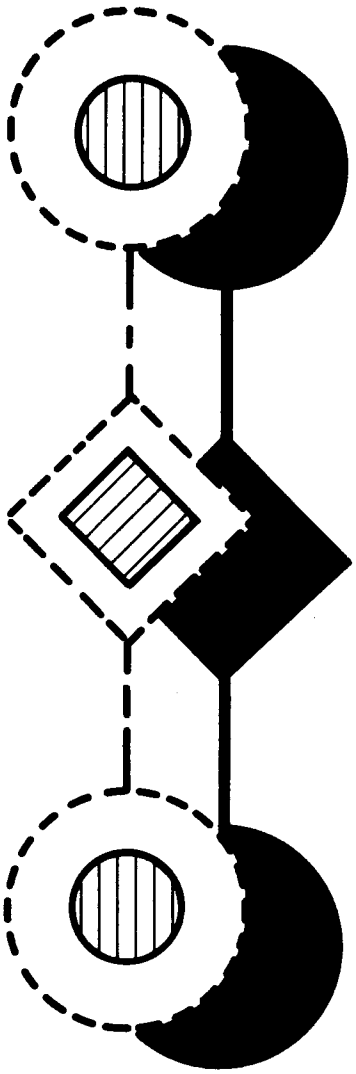
A FUNCTIONAL DESIGN APPROACH TO PWR SAFETY



M.K. De
J.A. Rumancik
A.J. Impink
J.R. Easter

Westinghouse Electric Corporation

A FUNCTIONAL DESIGN APPROACH TO PWR SAFETY

M.K. De
J.A. Rumancik
A.J. Impink
J.R. Easter

Nuclear Technology Division
Westinghouse Electric Corporation
Pittsburgh, Pennsylvania

Presented at the
International Meeting on
Thermal Nuclear Reactor Safety
Chicago, Illinois, USA
August 29 - September 2, 1982

ABSTRACT

The present work in the U.S. nuclear industry directed towards improving response during emergency conditions consists of improvement in emergency procedures, post-accident instrumentation, alarm presentation, and the development of operator aids. This paper contains work in progress for the formulation of a possible basis for such an effort. The basis consists of using a functional relationship chart for PWR safety as a conceptual model for the plant. The functional relationship chart identifies elements important to safety starting from the abstract concepts of fission product barrier maintenance and proceeding to equipment details. The interactions have been structured by using a multilevel flow model of the plant which formulates the purpose, function and supporting systems in terms of mass and energy transport and storage processes, and their functional interrelationship by critical, controllable variables. The methodology for developing a set of critical safety function restoration procedures is also presented to demonstrate application of these concepts.

INTRODUCTION

As a consequence of the accident at TMI, there is presently a considerable effort in the U.S. nuclear industry directed towards improving response during emergency conditions in nuclear power plants. This work consists of improvement in alarm presentation, emergency procedures, post-accident instrumentation, and the development of operator aids. Westinghouse has recognized the importance of establishing the fundamental basis for all such efforts and for coordinating development from such a basis. This paper describes work in progress for the formulation of this basis and the application of these concepts to emergency procedures and alarm prioritization. The results of the present effort will eventually be used in determining the functional specifications for an Advanced Control Room (ACR). (See Abbreviations List)

It has been identified[1] that there were three main deficiencies in the control room at TMI: (1) There was a lack of adequate post-accident instrumentation and, therefore, the

capability to diagnose plant state; (2) the emergency procedures were designed for responses to single events and did not address the occurrence of multiple failures indicated by plant symptoms; and (3) the alarm system did not suitably alert the operators to the changes in plant state, but rather was a source of confusion. This paper describes the present ongoing effort at addressing the above deficiencies and integrating control room functional design aspects. The effort is composed of applications of new design methods which attempt at designing the control room on the functional aspects of the entire plant rather than on single events or on the requirements of each individual system designer. The new methods include the use of plant safety functions and functional flow models of processes to depict systems interactions during accident conditions. There is presently an effort to improve the control room for plant operability and availability also; however, these results are not presented in this paper.

CRITICAL SAFETY FUNCTIONS AND PLANT OPERATIONS DURING EMERGENCY CONDITIONS

This work was initiated in Phase II of the Electric Power Research Institute Disturbance Analysis and Surveillance project,[2,3] during

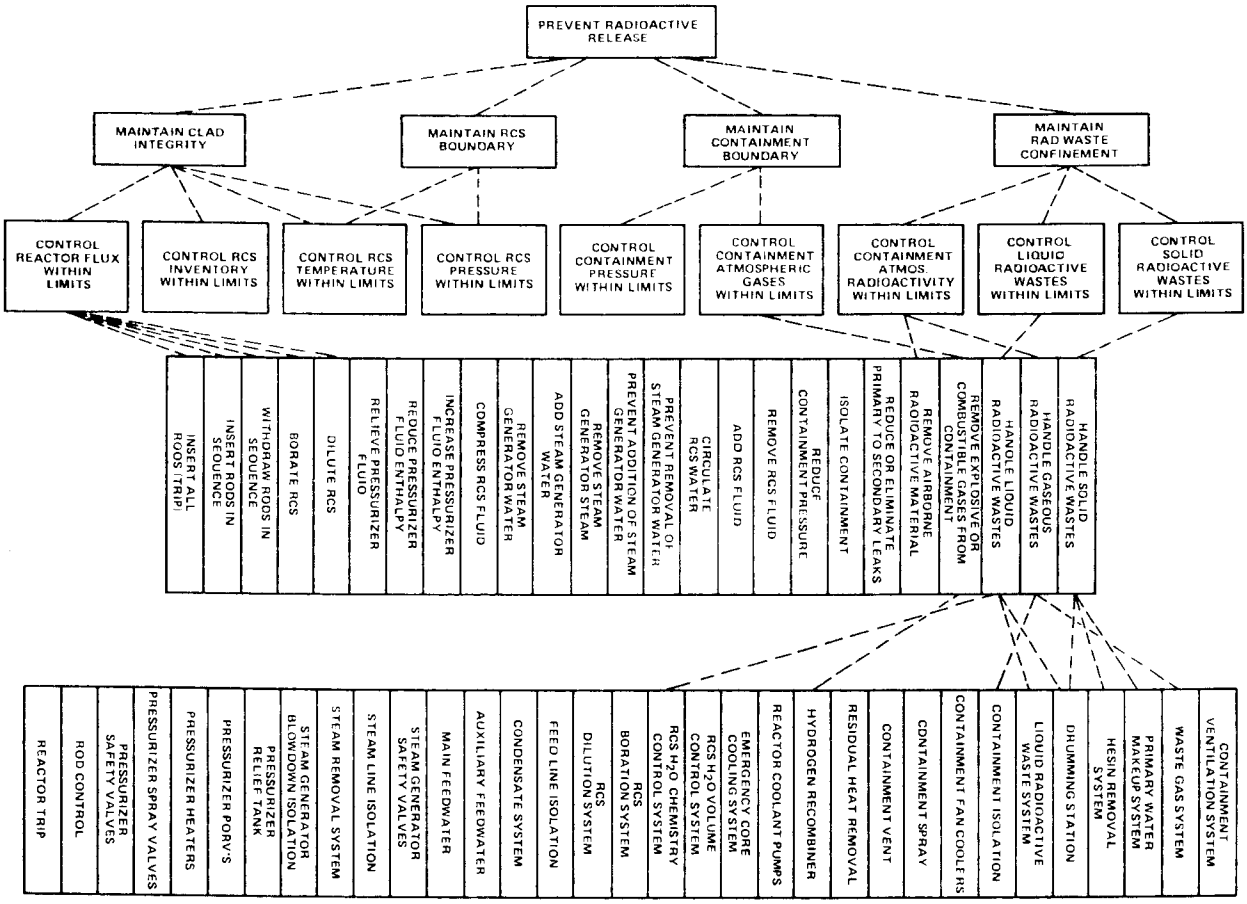


Figure 1. Critical Safety Requirements and Functions Chart

which a functional relationship chart for PWR safety was formulated as a conceptual model of a nuclear power plant. The functional relationship chart identified the primary objective in the design of a nuclear power plant from a public health and safety viewpoint, which is to prevent radioactive releases to the environment. Multiple fission product barriers are designed to achieve this objective, and are kept intact by maintaining critical parameters within limits. Systems and subsystems are provided to perform functions which maintain these critical parameters within limits and are composed of various individual components. Thus, the plant can be envisioned as a multilevel pyramid starting with the objective of preventing radioactive release and broadening continually until the individual component level is reached. Figure 1 is the top section of the aforementioned functional relationship chart and shows the critical parameters (safety functions) in the plant that have to be controlled within limits to maintain the integrity of the barriers which prevent the release of radioactive material to the environment. Also shown are the control requirements and available plant systems.

The set of critical safety parameters shown in Figure 1 has been used as the basis for constructing a set of plant safety status trees that would guide an operator to perform appropriate control actions to maintain plant critical parameters within limits. For example, Figure 2 shows the plant safety status tree for the critical parameter, reactor coolant system (RCS) pressure. The endpoints FP-1 and FP-2 in Figure 2 indicate that a response to high or low RCS pressure is required. The curve tagged 1 on the RCS Pressure vs T_{cold} graph is the limit on RCS pressure for overpressurization and vessel integrity concerns. The curve tagged 4 indicates the conditions at which the reactor coolant will change phase. Further, the endpoints are marked according to the priority of reponse required and are indicated by the amount of shaded area within the annulus. A set of plant safety status trees for all the critical safety parameters identified in Figure 1 then forms the basis for a network of control actions for plant safety. A set of critical safety function restoration guidelines is presently being developed to specify the control actions for the various combinations of critical safety function status. This work is being done for utilities to meet NRC requirements that were issued as a result of the accident at TMI. Presently, Westinghouse is continuing this effort by constructing a functional model of the entire plant, and therefore attempting to integrate the developed guidelines with the various functional aspects in an ACR design — particularly the alarm system.

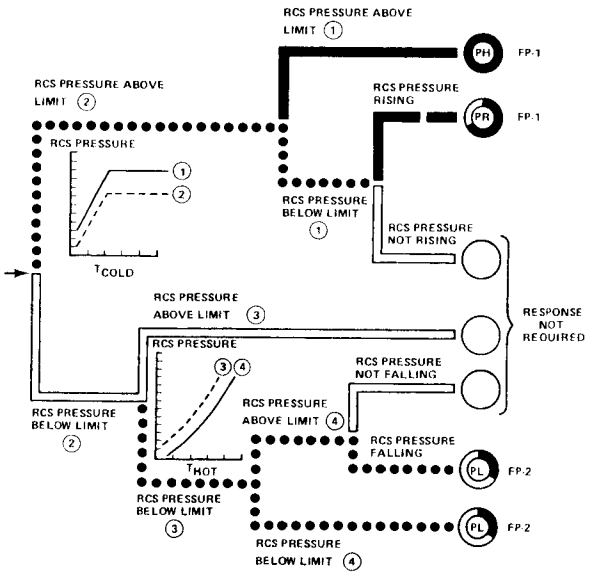


Figure 2. Plant Safety Status Tree for the Critical Parameter (RCS) Pressure

FLOW MODELS

The development of a functional relationship chart[2,3] for all plant systems used during emergency conditions was an attempt at representing their functions and interrelationships for plant control. However, it has been realized that the chart shown in Figure 1 is not the most suitable form for such a depiction. Lind[4,5,6] has proposed a method for describing process plants in terms of the topology of the pattern of pure energy and material (mass and energy) transport and storage. The technique is called "flow modeling." The basic assumption is that mass and energy processes can be described by two fundamental types of phenomena: transport and storage of material and energy. Figure 3 shows the five symbols (nodes) used in flow modeling and the following are some definitions taken from Lind.[4]

- **Storage Processes** include simple accumulation phenomena, i.e., pile-up of material or energy in a volume, and in addition may also include changes of material composition and changes of phase.
- **Transport Processes** include the transfer of material and energy between two locations in space by convection, conduction and diffusion phenomena.
- A **Barrier** is a permanent physical boundary that only functions to prevent the transport of material or energy across the boundary.
- A **Conditioning Subsystem** either controls the main process (e.g., Reactor Coolant Pressure Control System), or establishes and maintains proper function of the main system (e.g., component cooling).
- A **Conditioning Variable** is the physical variable in the main process that is controlled or maintained by a conditioning subsystem.
- **Processing Subsystems** function as sources or sinks of material or energy in relation to the main system.
- An **Aggregate** is a collection of interrelated transport and storage processes. Aggregates are used for representing plant subsystems for which the internal structure is ignored.

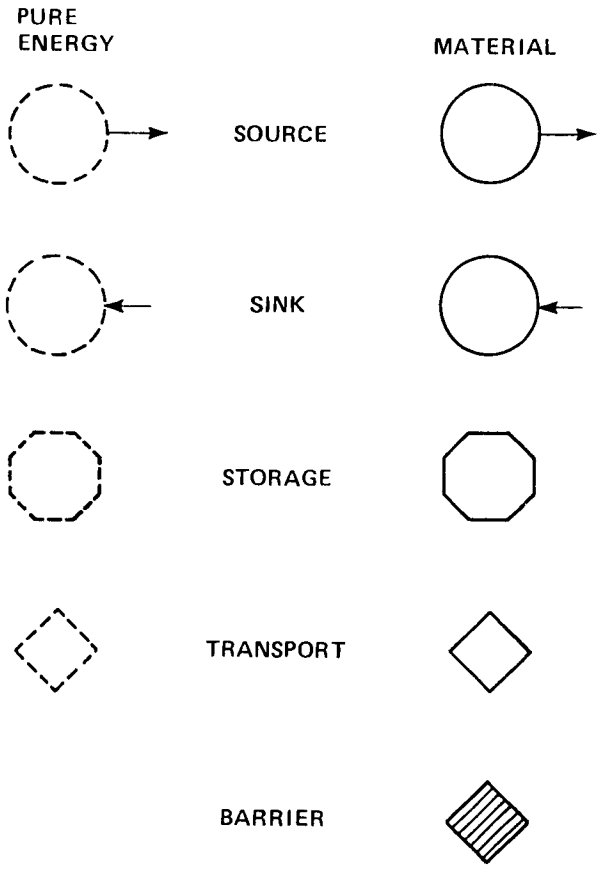


Figure 3. Symbols Used in Flow Modeling

A graphical description of the plant can be made through the use of the symbols shown in Figure 3 and defined above. This graphical description is termed a "flow structure" and describes the plant in terms of its fundamental processes and their relationships as opposed to a description of interconnections of processing components which are shown in piping and instrumentation diagrams (P&ID). The description of a plant in terms of its flow structure allows a decomposition of the plant into its systems and subsystems. This decomposition forms a hierarchy as shown in Figure 4 and depicts the functional relationships between plant processes.

FLOW MODEL DESCRIPTION OF A PWR DURING ACCIDENT CONDITIONS

Figure 5 illustrates the basic plant control problem that has to be addressed for accident situations in a PWR or any fission power producing facility. There are two integral aspects in the problem due to the nature of the fission process and its byproducts: transfer of fission product decay heat, and prevention of the release of fission products to the environment. These then become a complex systems engineering problem for nuclear power plants which have numerous systems and release paths that have to be controlled and monitored. It is necessary to determine why, when, and how various systems are used in the plant, and the consequence of failures of various systems and barriers. Only then can an information system (including alarms) be effectively designed to aid an operator in this complex task.

We attempt here to formally model this problem and then deduce the requirements for an information system for a control room. Figure 6 shows, in an aggregate manner using flow model terminology, the goal during emergency plant (Westinghouse SNUPPS) operations, i.e., the prevention of radioactive material release to the environment. Included in this goal is the requirement for continuous decay heat removal

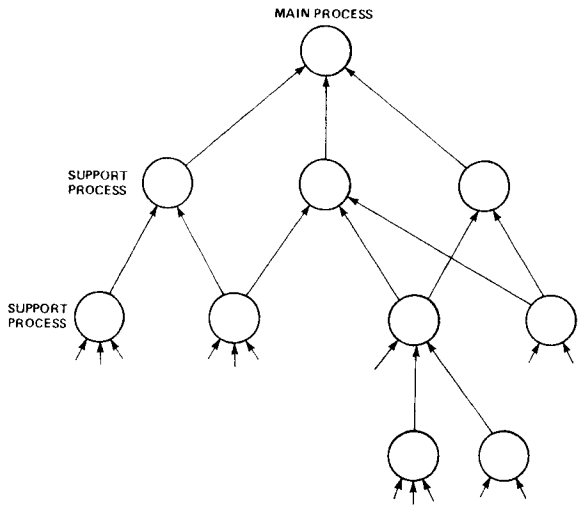


Figure 4. Decomposition of Plant Processes

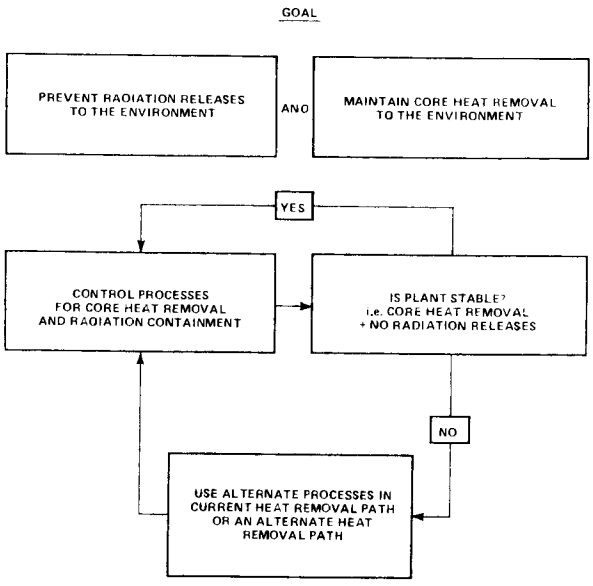


Figure 5. Block Diagram for Plant Control During Accident Conditions

to prevent a core melt. Figure 6 shows the barriers in a PWR that defend against radioactive release to the public, i.e., fuel rod material, fuel rod cladding, reactor coolant system boundary, and containment.

The fuel rod material must be prevented from melting to maintain fission products within the crystalline lattice in the solid fuel. As indicated in Figure 6, this first barrier is maintained by controlling the neutron flux in the core to keep the reactor subcritical during accident conditions. The second barrier is the fuel rod cladding. The fuel cladding may fail because of high internal pressure caused by molten fuel or a departure from nucleate boiling in the coolant. As shown in Figure 6, the integrity of the fuel cladding is maintained by controlling neutron flux, and pressure, temperature and inventory of the Reactor Coolant System (RCS). The neutron flux is controlled by the Reactor Trip and Emergency Boration Systems, and the pressure, temperature and inventory of the RCS are controlled by the core and RCS heat removal systems. The third barrier is the RCS boundary. This boundary (reactor vessel, primary piping, etc.) may fail due to overpressure conditions or by exceeding Nil Ductility Transition limits. NDT limits are avoided by controlling RCS pressure and temperature. The final barrier is the containment. The integrity of the containment building is maintained by controlling containment hydrogen concentration, pressure, and temperature. The radioactivity in the containment must also be controlled to avoid high radiation leakage rates and to minimize release if this last barrier is breached. These critical variables are controlled by the Containment Spray and Hydrogen Control Systems.

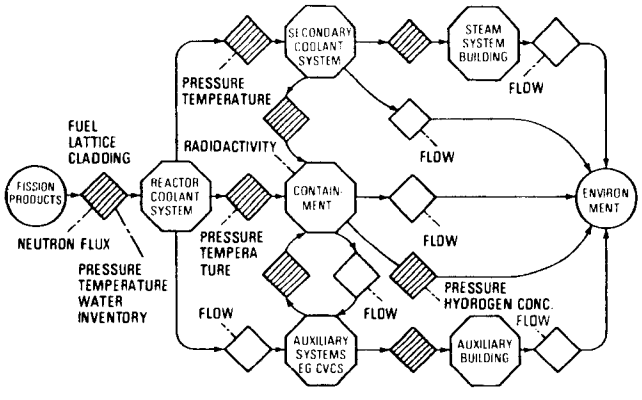


Figure 6. Flow Model of Radioactive Material Transport During Accident Conditions in a PWR

Also shown in Figure 6 are the barriers (components and piping) of the Secondary Coolant System (SCS), and the auxiliary systems to the RCS and SCS. The transport nodes indicate the existence of paths that result from the use of various plant processes. A correlation between transport nodes in Figure 6 and those in flow models of plant processes used for decay heat removal and other barrier maintenance functions (e.g., Containment Spray System) will identify the detailed release paths and implications of isolating process paths due to the failure of various barriers. The model in Figure 6 only addresses fission products in the core and contaminated coolants as sources of radioactive material. Similar models can be made to address radioactive release from radioactive wastes and spent fuel storage tanks which are independent problems.

Figure 6 shows the conditioning variables (critical safety parameters) that have to be maintained and controlled within limits to meet the overall objective. A distinction can be made here between variables that have to be controlled within limits, e.g., containment pressure and hyrogen concentration, versus variables that have to be continuously controlled to maintain a specific function. For

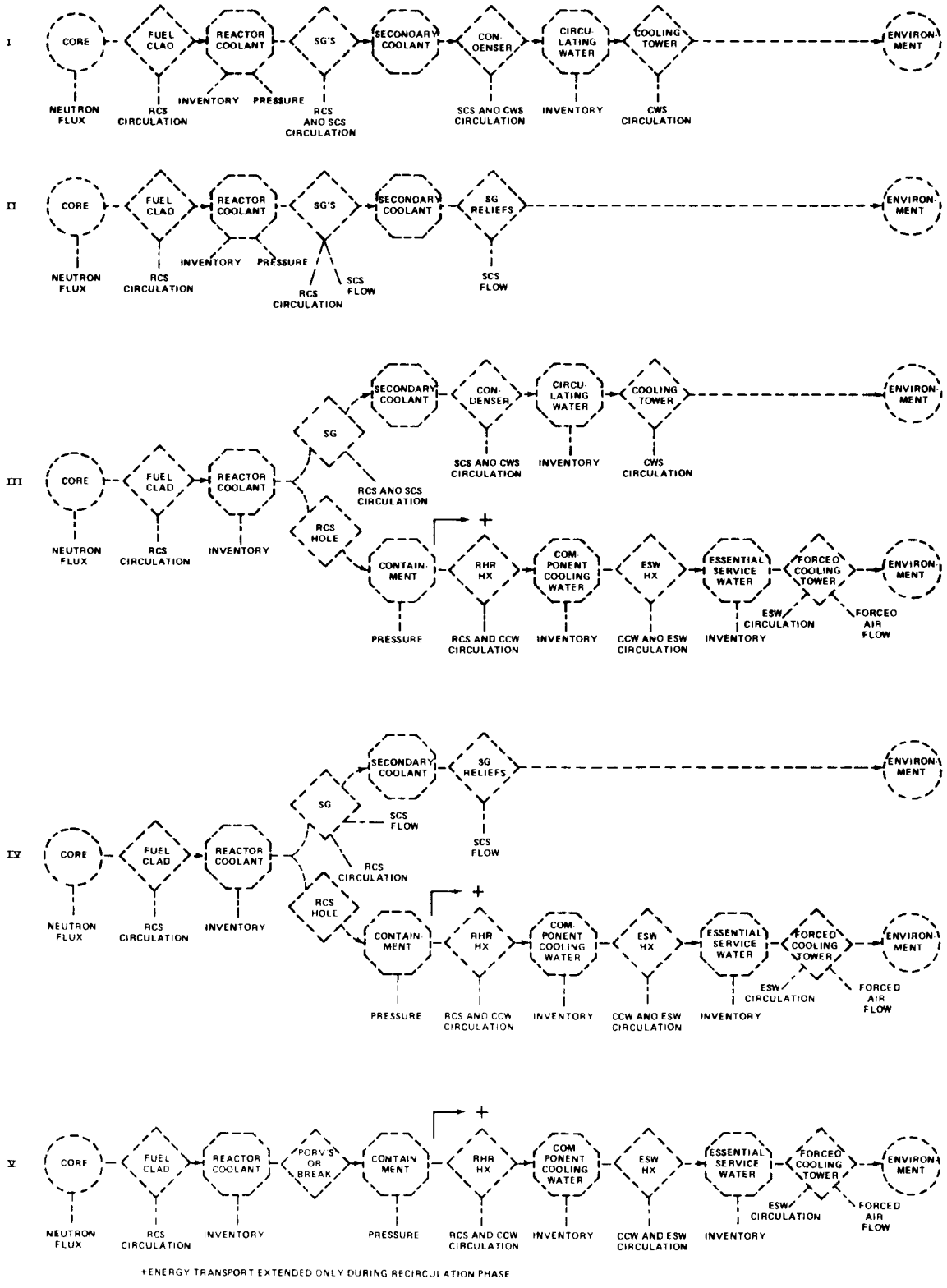


Figure 7. Heat Removal States During Accident Conditions in a PWR

example, the core heat removal function dictates continuous control of RCS pressure, temperature, and inventory. The processes (systems) conditioning the first type of variables are initiated only if the variable exceeds a calculated setpoint, whereas processes supporting heat removal are in continuous operation. It should be noted that the conditioning variables on the various nodes in Figure 6 are identical to the critical safety parameters shown in Figure 1. The material flow model in Figure 6, however, diagramatically further describes the matter of the problem. The details of the problem may then be described in further detail from this top level model.

Figure 7 shows, as energy flow models, the five distinct core decay heat removal paths (states) available during accident conditions in Westinghouse PWR Standard Nuclear Power Plants (SNUPPS). These five heat removal states (HRS) or paths can be defined as distinctly unique paths, via various coolant systems, through which decay heat may be transported from the core to the environment. They include only the stable plant states. For example, a steam line break into containment requires steam generator isolation and is not considered a stable plant heat removal state. Also, the cold shutdown heat removal state, to which the plant is transferred after the plant is stabilized following a reactor trip, is not included.

Corcoran[7] has identified the need for plant state identification and has suggested a tabular verbal format for listing plant states. Analysts, particularly in probabilistic risk assessment, continually consider decay heat energy flow paths as part of their modeling effort. However, there has not been a diagrammatic modeling formalism for describing plant state in terms of the fundamental mass and energy flows until the method proposed by Lind.[4] Such a formalism is particularly useful for ACR functional design work (procedures, alarms and instrumentation) since it provides a mechanism to formulate and describe the basis for specifying the need for equipment and analytical models. Further, the flow model formalism allows one to model and understand the interrelationship between systems (processes) in various anomalous conditions.

The heat removal states in Figure 7 may be viewed as the goal states the plant should be transferred to for various plant anomalies. Figure 8 shows the correlation between plant anomaly(ies) and heat removal states. This correlation is determined from plant protection systems design bases. The plant should be transferred to HRS-I for all anomalies that dictate a reactor trip and which are not in the main decision flow chart shown in Figure 8. As shown in Figure 7, the decay heat in HRS-I is transferred from the core to the reactor coolant and then to the secondary coolant at the steam generators. The energy is then transferred to the tertiary coolant (circulating water) at the condensers, and then to the environment at the natural draft

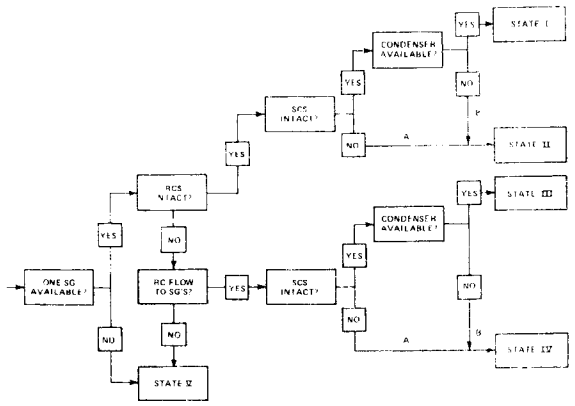


Figure 8. Main Decision Flow Chart for Determining Heat Removal Goal State During Accident Conditions in a PWR

cooling towers. Also shown in Figure 7 are the variables that must be suitably conditioned by various processes to maintain core heat removal in this state. The question of condenser availability in Figure 8 includes passive (breaks) or active failures that prevent energy transport via the condensers and cooling towers using tertiary coolant. Such failures dictate that the plant operational mode be transferred to HRS-II as shown in Figure 7 where energy is transported from the secondary coolant directly to the environment via the steam generator relief valves. HRS-II is also the desired goal state when the SCS boundary is not intact, e.g., steamline or feedline break, or stuck open condenser steam dump valves. The main steam isolation valves to the condenser are closed for such anomalies.

HRS-III and IV are the result of the RCS boundary not being intact, i.e., a loss of coolant accident resulting from a break, stuck open valve, etc. Steam generator (SG) tubes are not included as part of the RCS boundary here. An SG tube rupture dictates isolation of that particular SG. The heat removal state (path) or the coolant systems supporting energy transport are the same unless all four SGs are unavailable. SG availability is defined as the availability of feedwater to one SG which is intact (SG tubes, feedline, and steamline up to the MSIV and atmospheric steam dump valves). The top legs in HRS-III and IV shown in Figure 7 are determined by similar considerations as for HRS-I and II. The bottom legs for HRS-III and IV are identical; that is, they are a result of reactor coolant spillage into containment. Note that energy in the containment is transported to the environment by the Component Cooling and Essential Service Water systems only during the emergency core cooling recirculation phase. HRS-V in Figure 7 is the ultimate heat removal state which results from the unavailability of all SGs or a large break in the RCS boundary leading to inadequate reactor coolant circulation for heat transport to the secondary coolant.

The flow chart in Figure 8 identifies in a complete manner the basic diagnosis that must be done for plant control during emergency conditions. Plant diagnosis may be accomplished in a number of ways and degrees of reliability. Provided adequate instrumentation is available, the operator may symptomatically diagnose plant state using his own mental pattern recognition capability. However, this method is questionable for multiple failures for which the operator has not had a prior recognition. Alternatively, the operator may be given subflow charts for each question in Figure 8 to guide him in determining plant status. There is presently a considerable amount of work being conducted on automated diagnostic methods for plant state identification; these may be categorized[8] as symptomatic searches (pattern recognition[9]), or topographic searches[5,6] using mass and energy balances. The importance of plant surveillance instrumentation[10] (e.g., for Rx and SG levels) and signal processing techniques (e.g., noise analysis[11,12]) must be emphasized as being prerequisites to proper diagnosis. We shall not attempt here to solve the important and complex problem posed in Figure 8 but rather continue to describe the method for showing the interrelationships between processes, and the control actions necessary for transfer to a goal state once a diagnosis has been made.

Figure 9 shows process flow models for inventory control in HRS-I and II (Figure 9A), and HRS-III, IV and V (injection phase shown in Figure 9B and recirculation phase in Figure

9C). Figure 9D shows the flow structure for component cooling water (CCW) circulation which supports the pumps used in the processes shown in Figures 9A, B, and C, and also supports energy transport from the containment sump to the essential service water (Figure 7, HRS-III, IV and V). The transport nodes from the containment sump to the RCS in Figure 9C are also identified in the radioactive material transport flow model shown in Figure 6 between the containment and the auxiliary systems since a break in the ECCS in the auxiliary building would release radiation via the vents. These flow models are shown as examples of process flow structure and how supporting processes and/or components are identified. Also illustrated is how the interelationship between a supporting process (CCW) and the various processes it supports is determined and shown. There are numerous such complex functional interrelationships in a nuclear power plant and these are identified in a full set of flow models. Such a set has been completed for SNUPPS and includes the processes that condition nodes in Figure 6 (e.g., CSS), and all the vital support systems (component cooling, compressed gas and electric power systems) in a nuclear power plant. This complete flow model set forms the basis for a plant diagnostic and alarm system, and may also be a useful systems information format for developing fault and event trees in a risk assessment study.

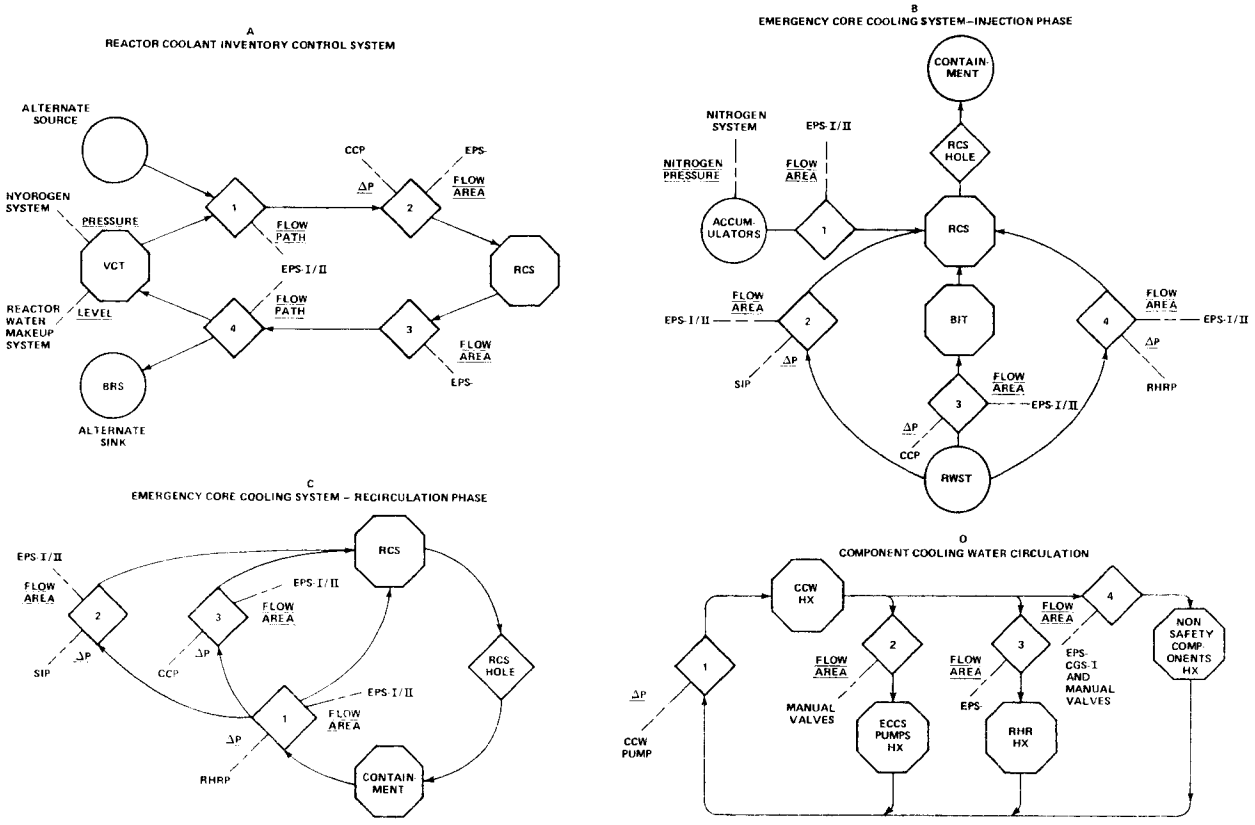


Figure 9. Examples of Flow Models for Processes Supporting Core Heat Removal

STATE ACTION NETWORKS

We have so far discussed a method for describing plant processes and their interrelationships in various plant states. Lind[4] has also proposed a method, for describing plant state transitions, which is closely related to flow models and conceptually similar to the precedence network theory developed for project management.[13] In this method, a prior distinction is not made between automatic and manual control actions since there is no formal difference between operating procedures and the specification of control action sequences for automatic systems. In a State Action Network (SAN), one shows the decomposition of control tasks required for a defined plant state transition. The basic postulate is that a task decomposition into sequential and concurrent action sets results from the topology of material and energy flow as described in flow models. The SAN formalism provides a structured method for plant control design, or for describing plant control tasks before any judgements (task analyses) can be made regarding their adequacy.

Figure 10A shows the basic symbol used in a SAN. A process (system or subsystem) or component is taken from an initial state S_1 to S_2 by a set of control actions. State changes can be indicated at various levels of detail, e.g., change in plant HRS, initiation of a process supporting heat removal, or initiation of a component in a supporting process. Therefore, tasks can be decomposed into subtasks and such a decomposition is made similar to the decomposition of flow structure in flow models.

There are basically two categories of control in process plants. One category includes control actions for flow structural changes in the plant. For example, transition from normal operating conditions to HRS-IV requires the activation and deactivation of various processes. Figure 10B shows the format for representing the decomposition into subtasks for the above type of control. The second category of control is the type where further decomposition is not possible due to the task being a functional "whole," e.g., a valve is modulated till a tank reaches a desired setpoint. The symbol for such control actions is shown in Figure 10C, and Figure 10D shows how the actions are combined in a control sequence. Figure 10D also shows that two systems (or components) are required to be in a particular state before a control action can be executed on one of them. Figure 10E shows the symbol for a conditional (c) task which is executed depending on the output of some logic other than what triggered the SAN it is included in. Finally, Figure 10F shows the symbol for representing alternate state actions to accomplish the same control function.

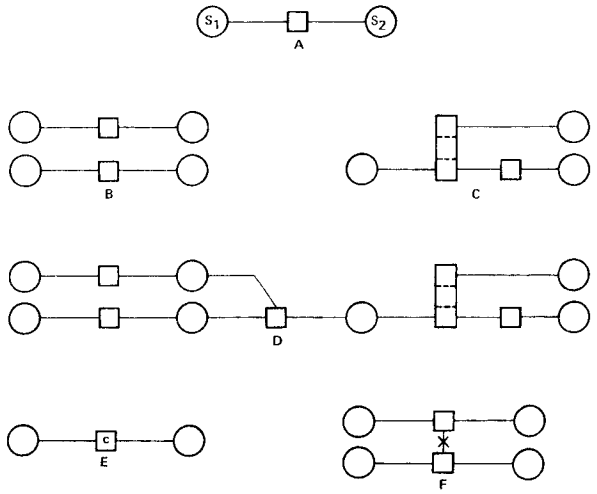


Figure 10. Symbols Used in State Action Networks

APPLICATION OF STATE ACTION NETWORKS FOR RESPONSE DURING EMERGENCY CONDITIONS IN A PWR

Figure 11 shows the main tasks, as a SAN, for plant transitions to HRS-I through V from normal operations above 15 percent of full power. Essentially, Figure 11 identifies the tasks necessary to suitably condition the heat removal paths identified in Figure 7, namely the control of processes that condition the variables identified in Figure 7. Figure 12 is an example of a decomposition of a task identified in Figure 11 to detailed subtasks. The tasks required to change the flow structure shown in Figure 9B to that in Figure 9C are identified in Figure 12. The subtasks for the components are determined from the identification of the various components needed to condition the variables in Figures 9B and 9C. The relationship between SANs and flow models is due to the nature of control actions required for mass and energy processes. However, not all tasks are related to heat removal. Containment isolation is related to the second aspect of the problem (radiation release) that was discussed earlier with references to Figures 5 and 6. A complete set of conditional control tasks for various combinations of failures of barriers have not been identified in Figure 11 and would affect the use of various processes. Alternatives for control actions for transition to a HRS have also not been shown in Figure 11.

The SAN in Figure 11 for transition into the five heat removal states is an attempt at formulating a response network to respond to passive and active multiple failures. As shown earlier in Figure 5, emergency response can be considered to consist of a transition to a heat removal state, followed by a possible degradation of heat removal state, and reponses required to isolate radioactive release paths being formed as a result of the failure of various barriers. The SAN formalism based on heat removal states

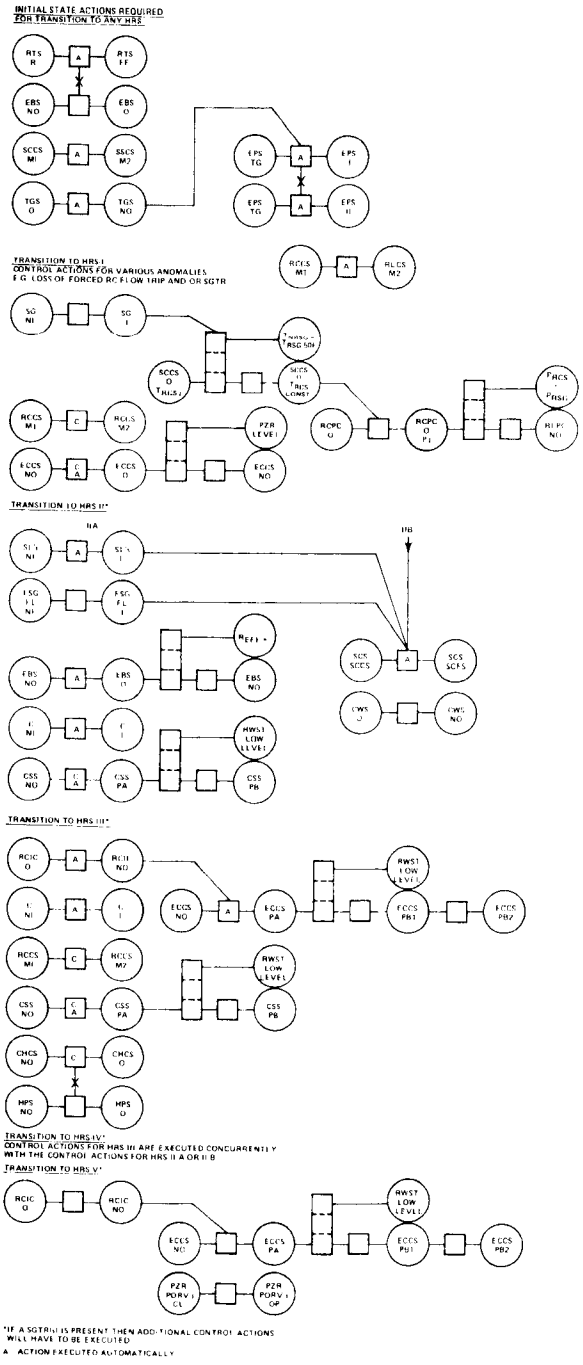


Figure 11. State Action Network for Transition to Heat Removal Goal States During Accident Conditions in a PWR

allows the inclusion of multiple failures into the network in a logically structured manner due to the mass and energy topographic basis.

The logic in Figure 8 triggers the conditional state action for transition to a heat removal state. Figure 8 shows in an aggregate form the categories of possible failures in a PWR and all failures fall into one of the categories. For example, the question "Condenser available?" includes all active and passive failures in the tertiary coolant portion of the plant heat removal path. Isolation of processes due to radiation release concerns may also result in the unavailability of the tertiary coolant system.

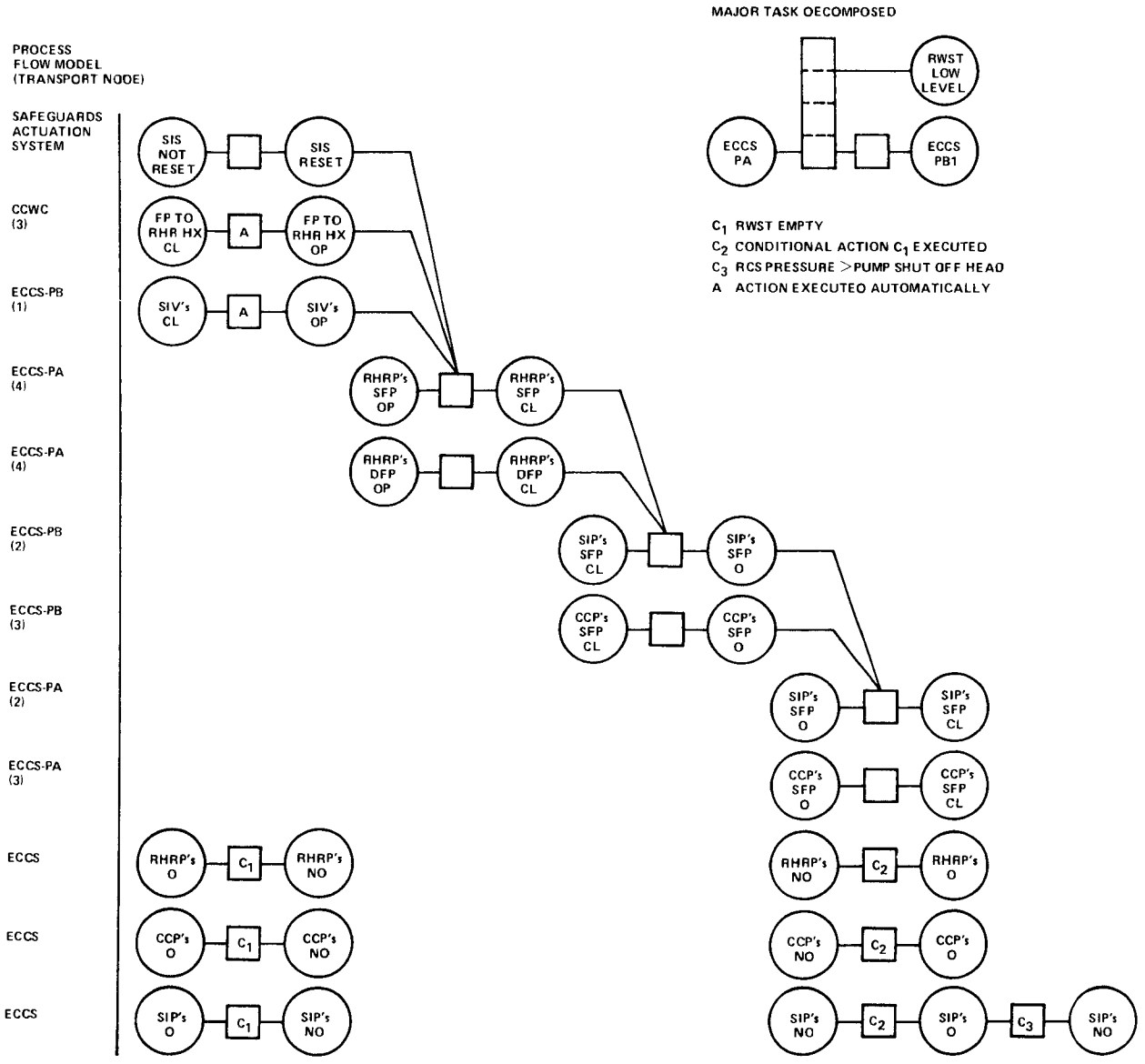


Figure 12. State Action Sequence for ECCS Transition from Injection to Cold Leg Recirculation Phase

Lind[4] has also proposed that the control heuristics or bases for the specification of state actions should be formulated. The heuristics consist of reasons for the precedence in state actions, preference of alternatives, and prioritization of concurrently required state action sequences. For example, one heuristic would be "reactor coolant must always exist." These heuristics will be the design bases for SANs, and also the knowledge data base for operators executing and monitoring the control actions. The detailed subtasks for the tasks identified in Figure 11 and the control heuristics are presently being developed and formulated.

The development of SANs from flow models for HRSs and radiation release paths is only the first phase of the development of an emergency response network. The second phase of the development will consist of scheduling of the tasks and determining whether the state action sequence can be adequately executed. Time constants from plant dynamic analysis will be necessary for such an evaluation. Control actions can then be designated as being manual or automatic using such schedular information. It should be noted that the above design method for developing an emergency response scheme can also be used for a formal task analysis of existing normal or emergency response networks (procedures). To date, this method is the only formalism that fundamentally describes process plant operations and therefore allows a proper and complete determination of the plant variables that have to be monitored to verify the execution of control actions.

INFORMATIONAL REQUIREMENTS FOR PLANT CONTROL

The informational requirements for plant state indentification and control during emergency conditions may now be identified from the formulation presented above. The

TABLE I
HIERARCHY OF INFORMATION FOR PLANT CONTROL

Level	Identification
I	Identification of the status of barriers and radiation releases to the environmnent (see Figure 6) and Identification of the plant heat removal goal state (see Figures 7 and 8).
II	Identification of the capability of the processes conditioning the nodes in the flow models representing the first level. Includes monitoring of the conditioning variables and overall process performance (mainly mass and energy flows).
III	Identification of the status of the nodes and the variables that have to be conditioned to support the above processes. The variables may be conditioned by components or supporting processes.
	The lowest level identifies the status of individual components.

alarm system will be an integral part of the required information and will consist of annunciators that will alert the operating crew to changes in plant state based on the above formulation. The requirements for post-accident instrumentation may then be derived in a formal manner from such informational requirements.

Table I lists the information required for plant control during accident conditions and shows how flow models allow a hierarchical representation of the information. The hierarchy of information for the second and lower levels is based on the decomposition (as shown in Figure 4) of plant flow structure and identification of supporting subprocesses and/or components. See Goodstein[14] for a complete discussion on an informational hierarchy based on a system's decomposition as illustrated in Figure 4 and discussed in this paper.

Table II lists and categorizes the alert conditions that should be addressed by an alarm system for plant control; such a categorization is consistent with the proposed overall information system philosophy. Category 1 is for power production and has not been dealt with in this paper. Category 2 includes plant anomalies shown in Figure 8 and all other anomalies that dictate a reactor trip and transition to HRS-I. Category 3 includes anomalies in control actions during transition to an HRS, and Category 4 includes recoverable anomalies at steady-state operation at an HRS. Category 5 includes anomalous conditions that dictate a degradation of HRS and are determined by the logic in Figure 8.

The various categories require different degrees and types of alert. For example, an alert for Category 3 may be a blinking message on a cathode ray tube (CRT) display which the operator monitors to verify his control actions, whereas anomalies in Category 4 and definitely Category 5 require a much more drastic alert mechanism. The alarm categories include in them anomalies such as loss of barriers and potential release of radioactive material to the environment. An annunciator system based on Figure 6 could be used to alert the operator to execute prescribed conditional control actions for failures of various barriers, or to determine a suitable

TABLE II
CATEGORIZATION OF ALARMS

1.	Recoverable anomalies during power production. a. Anomalies related to a state action b. Anomalies not related to a state action
2.	Anomalies dictating a reactor trip.
3.	Recoverable anomalies related to state actions for transition to a heat removal state (HRS).
4.	Recoverable anomalies during steady HRS operation.
5.	Anomalies dictating a degradation of HRS.

control action where one has not been prescribed. The urgency of a response would depend on the severity of or potential for release and this can be encoded in the annunciator system as various degrees of alert.

Finally, Figure 13 shows a possible annunciator to indicate the status of core heat removal. Such an annunciator system could be used for two purposes: to alert the operator and indicate the heat removal goal state he must achieve and maintain, and to alert and indicate the "health" of the conditioning variables and therefore processes supporting the current heat removal goal state. The operator can then be directed to displays (based on the informational hierarchy shown in Table I) to investigate the status of the processes conditioning the variables for heat transport. If the operator is unable to restore the "health" of the process(es), he is dictated by the annunciator to a degraded heat removal state to maintain core heat removal and, therefore, plant safety.

CONCLUSIONS

A basis for response during emergency conditions in a PWR has been proposed using two new modeling tools: flow models and state action networks. The aim of this fundamental approach to such a complex problem is to formulate a common basis for emergen-

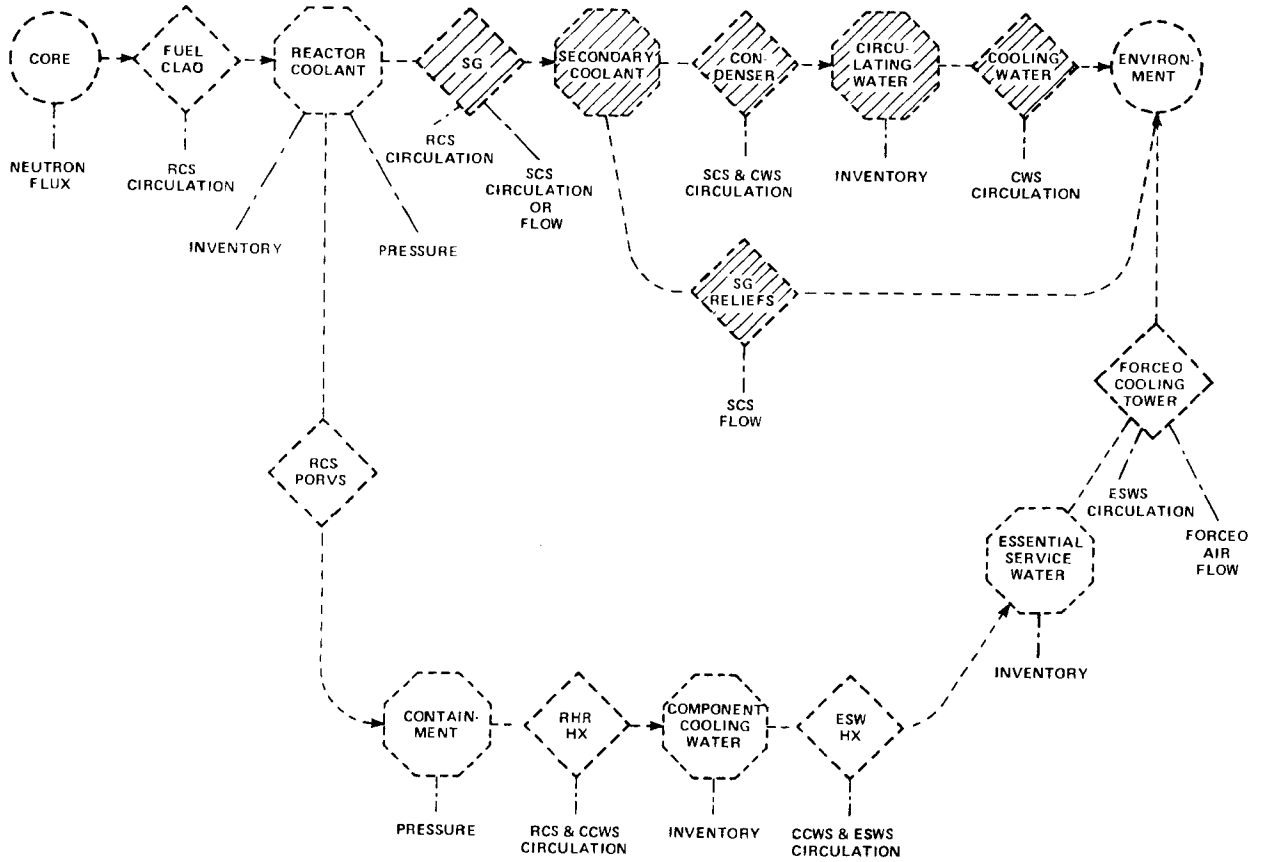


Figure 13. A Possible Annunciator System to Indicate the Status of Core Heat Removal (e.g., Loss of Secondary Heat Sink Dictates Heat Removal State V)

cy procedures, alarm prioritization, post-accident instrumentation, and advanced diagnostic methods for an advanced control room. The fundamental nature of the formulation allows one to include responses to multiple failures in a logically structured manner, and therefore extend the prescribed capabilities of a control room as much as desired. However, the complexities and utility of the proposed approach will only be realized once a representative application has been made.

ACKNOWLEDGEMENTS

We wish to thank our colleagues from various organizational units in Westinghouse that are involved in the work presented in this paper.

REFERENCES

1. *Clarification of TMI Action Plan Requirements,* U.S. Nuclear Regulatory Commission NUREG-0737, November, 1980.

2. Rumancik, J. A., Easter, J. R., and Campbell, L. A., "Establishing Goals and Functions for a Plant-Wide Disturbance Analysis and Surveillance System (DASS)," *IEEE Trans. Nucl. Sci., 28,* pp. 905-912, (1981).

3. Gallagher, J. M., et al., "A Process for Design of a Plant-Wide Disturbance Analysis and Surveillance System," Report NP-2240, Electric Power Research Institute (1982).

4. Lind, M., "The Use of Flow Models for Design of Plant Operating Procedures," in *Proc. IWG/NPPCI Specialists' Meeting on Procedures and Systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations,* December 5-7, 1979, Garching, Federal Republic of Germany, N-38-79, NKA/KRU-PZ (79) 26.

5. Lind, M., "The Use of Flow Models for Automated Plant Diagnosis," in Rasmussen, J. and Rouse, W. B. (Eds) *Human Detection and Diagnosis of System Failures,* Plenum, New York, 1981.

6. Lind, M., "Multi-Level Flow Modeling of Process Plant for Diagnosis and Control," This conference.

7. Corcoran, W. R. et al, "Nuclear Power Plant Safety Functions," *Nuclear Safety, 22,* pp. 179-191, 1981.

8. Rasmussen, J., "Models of Mental Strategies in Process Plant Diagnosis," in: Rasmussen, Jr. and Rouse, W. B. (Eds.) *Human Detection and Diagnosis of System Failures,* Plenum , New York, 1981.

9. Pau, L. F., "Application of Pattern Recognition to Failure Analysis and Diagnosis," Ibid.

10. Hsu, Y. Y. and Hon, A. L. M., "Some Possible Ways to Improve Nuclear Power-Plant Instrumentation," *Nuclear Safety, 22,* pp. 728-737, 1981.

11. Thie, J. A., "Surveillance of Instrument by Noise Analysis," *Nuclear Safety, 22,* pp. 728-737, 1981.

12. Byford, R. G. and Geis, C. G, "An Advanced Digital Metal Impact Monitor," *IEEE Trans. Nucl. Sci., 29,* pp. 993-999 (1982).

13. Burman, P. J., *Precedence Networks for Project Planning and Control,* McGraw Hill, New York, 1972.

14. Goodstein, L. P., "Computer-Based Operating Aids," in *Proc. Design, 82,* Birmingham, UK, September 22-23, 1982.

ABBREVIATIONS

ACR	Advanced Control Room
BIT	Boron Injection Tank
BRS	Boron Recycle System
C	Containment
CACS	Containment Air Cooling System
CCP	Centrifugal Charging Pump
CCW	Component Cooling Water
CCWC	Component Cooling Water Circulation
CGS	Compressed Gas System
CHCS	Containment Hydrogen Control System
CSS	Containment Spray System
(PA PB)	(Injection Recirculation)
CL	Closed
CWS	Circulating Water System
DFP	Discharge Flow Path
EBS	Emergency Boration System
ECCS	Emergency Core Cooling System
(PA PB)	(Injection Recirculation, 1 = Cold Leg, 2 = Hot Leg)
EPS	Electric Power System
(I II)	(Offsite Diesel)
ESWS	Essential Service Water System
FE	Function Executed
FL	Feedline
FP	Flowpath
FSG	Faulted Steam Generator
HPS	Hydrogen Purge System
HRS	Heat Removal State
Hx	Heat Exchanger
I	Isolated
M	Mode of Operation
MSIV	Main Steam Isolation Valve
NI	Not Isolated
NO	Not Operating
NRSG	Not Ruptured SG
O	Operating
OP	Open
PA	Phase A
PB	Phase B
PORV	Power Operated Relief Valve
PWR	Pressurized Water Reactor
PZR	Pressurizer
R	Ready
RCCS	Reactor Coolant Circulation
(M1 M2)	System (Forced Natural)
RCIC	Reactor Coolant Inventory Control System
RCPC	Reactor Coolant Pressure Control System
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RHRP	Residual Heat Removal Pump
RSG	Ruptured Steam Generator
RTS	Reactor Trip System
RWST	Refueling Water Storage Tank
Rx	Reactor
SAN	State Action Network
SCCS	Secondary Coolant Circulation
(M1 M2)	System (Main Auxiliary)
SCS	Secondary Coolant System
SCFS	Secondary Coolant Flow System
SFP	Suction Flow Path
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIP	Safety Injection Pump
SIS	Safety Injection Signal
SIV	Sump Isolation Valve
SL	Steamline
SNUPPS	Standard Nuclear Power Plants
T_{cold}	RCS Cold Leg Temperature
TGS	Turbine Generator System
TMI	Three Mile Island
VCT	Volume Control Tank
ΔP	Differential Pressure

Nuclear Technology Division
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, Pennsylvania, 15230, USA