

CONF-860414--2

DISCLAIMER

By acceptance of this article, the publisher or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering the article.

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.

Instrumentation and Controls Division

CONF-860414--2

DE86 007240

**STATE AND DATA TECHNIQUES
FOR CONTROL OF DISCONTINUOUS SYSTEMS**

R. A. KISNER

Oak Ridge National Laboratory*

Presented to: Sixth Power Plant Dynamics,
Control, and Testing Symposium

April 14-16, 1986
Knoxville, Tennessee

MASTER

*Operated by Martin Marietta Energy Systems, Inc., for the U. S. Department of Energy under Contract No. DE-AC05-84OR21400.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Jsw

STATE AND DATA TECHNIQUES FOR CONTROL OF DISCONTINUOUS SYSTEMS

R. A. Kisner

Oak Ridge National Laboratory*
Oak Ridge, TN 37831

1. INTRODUCTION

The need for automated control systems becomes clear as the complexity of nuclear power plants increases and economic incentives demand higher plant availability. A control system with intelligence distributed throughout its controllers allows reduction in operator workload, perhaps reduction in crew size, and potentially a reduction in on-line human error. In automated systems of this kind, each controller should be capable of making decisions and carrying out a plan of action.

This paper describes a technique for structured analysis and design of automated control systems. The technique integrates control of continuous and discontinuous nuclear power plant subsystems and components. A hierarchical control system with distributed intelligence follows from applying the technique. Further, it can be applied to all phases of control system design (phases of design are discussed in other references¹). For simplicity, the example used in the paper is limited to phase 1 design (basic automatic control action), in which no maintenance, testing, or contingency capability is attempted.

An advanced large-scale nuclear reactor system is analyzed, and an automatic control structure developed. The automatic control system involves human operators to the extent of only specifying the mode desired and the power level. Other duties of the operators, which include monitoring and scheduling, involve occasional indirect interaction. Interface for manual operation is possible with this design, although not pursued in this paper.

2. BACKGROUND

Consider the traditional design of a "semi-automatic" plant control system: (1) Servo controllers are installed on those plant systems that exhibit continuous parameter behavior. Servo control over one or perhaps two variables is realized. However, human operators start or prepare the system for operation. Set points are generated by the operators, who occasionally adjust and optimize them as plant conditions change. (2) sequence control-

*Operated by Martin Marietta Energy Systems, Inc., for the U. S. Department of Energy under Contract No. DE-AC05-84OR21400.

lers are installed on a few critical subsystems which exhibit discontinuous parameter behavior, such as those that have only off-on or start-run-stop states. Thus, at an operator's command, a timed sequence of actions can realign system valves, start pumps, or do whatever else is required to ready the system. (3) The operators carry out most of the discrete actions required to operate the plant. They, in turn, are following prescribed written procedures that have been compiled by designers and other experts.

The operator's workload becomes high during transition periods, such as maneuvering from one power level to another or as abnormal conditions develop. At such times he becomes involved with the moment-by-moment operation of subsystem controllers and must, as well, maintain global control of the plant. The operator's workload is low during steady-state periods. In adhering to the semi-automated design approach, very little intelligence and capability is given to the subsystem controllers to reduce the operating crew's workload during active periods.

3. CONTROL STRUCTURE

Integrated operation of the plant systems at a high level is required to effect automatic control and coordination of the components of a nuclear power plant. The structure and function of the plant control system becomes an important factor in effectively using automatic control.

To create a control structure, the plant is divided into subsystems and grouped by prime, support, or utility relationship to the plant. An example subsystem grouping with associated controllers for an advanced nuclear plant is shown in Fig. 1. The figure is organized according to prime systems, but with support and utility systems also shown. The information concerning the subsystems shown in the figure can be expanded to include controller signal requirements by indicating possible modes of operation and data flows. A sample of this information is given in Table 1. In the table, the data flows are grouped according to input and output relation to the subsystem. The input and output flows are further divided as follows: efferent flows are commands or data flowing to subordinates; afferent flows are status or data flowing to supervisors; and transferent flows are inhibits or permissives laterally communicated at the same level in the control system hierarchy.

Operating procedures are analyzed along with other data obtained from subject matter experts, including designers, operators, and maintainers. Specific sequences and plant mode changes are analyzed such as startup, shutdown, power ascent, and power descent. From these analyses and the plant information in Table 1, state dynamic and data transformation models are created. These models reflect the functional relationship required to perform these sequences and mode changes. The building of models for the basic sequencing and major mode changes of the power plant constitutes the first phase effort of the several phases involved in the design of an automated plant control system. Other subsequent phases will add automatic testing and validation, and control capability for degraded and faulted conditions.

In an actual design setting, the design would proceed until all transitions and states are included so that the plant would be fully automatic over many modes. However, only the startup transition from plant at cold shutdown to plant at minimum power is analyzed in this paper. This results in incompleteness in the state dynamic models and data transformation models for the plant, because some support systems are assumed to be already operational as initial conditions of the cold shutdown state and other systems are not called into service during this transition.

The basic method used to develop the automatic control system is an extension of the structured analysis and design techniques of Yourdon¹. The approach is first to build a logical model of the control system, then from it build a physical model of the computer processors, interconnection networks, and code environment. The physical model will not be treated in this paper. The logical model consists of two sub-models: one modeling the interface of the control system to its environment, and one modeling the internal behavior of the control system. Logical modeling is generally implementation free, that is, the effort should be independent of programming language or computer type. The context diagram and the external event list are the tools used to create the environment model. Network graphics tools, which are used to create the behavioral model, model the flow and transformation of data through a system, the time-oriented behavior of the discrete states that a system may exhibit, and the organization of stores of data associated with the data transformations. The first two tools, data flow diagram (DFD) and state transition diagram (STD), are used in modeling the plant control system. Modeling of the stored data, by entity relationship diagramming (ERD), has not been done for this system at this time.

The data flow diagramming technique is illustrated in Fig. 2. The transformation scheme shows inputs and outputs as labeled arrows (flows) and the labeled circles (the transformations) represent work done on the inputs to produce the outputs. Other features of the diagram are explicit indications of the stored data used by the transformations and of the boundaries of the system under study.

The state transition diagramming technique is illustrated in Fig.3. The state, shown as a rectangle, represents an externally observable mode of behavior. Each state represents a unique status of the transformation with which it is associated, and the transformation can be in only one state at a time. A set of conditions triggers a sequence of actions that drives the systems to the next state. The conditions may be a complex combination of many variables and parameters, and the actions may also be very complex. Formally this model is a finite automaton with output organized as a Mealy machine². In a Mealy machine, the output is a result of the transition, and the state is passive because it is waiting for the proper condition to trigger it.

One of the advantages of this method of modeling is the linking of the data, state, and store data diagrams that it provides. This integration allows a data flow diagram to control a state transition diagram and vice versa. The actions resulting from a state transition may generate an enable or disable command to a data transformation, thus turning a data flow and

the operations being performed on it on or off. Likewise, the outflow of a data transformation can set the condition for a transition in a state transition diagram. This is shown in Fig. 4. The data flow diagram and state transition diagram may be associated together to form a package diagram. The package diagram may contain many data flow diagrams and state transition diagrams. This minimizes external interfaces to the package, and forms the means for grouping and organizing the control system structure.

The control organization follows from the logical modeling methods described above once the plant is resolved to its basic prime and support subsystems. Plant startup follows a procedure that cuts across subsystem boundaries, as any plant-wide state change. This results in packages that control a mixture of associated subsystems. The distinction between prime and support tends to disappear as they are packaged together to allow the procedures to enable entire systems by simple commands.

A nuclear power plant is primarily driven by state transitions, because of the large number of subsystems enabled and disabled involved in mode change. This results in disconnected sets of data transformations, of which a minimal number will be active at a given time.

4. AUTOMATED CONTROL SYSTEM EXAMPLE

A preliminary Phase 1 design has been done using the structured techniques for control software described. Figure 5 illustrates the context diagram which indicates the boundary of the automated control system. The context diagram makes a simple starting point for system design. Physical equipment are shown as terminations (drawn as squares) to the data flow to and from the control system software (drawn as a bubble). Human subsystems, shown as a termination, are usually separated from other plant systems because of the problematic nature of the required interface. Thus the delineation is made between sensors and actuators, and the control software.

Except for an information-only data line to the planning portion of the control system, no links to the safety system are considered. This is a deliberate design strategy to allow independent assessment by the safety system of the plant condition. The safety system is assumed to be completely independent of the control system and internally possesses the intelligence to recognize plant conditions and take proper action.

The availability of process data is taken for granted in this example. A real-time database management system is required to supply all the needed information about plant components and process variables to any controller regardless of its position in the control system hierarchy or location in the plant. The on-line data base is represented as a data store in the model.

The system package in Fig. 5 can be magnified to show the internal data flows and transformations (transitions of state are as yet hidden in the bubbles). This method of zooming or magnifying the contents of a package can be carried out until the bottom-most element of the control system is

reached. The contents of the system package are shown in Fig. 6. In the figure, seven packages are shown that together constitute the top-level diagram for the basic automatic control phase of the system design. Each package is numbered. A hierarchical numbering scheme is carried by each child diagram to indicate its parent, the same as section headings in a report.

Although Fig. 6 shows the automated control system as a network, it may also be redrawn as the hierarchy shown in Fig. 7. Drawn in this way, the subordinate and supervisory relationships are more apparent. At the lowest level, data changes at a high rate, and the time frame is short for the decisions and objectives of the lower levels. The data required to support higher blocks change more slowly, and the time frame that decisions span is long.

The following paragraphs discuss systems 1, 2, 4, and 5 shown in Figs. 6 and 7. System 3, the continuous system supervisory controller and optimal coordinator, has been discussed in another paper³. System 6, 7, and the plant sensors and actuators are included for completeness but not discussed further.

Package 1.0

The model for the planner (1.0) and situation assessment (6.0) packages is taken from an analysis of operator decision-making tasks⁴. The analysis concludes that decision making can be modeled by three related tasks: (1) situation assessment, (2) planning and commitment, and (3) execution and monitoring.

Within the library of plant modes and states in the planning subsystem, an overall state transition description is present to guide the decision making and sequence selecting process. Fig. 8 shows an incomplete state transition diagram for the plant. Many of the transitions have been left out, especially those for shutdown. A variety of possible equipment and subsystem operational statuses are associated with each state. Table 2 lists some of these statuses as initial conditions for the cold shutdown state. Many variations of the cold shutdown state, or for that matter any state, exist because of different possible initial conditions. Each set of initial conditions will require a different sequence of states or actions of subordinate subsystems to take the plant from its current state to the destination state.

Package 2.0

The initial conditions, initial state, and destination state are passed to the configuration subsystem, package 2.0. With this information, a string of connecting states and their transitions are selected either from a library of precalculated state transition diagrams or by a rule-based processor.

The state transition sequence in Fig. 9 was selected based on the initial conditions given in Table 2 and the initial and final plant states of "waiting in cold shutdown" and "minimum power under supervisory control." The sequence strings together four inner states: (1) non-nuclear systems starting, (2) reactor starting and additional non-nuclear systems starting, (3) reactor and plant heating up, and (4) power increasing to minimum. To initiate a transition to the next state, five conditions are monitored (1) plant startup signal from planner; (2) loops started, condensate cleanup completed, and turbine on turning gear; (3) reactor critical, vacuum established, and turbine auxiliaries operating; (4) hot shutdown temperatures reached, steamline prewarmed, turbine-generator prewarmed, and steam generator chemistry is within specification; and (5) minimum power reached, feedwater supply is on supervisory control. These conditions are available either from the data handling system or from the lower-level controllers involved with producing the state. When the conditions are met, the actions shown beneath them are executed. The next state immediately occurs because the actions are associated with the transitions. This is characteristic of a Mealy model, where the states are predominately a passive aspect of the control system, in which the state is waiting for external conditions to occur.

Package 4.0

The package, "control prime plant systems," consists of eight lower level packages, each corresponding to one of the prime plant systems. These packages are shown on Fig. 10 with their input and output data flows. Solid lines represent data flow paths into or out of the system within the package. A data flow path may consist of continuous or intermittent data types. The flow path usually does not represent a single element of data but is composed of multiple streams or packets that are grouped under a common name. The dashed lines represent control flows and prompts that activate internal features of a package. The control flows provide only one bit of information, being either on or off. The prompts are momentary control flows that initiate an action (e.g., set a condition for a state transformation or enable a data transformation). The control flows also may be grouped under a common name. Control flows are generally associated with producing a structural change in a package, whereas data flows are operated on to produce new data flows.

Package 5.0

The "control support systems" package consists of six lower level packages as shown in Fig. 11. The particular set of subsystems, whose control is represented by these packages, is selected to best accomplish the sequence of actions required by the equipment design and their interconnection. We consider the procedures and the advice of subject matter experts to be the best source of instructions for startup and operation of a normally functioning system. Thus the packaging of the elemental actions derived from these sources proceeds in a bottom-up mode. The same solid and dashed line data and control flow representations apply to package 5.0.

5. CONCLUSION

More work has been done than is shown in these diagrams⁵. However, this paper demonstrates a framework onto which additional plant maneuvers can be appended until a reasonable phase 1 system is formed. The data flow and state transition modeling and diagramming techniques describe the functionality of the automated control system for the next steps in software design. Then the subsequent phases of adding intelligence to the automated control system can proceed. The second phase considers features to determine operability of plant components and systems and makes minor changes in the sequence of an operation or initial conditions. The third phase of design adds the capability of control under degraded conditions, which includes detecting a deviation, diagnosing the situation, making a decision as to what plan should be followed, and executing the plan (and monitoring for success).

1. P. T. Ward and S. J. Mellor, Structured Development for Real-Time Systems, Vol. 1&2, Yourdon Press, 1985.

2. J. E. Hopcroft and Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, 1979, pp. 16-45.

3. G. V. S. Raju and R. A. Kisner, "Distributed and Hierarchical Control Techniques for Large-Scale Power Plant Systems," Proc. Computer Applications for Nuclear Power Plant Operation and Control, Int'l Topical Meeting, ANS, Pasco, Washington, Sept. 8-12, 1985.

4. W. B. Rouse, R. A. Kisner, P. R. Frey, and S. H. Rouse, "A Method for Analytical Evaluation of Computer-Based Decision Aids," NUREG/CR-3655, ORNL/TM-9068, July, 1984.

5. R. A. Kisner, "Automating Large-Scale Reactor Systems," Proc. Computer Applications for Nuclear Power Plant Operation and Control, Int'l Topical Meeting, ANS, Pasco, Washington, Sept. 8-12, 1985.

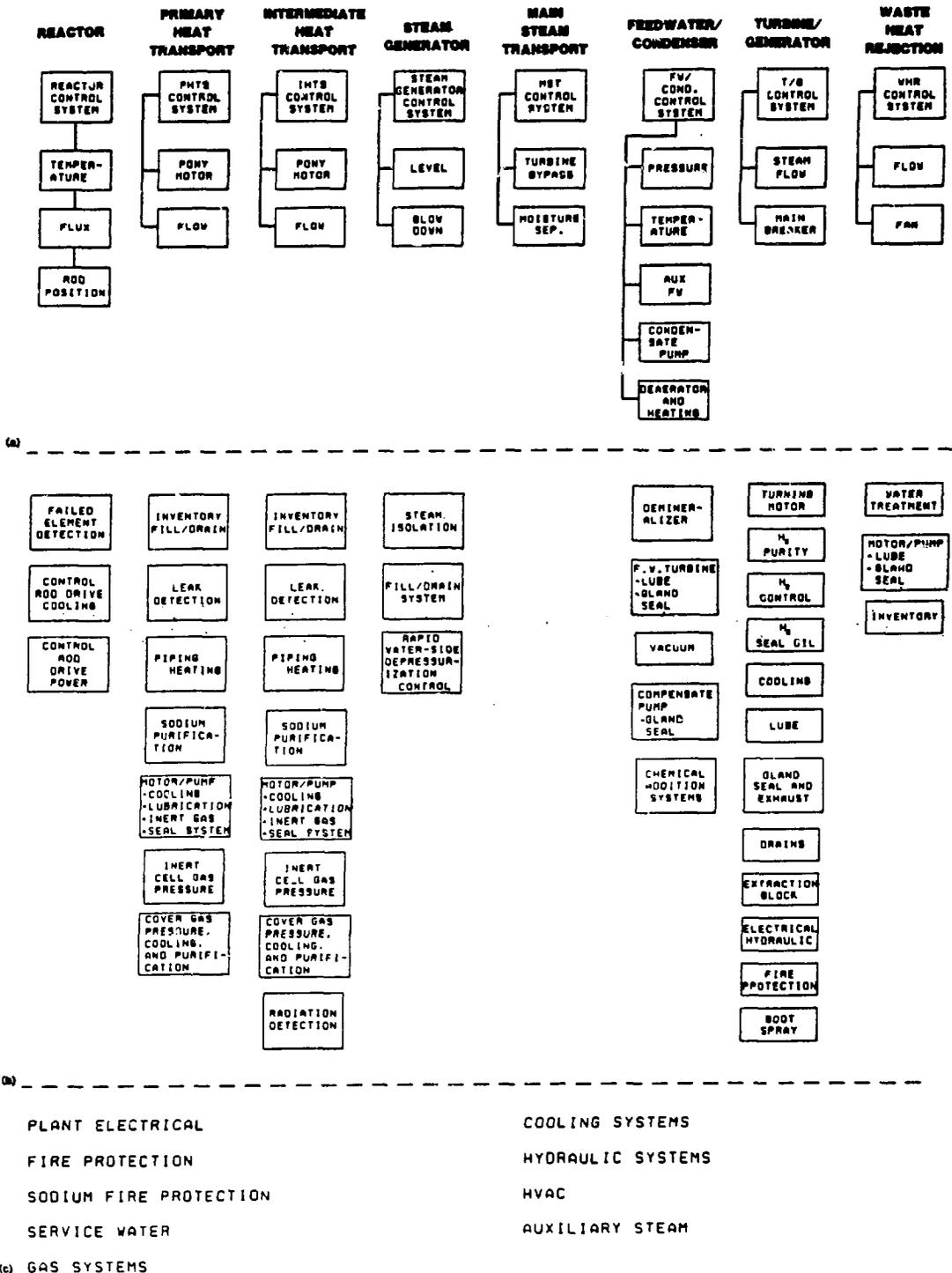
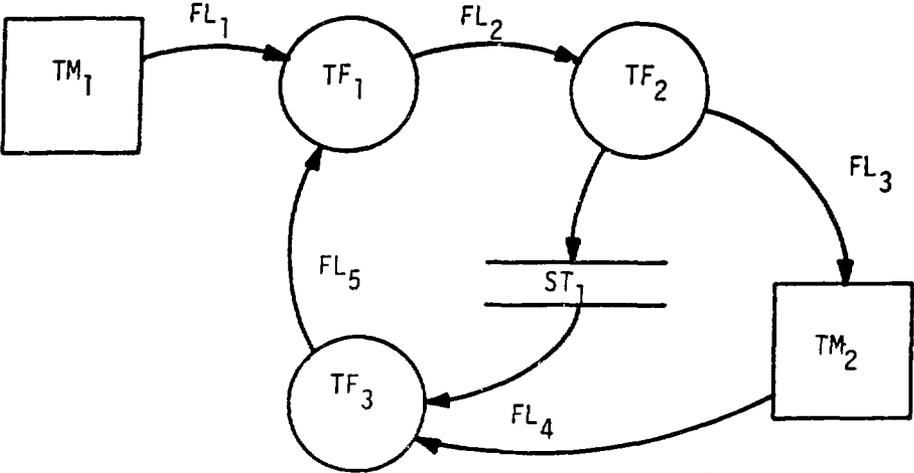


Fig. 1. Local Controllers for an Advanced Nuclear Plant: (a) Prime Plant Systems, (b) Plant Support Systems, (c) Plant Utility Systems.

Table 1. Sample of one of Many Sheets Showing Plant System's Data Flow and Modes of Operation.

System	Mode*	Input			Output		
		Afferent	Efferent	Transferent	Afferent	Efferent	Transferent
Heat rejection (prime)							
Cooling tower flow control			On/off	Inhibit from gland seal water; inhibit from pit level		Motor breaker	Inhibits generated in turbine bypass system
Cooling water mode control	River sink; river/tower; tower sink		Circulating loop configuration			Sluice gate; water valves	
Cooling tower fan control	Run; off; de-ice	Outside air temp.; water temp.	On/off; De-ice			Motor breaker; reversing relay	
Reactor (Support)							
Failed element		Neutrons			Degree of fission prod. release	Controls	Enable precision analysis system
CPDM cooling			Enable/disable cooling system		Status of system	Close breakers	
CRDM power			Enable/disable		Status	Close breakers	
RG cover gas pressure, vent control, purification and cooling		Pressure; purity	Pressure (sp), purity (sp)		Status of valves and pump cooling	Run sample; valve position; pumps (on/off)	
Inert Cell gas pressure			On/off			Gas valves	
Fill/drain (inventory control)		Vessel level; fill flow; drain flow; sodium pump level	Vessel level (sp)			Sodium makeup pumps; valves	Inhibit purification system
Leak detection		Hydrogen; O ₂	On/off		Degree of leakage		



- Data Flow (FL):** A pipeline through which streams or packets of known composition flow.
- Transformation (TF):** Changes incoming flows to outgoing flows.
- Data Store (ST):** Retains (or delays the flow of) data for later use by the transformations.
- Termination (TM):** Marks the edge of the model (a system outside of the system under study).

Fig. 2. Example Data Flow Diagram.

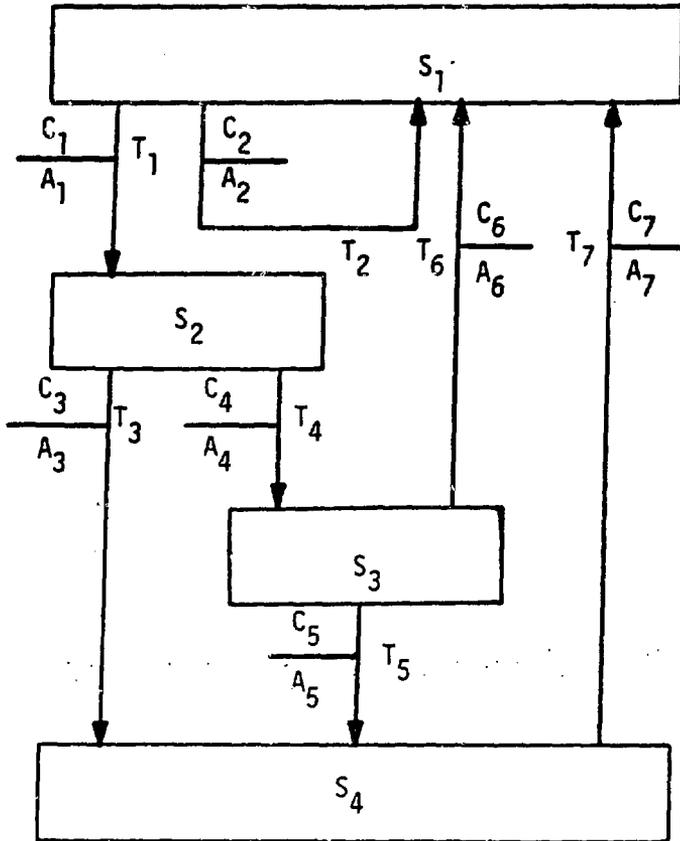


Fig. A.2. State transition diagram.

- State (S)** A mode of behavior of the system that has a unique combination of conditions and destination states. The state is passive because the control system is waiting for conditions to occur.
- Transition (T)** The movement of the system from one state to another.
- Condition (C)** Cause for the system to move from one state to another. Conditions may be generated internally or externally to the system or by time period.
- Action (A)** Carried out by the system as it moves from one state to another. An action can enable/disable a transformation, trigger a "one-shot" transformation, signal a specific condition, set a timer, or issue a control signal.

Fig. 3. Example State Transition Diagram.

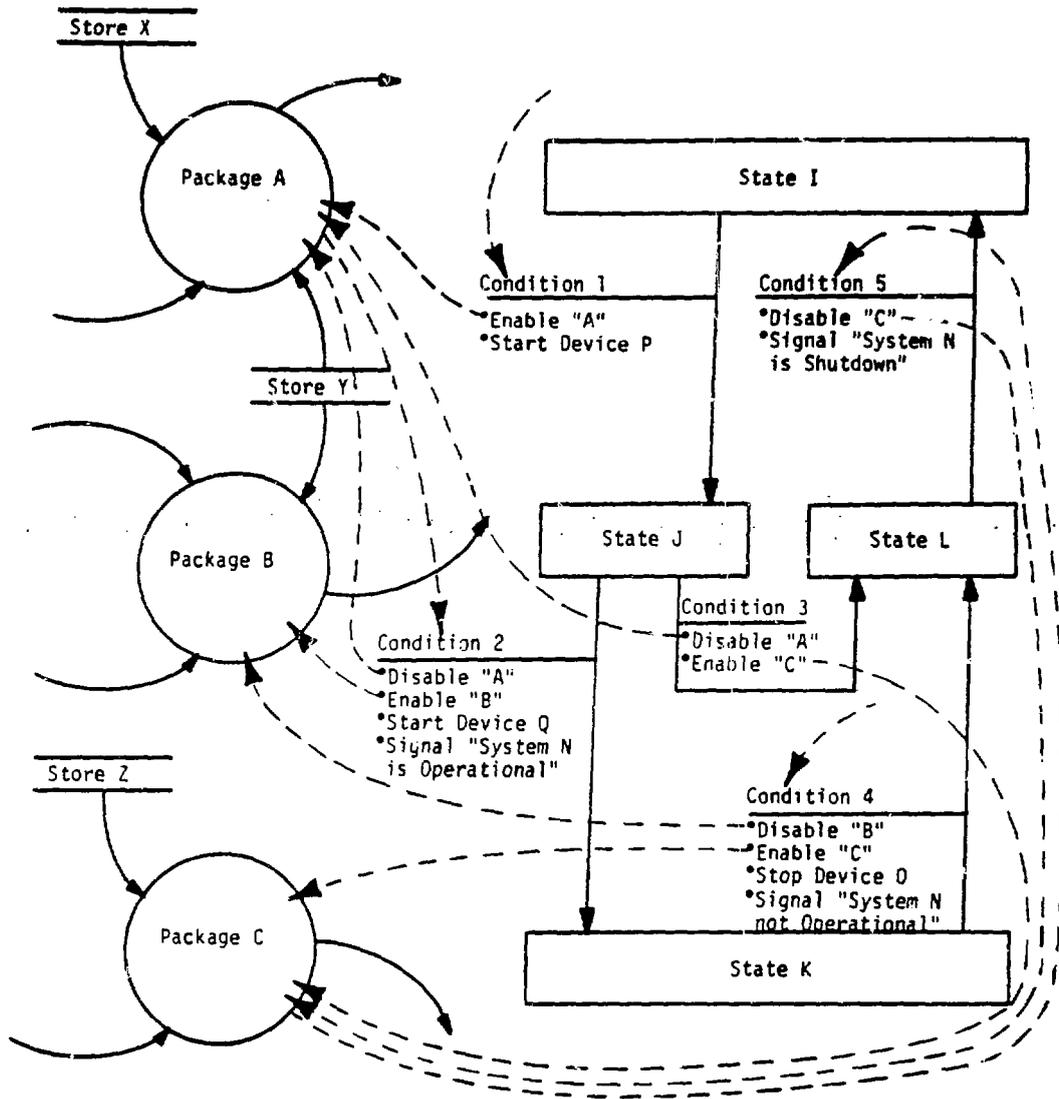


Fig. 4. Example showing DFD and STD interaction. The dashed lines, normally not shown, connect the action statements of the STD with the packages in the DFD and condition requirements of the STD with internal calculations made in the packages.

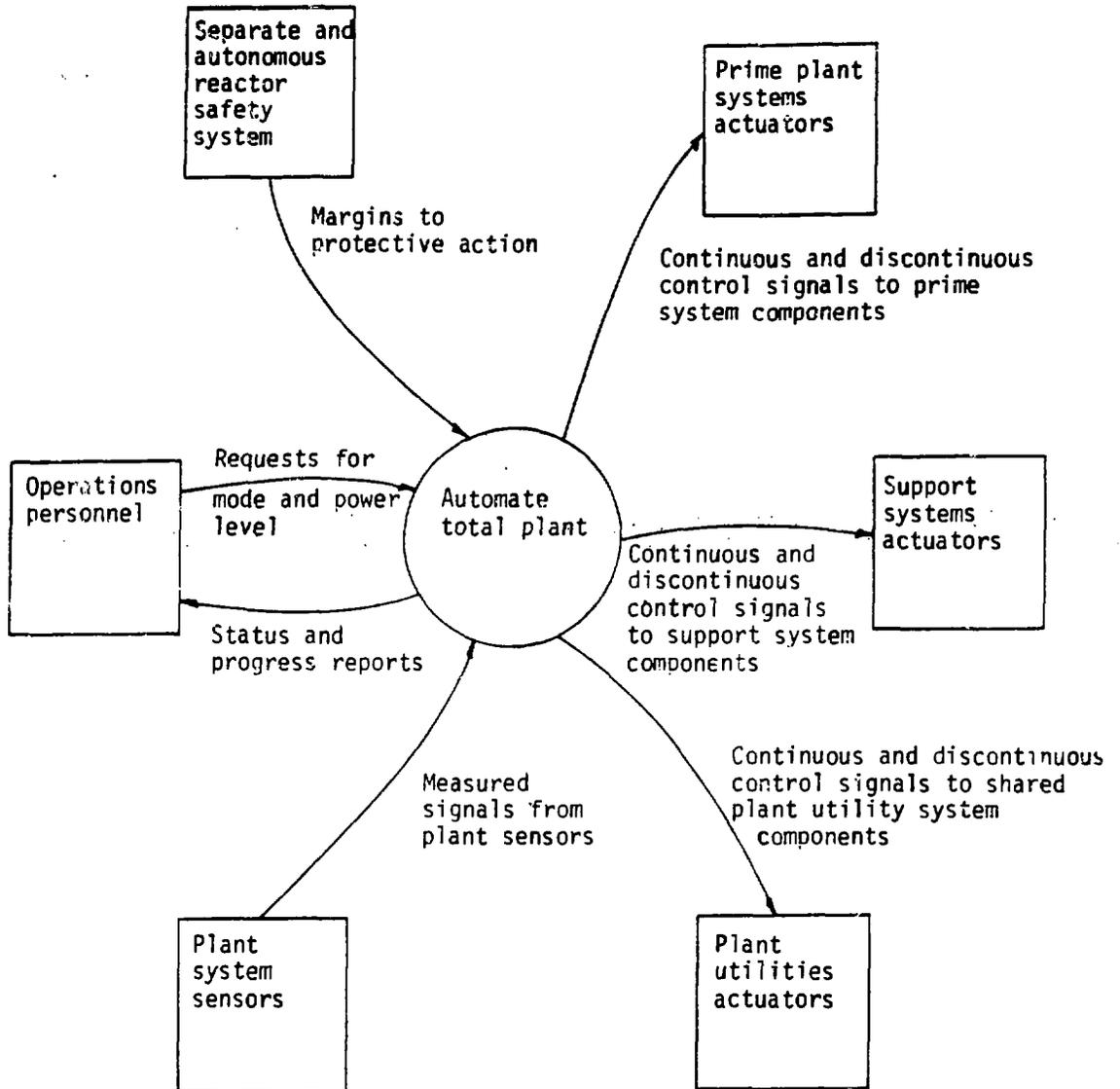


Fig. 5. Context diagram showing automated control system and plant equipment boundary.

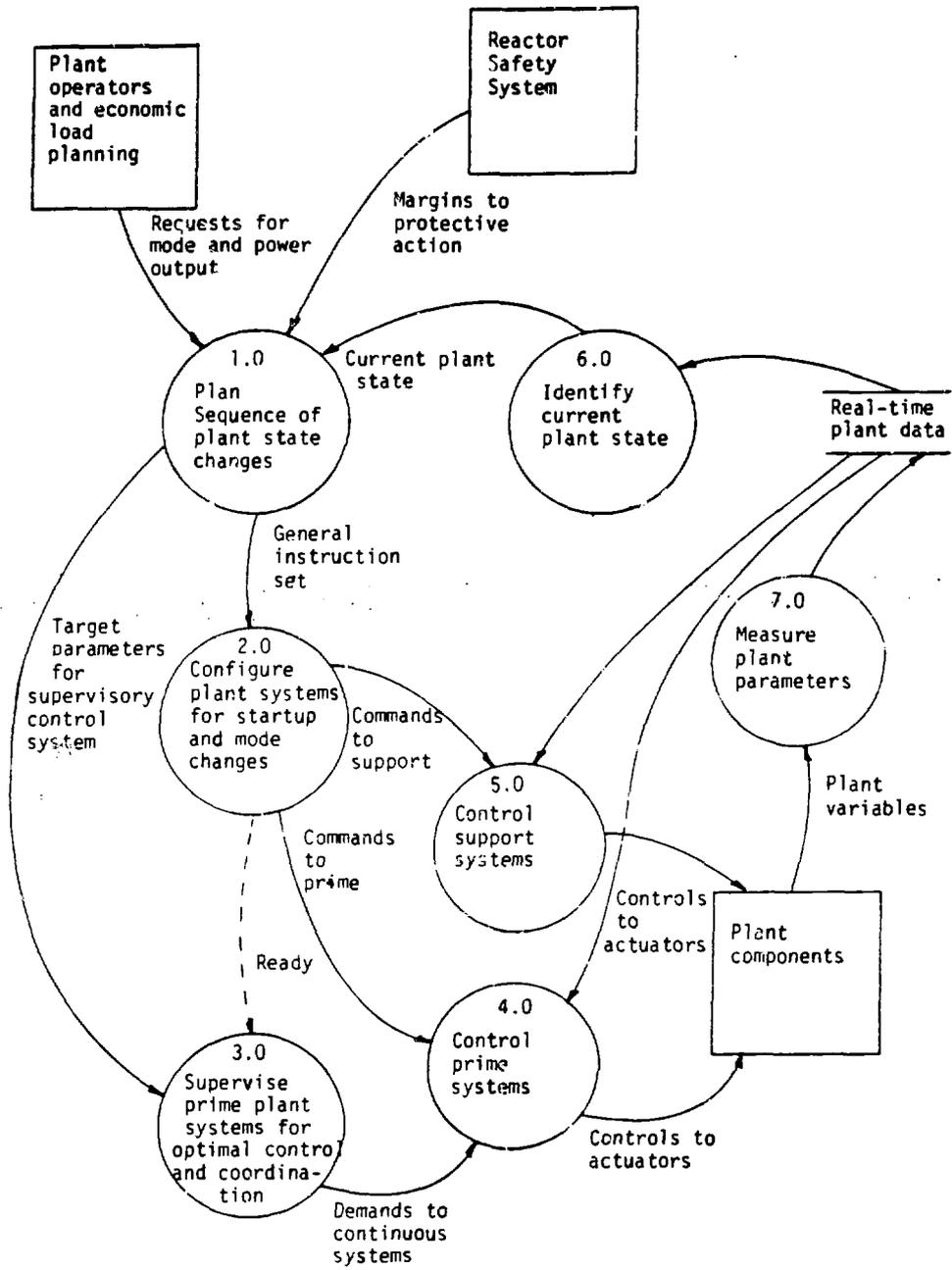


Fig. 6. Top-Level Diagram Which Shows Data Flows For Automated Plant.

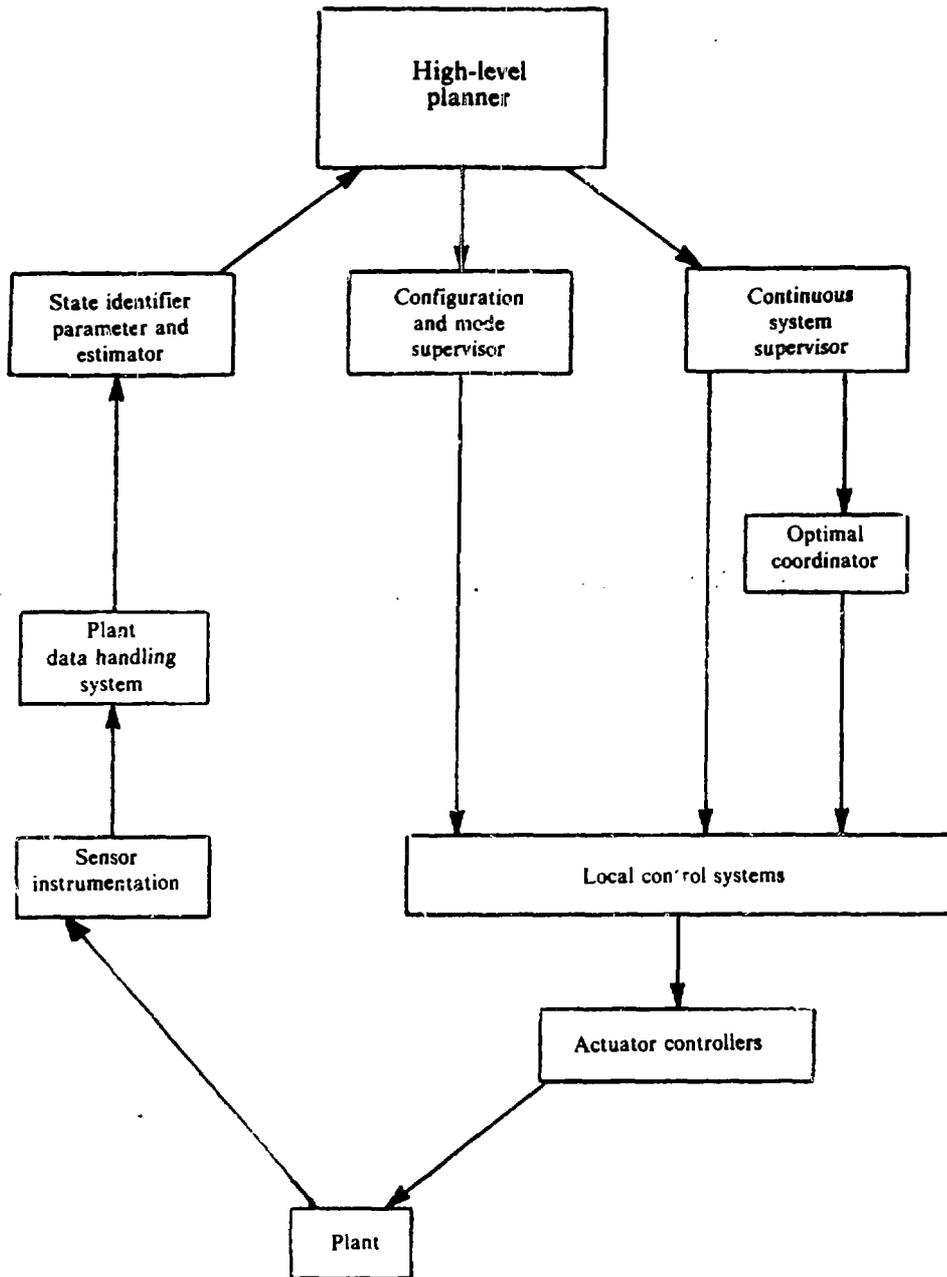


Fig. 7. Hierarchical Representation of the Automated Control System.

**Table 2. Partial descriptions of initial conditions:
WAITING IN COLD SHUTDOWN.**

Refueling is complete

Primary and secondary control rod drive motors are inerted and their cooling systems are operational

Electric heating and cooling established with the steam generators and auxiliary vessel recirculating to the protected air-cooled condenser (PACC)

Leak detection and failed fuel element system is operational

PHTS and IHIS are full and on pony motor flow

PHTS and IHIS have reached temperature setpoint of 400°F

Reactor, PHTS, and IHIS have reached cover-gas, pressure-control setpoint

One cold trip is in operation for the PHTS and one for the IHIS

Vent freeze seals have been established for sodium piping

One sodium purification-impurity monitoring system is in operation for the PHTS and one for the IHIS

All plant utilities are operational

All necessary system tests have been performed and passed

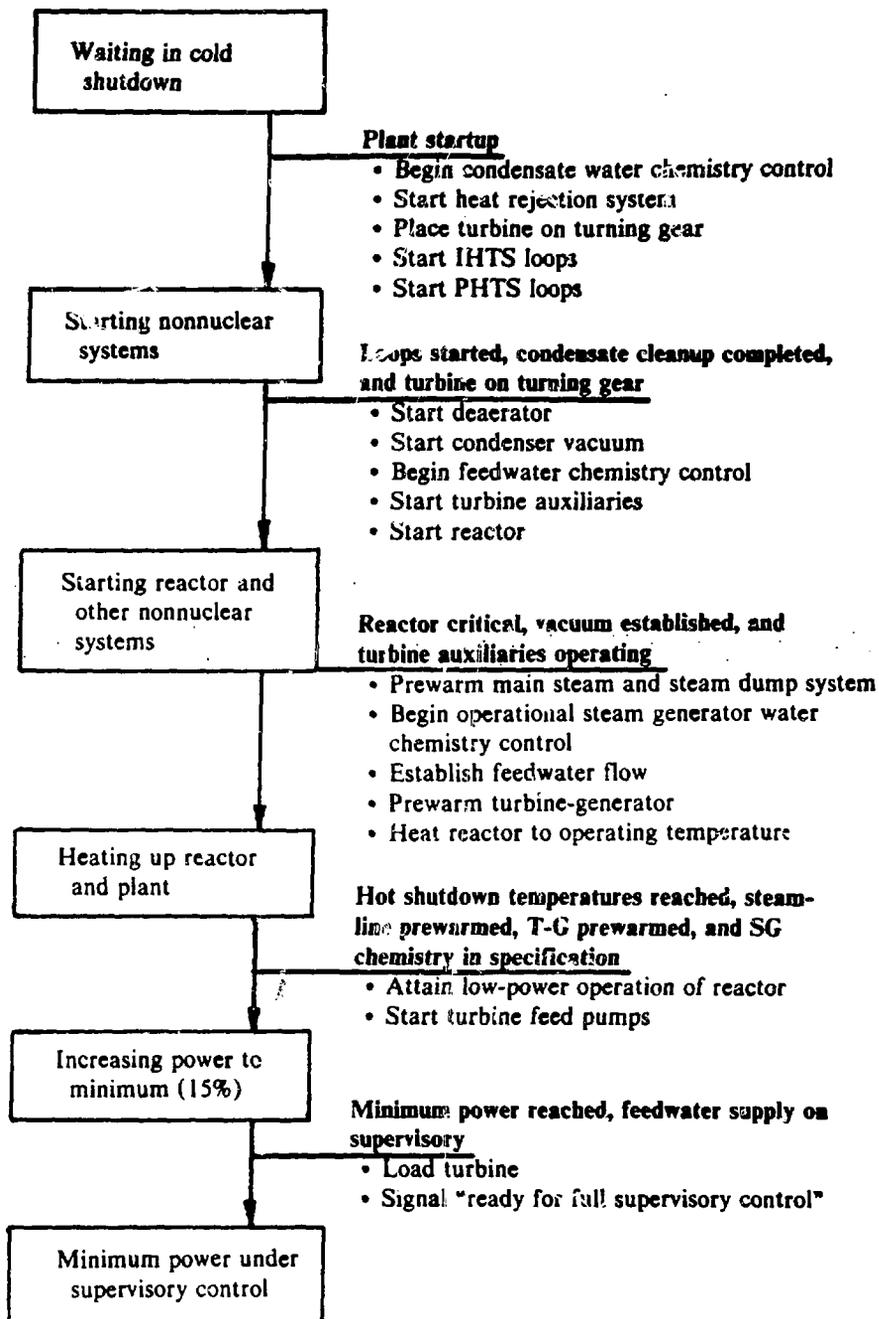


Fig. 9. State transitions with initial state "waiting in cold shutdown" and final state "minimum power under supervisory control."

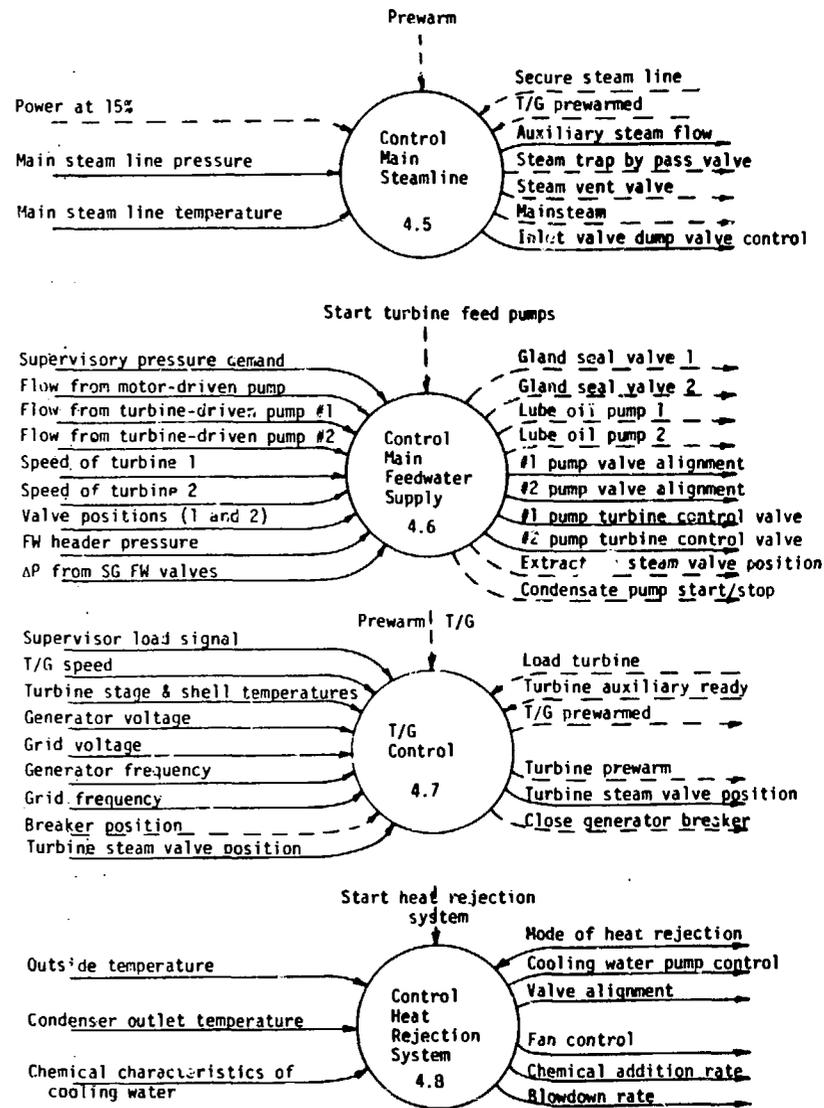
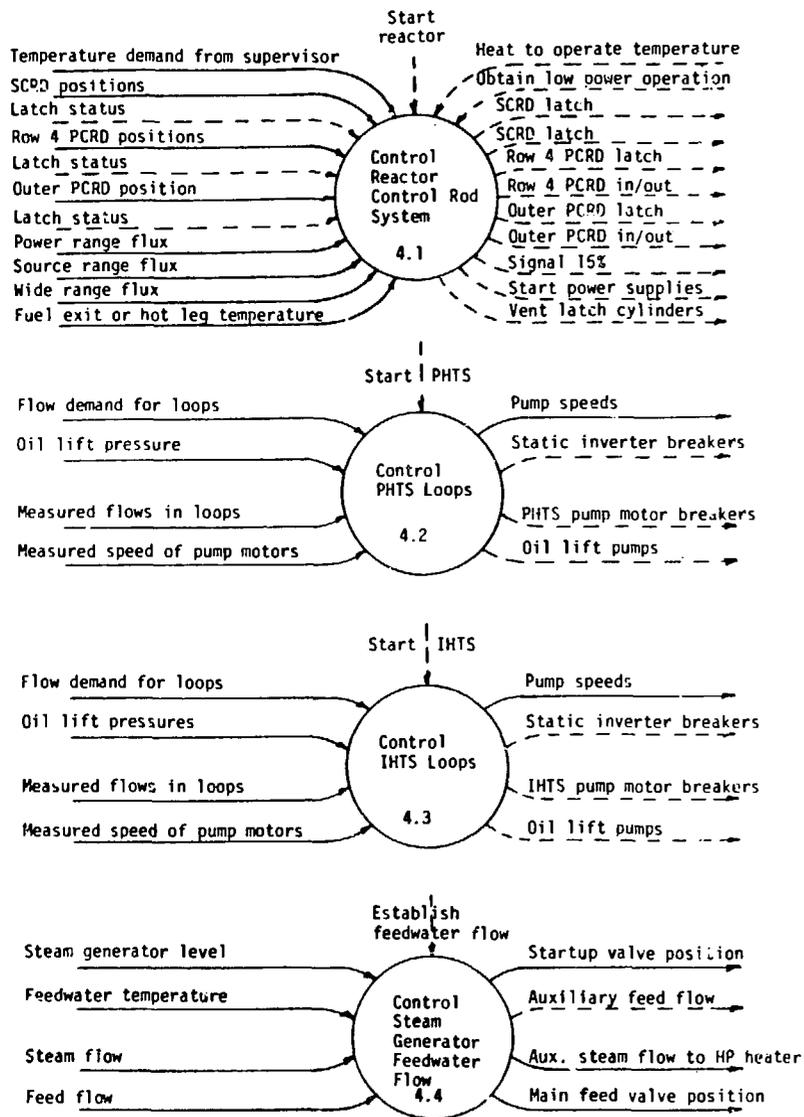


Fig. 10. Prime control packages which are the inner details of top-level package 4.0.

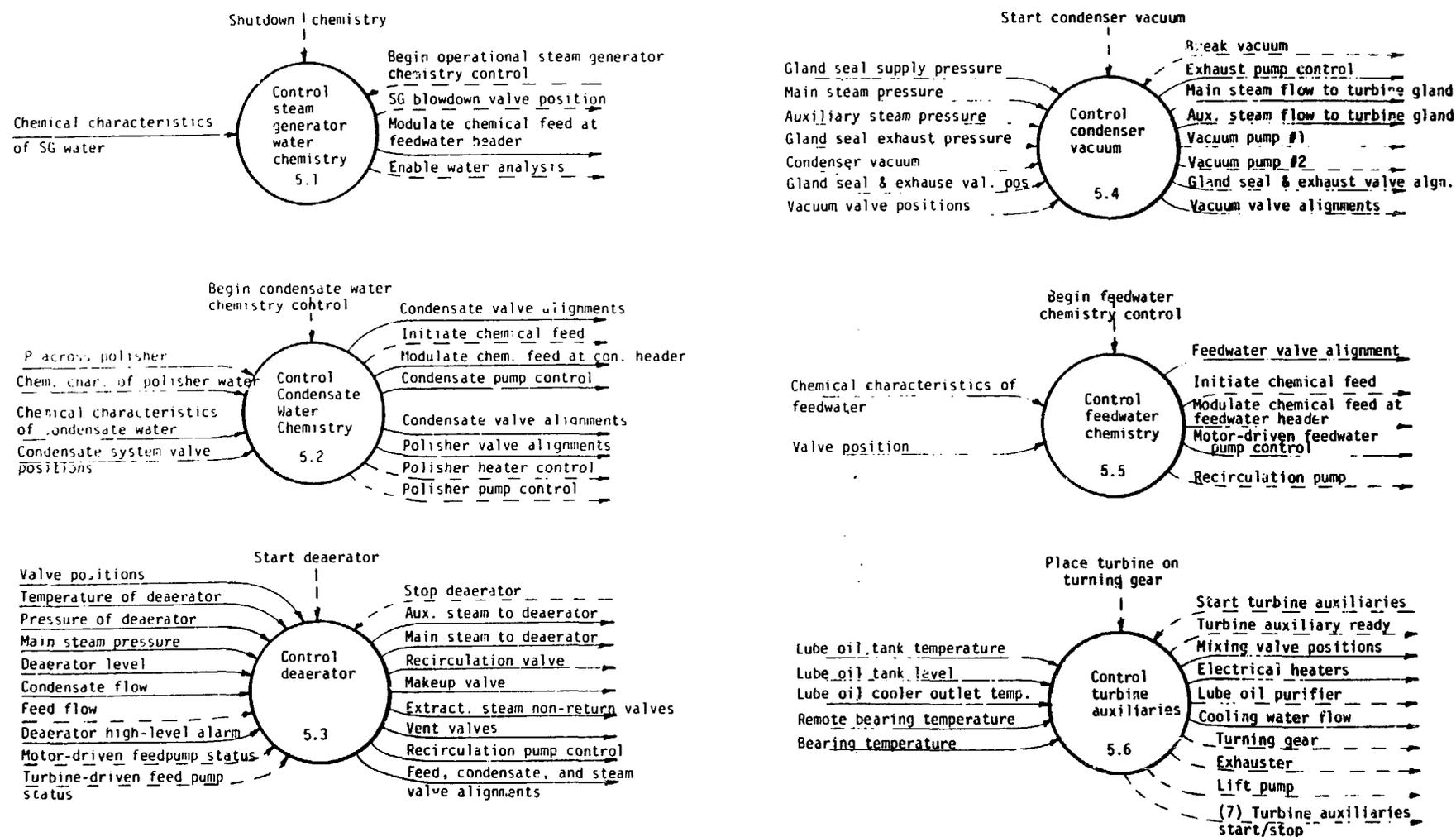


Fig. 11. Support control packages which are the inner details of top-level package 5.0.