditional Probabilities of Seismic Induced Failures for Structures and Components for the Zion Nuclear Generating Station. Zion Safety Study, 1980.
5. Wesley, D.A. and Hashimoto, Seismic Structural Fragility Investigation for the Zion Nuclear Power Plant, NUREG/CR-2320, 1981.
6. Wesley, D.A., et al., Seismic Fragilities of Structures and Components at the Millstone 3 Nuclear Power Station, Millstone 3 Safety Study, 1984.
7. Kaplan, S., and Garrick, B.J., On the Quantitative Definition of Risk. *Risk Analysis*, Vol. 1, pp. 11-27, 1981.
8. Mosleh, A. and G. Apostolakis, G., The Assessment of Probability Distributions from Expert Opinions with an Application to Seismic Fragility Curves. *Risk Analysis*, Vol. 6, No. 4, pp. 447-461, 1986.
9. Morris, P.A., Combining Expert Judgments: A Bayesian Approach. *Man. Sci.*, Vol. 23, pp. 679-693, 1977.
10. Goodman, J., Structural Fragility and Principal of Maximum Entropy. *Structural Safety*, Vol. 3, pp. 37-46, 1985.
11. George, L. and Mensing, R.W., Using Subjective Percentiles and Test Data for Estimating Fragility Functions. Lawrence Livermore National Laboratory, UCRL-84157, 1981.
12. Nilsson, N.J. *Problem Solving Methods in Artificial Intelligence*. McGraw Hill Book Company, 1971.
13. Naylor, C., Build Your Own Expert System. Halsted Press, 1985.
14. Sriram, D., et al., Knowledge-Based Expert System in Structural Design. *Computers and Structures*, Vol. 20, No. 1-3, pp. 1-9, 1985.
15. Yao, J.T.P., et al., Fuzzy Logic Approach in Metals Fatigue. CE-STR-83-35, Purdue University, 1985.
16. Yao, J.T.P. and Zhang, Z.J., The Development of SPERILL Expert System for Damage Assessment. CE-STR-88-29, Purdue University, 1986.
17. Shortliffe, E.H., *Computer-Based Medical Consultations: MYCIN*. American Elsevier, 1976.

18. Charnaik, E. and McDermott, D., *Introduction to Artificial Intelligence*. Addison-wesley, 1984.
19. Rich, E., *Artificial Intelligence*, McGraw-Hill, 1983.
20. Winston, P.H., *Artificial Intelligence*, McGraw-Hill, 1983.
21. Winston, P.H. and Horn, B.H., *LISP*, Addison-Wesley, 1981.
22. Shepard, R., et al., Damage Analysis of Imperial County Service Building. *J. Structural Engrg.*, Vol. 109, No. 7, pp. 1711-1726, 1983.
23. Akiyama, H., *Aseismic Ultimate Design of Building Structures*. Tokyo University Press, 1980.
24. Park, Y.J., Seismic Damage Analysis of Reinforced Concrete Buildings. *J. Structural Engrg.*, Vol. III, No. 4, pp. 740-757, 1985.
25. US/JAPAN Cooperative Earthquake Engineering Research Program, Proc. 1st Seminar on Repair and Retrofit of Structures, 1980.
26. US/JAPAN Cooperative Earthquake Engineering Research Program, Proc. 2nd Seminar on Repair and Retrofit of Structures, 1981.
27. US/JAPAN Cooperative Earthquake Engineering Research Program, Proc. 3rd Seminar on Repair and Retrofit of Structures, 1982.
28. International Association for Earthquake Engineering, Earthquake Resistant Regulations: A World Lits - 1984.
29. Berg, G.V., Seismic Design Codes and Procedures. EERI, 1982.
30. Housner, G.W. and Jennings, P.C., *Earthquake Design Criteria*. EERI, 1982.
31. Applied Technology Council, Tentative Provisions for the Development of Seismic Regulations for Buildings. National Bureau of Standards, 1978.
32. Cornell, C.A., A Probability-Based Structural Code. *J. Amer. Concrete Inst.*, Vol. 66, pp. 974-985, 1969.
33. Ang, A.H. and Cornell, C.A., Reliability Bases of Structural Safety and Design. *J. Structural Div.*, ASCE, Vol. 100, No. ST9, pp. 1755-1769, 1974.
34. Ellingwood, B., Reliability of Current Reinforced Concrete Design. *J. Structural Div.*, ASCE, Vol. 105, No. ST4, pp. 699-712, 1979.
35. Ellingwood, B., Reliability Based Criteria for Reinforced Concrete Design. *J. Structural Div.*, Vol. 105, ST4, pp. 713-727, 1979.
36. Ellingwood, B. and Ang, A.H., Probabilistic Study of Safety Criteria for Design. Structural Research Series No. 387, Dept. of Civil Engrg., Univ. of Illinois, 1972.
37. Cornell, C.A., Requirements for Probabilistic Approach, in Probabilistic Approaches to Structural Safety. *J. Amer. Concrete Inst.*, Vol. 73, No. 1, pp. 37-48, 1976.

38. Galambos, T.V. and Ravindra, M.K., Tentative Load Resistance Factor Design Criteria for Steel Buildings. Structural Div. Res. Report No. 18, Washington University, 1973.
39. Ravindra, M.K., et al., Illustrations of Reliability-Based Design. *J. Structural Div.*, ASCE, Vol. 100, No. ST9, pp. 1789-1811, 1974.
40. Ellingwood, B., et al., Development of a Probability Based Load Criterion for American National Standard A58: Building Code Requirements for Minimum Design Loads in Building and Other Structures. National Bureau of Standards, 1980.
41. Ellingwood, B., et al., Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant. NUREG/CR-3428, 1984.
42. Smith, P.D., et al., Seismic Safety Margins Research Program - Phase I Final Report. 10 Volumes, NUREG/CR-2015, 1981.
43. Gergeiy, P., Seismic Fragility of Reinforced Concrete Structures in Nuclear Facilities. *Nucl. Engrg. & Des.*, Vol. 94, pp. 9-24, 1986.
44. Healey, J.J., et al., Structural Building Response Review. NUREG/CR-1423, Vol. I, 1980.
45. Singh, A.K., et al., Structural Building Response Review. NUREG/CR-1423, Vol. II, 1980.
46. Hasselman, T.K. and Simonian, S.S., Structural Uncertainty in Seismic Risk Analysis. NUREG/CR-1560, 1980.
47. Newmark, N.M. and Ridell, R., Statistical Analysis of the Resposne of Nonlinear Systems Subjected to Earthquakes. Department of Civil Engineering, UILU 79-2015, 1979.
- 48., Newmark, N.M. and Hall, W.J., Development of Criteria for Seismic Review of Selected Nuclear Power Plants. NUREG/CR-0098, 1978.
49. Kennedy, R.P., et al., Engineering Characterization of Ground Motion: Effects of Characteristics of Free-Field Motion on Structural Response. NUREG/CR-3806, 1984.
50. Clough, R.W. and Penzien, J., *Dynamics of Structures*, McGraw-Hill, 1975.
51. McGuire, R.K., Seismic Structural Response Risk Analysis, Incorporating Peak Response Regressions on Earthquake Magnitude and Distance. Department of Civil Engineering Research Report R 74-51, M.I.T., 1974.
52. Tsai, N.C., Seismic Analyses of Structures and Equipment for Nuclear Power Plants. BC-TOP-4, 1974.
53. Johnson, J.J., Soil-Structure Interaction: That Status of Current Analysis Methods and Research. NUREG/CR-1780.
54. Luco, J.E., et al., Engineering Characterization of Ground Motion: Soil-Strucure Interaction Effects on Structural Response. NUREG/CR-3805, Vol. 4, 1986.

55. Shieh, L.C., et al., Simplified Seismic Probabilistic Risk Assessment: Procedures and Limitations. NUREG/CR-4331, 1985.
56. Reddy, D.P., Seismic Soil/Structure Interaction Analysis Guidelines. SAN/1011-110, Vol. I, 1976.
57. Barneich, J.A., et al., Soil-Structure Interaction Parameters for Aseismic Design of Nuclear Power Stations. Woodward-Clyde Consultants.
58. Kennedy, R.P., et al., Engineering Characterization of Ground Motion: Effects of Ground Motion Characteristics on Structural Response Considering Localized Structural Nonlinearities and Soil-Structure Interaction Effects. NUREG/CR-3805, Vol. 2, 1985.
59. Miller, C.A., et al., Verification of Soil-Structure Interaction Methods. NUREG/CR-4182, 1985.
60. Yao, J.T.P., *Safety and Reliability of Existing Structures*, Pitman Publishing, Inc., 1985.
61. Zadeh, L.A., Fuzzy Sets. *Information and Control*, Vol. 8, pp. 338-353, 1965.
62. Zadeh, L.A., Outline of a New Approach to the Analysis of Complex Systems and Decision Processes. *IEEE Trans. on System, Man and Cybernetics*, SMC-3, pp. 28-44, 1973.
63. Brown, C.B. and Yao, J.T.P., Fuzzy Sets and Structural Engineering. *J. Structural Engrg.*, Vol. 109, No. 5, pp. 1211-1225, 1983.
64. Brown, C.B., A Fuzzy Safety Measure. *J. Engrg. Mechanics Div.*, ASCE, Vol. 105, No. EM5, pp. 855-872, 1979.
65. Elms, D., Use of Fuzzy Sets in Developing Code Risk Factors. *Civ. Engng. Sys.*, Vol. 1, pp. 178-184, 1984.
66. Yee, L.Y., The Development of, and Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage. Ph.D. dissertation, University of California, Los Angeles, 1988.

5. A PROTOTYPE EXPERT SYSTEM FOR SPARE PARTS INVENTORY CONTROL

Kil-Yoo Kim

1. Introduction

Spare parts inventory control is an important and complicated problem because it is not easy to decide which part to stock and how many of each part to stock. Excess inventory means a waste of money and warehouse storage, and a lack of spare parts can cause an expensive power replacement cost (at least \$500,000 per day).

Because of the importance and complexity of spare parts inventory control, many nuclear power plants have conventionally computerized spare parts inventory control systems. However, the functions of the systems are just to track warehouse parts inventory and at most to alert warehouse and purchasing personnel when an item reaches a preset minimum determined by an expert. A recent survey by the U.S. NRC [1] shows that 82% of the plants use management judgment and experience, and 65% use vendor recommendations to decide which part to stock. Therefore, the currently used method is not a systematic way to find the optimum stocking level. If some parameters, such as replacement energy cost, failure rate, lead time, etc., change significantly, it is difficult to find the optimum stocking level in such a non-systematic method.

Furthermore, the spare parts inventory of U.S. nuclear power plants is currently not well controlled according to the U.S. NRC [1]. The survey indicates, "more than half (57%) of the plants sometimes operated in a limiting condition for operation over the past year due to the unavailability of spare parts."

The objective of this task is to build an expert system for spare parts inventory control which can systematically decide the optimum stocking level using artificial intelligence techniques.

Ideally, this expert system should handle spare parts requirements in corrective maintenance (CM), preventive maintenance (PM) and predictive maintenance (PDM) where preventive maintenance and predictive maintenance are defined as in NUREG 1212 [1], as follows:

1. *Predictive Maintenance*

Techniques and activities employed to predict the onset of equipment malfunction or failure, e.g., vibration monitoring, acoustics monitoring, and oil analysis.

2. *Preventive Maintenance*

Regularly scheduled tasks (e.g., inspection, servicing, adjustment, calibration, replacement) intended to keep equipment in condition for operational or emergency use.

This expert system uses Intelligence/Compiler [2] as a language/tool (= expert system shell) on an IBM-PC/AT.

2. Methodology

2.1. Function of Expert System

The proposed expert system can be used by selecting menus as shown in Table 1. Each menu will be briefly explained here; greater detail can be found in the User's Manual (3).

Menu

1. Consultation
 - 1.1. Corrective Maintenance (CM)
 - 1.2. Preventive Maintenance (PM)
 - 1.3. Predictive Maintenance (PDM)
 - 1.4. Decide Optimum Stocking Level
2. Data Updating Access Path
 - 2.1. Basic Data Updating in Frame (= b-tree)
 - 2.2. Failure Rate Updating
 - 2.3. Find Preventive Maintenance Items
3. Sensitivity Analysis by Changing the Following Constraints
 - 3.1. Lead Time
 - 3.2. Risk Cost
 - 3.3. Failure Rate

Table 1: MENU

2.1.1. Consultation

Optimum Stocking Level

If the user selects 1.4 in the menu of Table 1, then the number of each spare part to stock is decided by a cost-effectiveness calculation and/or by the user's experience and by vendor recommendations. That is, at first the expert system determines optimum stocking level by the cost-effectiveness calculation, and then decides the optimum stocking level by combining the result of the cost-effectiveness calculation with the user's experience and judgment, and vendor recommendations in an inexact reasoning process by the inference engine. If the

user thinks his responses (i.e., inputs such as risk cost, loss fraction, interest rate, etc.) to the expert system introduce too large uncertainties in the cost-effectiveness calculation, he may prefer the vendor recommendations or his own experience and judgment to the result of the cost-effectiveness calculation. The cost-effectiveness calculation is explained in Section 2.2.

Corrective Maintenance (CM)

When specific spare parts are required by CM activities, the maintenance manager may ask or use this expert system by selecting 1.1 in the menu of Table 1.

Q: Which spare part item do you want to handle?

Ans: pump xxx

Q: How many spare items do you need?

Ans: 3

Then the expert system will think like a maintenance manager and make the following suggestions.

"The inventory of pump xxx is now empty although
the optimal stock level is 4.

Order 7 spare pump xxx right now since you need
3 spare pump xxx.

Original supplier was GE. The lead time is 2 months
if the original supplier can still supply the
spare pump xxx as usual."

Preventive Maintenance (PM)

When specific spare parts are required by PM activities, the maintenance manager may ask or use this expert system by selecting 1.2 in the menu of Table 1.

The following may be asked by the expert system and answered by the user.

Q: Which spare part item do you want to handle?

Ans: pump xxx

Q: How many spare items to you need?

Ans: 3

Q: When do you need the item?

Ans: Nov. 20, 1987

Then, the expert system will think like a maintenance manager and make the following suggestions.

"The inventory of pump xxx is now empty although the optimal stock level is 4.
3 spare pump xxx are required on Nov. 20, 1987.
You should order 4 spare items right now,
and order 3 more 1 month ahead of the scheduled preventive maintenance data if the original supplier GE can still supply the pump xxx."

Predictive Maintenance (PDM)

In this menu, if an item is entering or is within a wear-out period, the expert system suggests that the item be replaced immediately, or that it be untouched until the next planned outage, etc.

The fact that an item is entering or is within a wear-out period is known by the PDM activities.

Check Suppliers

After making some suggestions in the CM, PM and PDM, the expert system asks the user whether the original supplier can still supply the spare item, or not. If the original supplier can not supply the spare item any more, then the expert system selects the best suitable supplier among several suitable suppliers in the inexact reasoning process. The expert system also can consider an inter-utility cooperative parts loan system such as Pool Inventory Management (PIM).

2.1.2. Data updating access path

Basic Data Updating in Frame (= b-tree)

As shown in Figure 4, data in the b-tree are basic data of each spare part for inference. Since these data affect decisions or suggestions made by the expert system, if there occur situations such that the basic data should be changed, the user can change the data in the b-tree by using this menu.

Failure Rate Updating

The expert system decides the optimum stocking level by using generic data at the pre-start-up phase. During operating period, failure rate data are updated with the Bayesian method by checking reliability data, e.g., Nuclear Plant Reliability Data System (NPRDS) [4] and plant specific data. The optimum stocking level is decided with these new data.

In this version of the expert system the failure rate is not given by a distribution function, but a point-estimate value. Let's assume r' is the number of failures and t' is the period (prime means prior value). Then, prior failure rate λ' is $\frac{r'}{t'}$ (at the start up phase λ' is generic data). During the operating period, there will be some evidence data r and t (= plant specific data). By the Bayesian updating method, posterior failure rate λ'' is $\frac{r''}{t''}$, where $r'' = r' + r$ and $t'' = t' + t$. Thus, in Figure 1, failure rates can be updated from state 1 to state 3.

As a result of predictive maintenance activities such as vibration monitoring, failure rates of components or parts which are located in the wear-out period can be estimated. That is, in Figure 1 the failure rate of state 2 can be estimated.

Figure 1: Simplification of Hazard Function

Find Preventive Maintenance Items

In this menu, the expert system shows those items whose lifetimes are lower than one year.

2.1.3. Sensitivity analysis

In this menu, the expert system evaluates the impact of changing lead time, risk cost and failure rate on the optimum stocking level.

2.2. Cost-Effectiveness Calculation

The basic factor in decision-making concerning which parts to stock and how many of each part to stock is the cost-effectiveness calculation, which is as follows:

If a spare part of component were obtained, then the following cost (= Total Inventory Cost = TIC) would be incurred at present value.

$$\text{TIC} = \text{price} + \text{storage cost} + \text{maintenance cost}$$

However, if there were a failure of the item in the future, there would be the following loss of money (= LOSS) at present value, if the part were not in inventory.

$$\begin{aligned} \text{LOSS} = & (\text{price} + \text{risk cost}) \int_p^{r1+p} \left[\frac{1+j}{1+i} \right]^{t-p} f(t) dt \\ & + (\text{rec} \times \text{loss fraction}) \int_p^{r1+p} \text{lead time } (t) \left[\frac{1+j}{1+i} \right]^{t-p} f(t) dt \quad (1) \end{aligned}$$

where,

$$f(t) = \lambda e^{-\lambda t};$$

λ = failure rate;

i = interest rate;

j = escalation rate;

$r1 = \min (\text{remaining item lifetime, remaining plant lifetime});$
 $p = \text{period during which the item has been used};$
 $rec = \text{replacement energy cost rate};$
 $price = \text{current purchasing price of the item};$
 $loss \text{ fraction} = \text{fractional reduction of power due to failure of item};$
 $risk \text{ cost: See equation (2) below.}$

If LOSS is less than TIC, it would not be cost beneficial to acquire the spare part for inventory. If LOSS is larger than TIC, obtaining the spare part is cost effective. In this case, further checking is done as to whether acquiring another spare is also cost-effective. By this procedure optimum stocking level is calculated. Also, this model is applied to the case that many identical items are used in the power plant.

The previous model is applied only when the failure rate or hazard function is constant. This is an acceptable assumption if the item is in its useful period and it has not entered the wear-out period, or if the situation is that the remaining lifetime of the item is longer than that of the plant. Therefore, this model can be used in determining the optimum stocking level for CM and PM items.

However, many PDM items can enter the wear-out period and require a different evaluation. The hazard functions are no longer constant with time in the wear-out period. The expert system assumes that the hazard function of wear-out period increases linearly with time, i.e., $h(t) = kt$. Then

$$f(t) = k(t-t_0)e^{-\frac{k}{2}(t-t_0)^2} \quad (= \text{Rayleigh distribution})$$

Here, t_0 is the same as shown in Figure 1.

By using the Rayleigh distribution in the wear-out period, the cost-effectiveness calculation can be done for PDM items.

If the PM item is near the end of its lifetime, this can be checked with the expert system, which would tell the user to acquire the spare part. The user can also check whether he should obtain the spare part by the cost-effectiveness calculation for the PM item. That is, since its hazard function is made to increase linearly with time near the end of its lifetime (i.e., if an item lifetime remains less than twice its leadtime, it is assumed that its failure rate increases linearly with time), like the hazard function of the wear-out period, most cost-effectiveness calculations would result in acquiring of a spare part before the end of item lifetime.

The spare parts supplier's instability problem is handled by two methods. One is to change leadtime, and the other is to find a suitable supplier by the inexact reasoning process which is explained in '*Check Suppliers*' of Section 2.1.1. If some spare parts suppliers are out of business, or if they do not produce the same spare parts as they originally supplied, then the lead time of the item will change, i.e., increase. This increased lead time is used in the second term of Equation (1).

In the cost-effectiveness calculation, the increase in risk due to the lack of spare parts is also handled. Since the technical specifications of a nuclear power plant may accept continuing operation (e.g., 72 hours), in many cases, although a component fails in a system which has redundant components, the lack of spare parts can increase risk. The user can find an increased core melt frequency (Δ CMF) due to the failed component by using the SARA code [5]. Then, the risk cost is calculated as follows;

$$\text{risk cost} = \Delta\text{CMF} \times \frac{(\text{reduced period})}{365} \times \$5,000,000,000 \quad (2)$$

where,

'*reduced period*' means that if the spare part is available in inventory, then the time that the plant continues to run with a failed component can be shortened by the amount of the '*reduced period*', which reduces the risk of core melt frequency.

3. Structure of the Expert System

The structure/architecture of the expert system is shown in Figure 2. The user selects the menu and responds to the questions of the expert system. Then, the expert system considers many factors in the inference engine and suggests adequate actions.

The expert system, which is written with Intelligence/Compiler, represents knowledge by multiple paradigms such as rules, frames and logic. Details are to be found in Reference (3), which also includes a partial code listing of the expert system.

References

1. NUREG-12/2, "Status of Maintenance in the U.S. Nuclear Power Industry 1985," U.S. NRC (1986).
2. Intelligence Ware, Inc., "Intelligence/Compiler User's Manual," 1986.
3. Kim, K.-Y., Ph.D. Thesis, "Two Expert System Applications to Nuclear Power," University of California, Los Angeles, 1988.
4. Southwest Research Institute, "Reporting Procedures Manual for the Nuclear Plant Reliability Data System," 1989.
5. Sattison, M.B., Tullock, W.W., and Van Siden V.S., "System Analysis and Risk Assessment System (SARA) User's Manual," EGG-SPAG7532, 1987.

6. AN EXPERT SYSTEM TO ESTIMATE TIME, RATE AND MAGNITUDE OF RELEASE OF IMPORTANT RADIOACTIVE ISOTOPES, GIVEN A LOSS OF CONTAINMENT INTEGRITY

Kil-Yoo Kim

1. Introduction

In the unlikely event that an accident involving large scale core melt occurred in a light-water-cooled, nuclear power reactor, various preparations have been made to gather information to help guide any offsite evacuation steps, should they be necessary. These include measurement of radioactivity exterior to the reactor plant, as well as a group of measurements inside the containment. However, the existing measurement capability is inadequate to give quantitative information on the rate of escape of radioactive material, isotope by isotope, should a significant loss of containment integrity occur. Such information, together with continuing meteorological data, could place evacuation or sheltering measures on a much more certain foundation than is possible with the radioactivity measurements now provided.

This study is intended to explore the practicality of devising a simple expert system, which, together with the relevant instrumentation, could provide detailed information on rate of escape of radioactive isotopes from containment, at least approximately. A pressurized water reactor (PWR) with a large dry containment is used as the model for study.

2. Instrumentation

The expert system assumes the availability of the following parameters on an essentially continuous basis (all triply redundant):

- containment atmospheric temperature (five locations)
- containment pressure (five locations)
- containment sump level
- water level above containment floor
- refueling water storage tank level
- containment sump temperature
- hydrogen concentration
- carbon dioxide concentration

It is also assumed that the concentrations of the following isotopes can be obtained frequently (say, every minute) at several sampling stations in the containment:

 xenon 133, xenon 135, krypton 85, krypton 85m, iodine 131, iodine 133,
 cesium 134, cesium 137, rubidium 88 and strontium 90.

Tellurium is also of potential importance but may be more difficult to measure; hence the tellurium is assumed to be proportional to the cesium in the current version of the code. Other radioisotopes could be added to the list as appropriate.

Discussions with manufacturers of such sampling and measuring equipment indicate that sampling of the listed isotopes about every fifteen minutes is currently within the state of the art, and that with the appropriate emphasis, one might approach a sampling rate of once a minute (Archibald, 1988).

3. Physical Approach to Estimating Release Rate

It is assumed that the fission products in the containment atmosphere at any time are well mixed with the nitrogen and oxygen gas (and hydrogen and carbon dioxide, if any) and the steam, which, prior to occurrence of a loss of containment integrity, is ordinarily saturated and in equilibrium with the water in the sump or on the containment floor. Containment and sump water temperature are assumed to be the same, prior to an event involving significant leakage rates. Containment spray actuation or a hydrogen burn are detected and treated as such.

3.1 Magnitude of Release

The leakage rate determination involves the calculation of gas loss during the leakage period by direct observation of containment pressure and temperature.

The leakage rate computation is based on the ideal gas law in the form

$$P_{\text{gas}} V = W_{\text{gas}} R T_c \quad (1)$$

where

P_{gas} = absolute partial pressures of gases except H_2O inside containment

$$= P_{\text{total}} - P_{\text{H}_2\text{O}}$$

P_{total} = total pressure inside containment

$P_{\text{H}_2\text{O}}$ = partial pressure of H_2O vapor

V = net free internal volume of containment

W_{gas} = mass of gases except H_2O inside containment

T_c = temperature inside containment

R = gas constant

Leak fraction defined in the expert system is,

$$\begin{aligned}\text{leak fraction} &= \frac{\text{gas mass at state 1} - \text{gas mass at state 2}}{\text{gas mass at state 1}} \\ &= \frac{W_{\text{gas},1} - W_{\text{gas},2}}{W_{\text{gas},1}}\end{aligned}$$

where 1 minute is usually taken as the time interval between state 1 and state 2.

A_1 , the released amount of radionuclide 1 during state 1 to state 2, equals leak fraction x concentration of radionuclide 1, and the rate per minute is derived directly.

During most accidents, the containment atmosphere usually contains saturated steam. Therefore, during the depressurization of containment due to containment failure, it is assumed that $P_{\text{H}_2\text{O}}$ is obtained by the following rules.

- If sump water level decreases during depressurization, $P_{\text{H}_2\text{O}}$ is that pressure in equilibrium (saturated) with the sump water, because steam pressure in the atmosphere of containment corresponds (very nearly) to saturation pressure at sump water temperature.
- If sump water level does not decrease during depressurization, then $P_{\text{H}_2\text{O}}$ is set (as an approximation) at the saturation pressure at the atmosphere temperature inside containment.

3.2. Thermodynamic Properties

The water vapor properties in the calculation of leak rate are derived by using functions obtained by fitting the steam tables (USNRC, 1984). These properties include the saturation pressure of steam, P_{sat} ; saturation steam enthalpy, h_g ; the saturation water enthalpy, h_f ; and the enthalpy of evaporation, h_{fg} .

3.3. Resuspension

Because of the large amount of water and the steam condensation process, resuspension is not likely to be a significant effect in containment, except that a sudden depressurization could cause flashing of water which contains fission products (ANS, 1984).

Since the concentration of radionuclides of interest is monitored, on line (every minute), it is assumed that any resuspension effects are covered.

3.4. Location of Leakage from Containment

The appropriate leak location may be detectable by zoned pressure measurements, but this remains to be studied more deeply. The current plan is:

- to install instruments to measure pressure and temperature in five containment zones.

4. Basic scheme of the Expert System

The proposed prototype expert system is implemented with Knowledge Engineering Environment (KEE) (Intellicorp, 1986) on a Symbolics LISP machine. The expert system is named RELEASE.

The basic scheme of the expert system is shown in Figure 1. If temperature or pressure inside containment suddenly changes, the inference process of the expert system starts to check whether containment has failed or not. If it has failed, the expert system shows the released amount of radionuclides during each time interval (and the rate of release) and the leak location.

4.1. Knowledge Representation and Inference

The proposed expert system represents knowledge with multiple paradigms such as rules and frames. The expert system monitors pressure and temperature inside containment. However, since the environment inside containment is very harsh, measuring sensors may fail. Therefore, the expert system should have some logic to detect failed sensors, and should not involve them in the calculation of amount of radionuclide release. This expert system has two inference processes; one is related to diagnosing containment failure; the other is to help find failed sensors.

4.1.1. Inference to Find Containment Failure

The characteristics of containment failure are;

- Containment pressure in any zone suddenly drops
- Containment temperature in any zone decreases.

Therefore, if there is a sudden pressure and temperature drop inside containment, the expert system's inference process starts. However, since the pressure and temperature drop are not unique characteristics occurring only in the event of containment failure, the expert system checks the possibility of the other

Figure 1: Basic Scheme of RELEASE

phenomena such as the start of containment spray. Stored in the knowledge base are the following factors which increase pressure and temperature inside containment:

1. H₂ burning
2. High steam or gas generation due to the following:
 - core slump in large LOCA
 - reactor vessel failure
 - core-concrete interaction
 - debris quenching by spillover of sump water
 - accumulator water flow over molten core.

Also stored in the knowledge base are factors which decrease pressure and temperature inside containment.

1. Containment failure
2. Spray (or fan cooler) starts
3. the latter portions of transients which at the beginning initiate a pressure rise, for example, H₂ burning.

One example of the expert system's inference ability is illustrated by the following situation: If RWST level decreases, sump level increases and ECCS is off, the expert system deduces that spray has started. Thus, if there is a drop of pressure at $t = t_0$, it is not due to a containment failure, but due to spray. See (Kim, 1988) for details.

4.1.2. Failed Sensors

The expert system uses auctioneering of similar sensors or analytic reasoning to identify spurious readings.

4.1.2.1. H₂ deflagration

Since the peak temperature and peak pressure due to hydrogen burning are related to the change in hydrogen concentration, the expert system can check approximately whether the readings of temperature, pressure, and H₂ analyzer are consistent.

4.1.2.2. Sump level and evaporation

The expert system can also check whether or not the sump temperature sensor or sump level sensor has failed by using an energy balance relation between sump level, sump temperature, and the energy to vaporize the loss of mass in the sump.

If the energy balance is not satisfied, the inference is made that the temperature or level sensor of the sump (or floor level water height) is out of order. An approximate value of P_{H_2O} is obtained by using the atmosphere temperature inside containment, instead of using the sump water temperature.

5. Summary

A prototype expert system called RELEASE has been developed to explore the practicality of providing detailed information on the timing and rate of escape of radioactive isotopes from containment, given a large scale core melt accident and a subsequent loss of containment integrity.

Acknowledgments

This work was supported in part by Department of Energy Award DOE-DE-FG03-86SF16610, "Joint Application of AI Techniques, PRA, and Disturbance Analysis Methodology to Problems in Maintenance/Design of Nuclear Power Plants."

References

- ANS, (American Nuclear Society), 1984, "Report of the Special Committee on Source Terms."
- Archibald, W., 1988, Private Communication, Sentry Corporation.
- Intellicorp, 1986, KEE Software Development System User's Manual.
- Kim, Kil-Yoo, 1988, "Expert Systems Applied to Two Problems in Nuclear Power Plants," Ph.D. dissertation, University of California, Los Angeles.
- USNRC, 1984, NUREG/CR-3988, "MARCH 2 (Meltdown Accident Response Characteristics) Code Descriptions and User's Manual."

7. ON OPERATOR RESPONSE AID IN SEVERE EARTHQUAKES

Shuhhwa Lee

1. Background

Recent probabilistic risk assessment (PRA) studies [1,2] indicate that potential accidents initiated by large earthquakes are among the major contributors to public risk. Therefore, the seismic design of older plants, in particular, is being re-examined [3].

During a severe earthquake, any structure, system, or component (SSC) may fail; the plant may be driven into a very complex situation in which instrumentation and control (I&C) systems may also fail and provide operators with unreliable information about the processing parameters crucial to plant safety. What can operators do when faced with such complexity? Even though the likelihood of such a severe earthquake may be very low, its consequence may be more serious if mitigative measures are not thought out and implemented in advance.

Emergency procedure guidelines (EPGs) development [4], signal validation, and situation diagnosis are crucial then in this respect. The EPGs are the only material operators may follow in emergency conditions in addition to their own personal experience. A trend from event-specific EPGs to symptom-oriented ones is underway [5]. vonHerrmann performed a series of studies on plant status monitoring systems [5] as well as on emergency procedure guidelines [6,7,8]. Many studies [9,10,11,12] have addressed on signal validation and situation diagnosis, in general. And a deeper understanding of operator errors of cognition is in its developmental stages [13]. However, their application to seismic-induced failures remains largely undone. As a result, a systematic

study to aid operator response in severe earthquakes has not been developed yet, though some thought of a descriptive nature is available [14].

2. Objective

The objective of the present study is related to the measures to protect the plant from severe damage due to large earthquakes, namely, the improvement of operator capability to respond to seismic damage through the use of EPGs. The fact that the symptoms presented to operators may be unreliable in the case of severe earthquakes endangers the validity of actions in EPGs. It is the purpose of this study to deterministically identify possible weakness of EPGs, given a severe earthquake, as well as to probabilistically evaluate those identified weakness. It is expected that study results will provide valuable information for further studies on plant safety during severe earthquakes, e.g., the development of an expert system, the refinement of symptom-oriented guidelines, etc.

3. Approach

Three major steps are taken in this study, they are:

Step I: Review PRA reports to identify critical operator action sets (COAS).

A COAS contains those operator actions crucial to a specified event sequence, whose combined failure will lead the reactor to a core melt condition.

Step II: Identify possible confusions given some postulated structural system and component (SSC) or I&C failures which have an impact on the identified COAS when it is performed according to the instructions in the EPGs, and discuss possible remedies for them.

Step III: Estimate the likelihood of those postulated SSC or I&C failures given different degrees of earthquake-induced ground motion, and evaluate the conditional risks of operator failure.

4. PRA/Event Trees

PRA is a realistic analysis of the consequences that could potentially result from nuclear reactor accidents and a quantitative assessment of the likelihood of such occurrences. As a result, the first objective of a PRA is to construct a set of accident scenarios that begin with initiating events and end with a specification of actual offsite damages and injuries suffered. The second objective of a PRA is to quantify the likelihood of the accident sequences and the associated uncertainties. Because the event tree methodology provides a systematic approach to organizing the large number of potential accident scenarios and for evaluating their likelihood of occurrence, the event trees in existing PRA report may be used as an aid to identify critical accident sequences for our study.

Review and simplification, with no system redundancy and two consequences only (safe and core melt), of event trees in the Seabrook Station Probabilistic Risk Assessment (SSPAS) report [1] yields 49 safe sequences and 169 core melt sequences. Some of them may contain COAS and provide the basis for our case study as described in Section 6 of this paper [15].

5. EPG/Functional Restoration Guidelines

In the emergency operational state, plant parameters have exceeded the limits for reactor protection. The plant state has shifted from one that is

operator paced to one that is machine paced. Consequently, the operator's role has shifted from that of controlling the plant state to that of responding to the changing plant state.

EPGs provide the operator with a well defined framework for emergency operations. The operator's role and special needs are addressed through providing a network of predefined symptom-based strategies for systematically responding to any developing emergency transient. These system-based strategies derive from the emergency operation concepts of Optimal Recovery and Critical Safety Function Restoration.

The concept of Optimal recovery is based on the premise that radiation release and equipment damage can both be minimized through associating the symptoms of an emergency transient with predefined plant conditions and implementing an associated predefined event-related recovery strategy to achieve an optimal plant end state. The optimal end state varies with the emergency transient but is the state in which radiation release and equipment damage are minimized and plant conditions are stable with plant equipment operating in long term alignments. The most probable (i.e., design basis) transients exhibit characteristic symptoms that can be categorized in one of four basic categories:

- Reactor Trip (with no accident)
- Loss of reactor coolant
- Loss of secondary coolant
- Steam generator tube rupture

For each basic category, characteristic symptoms and optimal plant end states to minimize radiation release and equipment damage can be defined. Associated response strategies can also be defined.

The concept of Critical Safety Function Restoration is based on the premise that radiation release to the environment can be minimized if the barriers to radiation release to the environment are protected. The barriers that are provided in every nuclear power plant consist, at the minimum, of: fuel matrix and fuel clad, reactor coolant system pressure boundary, containment distance. For each of the barriers there is a set of functions that must be maintained on a continuing basis if the barrier is to remain intact. A set of safety functions that is sufficient for the fuel matrix/cladding, reactor coolant system pressure boundary and containment vessel barriers in a plant that is intended to be shut-down consists of:

- Maintenance of SUBCRITICALITY
- Maintenance of CORE COOLING
- Maintenance of HEAT SINK
- Maintenance of Reactor Coolant System INTEGRITY
- Maintenance of CONTAINMENT Integrity
- Control of Reactor Coolant INVENTORY

Situations can arise in which the integrity of a barrier is lost and cannot be restored even though all Critical Safety Functions are satisfied. In these situations, all available resources are directed toward minimizing further degradation of the failed barriers and keeping the rest of the barriers intact.

The Critical Safety Function Restoration concept is utilized to support the Optimal Recovery concept. This is accomplished by developing the associated function-related restoration strategies with separate operator diagnostic and control elements. The separate diagnostic element permits explicit monitoring

of the plant safety state while the operator is implementing event-related recovery strategies. The diagnostic element is solely a monitoring element and does not require operator control actions. As such, it can be performed by equipment or personnel independent of the operator. When Critical Safety Functions are satisfied, the plant safety state is satisfied and function-related restoration is not necessary. Only if a Critical Safety Function challenge is detected is the operator required to terminate optimal recovery and implement function restoration.

Review of the 49 identified safe sequences reveals that they do prevent reactor core from melting by protecting the first four critical safety functions from being defeated, and review of the 169 identified core melt sequences reveals that any of them does fail at least one of the four critical safety functions [15]. Based on the review result, it is found that the COAS is contained in the following four Function Restoration Guidelines:

- FR-S.1: Response to Nuclear Power Generation - ATWS
- FR-C.1: Response to Inadequate Core Cooling
- FR-H.1: Response to Loss of Secondary Heat Sink
- FR-P.1: Response to Imminent Pressurized Thermal Shock Condition.

A case study is then performed according to the contexts in these guidelines and their steps. The result of the case study is discussed in the next section.

6. Confusions and Remedies - Case Study

Several cases were examined and possible remedies for identified confusions discussed. For instance, the failure of the refueling water storage tank level indicator in a loss of coolant accident may prevent the operator from performing

the sump recirculation mode in time, allowing the pumps to get damaged due to running without water and to fail to perform the recirculation mode later. If so, core melt should result because there is not water to cool the core in the long term. A possible remedy for this case is that the sump level (or floor level) indicator is used to verify the RWST level indicator, that is, if the building has a high enough water level, the operator may go to the recirculation mode without waiting until the RWST low level alarm sounds (or at least the operator is given a specific warning).

As another instance, the failure of the normal charging path may prevent the operator from performing other rapid boration means, which are required for anticipated transient without scram (ATWS) situations. Given a ATWS, the operator is guided to perform high pressure injection due to the high temperature in the core. Any of the four high pressure injection paths may achieve the cooling purpose in the guideline. If the safety injection charging path is used, the reactor get cooling and goes subcritical. However, if the high head safety injection path is used, the ATWS situation remains and core melt may occur if the operator does not recognize the problem (failure in this path) in time. A possible remedy for this case is that the required core cooling paths for ATWS situations should be the safety intjection charging paths, with the high head safety injection paths as a supplement.

More cases were studied in reference 15 which is currently in preparation.

7. Likelihood Estimation

The likelihood of seismic-induced failure of a given SSCs or I&Cs will be estimated for an illustrative hazard curve. The conditional risk of selected combinations of failures which lead to operator confusion, given an earthquake, will also be estimated.

8. Conclusions and Recommendations

Symptom-oriented guidelines completely depend on indicators. A faulty indicator may cause the operator not to act on time, not to act correctly, or not to act at all. These types of errors may probably be avoided if an expert system can provide operators with some relevant engineering knowledge. For example: knowledge of how long the RWST water supply may last can be used to alert operators as to the possible failure of the RWST level indicator before the RWST gets empty. As a result, the development of an expert system and the refinement of the symptom-oriented guidelines are suggested for examination as potentially valuable future work.

References

1. "Seabrook Station Probabilistic Safety Assessment", PLG-9399, 1983.
2. "Kuosheng Plant Probabilistic Risk Assessment," Taipower Co., 1985.
3. Smith, C.B., "Generic Seismic Ruggedness of Power Plant Equipment, EPRI NP-5223, 1987.
4. "Westinghouse Owner Group Emergency Response Guidelines," July 1, 1987.
5. vonHerrman, J., Brown, R., and Tome, A., "Light-Water Reactor Status Monitoring During Accident Conditions," GUREG/CR-1440, EGG-EA-5153, 1980.
6. vonHerrman, J.L., "Methods for Review and Evaluation of Emergency Procedure Guidelines Volume I: Methodologies," NUREG/CR-3177, EGG-2243, Vol. I, Wood-leaver and Associates, Inc., 1983.

7. vonHerrmann, J.L., Brinsfield, W.A., and Brown, R.G., "Methods for Review and Evaluation of Emergency Procedure Guidelines Volume II: Applications to Westinghouse Plants," NUREG/CR-3177, EGG-2243, Vol. II, Wood-Leaver and Associates, Inc., 1983.
8. Brinsfield, W.A., Burns, E.T., McClymont, A.S., Mays, S.E., and vonHerrmann, J.L., "Methods for Review and Evaluation of Emergency Procedure Guidelines Volume III Applications to General Electric Plants," NUREG/CR-3177, EGG-2243, Vol. III, Wood-Leaver and Associates, Inc., 1983.
9. Tzanos, C.P., "A Methodology of Plant-Wide Data Validation and Fault Identification," ANL/RAS 84-3, 1984.
10. Deegan, P.B., McDonald, M.E., and Province, R.E., "DICON An Expert Systems Approach to Diagnosis and Control Guidance with LMFBR Application Phase III - Preliminary Validation," WAESD-SR-94000-54, 1984.
11. Guarro, S.B., Szabo, J., and Okrent, D., "Multi-Level Approach for Structural Definition of a Plant-Wide DAS-Disturbance Analysis System," UCLA-eng-8424, 1984.
12. Guarro, S.B., and Okrent, D., "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Application," UCLA-ENG-8507, 1985.
13. Schryver, J.C., Knee, H.E., and Palko, L.E., "The Integrated Reactor Operation/System (INTEROPS) Model for Simulation of Advanced Reactor and Control System Concepts: Summary of Prototype Development," ORNL/TM-10598, 1988.
14. Letter to David Okrent, ACRS member, from C. Michelson, ACRS member, September 9, 1987.
15. S.H. Lee, "On Operator Response Aid in Severe Earthquakes," Ph.D. dissertation, in preparation, University of California, Los Angeles, CA.

Appendix A: List of Publications

1. Arueti, S. and D. Okrent, "Combining Objective and Subjective Techniques for Assessing Quality of Management," Proc. Conf. on Structural Mechanics in Reactor Technology (SMiRT 9), paper M3/3, Lausanne, Aug. 17-21, 1987.
2. Arueti, S., "A Computerized Experiment for Comparison between Methods of Uncertainty Propagation," Proc. Conf. on Artificial Intelligence and Other Innovative Applications in the Nuclear Industry: Present and Future, Aug. 31 - Sept. 2, 1987, Snowbird, Utah.
3. Arueti, S. and G. Apostolakis, "A PRA-Based Data Analysis Procedure for Use in Computerized Decision Aids," Proc. Conf. on Artificial Intelligence and Other Innovative Applications in the Nuclear Industry: Present and Future, Aug. 31-Sept. 2, 1987, Snowbird, Utah.
4. Arueti, S. and D. Okrent, "A Decision-Making Aid for Maintenance Activities," International Topical Meeting on Safety and Reliability, Pittsburgh, April 2-7, 1989.
5. Arueti, S. and D. Okrent, "A Knowledge-Based Prototype for Optimization of Preventive Maintenance Schedules," The Role and Use of PCs in Probabilistic Safety Assessment and Decision Making, Post-SMiRT 10, Beverly Hills, CA, Aug. 21-22, 1989.
6. Guarro, S.B., "PROLGRAF-B. A Knowledge-Based System for the Automated Construction of Nuclear Plant Diagnostic Models," Proc. Conf. on Artificial Intelligence and Other Innovative Applications in the Nuclear Industry: Present and Future, Aug. 31-Sept. 2, 1987, Snowbird, Utah.
7. Guarro, S.B., "A Logic Flowgraph Based Concept for Decision Support and Management of Nuclear Power Operation, Post-SMiRT 9 Seminar," Accident Sequence Modelling: Human Actions, System Response, Intelligent Decision Support," Munich, FDR, Aug. 24-25, 1987.
8. Guarro, S.B., "A Logic Flowgraph Based Concept for Decision Support and Management of Nuclear Plant Operation," Reliability Engineering and System Safety 22, 1988.
9. Kim, K.-Y., P.Y.C. Chen and D. Okrent, "An Expert System for Spare Parts Inventory Control," Proc. Conf. on Artificial Intelligence and Other Innovative Applications in the Nuclear Industry: Present and Future, Aug. 31-Sept. 2, 1987, Snowbird, Utah.
10. Kim, K.-Y. and D. Okrent, "An Expert System for Radionuclide Release From Containment," Proc. SMiRT 10, Anaheim, California, Aug. 14-18, 1988.
11. Lee, S.-H. and D. Okrent, "Expert System to Assist Diagnosis in Severe Earthquakes," NUCSAFE '88, Avignon, France, October 1988.
12. Yee, L.-Y. and D. Okrent, "The Development of an Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage," Proc. Conf. on Artificial Intelligence and Other Innovative Applications in the Nuclear Industry: Present and Future, Aug. 31-Sept. 2, 1987, Snowbird, Utah.

13. Yee, L.-Y. and D. Okrent, "The Development of an Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage," Proc. SMiRT 9, paper M3/2, Lausanne, August 17-21, 1987.
14. Yee, L.-Y. and D. Okrent, "The Development of an Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage," NUCSAFE '88, Avignon, France, October 1988.
15. Yee, L.-Y. and D. Okrent, "The Development of an Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage," The Role and Use of PCs in Probabilistic Safety Assessment and Decision Making, Post-SMiRT 10, Beverly Hills, California, August 21-22, 1989.

Appendix B: List of Theses

1. Arueti, S., "A Prototype Knowledge Based System for Preventive Maintenance Optimization, Ph.D. Thesis, University of California, Los Angeles, March 1989 (UCLA-ENG-8942).
2. Chen, P.Y.C., "Intelligent Inventory Control System," M.S. Thesis, University of California, Los Angeles, 1986.
3. Kim, K.-Y., "Expert Systems Applied to Two Problems in Nuclear Power Plant; Part I: An Expert System for Spare Parts Inventory Control, Part II: An Expert System for Radionuclide Release from Containment," Ph.D. Thesis, University of California, Los Angeles, December 1988 (UCLA-ENG-8944).
4. Lee, S.-H., "Operator Response Aid in Severe Earthquakes," Ph.D. Thesis in progress.
5. Yee, L.-Y., "The Development of an Expert System for Finding Fragility Curves of Building Structural Systems in the Preliminary Design Stage," Ph.D. Thesis, University of California, Los Angeles, December 1988 (UCLA-ENG-8943).

END

**DATE
FILMED**

4 / 16 / 92