NUREG/CR–5213
Vol. 2

The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability

Main Report

Prepared by D. D. Woods, H. E. Pople, Jr., E. M. Roth

Westinghouse Science and Technology Center

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Information Resources Management, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR--5213-Vol.2

TI90 013882

The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability

Main Report

Manuscript Completed: May 1990
Date Published: June 1990

Prepared by
D. D. Woods,[1] H. E. Pople,[2] E. M. Roth

Westinghouse Science and Technology Center
1310 Beulah Road
Pittsburgh, PA 15235

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN D1167

[1]Cognitive Systems Engineering Laboratory
The Ohio State University

[2]University of Pittsburgh and Seer Systems

ABSTRACT

The U. S. Nuclear Regulatory Commission is sponsoring a program to develop improved methods to model the cognitive behavior of nuclear power plant (NPP) personnel. A tool called Cognitive Environment Simulation (CES) was developed for simulating how people form intentions to act in NPP emergencies. CES provides an analytic tool for exploring plausible human responses in emergency situations. In addition a methodology called Cognitive Reliability Assessment Technique (CREATE) was developed that describes how CES can be used to provide input to human reliability analyses (HRA) in probabilistic risk assessment (PRA) studies.

This report describes the results of three activities that were performed to evaluate CES/CREATE: (1) A technical review was conducted by a panel of experts in cognitive modeling, PRA and HRA; (2) CES was exercised on steam generator tube rupture incidents for which data on operator performance exist; (3) a workshop with HRA practitioners was held to analyze a "worked example" of the CREATE methodology. The results of all three evaluations indicate that CES/CREATE is a promising approach for modeling intention formation. Volume 1 provides a summary of the results. Volume 2 provides details on the three evaluations, including the CES computer outputs for the tube rupture events.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

The authors would like to express their appreciation to Thomas G. Ryan, for the guidance and support he has provided throughout this research program. Dr. Ryan was the NRC Project Manager, from the initiation of this research program up to the phases of research described in this paper. We would also like to thank Paul Lewis, who is the current NRC Project Manager, for his enthusiastic support of the project; and Lewis F. Hanes, manager of the Information System and Human Sciences Research Department at the Westinghouse Science and Technology Center, for his substantial contribution in maintaining the momentum of the project.

We would also like to thank:

Dr. Michael Coombs of the New Mexico State University, Prof. Allen Newell of Carnegie-Mellon University, Dr. Richard Pew of Bolt Beranek and Newman, Mr. Jon Young of Lynette & Associates, and Mr. John Wreathall of Battelle Laboratories (now at Science Applications International Corporation), for their participation in the technical review workshop. Their review of the model development work and their helpful comments greatly contributed to further steps in the development and evaluation of the CES modeling tool.

Ed Dougherty and John Wreathall at Science Applications International Corporation, and David Gertman at Idaho National Engineering Laboratory for their participation in the CREATE workshop which examined how to use the CES modeling capabilities in Human Reliability Analysis.

Westinghouse's Nuclear Advanced Technology Division allowed the project to use the Engineering Simulator in the Dynamic Systems Simulation (DSSL) Laboratory, a high fidelity NPP computer simulation, on an as available basis. The Man-Machine Functional Design group of Westinghouse's Nuclear Technology Division provided access to its AI computers and other hardware for interfacing to the plant simulation in the DSSL Laboratory. The personnel of the DSSL Laboratory patiently supported our use of their excellent facility.

Finally, we gratefully acknowledge the efforts of William Elm, formerly of the Man-Machine Functional Design group, and Glenn Elias, formerly of the Westinghouse Research and Development Center, who provided the knowledge and perseverance to setup and run the CES computer program in the DSSL Laboratory.

1. INTRODUCTION: MODELING OPERATOR COGNITIVE ACTIVITY FOR HUMAN RELIABILITY ASSESSMENT

The quality of human performance frequently has been shown to be a substantial contributor to nuclear power plant safety (e.g., Trager, 1985, Reason, in press[1]). A significant factor in determining human action under emergency conditions is *intention formation* -- deciding on what actions to perform.[2] Because errors of intention, which are often referred to as "cognitive errors" are an important element of overall human contribution to risk, the nuclear industry has recognized the need for more effective ways to capture this component of human error (Moray and Huey, 1988; Ward, 1988).

The U.S. Nuclear Regulatory Commission has embarked upon a program of research to build a computer simulation of human intention formation (how people decide on what actions are appropriate in a particular situation) in order to better predict and reduce the human contribution to risk in nuclear power plants (NPPs). The model simulates the cognitive activities involved in responding to different accident situations. It is intended to provide an analytic tool for predicting likely human responses, and the kinds of errors that can plausibly arise under different accident conditions. It is envisioned as a tool to support human reliability analysis that is analogous to the analytic tools for modeling physical processes in the plant that are used in PRAs.

This research program has consisted of a feasibility study (completed in April of 1986) which determined that it is practical to build such a cognitive model based on techniques from artificial intelligence (AI). The results of the assessment are reported in Woods and Roth,1986, NUREG/CR-4532. The feasibility study identified a specific AI software system which could serve as a vehicle for model development.

The research project then focused on simulation model development and the application of the model to Human Reliability Analysis (HRA). The results are reported in Woods, Roth and Pople (1987), NUREG/CR-4862. Specifically:

- A tool for simulating how people form intentions to act in emergency operations in NPPs was developed using AI techniques. The model, called Cognitive Environment Simulation or CES, can be used to explore human intention formation in the same way that reactor codes are used to model thermodynamic processes in the plant.

- A methodology, called Cognitive Reliability Assessment Technique or CREATE, was developed which specifies how this capability can be used to enhance measurement of the human contribution to risk in Probabilistic Risk Assessment (PRA) studies.

---

1 J. Reason. *Human Error.* Cambridge University Press, England, in press.

2 This is contrasted with the execution of intentions -- carrying out the sequence of actions decided upon (cf., Woods and Roth, 1986).

The research project then focused on several kinds of evaluation of the CES tool and the CREATE methodology:

1) An evaluation workshop was held in July, 1987 to obtain technical input from a highly distinguished panel of independent experts in the fields of HRA, PRA, AI, and cognitive modeling on both the CES cognitive model and the CREATE methodology for using CES to provide input on human reliability to PRA. There was unanimous consensus that the project represents first-rate technical work that has advanced the state of the art in modeling operator behavior and in HRA.

2) Based on recommendations from the technical review workshop, CES was exercised on a family of tube rupture incidents for which data on human operator behavior was also available in order to assess the ability of CES to capture aspects of human intention formation. This required linking CES to a plant simulator and expanding the CES knowledge base and processing mechanisms. Results showed that changes in the CES knowledge base and changes in incident complexity produce plausible changes in CES behavior.

3) A workshop with HRA practitioners was held to analyze a "worked example" of the CREATE method to evaluate the role of CES/CREATE in HRA. The worked example was based on the same family of tube ruptures used to exercise CES. The results showed that while CES/CREATE needs to mature further (e.g., ability to handle a greater range of NPP events; improved interface and accessibility), the CREATE process has the potential to provide useful qualitative and quantitative inputs to PRA that cannot be obtained in other ways.

Additional work is underway to make the CES modeling tool more accessible to a wider set of potential users, and to further expand and demonstrate its capabilities by exercising CES on additional events of interest to the NRC.

This volume provides details on the evaluation of the CES simulation tool itself, the evaluation of how it can be used in HRA and PRA, and information on the current state of development and use of CES. Volume 1 provides an overview of the evaluation activities.

Chapter 2 of this volume provides an overview description of the CES simulation model and the CREATE methodology. Chapter 3 reports the results of the cognitive model evaluation workshop. Chapter 4 describes the results of the CES exercises on simulated emergency events. Chapter 5 reports the results of the HRA workshop held to review the CREATE process. Chapter 6 provides a summary and discussion of the main conclusions from the evaluation exercises.

2. OVERVIEW OF CES AND CREATE

This section provides an overview description of the CES simulation tool for exploring human intention formation in emergency situations and the CREATE methodology for utilizing CES to provide input to HRA/PRA studies. More detailed descriptions of CES and CREATE can be found in NUREG/CR-4862.

2.1 THE CES MODELING TOOL

The development of a cognitive simulation tool in this project focused on one part of human behavior: *human intention formation* (i.e., deciding what to do). This scope was chosen, first, because models and techniques are already available to assess the form and likelihood of execution errors in human reliability studies (e.g., Reason and Mycielska, 1982; Swain and Guttman, 1983). A second reason for selecting this scope is because erroneous intentions are a potent source of human related common mode failures which can have a profound impact on risk -- as actual accidents such as Three Mile Island and Chernobyl have amply demonstrated (Reason, in press). Intentions to act are formed based on reasoning processes. The scientific disciplines that study these processes are called cognitive sciences or mind sciences and include a variety of fields such as cognitive psychology and artificial intelligence. Models of these processes are called "cognitive models."

CES is an analytic computer simulation that simulates cognitive activities underlying operator intention formation in emergencies. Built into the simulation is the ability to change elements or parameters in meaningful ways in order to investigate the cognitive consequences of changes in the man-machine system (e.g., changes in training, procedures, information displayed in control room). By simulating the cognitive activities required to successfully handle an emergency event, CES provides information about the complexity of the problem-solving situation posed by accident event sequences of interest. It provides an indication of the kinds of plant state information, NPP knowledge, and problem-solving activity necessary for correct situation assessment and intention formation. It also provides indication of the kinds of errors in situation assessment and intention formation that can arise.

The cognitive activities that underlie operator performance in NPP emergency conditions are numerous and complex. They include monitoring the plant, detecting unexpected situations, forming a situation assessment (e.g., identifying plant malfunction(s) or processes that can explain the unexpected plant behavior); allocating limited attentional resources (e.g., deciding what to look at or what to do next given human attentional limitations); and response planning (e.g., accessing/adapting appropriate procedures). CES includes rudimentary versions of each of these cognitive activities. It monitors and tracks changes in plant state, detects unexpected plant behavior, formulates hypotheses to account for unexplained plant behavior, and formulates intentions to act based on its situation assessment.

The strategy employed in developing CES was to build a broad "framework" model that provides a conceptual framework within which to develop/incorporate overtime deeper narrow scope submodels of the different cognitive activities over time (cf. NUREG/CR-4532 for a rationale of this approach). The objective was to implement rudimentary versions of each of the cognitive activities that underlie

intention formation to produce a runnable broad-scope simulation. Further development efforts can then focus on deepening the psychological fidelity of different aspects of the simulation as new data or more sophisticated models of particular cognitive activities become available or can be developed (e.g., incorporating a more elaborate model of monitoring; decision-making under uncertainty; response planning).

CES allows exploration of plausible human responses in different emergency situations. It can be used to identify what are difficult problem-solving situations, given the available problem-solving resources (e.g., specific procedural guidance, operator knowledge, person-machine interfaces). By simulating the cognitive processes that determine situation assessment and intention formation, it provides the capability to establish analytically how people are likely to respond, given that these situations arise.

It is difficult and expensive to collect extensive empirical data on emergencies, especially rare ones; however, using CES as an analytical tool, an analyst can more cheaply explore behavior across a variety of incidents and variations on incidents to perform a kind of sensitivity analysis. In this sense CES can be thought of as analogous to reactor codes, which are computer simulations that are used to predict reactor behavior. Both these analytical tools are efficient mechanisms to predict performance. As in the case of reactor codes, the knowledge and capabilities encoded in the CES model are expected to expand and evolve as new empirical data from simulator studies or actual incidents become available.

A plant operator receives input about the plant as reflected in control room displays and alarms. CES also requires input on the states of plant processes. CES takes as input a time series of those values that describe plant state which would be available to be looked at by operational personnel (either a hand-generated series of time steps through an incident, or dynamically generated data from NPP simulation models). The dynamic stream of input data constitutes a virtual display board which the CES simulation monitors to track the behavior of the plant over time, to recognize undesirable situations, and to generate responses which it thinks will correct or cope with these situations (intentions to act). Its output is a series of these intentions to act which must be executed and therefore modify the course of the incident. Figure 2-1 diagrams this process in the case where a high fidelity plant simulation is used to provide the inputs to CES. In this case, plant data that would be available to an operator is automatically extracted from the high fidelity plant simulation. Based on this input, CES generates intentions to act. These are executed by a human intermediary who inputs the necessary commands to the high fidelity plant simulation (i.e., serving as a board operator).

An analyst can examine a record of CES's information processing activities as the incident unfolds in time. The analyst can see what data the CES computer simulation gathered, what situation assessments were formed, what hypotheses were considered, pursued or abandoned, and what plant behaviors were "thought" to be expected or unexpected. This output looks very much like a description of the cognitive activities of actual operators responding to an incident in a plant simulator. The difference is that one is an analytical description of what people might do given certain assumptions, and the other is an empirical description of what some specific people did do in a simulation of an incident.

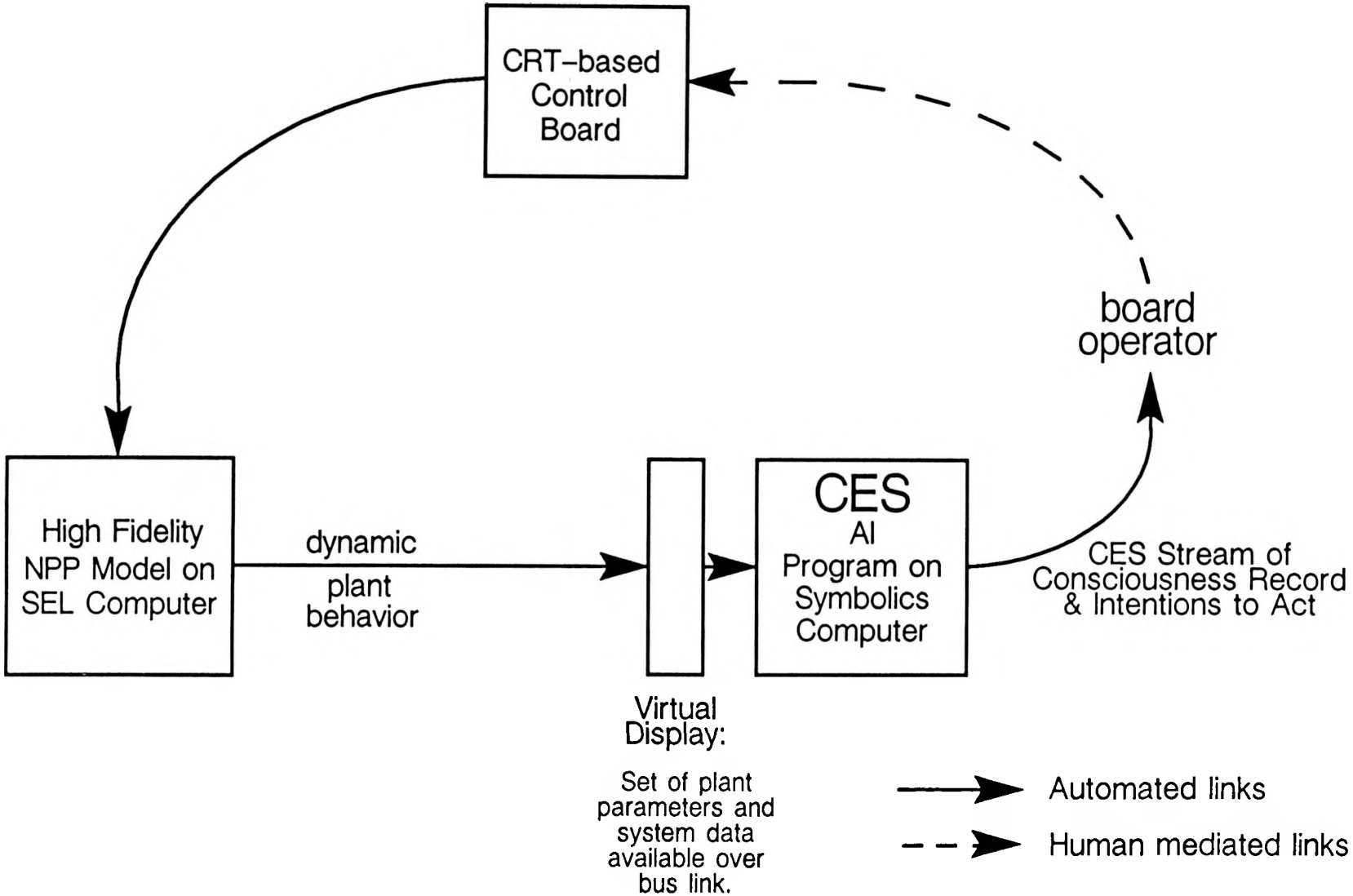

Figure 2-1. Overview of the facility set up and used to exercise CES. CES obtains time-stamped plant parameter status input from a dynamic plant simulation. Based on this input CES generates intentions to act. These are executed by a human intermediary who inputs the necessary commands to the high fidelity plant simulation (i.e., serving as a board operator).

An important feature of CES is the ability it gives an analyst to explore the consequences of changes in the assumptions about the event, or the characteristics of the operators, on the potential for errors of intention. The analyst can vary the base incident (e.g., introducing failed sensors that obscure critical information), or the assumptions about what the operator can be expected to know (e.g., based on training or procedures), and observe what impact this has (if any) on the situation assessments and intentions to act generated by CES.

As an AI system, CES contains two major types of information. First, it contains a *knowledge base* that represents operator knowledge about the power plant, including how processes work or function, what evidence signals different plant states including faults, relationships between plant states, and actions to correct abnormalities. Second, it contains information on processing techniques *(inference engine)* that represents how operators process external information (displays) and how knowledge is called to mind under the conditions present in NPP emergencies. Further details on the CES cmputer simulation are provided in chapter 4 and NUREG/CR-4862.

2.2 CES ANALYTICAL ENVIRONMENT

In order to exercise the CES model on the test incidents, we had to be able to generate a stream of plant behavior for the incident as input to CES (Figure 2-1). Furthermore, while CES acts as the control room supervisor, we needed a mechanism to be able to act as a board operator and take manual actions as the incident required.

To do this effectively and efficiently, we created a custom analytical environment where the CES computer simulation was interfaced to a high fidelity NPP simulation model. This was accomplished by taking advantage of the Dynamic Systems Simulation Laboratory (DSSL) facility located at Westinghouse's Energy Center in Monroeville, PA. Figure 2-2 shows a diagram of the computers in the DSSL facility and their links. Figure 2-3 is a picture of the facility.

The DSSL provides a direct connection between computers specialized for running plant simulation models (SEL-Gould computers) and computers specialized for running AI based software (Symbolics LISP processing computers). This capability allows AI programs to be run practically and efficiently in conjunction with large real-time numerical codes. As shown in Figure 2-2, the facility includes a Symbolics 3650 which is a large, high performance LISP machine (16 MB of RAM; 1.1 GB of disk). The current implementation of the CES modeling tool runs on this computer. CES is implemented as a specific instance of the EAGOL artificial intelligence problem solving system. EAGOL is a software system and proprietary product of Seer Systems that builds on the conceptual framework of the CADUCEUS AI system developed by H. Pople for internal medicine (Pople, 1982; 1985). The EAGOL software is written in LISP in the Symbolics software development environment.

The DSSL facility also includes two SEL 32/87 computers that support real-time plant simulation software. In this project we used a high fidelity training NPP simulation model resident on the SEL that simulates a Westinghouse three loop Nuclear Steam Supply System (NSSS).

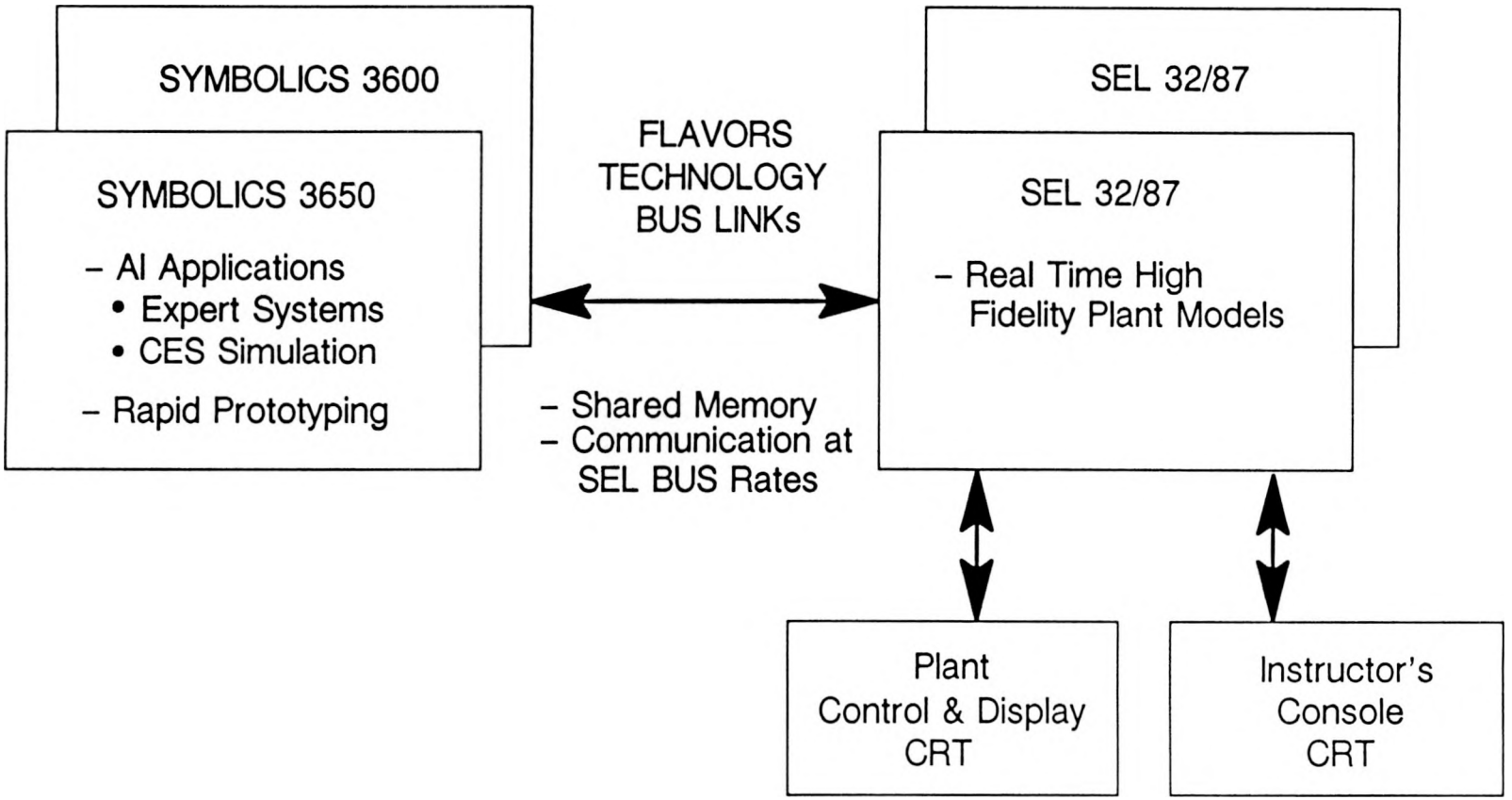

Figure 2–2. Block diagram of the computers and bus–link at the Westinghouse Dynamic Systems Simulation Laboratory that were used for the CES exercises. (CES resides on the symbolics computer and receives input from a dynamic plant simulation that runs on the SEL computer.)

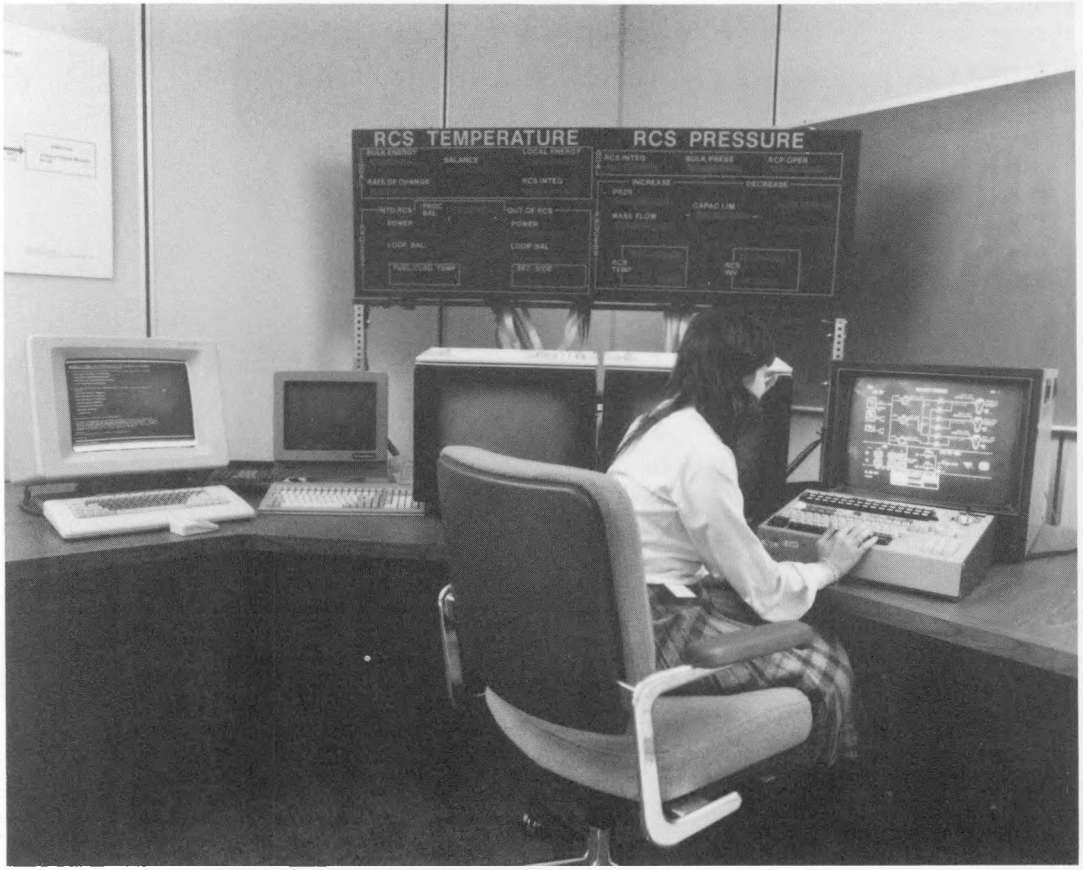

Figure 2–3. Photograph of the facility used for CES exercises that shows the screen that provides a window on CES internal activities, the CRTs used to call up plant displays and controls, and the instructors console.

A shared memory link produced by Flavors Technologies, Inc. connects the Symbolics computer and the SELs. The Flavors link allows interchange of data between the two computers at essentially the bus rate of the machines, with virtually no protocol overhead. The application on the SEL is virtually unaware that the AI application on the Symbolics is accessing data. The Symbolics machine accesses data as if the data were resident in its own physical memory. This is a very elegant means of linking the two processes as it imposes virtually no changes to the numeric codes yet it integrates them into the AI application in real time.

The DSSL facility enables an analyst to simulate an NPP accident event on the high fidelity plant simulation and have the output of the plant simulation be directly fed as input to CES. The NPP simulation is controlled via an instructor's CRT console. The instructor's console on the plant simulation allows an analyst to specify the plant initial conditions, and the kind, size and timing of different plant failures. An analyst can then start the incident and observe CES react to dynamically changing plant data. In addition to the instructor's console, there is a second CRT connected to the high fidelity plant simulation that serves as a computer based operator's panel. Using this CRT, the analyst can call up graphic displays of plant status and computer-based plant controls to execute the necessary operator actions. One of the benefits of this facility is that it allows the analyst to view the behavior of the plant (on the plant display and control CRT) and the response of CES to that plant behavior (on the AI computer) in parallel at each time step (See Figure 2-4). This allows the analyst to have an independent assessment of plant state to compare to the situation assessment being built up and revised by CES.

The DSSL facility greatly facilitated CES set up, CES exercises, and the development of required extensions to CES capabilities. It also provides a model demonstration for how to set up the CES modeling tool at other sites. Additional work is underway to examine hardware, inter-computer communication strategies, and cost factors to recommend to the NRC how to set up the CES tool for future use.

2.3 THE CREATE METHODOLOGY

CREATE describes a methodology for using the capabilities of CES to better evaluate the potential for significant human errors in PRA analysis. In CREATE, CES is run on multiple variants of accident sequences of interest. The variants are selected to provide cognitively challenging situations. The goal is to identify sets of conditions (characteristics of the situation and/or the operator) that combine to produce intention failures with significant risk consequences. Once the range of plausible intention errors and the conditions under which they will arise are identified, a quantification procedure is used to assess the likelihood of these intention errors.

The CREATE methodology involves two main stages: a modeling stage where CES is used to find situations that can lead to intention failures and therefore to erroneous actions; and a systems analysis input stage where the results of the cognitive modeling are integrated into the overall systems analysis. A diagram of the CREATE process is provided in Figure 2-5.

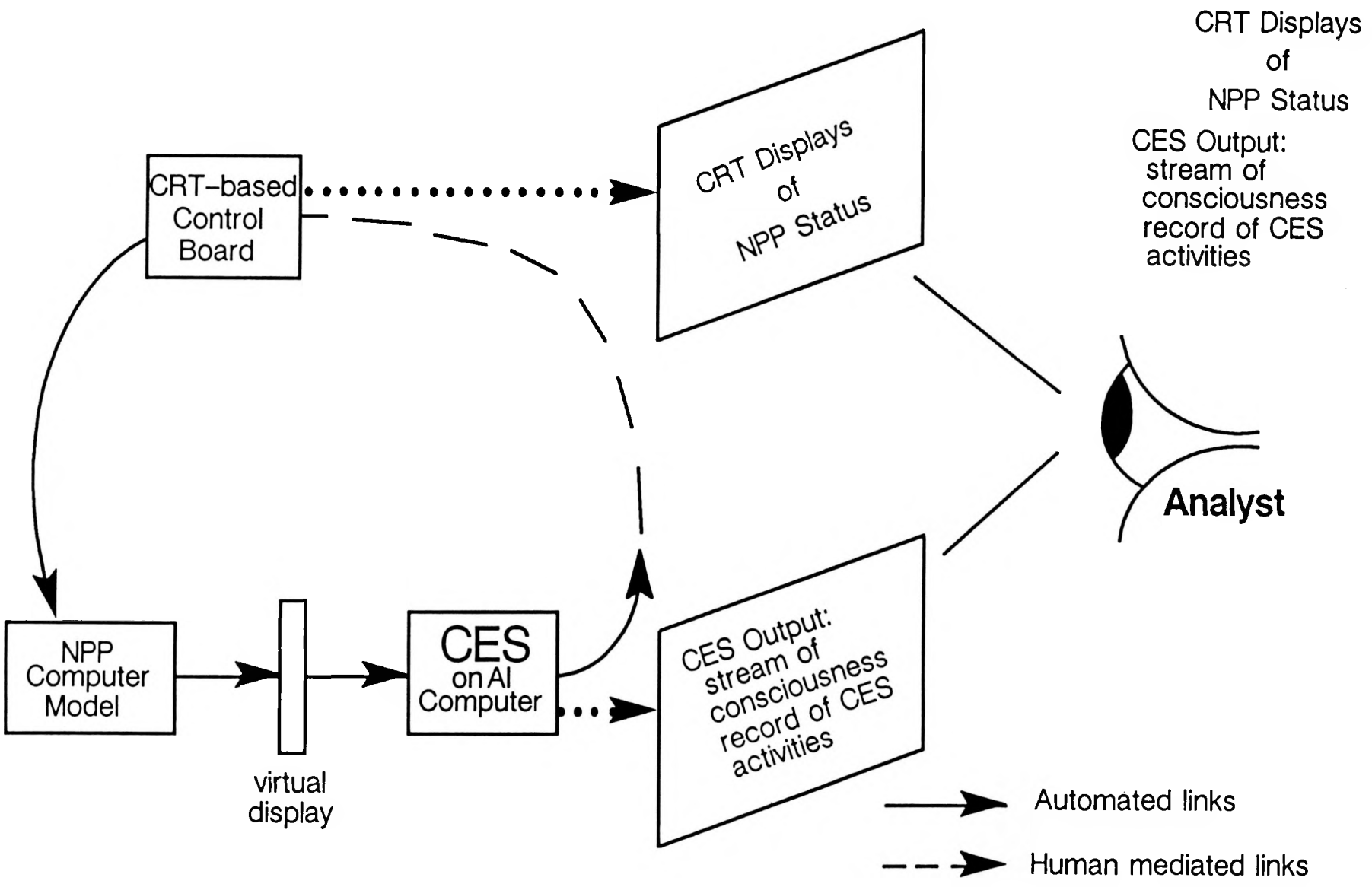

Figure 2–4. In the facility used for CES exercises, an analyst can observe CES through a 'stream of consciousness' record of its information processing activities. At the same time, the analyst can monitor NPP state through the CRT displays on the computer-based control board.

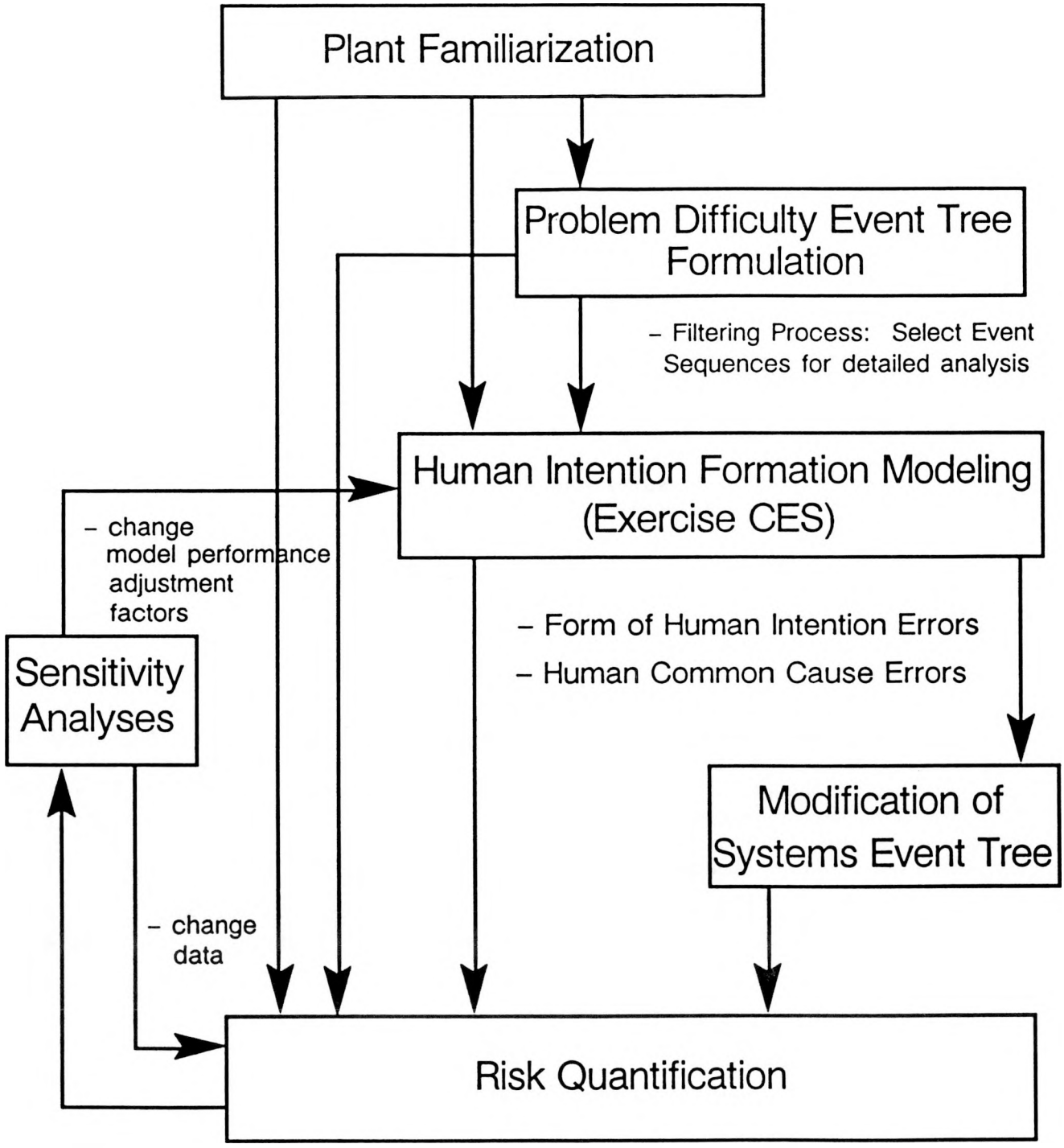

Figure 2–5. Block diagram of the CREATE methodology (from Woods, Roth, and Pople, 1987).

Note that CES plays the same role in the CREATE methodology that simulation codes for physical plant processes play in reliability analyses of physical systems. In both cases we are dealing with complex, dynamic processes whose behavior is affected by too large a set of interacting factors to be tractable without a simulation. The modeling stage provides the backbone of the analysis in that it defines the critical elements to be aggregated and how they are to be aggregated. Frequency estimation techniques are then used to establish the probabilities to be aggregated.

Because CES is a simulation code, it requires detailed and complete input to run an incident, and the analyst receives a detailed record of the simulation's behavior in the incident. This means that using CES in the modeling stage ensures explicit consideration and detailed analysis of the factors that contribute to human intention errors.

The main steps in the systems analysis input stage are:

- Modify the systems analysis event/fault trees to reflect the effects of intention errors identified in the modeling stage (e.g., to reflect errors of commission or common-cause errors that might have been identified),

- Employ a quantification procedure to assess the likelihood of these intention errors,

- Combine intention error estimates with execution error estimates.

The procedure for estimating likelihoods (cognitive reliability estimates) from CES assumes that the major element of uncertainty in predicting operator behavior rests on assessing the probability that the situation will arise which produced an intention failure when simulated in CES.

To estimate these likelihoods two questions need to be considered:

- How likely is it that the problem solving demands in effect in that CES run (i.e., the particular characteristics of the incident) will arise in the actual NPP?

- How likely is it that the particular set of problem solving resources modeled in that CES run (e.g., the NPP knowledge encoded that reflect what an operator might be assumed to know based on training, procedures, experience) will be in effect?

Ideally, these questions are answered by examining empirical data on how often these problem-solving demands and resource situations arise. However, as in all aspects of PRA there is a paucity of empirical data from which to derive the frequency estimates. When empirical data is lacking expert judgment techniques are employed to generate the probability estimates, (e.g., Seaver & Stillwell, 1983; Embrey, Humphreys, Ros, Kirwan, and Rea, 1984).

3. EVALUATION ACTIVITY 1: COGNITIVE MODEL EVALUATION WORKSHOP

3.1 OBJECTIVES AND PROCEDURES OF TECHNICAL REVIEW

This chapter documents the procedure and results of a technical review workshop that was held on July 29 and 30, 1987. The purpose of this workshop was to obtain a technical evaluation of the CES model and the CREATE methodology as developed up to that point. A highly distinguished, five member technical review team was assembled that included internationally recognized leaders in AI, Cognitive Modeling, Human Factors, HRA and PRA. The team included:

- An internationally recognized researcher in Artificial Intelligence, who was one of the founders of the AI field.
- A leader in human performance modeling who has conducted a major study of operator decision making in nuclear power plant emergencies and built cognitive models for aerospace applications.
- A recognized leader in Probabilistic Risk Assessment.
- A leading researcher and practitioner in Human Reliability Analysis.
- A leading researcher in the use of AI to model reasoning in complex, dynamic worlds.

Members of the review team were asked to provide technical input and evaluation on the CES cognitive model, the CREATE methodology for employing CES for improved human reliability assessment, and the remaining evaluation plans. They were asked for individual responses in the form of preliminary verbal reactions at the end of the workshop and individual written reports.

3.2 RESULTS OF THE TECHNICAL REVIEW

There was unanimous consensus among review team members that the project has pushed the state-of-the-art in cognitive modeling of decision making in complex worlds, artificial intelligence, and human reliability.

As a problem solving system, CES was judged to have pushed the state-of-the-art of AI diagnostic systems. It was recognized as unique in its ability to handle multiple hypotheses in diagnostic situations of realistic complexity. The reviewers saw this as a fundamental requirement for a system to be of real utility as a model of operator intention formation in NPP emergency conditions.

CES/CREATE was judged to be a major step forward towards the goal of soundly based human reliability techniques (cf., Moray and Huey, 1988; Elkind, Card, Hochberg, and Huey, 1990).

The reviewers strongly emphasized that CES was a significant achievement that has broad applicability in other areas as well as human reliability.

The reviewers unanimously judged that the development work established the viability of this approach to model operator behavior and to advance the state of human reliability analysis.

With respect to additional model development and evaluation, the reviewers stated that, while the development effort up to that point had resulted in new important functionalities, both CES and CREATE are "green" and untested. Given limited project resources, they strongly recommended that the next step should be to exercise CES and CREATE to identify and resolve additional technical hurdles that will undoubtedly emerge. They recommended that the next step should focus on exercising CES on test incidents where empirical data on operator cognitive behavior already exist. The project followed this recommendation, and initial CES testing was based on exercising CES on a family of steam generator tube rupture incidents where empirical data on operator behavior were already available (from Pew et al., 1981; Woods, Wise and Hanes, 1982; Woods, 1982). In the longer term, the panel also noted the need for an ongoing process of empirical validation as the model matures.

The reviews also strongly emphasized the need for more detailed specification of the impact of CREATE on HRA and PRA. They recommended that, given the limited project resources, this activity should focus on a "worked example," that is, select a case and carry out the CREATE steps on that case. The review team suggested that a workshop involving several HRA practitioners and researchers would be a good mechanism for carrying out this analysis. This recommendation became the basis for the CREATE Workshop which is summarized in the section titled "Evaluation Activity 3: The CREATE Workshop" of this volume.

4. EVALUATION ACTIVITY 2: THE CES MODELING TOOL

4.1 OBJECTIVES AND APPROACH

The purpose of this task was to assess whether the CES simulation could produce behavior that plausibly parallels operator intention formation. This was done by exercising CES on events for which empirical data on actual operator behavior existed. Note that this is the initial step in assessing the ability of a system like CES to accurately model operator intention formation.

Three test cases were run. All were variants of a steam generator tube rupture. Case 1 was a "text book" steam generator tube rupture in that the tube rupture was the only fault present. Cases 2 and 3 used a diagnostically more challenging event. Several faults were introduced in addition to the tube rupture to complicate the diagnosis. In particular there is a power outage at the start of the event that lasts approximately a minute. This results in the loss of the air eject radiation alarms. This means that an important leading indicator supporting diagnosis of the tube rupture is no longer available. In addition, a seal leak was introduced in each of the reactor coolant pumps. This complicates the diagnosis further because the seal leak can account for some of the observed symptoms that are actually due to the steam generator tube rupture. A seal leak following a loss of offsite power is plausible since during the power outage there is inadequate flow of coolant through the seals (because the charging pumps shut down).

Cases 2 and 3 both used the same accident scenario. What varied was the knowledge about seal leaks encoded in the CES knowledge base.

There were two objectives in running these three events:

1) To demonstrate that the ability of CES to diagnose the tube rupture will vary with the complexity of the diagnostic task in ways that parallel the differences observed in the behavior of human operators confronted with these events.

2) To demonstrate that changes in the knowledge encoded in the CES knowledge base that reflect differences in operator knowledge (e.g., due to training or experience) would lead to plausible changes in CES diagnostic and decision behavior.

In exercising CES on these events, we identified a number of areas where there was a need to expand CES reasoning capabilities in order to model more accurately the kind of reasoning that human operators perform. The capabilities of the Eagol AI system on which CES is built were extended accordingly.

Data from simulated steam generator tube rupture accidents run with experienced crews (e.g., Woods, Wise, and Hanes, 1982) were used to compare to CES behavior in these incidents.

Section 4.2 describes the cognitive demands imposed by the test cases, and human operator performance in similar incidents.

Section 4.3 presents the actual output protocols of CES for the three test cases.

Section 4.4 discusses conclusions drawn from the CES behavior in these test cases.

Section 4.5 describes the CES knowledge base developed to exercise CES on the test cases.

Section 4.6 describes the enhancements that were made to the EAGOL AI system on which CES is built in preparation to run the three test cases.

4.2 HUMAN PERFORMANCE ON THE TEST INCIDENTS

Case 1 is a "textbook" steam generator tube rupture in the sense that only a single fault is present and there is a highly specific and salient cue that indicates the presence of a tube rupture: radiation in the secondary side of the plant. This cue strongly evokes the hypothesis of a tube rupture, and follow up diagnostic search reveals plant behaviors consistent with this hypothesis. Data from both actual and simulated steam generator tube rupture incidents indicates that human operator diagnosis of a "text book" steam generator tube rupture is highly reliable and occurs very quickly and very early in the sequence of events (cf., Pew et al., 1981; Woods, 1982; Woods and Roth, 1982[3]).

Now consider what happens in the variant where the radiation indications do not occur. From a problem solving point of view the incident is a *loss of leading indicator* incident (LOLI) -- a highly specific indicator of a diagnostic category is missing. Given the absence of secondary radiation signals, there is a much larger set of hypotheses that are consistent with the initial set of abnormal plant behaviors (low level, low pressure), and which should be explored during diagnosis. The results of the initial diagnostic search will eliminate some possibilities. In particular, the evidence will be consistent with a break but it will not be possible to conclusively establish the type of break. Only when there is a visible increase in level in the faulted steam generator that is not otherwise accounted for, is it possible to definitively diagnose the tube rupture. Since it takes some time for this evidence to be detectable by any agent given the current displays of information, the diagnosis of a steam generator tube rupture will take much longer than in the textbook case. Furthermore, some knowledge or processing bugs may lead the human problem solvers to miss or mis-interpret the evidence when it is observable. Woods et al. (1982) ran the loss of leading indicator tube rupture with experienced crews, and the data clearly show this pattern of results. In that study the time required to definitely diagnose a tube rupture following a loss of offsite power ranged from 4.5 to 20 minutes. In contrast, diagnosis time for a "textbook" steam generator tube rupture averages approximately one minute (Woods, et al., 1982; Woods and Roth, 1982).

In the current CES exercises (cases 2 and 3) we complicated the event further by adding a reactor coolant pump leak. The seal leak could partially account for some of the tube rupture symptoms. This could lead less experienced operators to fail to diagnose the tube rupture or to severely delay diagnosis. As part of this project we collected data on human performance on this event for comparison with

3 D. D. Woods and E. Roth. *Operator performance in simulated process control emergencies.* Unpublished study, 1982.

the CES behavior. We ran three two-person crews of NPP control room training instructors on a high fidelity training simulator.

Table 4-1 summarizes the sequence of events in the two LOLI accident scenarios for which data on human performance were available (i.e., data from Woods, et al., 1982; and the additional data collected as part of this project). Tables 4-2 and 4-3 contain summary descriptions of operator behavior in these two events. In both sets of runs crews took longer to definitively diagnose the tube rupture, and entertained more alternative hypotheses prior to correct diagnosis than in the case of "textbook" tube ruptures.

4.3 CES RUNS

Once the set of test incidents were defined, and the data on experienced operator performance in these incidents was examined, the next step was to set up CES to run these three test cases. NPP knowledge relevant to diagnosing and responding to steam generator tube rupture events needed to be encoded in the CES knowledge base.

In order to determine what knowledge to encode in the CES knowledge base it was necessary to identify the range of knowledge that relevant populations of operational personnel possess about the NPP functions, systems, and faults relevant to this incident.

Some of this information was already available from the data gathered in the Woods et al. (1982) study of operator performance. In addition, the current procedures for these incidents were examined, and NPP control room simulator instructors were interviewed about operator knowledge and actions in these incidents.

Figure 4.1 presents the hierarchy of diagnostic categories currently encoded in the CES knowledge base. The knowledge encoded primarily covered the major classes of loss of coolant accidents (LOCAs) and their effects on primary system parameters. The current knowledge base is still shallow in many areas related to tube rupture incidents. However, enough knowledge base construction was carried out to generate CES outputs that demonstrate plausible behavior.

Once the knowledge base was developed, the next step was to set up the test cases on the high fidelity NPP simulator to provide input to CES. A time-stamped set of plant parameter data was input from the high-fidelity NPP simulator to CES every ten seconds. At present 188 plant parameters are input to CES at each time step. CES monitors these inputs, looking for anomalies in behavior such as parameter levels, rates of change, or direction of change, that are unexplained by known influences, as well as goal-violations (i.e., parameter values outside normal control limits). CES then produces as output a description of the plant disturbances it detects, the hypotheses it entertains, the diagnoses it forms, and the set of actions it recommends to be taken.

The actual output protocols of CES for each of the three test cases are presented below. Commentary explaining the CES behavior is interweaved with the CES output. The commentary appears in italics and is not part of the CES output.

Table 4-1

Sequence of Events for Two Loss of Leading Indicator Incidents For Which Data on Human Operator Behavior was Available

- Main Features (Common to Both Variants):
  - Loss of Electric Power
  - Steam Generator Tube Rupture, begins after loss of power
  - No secondary radiation alarms occur
- Variant 1: 6 crews of experienced operators (Woods, et at., 1982)
  - Power restored almost immediately; manually restart charging pumps
  - Tube rupture in SG C
- Variant 2: 3 crews of two person instructors
  - Power restored 2 to 3 mins after trip; charging pumps restart automatically
  - Tube rupture in SG B
  - Small seal leak also present

Table 4-2

Summary of Human Performance in the Woods, et al.(1982) Loss of Leading Indicator Incident (Tube Rupture Following Loss of Electric Power; 6 Crews of Experienced Operators)

- Situation Assessment 1: Recognized variation on 'normal' or expected reactor trip behavior.

- Situation Assessment 2: Recognized 'abnormal' or unexpected trip.

    - o Cue was primary system pressure and level decreasing with either maximum net charging or safety injection (SI) on (5 of 6 crew after 5 to 11 mins).

    - o For one crew, the variation on normal trip situation assessment persisted for 20 mins).

- Situation Assessment 3: Pursued possible explanations:

    - o Continuing level and pressure decrease indicates break but they did not know where (5 of 6 crews).

    - o LOCA possibility was dominant hypothesis, but no closure because no indications of abnormal containment.

    - o Typical search pattern included: Pressure Operated Relief Valves closed? spray on? excessive cooldown? abnormal containment conditions (pressure, radiation, sump level)?

    - o One crew actively pursued steam generator tube rupture hypothesis: stopped all auxilliary feed water flow to observe if any steam generator level increasing without feed flow (faulted steam generator 7% different from the other steam generators at the time of diagnosis; tube rupture suspicion arose 1 minutes following Situation Assessment 2).

- Situation Assessment 4: identified steam generator tube rupture:

    - o Tube rupture suspicion triggered by recognizing abnormal steam generator level behavior (5 crews).

    - o Recognition probably was based on little or no auxilliary feedwater flow and steam generator level increasing (5 crews). Large differences in level across steam generators were not noticed for some time and auxilliary feedwater flow was throttled, perhaps several times.

    - o Faulted steam generator level was about 2-16% narrow range (nr), 71%nr, about 45-50%nr, about 30-40%nr, and about 50-55%nr respectively when the diagnosis was made by the various crews.

    - o The level difference between faulted and non-faulted steam generators was about 10-16%nr, 42%nr, over 22%nr, about 26-32%nr, and about 39-41%nr respectively.

    - o The recognition of abnormal steam generator behavior arose 4.5, 7, 7.5, and 13 minutes following Situation Assessment 2. It occurred 20 minutes after the trip for the crew which did not recognize an abnormal trip.

Table 4-3

Summary of Human Performance in the Loss of Leading Indicator Incident with Addition Seal LOCA (3 Two-Person Crews of Control Room Training Instructors)

- Situation Assessment 1: Recognized variation on 'normal' or expected reactor trip behavior.

- Situation Assessment 2: Recognized 'abnormal' or unexpected trip.

    - o Cue was primary system pressure and level decreasing with either maximum net charging or safety injections on (2 crews).

    - o One crew, may have missed that there was an abnormality (he was very surprised to see large difference in SG levels later in incident).

- Situation Assessment 3: Pursued possible explanations.

    - o Continuing level and pressure decrease indicated break but they did not know where (2 crews). LOCA possibility was dominant hypothesis, but no closure because there were no indications of abnormal containment.

    - o For one crew, insufficient evidence to go to event specific procedures; they evaluated SI termination criteria.

    - o Typical search pattern included: Pressure Operated Relief Valves closed? spray on? excessive cooldown? abnormal containment conditions (pressure, radiation, sump level)?

- Situation Assessment 4: Identified steam generator tube rupture:

    - o Tube rupture suspicion triggered by recognizing abnormal SG level behavior (all 3 crews).

    - o The cue was one SG level well into narrow range while others still in wide range (about 24% narrow range (nr), about 30% nr, and about 30% nr) when monitoring SG level for another purpose. One crew did not recognize 28%nr in one SG and others still on wide range as abnormal.

    - o The recognition of abnormal SG behavior occurred 13, 17, 18 minutes after the trip.

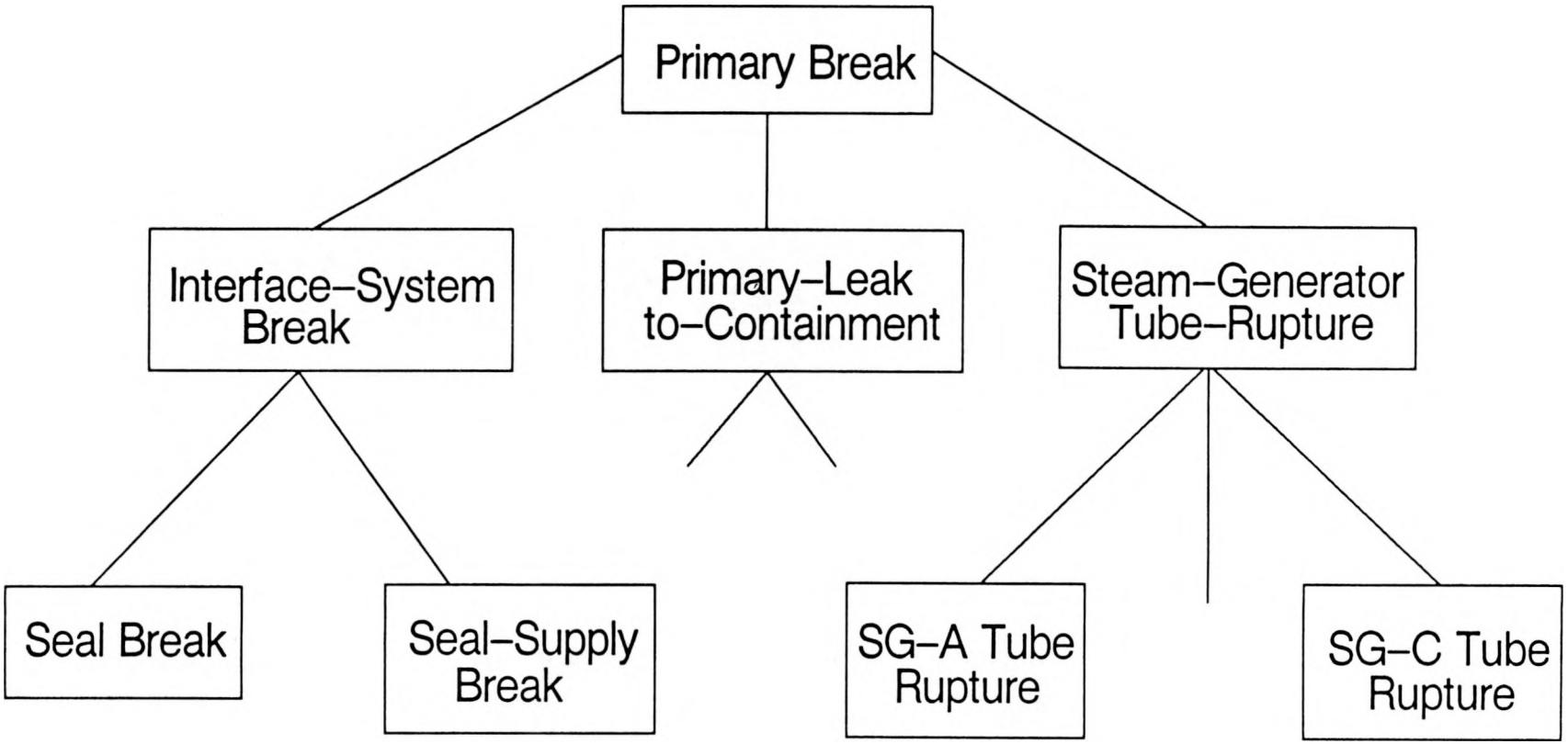

Figure 4–1. Hierarchy of diagnostic categories currently encoded in CES.

4.3.1 Case 1: "Textbook" Steam Generator Tube Rupture

The first run was a "textbook" steam generator tube rupture. The behavior of CES in this run paralleled the behavior of human operators on this event. It was able to definitively diagnose the steam generator tube rupture as soon as the air eject radiation alarm occurred. It then successfully identified the faulted steam generator (Steam Generator B in this case).

CES Output Protocol for Case 1:

Observations at time 40 concerning PRZR-LVL . . .

> We note a LOW-VALUE goal violation, yet the value of PRZR-LVL is continuing to DECREASE at a SLIGHT rate. This behavior can be accounted for by the SLIGHT DECREASING-PROGRESSION induced-by NET-CHG-LTDWN.
>
> *At this point, the program notices a goal violation: Pressurizer Level (PRZL-LVL) is below target value. Goal violations are one of several types of anomalies that might call for interpretive and/or control actions. In this case, the observed behavior is found to be consistent with the known influence (i.e., there is negative net charging), so no further analysis is called for.*

Observations at time 90 concerning PRZR-LVL . . .

> We note a discrepancy between the net-influence known to be impacting the behavior of PRZR-LVL and the observed behavior of this parameter -- the latter being a SOMEWHAT-GREATER DECREASING-PROGRESSION than the former. Because this is a relatively small difference, it may be nothing. Then again, it may suggest the presence of an unknown, abnormal influence.
>
> There is only one possible explanation for this:
>
> PRIMARY-BREAK is fairly strongly suggested by the observed behavior.
>
> The following behavior is consistent with this hypothesis, but could alternatively be explained by other known influences:
>
> PRZR-PRESS DECREASING-PROGRESSION . . fairly strongly suggestive
>
> *The tube-rupture fault, injected at time 80, causes an increased rate of outflow from the primary system. The program recognizes that the magnitude of this flow can no longer be accounted for by the net negative influence of the charging/letdown system, so it generates an "hypothesized influence" that must be explained. Because of the limitations of the current knowledge base, the only fault that the program knows about that can account for such an outflow is some sort of primary break, a category which includes the various types of LOCA's, tube-ruptures, etc. that might occur. A more complete knowledge base would also take account of energy events that can have an impact on primary coolant level. At this point the program also notices that pressurizer pressure (PRZR-PRESS) is also decreasing, and notes that this behavior is consistent with the primary break hypothesis.*

Observations at time 120 concerning PRZR-PRESS . . .

There is now unequivocal evidence of an unexplained DECREASING influence on PRZR-PRESS.

If we make the assumption that PRZR-PRESS and PRZR-LVL have a common cause, there would be only one possible explanation for this: PRIMARY-BREAK. With this evidence, the conclusion of PRIMARY-BREAK can be made with some confidence. More specifically, we find that the anomalous behavior in PRZR-PRESS and PRZR-LVL is due to one of the following: INTERFACE-SYSTEM-BREAK, STEAM-GENERATOR-TUBE-RUPTURE, or PRIMARY-LEAK-TO-CONTAINMENT.

The program has now concluded that the problem is indeed a primary break, based on the further evidence of an unexplained downward influence on primary pressure. It then considers the more specific categories of primary break faults, and for each -- it weighs the pros and cons, based on the availability and need for additional evidence. In the next section it goes through each type of break it knows of and lists each piece of evidence that would support that hypothesis and has not yet been observed. For each piece of evidence listed it indicates how strongly the piece of evidence would support the hypothesis if it were observed (e.g., "strongly indicative") and the certainty with which the piece of evidence would be expected if the hypothesis were true (e.g.,"fairly strongly indicated").

Concerning INTERFACE-SYSTEM-BREAK, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . weakly indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

Concerning STEAM-GENERATOR-TUBE-RUPTURE, the following expected change has not been observed:

AIR-EJECT-RAD INCREASING-PROGRESSION . . strongly indicative, fairly strongly indicated

Concerning PRIMARY-LEAK-TO-CONTAINMENT, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . moderately indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

Observations at time 190 concerning AIR-EJECT-RAD . . .

There is now unequivocal evidence of an unexplained INCREASING influence on AIR-EJECT-RAD.

If we make the assumption that AIR-EJECT-RAD and PRZR-LVL have a common cause, there would be only one possible explanation for this: STEAM-GENERATOR-TUBE-RUPTURE-PRESENT.

With this evidence, the conclusion of STEAM-GENERATOR-TUBE-RUPTURE can be made with some confidence. More specifically, we find that the anomalous behavior in AIR-EJECT-RAD, PRZR-PRESS, and PRZR-LVL is due to one of the following: S/G-C-TUBE-RUPTURE, S/G-B-TUBE-RUPTURE, or S/G-A-TUBE-RUPTURE.

Within two minutes of the onset of the tube-rupture fault, the program notes high levels of secondary radiation. Specifically the air eject radiation alarm goes off (air-eject-rad), which in conjunction with the earlier evidence of pressurizer level and pressure anomalies, signals a tube-rupture in one of the steam generators. This provides no basis for localizing the fault further, however. Which of the three steam generators is the faulted one remains to be resolved.

We note the occurrence of a RX-TRIP at time 350. Consequences of this include:

TURB-POWER DECREASING-PROGRESSION
NUC-POWER DECREASING-PROGRESSION
PRZR-TARG-LVL DECREASING-PROGRESSION
T-REF DECREASING-PROGRESSION

Certain events cause the program to revise its concept concerning what constitutes nominal behavior. Here we see the program taking note of some of the changes in parameter behaviors that are to be expected following a reactor trip (RX-TRIP). With this knowledge "in mind", the program will not attempt to find other explanations for these behaviors as they occur -- but it will note and attempt to find explanations for behaviors that fail to conform to these expectations.

We note the occurrence of a PRE-RESET-SI-SIG at time 350. Consequences of this include:

CHG-FLO DECREASING-PROGRESSION
CHG-ECCS-FLO-B INCREASING-PROGRESSION
CNTMT-PH-A-SIG YES

Similarly at this point the program notes that safety injection has come on (PRE-RESET-SI-SIG) and lists the changes in the plant that it expects as a result.

Observations at time 350 concerning T-AVG . . .

We note a LOW-VALUE goal violation,

At this point the program notes that primary system temperature (T-AVG) is low. Incompleteness of the knowledge base prevents the program from generating hypotheses to account for this, but it calls attention to the problem.

Observations at time 600 concerning S/G-LVL-B . . .

We note a discrepancy between the net-influence known to be impacting the behavior of S/G-LVL-B and the observed behavior of this parameter -- the latter being a GREATER INCREASING-PROGRESSION than the former. Because this is a fairly significant difference, it almost surely suggests the presence of an unknown, abnormal influence.

There is only one possible explanation for this: a S/G-B-TUBE-RUPTURE, which can fully explain the observed abnormality in PRZR-LVL.

What the program looks for in order to clinch the diagnosis of a tube-rupture in a specific steam generator is a situation where the level of water in the steam generator is rising at a faster rate than can be explained on the basis of known inputs. In this case, the operator has turned off feed-water to steam-generator B but the level has continued to increase -- leading to the diagnosis of a steam generator tube rupture in steam generator B (S/G-B-TUBE-RUPTURE).

4.3.2 Case 2: "Tube Rupture With Loss of Offsite Power and Seal Break (Refined Knowledge)"

In the second case there are several faults present in addition to the tube rupture that complicates the diagnosis. In particular, a power outage occurs that lasts approximately a minute, that results in the loss of the air eject radiation alarms. (Without power, the condenser vacuum fails preventing the normal venting of steam and water vapor past the radiation sensors.) This means that an important leading indicator supporting diagnosis of the tube rupture is no longer available. In addition, a seal leak is introduced in each of the reactor coolant pumps (A plausible consequence of the power outage). This complicates the diagnosis further since the seal leak can partially account for the symptoms observed.

Case 2 and 3 were run using exactly the same NPP incident, the only thing that varies between the two cases is the knowledge that CES possesses about seal leaks. In particular, in Case 2 the knowledge encoded in CES included the fact that seal leaks could only have a moderate effect on the rate of decrease in pressurizer level. This knowledge was sufficient to allow CES to recognize that the seal leak could not entirely account for the rate of decrease in pressurizer level and that it needed to identify an additional unknown influence, that is, the tube rupture. CES successfully diagnosed both the seal leak and the tube rupture. It then went on to correctly identify the faulted steam generator (Steam Generator C in this case).

In Case 2, the knowledge encoded in CES describing the relationship between pressurizer level (PRZR-LVL) behavior and the possibility of a seal break contains a constraint limiting the qualitative magnitude of the PRZR-LVL decrease that can be explained. The specific 'coupler' included in the CES knowledge base was:

```
(defcplr t7
      (occurrence #$x seal-break)
   (and ((influence #$p total-seal-inj-flo
         (congruent $!(type (behavior #$p)) increasing-progression)
         ) 4 2)
   ((influence #$q przr-lvl
         (qual-lessp #!(magnitude #$q) moderate)) 2 2))
   (and (occurrence #$y total-seal-inj-flo)
      (relator (#!(level #$y))
         ((> 40))))
   )}
```

Couplers are the basic unit of knowledge representation in CES (see section 4.5). This coupler indicates that seal breaks cause total-seal-injection flow to increase and pressurizer level to increase, but puts a limit on how large an effect it can have on pressurizer level (i.e., only a moderate amount).

CES Output Protocol for CASE 2:

> *For the first 100 seconds or so, this case follows much the same course as the previous one. The principal difference is that there is a power failure that complicates the tube-rupture scenario, causing numerous secondary faults in pumps, seals, power-operated valves, sensors, etc. These have their own consequences, which begin to show up around time step 110.*

Observations at time 10 concerning PRZR-LVL . . .

> We note a LOW-VALUE goal violation, yet the value of PRZR-LVL is continuing to DECREASE at a SLIGHT rate. This behavior can be accounted for by the SLIGHT DECREASING-PROGRESSION induced-by NET-CHG-LTDWN.

We note the occurrence of a RX-TRIP at time 70. Consequences of this include:

> TURB-POWER DECREASING-PROGRESSION
> NUC-POWER DECREASING-PROGRESSION
> PRZR-TARG-LVL DECREASING-PROGRESSION
> T-REF DECREASING-PROGRESSION

We note the occurrence of a POWER-FAILURE at time 70. Consequences of this include:

> AUX-FEED-MOTOR-C DISABLED
> AUX-FEED-MOTOR-B DISABLED
> AUX-FEED-MOTOR-A DISABLED
> CNDNSR-VACUUM DISABLED
> LTDWN-ACTUATOR DISABLED
> CHG-PUMP DISABLED
> RX-TRIP YES

Observations at time 90 concerning PRZR-LVL . . .

We note a discrepancy between the net-influence known to be impacting the behavior of PRZR-LVL and the observed behavior of this parameter -- the latter being a SOMEWHAT-GREATER DECREASING-PROGRESSION than the former. Because this is a relatively small difference, it may be nothing. Then again, it may suggest the presence of an unknown, abnormal influence.

There is only one possible explanation for this:

PRIMARY-BREAK is fairly strongly suggested by the observed behavior.

The following behavior is consistent with this hypothesis, but could alternatively be explained by other known influences:

PRZR-PRESS DECREASING-PROGRESSION . . fairly strongly suggestive

Observations at time 100 concerning PRZR-PRESS . . .

There is now unequivocal evidence of an unexplained DECREASING influence on PRZR-PRESS.

If we make the assumption that PRZR-PRESS and PRZR-LVL have a common cause, there would be only one possible explanation for this: PRIMARY-BREAK. With this evidence, the conclusion of PRIMARY-BREAK can be made with some confidence. More specifically, we find that the anomalous behavior in PRZR-PRESS and PRZR-LVL is due to one of the following: INTERFACE-SYSTEM-BREAK, STEAM-GENERATOR-TUBE-RUPTURE, or PRIMARY-LEAK-TO-CONTAINMENT

Concerning INTERFACE-SYSTEM-BREAK, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . weakly indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

Concerning STEAM-GENERATOR-TUBE-RUPTURE, the following expected change has not been observed:

AIR-EJECT-RAD INCREASING-PROGRESSION . . strongly indicative, fairly strongly indicated

Concerning PRIMARY-LEAK-TO-CONTAINMENT, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . moderately indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

At time step 100 CES notes that the decreases in pressurizer pressure and pressurizer level are too large to be accounted for by known influences. This causes it to conclude that there is a primary break. At this point however, it is unable to further specify the nature of the break.

Observations at time 110 concerning T-AVG . . .

We note a HIGH-VALUE goal violation, the cause of which can be traced to the CONDENSER-STEAM-DUMPS being used to REGULATE T-AVG.

More specifically, the problem is apparently due to the CNDNSR-VACUUM being in DISABLED rather than OPERABLE state.

CES notes that T-AVG (mean temperature in the primary reactor vessel) is high. It recognizes this as a goal vilolation and attempts to explain the goal violation and to take action to correct it.

T-AVG is high because the power failure, among other things, resulted in the loss of condenser vacuum (CNDNSR-VACUUM). This effectively eliminated the condenser steam dumps as a heat sink. CES recognizes this, and marks this system "unavailable" as a means of controlling T-AVG. It selects the atmospheric steam dumps -- the steam-generator pressure operated relief valves (PORV's) -- as primary backups for temperature control.

Observations at time 140 concerning SEAL-RETURN-FLO-C . . .
A HIGH-VALUE suggests an abnormal INCREASING-PROGRESSION influence.

There is only one possible explanation for this: a SEAL-BREAK, which can account for only part of the observed abnormality in PRZR-LVL.

The power outage in this case lasted approximately 60 seconds, long enough for the lack of adequate cooling to damage the seals on the reactor coolant pumps. This was purposely prolonged by the experimenter to complicate the process of diagnosis, by providing an alternate explanation for primary pressure and level behavior. Note that in this case, the program has correctly diagnosed the seal break, but recognized that the magnitude of the apparent LOCA cannot fully be explained by the relatively minor losses expected with a seal break.

We note the occurrence of a PRE-RESET-SI-SIG at time 230.
Consequences of this include:

CHG-FLO DECREASING-PROGRESSION
CHG-ECCS-FLO-B INCREASING-PROGRESSION

These two changes reflect the substitution of safety injection for normal charging flow.

CNTMT-PH-A-SIG YES

A note of caution at time 230 concerning the means to REGULATE T-AVG:

The actions DEACTIVATION S/G-C-PORV-BLOCK-VALVE, DEACTIVATION S/B-B-PORV-BLOCK-VALVE and DEACTIVATION S/G-A-PORV-BLOCK-VALVE have left as the best remaining method for pursuing this goal BLEED-AND-FEED, which entails some adverse consequences. We must consider the rationale for these changes to see whether they might be reversed. These actions were apparently taken to PREVENT RADIOACTIVE-EMISSIONS in the event that one of the following abnormal conditions is present: S/G-A-TUBE-RUPTURE S/G-B-TUBE-RUPTURE S/G-C-TUBE-RUPTURE.

The program has knowledge of the various primary and backup control regimes that are available for regulating goal-related parameters within nominal limits. The several methods for maintaining T-AVG, for example, include condenser steam dumps, atmospheric steam dumps, and pressurizer PORV's (the bleed and feed operation). These methods are described to the program in terms of their enabling conditions, principal effects and side effects.

The program's comment above arises as a result of actions to close the steam-generator PORV block valves -- something that an operator, concerned about the prospect of radioactive emission from a suspected tube-rupture, might do (cf. Ginna). The program has noticed the valve closings, and drawn out the implication with respect to availability of the steam-generator PORV's as potential steam dumps. It notes further that because of these actions, following on the heels of the failure of the condenser steam dumps, the steam generators are essentially lost as heat sinks, leaving only the undesirable option of bleed and feed on the primary side to control temperature in the reactor vessel.

Rather than accept this restricted option set, the program then undertakes to refute, if possible, the rationale underlying the actions taken (i.e., to determine whether there is any justification for keeping the steam generator PORV block valves closed.)

On checking the decision context, we find that there is an unresolved decision task that includes S/G-C-TUBE-RUPTURE, S/G-B-TUBE-RUPTURE and S/G-A-TUBE-RUPTURE. Efforts should be undertaken to rule these out if possible.

Since CES is still entertaining the possibility of a steam generator tube rupture it is unable to refute the need to keep the PORV block valves closed (i.e., to prevent radioactive release to the atmosphere in case of a tube rupture). CES indicates that a tube rupture must be ruled out before the action of closing the PORV block valves can be rescinded.

Observations at time 370 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 410 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 460 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 480 concerning S/G-LVL-C . . .

We note a discrepancy between the net-influence known to be impacting the behavior of S/G-LVL-C and the observed behavior of this parameter -- the latter being a GREATER INCREASING-PROGRESSION than the former. Because this is a fairly significant difference, it almost surely suggests the presence of an unknown, abnormal influence.

There is only one possible explanation for this: a S/G-C-TUBE-RUPTURE, which can fully explain the observed abnormality in PRZR-LVL.

CES successfully diagnoses the tube rupture at this point when it notices that level in steam generator C is increasing at a faster rate than can be explained on the basis of known influences. Specifically it notices that level is continuing to rise even though feedwater to the steam generator has been turned off.

At this point, the case can be made for restoring the secondary heat sink by reopening the block valves on the other two steam generators, a capacity that the program does not yet exhibit.

Observations at time 480 concerning CNTMT-AMBIENT-TEMP . . .

There is now unequivocal evidence of an unexplained INCREASING influence on CNTMT-AMBIENT-TEMP. This is consistent with the diagnosis of SEAL-BREAK, previously noted.

Observations at time 500 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 550 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 610 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

4.3.3 Case 3: "Tube Rupture With Loss of Offsite Power and Seal Break (Naive Knowledge)"

Case 3 is the exact same NPP event as case 2. The only difference between the runs is in the knowledge encoded in the CES knowledge base. In particular, the knowledge encoded in CES about seal leaks was less refined in Case 3 than in Case 2. Whereas in Case 2 CES knew that seal leaks could only have a moderate effect on the rate of decrease in pressurizer level, in Case 3 CES did not know this. The knowledge about seal leaks encoded in the CES knowledge base indicated that seal leaks produce a decrease in pressurizer level, but did not include any information on the magnitude of effect to be expected. As a result when CES

found a seal leak it concluded that it had accounted for all the known plant symptoms and failed to diagnose the Tube Rupture.

In case 3 the coupler dealing with the seal break is changed so that there is no constraint on the magnitude of PRZR-LVL decreasing rate. The revised coupler is:

```
(defcplr t7
       (occurrence #$x seal-break)
  (and ((influence #$p total-seal-inj-flo
       (congruent $!(type (behavior #$p)) increasing-progression)
           ) 4 2)
   ((influence #$q przr-lvl
           ) 2 2))
   (and (occurrence #$y total-seal-inj-flo)
       (relator (#!(level #$y))
           ((> 40))))
   )
```

With respect to seal leaks this version of CES can be thought of as representing the knowledge of a highly inexperienced operator who understands the direction of effect to expect, but has not yet gained a feel for the relative magnitude of effects to expect. Knowledge of size of effects to expect is often referred to as "process feel", and is something that is built up from experience.

The Case 3 CES output is the same as the Case 2 output until the point where CES detects the seal leak (time-step 140). At that point, CES erroneously concludes that the seal leak can completely account for pressurizer level behavior.

It fails to diagnose the Tube Rupture and generates an intention to take an action (open the steam generator PORV block valves on all the steam generators, (including the faulted one) that could have serious negative consequences (release of radiation through the faulted steam generator).

CES Output Protocol for Case 3:

> ***This case uses exactly the same set of input data values as the preceding run; the only change is in the knowledge base. The program's behavior begins to deviate at time-step 140, where it makes an erroneous judgement concerning the seal break, and this in turn leads to a serious error of commission at time step 230.***

Observations at time 10 concerning PRZR-LVL . . .

> We note a LOW-VALUE goal violation, yet the value of PRZR-LVL is continuing to DECREASE at a SLIGHT rate. This behavior can be accounted for by the SLIGHT DECREASING-PROGRESSION induced-by NET-CHG-LTDWN.

We note the occurrence of a RX-TRIP at time 70. Consequences of this include:

TURB-POWER DECREASING-PROGRESSION
NUC-POWER DECREASING-PROGRESSION
PRZR-TARG-LVL DECREASING-PROGRESSION
T-REF DECREASING-PROGRESSION

We note the occurrence of a POWER-FAILURE at time 70. Consequences of this include:

AUX-FEED-MOTOR-C DISABLED
AUX-FEED-MOTOR-B DISABLED
AUX-FEED-MOTOR-A DISABLED
CNDNSR-VACUUM DISABLED
LTDWN-ACTUATOR DISABLED
CHG-PUMP DISABLED
RX-TRIP YES

Observations at time 90 concerning PRZR-LVL . . .

We note a discrepancy between the net-influence known to be impacting the behavior of PRZR-LVL and the observed behavior of this parameter -- the latter being a SOMEWHAT-GREATER DECREASING-PROGRESSION than the former. Because this is a relatively small difference, it may be nothing. Then again, it may suggest the presence of an unknown, abnormal influence.

There is only one possible explanation for this:

PRIMARY-BREAK is fairly strongly suggested by the observed behavior.

The following behavior is consistent with this hypothesis, but could alternatively be explained by other known influences:

PRZR-PRESS DECREASING-PROGRESSION . . fairly strongly suggestive

Observations at time 100 concerning PRZR-PRESS . . .

There is now unequivocal evidence of an unexplained DECREASING influence on PRZR-PRESS.

If we make the assumption that PRZR-PRESS and PRZR-LVL have a common cause, there would be only one possible explanation for this: PRIMARY-BREAK. With this evidence, the conclusion of PRIMARY-BREAK can be made with some confidence. More specifically, we find that the anomalous behavior in PRZR-PRESS and PRZR-LVL is due to one of the following: INTERFACE-SYSTEM-BREAK, STEAM-GENERATOR-TUBE-RUPTURE, or PRIMARY-LEAK-TO-CONTAINMENT

Concerning INTERFACE-SYSTEM-BREAK, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . weakly indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . weakly indicative, fairly strongly indicated

Concerning STEAM-GENERATOR-TUBE-RUPTURE, the following expected change has not been observed:

AIR-EJECT-RAD INCREASING-PROGRESSION . . strongly indicative, fairly strongly indicated

Concerning PRIMARY-LEAK-TO-CONTAINMENT, the following expected changes have not been observed:

CNTMT-PRESS INCREASING-PROGRESSION . . moderately indicative, fairly weakly indicated

CNTMT-SUMP-LVL INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

CNTMT-AMBIENT-TEMP INCREASING-PROGRESSION . . moderately indicative, fairly strongly indicated

Observations at time 110 concerning T-AVG . . .

We note a HIGH-VALUE goal violation, the cause of which can be traced to the CONDENSER-STEAM-DUMPS being used to REGULATE T-AVG.

More specifically, the problem is apparently due to the CNDNSR-VACUUM being in DISABLED rather than OPERABLE state.

Observations at time 140 concerning SEAL-RETURN-FLO-C . . .
A HIGH-VALUE suggests an abnormal INCREASING-PROGRESSION influence.

There is only one possible explanation for this: a SEAL-BREAK, which can fully explain the observed abnormality in PRZR-LVL.

At this point CES successfully diagnoses the seal break.

Note that in the absence of knowledge concerning likely rates and magnitudes of effects, the program has no basis for concluding that this seal break cannot entirely account for the rate of decrease in pressurizer level and pressure. It concludes that the seal leak accounts for all the anomalies observed, which leads to a serious error of commission at time step 230.

We note the occurrence of a PRE-RESET-SI-SIG at time 230.
Consequences of this include:

CHG-FLO DECREASING-PROGRESSION
CHG-ECCS-FLO-B INCREASING-PROGRESSION
CNTMT-PH-A-SIG YES

A note of caution at time 230 concerning the means to REGULATE T-AVG:

The actions DEACTIVATION S/G-C-PORV-BLOCK-VALVE, DEACTIVATION S/B-B-PORV-BLOCK-VALVE and DEACTIVATION S/G-A-PORV-BLOCK-VALVE have left as the best remaining method for

pursuing this goal BLEED-AND-FEED, which entails some adverse consequences. We must consider the rationale for these changes to see whether they might be reversed. These actions were apparently taken to PREVENT RADIOACTIVE-EMISSIONS in the event that one of the following abnormal conditions is present: S/G-A-TUBE-RUPTURE, S/G-B-TUBE-RUPTURE or S/G-C-TUBE-RUPTURE.

On checking the decision context, we find that S/G-A-TUBE-RUPTURE, S/G-B-TUBE-RUPTURE and S/G-C-TUBE-RUPTURE were at one time part of the diagnostic considerations to explain the PRZR-LVL behavior.

However, that abnormal behavior has subsequently been explained by SEAL-BREAK. Therefore, the purpose behind these actions is no longer relevant, and they should be rescinded forthwith.

Again, the program attempts to refute the rationale for the actions that caused a loss of effective temperature control. In this case, however, it develops what it takes to be a convincing, albeit erroneous, argument based on its belief that the previously concluded seal break accounts for the observed anomalies in primary level and pressure. Because of this, the program fails to activate the knowledge required to detect anomalies in steam generator level behavior, and therefore fails to diagnose the tube rupture. It concludes that the steam generator PORV block valves can be re-opened.

Observations at time 370 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 410 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 460 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 480 concerning CNTMT-AMBIENT-TEMP . . .

There is now unequivocal evidence of an unexplained INCREASING influence on CNTMT-AMBIENT-TEMP. This is consistent with the diagnosis of SEAL-BREAK, previously noted.

Observations at time 500 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 550 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

Observations at time 610 concerning T-AVG . . .

We note a HIGH-VALUE goal violation

4.4 EVALUATION OF CES CASE RUNS

The three case runs successfully demonstrate the ability of CES to follow a dynamically changing event using actual high fidelity NPP control room simulator data as input. This in itself is a significant achievement.

In addition the runs demonstrate the ability of CES to provide insight into which accident scenarios will be straightforward to diagnose and which will be cognitively demanding. CES was able to diagnose the "text-book" tube rupture rapidly. It had more difficulty with the tube rupture with loss of off-site power. In this respect the performance of CES closely paralleled the performance of human operators under similar conditions. A simulation model that can objectively demonstrate which accident scenarios of interest are straightforward to diagnose and which are likely to be error-prone can be a valuable tool for HRA analyses.

The runs also successfully demonstrated the ability to change CES parameters to produce plausible changes in behavior on the same accident situations. Case 2 and 3 were run on exactly the same accident scenario; the only difference was in the knowledge CES had about seal leaks. In Case 2 where CES had refined knowledge about seal leaks and their potential magnitude of effects, it successfully diagnosed a complex multiple failure event. In Case 3 where there were gaps in the CES knowledge about how large the effects of a seal leak could be, CES failed to diagnose the Tube Rupture. Further, it decided to take an action (an error of commission) that could have serious consequences. It decided to open the steam generator PORV block valves, which could potentially lead to radioactive release to the atmosphere through the faulted steam generator.

Case 2 and 3 begin to demonstrate how modifications to the CES knowledge base can be used to model differences in knowledge among operators (e.g., experienced versus inexperienced operators), and the implication of gaps in knowledge or faulty knowledge on how operators are likely to act in different accident scenarios.

4.5 CURRENT CES KNOWLEDGE BASE

The CES knowledge base established under the early CES development work was quite limited. Steam generator tube rupture events involve a very large amount of plant functions and systems. This necessitated expanding the knowledge base to address more aspects of the NPP. The expansion of NPP knowledge was limited to those aspects that are critical to operator decisions and actions in these tube rupture events. This section describes the current state of the CES knowledge base.

There are several kinds of expressions in the knowledge base for CES that can be used to represent specific knowledge that an operator or team may possess about the plant and also the organization of that knowledge. The most basic unit of knowledge representation is called a *coupler*. Couplers express a relation about the NPP. For example, "primary-break" is coupled to "pressurizer level". When either terminus (or node) is activated, the item it is coupled with is suggested (thus reasoning can flow in both directions). If "decreasing pressurizer level" is activated (e.g., a level decrease is observed from some instrument or display), then it suggests the possibility of "primary break"; and if "primary break" is activated (i.e., suspected or deduced), then it suggests "decreasing pressurizer level".

The following provides a stylized version of a coupler describing the effect of a primary break on pressurizer level and pressurizer pressure:

Occurrence: Primary-break

Influence: PRZR-LVL
Behavior: Decreasing-Progression
Influence: PRZR-PRESS
Behavior: Decreasing-Progression

Note that for economy of representation, a single coupler can encode the relationship between one "occurrence" and several "influences". In this case the effect of a primary break on pressurizer level and pressure is encoded in a single coupler.

The nodes in a coupler can represent potentially observable plant behaviors (e.g., "decreasing pressurizer level") or plant states that are inferred from observable data (e.g., "inadequate heat sink"; "steam generator tube rupture").

A coupler also encodes the strength of relation between the two items linked. For example, associated with the coupler linking "pressurizer level" and "steam generator tube rupture" is a strength value that reflects how strongly knowing that pressurizer level is decreasing suggests the possibility of a steam generator tube rupture. Since couplers allow bi-directional inference and since the strength of implication need not be identical in both directions, there are two strength values associated with each relationship in a coupler, one for the strength of association in each direction. For example, a steam generator tube rupture definitely is an influence to decrease pressurizer level, while decreasing pressurizer level by itself merely suggests the possibility of a steam generator tube rupture because it could indicate other conditions as well. The strength parameters take on values between 1 and 5, with 5 indicating the strongest relation.

Another part of a coupler is called the *relator*. The relator expresses conditionalities in the relationship between the two sides of the coupler. This can be used in several ways. For example, the relator can specify different conditions that vary the specific nature of the relationship between the two items, e.g., the relationship between "pressurizer level" and "steam generator tube rupture" varies depending on "primary/secondary pressure differential".

It can also be used to specify the context in which a relation applies. For example, the relator can be used to indicate that pressurizer pressure will only affect pressurizer relief tank level when the pressurizer relief valve and block valve are open.

The coupler below illustrates the use of a relator in a coupler:

Occurrence: Adjust-rate-transaction
Subject: Operator
Object: Chg-flow
Direction: Increase

Influence: PRZR-LVL
Behavior: Increasing-Progression

Relator: Chg-pump
State: Operable

This coupler describes the effect of an operator action (controlling charging flow) on pressurizer level. The relator is used to encode the fact that charging can only be used to control pressurizer level when the charging pumps (Chg-pump) are operable (i.e., the pumps have to be operable for there to be charging flow).

This example also illustrates one of the primary strengths of the coupler formalism -- the same mechanism is used to represent both normal influences that result from control activities of operators or automatic systems (e.g., manual control of charging flow) and abnormal influences that result from faults (e.g., a primary break).

The fact that the same basic formalism is used to represent both normal and abnormal influences is important because it allows CES to track and sort out the multiple factors that impact plant process behavior during the course of an emergency event. It allows CES to maintain and update expectations about the behavior of plant processes as different factors that influence those processes are introduced or removed (e.g., when Safety Injection comes on, or is turned off). The ability to keep track of the multiple influences that are impacting on plant processes at any given time, both normal and abnormal, allows CES to form expectations about plant process behavior based on the known influences. If plant behavior deviates from expectation, CES is able to immediately note the discrepancy and search for additional unknown influences that might be accounting for the discrepancy. This allows CES to identify disturbances against the changing background of normal process dynamics. It also allows CES to keep track of faults even when their effect on plant processes is masked (e.g., when Safety Injection comes on causing pressurizer level to increase in spite of a break). Lastly it allows CES to detect and track multiple faults that are simultaneously influencing plant process behavior.

The couplers provided above are presented in a stylized form for ease of comprehension. Examples of couplers in the actual form encoded in the CES knowledge base appear in Section 4.3.

Another feature of the knowledge representation formalism is that plant states can be linked together in a hierarchy of concepts. For example, a steam generator tube rupture and a primary break to containment are both kinds of primary system breaks. Figure 4-1 shows the hierarchy of diagnostic categories currently encoded in CES.

This knowledge representation provides a powerful and flexible mechanism for representing knowledge about plant structure and function, disturbances and faults, goals and responses that NPP operators would be expected to know. Set up of the knowledge base requires data or hypotheses about what operational personnel do know (e.g., based on analysis of training programs). Knowledge provided to operators through external means such as procedures is also captured here. One can modify the information encoded in the knowledge base to represent differences that might exist among operators with respect to the depth and accuracy of the knowledge they possess about an NPP issue (e.g., simplistic versus highly accurate mental models of an NPP process). The knowledge representation can also be used to capture different organizations of plant knowledge that might reflect differences between less experienced and more experienced operators.

4.6 EXPANSION OF CES CAPABILITIES

The basic CES model architecture is reported in NUREG/CR-4862 Volume 2. There were two areas where significant enhancement in CES reasoning capabilities needed to be made to successfully run the three test cases: 1) in the ability to reason qualitatively about changes in parameter rates; 2) in the ability to detect safety goal violations and to identify and reason about options available for satisfying the safety goal.

Expanding Qualitative Reasoning about Rates of Change
In the past CES was only sensitive to direction of movement of plant parameters (e.g., either increasing or decreasing). There was no way to represent the magnitude of rate of change associated with different actions or events. For example, there was no way to distinguish the change in pressurizer level that would result from a small negative net charging from the change in pressurizer level that would result from a massive primary break. They both would be marked as resulting in a decrease in pressurizer level. As a result, CES could only detect and reason about situations where the direction of plant parameters was counter to the direction expected given the set of known influences on that parameter. For example, if pressurizer level was going down, and CES knew that there was positive net charging, it would mark the decrease in pressurizer level as an unexpected finding and search for the unknown influence that could account for pressurizer level behavior. However, if CES knew that there was negative net charging, then it would not detect abnormal decreases in pressurizer level behavior no matter how large, because it expected pressurizer level to be decreasing. It had no way to distinguish small rates of change from large rates of change.

In order to produce plausible behavior in the current set of runs it was necessary to expand the qualitative reasoning ability of CES. The knowledge representation formalism was expanded to encode and reason about the *magnitude* of rate of change in plant parameters that different normal and abnormal conditions would be expected to produce. It is now possible to distinguish the "small" rate of change in pressurizer level that would be expected from a small negative charging situation from the "large" rate of change that would be expected given a large tube rupture. This allows CES to be much more sensitive in detecting unexpected situations that require explanation. It can detect abnormal plant parameter behavior even in cases where the set of known influences can account for the observed direction of change of a parameter.

This capability was utilized in the present case runs to detect that the pressurizer level decrease is too large to be accounted for by the fact that let down is greater than charging, and to diagnose the presence of some kind of primary system break. It was also used in Case 2 to aid CES to identify multiple simultaneous faults: A seal leak and a tube rupture both simultaneously contributing to a decrease in pressurizer level. In that run CES first identified the seal leak, but recognized that the rate of decrease of pressurizer level was too great to be accounted for by the seal leak alone. It then searched further and uncovered the existence of a steam generator tube rupture as well.

Expanding Capability to Reason about Goals and Options Available to Meet Them
Another capability that was expanded was the ability to represent and reason about goals, goal violations, and alternative means for achieving critical NPP goals. The current version of CES includes the capability to represent critical NPP goals

such as regulating primary pressure or regulating T_{ave} (average temperature in the reactor vessel), the alternative options available for achieving those goals, and the desirability of each of those options. As example, one goal encoded in the CES knowledge base is to regulate primary system temperature (T_{ave}). Associated with the goal is a list of alternative means available for achieving that goal such as using the condenser steam dumps, the steam generator PORVs, or the pressurizer PORV. Each option has associated with it a "payoff" value that represents the desirability of that option. For example, the generally preferred option for controlling T_{ave} is automatic control via the condenser steam dumps and that option is assigned a value of 10; conversely, using the pressurizer PORVs to control primary system temperature (i.e., going to a bleed and feed) is a last resort option with negative consequences, so it is assigned a negative value of -5.

For each goal to be achieved CES dynamically keeps track of the means currently being used to achieve the goal (the one "selected"); what additional options are available for achieving the goal but are not currently being used (these are marked as "available"); and which options are currently unavailable (for example because they are being used in a conflicting manner in support of some other goal).

The ability to represent and dynamically keep track of alternative options available for achieving a goal greatly expands the capability of CES to reason about what are appropriate actions to take to achieve a desired goal. The current version of CES continuously monitors for violations of critical safety goals (e.g., primary pressure and temperature). If a goal violation is detected, a *goal tender* is created with the responsibility of deciding which of the available means are appropriate for reachieving the goal. This is normally accomplished by selecting the most desirable option among the ones available (i.e., the one with the highest "payoff" value); however in cases where none of the available options are desirable (e.g., where the available options all have negative values), CES will first examine each of the options that are coded as "unavailable" to determine the reasons they cannot be employed. If it determines that the grounds for an option being unavailable is no longer valid, or is not valid given the particular context, it will decide to reinstate that option rather than resort to an undesirable option.

The ability of CES to reflect on the rationale behind actions, and to rescind an action if it decides the rationale is not relevant in the current context, is a powerful feature. It allows CES to respond in a context-dependent manner. It also allows CES to take actions that go beyond the prescribed procedures. This enables CES to model the kind of reasoning that can lead operators to actions that go beyond procedures.

In the current set of runs this capability was used by CES to reason about the control of T_{ave}. In these runs after the tube rupture, the condenser steam dumps became unavailable, and the steam generator PORVs were all closed. T_{ave} became abnormally high and CES needed to decide on how to bring T_{ave} down. The only remaining option available was to go to a feed and bleed. Since this is a highly undesirable option, CES first examined the reasons why the steam generator PORVs were closed. It reasoned that the PORVs were closed to prevent radiation release through the faulted steam generator. It decided to isolate the faulted steam generator and use the PORVs on the remaining steam generators to control T_{ave} rather than go to a bleed and feed.

5. EVALUATION ACTIVITY 3: THE CREATE WORKSHOP

5.1 OBJECTIVES AND APPROACH

This chapter describes the third part of the evaluation efforts which examined the CREATE methodology for using the CES modeling tool in HRA. The approach was to hold a workshop where three HRA practitioners and researchers reviewed a worked example of how CES and the CREATE methodology can provide input on human reliability in PRA studies.

A package detailing the CREATE methodology and its application in the worked example was developed prior to the workshop for review by the workshop attendees. The example was developed around the textbook steam generator tube rupture and more diagnostically difficult variations on this root incident that formed the basis for the CES runs. Since the complete set of CES runs was not yet available at the time the workshop was held, the worked example was based on hypothetical CES runs.

The CREATE Workshop was held July 18 and 19, 1988. Tables 5-1 and 5-2 contain the agenda and objectives for the workshop. The workshop included a demonstration of the CES simulation running in tandem with a plant simulation and detailed discussions of the worked example prepared prior to the workshop. Based on going through the worked example of the CREATE process, the participants provided feedback on the internal consistency and viability of the CREATE procedure.

5.2 CREATE EXAMPLE

Consider a question a PRA or HRA analyst may ask -- what is the likelihood that the operators will correctly diagnose a steam generator tube rupture (cf., the Seabrook PRA study where this question was asked)?

The difficulty of this operator task is related to the crew's ability to carry out various cognitive or information processing activities: What information must be monitored and gathered? What knowledge must be activated and utilized to determine the state of the plant and appropriate responses?

The CES/CREATE approach to HRA is based on the *demand-resource mismatch* view of human error (Rasmussen, 1986; Woods, 1989). In this view, the difficulty of a problem depends on both the demands posed by the problem itself and on the resources (e.g., knowledge, plans) available to solve the problem.

One can test the difficulty posed by a domain incident, given some set of resources, by running the incident through the CES simulation. CES is used to translate from the language of NPPs to the language of problem solving i.e., what knowledge is available to be used and how is it activated and brought to bear in the cognitive activities involved in solving dynamic problems? One can investigate how changes in the incident (e.g., obscuring evidence, introducing another failure) affect the difficulty of the problem for a given set of knowledge resources.

Table 5-1

CREATE WORKSHOP AGENDA

July 18, 8 am - 12

Introduction, Logistics and Objectives
D. Woods

Briefing on CES
D. Woods

Demonstration of CES during simulate plant incident
H. Pople, D. Woods, E. Roth

Briefing on CREATE
E. Roth
1 pm - 5 pm

Overview of the Example Incident
D. Woods & E. Roth

Work through CREATE steps of the example incident
All
July 19, 8 am - 12

Work through CREATE steps for the example incident
All
1 pm - 5 pm

Discussion of worked example:
Implications for PRA/CREATE interface
All

Wrap up

Table 5-2
CREATE WORKSHOP

Objective

To obtain input from experts in HRA on how the CES model can be used in PRA studies to improve estimates of human cognitive reliability.

- areas where CREATE provides new information to be used in the PRA or requires new information from the PRA;
- areas were the interface between CREATE and PRA techniques requires more detailed specification;
- new avenues for utilizing CES to illuminate human reliability issues.

Method

Work through an example incident using CES runs to provide input on human reliability.

Conversely, one can investigate how changes in the knowledge resources (e.g., improved mental models of device function) or processing resources (e.g., the size of the field of attention) affect performance, especially errors of commission.

The first step in the modeling stage of the CREATE process is to define problem difficulty event trees. Typically, root accidents or event sequences defined during the event tree formulation stage in the PRA systems analysis stage will be underspecified with respect to features of the situation that impact information processing and problem solving. A critical element of CREATE is to define plausible variants of the root events that can lead to increased cognitive task complexity. The problem difficulty event tree defines variants on the root accident sequence that challenge the problem solving capabilities of the operator because they degrade the ability to perform required tasks or because they impose additional tasks.

The heuristic for building the problem difficulty event tree is to identify *complicating factors*, that is, some variation or difficulty that goes beyond the standard method for handling the situation such as:

- human execution errors,
- additional machine failures (e.g., valves that stick open, systems that fail to work as demanded),
- missing information (e.g., sensor failures),
- multiple major faults (tube rupture with an unisolatable steam release from the faulted steam generator),
- situations which remove or obscure the usual evidence or critical evidence (e.g., a loss of leading indicator incident such as a loss of offsite power prior to a steam generator tube rupture),
- complex situations where different parts of the situation suggest responses which conflict with each other (e.g., the Ginna incident),
- situations that require actions that depart from the usual (e.g., total loss of feedwater).

Examination of simulator studies and actual incidents revealed that one characteristic of steam generator tube ruptures is the presence of a leading indicator, that is, a signal that is a highly salient, very certain indicator that this and only this accident category is underway -- secondary side radiation indications. Given this, one variant on the root incident is to remove, disable, make unavailable or obscure this leading indicator -- in other words, a loss of leading indicator incident. One specific scenario that accomplishes this is a loss of power just prior to the start of the break.

Identification of this incident variant can happen in several ways during the plant familiarization phase of the PRA. One can examine simulator studies or actual incidents related to the question at hand. One may discuss the incident with training instructors or observe crews handle the incident on a training simulator. One may start to carry out CES runs and discover that the problem is easy

because of the leading indicator. One may know from past CREATE HRA analyses that loss of leading indicator incidents are significant from a human cognitive error point of view.

In any case, we now have two incidents to examine from the perspective of problem difficulty. The base incident is a *textbook* steam generator tube rupture and the variant is a loss of leading indicator tube rupture, specifically, loss of power followed by a steam generator tube rupture.

5.3 HYPOTHETICAL OUTPUTS OF MODELING RUNS

The incidents used for the worked example of CREATE are basically the same as those used to exercise CES (i.e. a textbook tube rupture and a tube rupture with a loss of off site power). See Chapter 4 for more details on exercising CES on these incidents and on CES behavior in these incidents. However, the results of the CES exercises were not completed at the time that the HRA workshop was held. Consequently, the worked example was based on hypothetical outputs. The objective was to assess to what extent the types of outputs that can potentially be generated from a cognitive simulation model could provide useful input to an HRA/PRA analysis.

The hypothetical set of outputs that were used as the basis of the CREATE worked example are described below. They were generated based on an analysis of the cognitive demands of the situation, and empirical data of operator performance during simulated events (See section 4.2). The set consists of three alternative decision trajectories that imply diagnosis of the tube rupture at different points in the evolution of the event. In the textbook case diagnosis is triggered by the secondary radiation alarms. In the LOLI tube rupture the trigger for diagnosis is less clear. Two alternative decision trajectories are considered: An *active search trajectory,* where the operators are actively formulating and testing hypotheses; and a *passive monitoring trajectory,* where the operators are passively monitoring the plant, waiting for definitive evidence to emerge. In the active search trajectory, diagnosis would be expected as soon as there is any visible evidence that can potentially discriminate among the viable hypotheses. In the tube rupture event the first opportunity is when there is visible evidence of an unexplained discrepancy in levels among the steam generators (e.g., when level in the faulted steam generator enters the narrow range indicator while the others are still on the wide range indicator). In the passive search trajectory, more extreme steam generator level behavior is needed to capture operator attention (e.g., a wide discrepancy in steam generator levels that cannot be explained; level in the faulted steam generator continuing to increase even after feedwater flow has been stopped; high level steam generator alarm on the faulted steam generator). Figure 5-1 graphically indicates for each trajectory the time window within the tube rupture event when diagnosis would be expected. In each case the time window is defined with respect to the occurrence of critical cues pointing to a steam generator tube rupture.

The three trajectories and their rationale are described more fully below.

Textbook Case
In the case of the textbook steam generator tube rupture, the model is hypothesized to directly and quickly diagnose the fault category. A highly salient

cue occurs very early in the sequence of events. Because the cue is very salient the model sees the change. The signal is unexpected in this context (normal plant operation) so that CES devotes processing resources to interpreting its significance. CES has knowledge that this signal, secondary side radiation monitors (steam generator blowdown and condenser air ejector) indicating high radiation, is a highly certain indicator of the presence of a steam generator tube rupture. In other words, a steam generator tube rupture is very much the strongest candidate explanation for the unexpected finding of secondary radiation. This explanation is also consistent with all the other findings that CES has observed about plant state, e.g., decreasing pressurizer level, decreasing pressurizer pressure, etc., and findings that CES later observes, such as increasing steam generator level in one steam generator. Thus, diagnosis should occur highly reliably and very early in the sequence of events.

Note that the actual CES run reported in Chapter 4 matched this description.

Loss of Leading Indicator
Now consider what happens in the variant where the radiation indications do not occur. From a problem solving point of view the incident is a ***loss of leading indicator*** (LOLI) incident -- a highly certain indicator of a diagnostic category is missing. The early salient cues that CES sees are decreasing pressurizer level, decreasing pressurizer pressure, increasing charging flow, letdown isolation, etc. These are unexpected findings given the plant was in a normal power production state and initiate diagnostic search. Given the absence of secondary radiation signals, there is a much larger set of hypotheses that are consistent with the initial set of abnormal plant behaviors (low level, low pressure), and which should be explored during diagnosis.

The initial diagnostic search encounters evidence consistent with a primary system break but which type will not be conclusively established, although the strongest candidate is the loss of primary coolant (LOCA) category.

LOLI 1. Active Search (Hypothetical CES Output):
The question then is how does CES uncover the actual state of the plant. In one trajectory, called *active search*, CES actively searches for evidence to determine whether or not a steam generator tube rupture is present. In this case the list of possible explanations includes primary break to containment and steam generator tube rupture (both are primary system breaks). The primary break to containment is the strongest possibility; steam generator tube rupture is lower on the list. This ordering was established through interviews with instructors -- when asked, "what would account for low primary system level and pressure" operational personnel think of LOCA as a possibility first and tube rupture much later.

As a result, the primary break to containment possibility will guide diagnostic search first. However, there is no indication of containment abnormalities. This is inconsistent with this hypothesis and leads to the evaluation of other candidates. Eventually, the steam generator tube rupture will capture processing and guide diagnostic search. When this occurs CES will look for evidence that it knows would be associated with the presence of a tube rupture, e.g., secondary radiation, abnormally increasing level in one steam generator, etc. Note how this process consists of ***knowledge-driven*** diagnostic search triggered by the unexpected findings of decreasing primary system pressure and level.

When this kind of CES run will uncover the tube rupture depends on when there is visible evidence for the diagnostic search to detect (as well as its knowledge about what plant indications reveal a tube rupture). This will not occur, generally, until the level in the faulted steam generator reaches the narrow range (i.e., the ability to discriminate that one steam generator level is increasing faster than the rest is very poor up to this point because of the instrumentation and displays). This analysis suggests that diagnosis will first occur reliably in this "active search" trajectory but it definitely will take longer than in the textbook case (because of the extra steps in the diagnostic process). The correct diagnosis will occur about the time that faulted steam generator level returns to the narrow range in the sequence of events for this incident. This result is shown in Figure 5-1 for the trajectory labeled LOLI active search.

Note that while none of the actual CES runs matched this case, it would be possible to produce this kind of behavior with CES.

LOLI 2. Passive Monitoring (Hypothetical CES Output):
In this trajectory, called *passive*, CES does not actively search for evidence to determine whether or not a steam generator tube rupture is present. It can only uncover the actual state of the plant if a new salient signal that suggests a tube rupture occurs which captures its attention. This is a data-driven process where a new salient finding triggers a new line of reasoning.

In the passive monitoring case, the primary break to containment possibility will guide diagnostic search. CES continues to wait for evidence of containment abnormalities and does not actively search for evidence associated with a steam generator tube rupture hypothesis. In effect, there is a missing piece of evidence -- the absence of the leading indicator decreases strength in that hypothesis.

Is there a new signal that could occur and trigger a line of reasoning relevant to the actual fault? Yes, if a salient cue indicated that there was an unexpected abnormally high steam generator level, CES would recover and diagnose the correct fault. If CES sees a signal indicating high steam generator level, this would be interpreted as an unexpected finding for the context and it would trigger diagnostic search to explain this finding. CES knows about two possible explanations for high steam generator level: steam generator tube rupture and poor regulation of steam/feed flow. Assuming there is no history of poor regulation to complicate matters, the diagnostic process triggered by decreasing primary system pressure/level and the new diagnostic process triggered by high steam generator level can be combined into one hypothesis that accounts for all of the findings CES has noticed through the incident.

There are three basic candidates for this cue. The potential cue that occurs earliest in the sequence of events is a major discrepancy between one steam generator level and the others. The detectability of this cue depends on the instrumentation and displays, expertise of the operators (to recognize that a difference across steam generators is an important cue), the history of manual control of emergency feedwater and control steam flows.

The second cue would be the state where level was increasing in one steam generator *when there was no emergency feedwater flow* into it. This would occur because as part of the reactor trip scenario operators manually control feedwater flow to regulate steam generator levels to a target level (e.g., 50%). Thus, as

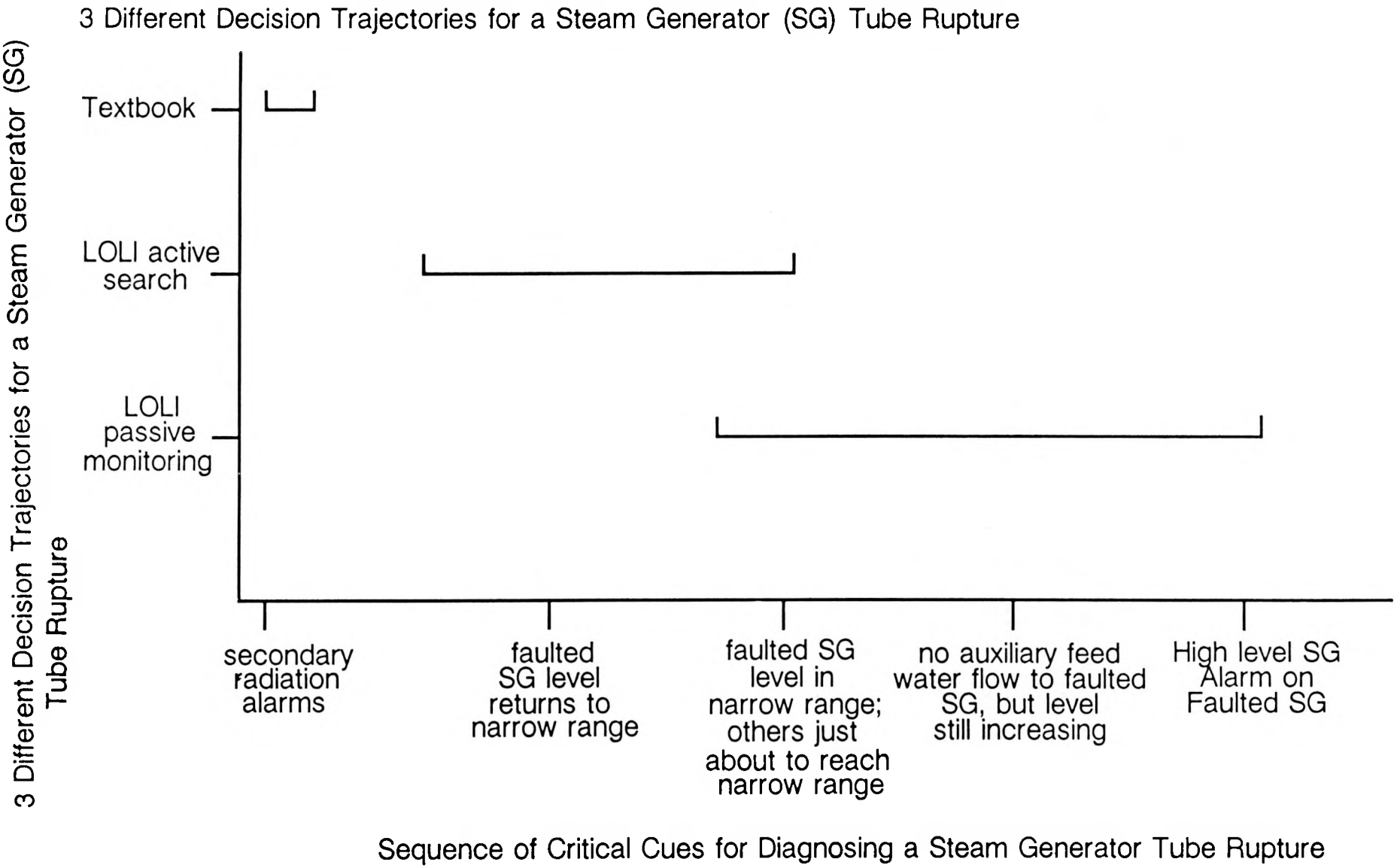

Figure 5–1. The time window during the course of a steam generator tube rupture event when correct diagnosis would be expected for each of three different decision trajectories (see text for a description of the three decision trajectories). In each case the time window is defined with respect to critical diagnostic cues that arise during the course of the event.

level increased, the operator would intermittently decrease feedwater flow until it was very low or zero (depending upon the amount of steaming underway to cool the reactor). Note that the operator controlling the balance of plant would be acting as a simple servomechanism controlling feedwater to a setpoint. This cue would generally be present about the stage of the sequence of events where faulted steam generator level reached its post-trip target value.

One of the actual CES runs presented in Chapter 3 approximates this second case.

The third cue is the high level steam generator alarm (78% for the plant simulated for the CES runs). This is also the setpoint for a procedure step in the function based portion of the Westinghouse Owners Group procedure guidelines.

Figure 5-1 notes the range through the sequence of events where the correct diagnosis would occur on this trajectory.

5.4 QUANTIFICATION

Suppose the PRA needs an answer to the question how likely is it that diagnosis in this incident will occur before some stage in the sequence of events, e.g., before faulted steam generator level reaches x. This question might be important to a risk analysis because of problems that would arise downstream in the incident depending on how long operators took to implement corrective responses. Examples for this case might include steam generator overfill leading to steam line failure or water flow leading to stuck open steam generator relief valves or the chance of radiation releases to the environment through steam generator relief valves. How does one use the results of the CES analysis to answer a question like this?

Again, there is an assumption behind CES/CREATE that human behavior (and CES behavior) varies as a function of mismatches between the cognitive demands imposed by the incident and the available problem solving resources. The procedure for estimating likelihoods (cognitive reliability estimates) from CES assumes that the major element of uncertainty in predicting operator behavior rests on assessing the probability that the situation will arise which produced an intention failure, when that situation is simulated in CES. As a first approximation, it can be assumed that any intelligent agent would exhibit the behavior produced by CES with a probability approaching one, when placed in the same situation, i.e, given the cognitive demands imposed by the incident and the available problem solving resources.

The analysis during the modeling stage revealed different trajectories for steam generator tube rupture diagnosis depending on different operator and incident factors (Figure 5-1). The question at this stage is how likely is the incident to go down one of these trajectories.

To estimate these likelihoods, two questions need to be considered (Figure 5-2).

- How likely is it that the problem solving demands in effect during that CES run will arise in the actual NPP?

- How likely is it that the particular set of problem solving resources modeled in that CES run will be in effect?

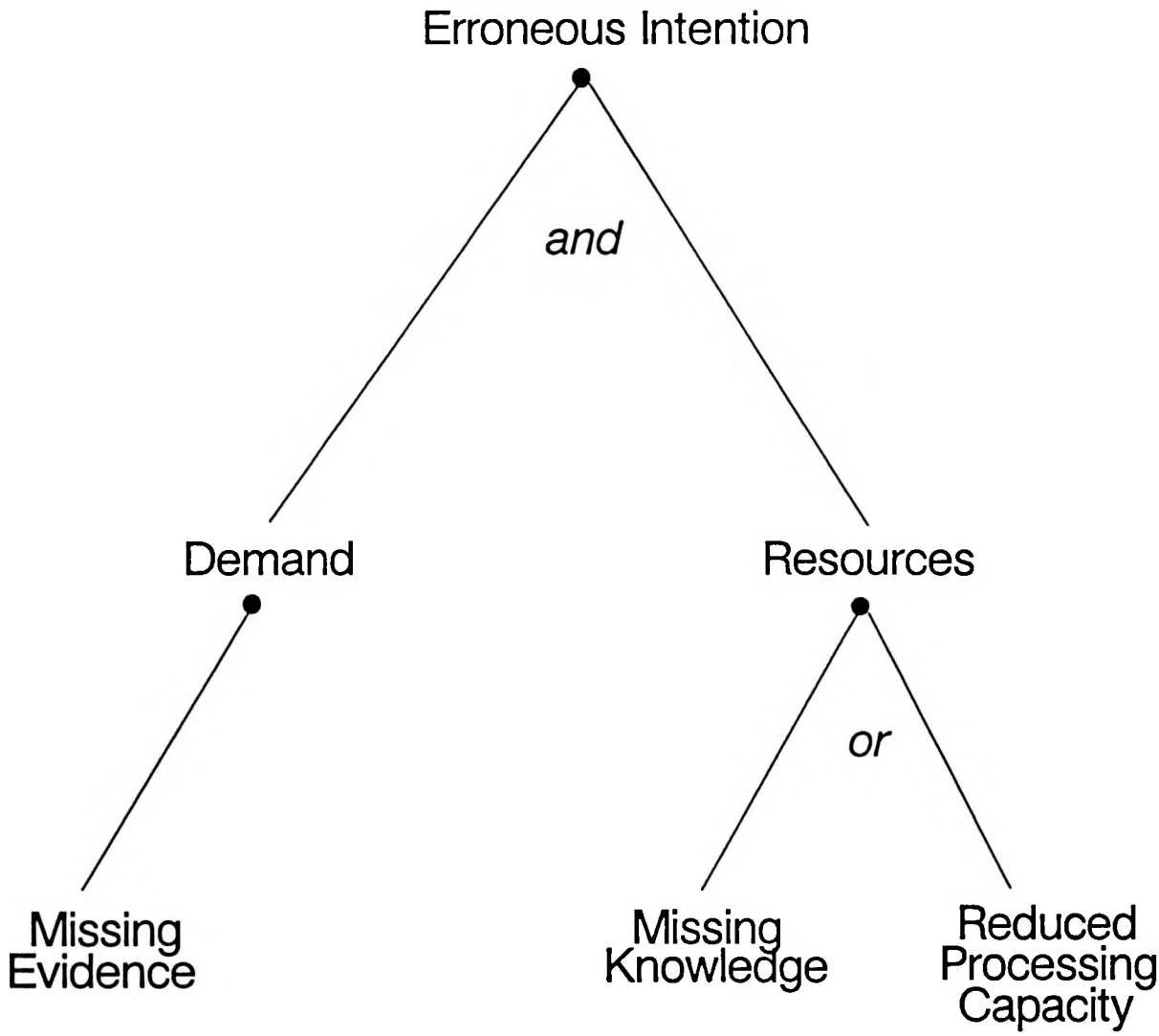

Figure 5–2. Demand–resource view of human error. The difficulty of a problem depends on both the demands posed by the problem itself and on the resources (e.g., knowledge, plans) available to solve the problem.

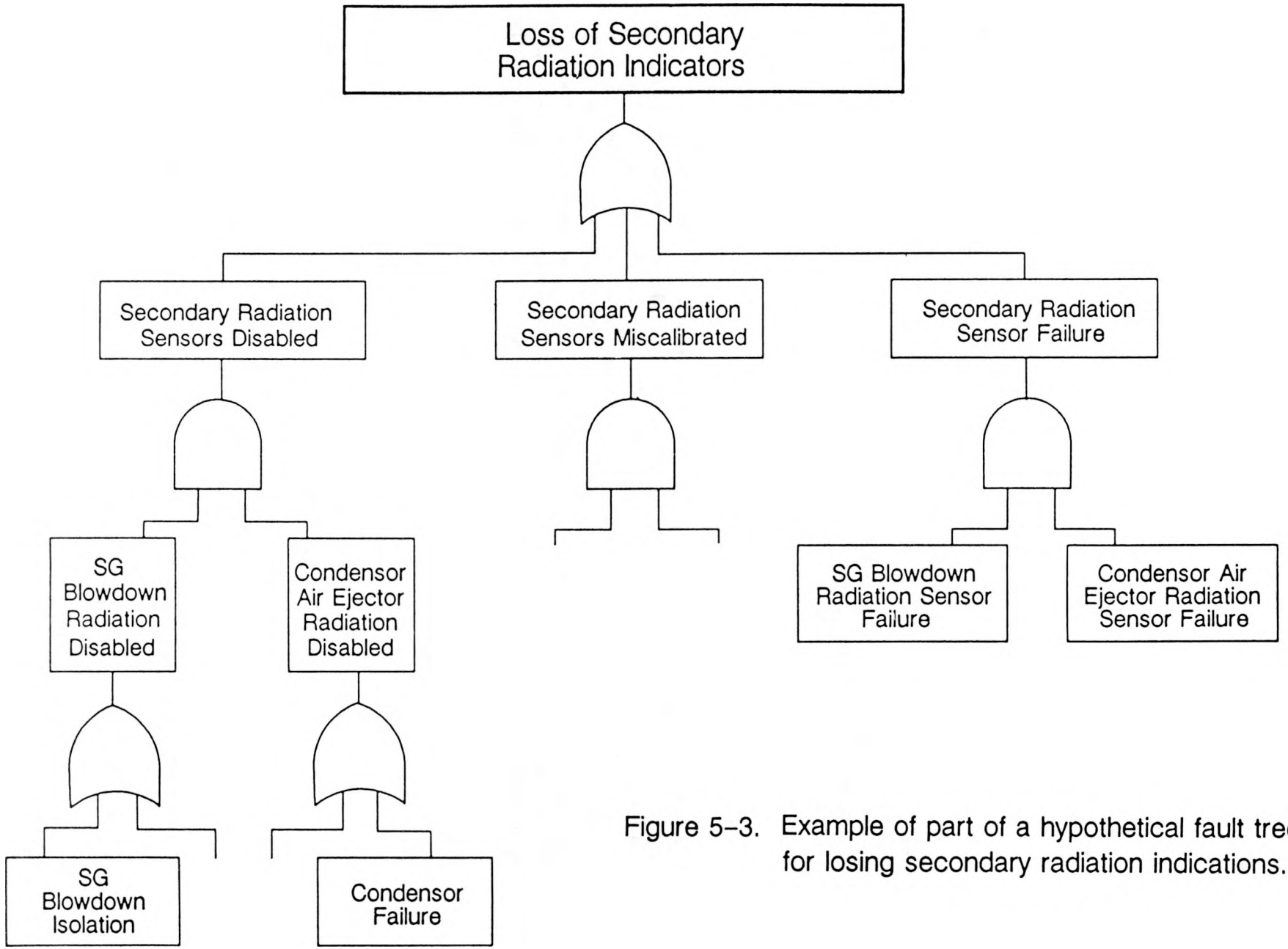

Figure 5-3. Example of part of a hypothetical fault tree for losing secondary radiation indications.

In this particular case, these questions become:

- How likely is a loss of leading indicator tube rupture?
- How likely is the crew to go down the active search or passive diagnosis paths or subpaths in the hypothetical CES analysis?

The probability of the problem solving demands (i.e., the occurence of a LOLI tube rupture) can be estimated with existing engineering and systems reliability techniques. The difficult problem solving situation becomes the top level outcome in the fault tree, and the likelihood of elements in the fault tree can be estimated from existing data bases on system reliability (e.g., Licensing Event Reports) or based on the judgment of those knowledgeable in the relevant area of plant systems and equipment.

Typically the top node in the fault tree will represent a class of physical situations that produce the same psychological result with respect to problem-solving demands. In the current example the top node in the fault tree would be loss of secondary ratiation indications. While CES may be run on only one or a few incidents that are instances of a class, it is necessary to aggregate the probabilities of all the ways this cognitively challenging situation could arise in the quantification process. Figure 5-3 contains an example of a part of a fault tree for losing secondary radiation indications. In the case we ran secondary radiation sensors were disabled due to a loss of power but other ways to lose secondary radiation indicators include sensor failures and sensor miscalibrations.

The next question is to establish how likely is a crew to go down the active search or the different passive monitoring trajectories? To answer this question requires consideration of what are commonly called performance shaping factors (Swain & Guttmann, 1983). The issue is what factors are likely to affect the proportion of crews that are likely to fall into each of the different decision trajectories and subtrajectories depicted in the analysis? The cognitive analysis described above indicates several relevant performance shaping factors: quality of information available on the display board; the characteristics of the procedures; the skill and experience of the crew; the quality of crew coordination.

Note that some of these factors are fixed properties of the plant or situation in question. This is true of both the quality of information provided on the control board and the procedures. To assess the impact of these factors the HRA analyst can examine the actual control board and procedures, or obtain input from plant operational personnel.

Examination of control board displays and relevant procedures indicates that in the case of a LOLI tube rupture these factors are likely to contribute to a delay in diagnosis. The data on steam generator level behavior typically available on the control board make it relatively difficult for an operator to detect abnormal steam generator level behavior, at least early in the incident. Examination of procedures reveals that in the case of a LOLI tube rupture there would be no procedural guidance to investigate the possibility of a tube rupture until the high steam generator level alarm occurs.

The degree of skill and experience of the operators, and the quality of crew coordination will also affect which trajectory a crew is likely to follow. Highly

skilled operating teams with good crew coordination should detect abnormal steam generator level behavior earlier. These crews are likely to either actively pursue a diagnosis (i.e., the active search trajectory) or to detect abnormal steam generator behavior at the first opportunity (i.e., the first marker on the passive monitoring trajectory). Poor crew coordination will delay detection until the second or the third markers on the passive trajectory (i.e., when level in the faulted steam generator continues to rise even though there is little or no feedwater; and when the high steam generator level alarm is reached).

A question to be answered is what proportion of crews are likely to fall into each of these classes. There are several ways these can be estimated. One approach is to estimate these proportions based on empirical data (e.g., simulator trials). This was essentially the approach taken in the CES/CREATE exercise (See section 4.2). Another is to obtain the estimates from plant operational or training personnel. A third is to elicit the probabilities using formal expert judgment techniques.

The HRA analyst may convene a panel of experts to generate the required frequency estimates to quantify the likelihood of operators following each of the trajectories. Any of several available techniques for eliciting frequency judgments from groups of experts may be used (e.g., the structured elicitation technique used in NUREG-1150; the SLIM-MAUD procedure developed by Embrey, Humphreys, Rosa, Kirwan & Rea, 1984). The difference that CES makes is that the questions asked the experts will be more specific and more within their range of experience. In addition, the answer to the question, who is the appropriate expert, will be more clearly defined.

Expert polling techniques can also be used to generate uncertainty bounds around the point estimates. A suggested procedure is the direct estimation procedure developed by Seaver and Stillwell (1983) and adopted in SLIM-MAUD. In this procedure judges are asked to make a direct estimate of the upper and lower bounds for probability estimates by indicating a value on a probability/odds rating scale.

An alternative mechanism is to use existing human performance data. This was the approach taken in the present CES/CREATE exercises. In this case, data are available on six experienced crews and three crews of instructors in the loss of leading indicator tube rupture (cf., Tables 4-2 and 4-3 for summaries). These data reveals that 1 out of 9 crews correctly diagnosed the fault through the active search mode, while the remaining 8 (including all of the instructor crews) only diagnosed the fault through the passive mode. Within the passive diagnosis category, 4 crews solved the problem based on a major discrepancy between one steam generator level and the others (i.e., faulted/intact steam generator level differences of between 16 and 30% on the narrow range scale) and 4 crews only solved the problem when feedflow was zero or near zero and they noticed that level continued to increase (in one case faulted steam generator level was 71% narrow range before the correct diagnosis was made). These empirical data could be used to estimate probabilities, or they can be adjusted based on expert judgment of their relevance to a particular case.

5.5 WHAT DID WE LEARN ABOUT HUMAN RELIABILITY FROM THE CREATE EXAMPLE?

The CES/CREATE analysis of the diagnosis phase of a LOLI tube rupture established a variety of findings about human performance.

First, the LOLI steam generator tube rupture is much more difficult to diagnose than a textbook steam generator tube rupture. This means that diagnosis of a textbook steam generator tube rupture is extremely reliable (in the absence of some complicating factor a human diagnostic error is not plausible). With respect to the LOLI steam generator tube rupture, diagnostic difficulties are much more likely. If we had a meaningful way of relating difficulty to reliability, this result alone would indicate a major change in the estimate of human performance. However, there is no macroscopic mapping of difficulty onto reliability.

Second, the CES/CREATE analysis indicates the points in the sequence of events of an LOLI steam generator tube rupture where the operating team is likely to reach the correct diagnosis. If the operating team, actively pursues the tube rupture hypothesis, diagnosis is likely to occur as soon as detectable symptoms of level abnormality in the faulted steam generator begin to appear. If the operating team is on the passive monitoring trajectory there are three major markers that provide increasingly salient evidence of a tube rupture (See Figure 5-1). Level of skill and degree of crew coordination will determine to which of these cues the crew will respond to.

The CREATE worked example reveals a high likelihood of delay in correct diagnosis of a LOLI tube rupture. In addition, the CES runs point to the possibility of diagnostic error when an additional complicating factor is present that produces indications consistent with abnormal containment conditions. Given the context of the situation, these indications would be taken as consistent with, and confirming of a LOCA event. An example of this behavior was demonstrated in the CES Case 3 run. In that case the complicating factor was a reactor coolant pump seal leak to containment, which is a concern following a loss of electric power. The CES analysis indicated that a diagnostic error (i.e., concluding that the seal leak was the only fault present) leading to an error of commission (i.e., opening the PORV block valves) is plausible under those circumstances.

There are a variety of human performance implications of the delayed diagnosis of a steam generator tube rupture. First, the delayed diagnosis is likely to lead to an error of commission relative to the steam generator tube rupture procedure (but note that the operating team does not know that the tube rupture procedure should be followed since they think that they are in a different situation). In particular, the operating crew may begin releasing steam from all of the steam generators in order to control primary system temperature or to begin a primary system cooldown (e.g., following a post-LOCA cooldown procedure). This action is erroneous given the fact that a steam generator tube rupture is underway in one steam generator. The steam generator response calls for isolation of the faulted steam generator prior to beginning a primary system cooldown. The CES case 3 run suggests the plausibility of this type of operator action.

There are other human performance consequences of a delayed diagnosis which we did not pursue in detail in the worked example, but deserve mention. The likelihood of operator erroneous actions in carrying out preplanned maneuvers in

response to a steam generator tube rupture may go up. The coordination of a primary system cooldown in order to maintain a subcooling margin followed by a primary system depressurization in order to stop safety injection inflow and equalize primary system and faulted steam generator pressures is a non-trivial operator task. Following delayed diagnosis of the steam generator tube rupture, the operating crew may feel considerable time pressure to complete these maneuvers quickly. The time pressure derives from the desire to avoid overfilling and overpressurization the faulted steam generator. One possible operating crew response in this situation is to execute the primary system cooldown and depressurization in parallel rather than in series as called for in the tube rupture procedure.

Other human performance issues are related to possible operating team responses to anticipated or actual overfilling or overpressurizing of the faulted steam generator. The delayed diagnosis produces a situation where the response to the tube rupture does not begin until level in the faulted steam generator reaches 45% to 80% narrow range. The delay means that the operating crew is very likely to face the situation of an overpressured faulted steam generator releasing contaminated steam to the environment via a power operated relief valve or a safety valve. They are also very likely to face the situation of water in the steam lines and the possibility of steam line ruptures, i.e., a steam generator tube rupture with an unisolatable steam leak. Understanding the likelihood, consequences, and risks of these situations requires PRA plant response analyses, as well as additional human performance analyses. This is one example of how human performance issues can flag the need for PRA analyses that might not have otherwise been performed (or at least change their priority for analysis within the plant portion of the PRA; cf., Dougherty, in press; Woods, in press).

With respect to the human performance issues associated with the above situations, note that there may be little procedural guidance available for the operating crew. For example, the emergency procedures do not specify how the operator should react to the possibility or actuality of a radiation release through the faulted steam generator relief valves. While this release may be relatively small, it is not without practical significance (e.g., reactions of the public; concerns of the utility). The operating crew will need to respond to the situation, faced with little guidance and conflicting concerns. There are a variety of ways the operating crew might respond depending on their knowledge, skill, and perceived goal tradeoffs. Possibilities range from ignoring the small radiation release and focusing on the steam generator tube rupture procedure; to attempting to redirect the radiation release to the balance of plant (instead of to the environment) by opening a steam path from the faulted steam generator to the balance of plant (note the economic tradeoff that might be a part of this decision); to blocking the power operated relief valve to gain some extra margin before release would occur (creating the potential for an unisolatable steam leak should the safety valves open and fail to shut).[4] These represent only a subset of possible operator responses. The main point is that the situation created by the delay in tube rupture diagnosis places high cognitive demands on the operators, and the potential for human error with safety consequences becomes greater.

In summary the CES/CREATE analysis identified several consequences for human performance in a LOLI steam generator tube rupture, possibilities for erroneous

4 This occurred as part of a steam generator tube rupture response during the Ginna incident in 1982 (Woods, 1982).

actions, and a variety of potential safety consequences. For example the fact that a radiation release to the environment through the faulted steam generator relief valves is a likely consequence of delayed diagnosis. The analysis also showed the parallel relationship between the plant and human portions of a PRA where an analysis of human reliability generates new plant response questions to be analyzed, as well as where analysis of plant responses generates questions about human performance (cf. Woods, in press).

5.6 WORKSHOP CONCLUSIONS

The workshop participants were given a demonstration run of CES in the DSSL facility. The worked example was then presented and discussed in depth.

The workshop results showed that, while there are a number of detailed interface points between CREATE and PRA that remain to be resolved, the CREATE process does provide useful qualitative and quantitative inputs to PRA that cannot be obtained in other ways.

The workshop participants commented that:

(1) CES/CREATE represents the best available tool to identify operational problems related to making a diagnosis or decisions following an offnormal incident. Its findings, with some interface development can fit directly into HRA.

(2) Existing methods of estimating human reliability treat human behavior in a simplistic manner. The CES modeling tool is one of the first methods for exploring the complexities of operator decision making.

(3) CES/CREATE needs to be expanded to handle a wider range of incidents and factors that affect decision making,

(4) An analyst interface to CES/CREATE needs to be developed so that a wider range of experts can use the system.

6. SUMMARY AND CONCLUSIONS

The results of all three evaluation exercises indicate that CES represents a viable approach to modeling NPP operator intention formation during normal and emergency operations, and can potentially provide valuable input to HRA analyses.

The expert review panel unanimously indicated that the project was pushing the state of the art in AI, cognitive modeling for complex worlds, and HRA. CES/CREATE was judged to be a major step forward towards the goal of soundly based human reliability techniques. However they also stressed that CES and CREATE need to be more fully exercised on a broad set of test incidents on which empirical data on human operator performance exists. This is critical for two reasons. First it is important to stress the modeling capabilities of CES by exercising it on events that place different modeling demands (e.g., that require representing a different portion of the plant; or different aspects of human decision making) in order to identify places where capabilities need to be expanded. Second it is important to provide evidence that CES performance parallels the performance on human operators when presented with similar events, to serve as bench marks.

The exercise of CES on the three Steam Generator Tube Rupture cases represents an important step in that development and evaluation process. The three case runs successfully demonstrated the ability of CES to follow a dynamically changing event using actual high fidelity simulator data as input. CES monitored plant parameters, formed hypotheses, and generated intentions to act in a plausible manner.

The runs demonstrated the ability of CES to provide insight into likely operator responses to accident situations under different conditions. The contrast between the Case 1 ("Text book" Tube Rupture) and Case 2 (Multi-fault event) demonstrated that CES can be used to provide an objective means of distinguishing which event scenarios are likely to be straightforward to diagnose and which scenarios are likely to be cognitively challenging, requiring longer to diagnose and potentially leading to human error. The contrast between Case 2 and Case 3, where the accident event sequence presented to CES was identical, but the knowledge encoded in CES varied, demonstrated the potential to use CES to explore the consequences of differences in operator knowledge (e.g., based on differences in training or procedures) on intention formation and the potential for human error.

The CREATE workshop demonstrated how CES outputs could be used to provide useful qualitative input to HRA on the cognitive demands placed by different accident scenarios and the potential for errors of intention. The HRA and PRA participants in the workshop indicated that CES/CREATE represents the best available tool to identify operational problems related to making a diagnosis and decisions in emergency events. At the same time they indicated the need for significant further expansion and benchmarking of CES capabilities.

6.1 ADDITIONAL WORK UNDERWAY

Based on the results obtained to this point, additional work is planned on several fronts. The CES tool will be used to analyze several incidents of interest to the

NRC in order to expand the range of NPP scenarios and operator factors that CES can address. This work will also extend the evaluation of the CES tool to new incidents. In order to make the CES tool accessible to a wider range of experts, the process of using the model to analyze the above incidents will be traced to define what would be a useful analyst interface. Finally, the computer and NPP simulator environment set up for CES use in the evaluations will be used as a model to examine how to set up a similar facility for the NRC. Possibilities being explored include connecting CES to the NRC NPP control room training simulation of the NRC Technical Training Center at Chattanooga, Tennessee, as well as to other NRC in-house plant simulations.

7. REFERENCES

1. E. M. Dougherty. Human reliability analysis - Where shouldst thou turn? *Reliability Engineering and Systems Safety,* 29 (3), 283-299, 1990.

2. J. Elkind, S. Card, J. Hochberg, and Huey B., (Eds.). *Human Performance Models for Computer Aided Engineering.* National Academy Press, Washington, DC, 1990.

3. D. E. Embrey, P. Humphreys, E. A. Ros, B. Kirwan, and K. Rea. *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment.* Technical Report NUREG/CR-3518 or BNL-NUREG-51716, Department of Nuclear Energy, Brookhaven National Laboratory, 1984.

4. N. Moray and B. Huey, (Eds.) *Human Factors Research and Nuclear Safety.* National Academy Press, Washington, D. C., 1988.

5. R. W. Pew, D. C. Miller, and C. E. Feehrer. *Evaluation of Proposed Control Room Improvements Through Analysis of Critical Operator Decisions.* Electric Power Research Institute, Palo Alto, CA, 1981. NP-1982.

6. H. E. Pople, Heuristic methods for imposing structure on ill-structured problems: the structuring of medical diagnostics. In P. Szolovits, editor, *Artificial Intelligence in Medicine,* Westview Press, Boulder, CO, 1982.

7. H. E. Pople. Evolution of an expert system: from internist to caduceus. In I. DeLotto and M. Stefanelli, editors, *Artificial Intelligence in Medicine,* Elsevier Science Publishers B.V. (North-Holland), New York, 1985.

8. J. Rasmussen. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering.* North-Holland, New York, 1986.

9. J. Reason and K. Mycielska. *Absent Minded? The Psychology of Mental Lapses and Everyday Errors.* Prentice-Hall, Englewood Cliffs, NJ, 1982.

10. D. Seaver and W. G. Stillwell. *Procedures for Using Expert Judgment to Estimate Human Error Probabilites in Nuclear Power Plant Operations.* Technical Report NUREG/CR-2743, Sandia National Laboaratories, 1983.

11. A. D. Swain and H. E. Guttmann. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* National Technical Information Service, Springfield, VA, 1983. NUREG/CR-1278.

12. E. A. Trager, Jr. *Case Study Report on Loss of Safety System Function Events.* Technical Report AEOD/C504, Office for Analysis and Evaluation of Operational Data, U. S. Nuclear Regulatory Commission, 1985.

13. D. A. Ward. *Will the LOCA mind-set be overcome?* Paper at IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA, June 1988.

14. D. D. Woods, On taking human performance seriously in risk analysis: *Comments on Dougherty. Reliability Engineering and Systems Safety,* 29 (3), 375-381, 1990.

15. D. D. Woods, Operator decision making behavior during the steam generator tube rupture at the Ginna nuclear power station. In W. Brown and R. Wyrick, editors, *Analysis of Steam Generator Tube Rupture Events at Oconee and Ginna,* Institute of Nuclear Power Operations, 82-030, 1982.

16. D. D. Woods and E. M. Roth. *Models of Cognitive Behavior in Nuclear Power Plant Personnel.* U. S. Nuclear Regulatory Commission, Washington DC, 1986. (NUREG/CR-4532).

17. D. D. Woods, E. M. Roth, and H. Pople. *Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment.* U. S. Nuclear Regulatory Commission, Washington DC, 1987. (NUREG/CR-4862).

18. D. D. Woods, J. A. Wise, and L. F. Hanes. *Evaluation of Safety Parameter Display Concepts.* Electric Power Research Institute, Palo Alto, CA, 1982. NP-2239.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-5213
Vol. 2

2. TITLE AND SUBTITLE

The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability

Main Report

3. DATE REPORT PUBLISHED

MONTH: June | YEAR: 1990

4. FIN OR GRANT NUMBER

D1167

5. AUTHOR(S)

D.D. Woods[1], H.E. Pople[2], E.M. Roth

[1]Cognitive Systems Engineering Laboratory, The Ohio State University

[2]University of Pittsburgh and Seer Systems

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

July 1987 - December 1989

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Westinghouse Science and Technology Center
1310 Beulah Road
Pittsburgh, PA 15235

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Division of Systems Research
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

The U.S. Nuclear Regulatory Commission is sponsoring a program to develop improved methods to model cognitive behavior of nuclear power plant (NPP) personnel. A tool called Cognitive Environment Simulation (CES) was developed for simulating how people form intentions to act in NPP emergencies. CES provides an analytic tool for exploring plausible human responses in emergency situations. In addition a methodology called Cognitive Reliability Assessment Technique (CREATE) was developed that describes how CES can be used to provide input to human reliability analyses (HRA) in probabilistic risk assessment (PRA) studies. This report describes the results of three activities that were performed to evaluate CES/CREATE: (1) A technical review was conducted by a panel of experts in cognitive modeling, PRA and HRA; (2) CES was exercised on steam generator tube rupture incidents for which data on operator performance exist; (3) A workshop with HRA practitioners was held to analyze a "worked example" of the CREATE methodology. The results of all three evaluations indicate that CES/CREATE is a promising approach for modeling intention formation. Volume 1 provides a summary of the results. Volume 2 provides details on the three evaluations, including the CES computer outputs for the tube rupture events.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Artificial Intelligence
Human Reliability
Probabilistic Risk Assessment
Cognitive Model
Nuclear Power Plant
Human Error
Problem Solving
Human Factors
Cognitive

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page) Unclassified

(This Report) Unclassified

15. NUMBER OF PAGES

16. PRICE