DISCLAIMER

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

A LOGIC FLOWGRAPH BASED CONCEPT FOR DECISION SUPPORT AND MANAGEMENT OF NUCLEAR PLANT OPERATION

UCRL--969.1

DE87 012629

Sergio B. Guarro

University of California

Lawrence Livermore National Laboratory

and

Department of Mechanical, Aerospace
and Nuclear Engineering, UCLA

International Post-SMIRT 9 Seminar

"Accident Sequence Modeling:
Human Actions, System Response,
Intelligent Decision Support"

Munich, FRG, Aug. 24-25, 1987

MASTER

EBB

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

1. INTRODUCTION

The use of automated decision support tools in nuclear power plant control rooms is being proposed as a means of facilitating the tasks of human operators, especially during plant transients originated by equipment malfunctions or failures. It is expected that by use of such tools the problem of analysing unforeseen plant conditions and determining the best course of action to be chosen will be made more manageable for plant operation personnel. It is also hoped that the human error rate associated with the process of making decisions under stress-conditions will be significantly reduced. A further advantage from the use of automated decision tools is expected to be in the speed by which information regarding the plant process can be gathered and analysed during rapidly evolving accident or transient sequences.

In the U.S. the evolution of automated decision support tools for plant operators has spanned from "event-oriented" diagnostic systems to "symptom-oriented" computer-based emergency operating procedures [1,2]. A problem common to both kind of systems is in the initial level of effort required for development of the associated models and software. In the following we will discuss some of the general issues that arise in the development and application of these decision-support systems. We will also propose and discuss an approach founded on the application of an event diagnosis and plant stabilization philosophy. This approach is based on the use of logic flowgraph process-oriented models [3] -- arranged in a modular architecture and developed with the aid of an expert-system model builder -- as a possible means of achieving the development of an automated and integrated plant management system. This approach should allow the developer to achieve a high process recovery and management capability with a focused and controlled expenditure of development time and resources.

2. DIAGNOSIS-BASED AND SYMPTOM-BASED PLANT RECOVERY

The development of a decision support tool for the operators of such a complex engineering system as a nuclear power plant should be based on careful consideration of the overall strategy applied to achieve high plant safety availability, and on our best understanding of what is needed by the plant operators when unanticipated plant transients do occur.

Figure 1 represents in a conceptual way the relation between normal or mildly perturbed plant condition states on one hand, and the set of plant conditions calling for the intervention of safety systems on the other. An accident sequence, if unchecked, could take the plant along the dashed line trajectory from a state of "normal operation" (inner circle), through the "safety feature" region, and into the "uncontrolled transient" region. The safety feature concentric layer synthetically symbolizes in

the figure the "defense-in-depth" concept which is embedded in the design of nuclear power plant safety systems. This concept implies that if an accident is initiated, the progressive sequence of events that could lead to loss of control can be halted and stabilized by one among a set of independent emergency systems. These thus constitute a series of consecutive barriers between safe operation of the plant and the uncontrolled accident region.

In terms of decision support tools, the "defense-in-depth" concept has fostered research for development of symptom-based monitoring systems, which would help make sure that the plant operators maintain the plant in a controlled, though not necessarily normal, operational state [4,5]. To achieve this, computer database and software prototypes have been or are being developed that would indicate at any time which safety systems are functional and which ones should be used, according to the standard plant emergency operating procedures. Making such information available is important and necessary. However, it should not be considered as a complete alternative to giving the plant operator(s) an early and timely opportunity to revert the plant to normal operating conditions.

The latter goal is achievable through the development and use of plant diagnostic tools and offers to the operators the advantage of not having to rely entirely on a faultless intervention and operation of the stand-by safety systems. This concept is illustrated in Figure 1 by the window identifying the area of activation of a recovery strategy based on early diagnosis and fault compensation or suppression. This strategy leads to a normal plant state via a recovery trajectory (end point within the normal operation region). Figure 1 also shows that a "stabilization strategy" based on a symptom-based application of safety features and emergency procedures produces a controlled plant state outside the normal operation region. Such a stable state is normally one of plant hot shutdown.

The need to balance recovery and stabilization strategies does not just constitute an academic subject of discussion: one unlearned, or overlooked, lesson from the TMI event is that in the initial stages of that accident a window of opportunity to keep the plant from entering the more uncertain and dangerous area of safety system operation was missed. This occurred when the operators were not able for about 8 minutes to diagnose the origin of the steam generator dryout problem in a block-valve located on the only available auxiliary feedwater line which had been left locked in the closed position. It is today possible, by use of process-oriented rather than event-oriented models, to develop automated diagnostic systems with capabilities substantially more extended than those that would be sufficient to cope successfully with such a relatively straightforward initial fault condition. Full development of systems with extended diagnostic capabilities is pursuable, provided well

coordinated and adequately supported research resources are committed.

3. PLANT PROCESS AND ACCIDENT SEQUENCE MANAGEMENT

Successful management of a plant process depends on the ability to carry out correctly and on a timely basis a number of functions involving intelligent interpretation of independently collected pieces of instrument information, as well as decision making based on the ascertained content and implications of this information. During accident sequence conditions, the same basic functions must be performed by the plant operators and by the plant operation supervisors under much tighter time constraints and more severe conditions of stress. One of the most common objections to the use of automated diagnostic and decision aid tools is that they would not provide any capability of correctly interpreting a possible operational transient situation better than that already possessed by a trained and experienced operating crew. This may or may not be true, but it should not be overlooked or underestimated that a well designed diagnostic system can integrate and make more reliable the plant operators' abilities by providing a solid support base of stored collective knowledge and information. This base of knowledge and information is difficult to maintain at a uniform level of high reliability within the small crew of individuals who are responsible for running a plant at any given time, especially under the unexpected and stressful circumstances that can develop in the course of an accident.

During the development and progression of an operational transient or (in the worst case) of an accident, the most important process management functions that can be performed by the plant operating crew can be listed as follows:

1. Transient Symptoms Detection: realization and identification of plant parameter conditions that represent a deviation from the normal operational plant state(s).
2. Plant Status Identification: interpretation of combined symptoms and available elements of information to achieve a correct understanding of the plant current status and of the nature of an existing problem (e.g.: loss of primary coolant, insufficient rate of primary coolant system heat removal, etc.)
3. Originating Fault Identification: interpretation of combined symptoms and available elements of information to arrive at a diagnosis of the existing plant conditions in terms of identification of the originating causes and of their propagation paths through the plant process and systems (e.g.: diagnosis of primary coolant loss as due to primary coolant pump seal leak).

4. Plant Stabilization: utilization of the plant status assessment made in Step 2, as the initial element for the identification of viable emergency actions to stabilize the plant in a safe new state, usually requiring plant shut-down and the operation of one or more safety systems for some length of time.
5. Plant Operability Recovery: utilization of the diagnostic deductions made in Step 3 to identify recovery actions to be performed in order to suppress the initiating causes of an operational transient and to return the plant to full operability in the shortest possible time. In some cases this may be achieved safely and quickly enough to avoid the need for Step 4. In other cases it will not. Even in the latter case there will be a benefit from allowing a quicker "post-mortem" (i.e. post shut-down) plant operability recovery.

Research on the role of the operators and of possible operator automated decision aids has focused primarily on functions 2 and 4 of the above list [4-6]. A recent review paper on this subject [2] states: "...Since the TMI-2 accident, considerable work has been devoted to developing event-independent emergency operating procedures. These symptom-and function-based procedures stress transient management rather than malfunction detection ... A major casualty is DASS (Disturbance Analysis and Surveillance System), which is largely event-based and concerned with malfunction detection..." On the subject of automated operating procedures as a decision aid to the operators the same source adds: "... The process of encoding event-independent procedures is fairly simple because of their rule based structures. The following is an example:

RC/P-4 (Reactor Cooling Procedure-4): If [Reactor Pressure Vessel] cooldown is required, but cannot be accomplished, and all control rods are inserted beyond the [maximum subcritical banked withdrawal position], then alternate shutdown cooling is required; enter... Contingency 5."

This approach to the management of plant transients appears to be based on the assumption that, in the presence of plant system malfunctions, some alternate success path to stabilize the plant can always be identified by following recipe-like procedures, and that the operator does not have to worry about recovering the functionality of the system(s) that is (are) originally malfunctioning. The underlying belief is that a transient can be understood and managed satisfactorily by plant operators who have identified malfunctions symptoms but do not know or understand the malfunction causes. We note that a close look at the early stages of the TMI-2 accident offers evidence directly contradicting this belief. During the crucial first 30 or 40 minutes of the accident, the behavior of the operating crew was

undeniably affected by their inability to recognize the "closed" position of a block valve on the auxiliary feedwater line as the cause of a steam generator dryout, and, immediately after, to recognize that a stuck-open pressurizer PORV (Power/Operated Relief Valve) was responsible for the primary system depressurization and loss of coolant.

Much can be argued about the issues that have been presented above. One can easily agree that plant models for decision support should eventually be developed as event-independent models, since too many variations of possible event sequences may actually exist and possibly develop. One may want to consider, however, whether symptom-based procedures are flexible enough to constitute the final solution to this problem. A different and in our opinion more balanced approach is one which will attempt to diagnose the reasons underlying an undesired plant state, and which will make exclusive recourse to quick, procedure-driven identification of alternate success paths for plant stabilization only if a ready diagnosis and recovery cannot be identified within a safe -- i.e., short enough -- period of time. Even when this latter is the only initially available course of action because there is not enough time and/or it is too risky to follow a different strategy, the capability for fast, computer aided diagnosis and recovery can be utilized for plant post-trip analysis and for a readier resuming of normal operation. We stress again the concept expressed in Fig. 1: in terms of "defense-in-depth", diagnosis and recovery can represent the first defense barrier against accident progression. Giving up this defense means automatically allowing an operational transient to move one step closer to potential accident sequence conditions. This implies a considerable amount of faith in the absolute readiness and availability of the second line of defense, represented in almost all cases by the stand-by plant safety and emergency systems.

4. AN INTEGRATED CONCEPT FOR PROCESS AND PLANT MANAGEMENT

If one agrees that event-based models and analysis may be impractical and that procedure-based models represent a useful interim compromise but not the ultimate ideal answer, the next question should be what ways of approaching the problem are available as possible alternatives for the future. We discuss here the indications we have gathered from our experience in the development of one of these possible alternatives. The approach that we are going to discuss is based on the integration of all five functional objectives for process management that were discussed in the previous section e.g.:

1. Transient Symptom Detection
2. Plant Status Identification

3. Originating Fault Identification

4. Plant Stabilization

5. Plant Operability Recovery

Of these five functional objectives, 1, 2 and 4 can be accomplished by rather well established means. More specifically, Objective 2 can be based on the assessment of the availability of a set of important "plant critical functions" as discussed in [6] and [7]. Objective 4 will then be achieved by pre-cataloguing logic combinations of alternative success paths and plant systems necessary to accomplish these functions. This can take the form of computer aided procedural instructions as was discussed in the previous section. A perhaps simpler way of achieving the same objective could consist of the use of an "expert system" to display to the plant operators decision tables and success trees showing the needed and available combinations of stand-by equipment that can be put in operation to accomplish a given critical plant function [4,7]. Knowledge regarding the availability of alternate success paths to accomplish a critical function obviously represents very valuable information for the plant operators when such a function is threatened or jeopardized as a result of an occurring transient.

Whenever a system is found to be inoperable, be it part of the "normal" success path for a given critical function, or part of one of the alternate success paths, Objectives 3 and 5 would become actively pursued by the automated plant management and operator aid system. References [7] and [8] discuss some of the more important aspects of a possible architectural arrangement for a plant management system called CAPAM (for "computer aided plant analysis and management") that would hierarchically combine the five functional objectives that were just enumerated. The proposed CAPAM hierarchical arrangement includes three levels of functionality progressively available to the plant operators, with increasing degrees of information content displayable at each level. Figure 2 illustrates the basic functionalities made available by the CAPAM at each level of analysis and display.

The top level -- Level One -- contains a color-coded warning and alarm functionality which essentially corresponds to Functional Objectives 1 and 2 of the list given at the beginning of this section. The color coding is determined by a "threat severity rank" corresponding to varying degrees of jeopardy for each displayed plant critical function. This rank is assigned on the basis of the number of success paths, among all of those that are applicable for the accomplishment of a given critical function, which have become unavailable as a result of a developing transient. Instrumentation-provided signals and symptoms must be appropriately interpreted to arrive at this determination. The CAPAM concept discussed here is based on the representation and analysis of anti-core-melt critical functions for a commercial

PWR plant, which are identified and classified as:

- 1) Reactivity Control (RC)
- 2) Core Heat Removal (CHR)
- 3) Primary Energy and Mass Inventory Control (PEMIC)
- 4) Reactor Coolant System Heat Removal (RCSHR)

The CAPAM "Level Two" provides plant management information related to Functional Objectives 2 and 4. Plant status information is here provided at a greater level of resolution than in Level One. In particular, while in Level One the plant operator is only informed about the total or partial compromise of a given plant critical function, Level Two describes the availability or unavailability of the specific success paths and plant systems which are dedicated by design or are in any case applicable for the fulfillment of that function.

Tables I and II illustrate the concepts employed in the implementation of the CAPAM Level One and Level Two, respectively. The plant state (i.e., mode of operation), as exemplified in Table II, serves as a switch for the activation of the portion of the truth table model which is used to identify the applicable specific critical function success paths and determine their availability or unavailability. A specific PEMIC (Primary Energy and Mass Inventory Control) critical function example is also presented in Tables I and II. This example is a simplified version, in terms of the detail given in the description of success paths and associated plant systems, of a real life application model, but is quite sufficient to illustrate the concept. If the plant is at power (Plant State A) Table II shows that the PEMIC function can be accomplished by either of the two success paths A1, A2. Path A1 requires the plant systems: Pressurizer Heaters, Pressurizer Sprays, and Level Control System. Path A2 requires the plant systems: PORVs and Level Control System. If the plant cannot be maintained at power because both success path A1 and A2 are unavailable, the plant can be made to enter Plant State B (Shutdown with pressure/level excursion), enabling Success Paths B1 and B2. These require, respectively, plant systems: PORVs and Safety Injection (success path B1); or: Safety Valves and Safety Injection (success path B2).

For all of the mentioned success paths, the key telltale parameters "pressurizer pressure" (PP), and "pressurizer level" (PL) are used as redundant ways of determining the availability of a given success path. For example, if we assume that the plant is in State B (Shutdown with pressure or level excursion), it is known that the PORVs and Safety Injection systems can maintain PP and PL within specified design limits. If these

limits are exceeded by either parameter, the CAPAM Level Two will infer that Success Path B1 is not succeeding, even though there is no more specific indication of failure of the PORV and Safety Injection systems. Under these circumstances the operator will have to decide, based on the availability or not of diagnostic information on the nature of the problem, whether to try to recover the availability of path B1 or switch his/her attention to monitoring the activation of path B2.

The CAPAM Level Three contains the system detailed knowledge base and, on request, can provide detailed diagnostic and recovery information on system or component status. It is endowed with operational capabilities corresponding to Functional Objectives 3 and 5 of the list presented previously in this section. It should be noted that different degrees of operator support capability may result from the different choices that are possible with regard to the system models adopted to represent the Level Three knowledge bases. The CAPAM concept proposed here uses a "network-based" plant model, which we believe has the capability of a considerably more powerful and efficient representation than that obtainable from the more conventional fault-tree/alarm-tree techniques usually employed in discrete state modeling. In CAPAM, plant systems are modeled in Level-Three by means of Logic Flowgraph Methodology (LFM) networks [3,9]. The features and capabilities of LFM are briefly discussed in one of the following sections. In essence, this modeling technique allows the system analyst to develop a synthetic graph representation of the cause-effect relations existing between plant physical parameters, control variables, protective devices and failure mechanisms. This "flowgraph" representation is then stored in computer memory and can be automatically analyzed on line, in combination with input signals from the plant instrumentation, to produce "diagnostic trees" and "recovery trees". When a disturbance is in progress, these small boolean trees can in most cases identify disturbance root causes, and, in addition, provide prescriptions on how to achieve system recovery without the use of alternative success paths (i.e., systems) for the affected plant critical function [7].

5. NEXT AVAILABLE PATH ACTIVATION - LAST LOST PATH RECOVERY

It is logical to assume that the amount of effort dedicated by the operators to diagnosis and recovery of needed but unavailable systems would increase as a function of the number of Success Paths already lost for any given critical function. Thus, if we refer again to Table II and assume that the plant is in State A at the beginning of a transient, with an indication that Success Path A1 has become unavailable, we may conclude that the identification and suppression of the causes of this unavailability may be useful but not vital or urgent. However, in a situation in which Success Path A2 and B1 have also failed and B2 is the only one remaining, the prudent course of action

would clearly be to dedicate as much attention as possible to the diagnosis and recovery of B1 as to the maintaining the availability of B2. A1 and A2 would be considered low priority for recovery in a progressed transient, since the plant would be well into State B and no longer capable of being stabilized within State A.

These concepts can be summarized in a "NAPA - LLPR (Next Available Path Activation - Last Lost Path Recovery) Criterion" for plant management. This proposed criterion simply states that the attention of a "plant management system" (which means the computer based algorithms and the operating crew making use of them) should at any time during an operational transient be apportioned between: a) making sure that the currently needed success path is operable, and b) attempting to diagnose and recover the last success path to have been found unavailable upon demand, or to have become unavailable during operation. The relative importance of these two objectives shifts from the former to the latter as a function of the number of already lost success paths within any of the major plant critical functions. We can conceptually define and "measure" this relative importance with a "path-recovery vs. path-monitoring index" (PRPMI), and arbitrarily assign to it a value between 0 and 1: a value of 0 signifies that total attention is dedicated by the operating crew to success path monitoring, whereas a value of 1 means that total attention is dedicated to success path recovery. If we plot the PRPMI as a function of the fraction of total success paths that have been lost, we can visualize this concept in the stepwise plot shown in Figure 3. The plot indicates that the interest of the plant operators should logically shift from a balance of priorities assigned to monitoring versus recovery at the onset of a transient, to a necessary total commitment to recovery of the "last lost" path when no further paths and lines of defense are left available.

The fraction of success paths lost within a plant critical function, as we mentioned before, is assessed and displayed within CAPAM in Level One. The associated information is provided to the plant operating crew by means of a color coded display for each critical function icon. Table I gives an example of such a scheme for a generic case, and for the PEMIC function already discussed in this section.

6. LOGIC FLOWGRAPH BASED DIAGNOSIS IN CAPAM LEVEL THREE

The proposed means to achieve CAPAM Functional Objectives 3 and 5 is the development and use of LFM models for the plant systems of interest. The Logic Flowgraph Methodology (LFM) was specifically developed as a means of constructing computer implementable models of complex plant processes, such as those taking place in nuclear power or chemical plants [3]. The LFM models take the form of directed graphs, with relations of causality and

conditional switching actions represented respectively by "causality edges" and "conditional edges" that connect network nodes and special operators. Of these, the first represent important process variables and parameters, and the latter represent the different types of possible causal or sequential interactions among them.

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

The reader interested in the details of the grammar and syntax of the LFM simulation framework will find detailed explanations and discussions in [3] and [9]. For the purpose of illustrating some of the fundamental concepts utilized in LFM we can refer to the simple LFM graph depicted in Figure 4. The graph shows that between variable #1 (V1) and variable #2 (V2) there normally exists a causal relation of direct proportionality in terms of possible deviations from rated steady-state values. This is indicated by the "default" (i.e., shown as unconditioned) +1 gain value in the directed "multiple gain box" (MGB) between V1 and V2. However, when a condition of moderate positive variation from steady-state occurs for variable #3, that is, $V3 = +1$, the causal link between V1 and V2 is no longer valid, as shown by the 0 gain value that is pointed at in the same MGB by the "true" outcome of the condition test "is $V3 = +1$?". This test is in turn represented by the diamond box ("test box" or TB in the LFM denomination conventions) along the conditional edge from V3 to the gain box.

As explained above, the computer executable interpretation of the LFM models makes them well suited for the analysis of complex processes and the diagnosis of unexpected situations that may occur in such processes. The LFM inferential analysis code automatically develops from the LFM graph models complete logic tree analyses of important events occurring in the modeled process. The only input needed by the LFM "inference engine" is the specification of a "top event", i.e. the event for which an analysis or explanation is required. If any other conditions and events existing in the process are observable (i.e. can be detected), they can also be input. The code will use these to limit the space of search for the "root cause" events and conditions that can be logically deduced as the ones determining the top event. To work with a simple example of these concepts we can refer again to Fig. 1. If we ask the LFM code to determine for what conditions we can have the top event " $V2 = 0$ "

(meaning that the variable is at its unperturbed steady-state) and we do not provide any further information, the code will give us back the following answer:

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

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

"V1 = 0"

The LFM models and software perform functions very similar to those typically attributed to diagnostic "expert systems" developed in the AI (artificial intelligence) domain, but are intended for the representation of the actual physical relations of cause and effect existing in a given process, rather than of intuitively understood and incomplete symptom correlations. If we adopt for a moment the language of the artificial intelligence community, we can thus say that LFM is meant to express and develop "deep knowledge" models of a given physical process, rather than "heuristic" and intuitively based ones.

To provide an example of application of LFM in the development and use of CAPAM Level Three models, we show in Figure 5 the logic flowgraph representation of the level control system of a generic Westinghouse PWR nuclear power plant. We recall that the pressurizer level is one of the two parameters that were in Section 4 and in Table II identified as key "telltale parameters" with regard to assessing the status of the PEMIC (Primary Energy and Mass Inventory Control) critical function. In such a plant the level control function can be achieved by either controlling the output of a positive displacement pump, or by regulating a valve on a parallel line fed by a centrifugal pump. The operator's option of choosing between these two control options is represented in the flowgraph model by the binary variable LCO (Level Control Option): the binary value 1 for this variable indicates that the positive displacement pump speed regulation option has been selected, whereas the value 0 means that the valve regulation option is presently being used. Figure 5 intentionally omits showing, for the sake of clarity, a number of process variables that would normally be included in an actual diagnostic model: the ones shown are those that give the essential physical representation of the system and are sufficient to explain the example of diagnostic and recovery analysis that is shown in Figure 6 (a and b).

The diagnostic analysis shown in the logic tree in Figure 6a shows how the LFM driven CAPAM Level Three would assess a situation in which the level control capability (while in control valve regulating option) is going to be lost because of a

lock-out (in the closed position) of a block valve located in series to the regulating valve itself. The diagnosis can be summarized as a boolean "anded" association of the following four events:

- 1) External disturbance inducing: level decrease
- 2) Measured pressurizer level: low
- 3) Selected control option: valve regulation
- 4) Block valve position: closed

With this information the operator could proceed according to his/her own assessment on the next needed action, or request the CAPAM system to perform a recovery analysis. In order to do this he will have to change the "top event" of the completed diagnostic analysis (i.e.: "level = low") into a target success state (e.g.: "level = normal") and keep the external initiating cause (i.e.: "external disturbance inducing level decrease") as a boundary condition for the analysis. The result is shown in Figure 6b. The recovery analysis identifies in this case two possible alternative actions for successful reversal of the disturbance event, that is:

- 1) Keep the control option in the valve regulation mode and open the closed block valve;

or:

- 2) Change the control option to the pump speed regulation mode.

7. TOOLS AND TECHNOLOGY FOR PLANT MANAGEMENT SYSTEM DEVELOPMENT

Logic flowgraphs are an example of diagnostic models that are suitable for use in an on-line plant management software system like CAPAM. The eventual practical implementation of such a system will strongly depend on how easily these or other models with similar features can be derived by plant analysts.

On the wings of the recent popularity of "artificial intelligence" (AI) and "expert systems" applications, a trend has been to seek alternatives to the complexity of the analysis needed for development of plant diagnostic and management models in the use of rule-based "heuristic" approaches borrowed from that domain. While this may be justifiable as a first approach to the problem, it is not a satisfactory overall strategy for two principal reasons. The first is that, as a result of decades of analysis and experience with nuclear power plant operation and safety analysis, we should be able to understand and interpret plant operational transients on the basis of formally, rather than heuristically structured, knowledge. The second is that the

models employed in expert systems do not offer, from the discrete modeling point of view, an advantage over even the older and proven logic modeling techniques employed in nuclear plant reliability and safety analysis (such as event-tree/fault tree techniques). In fact the currently available expert system modeling structures -- i.e., "frames" and "IF-THEN rules" -- are not generally well suited for the construction of deep-knowledge plant models of the type that we have discussed here. From a purely mathematical point of view, the "IF-THEN rules" that are so pervasively applied in expert systems are boolean expressions which could be derived and represented in totally equivalent event-tree or fault-tree format.

Expert system and AI technology can and should be used in power plant diagnostic model development for the part for which it is most suitable and advantageous. This appears to be in providing the plant analyst with a more productive and effective modeling environment within which he, or she, can develop his/her models. In essence, AI and expert-system technology does not offer today to the nuclear plant systems analyst better types of models but, rather, better and easier ways of producing the types of logic models that can be identified or defined as the best suited for the modeling task. A verification of the idea of combining the use of expert-system and logic modeling techniques specifically developed for nuclear plant modeling and analysis, is being explored within our research in the concept of a logic-flowgraph model builder [10]. The functionality of such a model builder is achieved via a query-driven translation process. This transposes the process knowledge contained in piping and instrumentation diagrams (P&IDs), technical specification and functional description documents, and the mind of the user/analyst, into the syntactical form required for assembling an LFM representation of that knowledge. The successive steps of the query-based user/model builder interaction are listed below for an illustration of the concept:

- 1- List principal components in the P&ID of the system to be modeled (e.g., pump, control valve, flow meter).
- 2- List "connectors" between components (e.g., pipes, wires, pneumatic lines).
- 3- Identify essential parameters characterizing functionality of components identified in Step 1 (e.g., pump speed, control valve position, measured flowrate).
- 4- Recognize and identify the direct cause-effect relations between parameters within each component (e.g., "pump flowrate driven by, and proportional to, pump speed").
- 5- Recognize and identify cause-effect relations between parameters linked by connectors across component boundaries (e.g., "valve flowrate equal to pump flowrate").

- 6- Identify feedback and feedforward causality loops and perform essential logic consistency checks (e.g., verify that no intrinsically unstable positive-gain feedback loops have been erroneously introduced).
- 7- Identify "multiple interaction process nodes", that is, parameters directly influenced by more than one other parameter.
- 8- Identify and show the effect of process faults on the normal process causality relations and classify faults into the fundamental classes of: a) component internal faults, and b) faults in component connectors. The classification process will account for the specific type and nature of the component or connector being examined, and a suitable database of "typical faults" will be used to query and guide the user of the model builder to the identification and specification of the fault types that are applicable to the individual elements of the plant system being modeled.

When completed, the LFM model builder should demonstrate how an AI "object oriented" development and modeling approach can be combined with traditional systems analysis techniques to produce nuclear plant logic-flowgraph models, which in turn can provide diagnosis and recovery capabilities in a computer assisted plant management system.

CONCLUSIONS

The development of a process plant management system endowed with monitoring, diagnosis, and recovery oriented functionality is today made possible by progress in logic and discrete modeling techniques, as well as by advances in the computer hardware and software technology field that is today known as the "artificial intelligence" and "expert system" technology field.

The application of a full diagnostic and recovery oriented process plant management system is fully attuned with the philosophy of "defense in depth", which is well understood and accepted within the nuclear power plant safety technical community. It can also be concluded that concrete gains in both plant safety and availability can be achieved by use of an operator-aid system that is designed to minimize challenges to backup safety and emergency systems. The engineering challenge of developing such a system can be successfully faced with the help of appropriate tools for construction of the discrete system models on which the system will have to be founded.

Examples of means of achieving a desirable level of functionality for a computer based plant management system were presented and discussed. Also discussed was the concept of a "model builder"

expert system which is being developed in order to automate and simplify the construction of the models that the plant management system would have to utilize. Other types of models and model-building aids are likely to be conceptualized and proposed for application in the next few years.

Discussion of rationales for intended functionality and scope of possible operator decision support aids should be fostered and encouraged. The impact of the choices that are made in this technical area is potentially far reaching. Thus, such a discussion should not remain confined to a narrow and specialistic domain. The material presented here provides the reader with a view of the current state of the art in the field, and of what it may allow us to target for practical application in the near future. It also offers a broad discussion of the general issues facing the designer of nuclear power plant decision support tools, in order to provide perspective on other concepts that have been or will be proposed.

REFERENCES

1. A.B. Long: "Technical Assessment of Disturbance Analysis Systems", Nuclear Safety, Vol. 21, No. 1, 1980.
2. D.G. Cain: "Review of Trends in Computerized Systems for Operator Support", Nuclear Safety, Vol. 27, No. 4, 1986.
3. S. Guarro, D. Okrent: "The Logic Flowgraph: a New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", Nuclear Technology, Vol. 67, Dec. 1984.
4. W.R. Nelson: "Response Trees for Nuclear Reactor Operations", NUREG/CR-3631 (EGG-2293), February 1984.
5. BWR Owners' Group: "Emergency Procedures Guidelines BWR 1 through 6," Rev.3, General Electric Company, San Jose, CA, March 1983.
6. W.R. Corcoran et al.: "The Critical Safety Functions and Plant Operation", Nuclear Technology, Vol. 55, December 1981.
7. S. Guarro, D. Okrent: "Use of Logic Flowgraph Models in a Computer Aided Process Analysis and Management System", Proc. of the 1985 International Topical Meeting on Computer Applications for Nuclear Power Plant Operation and Control, Tri-Cities (Pasco), WA, Sep. 8-12, 1985.
8. S. Guarro, J. Szabo, D. Okrent: "Multi-Level Approach for Structural Definition of a Plant Wide DAS", UCLA-ENG-8424, September 1984.

9. S. Guarro, D. Okrent: "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", UCLA-ENG 8507, Dec. 1985.
10. S. Guarro: "PROLGRAF-B: A Knowledge-based System for the Automated Construction of Nuclear Plant Diagnostic Models," ANS Topical Meeting on AI and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, UT, Aug. 31-Sep. 2, 1987.

Figure 1: Plant Recovery and Stabilization Strategies

Figure 2: Functions and Structure of the CAPAM System

Figure 3: Relative Importance of Success Path Recovery vs. Monitoring

Figure 4: Example of LFM Modeling Rules

Figure 5: LFM Model of PWR Pressurizer Level Control System

a) diagnostic inference

b) recovery inference

Figure 6: LFM-deduced Diagnosis and Recovery of Pressurizer Level Control System Disturbance

Table 1: CRPAM Level One Assessment of Plant Critical Functions

Number of unavailable success paths (out of N possible)		Threat severity rank	Critical function icon display color
Generic Case	PEMIC Example		
N	4 (of 4)	Function Lost	Red
N - 1	3 (of 4)	High	Purple
2 to N - 2	2 (of 4)	Medium	Yellow
1	1 (of 4)	Low	Grey
0	0 (of 4)	No Threat	Green

Table II: Example of Level Two Success Path Model Structure

Critical Function	Plant State	Success Path	Systems Needed		Telltale Parameters *	
PEMIC	A (at power)	A1	Heaters	Sprays	Lev.contr. sys.	PP PL
		A2	PORVs		Lev.contr. sys.	PP PL
	B (hot shutdown)	B1	PORVs		Sfty.injcn.	PP PL
		B2	Sfty.valves	Sfty.injcn.		PP PL
* PP = Pressurizer Pressure PL = Pressurizer Level						