DOE/ER/75781--T2

DEVELOPMENT OF ADVANCED DIRECT PERCEPTION DISPLAYS FOR NUCLEAR POWER PLANTS TO ENHANCE MONITORING, CONTROL AND FAULT MANAGEMENT

DE-FG02-92ER75781

B. G. Jones
S. Shaheen
Department of Nuclear Engineering
University of Illinois at Urbana-Champaign

N. Moray
D.V.Reising
P. M. Sanderson
Department of Mechanical and Industrial Engineering
University of Illinois at Urbana-Champaign

J. Rasmussen
HURECON, Denmark

SUMMARY

Traditional Single-Sensor-Single Indicator (SSSI) displays are poorly matched to the cognitive abilities of operators, especially for large and complex systems. It is difficult for operators to monitor very large arrays of displays and controls, and to integrate the information displayed therein. In addition, standard operating procedures (SOPs) are bulky (running to many hundreds of pages) and difficult to use, and operators may become lost. For these reasons, and also because it is becoming increasingly difficult to find replacements for aging hardware components, there is a trend towards computerized graphical interfaces for nuclear power plants (NPPs). There is, however, little rational theory for display design in this domain.

This report describes some recent theoretical developments and shows how to develop displays which will greatly reduce the cognitive load on the operator and allow the use of perceptual rather than cognitive mechanisms while using SOPs and to support state diagnosis and fault management. The report outlines the conceptual framework within which such a new approach could be developed, and provides an example of how the operating procedures for the start-up sequence of a NPP could be realized. A detailed description of a set of displays for a graphical interface for the SOPs of the feedwater system is provided as an example of how the proposed approach could be realized, and a general account of how it would fit into the overall start-up sequence is given.

Examples of "direct perception" or "ecological" configural state space displays to support the use of the proposed direct manipulation SOP interface are provided, and also a critical discussion which identifies some difficulties which may be anticipated should the general approach herein advocated be adopted.

Full details of the development of the displays, their graphical content, underlying theory, and notes on evaluation are provided in Appendices to the main report.

INDEX

FIGURES

Figures in Appendices are not indexed. They include a complete set of displays for Feedwater System start-up.

1.0 INTRODUCTION

In a recent report Moray et al. summarized our point of departure as follows:

> "Information about plant state is always constrained by the design of the human-machine interface, and the quality of such information in turn constrains the ways in which operators can think about problems. For example, some displays may require a painstaking synthesis of data derived from several or many separate gauges and displays, while others provide a direct perception of quite subtle plant states (Rasmussen and Vicente, 1989). Recent work in cognitive psychology suggests that displays of the latter kind should better support decision and diagnosis of plant state by the operator.
>
> The traditional control room display is a Single-Sensor-Single-Indicator display. There are almost as many independent displays as there are points at which system variables are measured, and operators must rely on their ability to perform complex cognitive operations to relate information from different sources to each other and thus to build up an understanding of the overall state of the system. This is particularly difficult when the system is in an abnormal state or when it is rapidly changing state.
>
> It is now widely agreed that displays should, as far as possible, avoid forcing operators to work at this "knowledge-based" (Rasmussen, 1986) level of operation where humans are slow and prone to error. With this in mind some alternative displays have already been proposed for NPPs. For example, the multivariate "star" display is well known (Coekin, 1969; Goodstein, 1981; Woods, Wise and Hanes, 1982), and a pressure-temperature plot (PT) is already in use in some BWRs to facilitate understanding of NPP thermal hydraulics (USNRC, 1988). An even more strongly integrated type of display which represents the Rankine cycle parameters in an animated graphical form has been suggested by Beltracchi, (1987)." (Moray, Jones, Rasmussen, Lee, Vicente, Brock and Djemil, 1993.)

In that report Moray et al. described experiments on Beltracchi's Rankine cycle display, in which the information from 35 analog meters was integrated into an

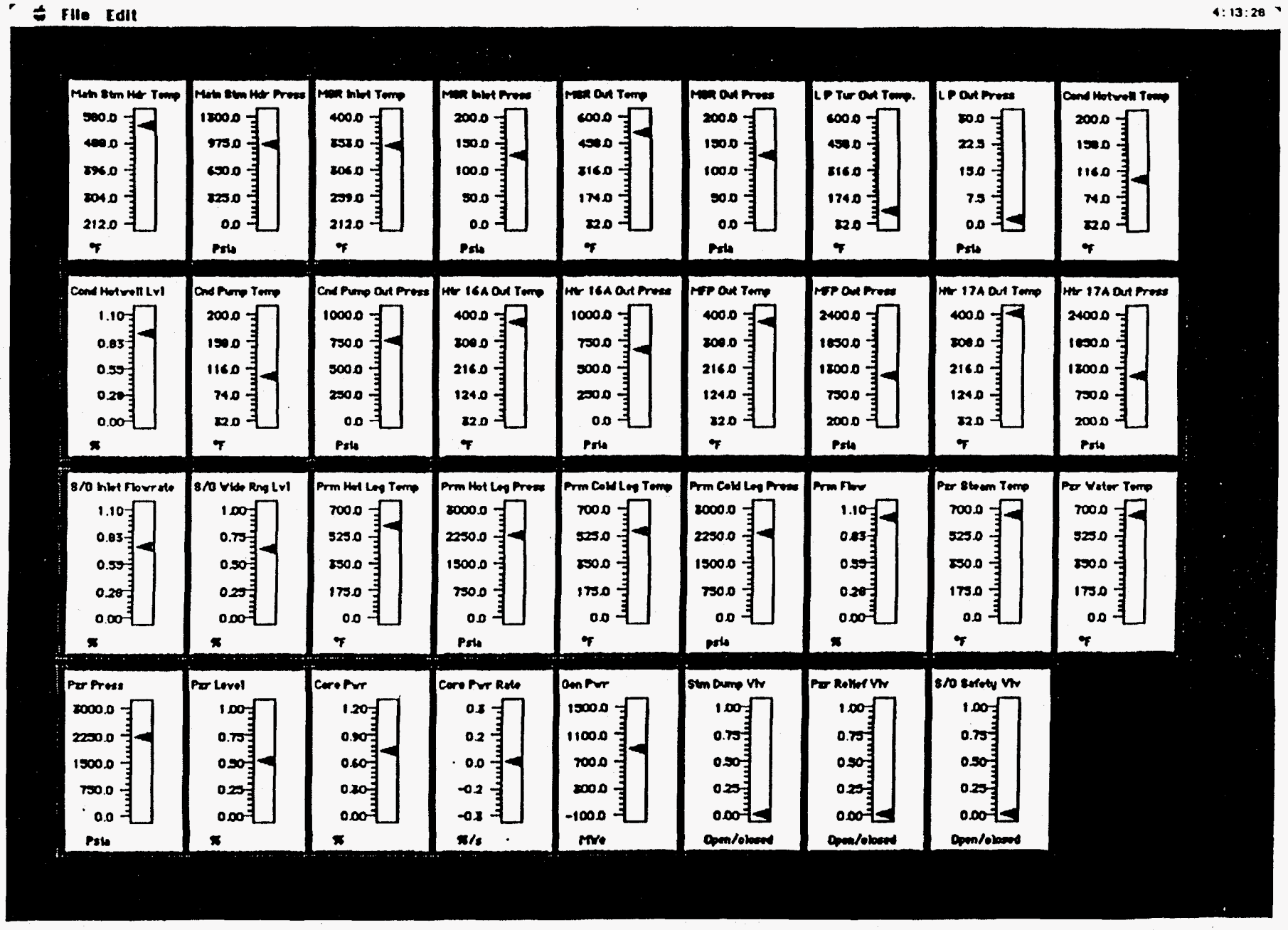


Figure 1: The simulated Analog Display evaluated by Moray et al (1993).

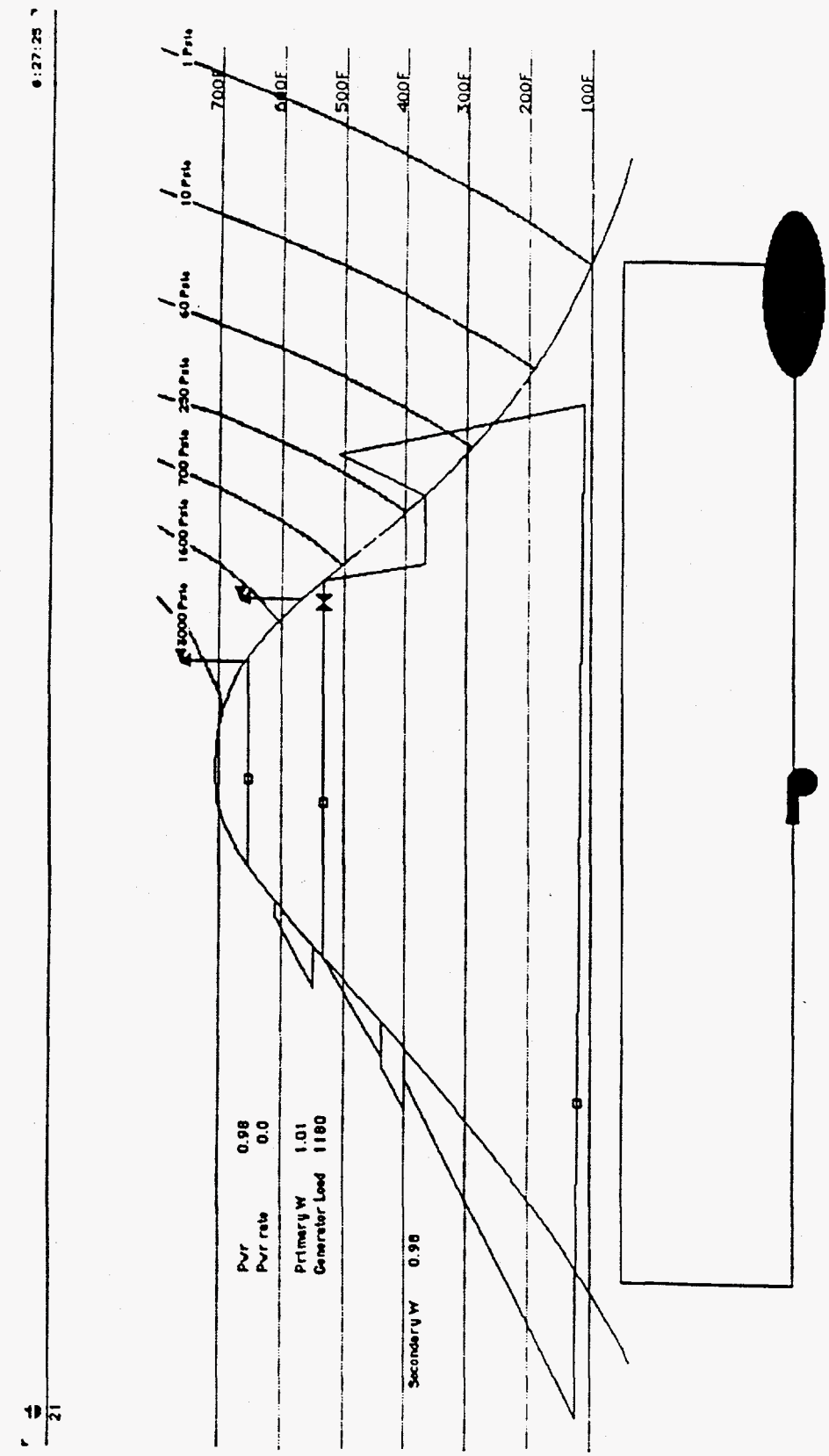


Figure 2: The Rankine Cycle Display evaluated by Moray et al (1993).

animated Rankine cycle diagram. Despite the fact that the display was unfamiliar to operators, nuclear power plant (NPP) operators showed an improvement of almost 30% in diagnosing transients using the Rankine display compared with the simulated analog displays. The two kinds of displays are shown in Figures 1 and 2 . In addition this approach has been investigated by Lindsay and Staffon (1988) (see also Rasmussen, Pejtersen and Goodstein (1994)) who have shown how the Rankine cycle can be made part of a display which includes other aspects of the mass-energy balance of a nuclear reactor. Rasmussen et al. (1994) discuss the properties of these displays in the general context of human-machine engineering design.

The traditional Single-Sensor-Single Indicator (SSSI) display is poorly matched to the cognitive abilities of operators, especially for large and complex systems. As stated above, there is now increasing evidence that such "integrated", "direct perception", and "direct manipulation" displays can provide a very powerful method of reducing mental workload and supporting diagnosis. An "integrated display is one where the values of several SSSI inputs are shown in a single display in such a way as to show their mutual inter-relations. "Direct perception" displays and "ecological" displays allow operators to perceive the locus of the plant in state space, without the need to perform complex calculations, steam table look-ups, etc., substituting pictorial displays for numerical displays. "Direct manipulation" interfaces provide displays containing icons representing controls, which, when manipulated by means of a cursor, mouse, or other input device directly act on the actual physical components represented by the icons, by means of the computer-plant hardware interface.

Our research aims to provide direct perception displays representing the plant configural state space which will greatly reduce the cognitive load on the operator and allow the use of perceptual rather than cognitive mechanisms to support state diagnosis and fault management. We believe that in addition to providing a more direct perception of plant state, the use of carefully designed graphical displays can play an important role in supporting the correct use of operating procedures. Instead of the enormous burden which text-based SOPs imposes on the operators, we believe that a well-designed direct manipulation graphical interface can allow the operator to navigate through a sequence of operations with a greatly reduced attention load, and a much reduced probability of misreading or misinterpreting

written SOPs, and of losing place during the navigation through the many tens or hundreds of pages required.

Further, the development of such a set of displays will support not only improved control rooms for NPPs, but will have relevance to all large and complex industrial systems, and will, in so far as these displays offer improved operator support, reduce human error and its consequences, lead to better fault management and hence greater safety, and also to greater productivity by increasing the efficiency of normal operation. The work is thus relevant to power generation, the management of chemical plants, nuclear waste processing, and the management of all large industrial systems, whether hazardous or not.

2.0 A PHILOSOPHY OF DISPLAY DESIGN.

The availability of powerful workstations which support elaborate graphics allows us almost unlimited freedom to develop new displays. As stated above, our philosophy is to integrate the information from SSSI sources so as to provide a coherent picture of system state, one which does not require the operator to perform elaborate cognitive operations on the data to determine what state the plant is in. Rather than displaying SSSI information, we wish to provide a display which directly reveals the locus of the plant in state space. The operator should be able to perceive directly displayed on the screen even the most deep and complex relationships among variables. Furthermore, where the operator must perform an elaborate sequence of operations over a period of minutes or hours, involving the manipulation and monitoring of many variables, the form of the display should lead the operators through the sequence without the need for them to consult complex written operating procedures.

An obvious example of such a sequence is the start-up sequence from cold shut-down of a NPP. In this case hundreds of variables must be controlled and monitored over many hours. Control actions must be taken at appropriate moments, and the plant must be monitored at all times to ensure that critical variables follow an appropriate trajectory towards the normal operating state, and above all that the values of the variables do not approach boundaries which are associated with hazardous plant states. The written SOPs for startup run to several

hundred pages, and require the operator to move backwards and forwards through different sections. The manuals do not in themselves provide a checklist facility for tracking progress, nor do they embody alarms, or indications that steps have been omitted, performed in the wrong order, or at the wrong time, or that in appropriate actions have been performed.

2.1 SOPs as a grammar of correct behavior.

Using the power provided by computerized control rooms, we can conceive a SOP design which is embodied in the plant interface. In a certain sense we can think of the entire sequence of operation as resembling a sentence, not of words but of behavior. Speaking grammatically requires one to choose words in a correct sequence according to rules, so that the sequence of spoken words results in the emission of a sentence which can be understood by a listener. Similarly the performance of any long sequence of actions, in a correct sequence governed by rules, results in the emission of a series of commands which can be understood by a plant of which the architecture embodies the same rules. SOPs are a way of ensuring correct rule-governed sequences of behavior.

Any large industrial plant is composed of a large number of quasi-independent sub-systems. Thus in an NPP we have the core, with the subsystems for controlling the position of rods and boron concentration; the feedwater sub-system; the steam-generating subsystem, the turbine sub-system, etc.. Each of these subsystems can be thought of as a "paragraph", within which we can represent required behavior as "sentences", the whole comprising the "document" which describes the passage from cold shut-down to full-power operation. We propose that a graphical interface should enforce the correct sequence of behaviors, prevent incorrect sequences, and provide constant feedback as to the state of the plant, and the location of the operator actions in the overall start-up sequence. (More generally, we believe that such an approach can support normal operations and recovery from fault conditions, but, as we shall see, there are difficult problems which have not yet been investigated in extending the proposed approach to fault management.)

2.2 The start-up sequence as the construction of the plant.

A start-up sequence can be thought of as equivalent to the construction of a plant from its components. A plant consists of many thousands of individual components , each of which is part of a larger component, or of a subsystem. Each group of subsystems makes up a large subsystem, and in the end the most complex subsystems make up the plant. During start-up operators bring components to states of readiness, by switching them on, providing power, pre-heating them, bringing them up to speed, etc. Once the components of a subsystem have been appropriately configured, we believe that in general the operators no longer think of the components, but of the subsystem as a single unit. Thus after closing a circuit breaker, operating a switch, and checking lubricating oil pressure and speed of rotation, an operator no longer thinks of those as individual parts or variables, but rather of "pump #123" as a single entity. A group of pumps which have been all brought up to operating condition is thought of as "feedwater system #3", and so on. And as the process of start-up continues, the operators' level of attention should switch appropriately, so that where details are no longer needed, attention is not given to details, but to the global properties of the system as a whole. The displays in a graphical direct manipulation interface should support the shift of thought between levels of abstraction and synthesis as they occur.

If, as Rasmussen et al. (1994) have suggested, the start-up sequence can be thought of as constructing the plant from its components, then the level at which operators think about the plant becomes progressively more global and more abstract. In fact operators at the same time, in a sense, both construct the plant and climb the "abstraction hierarchy" from the point of view of cognition (Rasmussen, 1986; Rasmussen et al., 1994). Usually SOPs do not support this economy of intellectual effort and this change of strategies, but given the power of computer graphic interfaces, we believe that it can be done, and at the same time will better support cognitive decision making by operators.

The process of start-up can be represented as in Figure 3, by a "bird's foot" lattice (Moray, Jones, Sanderson, Reising and Shaheen, 1995). We propose the name from the obvious resemblance of the parts of the diagram to the feet, ankle and legs of a bird, with the structure being repeated at each level of abstraction.

At the bottom of the diagram is a row of "toes", each of which corresponds to a single very simple component of the plant ("Parts"). In the process of starting up the plant these are "aggregated" into sub-systems , by selecting and connecting them, either physically or functionally. Each "ankle" thus represents the fact that a subsystem has been configured, and is beginning to run up towards its set point status as a result of the "start" procedure ("Processes"). When several such processes

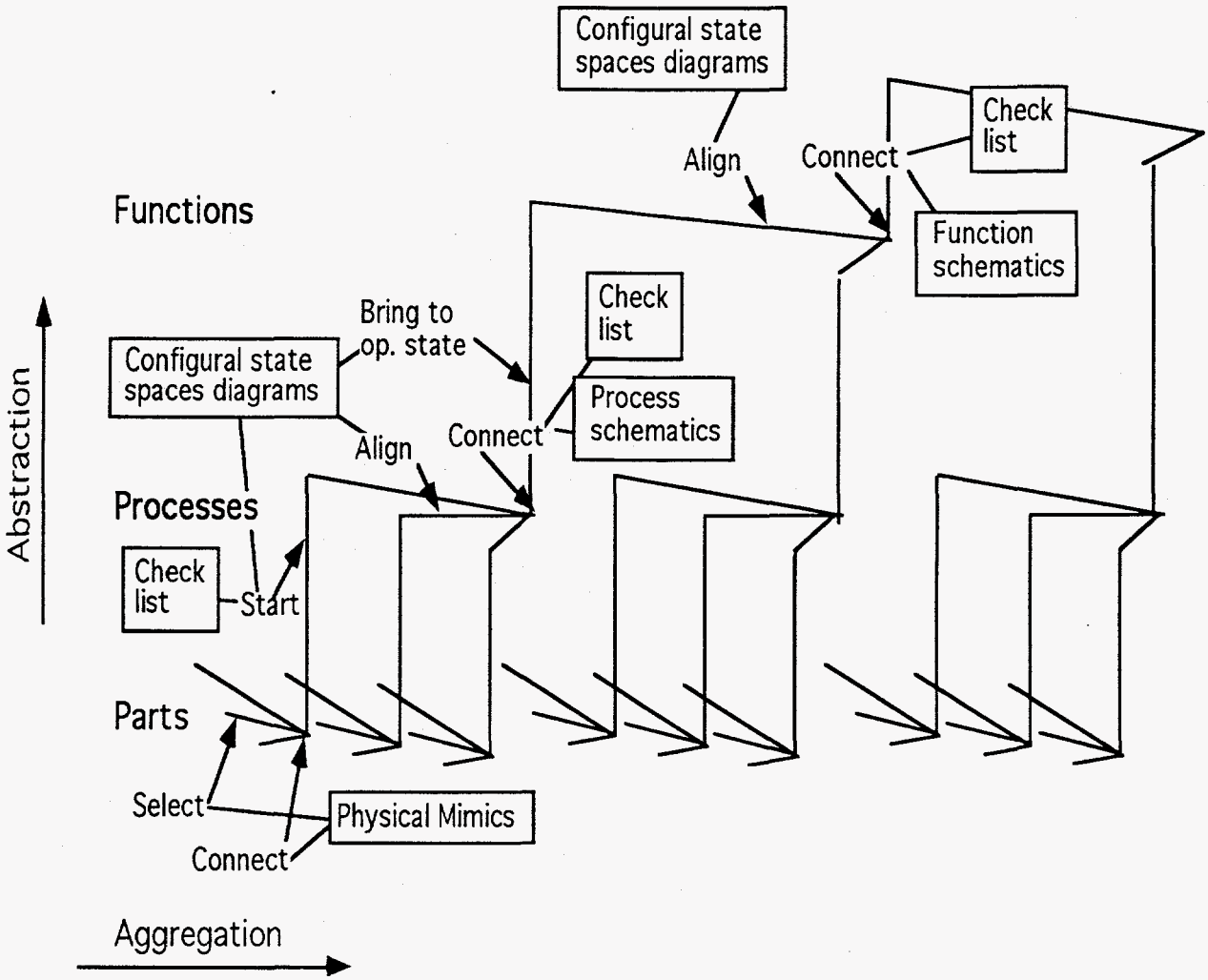


Figure 3. Bird's Foot Graphical Interface

are running, and when a check list has been used to ensure that all is normal, they must be "aligned" each with the other (to ensure synchronization, mass/energy balance, etc.). These are now the "toes" of a higher level synthesis, and the process proceeds up and to the right towards the fully synthesized and fully function normal operating conditions.

2.3 Supporting knowledge of plant state

The discussion so far has been concerned with displays which support SOPs from the point of view of operator *actions*, But as well as controlling the plant, it is essential that operators *monitor* the plant state. While minor divergences from set points, and from the trajectories between critical states, can be tolerated, variables must never be allowed to approach values which endanger the plant, or which represent values forbidden by licensed operating conditions. How best may knowledge of plant state be supported? In Figure 3 we see several boxes with labels such as "physical mimics", "configural state space diagrams", and "process schematics" and "function schematics". These represent different kinds of graphical displays, at different levels of an abstraction hierarchy (Rasmussen, 1986), supporting different modes of thought by the operator, and relevant to different levels of aggregation and integration of system components.

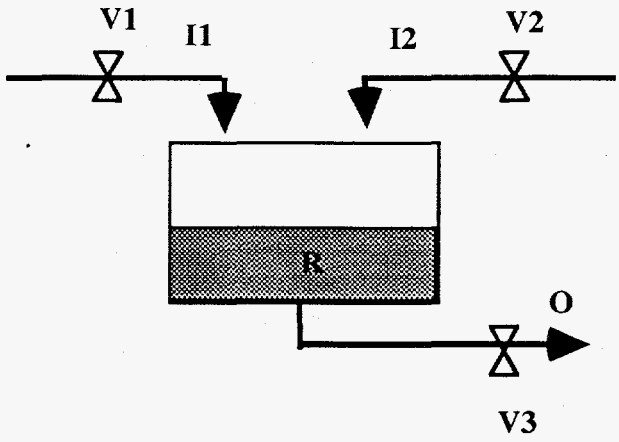
As noted earlier, recent years have seen the development of a new approach to display philosophy, including "ecological" displays, and "direct perception: displays", or more generally "integrated" displays. The essence of all these approaches is to avoid providing massive amounts of *data*, and provide instead relatively small amounts of integrated *information*. The aim is to allow operators to use their powerful perceptual abilities to interpret visually integrated information about plant state, instead of relying on their relatively weak reasoning ability to deduce the meaning of the relation between a large set of quantitative values. It is for that reason that the Rankine cycle display was developed and evaluated (Beltracchi, 1987; Lindsay and Staffon, 1988; Moray et al. 1993; Vicente et al., 1996).

For example, operators should not have to calculate rates of change: they should be able to *see* them directly as graphical trend displays. They should not have to deduce the value s of variables whose values depend on the concurrent values of several other variables: the results of the calculations, not the raw data, should be displayed. In the context of the graphical SOPs to be advocated in this report, one should supply integrated displays which provide as direct a view as possible of the state of the plant to support the use of the SOPs. Thus the time to assess the plant state is minimized, any tendency to approach hazardous conditions can be seen

before the boundary is reached, and the maximum efficiency of interpreting plant data is provided for the operators.

In general, we should use integrated, rather than SSSI displays. But integration is not by itself sufficient, and there is a serious question as to how far such integration should go and how its results should be displayed. Kelley (1968) pointed out many years ago that as one integrates more and more information one may provide higher and higher orders of integrated or differentiated information, but at the same time lose contact with the absolute values of the state variables. Several recent discussions have shown that it is far from simple to choose an appropriate level of integration (Sanderson, Flach, Buttigieg, and Casey, 1989). Recently Flach and Bennett (1992) have provided an elegant summary of the problem. Figure 4, taken from their paper, shows a simple hydraulic system. The goals of the operators are to maintain a specified level in the reservoir and to maintain a specified flow rate through the system by manipulating the valves. Figure 4 lists the variables and the constraints among them which together define the system. What is the best way to display them to the operator?

Figure 5, also from Flach and Bennett (op. cit.), shows a variety of possible encodings (displays) of information about the variables and the constraints. Some of them support integrated knowledge, some of them detailed knowledge. The variables listed under P are those which can be directly perceived in the display, while those under D have to be derived by the observer. The £ sign refers to the logical relations which define the system, and ¶ to the physical layout and construction of the system. To develop a complete system of direct perceptual displays for a complex system such as a NPP we must make appropriate choices for the variables which will be displayed, and then design an appropriate graphical representation of their values and relations. In Figure 5 we see a progression from a classical SSSI with no constraint information shown (Figure 5A), through a typical mimic diagram (Figure 5C), an "ecological" representation (to use the language of Vicente and Rasmussen, 1992) in Figure 5D, to a completely, but too greatly integrated display in which no details are available at all (Figure 5E). Note also how for different displays different aspects of the information are either directly represented physically (P) in the display or must be deduced (D) from the displayed data. It is critical to find the appropriate level which will combine the best of detail and integration. Indeed Moray et al.



Low Level Data (Process variables)	**High Level Properties (Process constraints)**
T = Time	K1 = I1 / V1 Relations between
V1 = Setting for Valve 1	K2 = I2 / V2 commanded flow (V)
V2 = Setting for Valve 2	and
V3 = Setting for Valve 3	K3 = O / V3 actual flow (I or O).
I1 = Flow through Valve 1	
I2 = Flow through Valve 2	
O = Flow through Valve 3	K4 = ΔR / (I1 + I2) Relations between reservoir volume (R), mass input (I1 + I2) and mass output (O).
G1 = Volume goal	K5 = R / G1 Relations between (R,O) states
G2 = Output goal (demand)	K6 = O / G2 and goal states (G1,G2).

Figure 4. A simple dynamic system and the information to be encoded in displays. What is the best way to represent the values of variables and the system constraints? (From Flach and Bennett, 1992.)

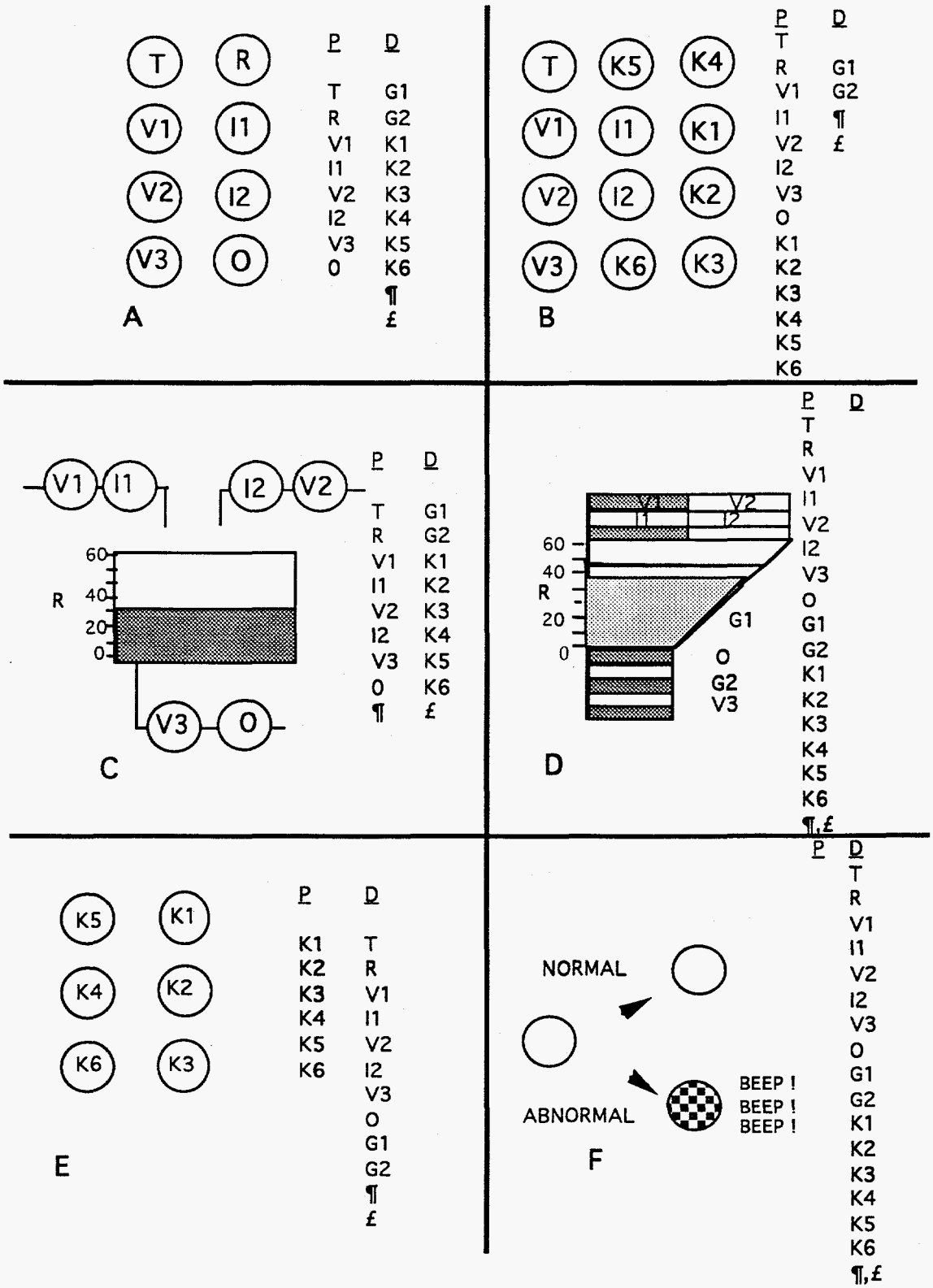


Figure 5. Various ways of displaying data as information (Flach and Bennett, 1992). The values of variables in columns labelled P can be directly perceived in the display. The values of variables in columns labelled D must be directly derived by calculation from data in the display.

(1993) found evidence that the Rankine cycle display would probably need to be supplemented by more detailed displays, since while overall diagnosis was well supported by the animated Rankine diagram, operators were unable to remember specific values of variables. (See also Vicente, Moray, Lee, Rasmussen, Jones, Brock, and Djemil, 1996.)

The aim is therefore to develop a suite of displays which will best support both global perception of system state, and at the same time allow operators access to detailed information when the latter is required, in order to support the graphical SOP interface which will guide the operators through the start-up procedures. Two classes of displays will be required,

1. An overview of the entire plant to allow the operators to navigate through the data space,
2. A series of integrated displays to deal with particular problems.

3.0 GRAPHICAL SOPs: THE "BIRD'S FOOT" DIAGRAMS

3.1 A graphical representation of the SOP sequence for start-up

We propose an integrated graphical interface as a substitute for written operating procedures during normal and abnormal operations. Operators see a progressively integrated and abstract representation of the plant as they configure the plant for normal operating, but the system preserves information about a route back to detailed subsystem operation in order to support fault management. The amount of detail displayed is always appropriate to the level of the current task, and the display knows the causal path to the relevant controls for both normal and abnormal operation. The suite of graphical direct manipulation displays developed here is an instantiation of the bird's foot lattice shown in Figure 3, specialized for the Feedwater Subsystem.

As stated earlier, the process of start-up of a nuclear power plant can be thought of as a process of "constructing" the operational state of the plant from its components. Written operating procedures are intended to guide operators through a process of starting sub-components and connecting them to make larger functional units. (For example, several individual "pumps" become a single "cooling unit".) These larger

components are then in turn interconnected to make components at a still higher level. The operator should progressively think in terms of more integrated but more abstract components as the process proceeds, but as presently written the level of detail in operating procedures does not support this change in level of cognitive activity.

SOP manuals usually consist of two kinds of information. The first is the set of written instructions to operators. These may include indications of set points, limits at which decisions must be made, values of variables at which switches should be thrown to activate new components, warnings, notices, alarm levels, etc.. The second is a series of flow charts which summarize the sequence of operations to be performed, with the steps numbered in sequence. Examples of both of these are shown in Figures 6 and 7.

To develop the behavioral sequential grammar as a bird's foot diagram, we note that the flow charts can be re-drawn in such a way as to support a hierarchical representation of the task. Certain groupings of numbered steps refer to particular subsystems. The contents of operating procedures can be represented as a lattice in which the lowest branches are the names of the simplest components, and the top node is the completed plant running under normal conditions. This process can be represented graphically by a "bird's foot" diagram. An example is shown in Figure 8, where some parts of the feedwater system are indicated. The list of the simplest components of the plant is written along the bottom of the lattice, and as procedures are carried out components are aggregated into subsystems, moving from left to right across the lattice. When several "toes" are collectively active, the "ankle" represents a complete functional unit, and the operator can now think in terms of connecting that functional unit to other completed units and details of the sub-units can be ignored. This is a process of moving to a higher level of abstraction which reduces the mental load on the operator. At the lowest horizontal level we require mimics of the plant sub-components. At each successive higher level we require process schematics representing larger units, and this process is repeated until the whole plant is "synthesized".

Dynamic graphics switch between levels as each sub-unit is configured and reaches normal operating conditions. Checklists are presented at each "ankle" node of the

```
**************************************************
*                    CAUTION                     *
* THE STEAM DUMPS SHOULD NOT BE OPENED UNLESS    *
* STEAM HEADER PRESSURE IS GREATER THAN 50 PSIG, *
* AND THE STEAM HEADER IS COMPLETELY DRAINED.    *
**************************************************
```

F. 54. Steam Dump Preparation for Plant Startup:

a. VERIFY/OPEN 1MS003A thru M and 1MS005A through M, Manual Isolation Valves for Steam Dump Valves (426' Turb Bldg).

b. VERIFY/SET the Pressure Mode Controller for 1092 psig.

c. ENSURE Steam pressure is less than 1092 psig.

d. PLACE the Pressure Mode Controller in AUTO.

e. PLACE the Steam Bypass Mode Selector Switch to RESET, and then to STM PRESS position.

f. TURN both Steam Dump Interlock A & B Selector Switches to the ON position.

g. ENSURE the CNDSR NOT AVAILABLE C-9 bypass-permissive light is OFF.

h. ENSURE the LOSS OF TURBINE LOAD INTLK C-7 bypass-permissive light is OFF.

55. PLACE PZR Level Control in Automatic by performing the following:

a. ADJUST 1FCV-CV121, Chg Pump Dsch Flow Cont Vlv, in MANUAL to match PZR actual level with demanded level.

b. MAINTAIN PZR actual and demanded level equal for 10-15 minutes.

c. PLACE 1LK-459, Master PZR Level Controller, in MANUAL.

d. PLACE 1FCV-CV121, Chg Pump Dsch Flow Cont Vlv, in AUTO.

e. ADJUST 1LK-459, Master PZR Level Controller, to MAINTAIN 1FCV-CV121 Controller demand signal stable and to MAINTAIN PZR actual level equal with demanded level.

f. PLACE 1LK-459, Master PZR Level Controller, in AUTO.

g. ENSURE 1FCV-CV121, Chg Pump Dsch Flow Cont Vlv, demand signal remains stable while maintaining PZR Level at demanded level.

Figure 6: An example of the written SOP Instructions.

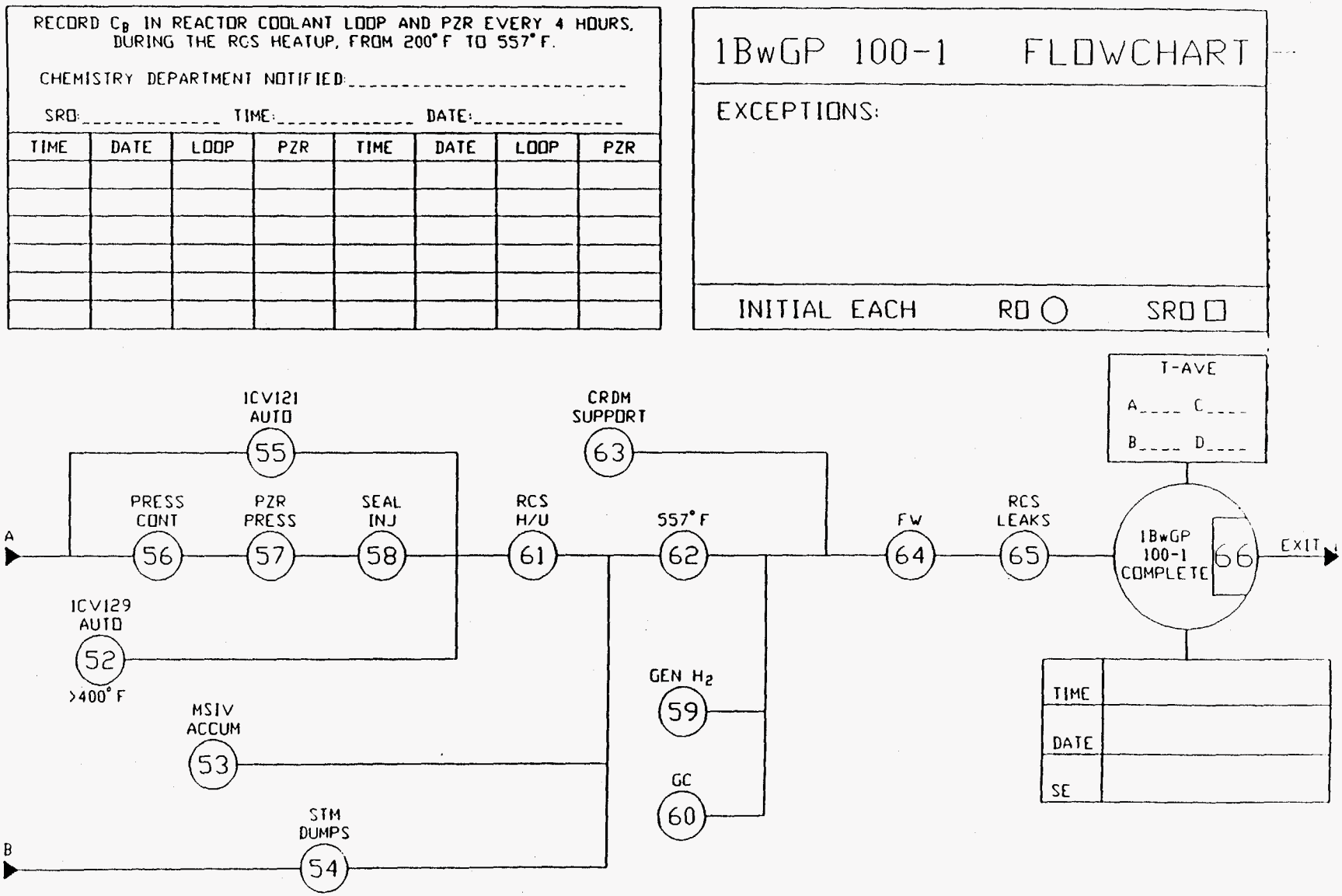


Figure 7: An example of the flow chart of the SOP instructions in Figure 6.

bird's-foot diagram. The convergence of "toes" represents the configuration of a higher functional unit from lower sub-units. The vertical lines represent

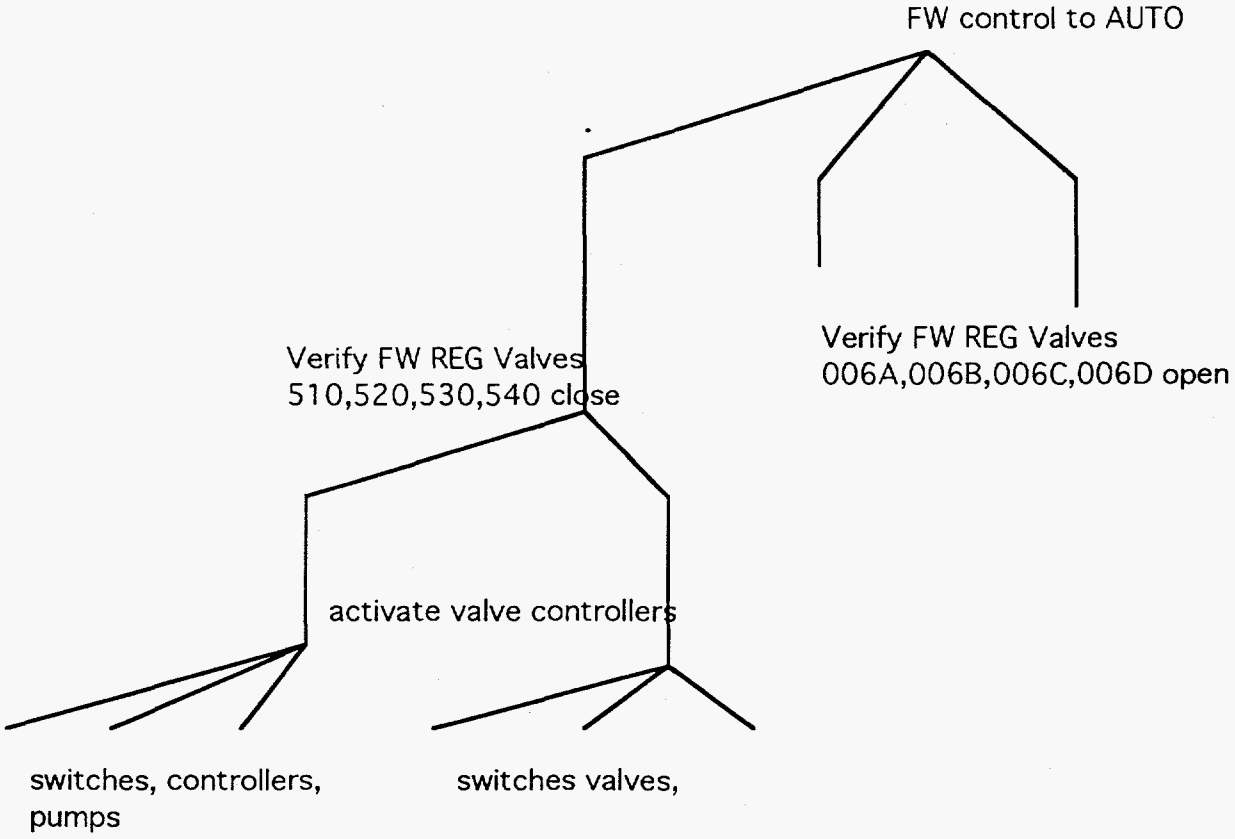


Figure 8. Bird's Foot Graphical Interface with some feedwater system components indicated.

a process running up to its normal operating conditions in a new functional unit. As an "ankle" is completed, the "toes" disappear, encouraging the operator to think at the next higher level of integration. Configural state space diagrams appear at each node showing constraints on the process , and the current location of the system with respect to those constraints, so that the operator can see how close the process is to the edge of the operating envelope, (for example how close to the designed pressure and temperature limits, how close to the regulatory limits, and how close to the failure of physical components).

The operator's task is to activate components and guide them to normal operating state by moving through the lattice, instead of having to read many pages of operating procedures. In a direct manipulation display actions on an icon on the screen result in changes in the object or process represented by that icon. Hence

moving a control on the screen by means of a mouse replaces the use of a manual switch on a traditional control panel. Fewer features remain on the display as the system moves upward in the abstraction space. The graphics also relate each node to a mimic of the relevant components so as to allow operators to use their expertise if unusual configurations are required to handle conditions not included in SOPs, thus coupling the intelligence of operators to the standard SOP and EOP designs. For example, if 2 out of 4 redundant pumps are required, and one does not start, the mimic diagram helps the operators to decide what steps to take to compensate, or work around, the problem. The lattice allows the system to retrace a path from current state to the components which are causally connected to that state so as to support manual intervention when required. A typical graphic, with a 9-toed bird's foot and four miniature configural state space or other diagrams is shown in Figure 9. By clicking on the miniature diagrams they can be expanded to fill the entire screen.

As a proof of principle we will describe a fairly complete prototype interface for a PWR feedwater system startup sequence.

3.2 Identifying the behavioral sequence.

In order to identify the required sequence of SOPs for the feedwater system, the designer performs a task analysis on the written procedures. The aim is to achieve the following:

- 3.2.1 Identify groups of numbered steps in the flow charts which comprise the different subsystem startup sequences.
- 3.2.2 Find the portions of the written SOPs which correspond to the numbered steps identified in 3.2.1.
- 3.2.3 Identify which SOPs which when completed correspond to the functional construction of an integrated subsystem.
- 3.2.4 Design a graphical layout in which each subsystem is composed from inputs represented as the "toes" of a bird's foot element, and in which if the actions are performed in the correct sequence from left to right at each level the complete sequence of subsystems will be synthesized and at their correct operating condition. Include access to "notes", warnings, checklists, etc. along vertical line from the ankle.

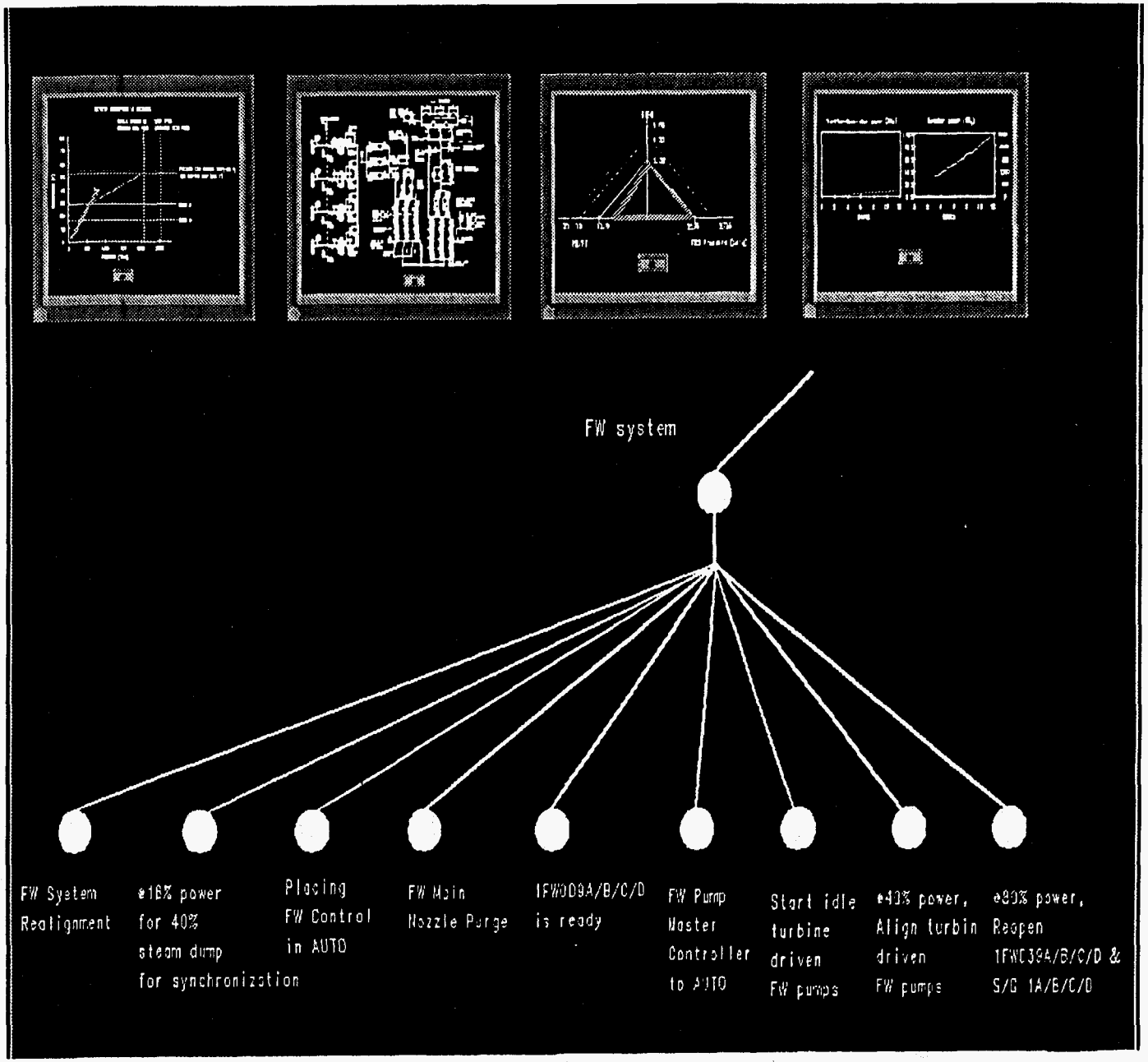


Figure 9: Main Feedwater Display.

- 3.2.5 Arrange the connections between those subsystems completed at a lower level to be the "toes" of the input at the next level, and arrange switching between pages so as to follow the sequence.
- 3.2.6 Connect the graphical interface to the plant hardware so that when the operator clicks on the appropriate icon switches will be thrown vales operated, etc.
- 3.2.7 Design integrated displays, mimics, configural state space diagrams, etc. showing the plant state, using "ecological" principles so that the operators can see how close the system is to desired set-points, constraint boundaries, alarm conditions, etc..
- 3.2.8 Connect input from plant sensors to the graphical interface to provide feedback to drive the plant state displays

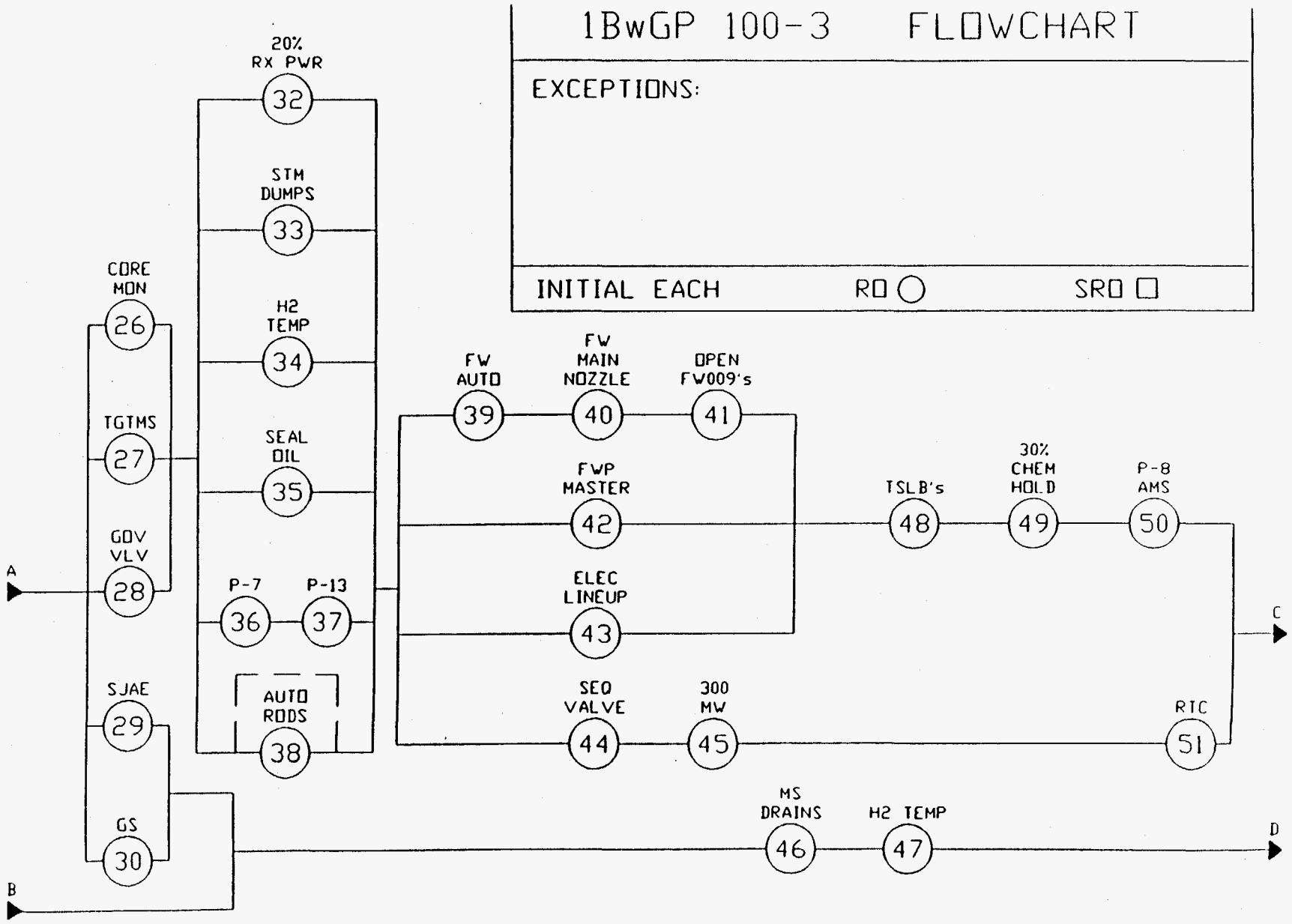
A detailed account of the theory, development and use of these displays is presented in Appendices A through D, taken from Shaheen (1996).

Figure 10 is one of the original flow charts, taken from a published SOP manual. Figure 11 shows the steps relevant to the feedwater system. Figure 12 shows the entire set of flowcharts converted into a hierarchical lattice. The "modes" represent major steps in the startup procedure, and are noted in the existing written SOPs. In Figure 12 the steps relevant to the feedwater system are indicated by underlining. The numbers refer to the steps indicated by the authors of the original SOP manual.

3.3 An example of how operators interact with the displays.

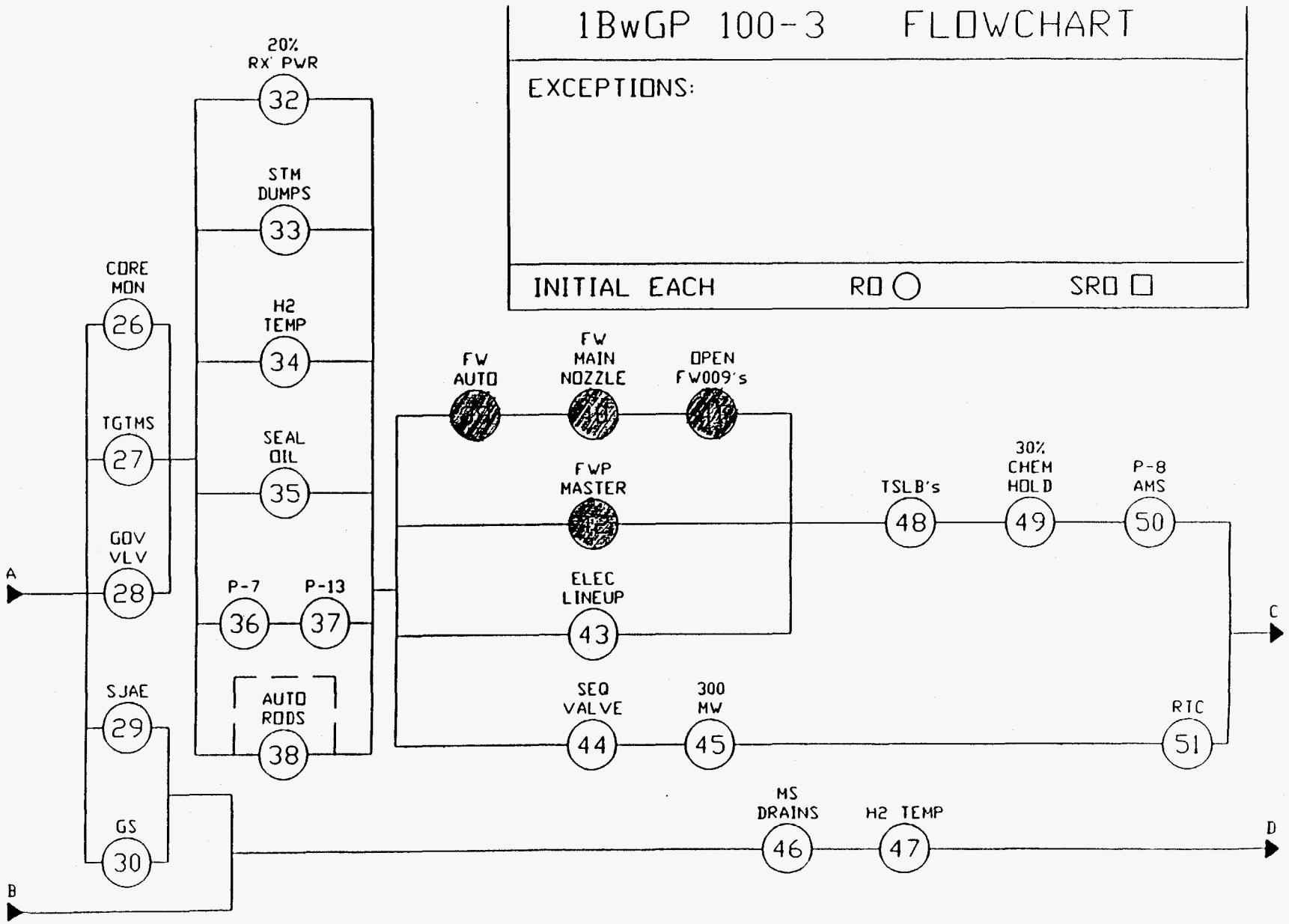
Consider Figure 13. Suppose that the operator has performed a number of steps, ending with "Verify All (or ave. flows) FW009s flow >= 120 gpm for 8 min." at toe #4, and has then clicked on the two "notes" and two "caution" icons, bringing up their screen content. The operator now clicks on the white node at toe #5, "Place C/S for 1FW009 valve to be opened in open position". The result is that Figure 14 appears. For English speakers, the natural tendency to read from left to right will reinforce training.

Using the mouse, the operator moves the control switch in Figure 14 from the "Close" to the "Open" position on any of the valves. The vertical line in the bar



-2-

Figure 10: A portion of the flow chart pertaining to the "Bird's Foot" Displays discussed.



-2-

Figure 11: A replication of Figure 10 with Feedwater Nodes indicated.

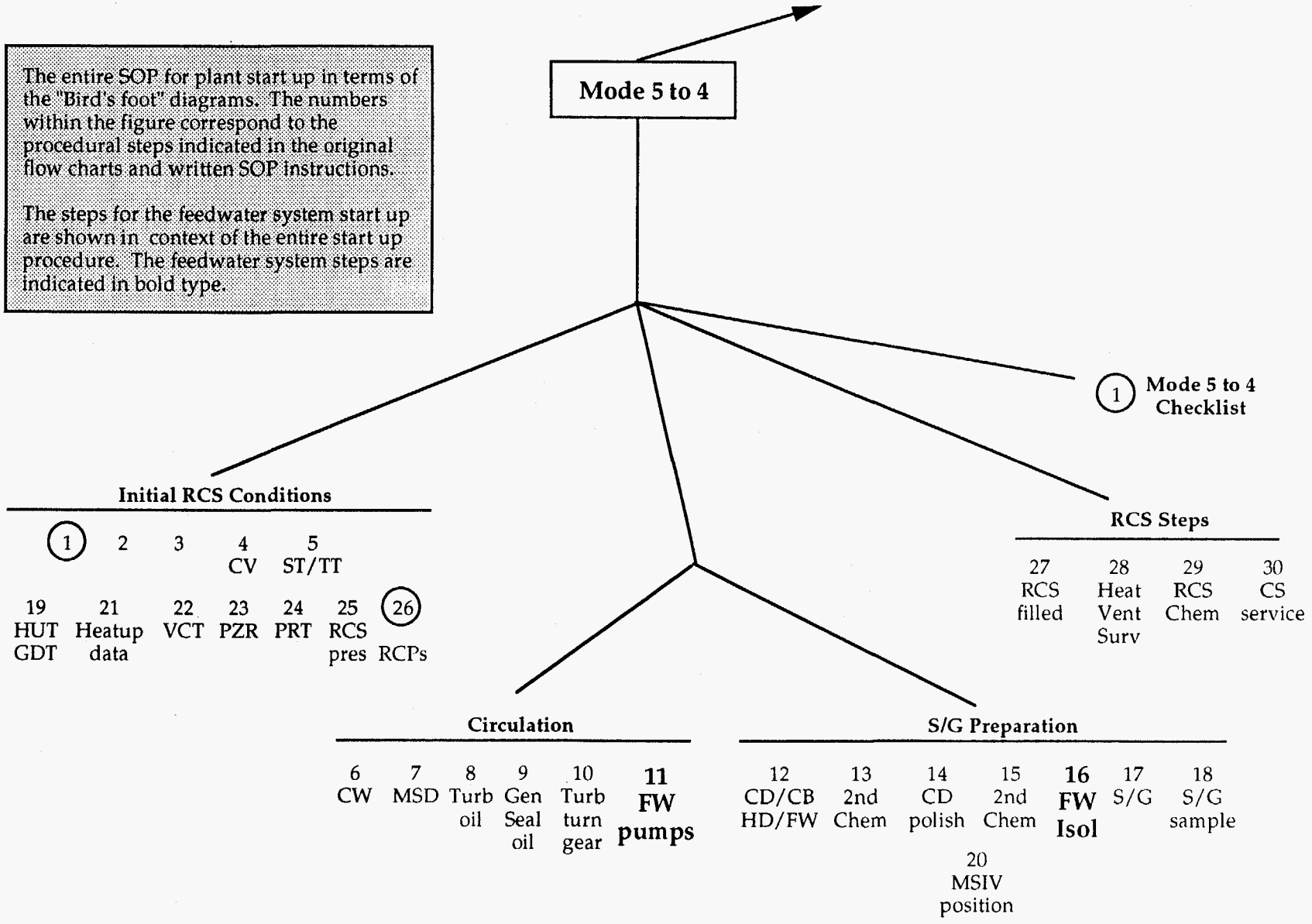


Figure 12 A: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

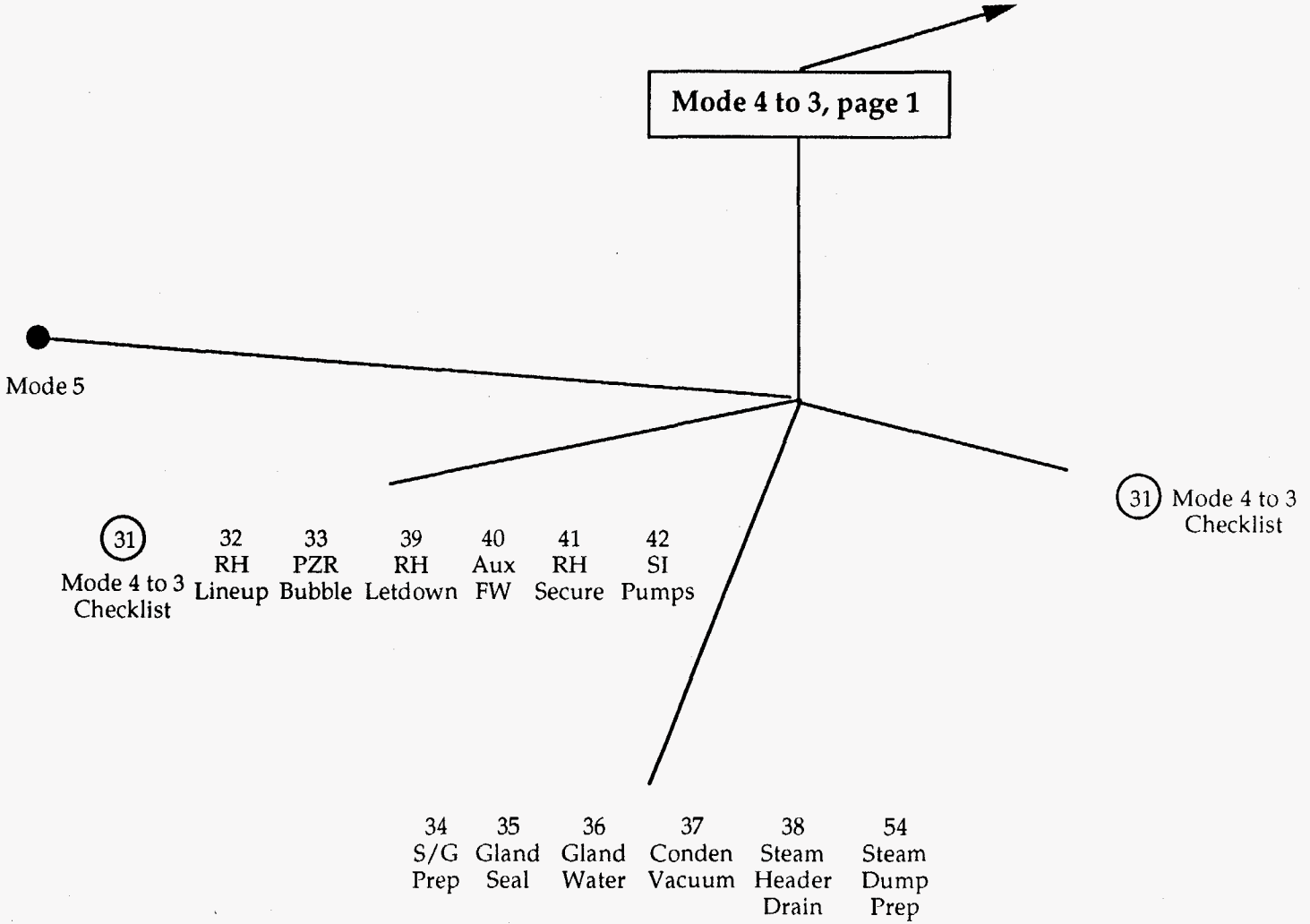


Figure 12 B: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

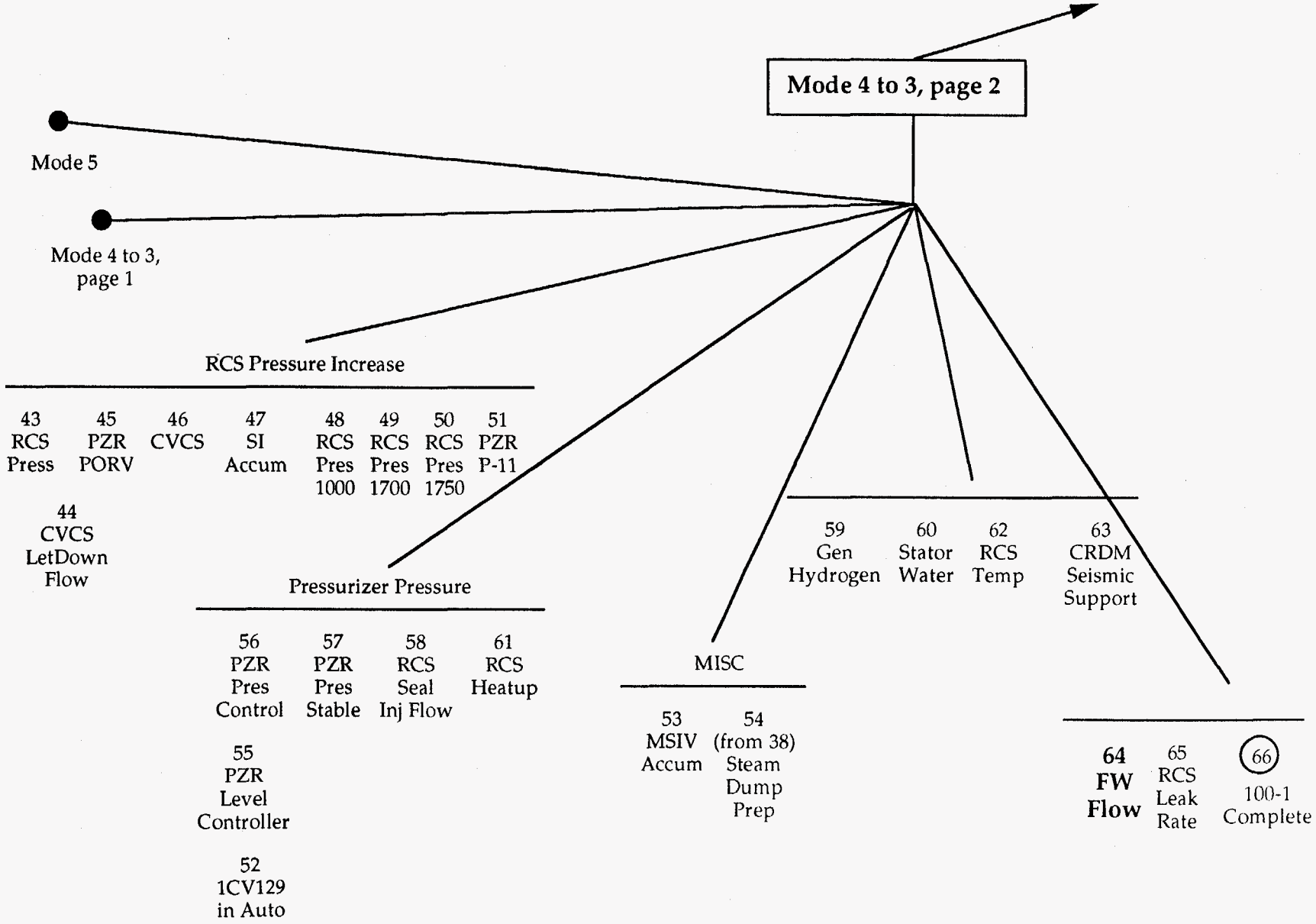


Figure 12 C: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

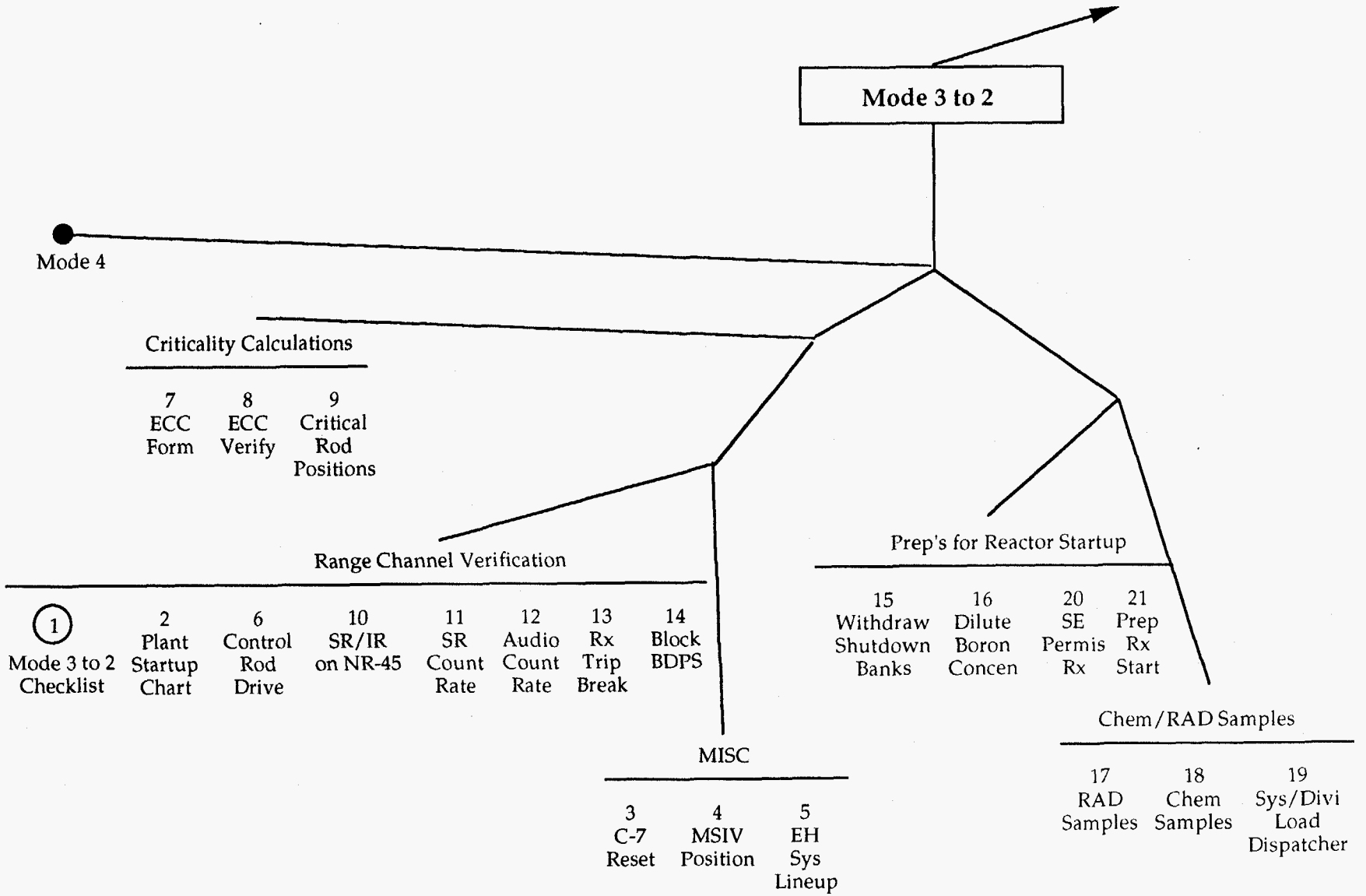


Figure 12 D: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

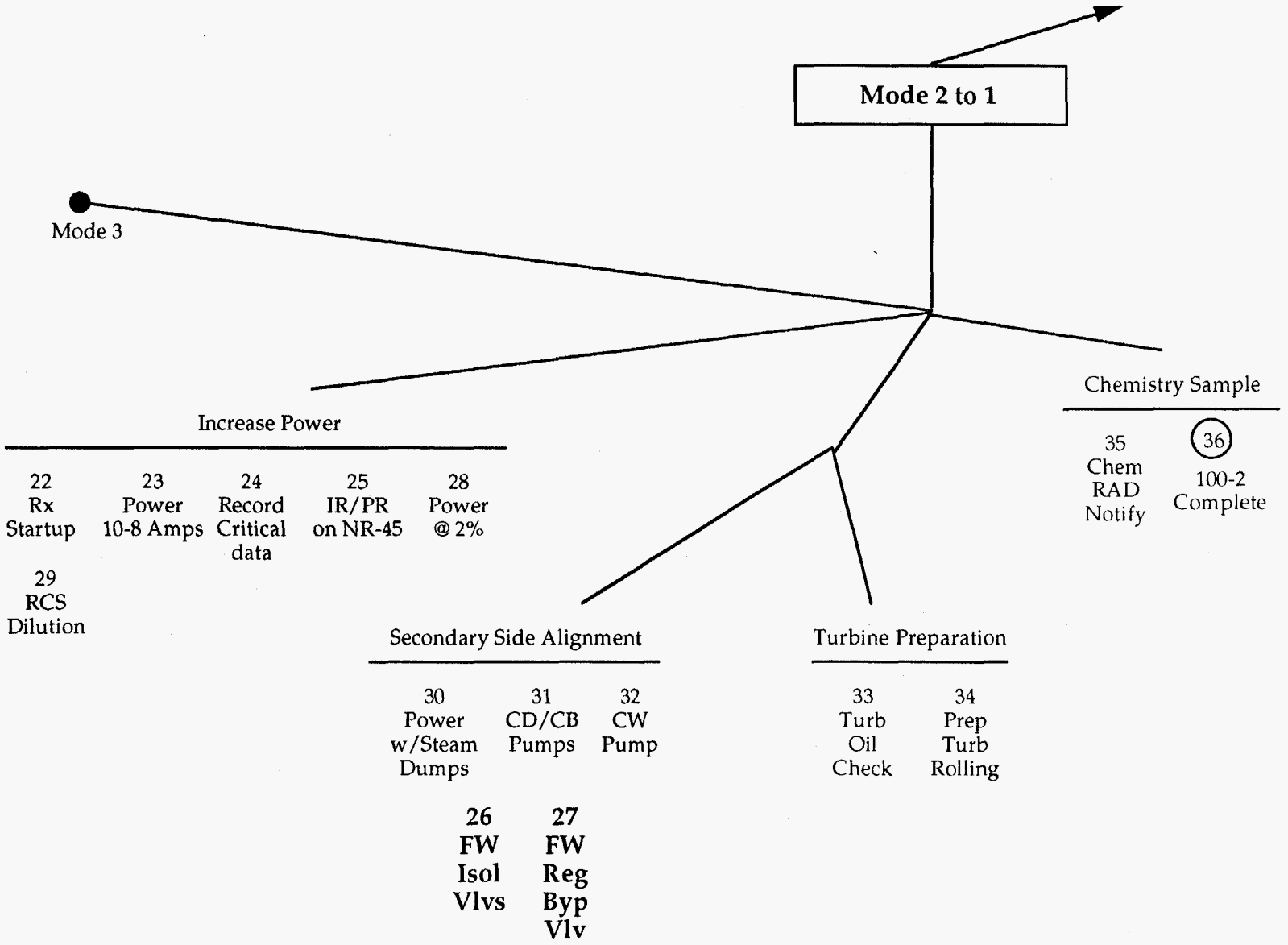


Figure 12 E: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

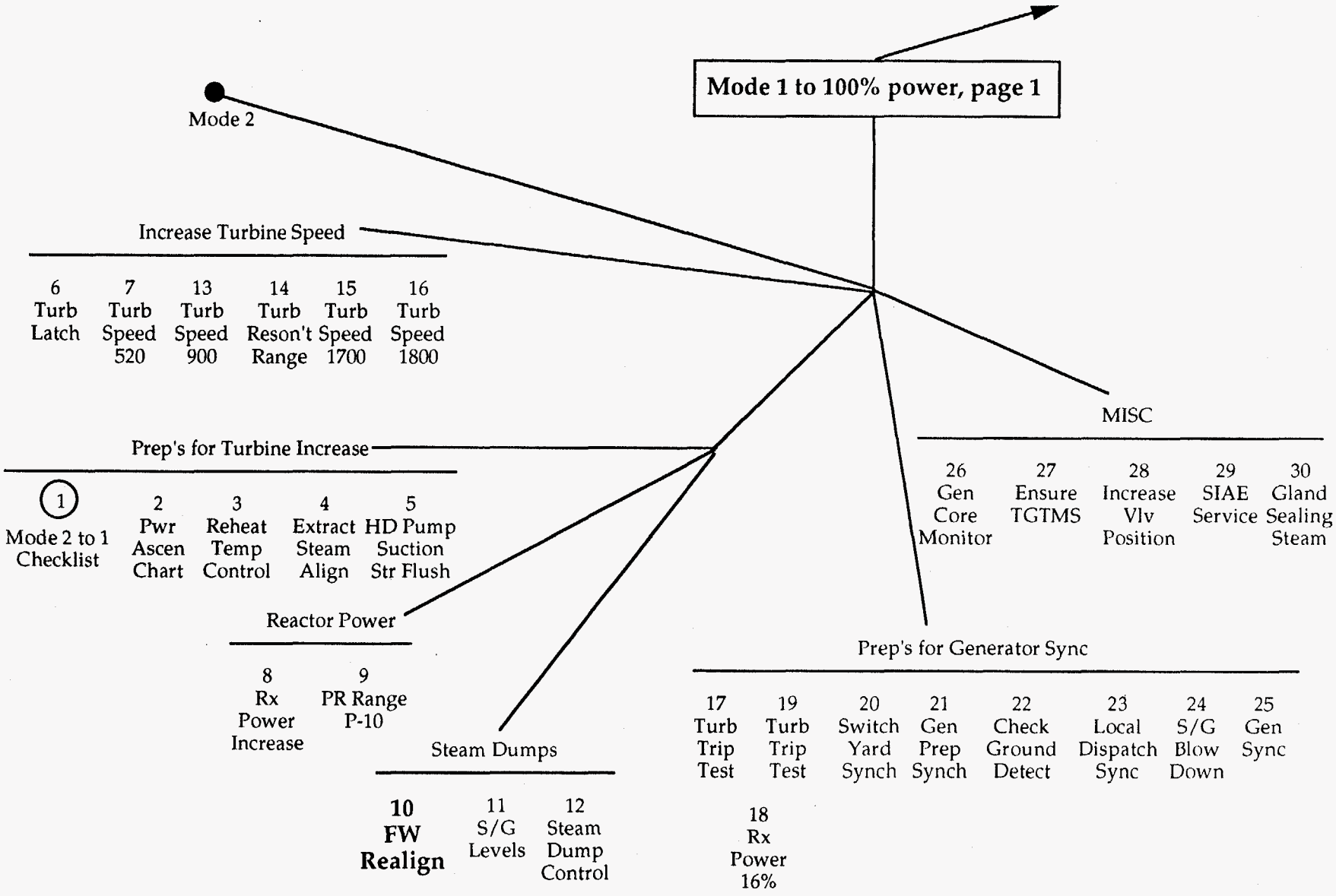


Figure 12 F: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

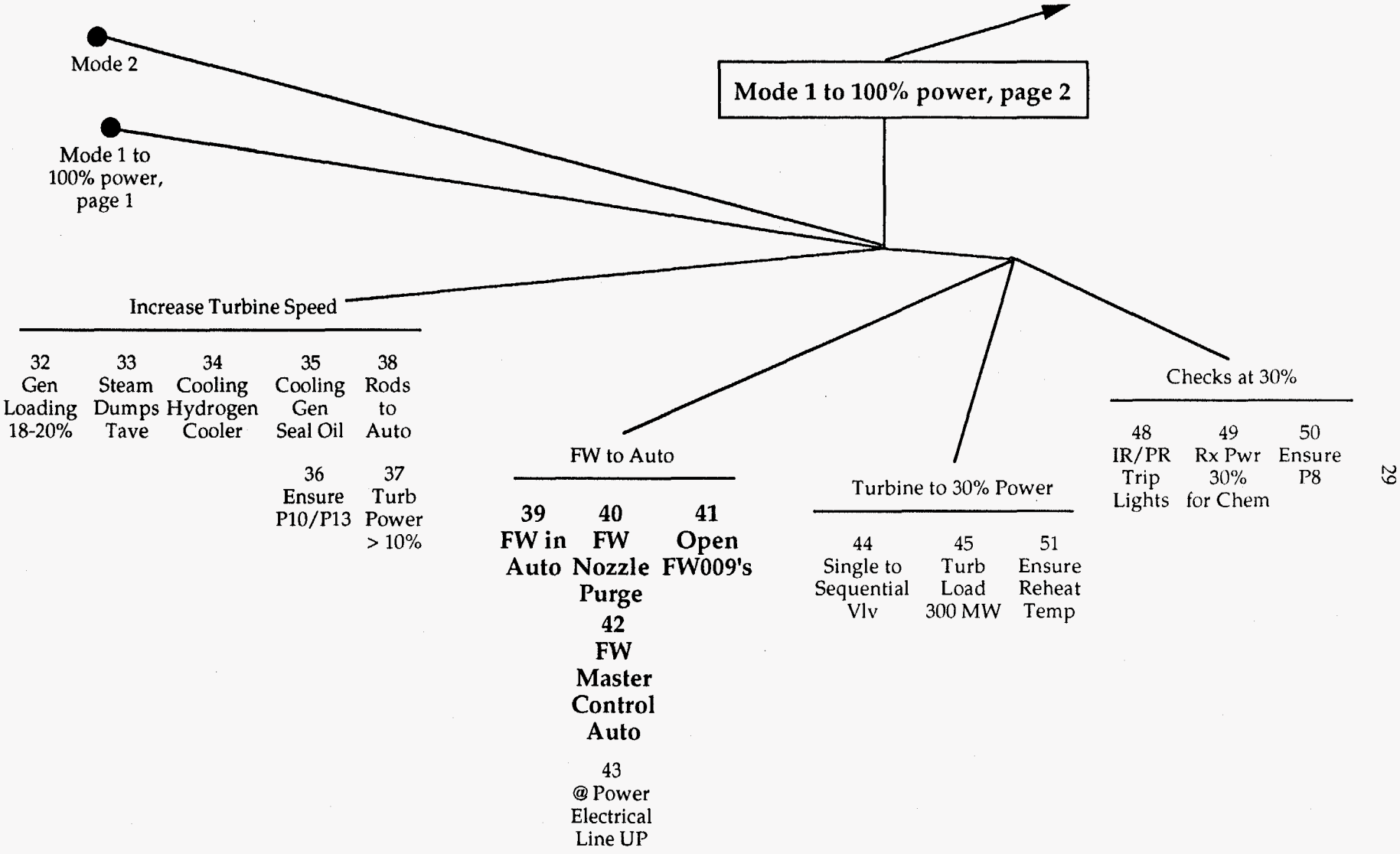


Figure 12 G: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

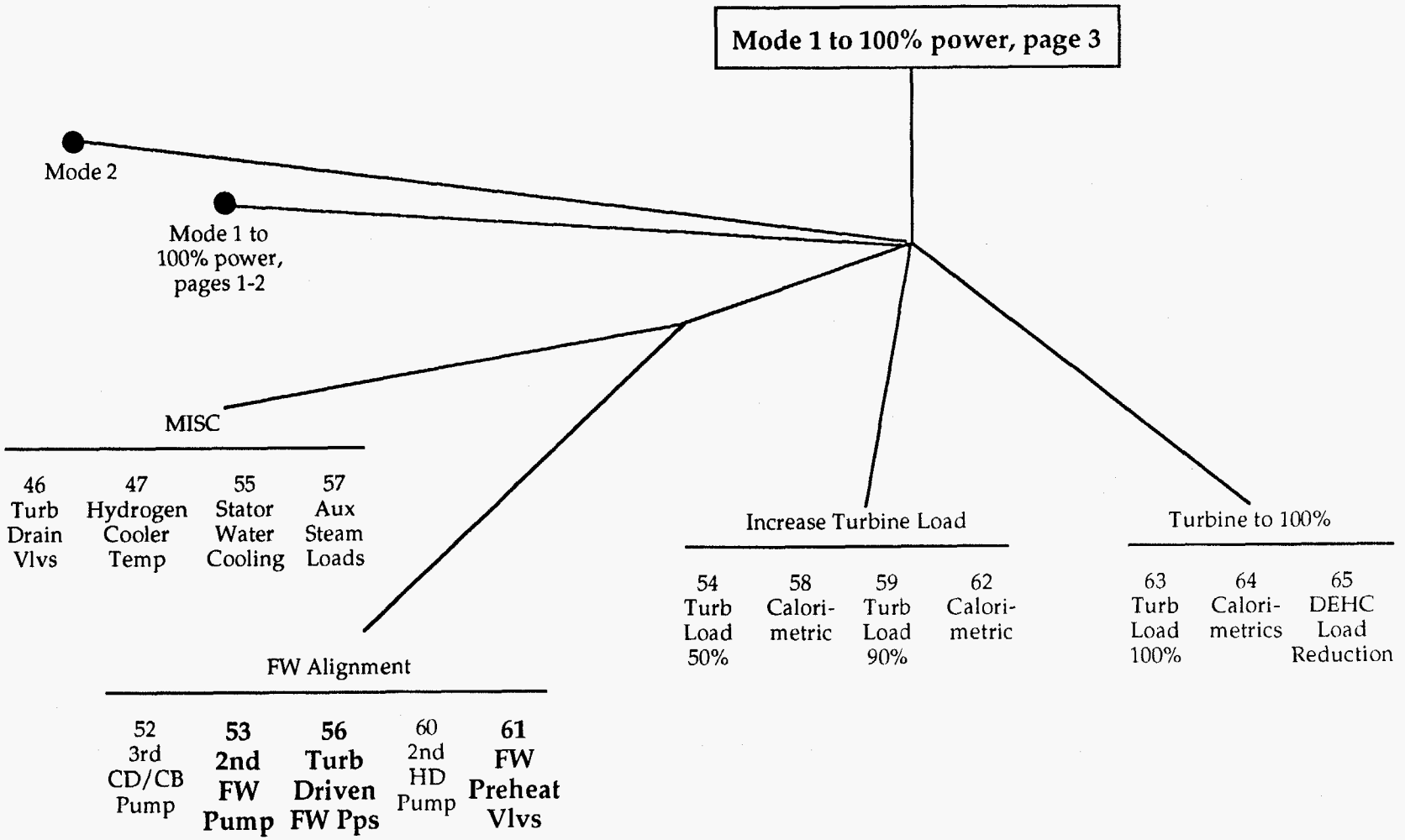


Figure 12 H: The SOP instructions for a pressurized water reactor presented in the "Bird's foot" format.

above the switch moves progressively from left to right, driven by a sensor of the valve position, indicating that the valve is opening, and when the valve is open the valve icon changes to outlined green. This process can be repeated for all the valves which are required. (In the example given in Figure 14, valves AFW009A,B, and c have all been opened manually.) If the controller is in automatic (which it should not be at this time) its mode must be changed using the icon at the bottom of Figure 14.

When all the valves required by the SOP have been opened, all the valves are outlined green to indicate normal operating conditions, and at that moment the node at the top of the page, labeled "1FW009A,B, C, and D Valves" changes to green to indicate that the conditions of the SOPs are satisfied. The screen then, a moment later, returns to Figure 13, and the node labeled "Place C/S for 1FW009 valve to be opened in open position" will be green, indicating that the condition is satisfied. The operator now moves to the next node to the right, clicks to open and read the Note, and then moves again to the right to the node labeled "Monitor FW pump and FW Reg Valve as FQW Isol Valves open". On clicking on that (white) node, the appropriate page of interactive graphics opens, leading the operator to take appropriate action as required by the SOPs.

This process continues until, in Figure 13, the operator has completed the actions associated with the page driven by the final white node, " Place controller for 1FW510/520/530/540 FW reg Valve in AUTO". As that action ends, all node are green, the top node "1W009A/B/C/D is ready" turns green, and the Figure disappears, shifting the operator to Figure 9. Note that throughout the process there are always present mimics, configural state space diagrams, etc., relevant to the Figure currently activated. These are in miniature at the top of the relevant page. For example, if the miniature diagram at the top of Figure 9 is clicked, Figure 15 appears, allowing the progress of the FW configuration to be monitored. (It would of course be possible to bring up the expanded Figures on other monitors. For choices among alternatives see the remarks below under Evaluation in Section 4.)

At this time on Figure 9 all the nodes to the left of "1W009A/B/C/D is ready" are green, since all those actions have been completed. The operator now clicks on the next node to the right, "FW Pump master Controller to AUTO" which is white, and the display is driven down to the lowest level of the pages relevant to that action.

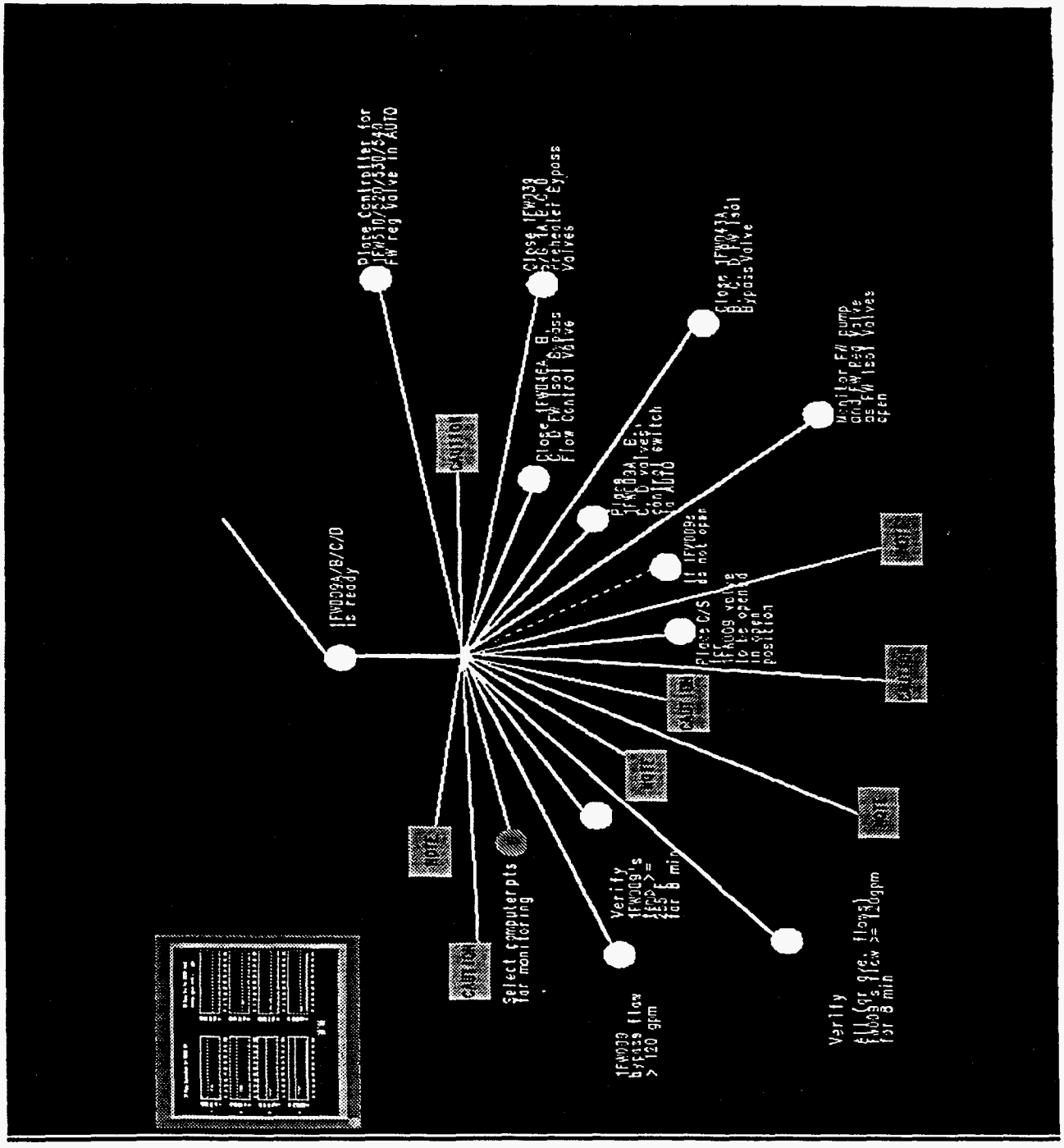


Figure 13: The "Preparation of 1FW009 Valves" Display.

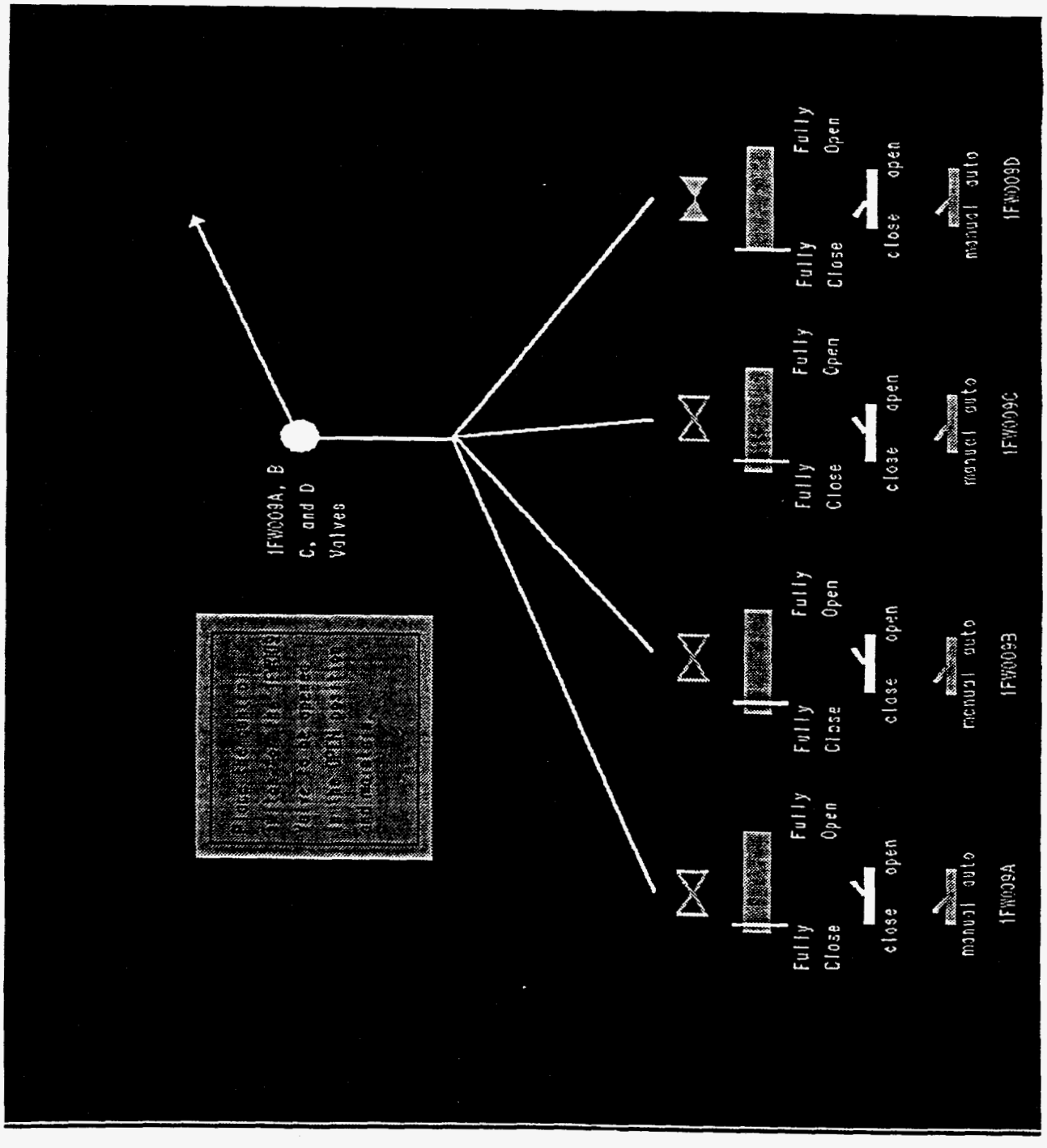


Figure 14: The "Placing 1FW009 Control Switch in Open" Display.

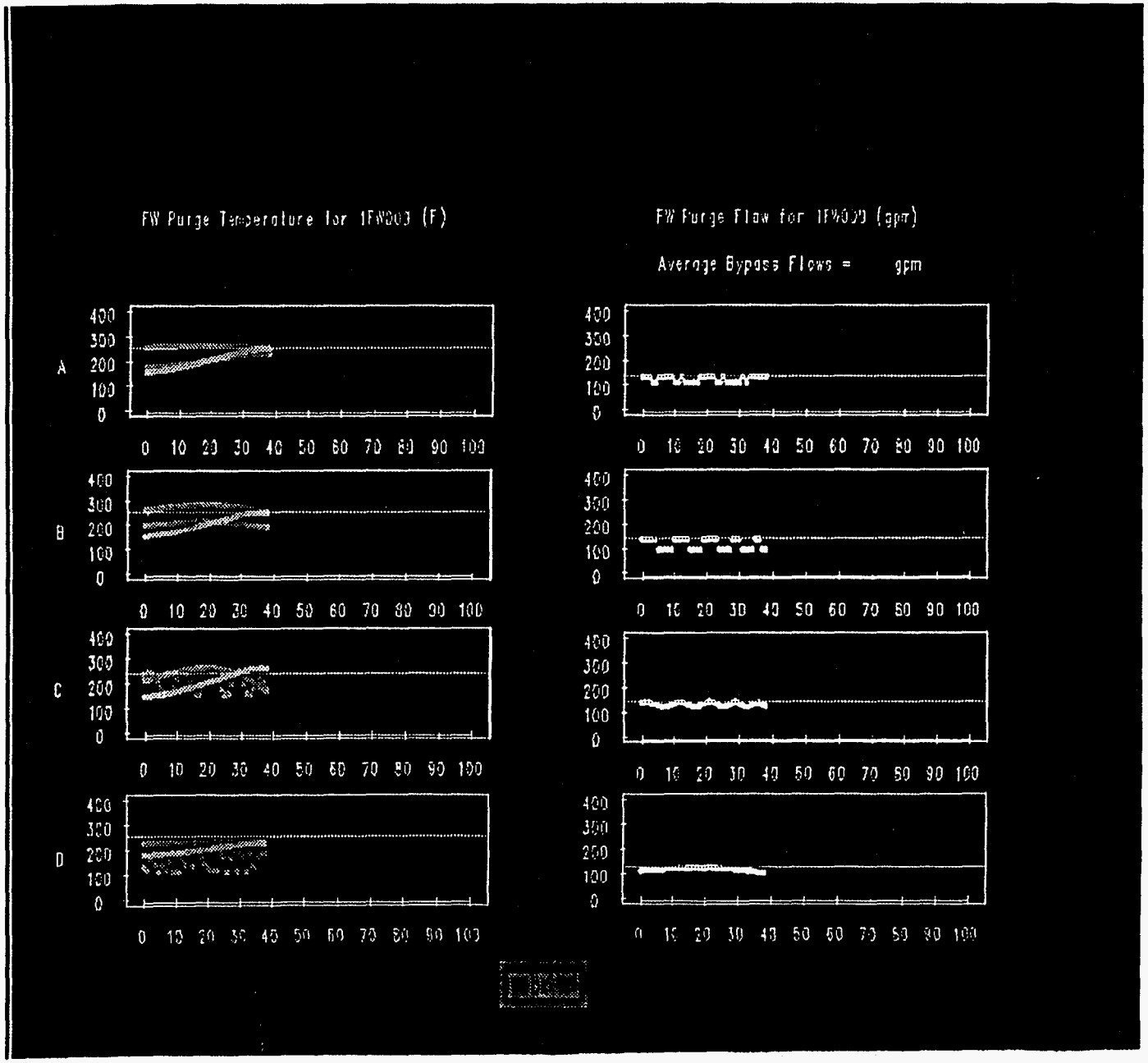


Figure 15: The "1FW009 Purge Temperature and Flow Rate" Display.

The operator then performs all the necessary steps, climbing up the bird's-foot tree until once more Figure 9 is reached. If all the actions have been performed correctly, "FW Pump master Controller to AUTO" is now green, and the operator can proceed again to the right. When finally the actions associated with "@80% power, Reopen 1FWD39A/B/C/D & S/G 1A/B/C/D" is completed, all nodes go to green, the "FW System" node goes to green, and the entire configuration of the feedwater system is complete. The system would then direct the operator to the next subsystem required, according to the Figure 12, if the overall lattice of the entire system were implemented.

If at any time the operator makes an error, or if the system develops a fault which is picked up and alarmed, the page with the appropriate step will reappear automatically, and the faulty step or component will be alarmed by the node being red. (For example if some how a fault developed and Valve 1FW009C closed, then all the nodes and arcs leading down to the valve icon on Figure 14 would become red, allowing the operator, by clicking on them successively, to retrace the path to the faulty component.

The above demonstration of the configuration of the feedwater system has been, for clarity, presented as if it were independent of the rest of the system, but that is of course not the case. Some steps of the configuration will be taking place while other parts of the system are configured at the same time, and in fact the sequence is that indicated by the step numbers in the original flow chart (Figure 7) or in Figure 12. Hence some of the steps will cause the operator to leave the FW system and work in other parts of the system which we have not shown here. But throughout, the geometry of the interactive graphics, with the simple rule that for each page tasks must be sequentially performed from left to right across the page, coupled with automatic page switching, will force the correct sequence of behavior from the operators. Within the scope of the present contract, the FW system was selected as a simple yet comprehensive proof-of-principle system for introducing the "brid's-foot" display concept.

3.4 Monitoring the plant state.

The above account shows how using the bird's foot lattice we can ensure that the operators perform the steps for start-up in an appropriate sequence. But as was

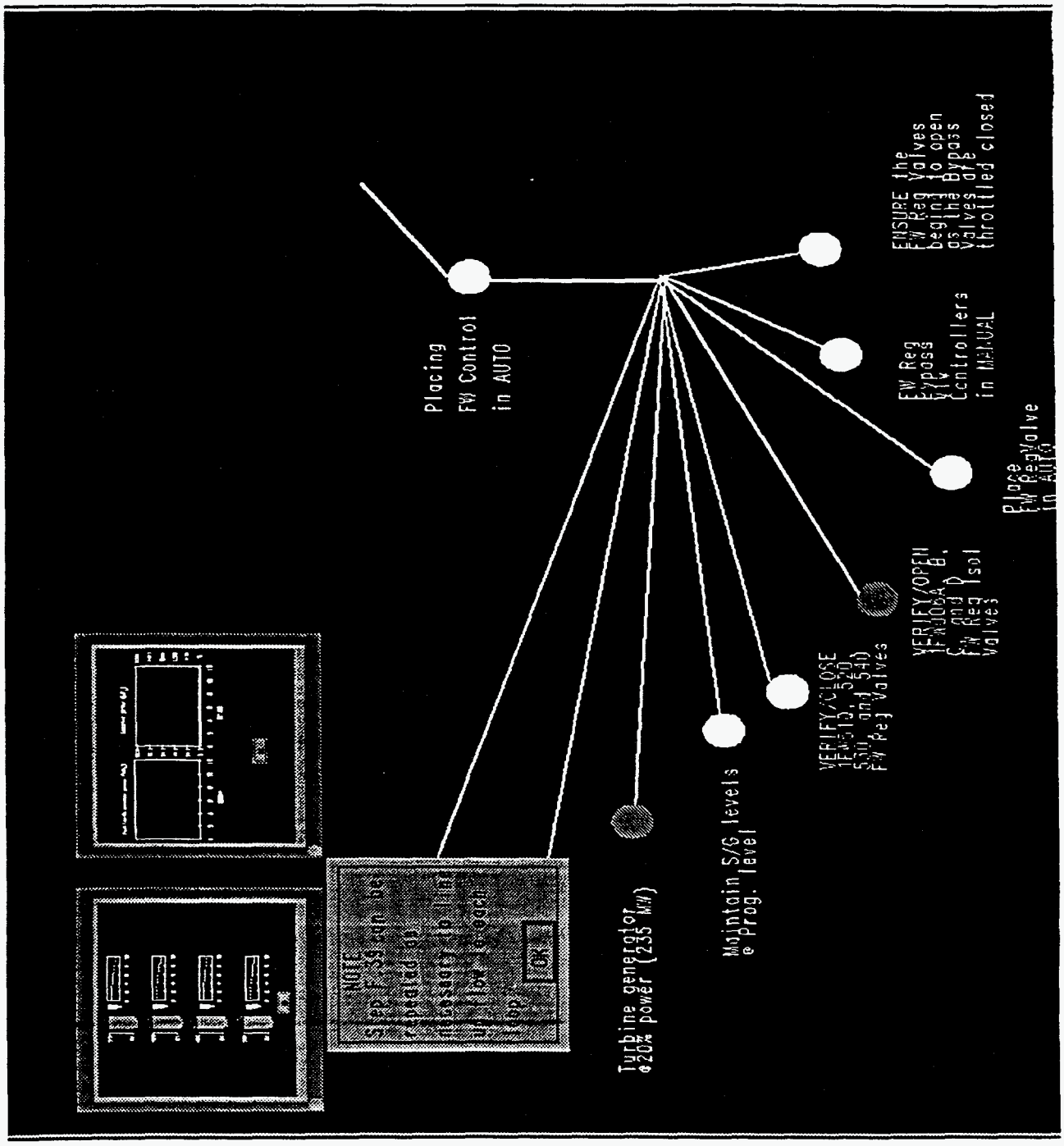


Figure 16: The "Placing Feedwater Control in Auto" Display.

indicated earlier, at the same time they must monitor the state of the plant and be alter for alarms, or for incipient problems. As was indicated, this is best done by using integrated configural state space displays. Some of these have appeared in some of the pages used as examples. For example, on Figures 9 and 16 both contain one or more small diagrams at the top of the page. These provide a continuously accessible set of ecological displays to support rapid perceptual analysis. In a real system with several screens, they would probably be available on a separate screen, although at all times they should be available as miniatures on the screens currently being used for SOP start up work, since it should not be necessary for the operator to change to a different screen in order to monitor, at least superficially, the most important of the plant parameters.

In the version as shown here, the miniature displays can be expanded to fill the screen by clicking on them, and we will now show how their content differs from more conventional displays. It should be born in mind that it has not been possible within this project to design a complete set of displays. Those now to be discussed are provided as exemplars of this approach to advanced display design.

3.4.1 Overall Mimic Diagram of Feedwater Subsystem. Figure 17

As Woods et al. (1982), Rasmussen (1986), Rasmussen et al. (1994), Moray et al. (1993) and many others have noted, displays should provide information, not just data. It is known that operators like mimic diagrams, because of the causal picture which these provide of the flows of mass and energy in a plant. We therefore believe that one display always available should be a mimic diagram, however crowded, of the plant, and that as configuration from cold shut-down to full power proceeds, the mimic should progressively change from white (inactive) to green, with red being used to indicate faults. Even though such a mimic will be very visually dense, it will help to orientate the operator as to which parts of the plant are running, which components are tagged out for maintenance, etc., and which parts remain to be configured. An interactive mimic could be used to access displays directly by clicking on hot spots, and these latter would be connected to appropriate levels of the bird's-foot lattice taking into account what had already been configured. Mimics of subsystems, such as Figure 18 for the FW system, should appear on all Figures where their information may be needed by operators.

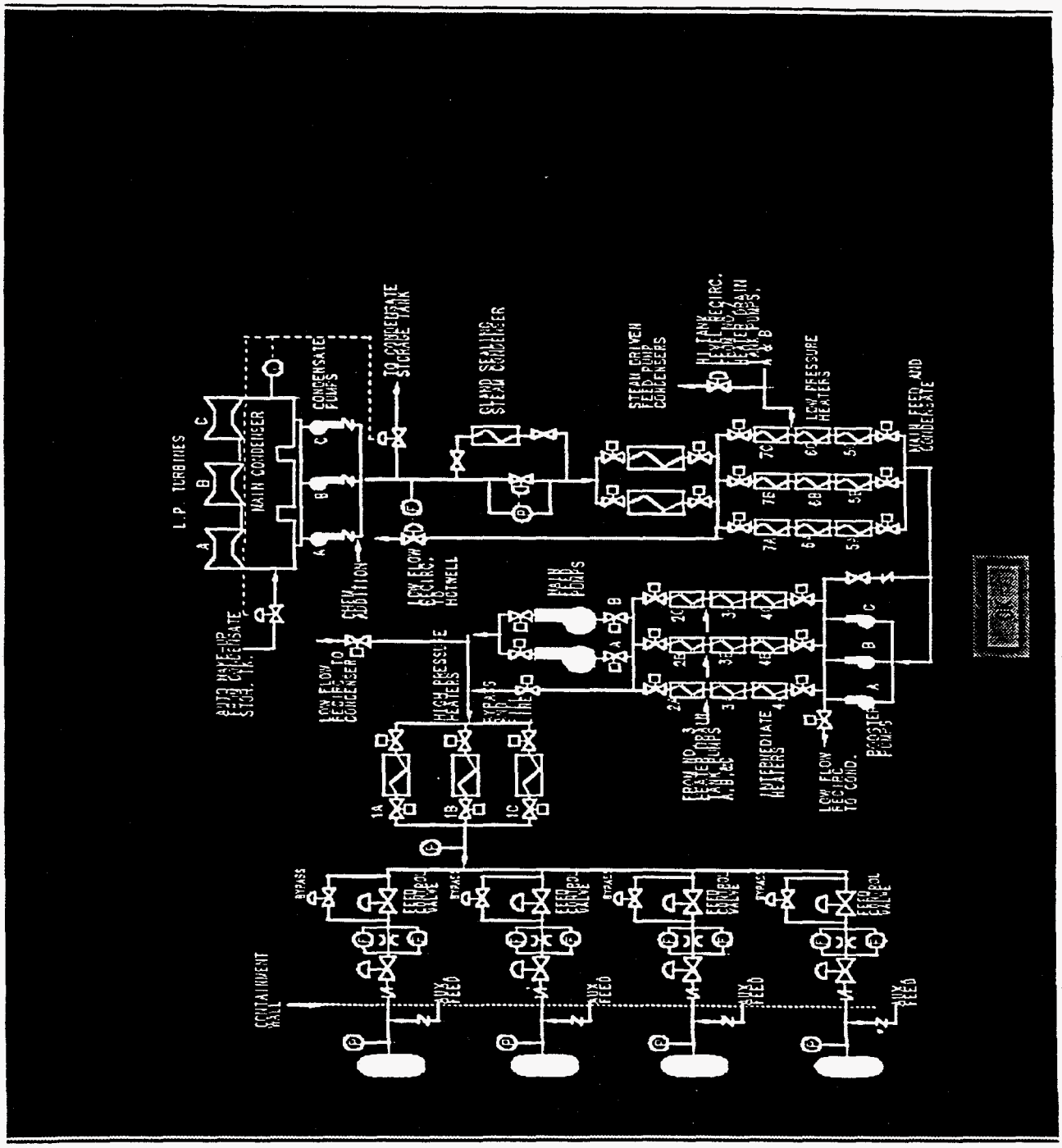


Figure 17: The "Feedwater System Mimic Diagram" Display.

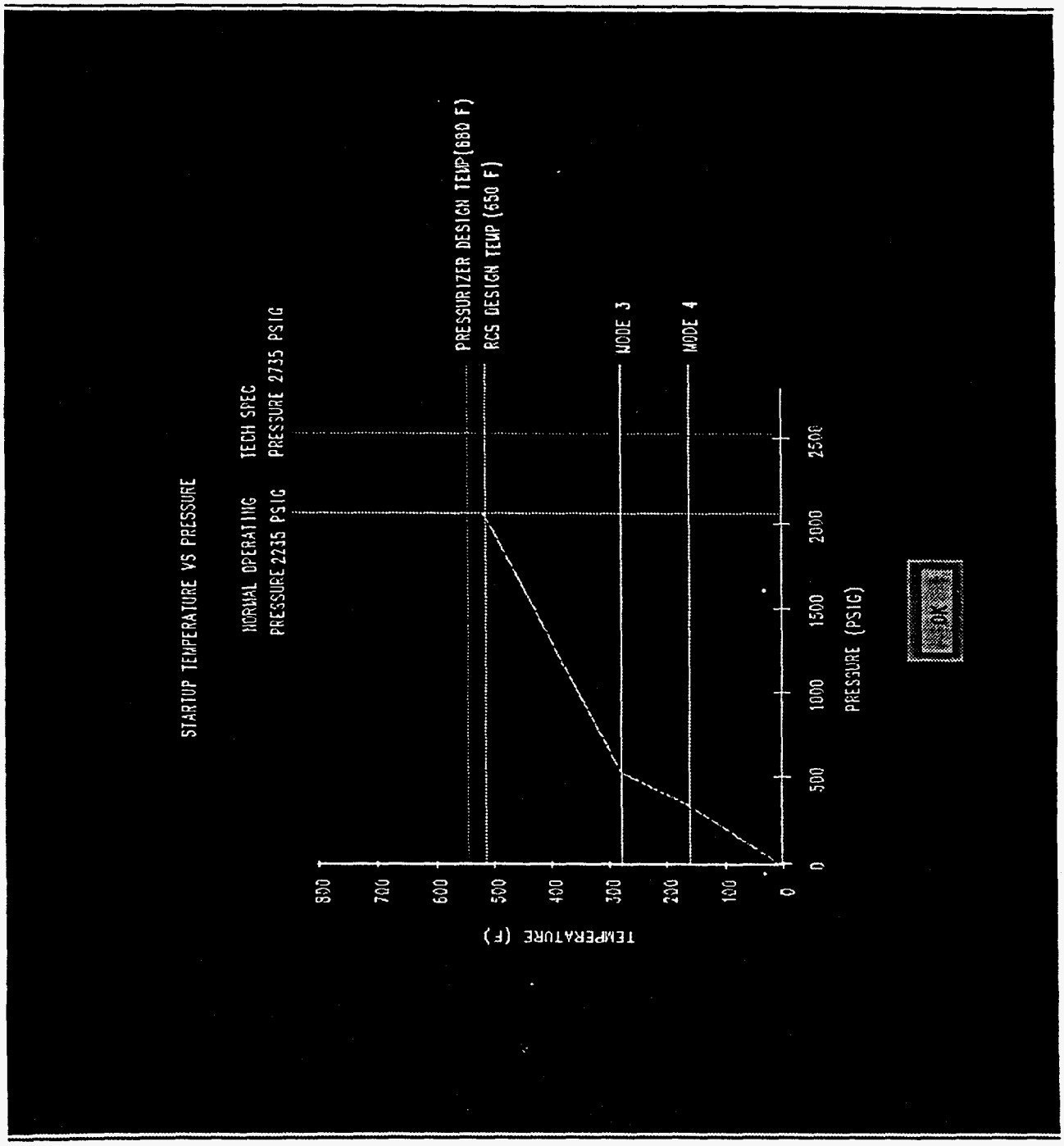


Figure 18: The "RCS Temperature vs RCS Pressure Plot" Display.

3.4.2 Temperature/Pressure/Mode Diagram. Figure 18

The first miniature figure on Figure 9 is one which shows the overall relations between temperature and pressure. It is shown enlarged in Figure 18. Instead of providing the values of temperature and pressure as numerical values, the values are presented graphically, and, more importantly, in relation to their functional meaning. Thus in Figure 18 there are three solid horizontal lines and one vertical solid line which divide up the temperature/pressure space. These are yellow, and indicate the expected values of temperature and pressure during Mode 4, Mode 3, and normal operating conditions, and the values at the moment of transition between Modes.. Two lines indicate the technical specification limits of operations, that is, "hazardous" limits which must not be exceeded. These are red in the original. In addition, there is a broken line running from the origin upwards and to the right, cyan in the original, ending near 500 degrees/2235 psig, the expected full power operating conditions. This line is approximately the trajectory which one would expect the temperature/pressure relation to follow as the plant is brought up to full power. The actual value of the pressure and temperature locus would then appear in green in relation to the cyan, expected line. This can be seen in the miniature in Figure 9, where the system has just passed beyond Mode 3, and where it can be seen that the actual measured temperature is slightly high.

Such a plot allows operators to estimate whether slight departures from the ideal locus are acceptable, or whether they are so far out of range as to be considered dangerous. Moreover, it is well known that operators make great use of trend graphs, and this kind of display is particularly meaningful trend graph, since it displays the safety margin at all times, allowing operators to make predictions from the slope of the trend line, and to anticipate future required safety actions. For a discussion of the value and cognitive importance of configural state space diagrams, see Rasmussen et al., 1994.

3.4.3 Power density/Temperature/Pressure Relations. Figure 19.

The task analysis performed on the written SOPs reveals that there is an important mutual relation between power density in kilowatts/foot, the core pressure (RCS pressure) and the temperature expressed as Departure from Nucleate Boiling Ratio (DNBR). These are normally presented as independent values, but the important property is their mutual relation. In Figure 19 a display has been developed which

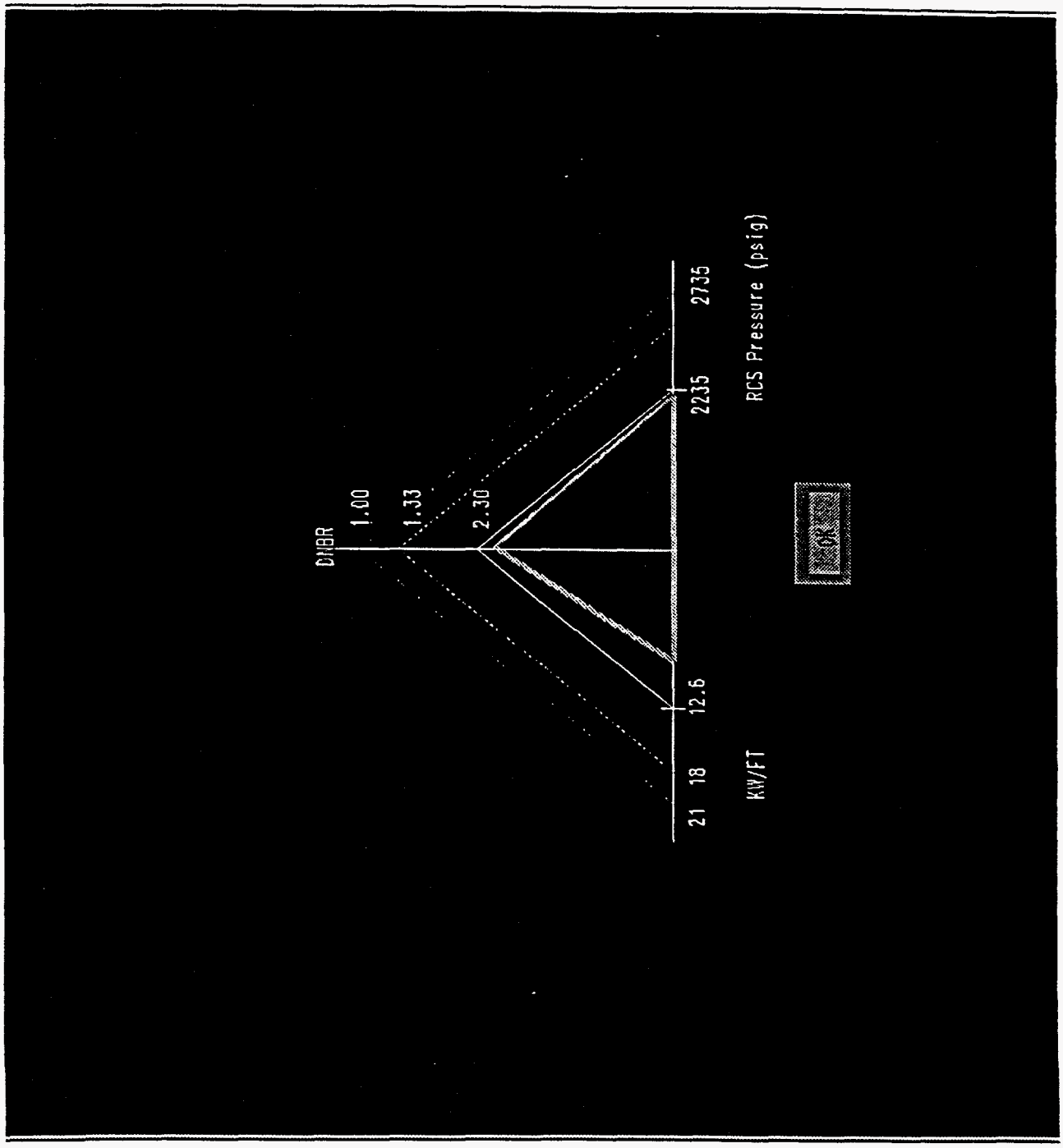


Figure 19: The "Safety Limit Envelopes" Display.

allows the operator to perceive directly whether this relation is satisfied in a safe and effective manner.

In the plant whose operating procedures we analyzed, normal full power operation is satisfied by DNBR = 2.30, RCS = 2235 psig, and KW/FT = 12.6. Since none of these variables can take a negative value, we can define a three-dimensional space with a common origin. We plot KW/FT from 0 increasing on the horizontal axis to the left, RCS Pressure increasing from 0 on the horizontal axis to the right, and DNBR on a n axis decreasing upwards from 0 where the other two axes meet. Any combination of KW/FT, RCS pressure, and DNBR is then represented by a locus in this space. Moreover, we can define a space of normal operation as a triangle whose apices are at DNBR = 2.3, KW/FT = 12.6 and RCS Pressure = 2235 psig., and this is indicated in Figure 19 by the thin solid white line. By choosing appropriate scales for the variables, this triangle can be made equilateral, isosceles, etc.. (In Figure 19 it is isosceles.) Any actual plant state can be represented by a triangle whose apices are the current values of the variables as measured by sensors in the plant. In Figure 19 this is indicated by the triangle bordered by a thick solid gray line. As long as the state variables do not exceed any of the normal operating values this triangle is drawn in green in the original display, so that as the plant state evolves towards full power, operators will normally see a green asymmetrical triangle inside a white isosceles triangle. At normal operating values the green triangle will overlie the white triangle. Departures from expected values will be revealed by asymmetries in the green triangle, since by choosing the scales on the axes appropriately, we can arrange that all normal states produce a green isosceles triangle whose base is bisected by the DNBR axis. Thus unusual states are readily detected by the distortions in the green triangle, in a way similar to the way in which distortions reveal abnormalities in the star diagram of Coekin (1969).

In Figure 19 two other triangles are indicated. The first, with its apex at DNBR = 1.33 encloses an area where operations are possible, but whose boundaries mark the values which regulations state must not be exceeded. The outer triangle, with an apex at DNBR = 1.00 define a triangle which encloses all states permissible under technical specifications. Operation outside this triangle is endangering the physical integrity of the plant. In the original diagram, the DNBR = 1.33 triangle is colored amber, and the DNBR=1.00 triangle is colored red. When the actual operating

values are outside the white triangle the color of the operating triangle changes from green to amber or to red as appropriate.

This display is an particularly clear example of the use of perceptually oriented displays instead of numerical values, and of the integration of information by means of appropriate geometry.

3.4.4 Other displays supporting plant state knowledge.

Several other graphs and graphics will be found associated with those pages where they are needed to monitor the results of actions taken according to the SOP structure. A more complete description of several of them and their use will be found in Appendix D. In all cases the aim is to represent knowledge which is relevant to the particular actions being taken. That is, as the plant is configured, and the level of operation moves up from the behavior of individual components to the behavior of integrated subsystems, so should the style and content of the supporting state diagram information change to match that progress. The overall principle is that *information should be provided in a form which supports the level and type of thinking being used by the operators.* If the operators are carrying out operations which deal with large scale mass/energy balances, they should be provided with information such as that shown in the Rankine cycle display, not with many individual measures of temperatures and pressures at different points in the plant. On the other hand, at times when they are dealing with detailed operations, the appropriate information and data should be available. We therefore require that displays should change according to the nodes of operation - literally so as the start-up sequence passes through Modes 1,2,3 and 4 and full power is approached.

To some extent this is already provided in the screens proposed here. For example, in Figure 14 the state of switches and valves are directly indicated, but these are not included in the higher level displays such as Figure 9. At high levels of the bird's foot hierarchy, integrated displays such as Figure 13 and 16 are more appropriate, and these are automatically presented on, or in relation to, the appropriate pages of the bird's foot hierarchy.

It will have been obvious from the text that the displays are intended to be colored. As far as possible color coding has been kept in accord with good human factors practice and industry convention (solid vs. outlines for valve states, red for faults

and green for normal, yellow for warning but not alarm states, etc..) To give a better feel for the appearance of the displays, three of them are reproduced here in color. See Figures 20, 21, and 22.

The first of these (Figure 20,) shows Figure 14 at the moment that the operator begins to open valves 1FW009A,B,C and D. The Note in the top left of the screen is a reminder of the actions to be taken. All four controllers are in manual mode, and hence shown dark green (normal, passive) , since no action is required on them. The first three valve manual controllers have been set to "open" and hence are shown as bright green (normal, active). The first three valve symbols are shown in outline bright green to indicate that they are open, while the fourth, which has not yet been opened by the operator, is solid green, to show that it is in its normal state at that time, but is not open. These symbols could be driven by the application of current to a motorized valve, but to prevent the kind of accident which occurred at Three Mile Island, an extra level of display is used. The position of the valve stem is indicated by the vertical yellow line on the horizontal bar. As the valve stem moves and the valve opens, it moves progressively from left to right across the bar. Since the operator has only just open the valves, the vertical lines are still to the lefty hand end, although the first three have begun to move as the valve opens. Note that the arcs at the top of the display, and the node to which they lead, are all gray, indicating that this step of the SOP has not been completed.

In the next Figure, all four valves have been opened. All valve symbols are outlined in green, and all four yellow bars at the right hand, or "valve open" end of the horizontal green bar. Since this stage of the SOP is complete, the arcs at the top of the Figure are now green, as is the node, and the arrow pointing to Figure 13. In the next moment this Figure will close itself automatically, and return the operator to Figure 13, which contains the next higher level of the bird's-foot lattice, where its associated node will now be green.

Finally, in Figure 21, we show what would happen if, owing to a mechanical fault, 1FW009B failed closed after it had been opened. In Figure 13 (or higher), the nodes and arcs leading back down to this page would all turn red, and when the operator clicked on them successively, he would arrive back on this page. We see that the trace is red back down to the faulty component, the manual switch has changed to closed and is red, the valve icon is solid and red (closed, abnormal), and the yellow

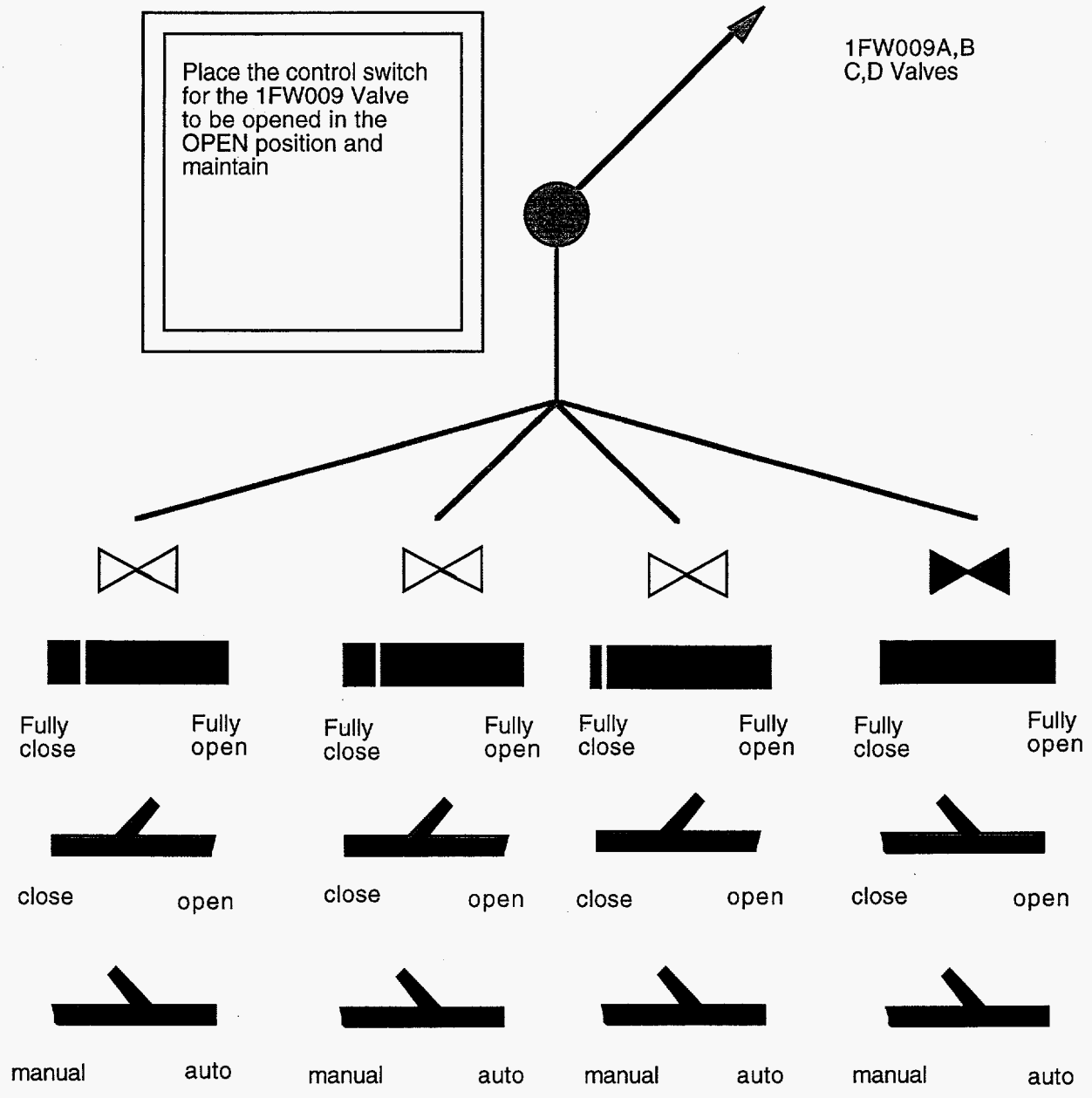


Figure 20: Full color display as 1FW009 valves begin to open.

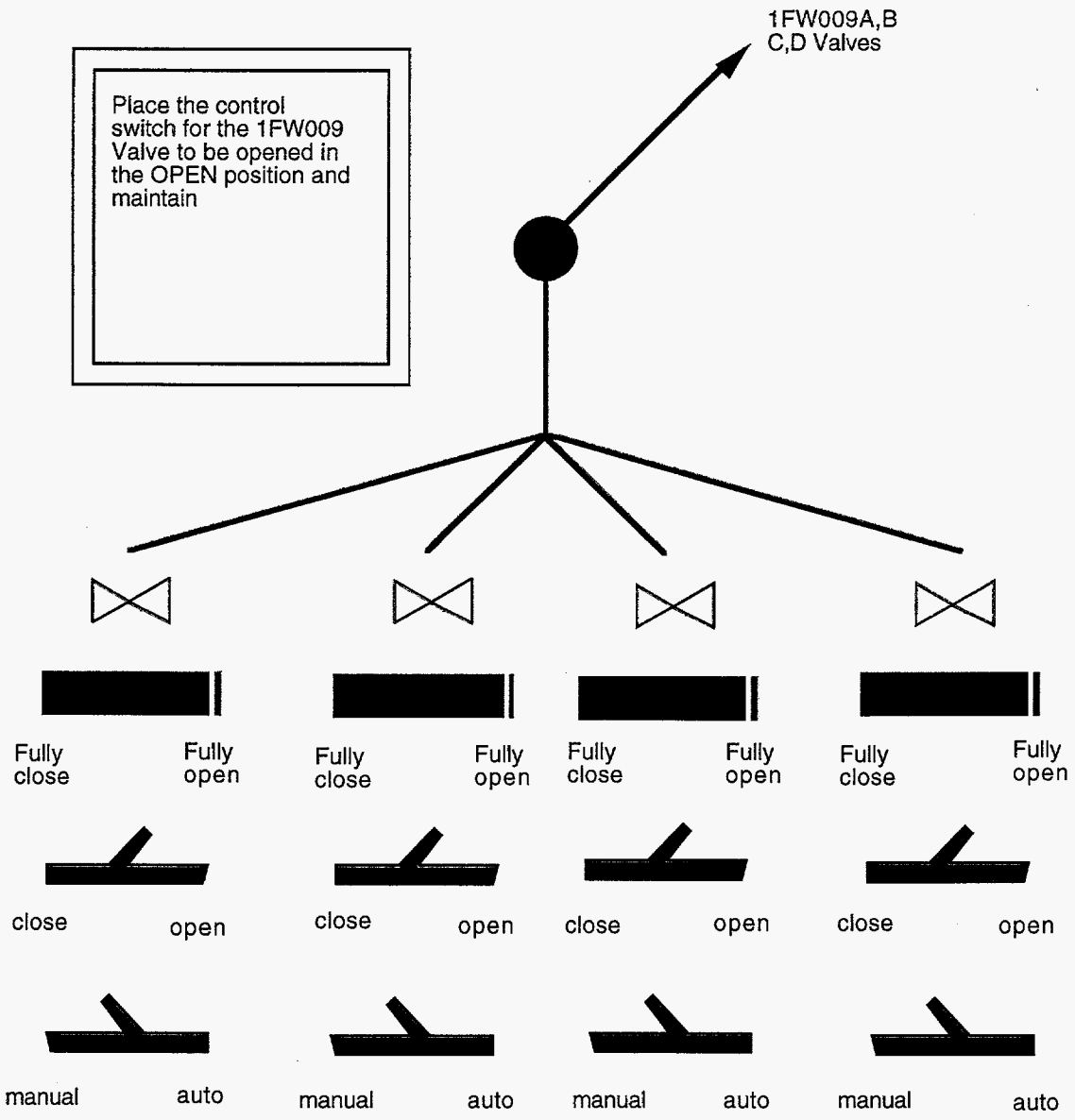


Figure 21: Full color display when 1FW009 valves are correctly configured

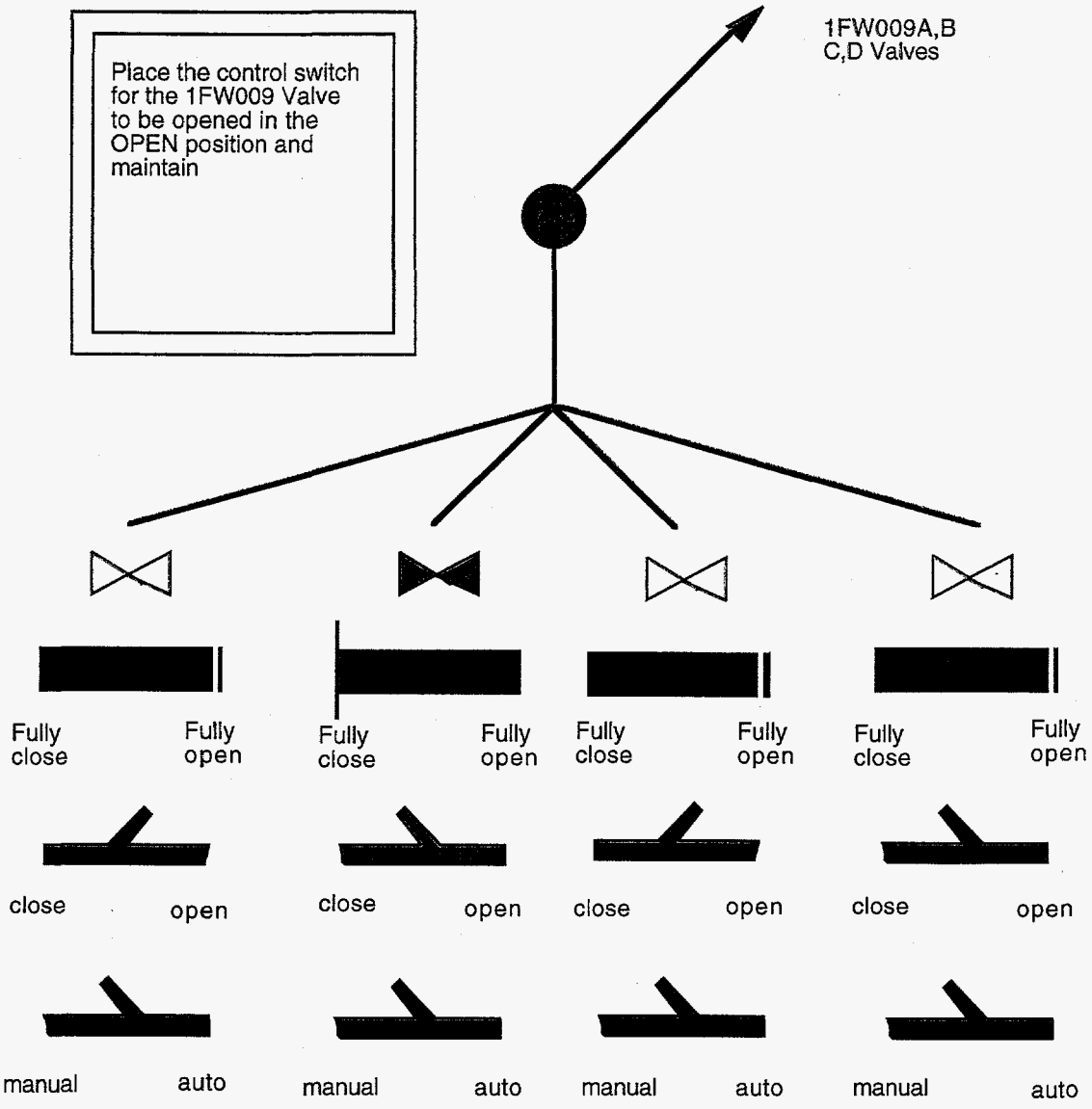


Figure 22: Full color display with a fault on valve 1FW009B. When the fault is corrected the Figure will revert to that in Figure 21.

line has moved to the left hand end of the horizontal bar. The clarity of the display and the links from higher levels supports a direct diagnosis of the fault, and the icons support identification of the failed components.

4.0 PROBLEMS AND EVALUATION.

In presenting these proposals for a new approach to graphics for NPP operation, several points need to be emphasized, since we believe that some features of this approach are certainly desirable, but others require much more research and development.

There is widespread agreement among those working in high technology human factors engineering that displays using integrated information are more effective than SSSI displays, and empirical evidence is beginning to accrue to this effect (Moray et al., 1993; Vicente et al., 1996; Rasmussen et al., 1994; Woods et al., 1982). On the other hand, there is a considerable art, rather than science, in designing such integrated displays (Reising and Sanderson, 1996), so that before implementing a particular realization of these ideas evaluation is needed, especially of failure modes.

We believe that the notion of guiding the operator through SOPs by means of a graphical display rather than by means of vast textually presented procedures is sound, and also that the idea of guiding the operators' thought to the appropriate level of abstraction by means of the bird's-foot diagrams or some similar approach is sound, but to date this approach has not been realized in a real plant or in a simulator.

The proposed set of graphics is particularly appropriate for the start-up sequence, passing from cold shut down to full power. *It does not follow that the same set of graphics is appropriate for monitoring, detecting faults, diagnosing faults and managing faults once the plant is running.* Consider what the occurrence of a red node in the bird's foot diagram means. If it occurs in Figure 13, then the natural thing to do is to click on it, back down to Figure 14 on node #5, and take appropriate action. It may be that one of the valves has failed into a different state, and this can then immediately be rectified, or at least the operator can try, by going into manual mode, to reset the valve and override the automatic controllers. But consider that

will happen if a red node appears in Figure 9. This is much later in the start-up sequence. Pressures and temperatures are now very high, and it is not at all obvious that if, on following the trail of red nodes down the bird's foot lattice, we find a valve in an abnormal state, that all that is required is immediately to reset it. This might result in severe thermal or mechanical shock to some part of the system.

It follows that if the approach advocated here were to be developed, great care would have to be taken to ensure that enough logic is present to provide only safe and appropriate routes for operators to follow. This should, it is true, be achievable if graphics are developed for all SOPs and EOPs, since by definition it is believed by the designers that the latter do indeed provide appropriate paths for all situations, and what we are doing here is not to get rid of SOPs and EOPs, but to make them available to the operators in a form which more effectively couples them to the psychological properties of the operators.

Evaluation of complex displays, direct manipulation graphics, and ecological displays is extremely difficult. Where operators are presented with a radically new kind of interface, it make take tens or hundreds of hours for them to become at ease with their use, even if, at the end, the system is preferred by operators and provides improved efficiency and safety. At present almost no new advanced graphical systems have been properly evaluated before being introduced, and as Moray (1993) has pointed out, this means that we can expect new and unforeseen human error modes. The difficulty of evaluating even a relatively simple system has been shown by the work of Christofferson, Hunter and Vicente (1996), where even after six months of training with a new ecological interface there were very great individual differences between operators. It is most important that if the proposals made in this report, *or in any similar report,* were to be realized, that very extensive testing in a full scope simulator be used to evaluate their efficacy. For example, Figure 23 shows an alternative geometry for Figure 19. In this case, only the locus of the state configuration is used, not the triangular form in Figure 19. In Figure 24 more than one level of the bird's foot lattice appears on a single page. And as mentioned earlier, there is the question of whether more than one screen should be used, so that the operators have to look at a different screen to examine configural displays but need not hide the bird's foot diagram while doing so. These and other similar alternatives cannot be decided for certain on theoretical grounds, and

demand adequate empirical evaluation, however costly and time consuming the latter may be.

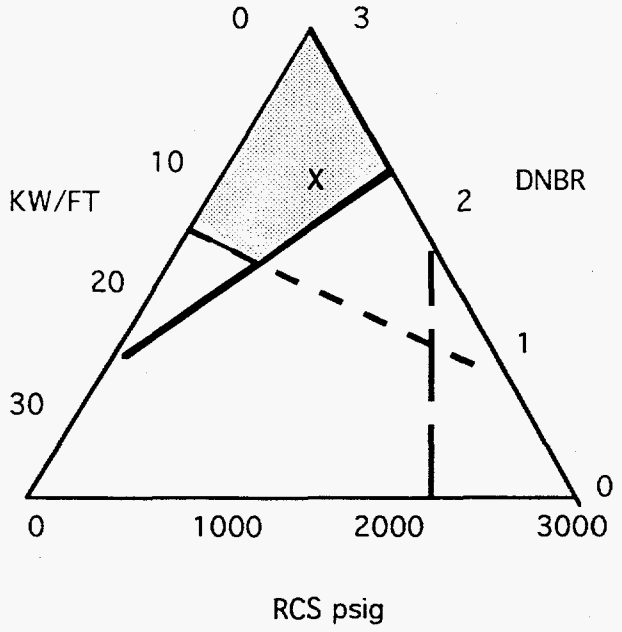


Figure 23. An alternative format for Figure 20. The normal operating conditions lie within the shaded area, and the locus of the plant state is indicated by the **X.**

Several other important questions about evaluation are relevant not simply to these displays, but to all advanced displays. A particularly important problem is how to choose scenarios for evaluation, and how much practice or how many operators should be tested, and other organizational problems. These and other problems, together with suggestions for scenarios for testing the feedwater displays, and discussions of the relations between the SOP and the state identification displays, are discussed in Appendix D.

5.0 SUMMARY

If computerized control rooms are to be developed, new kinds of displays should be considered, rather than images which are copies of traditional gauges, switches, etc.. In this paper we propose a new approach to the implementation of computerized SOPs, an approach which makes use of the power of computers to provide interactive direct manipulation interfaces which can replace written SOPs with graphics which guide the operators through the required steps. The images are

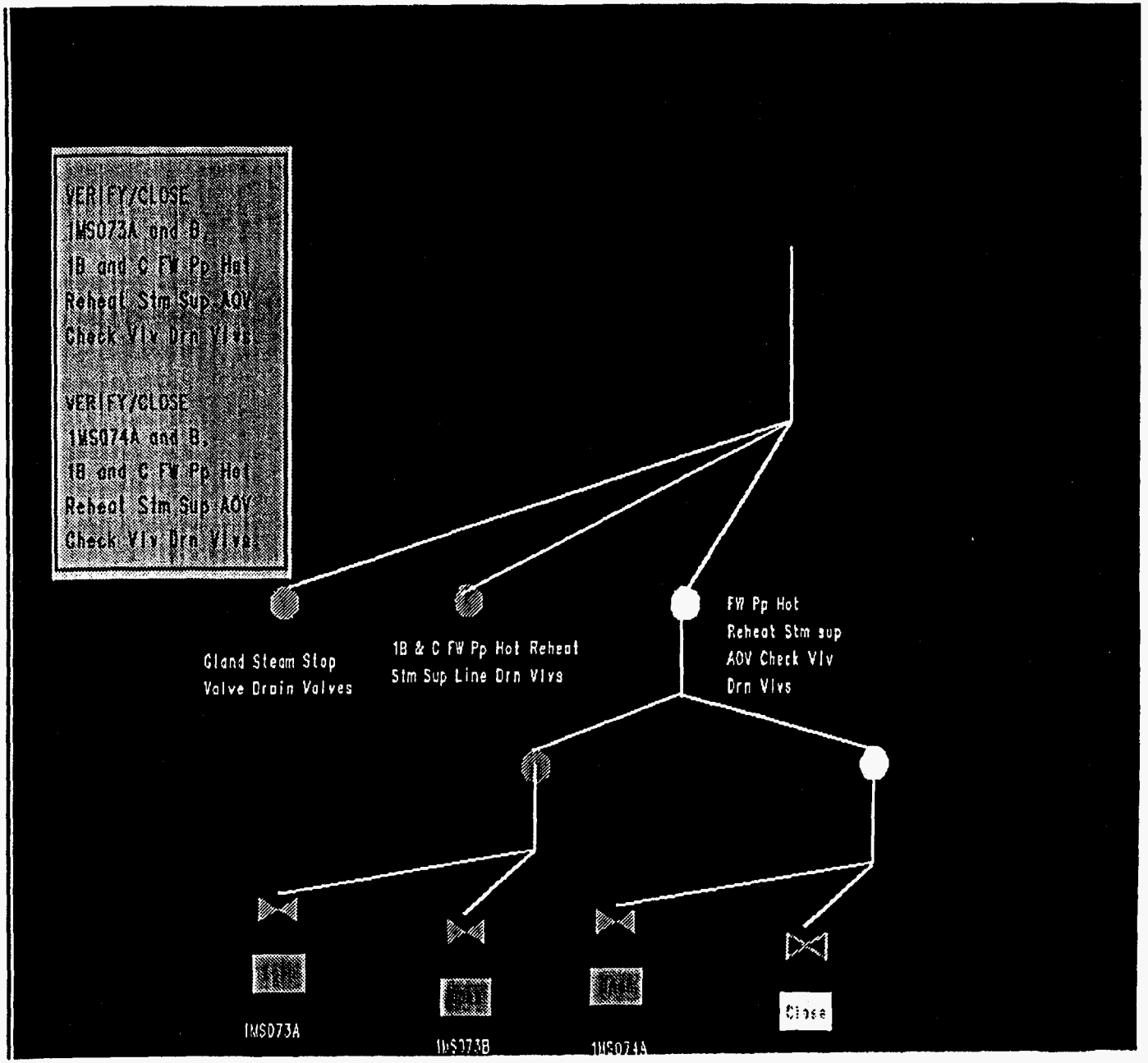


Figure 24: The "Verify/Close FW Pump Hot Reheat Steam Supplement AOV Check Valve Drain Valves" Display.

hierarchical, so that at all times the required information is presented to the operators in a form which supports the appropriate levels of thought required during the configuration and operation of the NPP. These graphical SOPs should be supported by integrated configural state space displays, mimic diagrams, etc., to allow operators to assess the state of the plant. Examples of the graphics for both kinds of displays are provided, with particular reference to the start-up of a feedwater system. Questions of evaluation are discussed.

6.0 ACKNOWLEDGMENTS

Our thanks are due to the personnel at the Commonwealth Edison Braidwood Nuclear Power Plant for discussions and assistance.

7.0 REFERENCES

Beltracchi, L. 1987. A direct manipulation interface for water-based Rankine cycle heat engines. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-17,* 478-487.

Christofferson, K., Hunter, C.N., and Vicente, K.J. 1996. A longitudinal study of the effects of ecological interface design on skill acquisition. *Human Factors, 38(3),* 523-541.

Coekin, J.A. 1969. A versatile presentation of parameter for rapid recognition of total state. *Proceedings of the IEE International Symposium on Man-Machine Systems.* Cambridge: UK. IEE

Flach, J.M. and Bennett, K.B. 1992. Graphical interfaces to complex systems: separating the wheat from the chaff. In *Proceedings of the Human Factors Society 36th Annual Meeting* (pp. 470-474). Santa Monica, CA: Human Factors Society.

Goodstein, L.P. 1981. Discriminative display support for process operators. In J. Rasmussen and W.B. Rouse (eds.) *Human detection and Diagnosis of System Failures.* New York: Plenum Press.

Kelley, C.R. 1968. *Manual and automatic control.* New York: Wiley.

Lindsay, R.W. and Staffon, J.D. 1988. A model based display system for the Experimental Breeder Reactor-II. In *Proceedings of Joint Meeting of the American Nuclear Society and the European Nuclear Society,* Washington, D.C.

Moray, N. 1993. Flexible interfaces can induce errors. In H. Kragt (ed.) *Enhancing Industrial Performance.* London: Taylor and Francis.

Moray, N., Jones, B.G., Rasmussen, J., Lee, J.D., Vicente, K.J., Brock, R., and Djemil, T. 1993. A performance indicator of the effectiveness of human-machine interfaces for nuclear power plants. *NUREG/CR-5977.* Washington, DC: United States Nuclear Regulatory Commission.

Moray, N., Jones, B., Sanderson, P.M., Rasmussen, J., Reising, D.V., and Shaheen, S. 1995. The "bird's-foot" integrated graphical interface for NPP operation. In Y. Anzai, K. Ogawa, & H. Mori (eds.) *Symbiosis of human and artifact. Proceedings of Sixth International Conference on Human-Computer Interaction.* Yokohama, Japan. Amsterdam: Elsevier.

Rasmussen, J. 1986. *Information processing and human-machine interaction: an approach to cognitive engineering.* New York: North Holland.

Rasmussen, J., & Vicente, K.J. 1989. Coping with human errors through system design: implications for ecological interface design. *International Journal of Man-Machine Studies, 31,* 517-534.

Rasmussen, J., Pejtersen, A.M., and Goodstein, L. 1994. *Cognitive systems Engineering.* New York: Wiley.

Reising, D.V. and Sanderson, P.M. 1996. Work domain analysis of a pasteurisation plant: Building an abstraction hierarchy representation. In *Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting* (pp. 293-297). Santa Monica, CA: Human Factors and Ergonomics Society.

Sanderson, P.M., Flach, J.M., Buttigieg, M.A., and Casey, E.J. 1989. Object displays do not always support better integrated task performance. *Human Factors, 31,* 183-198.

Shaheen, S. 1996. *Development of advanced direct perception displays for nuclear power plants to enhance monitoring, control and fault management.* Unpublished thesis for Master of Science in Nuclear Engineering, University of Illinois at Urbana-Champaign.

USNRC 1988. *Safety evaluation report related to the restart of Rancho Seco Nuclear Generating Station, Unit 1, following the event of December 26, 1985.* (NUREG-1286, Supplement No.1). Washington, DC. USNRC.

Vicente, K.J. and Rasmussen, J. 1992. Ecological interface design: theoretical foundations. *IEEE Transactions on Systems, Man and Cybernetics, SMC-22,* 589-606.

Vicente, K.J. , Moray, N., Lee, J.D., Rasmussen, J., Jones, B.G., Brock, R., and Djemil, T. 1996. Evaluation of a Rankine cycle display for nuclear power plant monitoring and diagnosis. Human Factors, 38(3), 506-521.

Woods, D. D., Wise, J. A., and Hanes, L. F. (1982). Evaluation of safety parameter display concepts. *(EPRI NP-2239).* Palo Alto, CA: EPRI.

8.0 REPORTS ARISING FROM CONTRACT

Moray, N., Jones, B., Sanderson, P.M., Rasmussen, J., Reising, D.V., and Shaheen, S. 1995. The "bird's-foot" integrated graphical interface for NPP operation. In Y.Anzai, K.Ogawa, & H.Mori (eds.) *Symbiosis of human and artifact. Proceedings of Sixth International Conference on Human-Computer Interaction.* Yokohama, Japan. Amsterdam: Elsevier.

Shaheen, S. 1996. *Development of advanced direct perception displays for nuclear power plants to enhance monitoring, control and fault management.* Unpublished thesis for Master of Science in Nuclear Engineering, University of Illinois at Urbana-Champaign.

APPENDICES

The following material is reproduced from Shaheen (1996), "Development of advanced direct perception displays for nuclear power plants to enhance monitoring, control and fault management." This thesis was written on the basis of the research completed under DE-FG02-92ER75781.

CHAPTER 2

DESIGN THEORY

2.1 Introduction

When mentioning "the control room" of a nuclear power plant, the most familiar picture is switches, indication lights, gauges, strip charts all over the benches and walls, see Figure 2.1, and this is not far from reality. With these thousands of pieces of information being displayed at once, some of the information irrelevant to the task in progress could be distracting to the operators and some of the crucial information may get ignored. With advancing technology, many displays now are presented on computer monitors which provide easy access and significantly reduce the clutter in the control room. However, most of these computerized displays are still the conventional types, single-sensor-single-indicators (SSSI). In SSSI displays, a tremendous amount of workload is placed on the operators for the need to integrate and reason with information, especially under stress.

Since human perception is faster and more accurate than human reasoning, it is logical to design an interface that supports this advantage. A design theory which attempts to solve this problem is the concept of ecological interface designs (EID). The word ecological refers to the underlying structure or affordance of the work domain. According to Gibson (1979)

"The affordances of the environment are what it offers the animal, what it provides or furnishes, either good or ill" (Gibson, 1979, p. 127)

also

"The observer may or may not perceive or attend to the affordance according to his needs, but the affordance being invariant, is always there to be perceived. An affordance is not bestowed upon an object by a need of an observer and his act of perceiving it. The object offers what it does because it is what it is." (Gibson, 1979, p. 139)

Based on this principle, EID displays use direct perception to allow the operators to "see" information or affordances and the relations among variables or the invariant rather than having to reason or calculate. In this chapter, the theory of ecological interface design using Rasmussen's abstraction hierarchy and means-ends hierarchy is discussed and previous work related to integrated display and EID are examined.

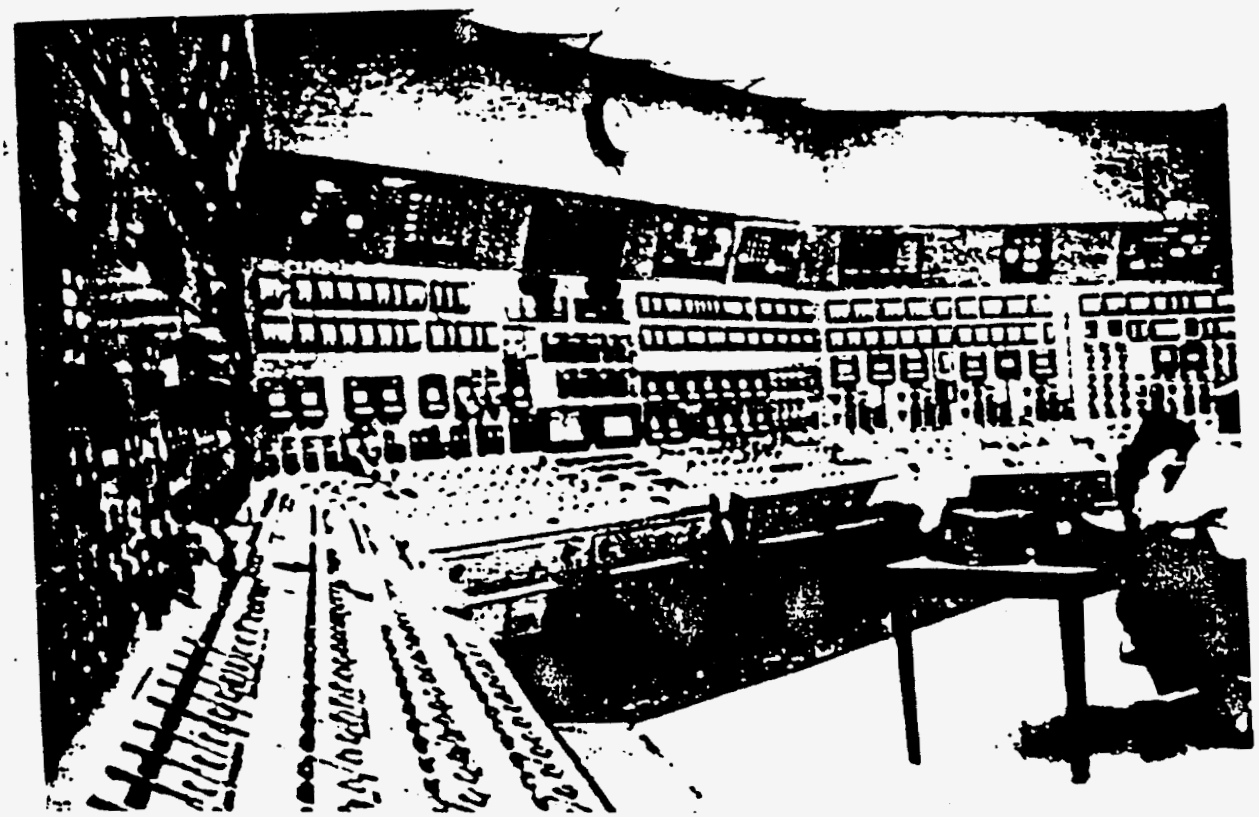


Figure 2.1 The TMI control room

2.2 Ecological interface design (EID)

2.2.1 Introduction

As stated earlier, EID is an alternative interface design solution to the conventional method. What makes EID a unique approach is that "Ecological interface design (EID) is a theory that provides principles for developing appropriate mappings between the process being controlled, the interface surface, and the operator's mental model." (Vicente and Rasmussen, 1987, p. 7)

Norman (1987) pointed out that there exist many mapping problems/gulfs causing difficulties in the human-machine interface. There are the gulf of execution and the gulf of evaluation. The gulf of execution is the difference between the user intention and his actions (on the input side of the system) and the gulf of evaluation is the difference between the system state and the user's mental interpretation of the system state (on the output side of the system). By minimizing these separations, direct manipulations can be achieved to an extent to provide operators with more control of the system.

An important aspect of the EID displays is to attempt to reduce the gaps between the gulfs by revealing the underlying structure of the system. From the ecological perspective, EID attempts to answer the questions: what is an effective way of presenting the complexity inherent in the domain and operator and how do operators cope with these problems. In this section, discussion of EID, abstraction hierarchy, and means-ends hierarchy are presented.

2.2.2 EID

As mentioned in the introduction section, the TMI accident demonstrated the need for an improved framework for interface design. The design of displays should be based on what humans naturally do best, perception (Rasmussen &Vicente, 1987). Perception is a very effective tool for detecting abnormalities using pattern recognition.

In a conventional control room design, often the operators are required to make quantitative readings from a display in order to determine the state of a certain parameter (Vicente & Rasmussen, 1988). The EID approach will be to develop a framework for interface design that supports the basic properties of the human cognitive system. EID is defined by Rasmussen and Vicente as the following:

"Ecological interfaces are characterized by representing the interior functional structures and states of a system in the human-machine interface in a way that matches the immediate task and the cognitive characteristics of the user." (Rasmussen & Vicente, 1987)

Furthermore, EID can be described as "trying to make the interface transparent, i.e., to support direct perception directly as the level of the user's discretionary choice, and to support the level of cognitive control at which the user chooses to perform" (Rasmussen & Vicente, 1987).

The EID is constructed using the skill, rule, and knowledge (SRK) taxonomy framework, the means-ends hierarchy, and the abstraction hierarchy. The SRK taxonomy (Vicente and Rasmussen, 1988) is proposed as a useful framework for describing the various mechanisms that people have for processing information. The means-ends hierarchy represents the goals and intentions of the operator. The abstraction hierarchy is a psychologically relevant form of representing the constraints in a work domain in a way that allows operators to cope with unanticipated events.

2.2.3 Information processing

A human-machine work domain can be described as a highly complex system which has one or more of the following characteristics: slow responses, many coupled parts, uncertainties, and risks. With the advancing technology in automation, the roles of operators in NPP are predominately process supervision and fault diagnosis.

Rasmussen's SRK (skills-rules-knowledge) taxonomy (1992) is an approach to describe operators' information processing. The SRK are three types of cognitive interpretation of information: the skill-based behavior (SBB), the rule-based behavior (RBB), and the knowledge-based behavior (KBB). The SBB is concerned with lower level controls. The RBB deals with simple mappings from signs. The KBB is related to analytical problem solving based on all system constraints. The SRK taxonomy can be mapped to the abstraction hierarchy in that the SBB supports the physical form and physical function levels; the RBB supports the generalized function level; and the KBB supports the abstraction function level.

In general, operators can use the SBB and the RBB in their day-to-day tasks because they require the operators to be familiar with plant components and procedures. However, when there is a system failure or a transient, they no longer support the operators for understandings of the plant status. During an abnormal operation, operators need to use the knowledge-based behavior (KBB) for analysis. However, thinking and reasoning are not simple tasks, especially under stress. (The SBB and the RBB are based

on perceptual processing.) The human perception is fast and effective and study showed that operators prefer to use perceptual processing, which also tends to cause fewer errors when compared with analytical problem solving (Reason, 1990). Since operators prefer to rely on direct perception for normal operation and transients, it is important to provide them with some interface that not only support the lower level processing (skills-based and rules-based) but also the knowledge-based behavior by displaying the embedded relationships among variables and systems.

2.2.4 Means-ends hierarchy

The affordances are offered by the environment to the animals in a variety of forms and one way that they can be organized is through a means-ends hierarchy. In a means-ends analysis of affordances, three questions are asked: why?, what?, and how?, see Figure 2.2. For everything organisms do, there should be a purpose, hence the question: "Why are we doing this?" After the purpose and intention are defined, identification of tools for accomplishing this purpose is needed. "What do we need to do/have in order to reach our goal?" Finally, there are purpose and tools, but "How are we going to do this task, with this method or with that method?". These simple questions illustrate the three levels of the means-ends hierarchy from the top down.

Even though the three levels are interrelated, there are some generic properties applicable to them. Each level deals with the same system and has its own terms, concepts, and principles. Also, the selection of the level depends on the operator's knowledge and interest in control of the system.

Means-Ends Levels of Description	Typical Control Tasks in Power Plant
Goals, purposes, and constraints.	Monitor production and safety specifications of the customers.
Abstract function: flow of mass, energy, and information.	Control of the flow of energy through the plant from source to electrical grid; Monitor major mass and energy balances for plant protection.
General functions.	Monitor and control individual functions such as coolant circulation, steam generation, power conversion from steam to electricity.
Physical processes of equipment and components	Adjust process parameters in order to align operational states of components and equipment to match requirements and limitations;
Form, location, and configuration of equipment	Connect and disconnect components; change anatomy and configuration of equipment and installations to match requirements of physical processes and activities.

Figure 2.2 Means-ends hierarchy

2.2.5 Abstraction hierarchy

In a complex, man-made work domain, there are sets of constraints that govern the reliability and safety of the system. The constraints are relationships among subsystem and variables. Because man-made systems are built according to some mathematical equations and theories and with a defined purpose, these constraints can be identified and be used as guidelines for operation. In some cases, however, when a failure occurs, the constraints for normal operation are no longer applicable. For instance, 100 C/ 212 F is the normal guideline for water's boiling temperature, but it changes when water is under pressure. The abstraction hierarchy (Rasmussen, 1979) is therefore developed to provide "a framework for identifying and integrating the set of goal relevant constraints that are operating in a given work domain."(Vicente, 1992, p. 12)

The abstraction hierarchy consists of five levels and each level has its own set of constraints, Figure 2.3. From the highest level to the lowest, the five levels are: functional purpose, abstract function, generalized function, physical function, and physical form. The functional purpose level illustrates the intent for which the system is designed. In the abstract function level, the overall physics and theories of a system in terms of mass balance, energy balance, etc. are defined. The generalized function is based on the concepts and relations characteristics of the physical process of related components, such as the feedback loops and circuits. In the physical function level, physical processes of the system or its part, such as what does one component relate to the others in the system, is described. This is the level at which physically limiting properties are represented and at which causes of malfunctions are typically identified. The lowest level is the physical form, which consists of the spatial locations and functions of components, such as valves, pumps, and gauges.

This hierarchy is constructed in similar order to the means-ends hierarchy in that the higher levels ask the question "why" whereas the lower levels ask the question "how." The lower level displays are represented by the conventional single-sensor-single-indicator type where states for each component are given. An example of higher level displays includes the DURESS interface where the energy flow and the output demand (constraints) are included as well as the components' data (see section 2.3.2)(Vicente, 1991).

The abstraction hierarchy is used to describe how operators cope with problems in a complex work domain. For instance, to bring a system on line, sometimes operators must think at the lower levels in terms of variables such as temperatures and valve settings. Other times, they must conceptualize at more abstract levels related to the thermodynamics of the system and energy balance. Also, they are required to think even more abstractly

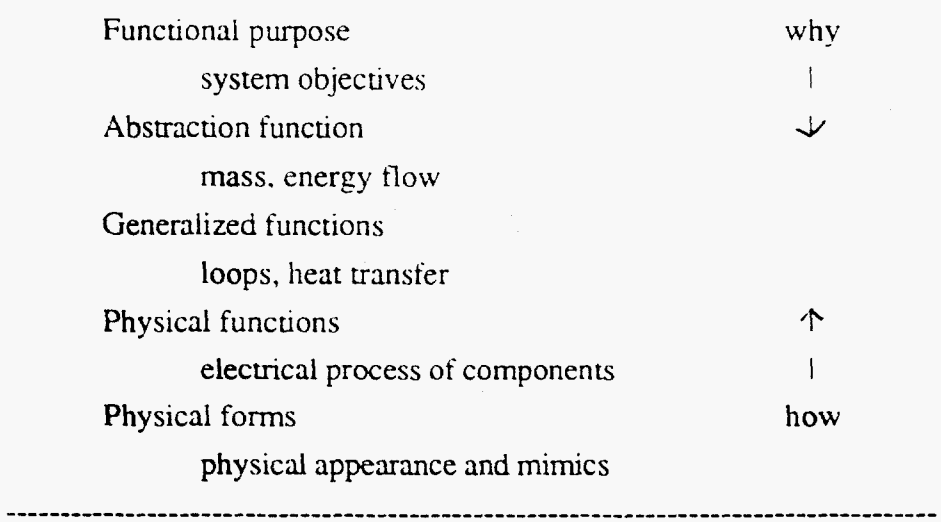


Figure 2.3 An abstraction hierarchy [taken from Rasmussen, 1986]

about plant production and safety. Operators are often moving from one level to the other in order to accomplish a task. By moving up in the hierarchy, less detail is provided and by moving down the hierarchy, more elementary data are presented.

When working with a system, going from one level of the means-ends hierarchy to another provides an effective way to cope with the complexity of any problem. At the higher level, even though fewer component states are provided that does not imply these information are lost. Data presented at the higher level is not just removal of details of status of the physical components, but a higher level integrated information is added based on the governing principles of various systems and components from the lower level (Rasmussen and Lind, 1981). Since each hierarchical level has its own terms, concepts, and principles, information presented must be converted and integrated to match the relevant abstract concepts. Some variables can be measured directly and some need to be calculated. An advantage with the multi-level approach in coping with complexity is that it leads to structured problem solving in diagnosis. In general, one might expect the mental workload to be reduced at higher level.

2.2.6 Summary

With some understanding of the hierarchical structure, the abstraction and the means-ends hierarchy "not only serve the purpose of a systematic description of the context in which supervisory decisions are made...(it also provides) the information processing strategies human can use for the different phase of the decision sequence and the performance criteria that control their choice in actual situation" (Rasmussen, 1986).

2.3. Previous work on EIDs

"There seems to be a clear consensus that graphical interfaces provide an opportunity to integrate data from complex process in a way that can greatly enhance the problem solving ability of human operators in the future." (Flach & Bennett, 1992, p. 470)

This section provides some examples of integrated graphical interface design related to the EID principles. The "star" display was based on the idea of showing the relations among variables rather than the individual values. This particular display has been implemented in several NPP control rooms, but there has not been enough evaluation of its effectiveness and there is little theoretical basis for the choice of variables or the arrangements within the star.

DURESS, on the other hand, is a research simulation constructed to demonstrate the EID theory and the findings are to be generalized to the real world systems. Empirical studies of this simulation illustrated that interface based on an abstraction hierarchy can provide more support for knowledge based behavior than an interface based on physical variables alone (Vicente, 1991).

Lastly, the Rankine cycle display (Beltracchi, 1987) is designed with the notion of EID and direct perception of relations. The Rankine display mimics the secondary loop of a PWR and it not only contains all variables from analog meters but the animated graphics also shows the relations of mass/energy balance and thermal dynamics. Moray, Jones, and Rasmussen (NUREG/CR-5977, 1993) reported that this display provides a direct mapping between the functions of a NPP and the functions of a Rankine cycle and improves diagnosis, even for novices.

The following sections include more detailed description of these interface designs and their evaluation results, when applicable.

2.3.1 STAR

As early as 1969, Coekin proposed an object or integral display, the "star" for nuclear power plants, Figure 2.4. An object or integral display is a when a group of data is presented as a single object. The "star" (Woods et al, 1987) is a safety parameters display for Westinghouse PWR and it is already implemented in several plants. A "star" consists of eight important parameters which form an octagon, and the values of these parameters are scaled and are represented by the length of the spokes. In general, the operators need to look up the plant status (from thermometers, pressure gauges), integrate values (calculations, steam tables), interpret data (comparison with Tech Specs, plant procedures),

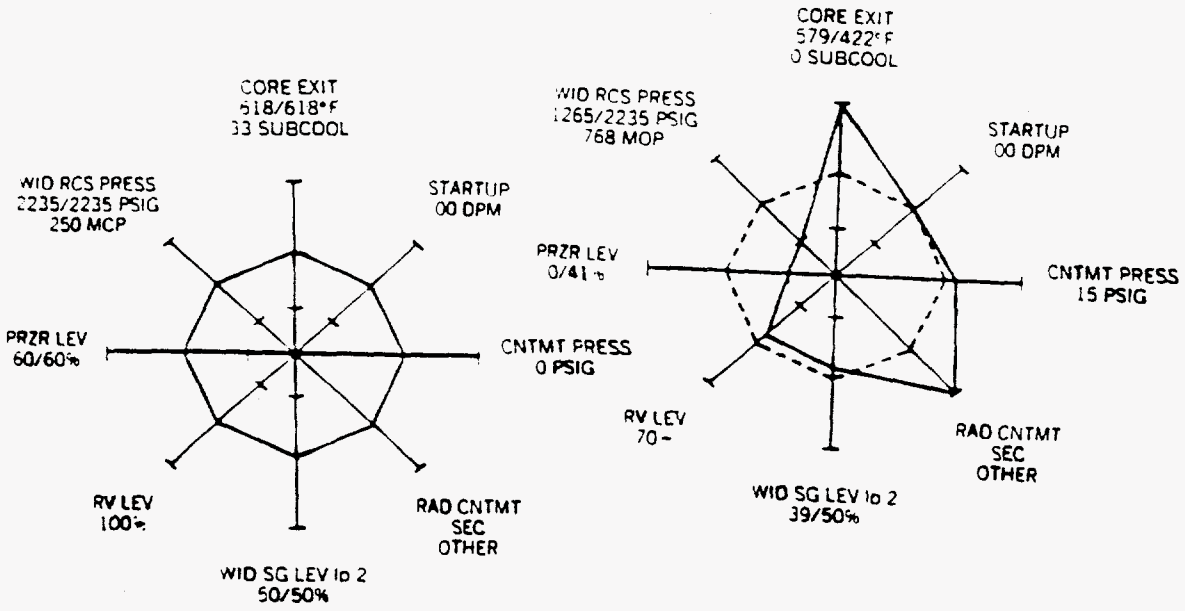


Figure 2.4 STAR displays [originally proposed by Coekin (1969)] for safety status of a NPP

and asses plant status (within range, off by 2%). Most plant data are related through the dynamics of systems and need to be integrated to determine if the systems are operating normally. The task of integration constantly places a great burden on the operators. With object displays, one advantage is that they capitalize on the parallel processing of objects to create multidimensional displays (Wickens, 1992).

As demonstrated by the "star", when everything is operating normally, the shape of the display is a perfect octagon, that enables the operators to simply glance at the display to perceive the plant status is normal. With the conventional displays, operators would have to search each of the eight actual values and determine the status by comparing with the reference values. It can be seen that for this task, the "star" display reduces the operators mental workload to some extent. Furthermore, it provides the operators with a mental "shape" of normal operating range. Anytime when the "star" is "out of shape", it alerts the operators for possible system failures. In addition to the easy access of information and detection of faults, in some cases, certain failures cause a definite shape to the polygon due to the coupling of the parameters and the arrangement on the display, thus provide a higher order understanding of the plant status.

Studies (Wickens, et al, 1984) show that this type of displays is better than the conventional single-sensor single-indicator displays in fault detection and information extraction. Properly designed integral displays enhance the operator's ability to extract information because they produce a better match between human cognitive characteristics and the cognitive demands of the tasks to be performed. In conclusion, integral displays can enhance multiparameter decision making and taking the advantage of human pattern recognition abilities, to aid the operators in detecting faults occurring in the system.

2.3.2 DURESS

DURESS, a thermal hydraulic process control system: DUal REservoir System Simulation, has been used to demonstrate the principle of the EID theory (Vicente, 1987), see Figure 2.5a and Figure 2.5b. DURESS is designed to simulate some real world problems, a dynamic interactive system with time lag on the controls and risks. DURESS consists of two feedwater sources that supply water to two reservoirs through two pumps. The operators need to keep each reservoir at prescribed levels to meet the output demand and prescribed temperatures by controlling the pumps, valves, and heaters.

The functional interface for DURESS is designed according to the principles of EID-making the invisible visible. The task of keeping the reservoir at a certain temperature and level is decomposed into every level of the abstraction hierarchy. Figure 2.5a is the physical (P) structure of DURESS. The P interface consists of components and their status as well as operator's goals (prescribed temperature settings and current demands). The functional display shows the demand and temperature (functional purpose), flow rate (generalized function), and valve settings (physical function). In addition, the display mimics the physical layout of the system. Figure 2.5b consists of both the physical and functional (P+F) structures of DURESS. The functional interface represents the abstraction function level in terms of its mass and energy balance. These mass and energy graphics are presented as a funnel metaphor. For example, the mass balance in reservoir 1 shows that the volume should be decreasing because the output is greater than the input (bottom is wider than the top). The P+F interface contains information at every level of the abstraction hierarchy.

An evaluation was conducted for both the P and the P+F interface displays with both expert and novice subjects through memory recall and diagnosis accuracy (Vicente, 1991). The results showed that subjects performed slightly better in the memory recall experiment with the P interface than with the P+F interface. However, in the diagnosis accuracy experiment, the P+F interface out performed the P interface at each level of analysis.

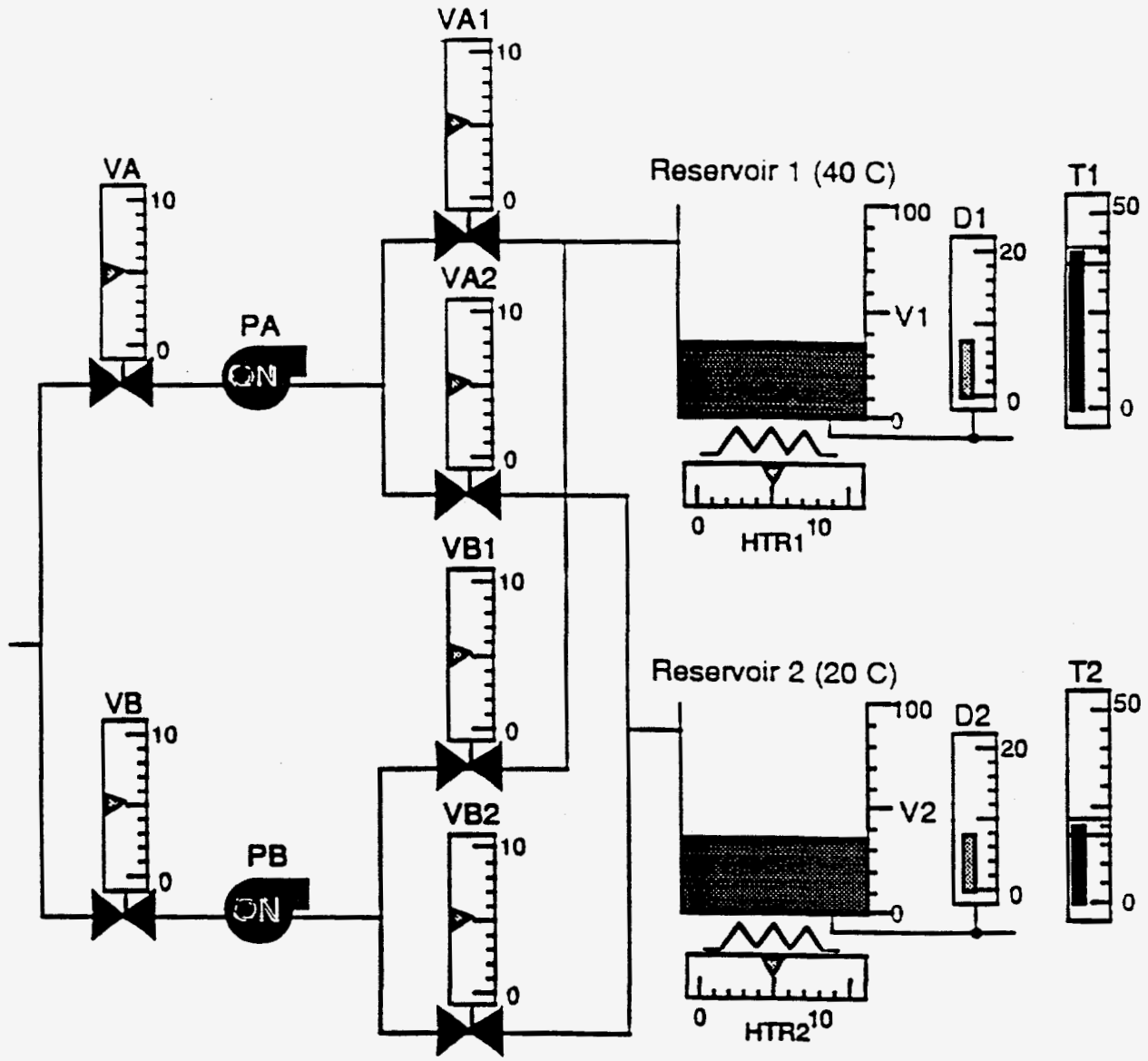


Figure 2.5a Physical (P) interface for DURESS[taken from Vicente, 1991]

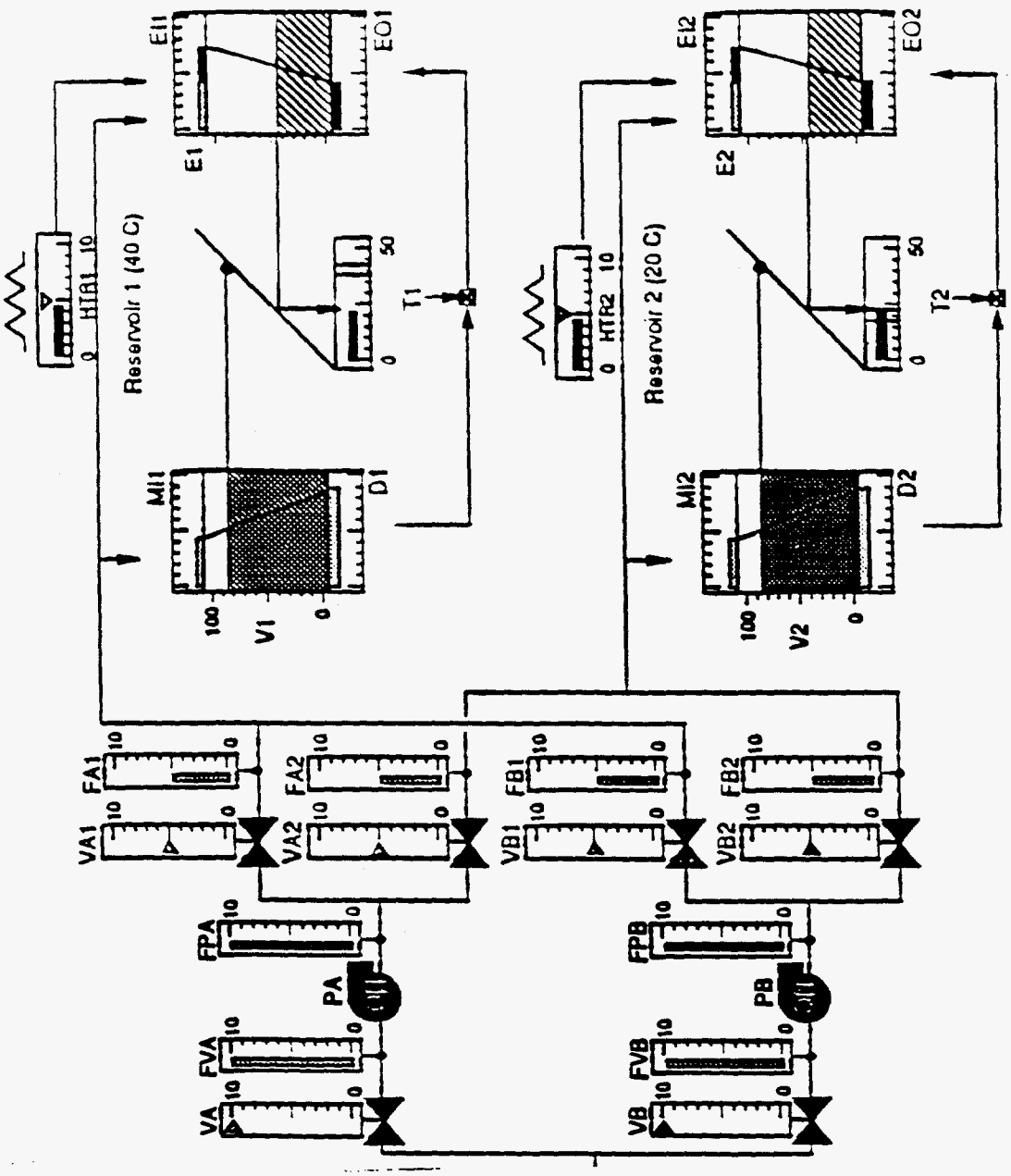


Figure 2.5b Physical + Functional (P+F) interface for DURESS[taken from Vicente, 1991]

2.3.3 Rankine cycle

The Rankine cycle display, Figure 2.6, is another application of the EID principles. The ideal Rankine cycle is a heat engine cycle composed of four phases. It is based on the principle that if the working fluid passes through the various components of the simple vapor power cycle without irreversibilities, frictional pressure drops would be absent from the boiler and the condenser, and the working fluid would flow through these components at constant pressure. Also, in the absence of irreversibilities and heat transfer with the surroundings, the processes through the turbine and pump would be isentropic.

The first phase consists of a constant pressure heat addition to a working fluid, changing its phase from liquid to vapor. In the second phase the fluid undergoes an isentropic expansion, producing work energy. In the third phase, the fluid condenses from a vapor to a liquid state in a constant pressure heat rejection process. In the fourth state, work is performed on the liquid through an isentropic compression process, which raises its pressure to complete the cycle. Each of the four phases corresponds approximately to different parts of the secondary cooling loop of a PWR.

Similar to the "star" display, the Rankine cycle represents many variables in a single graph (temperature-entropy plot) rather than separate meters. However, the quantitative values are provided to support the operators at lower cognitive levels (e.g.., temperature readings). In addition, the graphical representations of temperature and entropy also allow operators to perceive at higher cognitive levels, for example, the path of coolant and temperature differences (e.g., energy flow). The operators are free to extract information to support their tasks at any level of the hierarchy.

An evaluation was conducted by comparing the Rankine cycle display, with the conventional analog display and the analog display supplemented with animated plot of pressure temperature relations (Moray et al, 1993) The results showed that the Rankine display is better for detection and diagnosis of transients. The Rankine cycle display improved diagnosis ability by about 75% compared with the other two kinds of displays.

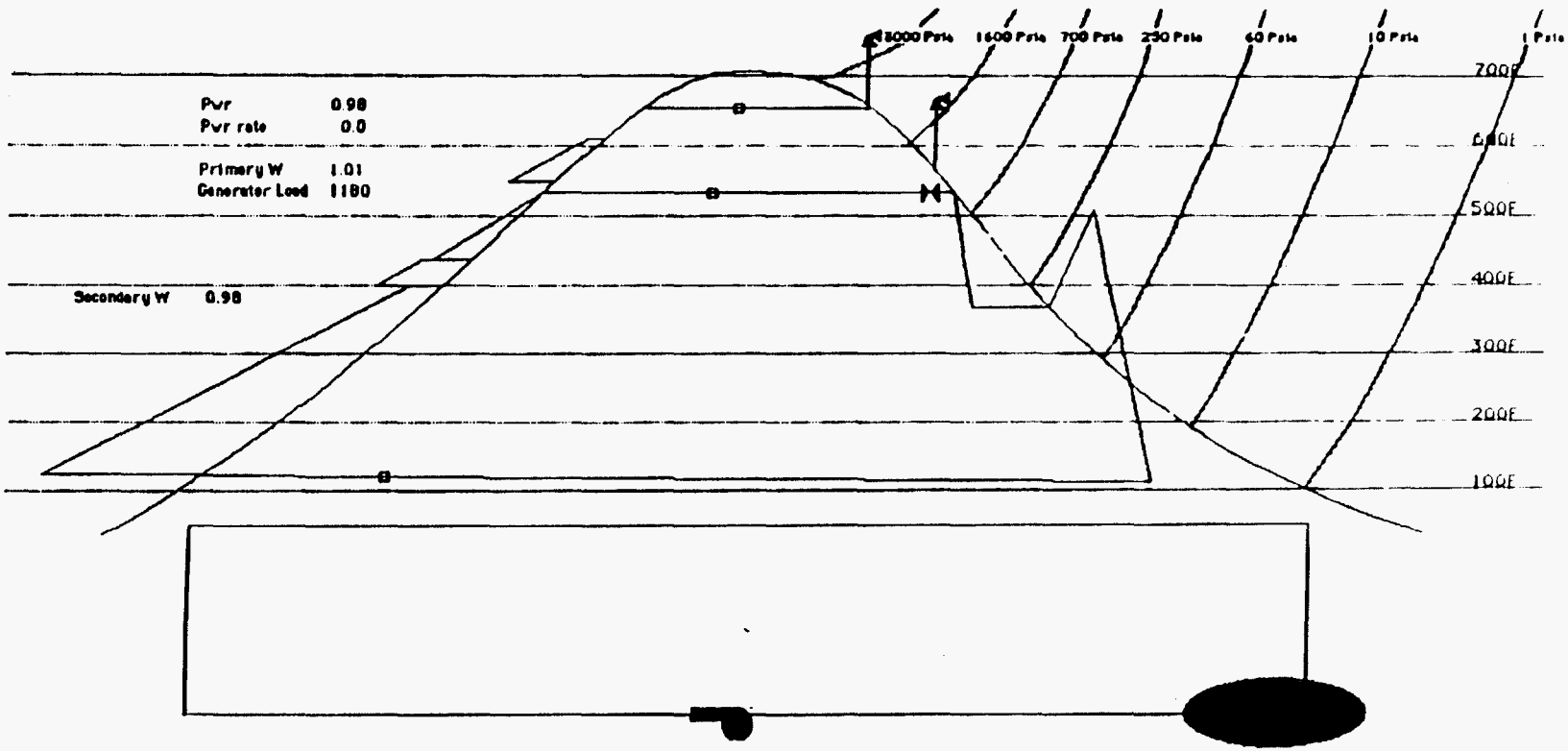


Figure 2.6 Rankine Cycle Display[taken from NUREG/CR-5977]

CHAPTER 3
THE DEVELOPMENT OF A GENERAL EID FOR PWRs: THE "BIRD'S FOOT DISPLAY"

3.1 Introduction

Based on the ideas discussed in section 2.1 - 2.3, Rasmussen, Moray, Jones, and Sanderson proposed to develop an integrated suite of EID displays for the PWR's control rooms. This thesis is part of their proposed work using Rasmussen's EID theory and the "Bird's foot display" to design a set of interface for the start up process related to the feedwater system of a PWR.

3.2 The "Bird's foot display"

The display design is based on Rasmussen's "Bird's foot display", Figure 3.1. In the "Bird's foot display", the vertical axis corresponds to the functional hierarchy and the horizontal axis represents the physical aggregation of components and systems. At the parts and components abstraction level, a set of physical components is selected and connected in an increasingly integrated configuration. These assembled components then are aligned to the specified operational state and are connected with other components and systems. This process is repeated until all required components are connected and aligned to serve goals formulated at higher levels of abstraction.

Follow the EID principle and the "Bird's foot display" design, first, the overall goals are decided to be production of electricity and safety of the plant. The abstraction level is represented by the electric output at the generator (flow of energy). At the functions level, the FW system is presented. For the physical processes, all subsystems to the FW are identified. Finally, at the parts and components level, all FW components are provided.

3.3 Procedures vs. Variables

In the "Bird's foot display", aggregation of parts and components are represented horizontally. After physical components are selected and connected, they are aligned to the next functional abstraction level. As the levels become higher, components are aggregated in an increasingly integrated configuration.

In order to implement the "Bird's foot display" design principles in this project, procedures and variables are mapped onto the "Bird's foot". Procedures are step-by-step instructions provided to the operators for conducting any plant operation, such as start up, shutdown, power operation, etc. In general, procedures correspond to the physical aggregation of components and systems.

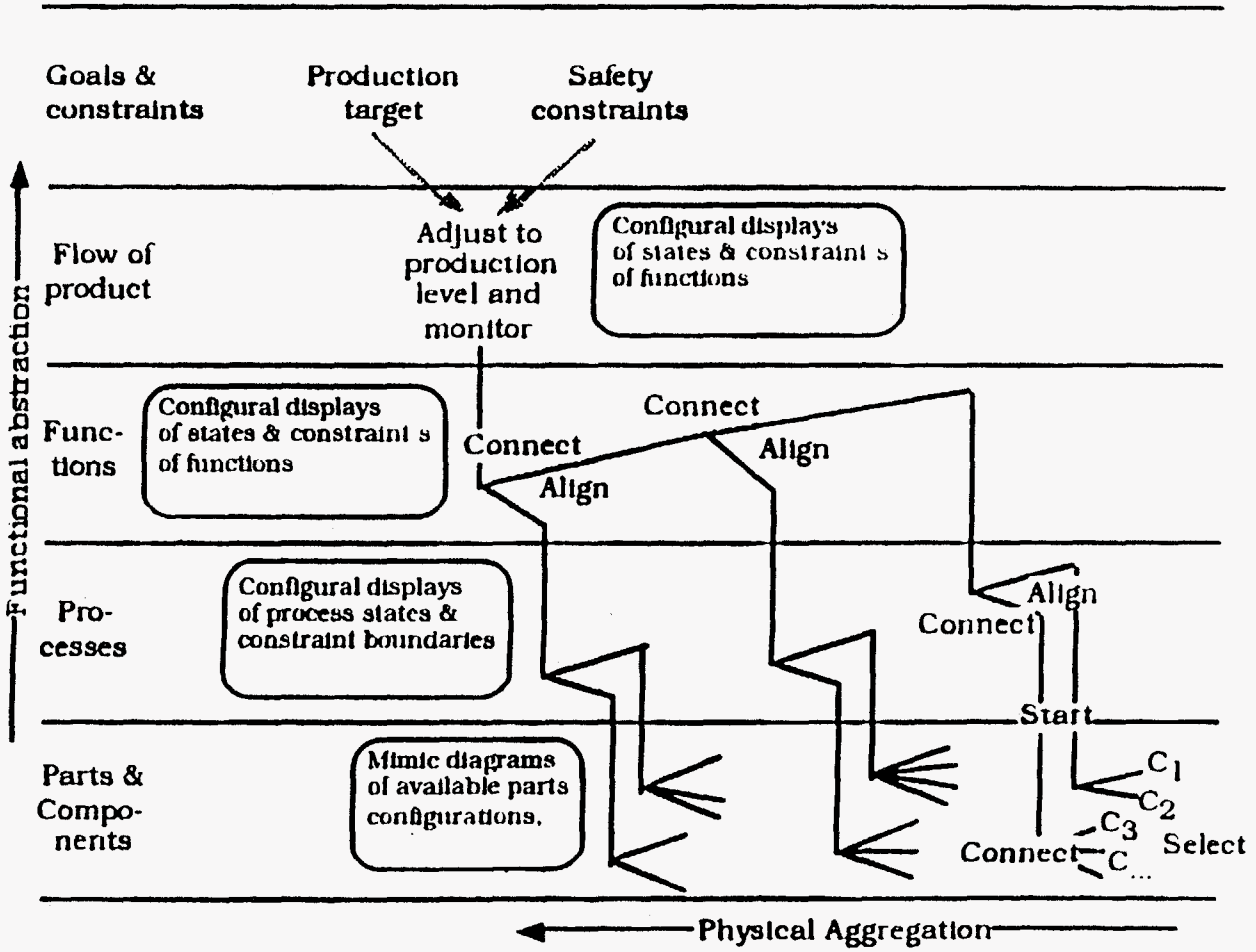


Figure 3.1 The "Bird's foot" hierarchy

The procedure chosen for this project to demonstrate the EID framework is the start up process. There are two reasons for this decision. First, the start up operation is a very lengthy and complicated process where errors are more likely to occur than for instance, during steady state operation. Because of this, start up procedures are good candidates for demonstrating fault detection and diagnosis in EID. In addition, it usually takes about two weeks to bring the plant up to power from a cold-clean core, and it involves almost every piece of equipment available. This leads to the second reason for this selection. The start up process can be described as an assembly task in functional terms which could be mapped onto the "Birds foot display" design principles. Physical components are started individually and connected with each other in sequence, then they are aligned to reach a certain state according system designs. At the new state, additional components and other systems are connected at a higher functional level and aligned in an increasingly integrated configuration. This process is repeated until all necessary components and systems are connected and aligned for a safe production.

Another important aspect of this project is the representation of variables. Variables are relevant information that is crucial to procedure execution and plant operation, such as RCS temperature and pressure. Refer back to the "Bird's foot display" diagram, from the processes functional abstraction level and above, configural displays of states and constraints are included to facilitate operations.

3.4 Overall structure

3.4.1 Introduction

The overall structure for the displays designed includes several key components. First, necessary procedures, variables and their constraints, and required hierarchical levels are identified. Second, at each abstraction hierarchy level, direct perception, direct manipulation, and affordance are presented. Third, faults are displayed through the state space diagrams and the system nodes. The following paragraphs will discuss these in detail.

3.4.2 Identification of procedures, hierarchical levels, and variables

To begin this research project, the operating procedures from the Braidwood Nuclear Power Plant and the fundamentals of nuclear physics and structures of NPP were carefully reviewed. After decided in using the start up process, a task analysis was performed on the operating procedures. All procedures related to the FW system for the start up process were selected and these procedures are used to construct the "Bird's foot displays".

Often each procedure is further divided into several steps and completion of this particular procedure requires completion of all the steps. This leads to the identification of required levels of hierarchy. For this project, generally only the bottom three levels are needed, i.e., functions, processes, and parts and components. The overall FW system is included in the functions level, subsystems to the FW system fall in the processes level, and components are categorized in the parts and components level. Operating procedures can be divided into two categories, either operation of physical components (the "toes" of the "Bird's foot") or alignment (the "leg" of the "Bird's foot"). When the procedures call for actions such as open valves, start a subsystem, or check status, they are represented by the "toes" part of the "Bird's foot". After these operations are completed, the subsystem reaches a different state by adjusting temperature, pressure, and/or flow, this alignment brings the subsystem to a higher abstraction level in order to connect with other subsystems and align, when applicable.

In addition to the operating procedures, variables are integrated into the display at different levels to support the knowledge-based behavior controls. These variables are identified and selected in two ways. The first method of selections is from the constraints that are embedded in the procedures. Certain procedures are required to be completed within some limits, such as "perform this step after temperature reaches 300 F." These variables are only presented with this particular procedure. The second method of selections takes the general constraints that are applicable for safe operation of the system. Several constraints need to be monitored throughout the entire course of operation. These variables are related to safety and production of the NPP, including the RCS temperature and pressure, power outputs, and safety limits. All variables are presented as configural displays of states and constraints.

3.4.3 Presentation of direct perception, direct manipulation, and affordance

At each level of the abstraction hierarchy, direct perception, direct manipulation, and affordance are provided when applicable. Physical components are designed to enable operators to perform tasks directly on the computer screen by clicking or dragging the mouse. This reduces the mapping problems of the gulf of execution. In addition, when actions are taken, the physical components or system nodes would provide immediate feedback by either changing color and/or texture. This would allow operators to perceive changes occurred right on the computer screen, thus minimizing the gulf of evaluation and hence achieving direct perception and direct manipulation.

The affordance is constructed with variables selected according to the previous section and their constraints for that level. These constraints are categorized into physics, Tech Specs, and operation, when possible. Physics constraints are limited by the nature of the variable, for instance, the boiling temperature of water in an open atmosphere is 100 C. Tech Specs and operation constraints are determined to allow safe operations well within the physics constraints. These constraints are presented in colors representing alarm states to provide operators essential information with direct perception capability.

3.4.4 Faults display

An important aspect of the EID displays is the ability to support the operators during a fault situation. Hence, the displays of faults are essential to the design of the interface. If a fault occurs, one of the following three things will happen. There will be either a change in the variable values or a change in the state of the physical components, or in most cases the combination of the two. If the fault only effects the variables, it will show on the state space diagrams as out of the operating constraint boundary. If the fault occurs due to a change of the state in some physical components, the mimics of these components will indicate an abnormal state (color change) on the displays and so will the subsystems and systems in which they are located. This provides operators with the means of tracing the fault up and down the hierarchy.

The construction of the display hierarchy begins with identifying FW related procedures and dividing them into subsystems. Each subsystem is further divided into subsystems, if applicable, then all components are identified. The displays are constructed so that components which serve the same function are presented in the same frame. For instance, there are four loops in a typical PWR and each loop has a 1FW009 valve and a 1FW006 valve. That means all four 1FW009 valves are presented in a frame and all four 1FW006 valves are presented in another frame, suffix A, B, C, and D are used to indicate each loop. One can click on the appropriate buttons to get from one frame to the other.

At the physical components level, only mimics of the components (e.g., valves and pumps) are provided, along with their controls (e.g., buttons and switches). These controls are located directly beneath the mimics to support operators with direct manipulation. In addition, written procedures, special notes and cautions are also provided with the frame. As the level gets higher, previous mimics are replaced by a node indicating the state of the subsystems. Also, integrated displays of states and constraints are provided to support operators at higher cognitive controls. Ideally, at the level of goals and purpose, there will be two nodes indicating the status of production and safety and various state space diagrams that provide operators with a clear understanding of the variables' relations.

3.4.5 Procedures

The plant operating procedures and the Technical Specifications (Tech Specs) are legal requirements for the NPP operations. The operating procedures are step-by-step instructions that are properly prepared and tested for operations as well as qualitative and quantitative guidelines for plant status. In most cases, these procedures are only presented on paper, but computer-based procedures may provide a better support than the paper-based procedures because of easy access to plant information while in execution (Goodstein, 1979). A major part of this project is to take the operating procedures and computerize them. For this thesis, the operating procedures are transferred from paper to computer screen using the "Bird's foot displays" principles to provide operators with clear instructions and mental models of the hierarchy.

Instead of transferring the entire procedural text from paper to computer word by word, this project takes the EID approach to transform the written procedures into a graphical display and control interface. This interface provides operators with the capability of direct manipulations of plant equipment by clicking a mouse and receiving feedback instantly.

As mentioned before, the start up process is a very lengthy and complex task. In general, the cold start up procedures are divided into 5 operational modes according to the Technical Specifications, see Table 3.1. Conditions set for these modes are based on the average coolant temperature, reactor power, and reactivity.

Table 3.1 Operational modes[taken from Braidwood Tech Specs Rev.1]

Modes Condition, K_{eff}	Reactivity	% Rated Thermal Power	Ave. Coolant Temperature
1. Power Operation	> = 0.99	> 5%	> = 350 F
2. Start up	> = 0.99	< = 5%	> = 350 F
3. Hot Standby	< 0.99	0	> = 350 F
4. Hot Shutdown	< 0.99	0	350 F > T_{ave} > 200 F
5. Cold Shutdown	< 0.99	0	< = 200 F

For the purpose of demonstrating the EID principles in NPP displays, this thesis only includes the start up procedures related to the FW system. Furthermore, it only consists of procedures from Mode 2 to Mode 1. These procedures cover a power range from approximately 16% to 80% and demand operations of various valves and pumps. In addition, they require monitoring of the RCS temperature and pressure, as well as certain individual valve temperatures and flow rates. The FW procedures related to the start up process from mode 2 to 1 are divided into 9 major steps. The following is a description of the procedures used for designing the interface.

1. FW system realignment.
*Start turbine driven FW pump.
*Stop the start up FW pump.

2. At 16% power, perform 40% steam dump for synchronization.
*Ensure that 1FW006A, B, C, & D and S/G 1 A, B, C, & D valves are open prior to synchronization.

3. Placing FW control in auto.
*Ensure turbine generator power is @ 20% (235 MW).
*Maintain S/G levels at programmed levels.
*Verify/Close 1FW 510, 520, 530, & 540 FW Regulating valves.
*Verify/Open 1FW006A, B, C, & D FW Regulating Isolation valves.
*Place FW Regulating valves in auto.
*Place FW Regulating Bypass valves controllers in manual.
*Ensure FW Regulating valves begin to open as the bypass valves are throttled closed.

4. FW main nozzle purge.
*Open FW Tempering Line Isolation valves 1FW035 A, B, C, & D.
*Slowly open FW Tempering Line Flow Control valves 1FW034 A, B, C, & D.
*Open FW Isolation Bypass valves 1FW043 A, B, C, & D.
*Manually slowly open FW Isolation Bypass Flow Control valves 1FW046 A, B, C, & D.
*Place 1FW046 A, B, C, & D valve controllers in auto.

5. Prepare 1FW009 A, B, C, & D valves.
*Select computer points for monitoring.
*Verify 1FW009 bypass flow > 120 gpm.

*Verify 1FW009's temperature > = 255F for 8 minutes.
*Verify all (or average flows) 1FW009's flow > = 120 gpm for 8 minuets.
*Place control switch for 1FW009 valves to be opened in the open position.
*Monitor FW pump and FW Regulating valves as FW Isolation valves open.
*Place 1FW009 valves control switch to auto.
*Close 1FW043 A, B, C, & D FW Isolation Bypass valves.
*Close 1FW046 A, B, C, & D FW Isolation Bypass Flow Control valves.
*Close 1FW039 S/G 1A, B, C, & D Preheater Bypass valves.
*Place controller for 1FW 510, 520, 530, & 540 FW Regulating valves in auto.

6. Place FW pump master controller to auto.
*Adjust in manual the FW pump master controller to maintain FW pressure greater than steam pressure.
*Place the FW pump master controller in auto.

7. Start idle turbine driven FW pumps.

8. At 40% power, align turbine driven FW pumps.
*Verify/Close 1ADV-65046 A/B and 1ADV-65047 A/B Gland Steam Stop Valves Drain valves.
*Verify/Close 1MS071 A/B, FW Pump Hot Reheat Steam Supply Line Drain valves.
*Verify/Close 1MS073 A/B and 1MS074 A/B, FW Pump Hot Reheat Steam Supply AOV Check Valve Drain valves.
*Verify/Close 1MS075 A/B, FW Pump Chest Drain valves.

9. At 80% power, reopen 1FW039 A, B, C, & D and S/G 1 A, B, C, & D valves.

3.4.6 Identification of variables

Variables of a NPP can be separated into two groups: derived and measured. The measured variables usually obtained from temperature sensors, pressure sensors, and level detectors out in the plant, for example, temperature of the feedwater line can be directly measured with a thermometer tapping into the pipe. These measurements are translated into electronic signals, sent to the control room, and converted back to some readable forms in a medium such as in stripe charts and pressure gauges. On the other hand, the derived variables are either calculations or abstract interpretations of some measured variable.

Through correspondence with the Braidwood nuclear power plant, a list of most commonly monitored variables for normal operation was obtained, see Table 3.2. Also from reviewing their procedures and technical manuals, several other variables were also identified and the most important ones among them were the plant safety limits. The safety limits for nuclear reactors are limits found to be necessary to protect the integrity of the physical barriers which prevent the release of radioactivity. For this project, not all variables from Table 3.2 are used and some additional ones are included.

Table 3.2 Normal operation variables

Variables	Units
Hot leg temp., Th	F
Cold leg temp., Tc	F
Excore core neutron flux monitors	% power
Turbine load	MW
Pressurizer water level	%
Pressurizer pressure	Psia
Pressurizer relief valve	Open/Closed
Rod position	Steps
Core power rate	%/sec
Taverage	F
Axial offset, ΔI	%
Quadrant power tilt ratio	no units
Power range channel deviation	%

The EID displays are intended to make constraints visible. There are three types of constraints most often found in a process plant: laws of nature, design intentions, and rules and regulations. The law of nature is the physics and basic principles behind the operation of the plant, for example, the melting point of uranium oxide fuel or saturation temperature and pressure curve. The design intention's constraints are chosen by the designer to ensure operation safety. Normally, these are built-in when equipment and systems are constructed. The constraints of rules and regulations are most conservative among the three. These constraints are place upon the process plant by government and company policies to further ensure safety of the plant and environment.

3.4.7 Safety limits

There are three safety limits for the PWR and they are the reactor coolant system (RCS) pressure, departure from nucleate boiling ratio (DNBR), and the amount of energy generated per foot (Kw/Ft.). Each of these is described below.

DNBR

The departure from nucleate boiling (DNB) is defined to be the ratio between the heat required for DNB to occur and the actual local heat flux.

$$DNBR = \frac{\text{heat flux required for DNB to occur}}{\text{actual local heat flux}}$$

When fission process is taking place, heat is generated from the release of binding energy. This heat is transferred from the fuel pellet to the zircalloy cladding then on to the coolant. As fission rate increases to increase reactor power, the cladding temperature increases and small steam bubbles will form on the cladding surface. This formation of bubbles is called nucleate boiling and it is a very important heat transfer mechanism in PWR because these steam bubbles collapse and transfer their energy to the coolant. However, if the steam bubbles cover a large percentage of the cladding surface then they would insulate the surface from the coolant, which may cause cladding temperature overheating and eventually cladding failures. Recall from the reactor physics section that the cladding is one of the barriers to prevent the release of radioactivity into the environment.

Therefore the departure from nucleate boiling (DNB) must be prevented and the derived variable for this is the DNBR. If DNBR is greater than one, the reactor can be assumed to be operating below the nucleate boiling heat transfer region. If DNBR equal to one, great difficulty exists in determining exactly what will happen. Therefore, a value greater than one has been conservatively chosen as the DNBR limit.

Power density (Kw/Ft.)

This safety limit also concerns the integrity of the cladding barrier. The power density limit is derived to prevent centerline fuel temperature from exceeding the melting temperature of uranium oxide. The melting temperature of the fuel is about 5000 F. As temperature of the uranium oxide fuel approaches its melting point, the fuel pellet expends and can cause excessive material stress on the cladding. This in turn may cause cladding

failure and release of fission product gasses. Since fuel temperature is not directly measurable, it is calculated in terms of energy production per foot of fuel rod (Kw/Ft.).

RCS Pressure

The third safety limit is the RCS pressure, the second barrier of PWR. The normal operating RCS pressure for the Braidwood NPP is 2235 psig and the Tech Specs limit is 2735 psig.

3.4.8 Other variables

Other important variables selected for display include temperature, pressure, generator level, reactor power, turbine-generator load, and pressurizer level and pressurizer pressure.

RCS pressure and temperature

In a PWR, there is a close coupling between the RCS temperature and the RCS pressure. The RCS pressure is maintained above the saturation pressure where boiling could occur and it is controlled by the pressurizer. During start up, temperature and pressure are closely monitored and controlled to ensure proper operation. The start up is divided into five modes by temperature and pressure and they are:

mode 5 --> 4, Temp.: 160 F --> 200 F	Pressure: 100 psig --> 325 psig
mode 4 --> 3, Temp.: 200 F --> 350 F	Pressure: 325 psig --> 425 psig
mode 3 --> 1, Temp.: 325F --> 547 F	Pressure: 425 psig --> 2235 psig

When entering and leaving an operational mode, there are checklists to make sure procedures are completed and ready for the next events. Due to the importance of temperature and pressure variables, a graph is developed for the cold start up process. The temperature for each mode is illustrated as well as the RCS design temperature (constraint of design intentions). On the pressure side, the normal operating pressure and the design pressure are also drawn to reveal the constraints. In addition, a curve is interpolated by connecting values of these two variables to illustrate the preferred path for increasing temperature and pressure.

Reactor power and turbine load

Reactor power and turbine-generator load represent the output (production) of the NPP. The power outputs are expressed in the unit of KW and as percentages. Normally,

NPP personnel express reactor power in percentage and turbine-generator load in MWe (mega watt electric). In general when all plant equipment is operating efficiently, the percentage of thermal output corresponds to the percentage of electric output, i.e., a reactor operating at 80 % of rated thermal power should generate approximately 80 % of its designed electric power (a 3000 MWt reactor operating at 80 % capacity (2400 MWt) would generate approximately 800 MWe). However, in some cases, certain equipment failures would cause a lower efficiency of the thermal to electric energy conversion. Thus, by presenting both power graphs in this format, operators can determine if the system is operating properly by looking at the difference between the percent of electric output and the percent of thermal output. Operators can perform this task with the goal of keeping the percent of electric output close to the percent of the thermal output by adjusting feedwater flow rate, for example.

Pressurizer level and pressure

The pressurizer of a PWR is located on one of the hot leg of the RCS to control pressure in the system. It contains a mixture of water and steam to maintain temperature at saturation for the desired pressure. When it is desired to increase the reactor pressure, the heaters in the pressurizer are energized to raise temperature and thus pressure. On the other hand, when it is desired to decrease the pressure, coolant is sprayed into the pressurizer to reduce temperature and thus lower the pressure. However, if the pressurizer is completely filled with water (going solid), then this pressure controlling ability is no longer effective. This was the reason that operators at TMI stopped coolant flow to the reactor because they thought there was too much water in it already and they did not want the pressurizer to "go solid". Therefore, it is important to maintain the correct steam/water ratio in the pressurizer by monitoring and controlling its pressure and level.

Generator level

The steam generators are heat exchangers. They are designed so that the radioactive primary coolant flows through the tube side and the clean secondary coolant (feedwater) flows through the shell side of the generator. The feedwater receives heat from the reactor coolant and boils away into steam. If there is too little or no feedwater, reactor heat can not be removed thus may cause overheating in the core. If there is too much feedwater in the S/G, the quality of steam is compromised, thus reduces the efficiency. Therefore it is important to maintain the steam generator level within desired range.

CHAPTER 4
DESCRIPTION OF THE EID DISPLAYS

4.1 Introduction

The arrangements of displays are presented in the order of the operating procedures. There are nine major steps to the start-up of the FW system and each major step is represented as a node in the main display. Displays can be categorized into 3 groups according to their functional abstraction hierarchical levels. There are the functions, processes, and the parts and components levels going down the hierarchy. In the functions level, FW system is monitored and controlled and configural displays of states and constraints are presented. The processes level includes subsystems as well as some components. For the parts and components level, mimic diagrams of parts configurations are provided for manipulation. The following paragraphs will discuss each display in the sequence of the start-up procedure. Due to the amount of displays involved, all graphs are included at the end of this chapter.

4.1.1 Main FW display

Figure 4.1 is the main FW display and it is categorized as a functions level display where only the general function of the FW system is monitored. In this diagram, each step for the FW start up is represented by a node. The main display includes the operating procedures in the order from left to right. It also has computer monitors that display variables and constraints as well as a mimic diagram of the entire FW system. In this case, there are four computer monitors and each one can be enlarged by clicking on the button located at the lower left-hand corner.

4.1.2 Temperature vs. pressure plot

The first CRT display, Figure 4.2, is a temperature vs. pressure time plot. As the FW start up procedures progress, the RCS temperature and RCS pressure are plotted on the display. In addition, the constraints for the RCS temperature are provided for operational modes 3, 4, and 5 (normal operation). and the constraints for pressure are provided as normal operating pressure and the Tech Specs pressure limits. These constraints show the affordance of operation. The solid line shows the time history of temperature and pressure; the end of the line shows the current state. The dotted lines indicate the constraints for these variables. Following the principles of EID, the thermodynamic relations between temperature and pressure are provided perceptually, and hence operators can perform without having to resort to higher levels of cognitive control.

4.1.3 Mimic diagram

The second CRT display, Figure 4.3, is a mimic diagram of a generic PWR FW system. When implemented, each object will act as a light that indicates the status of the component. This diagram is useful in that it provides a spatial relation of the parts and components. Furthermore, if some components need to be shut down for maintenance or due to malfunctions, this display will provide operators with the capability to redirect flow path and start the redundant components.

4.1.4 Safety limits graph

Keeping the constraints from Chapter 3 in mind, an integrated safety limit graph is constructed similar to the "star" display. In this graph, all three variables are shown with their constraints in the form of an equilateral triangle (all three sides are the same length). It is scaled so that the constraints of rules and regulations (operational constraints) form the inner triangle, the design constraints form the middle one, and the physics constraints form the outer triangle. During normal operation, the DNBR, the Kw/Ft., and the RCS pressure are not exceeding the rules and regulations' limits, lines connecting these three values (which form a triangle) will be shown inside the inner triangle, thus instantly tells operators that the safety limits are within range. If any limit exceeds the operational constraints, the values would fall outside of the inner triangle, hence alert the operators.

Figure 4.4 is the third CRT display and it is designed to reveal constraints of the three safety limits in a single graph. The three safety limits are DNBR, RCS pressure, and Kw/Ft. and each of these limits has an operational constraint as well as some physics constraints. Using these limits as boundaries, an operation triangle is created. This provides operators with the information that as long as the green triangle is within the white boundaries, the system is operating within limits.

4.1.5 Electrical output display

The last CRT display, Figure 4.5, presents the thermal output of the reactor and the electric output of the turbine-generator. This provides operators with a constant feedback of the power generated and sent to the electrical grid.

4.2 Use of displays

Each node in the functional level is a representation of more detailed procedures. For instance, when the first node is selected for FW system realignment, a new display, Figure 4.6, is presented with further instructions. Again, following the left to right order, operators need to start a turbine driven FW pump and then stop the start up FW pump. In

Figure 4.6, a subsystem (the turbine driven pumps) and components (motor driven FW pump and the start up FW pump) are all included in the process level. When the node for the turbine driven pumps is selected, the a new display of only the pumps will be presented in the parts and components level, see Figure 4.7. Figure 4.7 shows two pumps, each with its own run/stop button and manual/auto switch for controls.

When this procedure is completed, the computer program will bring back the main FW display, Figure 4.1, with updated variable states and procedure status. When the second node is selected for 40% steam dump for synchronization at 16% power, Figure 4.8 is brought up on the screen for opening of the 1FW006 valves. After that, the S/G valves are opened in Figure 4.9. Also in Figure 4.9, the 1FW006 valves' node indicates the status of the components. When both sets of valves meet the requirements, the display will return to the main FW system again with updated information.

Continuing with the procedure, the third node represents the placing of FW control in auto. When this node is selected, a more detailed instruction is provided in Figure 4.10. Due to the nature of this procedure, more variables and constraints are required and they are presented as configural displays specifically designed for this operation, Figure 4.11 and Figure 4.5. Figure 4.11 shows the S/G levels which need to be maintained at programmed levels for this step. Figure 4.5 is the thermal and electric power output graphs. In addition, each node Figure 4.10 will lead to parts and components level displays where operations take place, such as in Figures 4.12, 4.9 and 4.13. Figure 4.12 illustrates various controls for the 1FW510/520/530/540, FW Reg valves. There are manual/auto and open/close controls for the valves as well as manual/auto switches for the controllers of the valves. On the other hand, the FW Reg Bypass valves are throttle valves and as shown in Figure 4.13, the valves can be in any position between fully close and fully open with manual/auto switch controllers.

After FW control is placed in auto, again Figure 4.1 is brought up to allow the selection of the next operation, FW main nozzle purge, Figure 4.14. In addition to note and caution, this display contains many nodes for parts and components level displays. Figure 4.15 is the display for the 1FW009, FW Isolation valves. These are throttle valves with control switches for open/close and manual/auto. Figures 4.16, 4.17 and 4.18 are for valves 1FW035 (FW tempering Line Isolation valves), 1FW034 (FW tempering Line Flow control valves), and 1FW043 (FW Isolation Bypass valves), respectively. These are displays for opening and closing valves. Figure 4.19 is a display for the 1FW046, FW Isolation Bypass Flow Control, valves with open/close buttons and manual/auto switches.

The next step is to prepare 1FW009 valves, Figure 4.20. For this procedure bypass flow rate and temperature through the valves need to be monitored and these are in

the CRT. Figure 4.21 shows both purge temperature and purge flow for each of the valves and it also includes constraints by indicating the reference values of each valve. Figures 4.22 and 4.23 are mimic diagrams of the 1FW009 throttle valves. In Figure 4.22, control switches are placed in the open position and in Figure 4.23 a second set of control switches is placed in the auto positions. Figure 4.24 shows closing of the 1FW043 valves. When this step is complete, Figure 4.1, the main FW system display indicates this information in the node and is ready for placing FW Pump Master Controller in auto, Figure 4.25.

Figure 4.25 has one CRT for displaying FW and steam pressures. FW pressure can be adjusted with the controller and 1FW012, FW Pump recalculating valves, are operated in Figure 4.26. After this, the node for idling turbine driven FW pumps is selected from Figures 4.1 and 4.7 will be brought up for this procedure.

At 40% power, turbine driven pumps need to be aligned. Figure 4.27 shows the necessary components and Figures 4.28, 4.29, 4.30, and 4.31 are the mimics and instructions for the valves to be verified and closed. At 80% power, 1FW039 valves and S/G, Preheater Bypass, valves are reopened, see Figure 4.32.

When all steps are completed and operating normally, the main FW system display, Figure 4.1, will be presented and all lower hierarchical level displays are removed. This functions level diagram contains all lower level information (through indications of the nodes) and configural displays of states and constraints for safe operations.
means the valve is open.

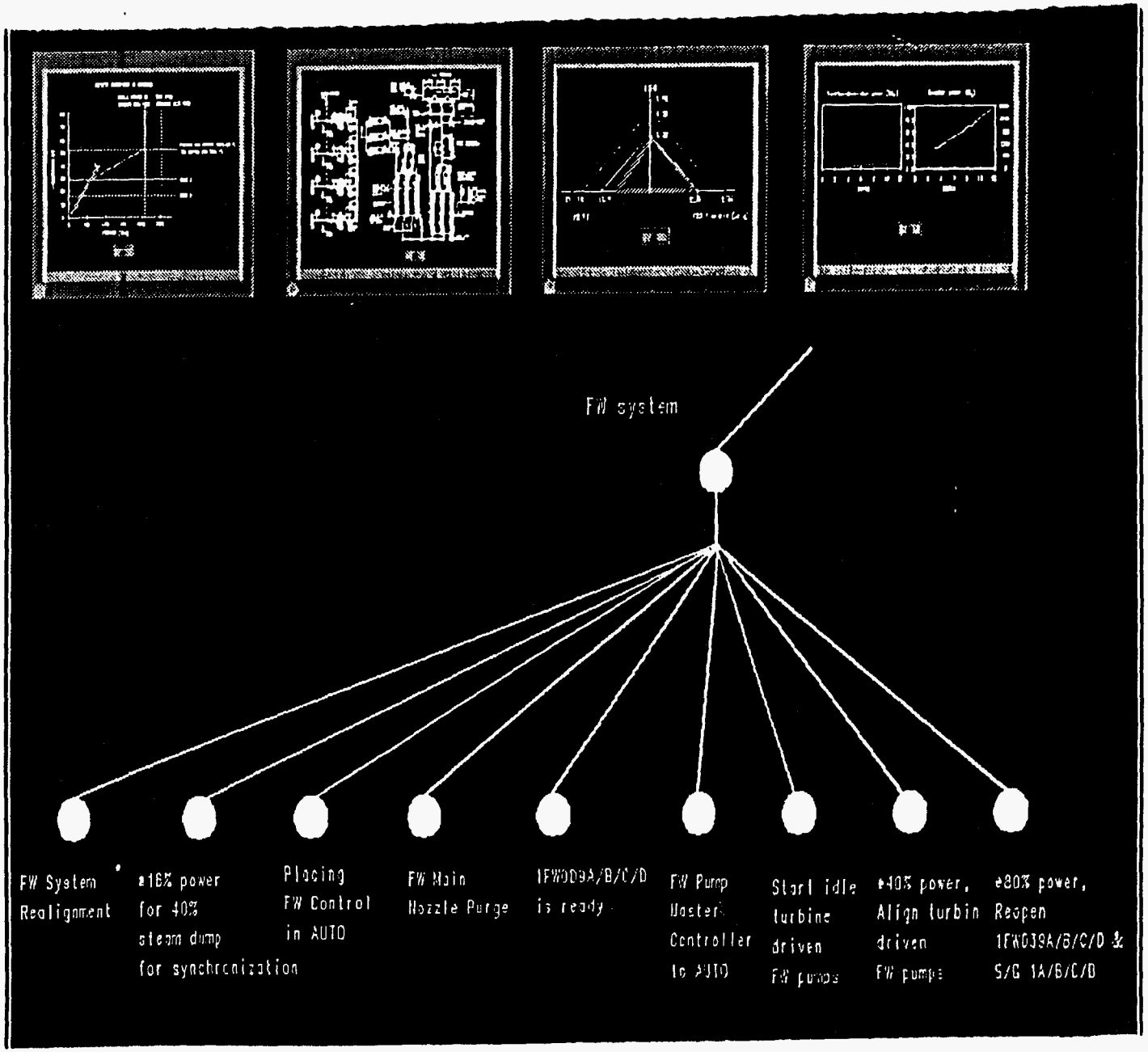


Figure 4.1 Main FW display

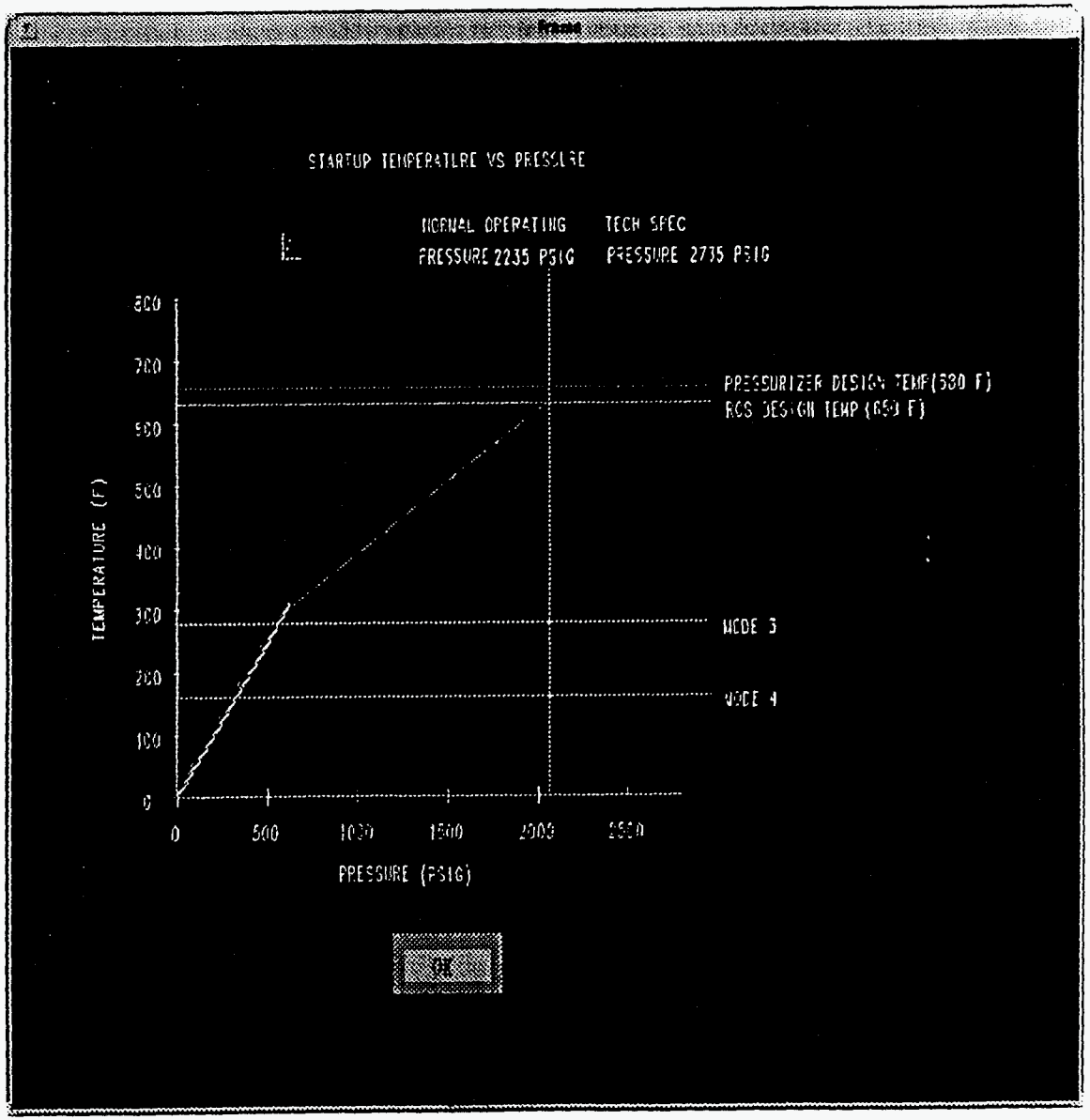


Figure 4.2 RCS Temperature/Pressure plot

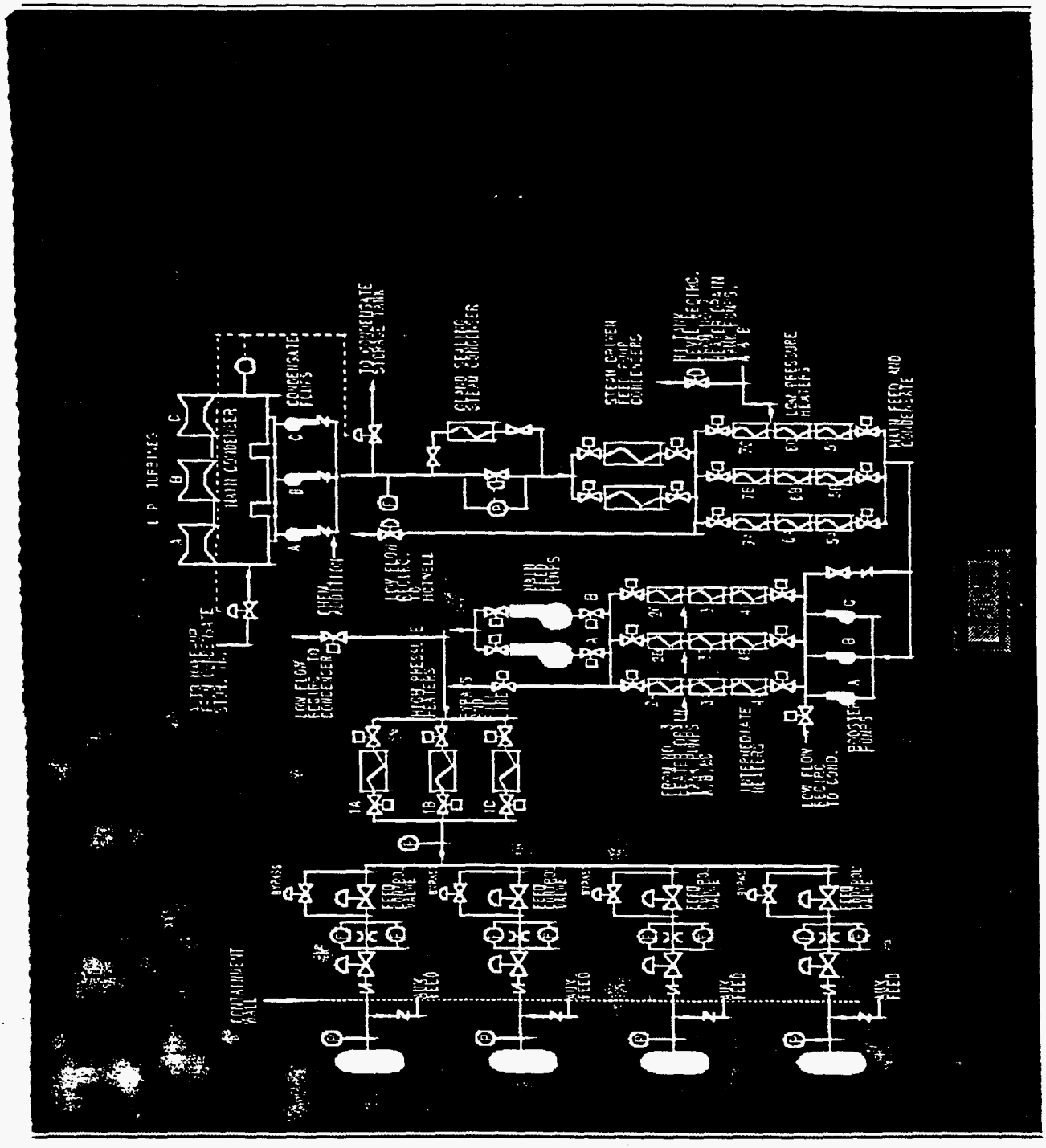


Figure 4.3 Mimic diagram of the FW system

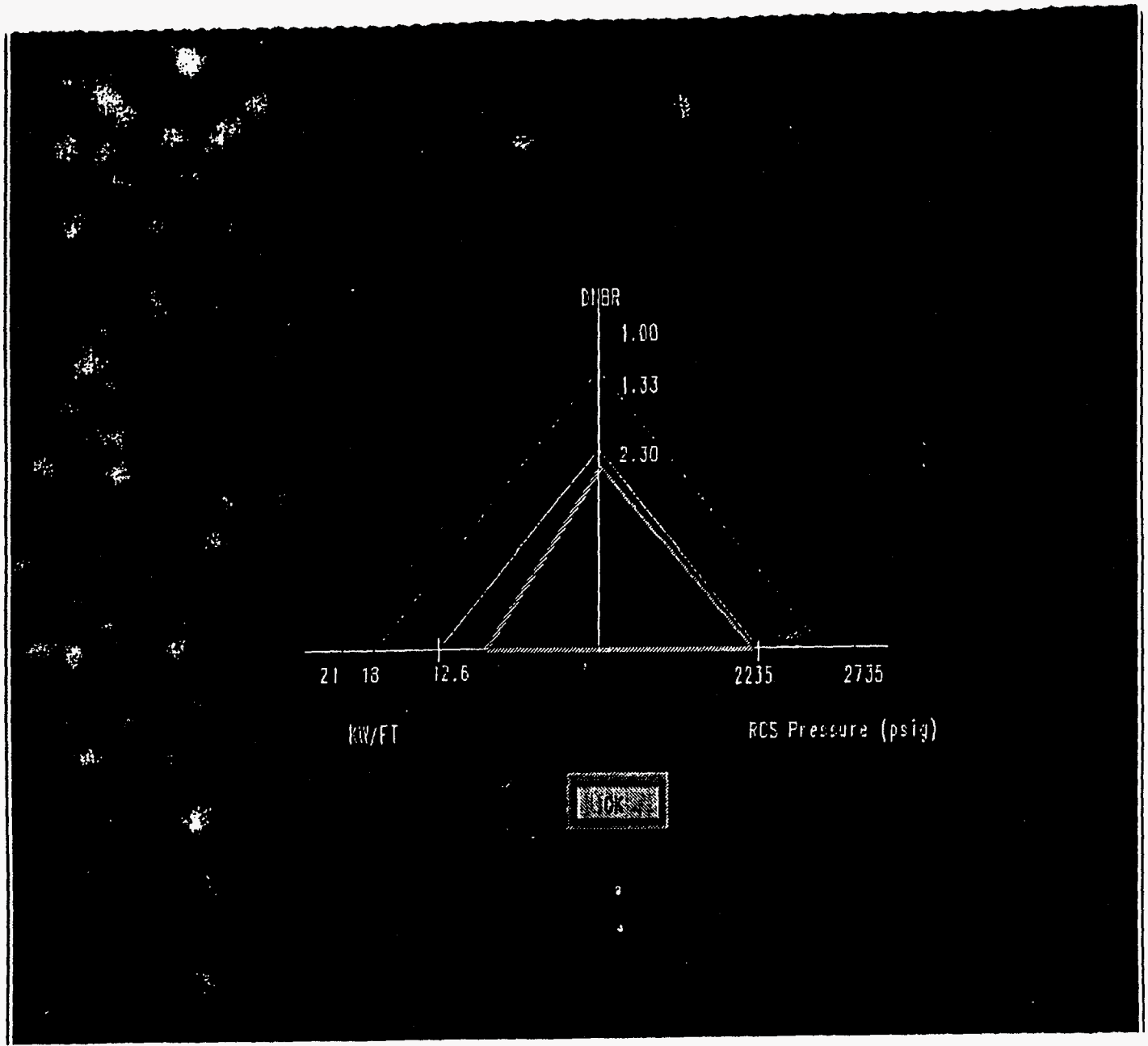


Figure 4.4 Safety limits graph

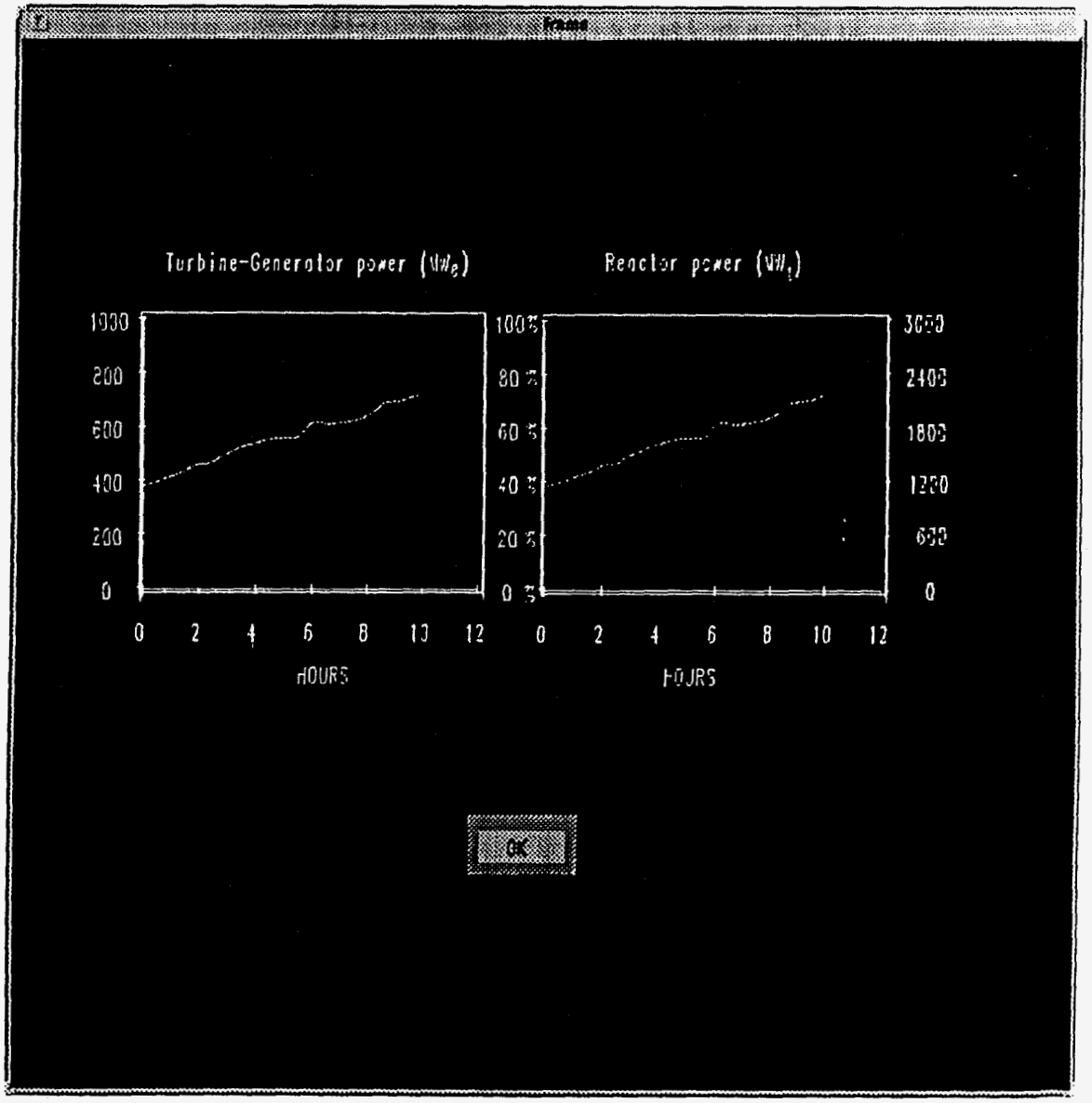


Figure 4.5 Electrical output display

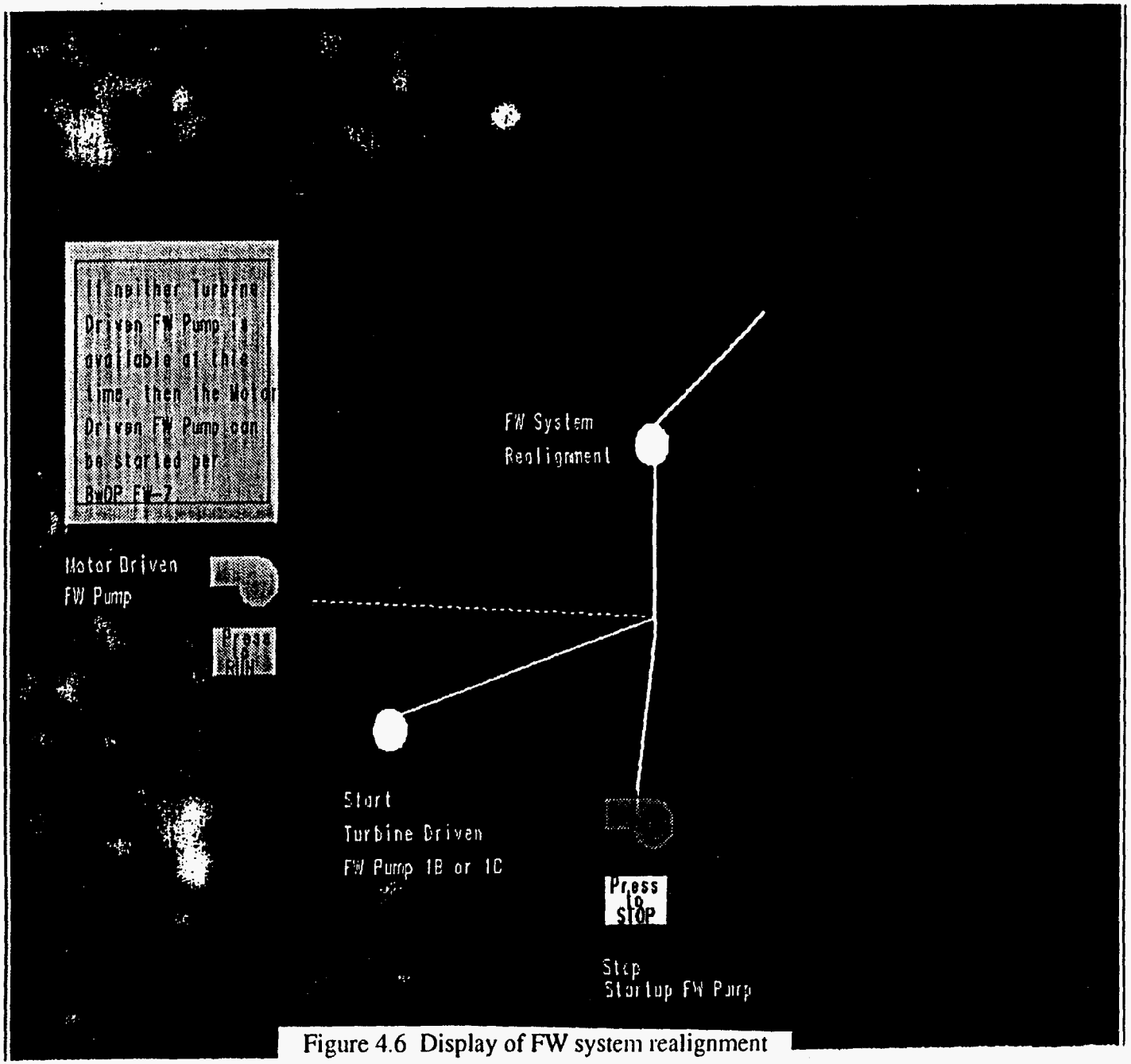


Figure 4.6 Display of FW system realignment

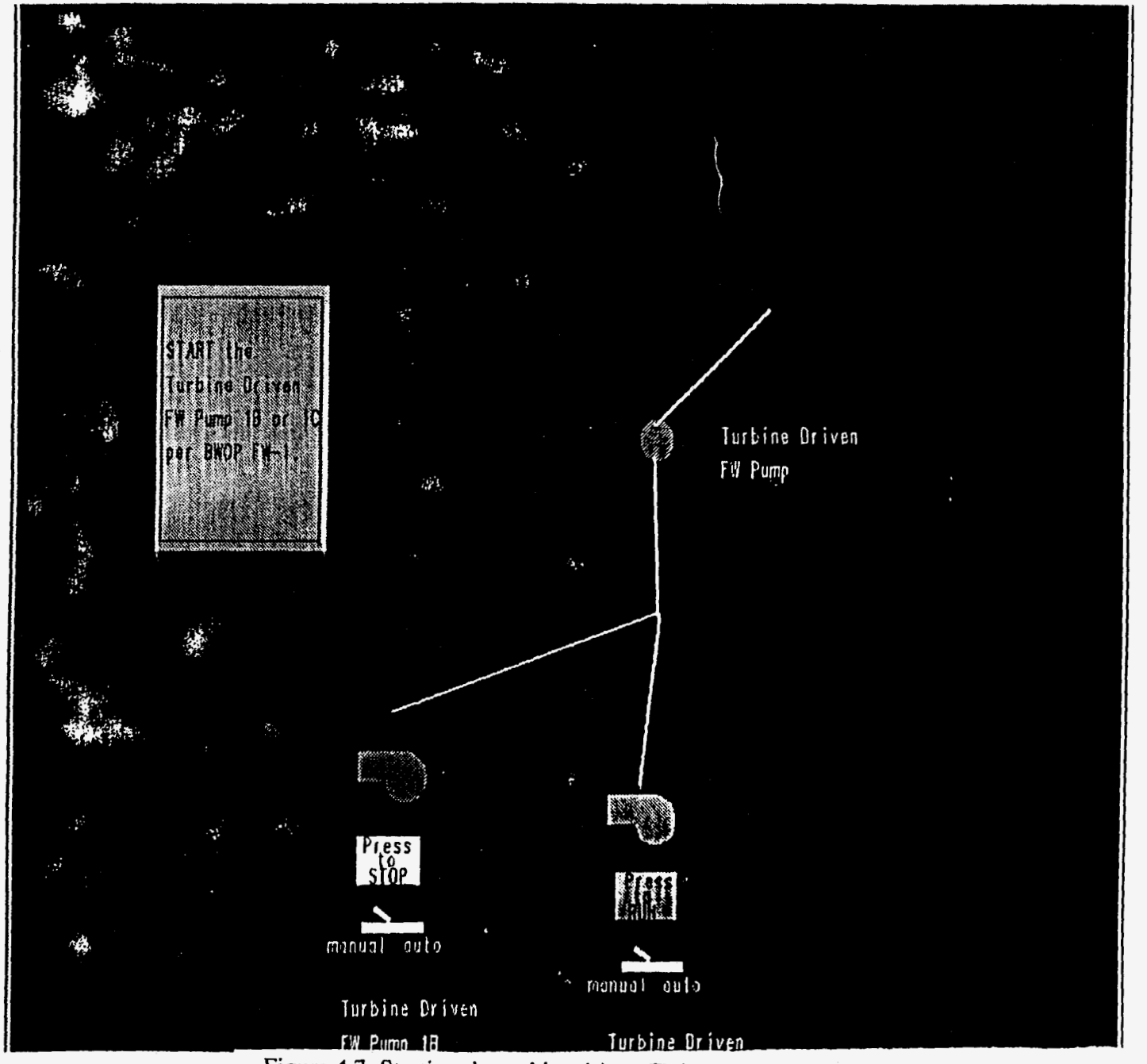


Figure 4.7 Starting the turbine driven FW pumps

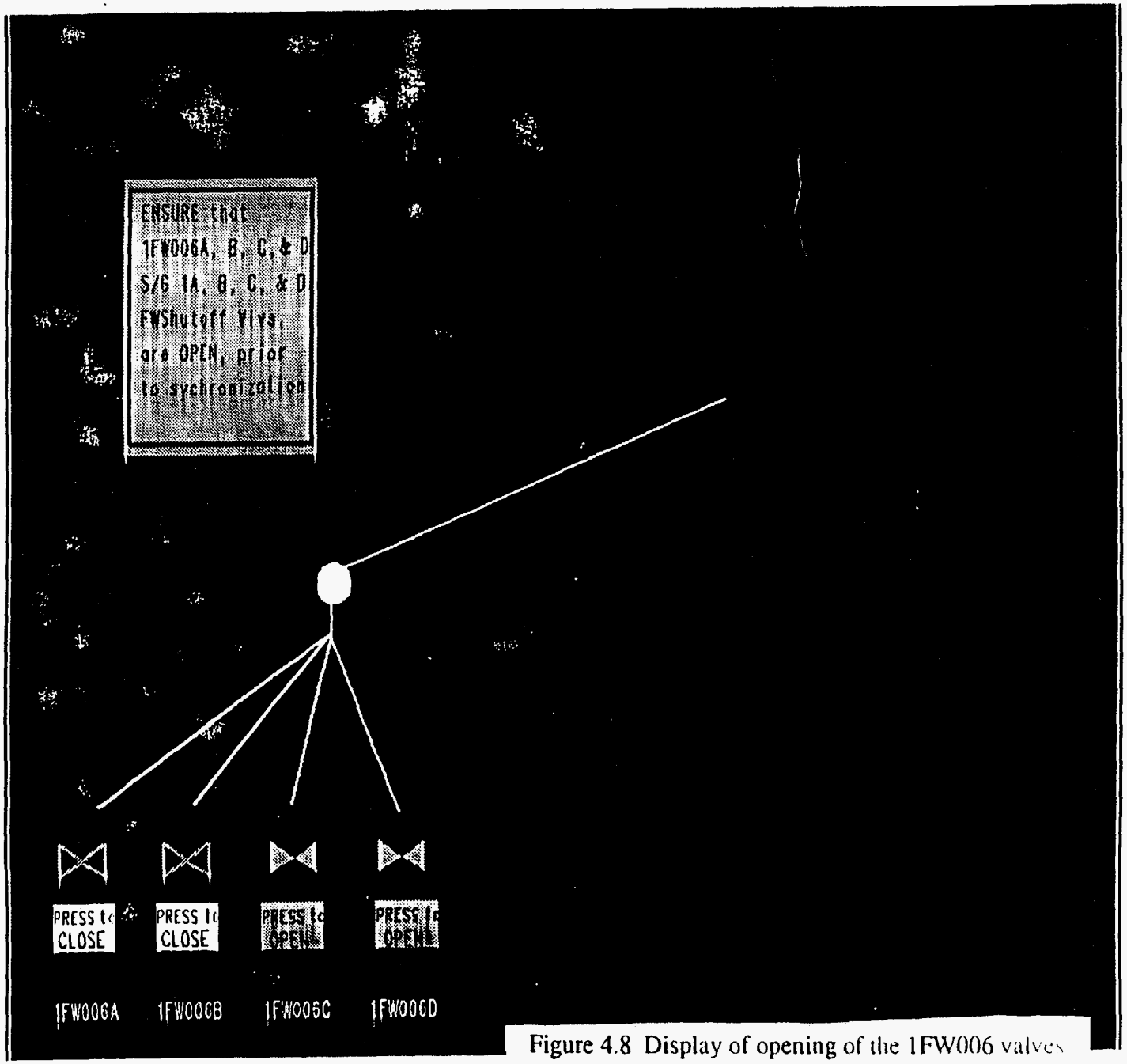


Figure 4.8 Display of opening of the 1FW006 valves

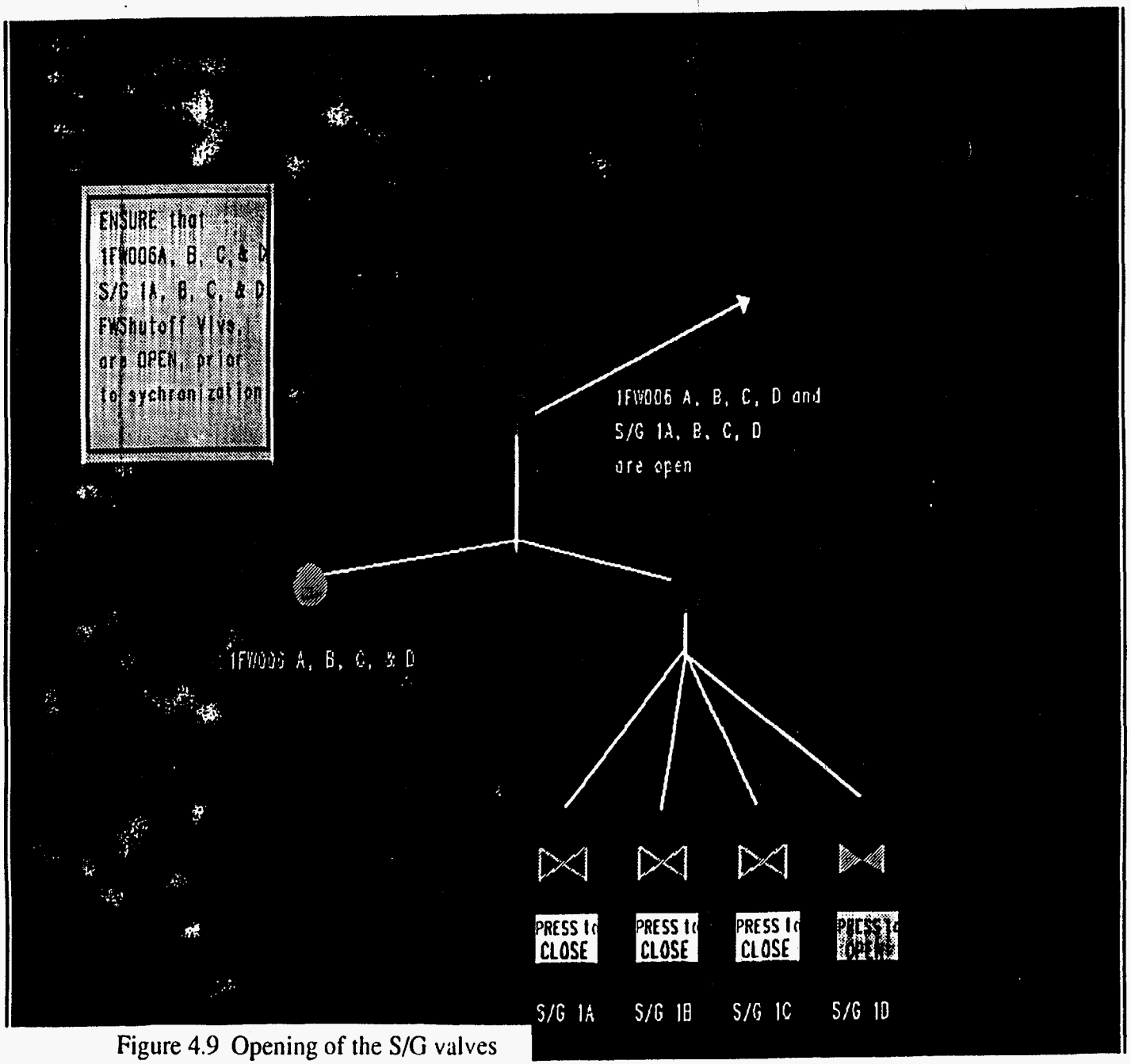


Figure 4.9 Opening of the S/G valves

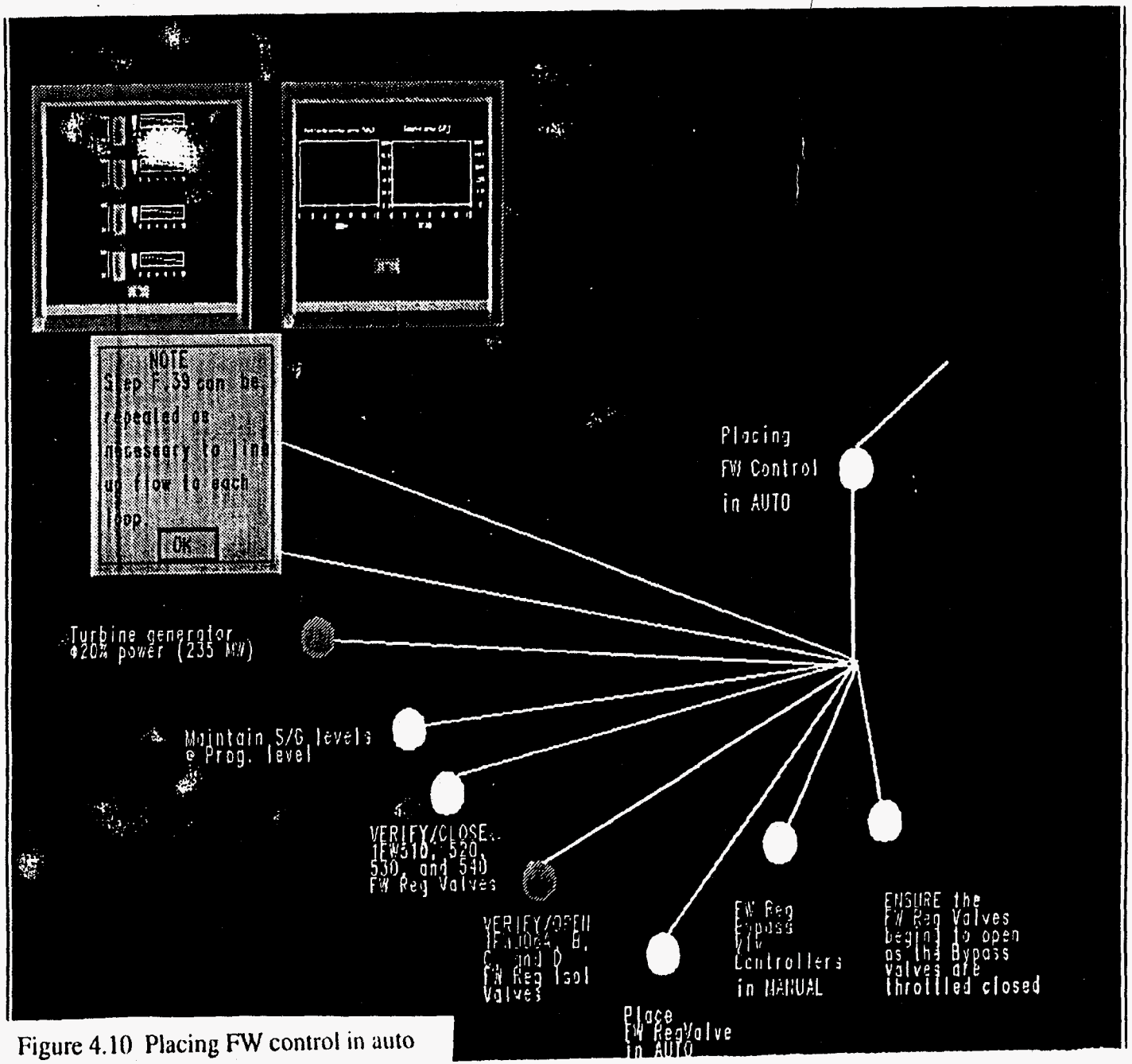


Figure 4.10 Placing FW control in auto

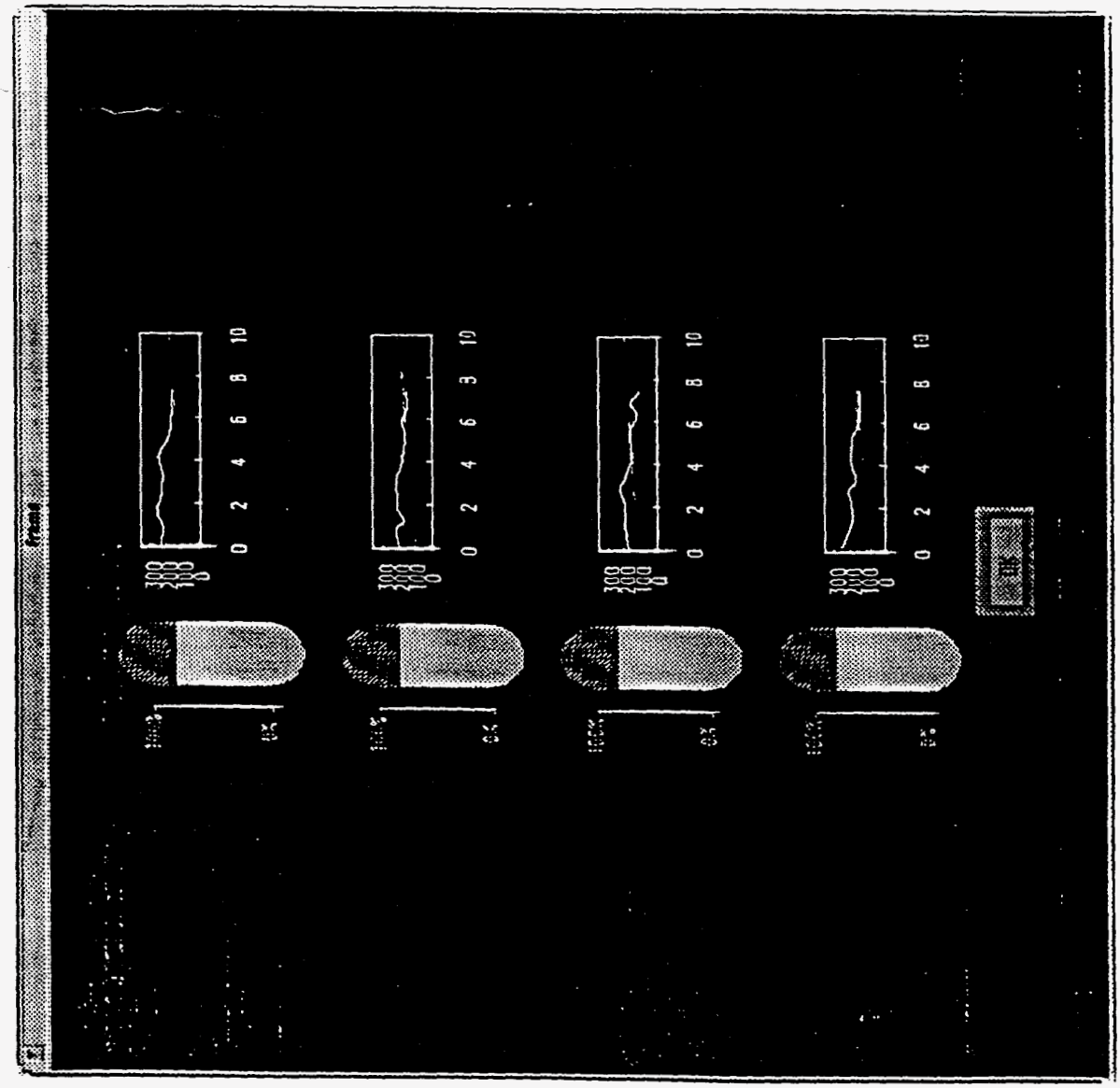


Figure 4.11 S/G levels diagram

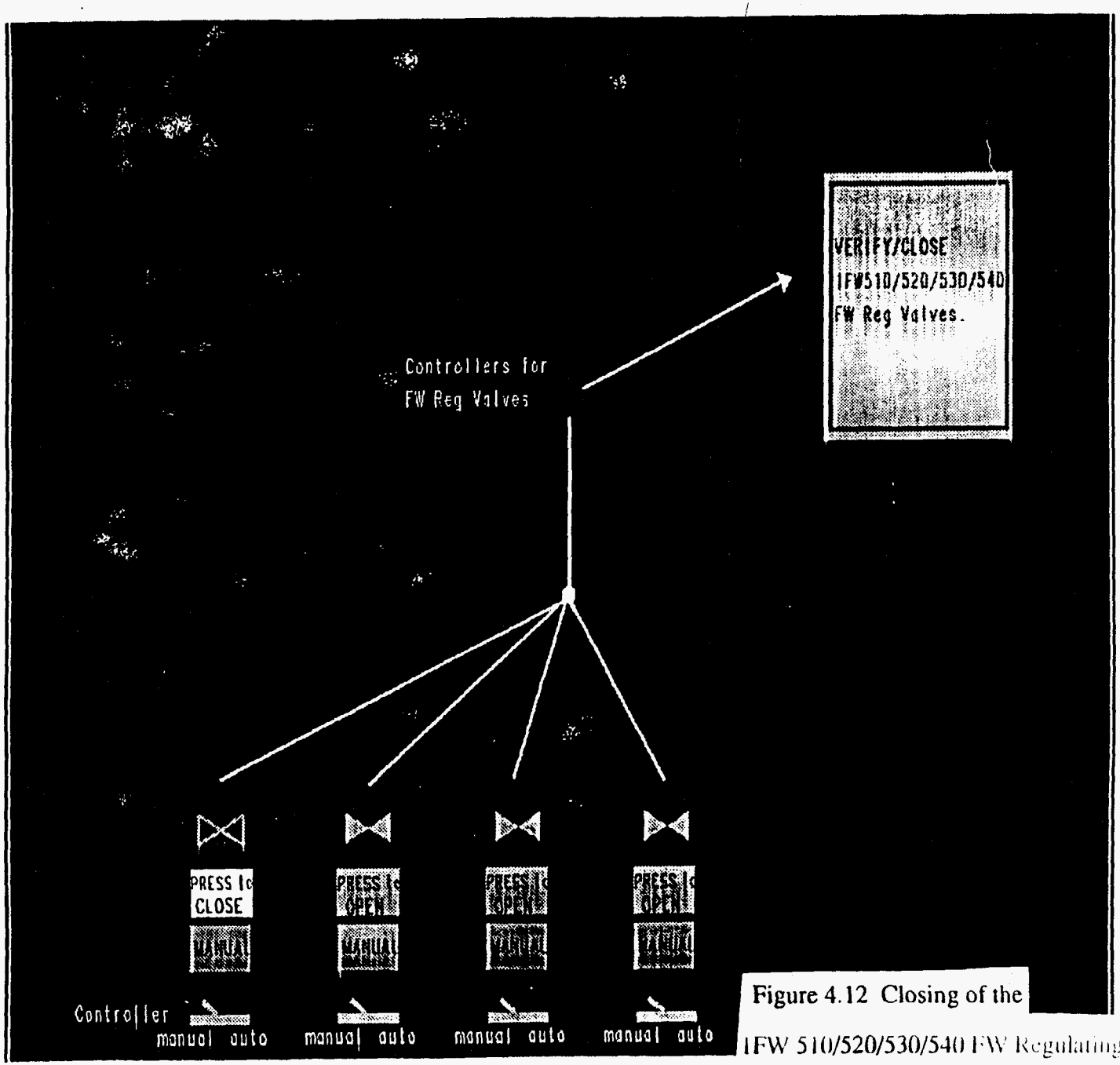


Figure 4.12 Closing of the 1FW 510/520/530/540 FW Regulating valves

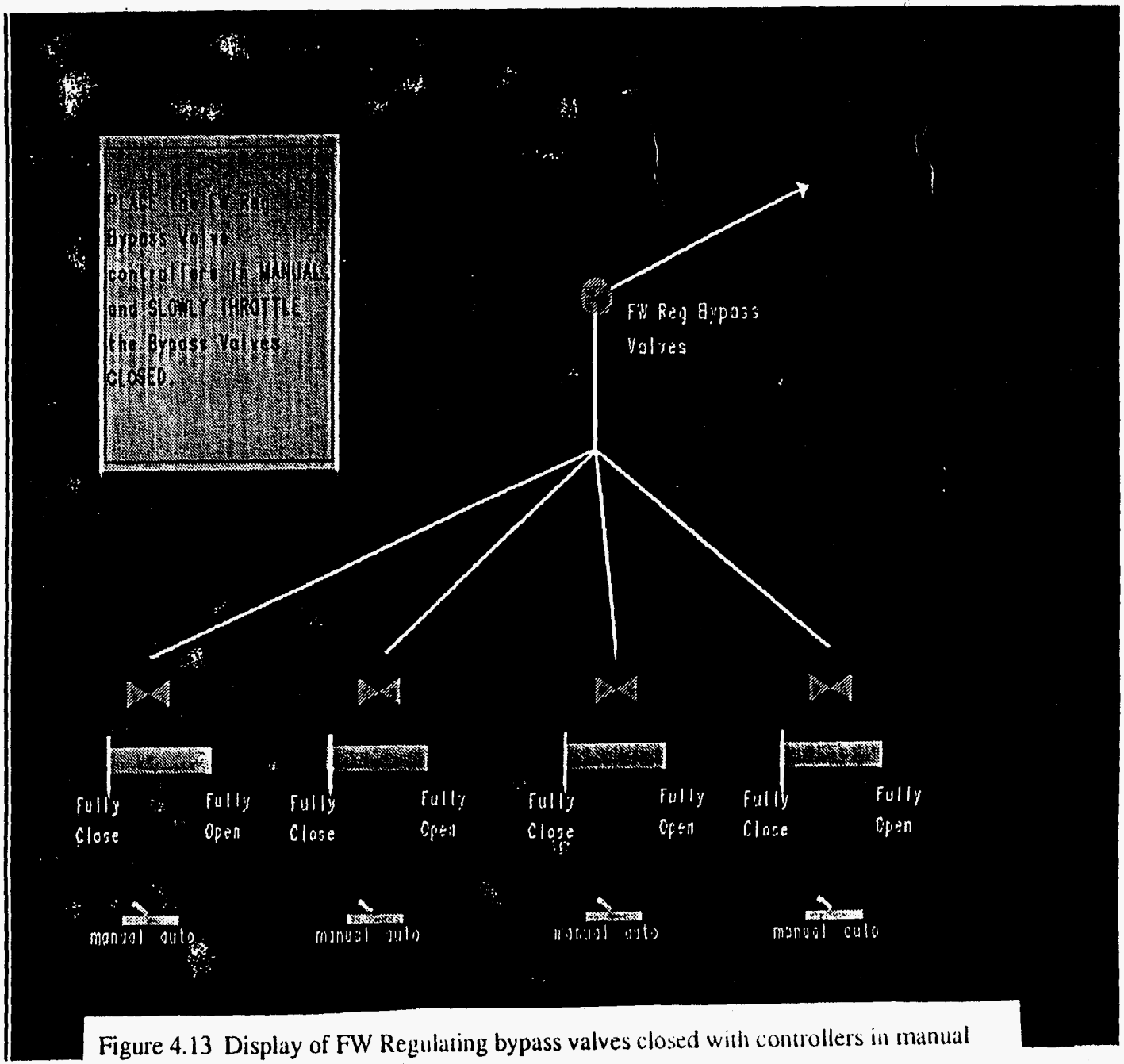


Figure 4.13 Display of FW Regulating bypass valves closed with controllers in manual

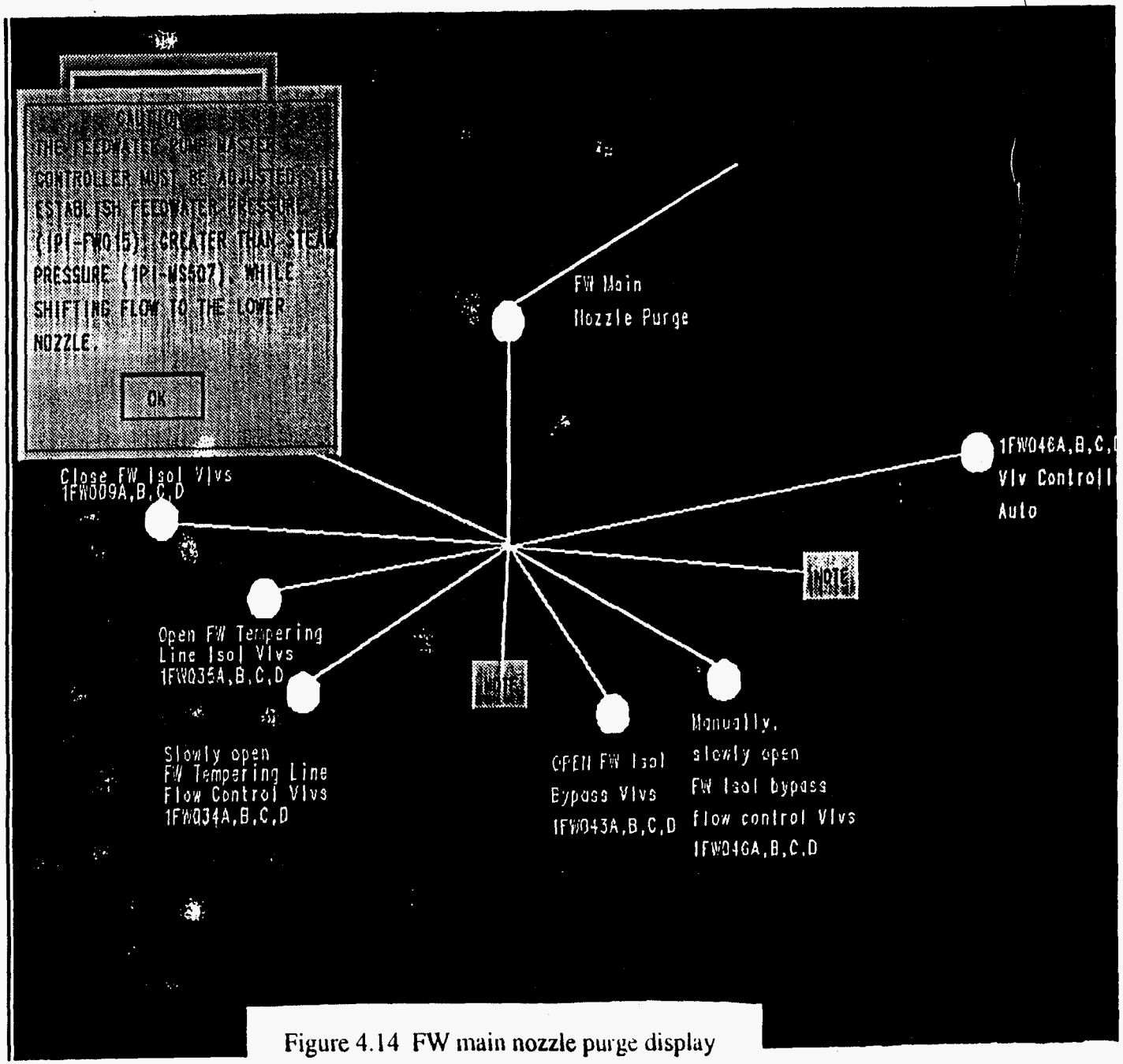


Figure 4.14 FW main nozzle purge display

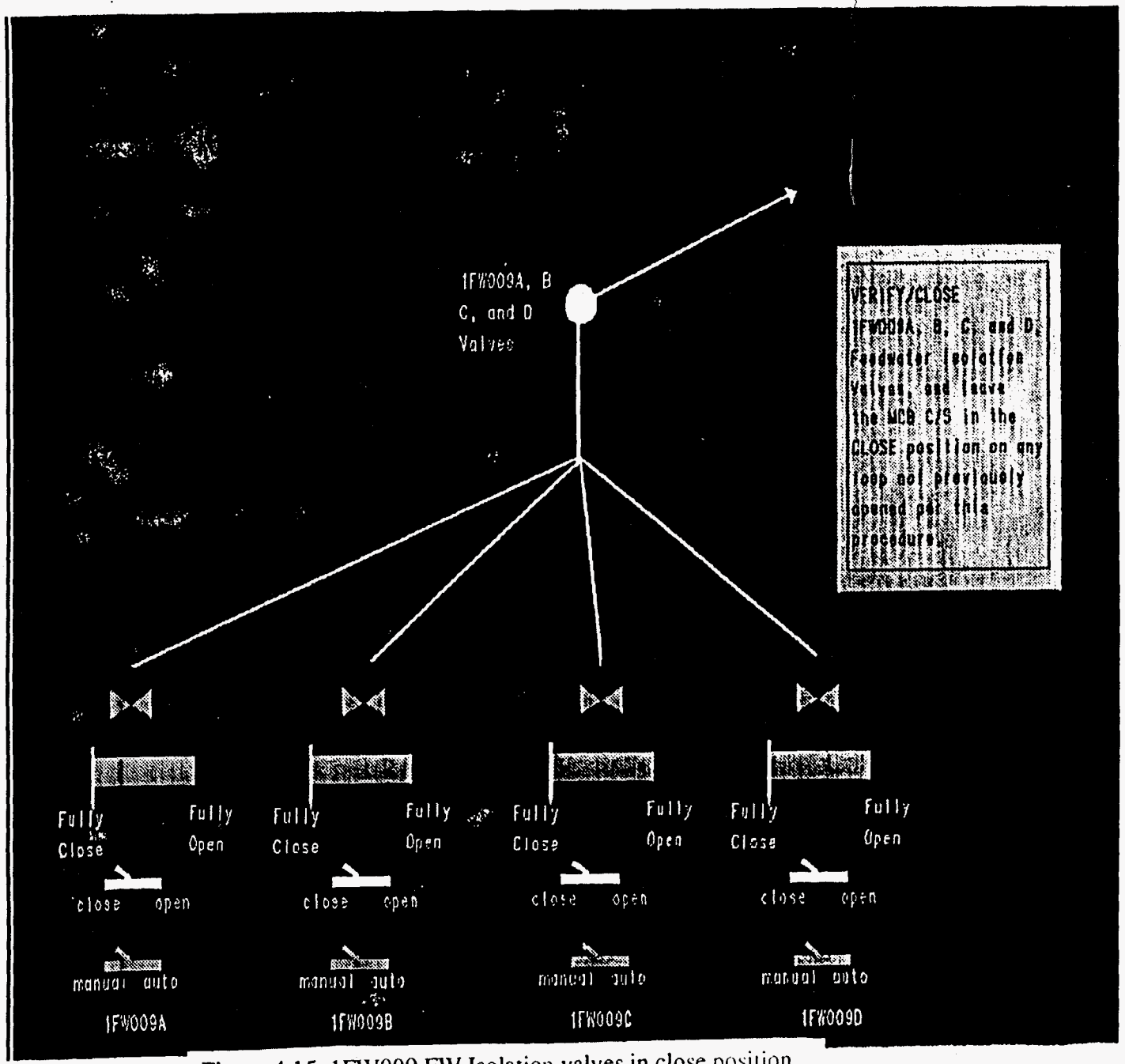


Figure 4.15 1FW009 FW Isolation valves in close position

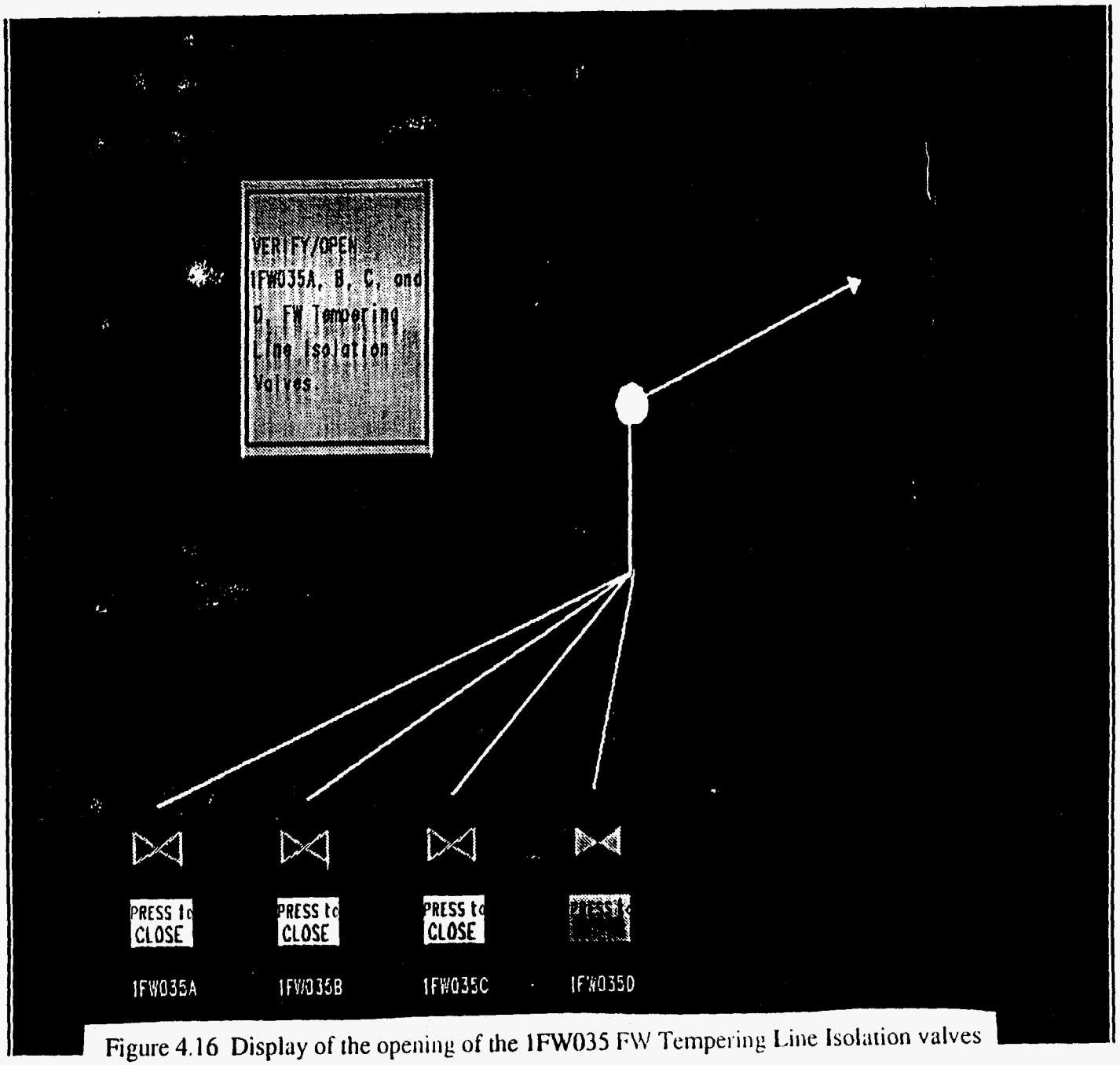


Figure 4.16 Display of the opening of the 1FW035 FW Tempering Line Isolation valves

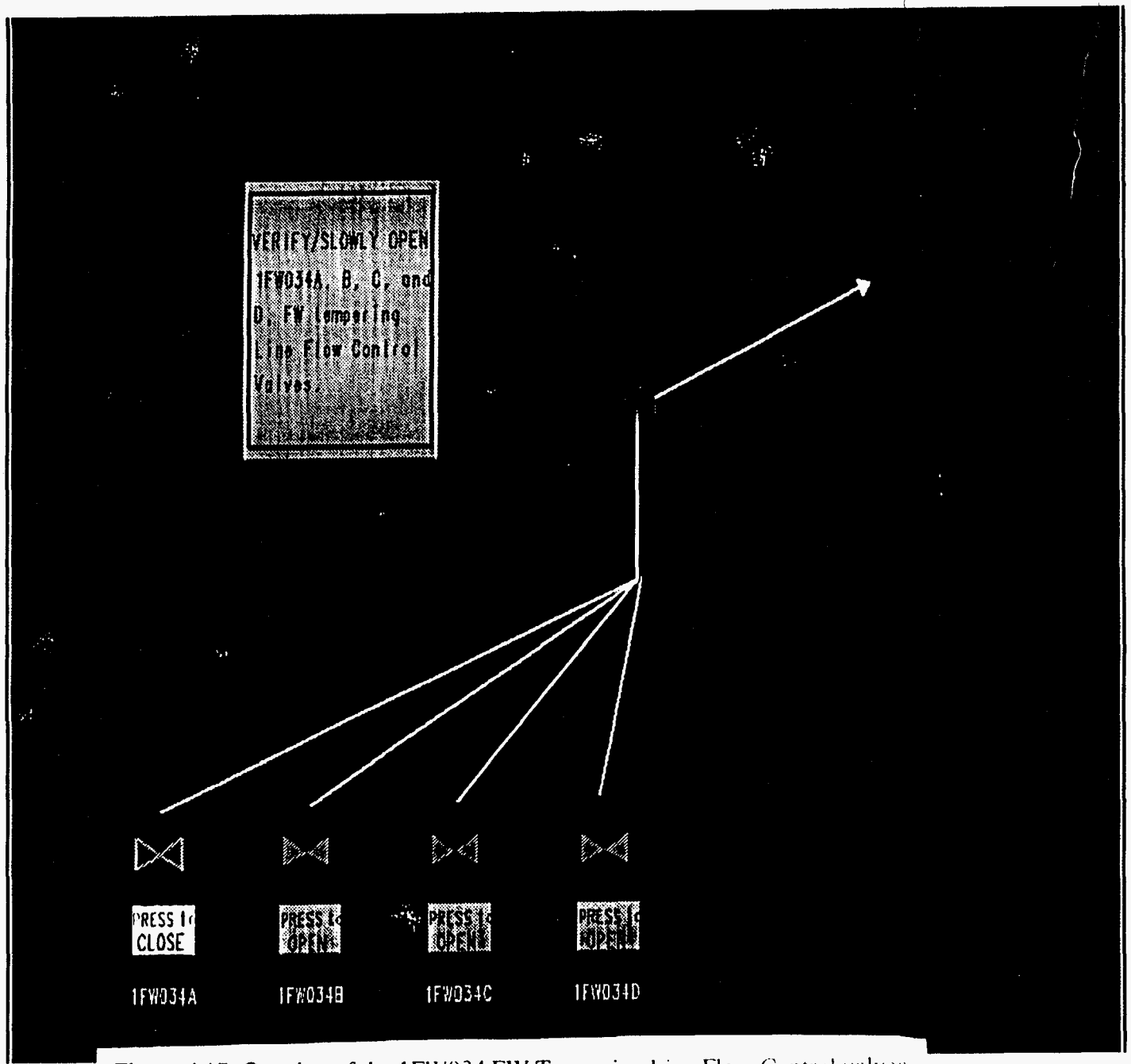


Figure 4.17 Opening of the 1FW034 FW Tempering Line Flow Control valves

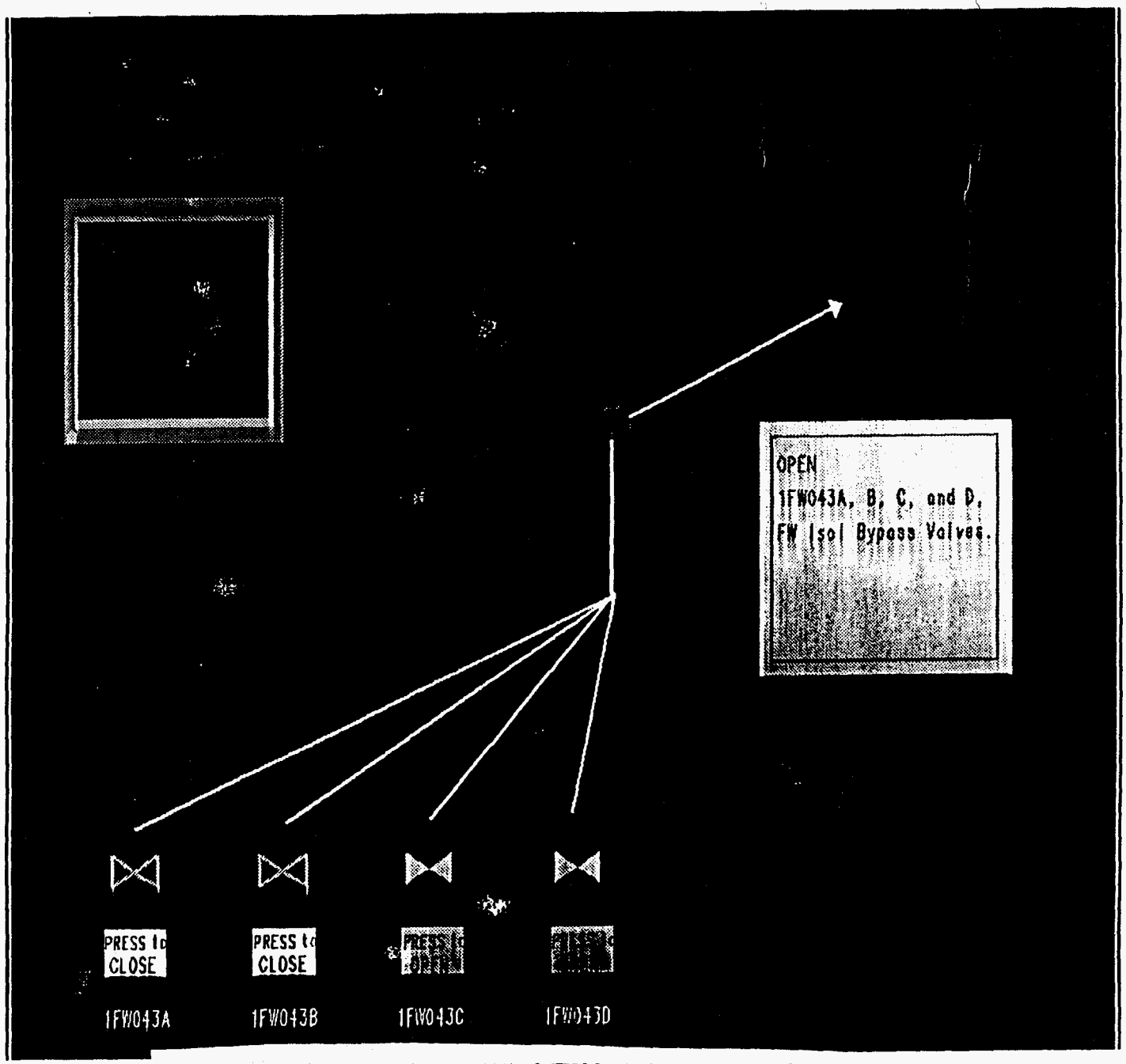


Figure 4.18 Opening of the 1FW043 FW Isolation Bypass valves

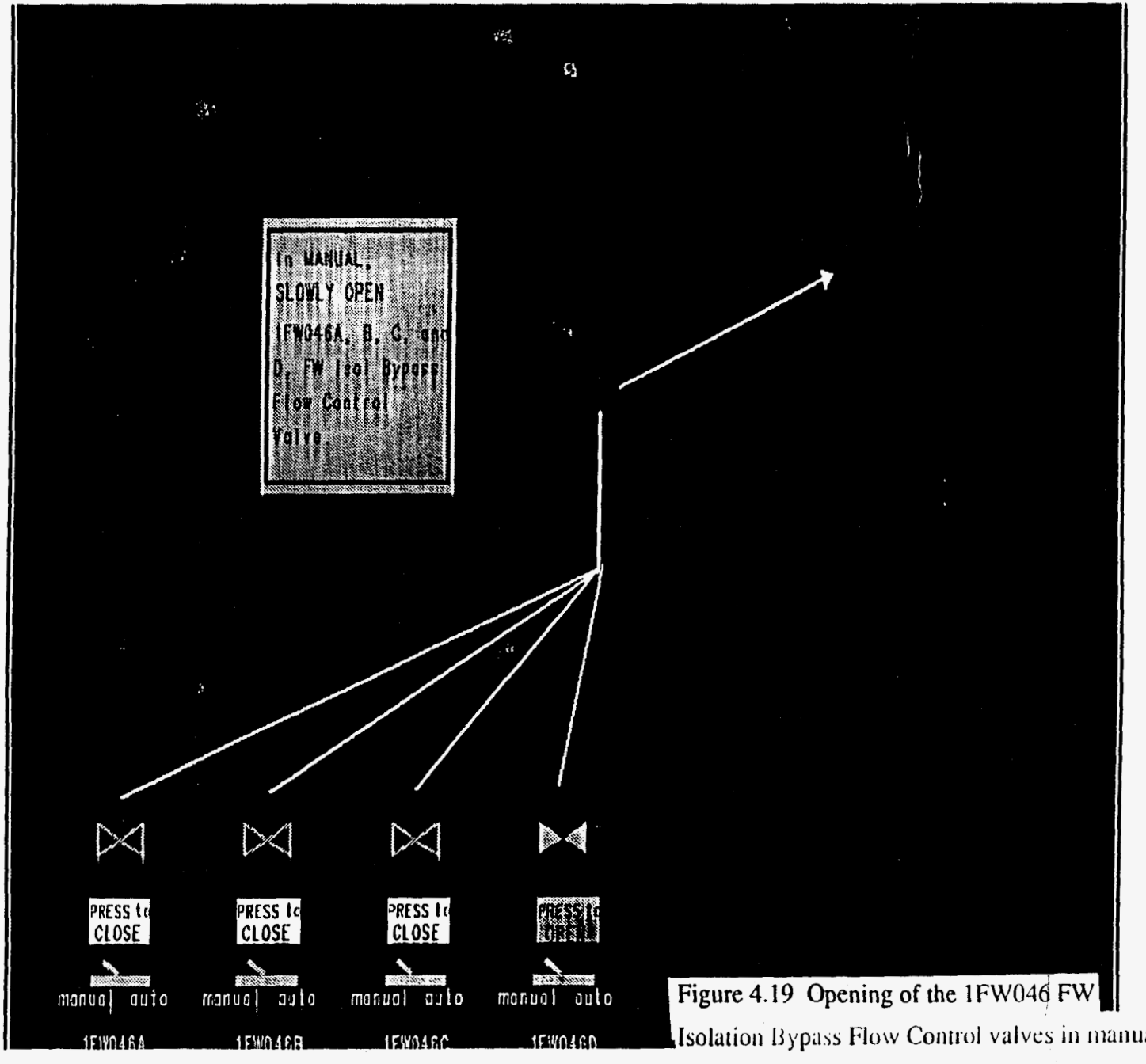


Figure 4.19 Opening of the 1FW046 FW Isolation Bypass Flow Control valves in manual

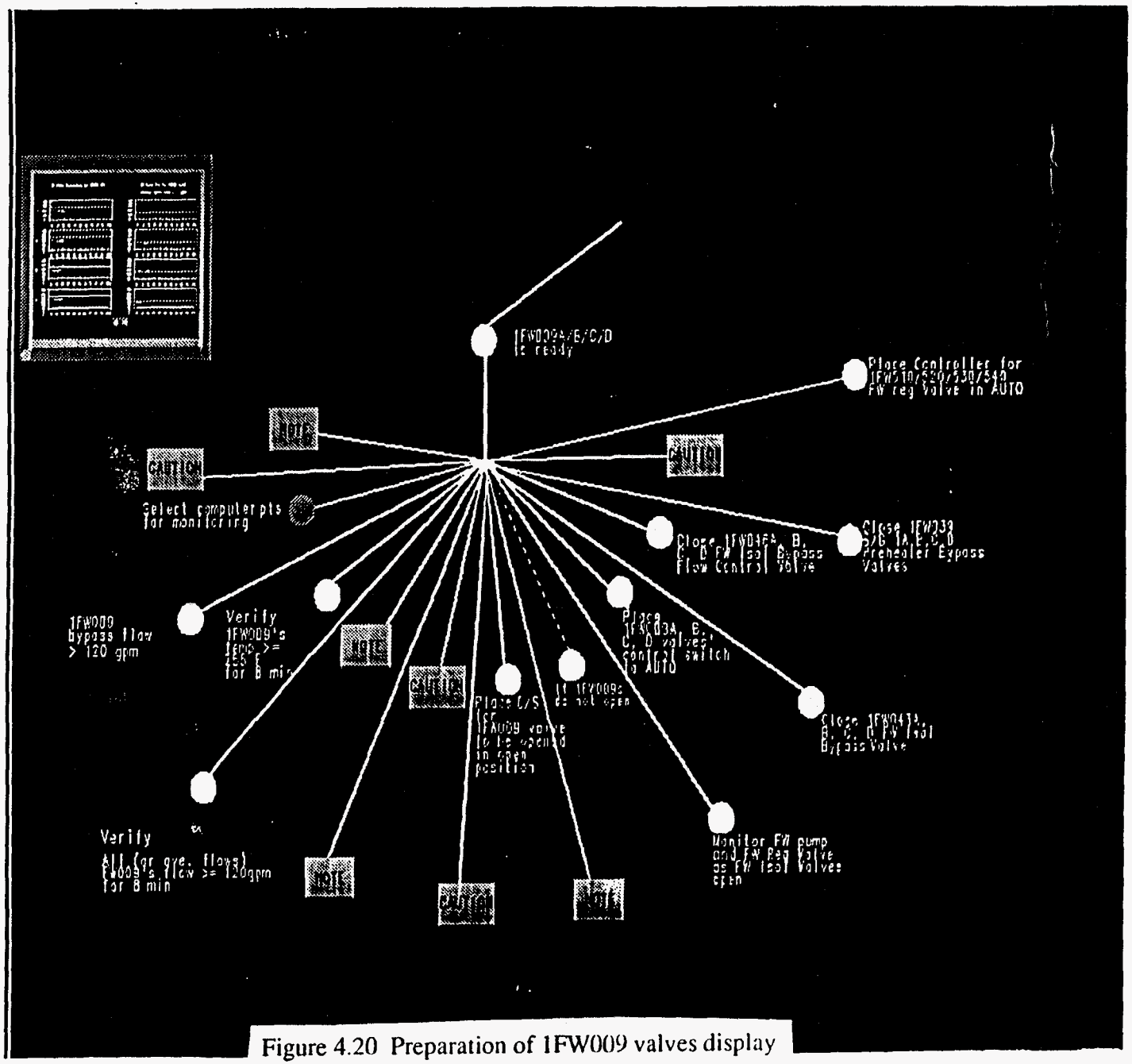


Figure 4.20 Preparation of 1FW009 valves display

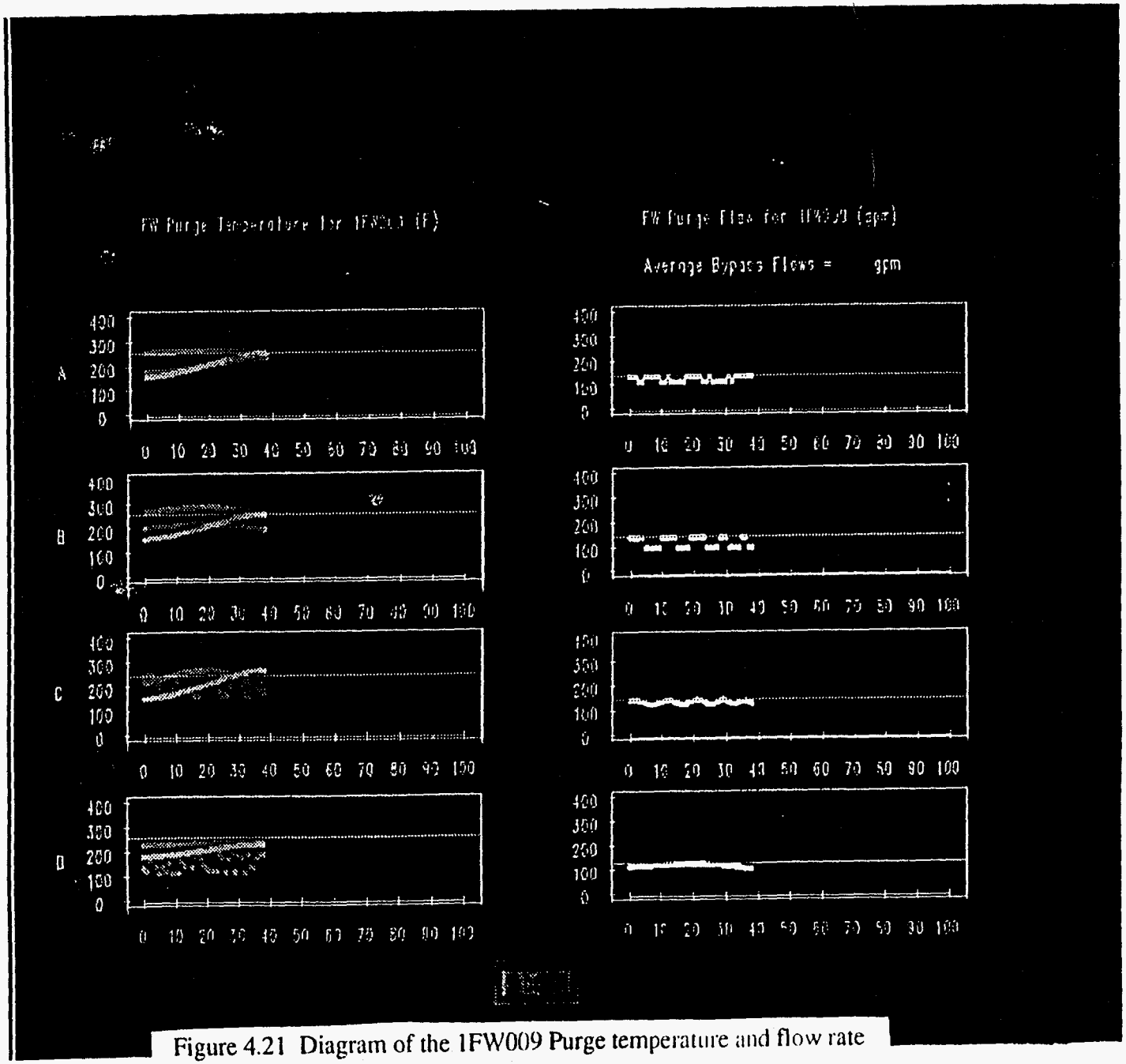


Figure 4.21 Diagram of the 1FW009 Purge temperature and flow rate

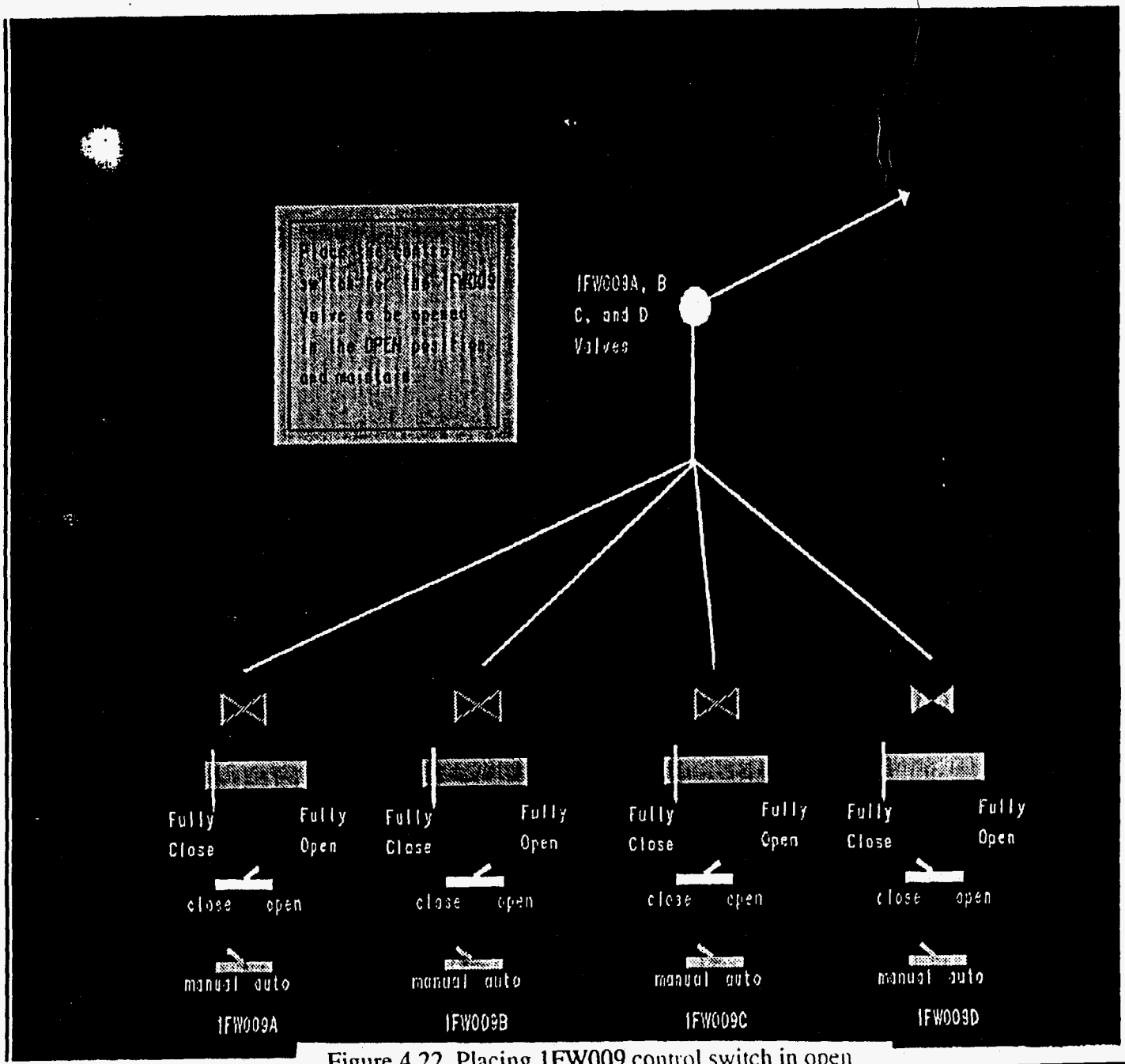


Figure 4.22 Placing 1FW009 control switch in open

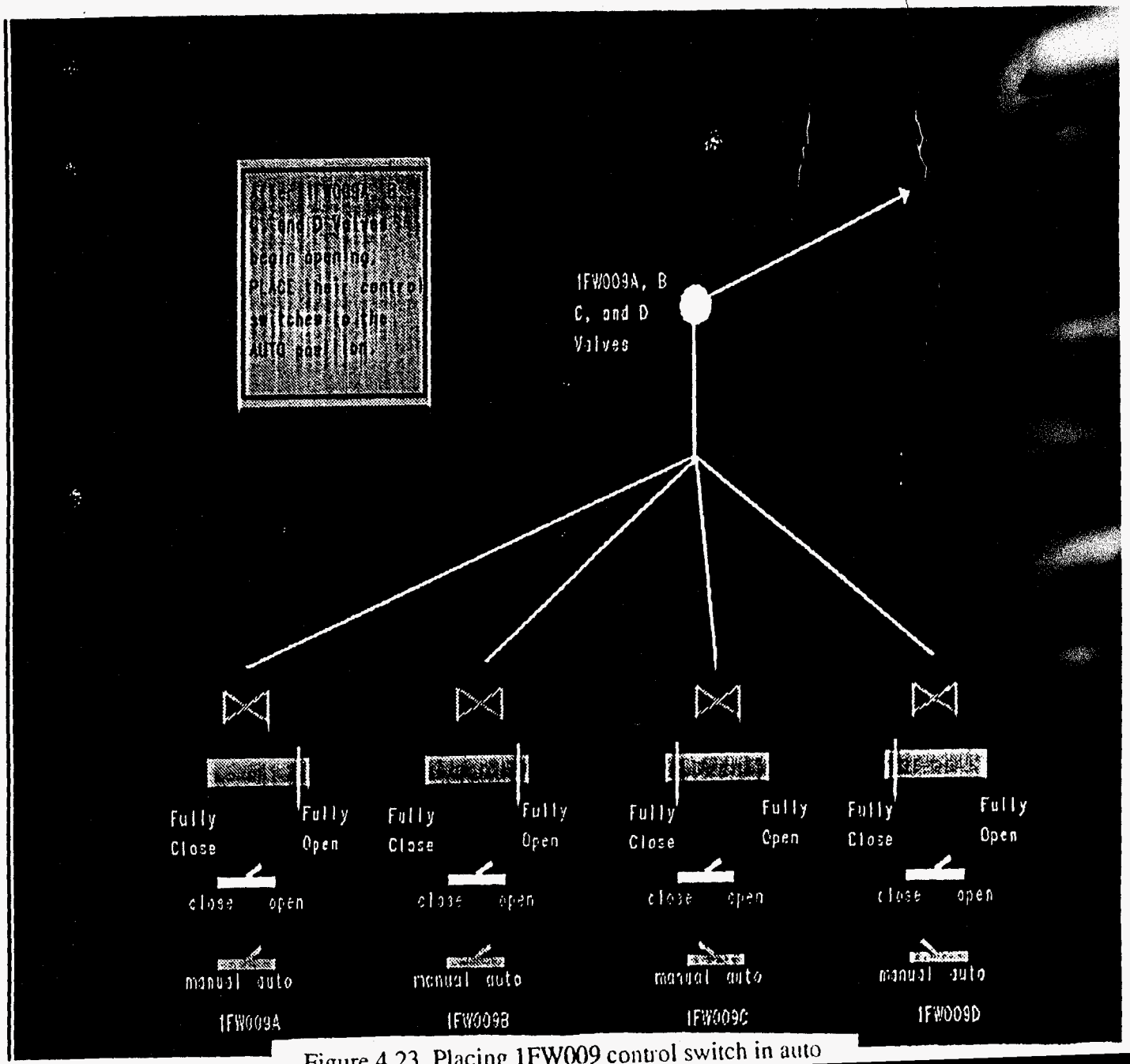


Figure 4.23 Placing 1FW009 control switch in auto

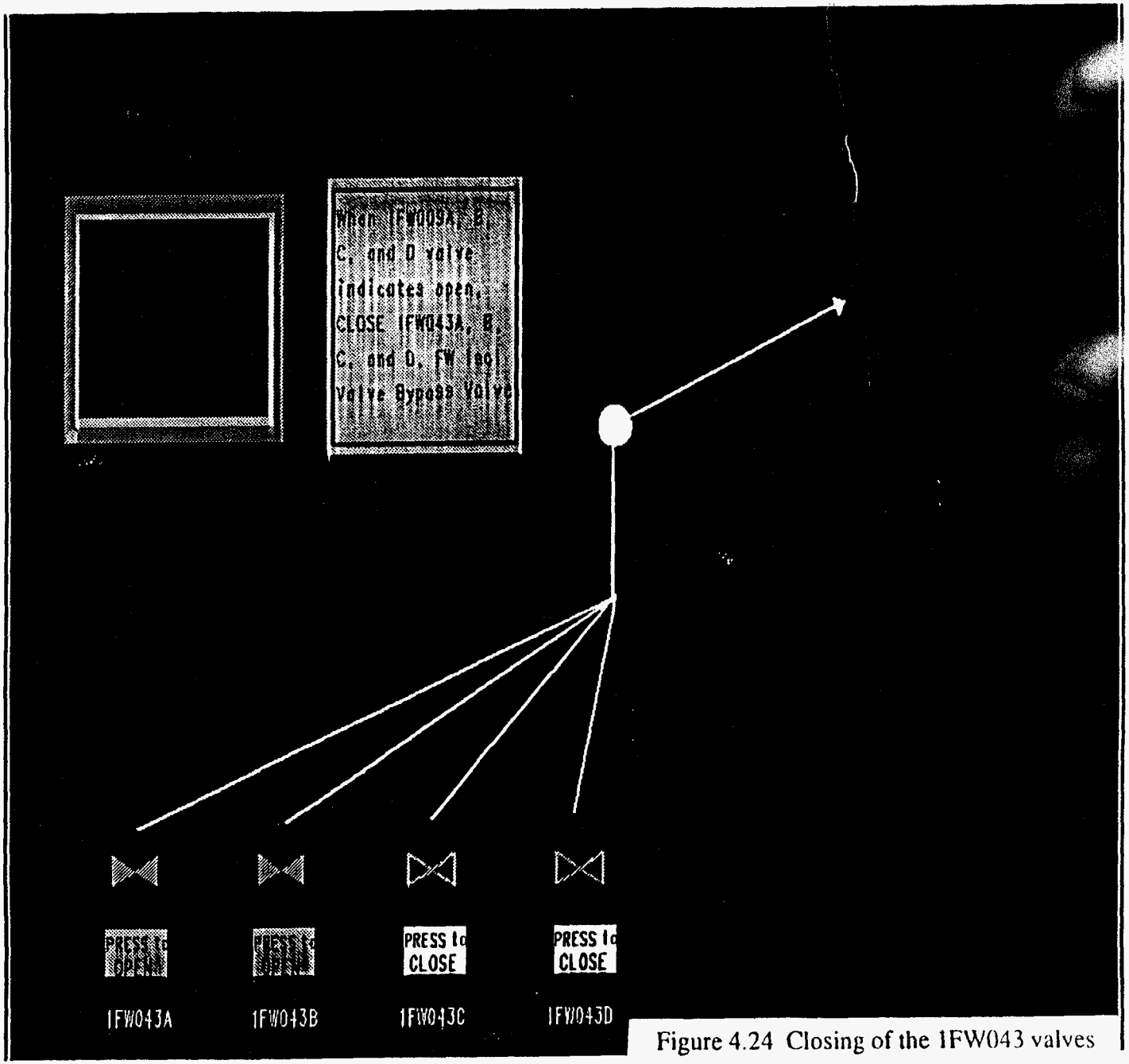


Figure 4.24 Closing of the 1FW043 valves

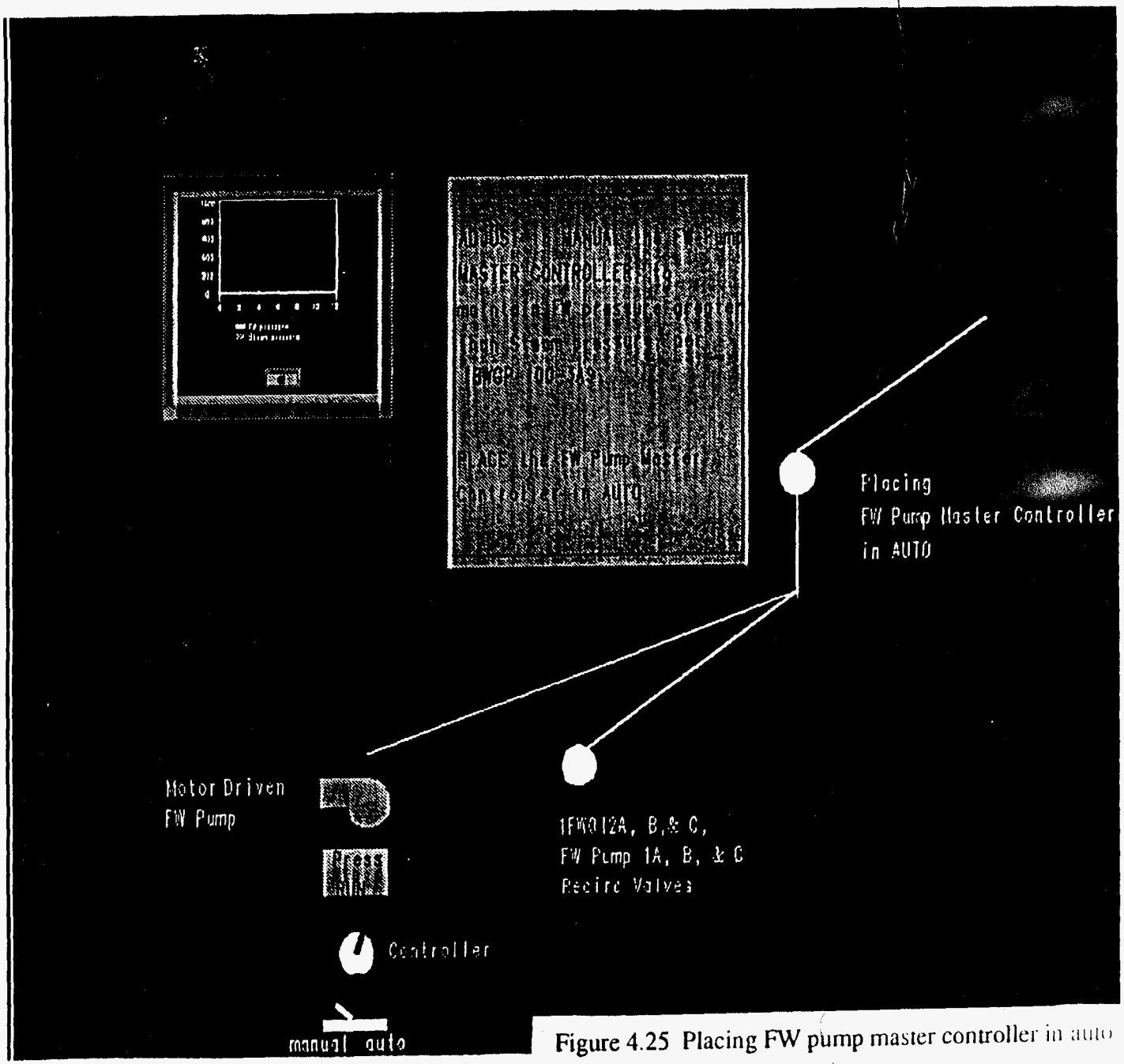


Figure 4.25 Placing FW pump master controller in auto

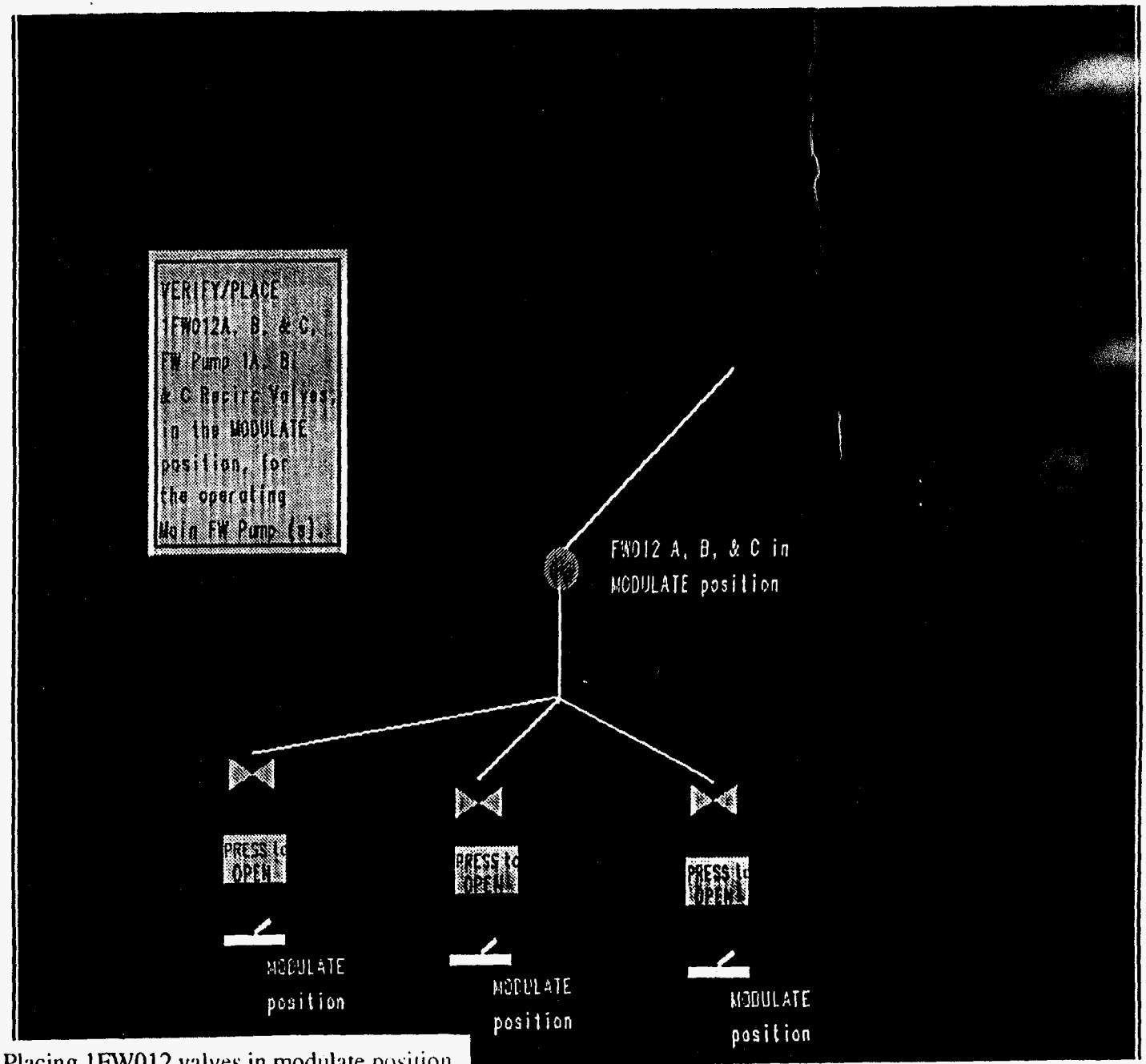


Figure 4.26 Placing 1FW012 valves in modulate position

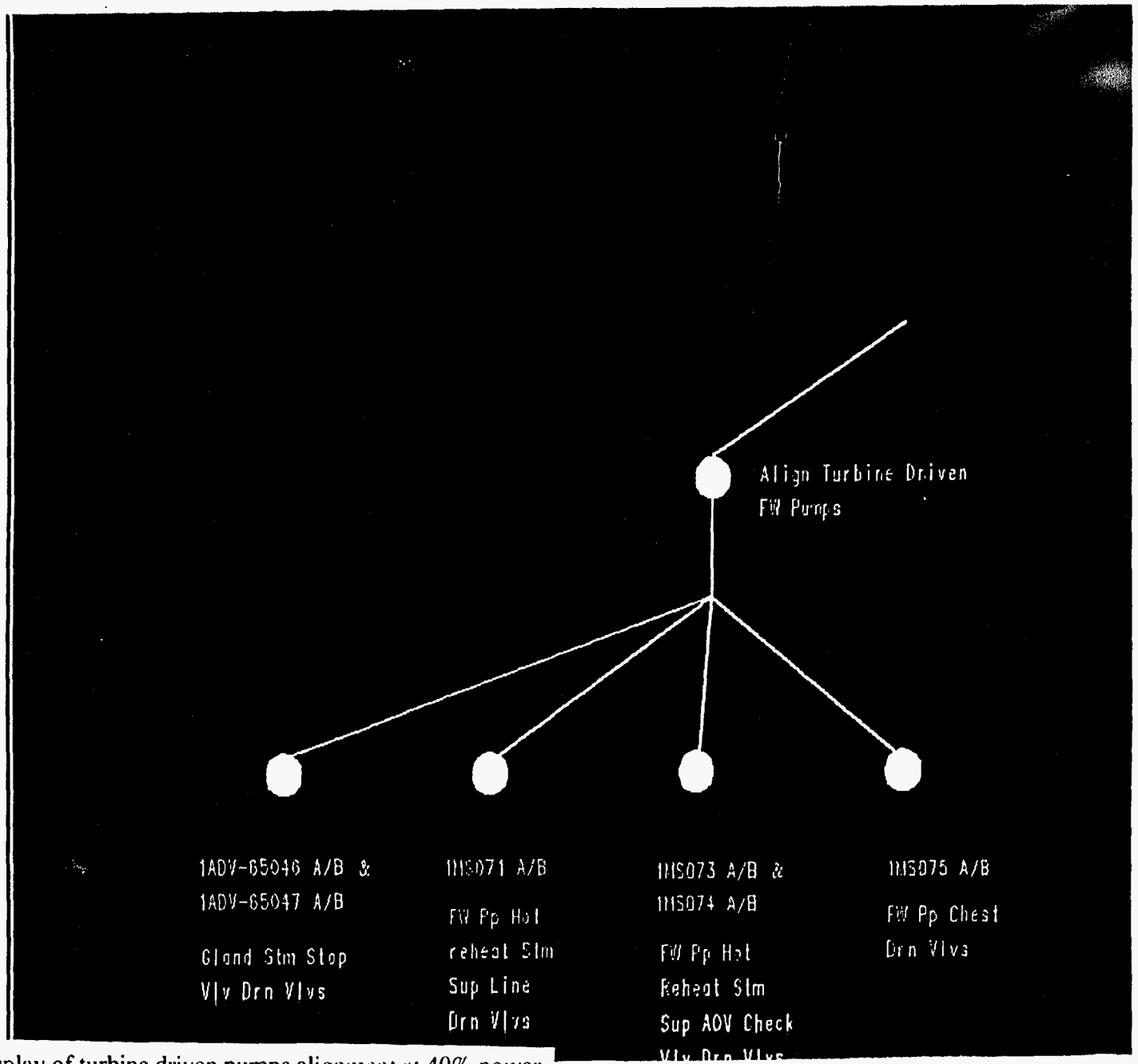


Figure 4.27 Display of turbine driven pumps alignment at 40% power

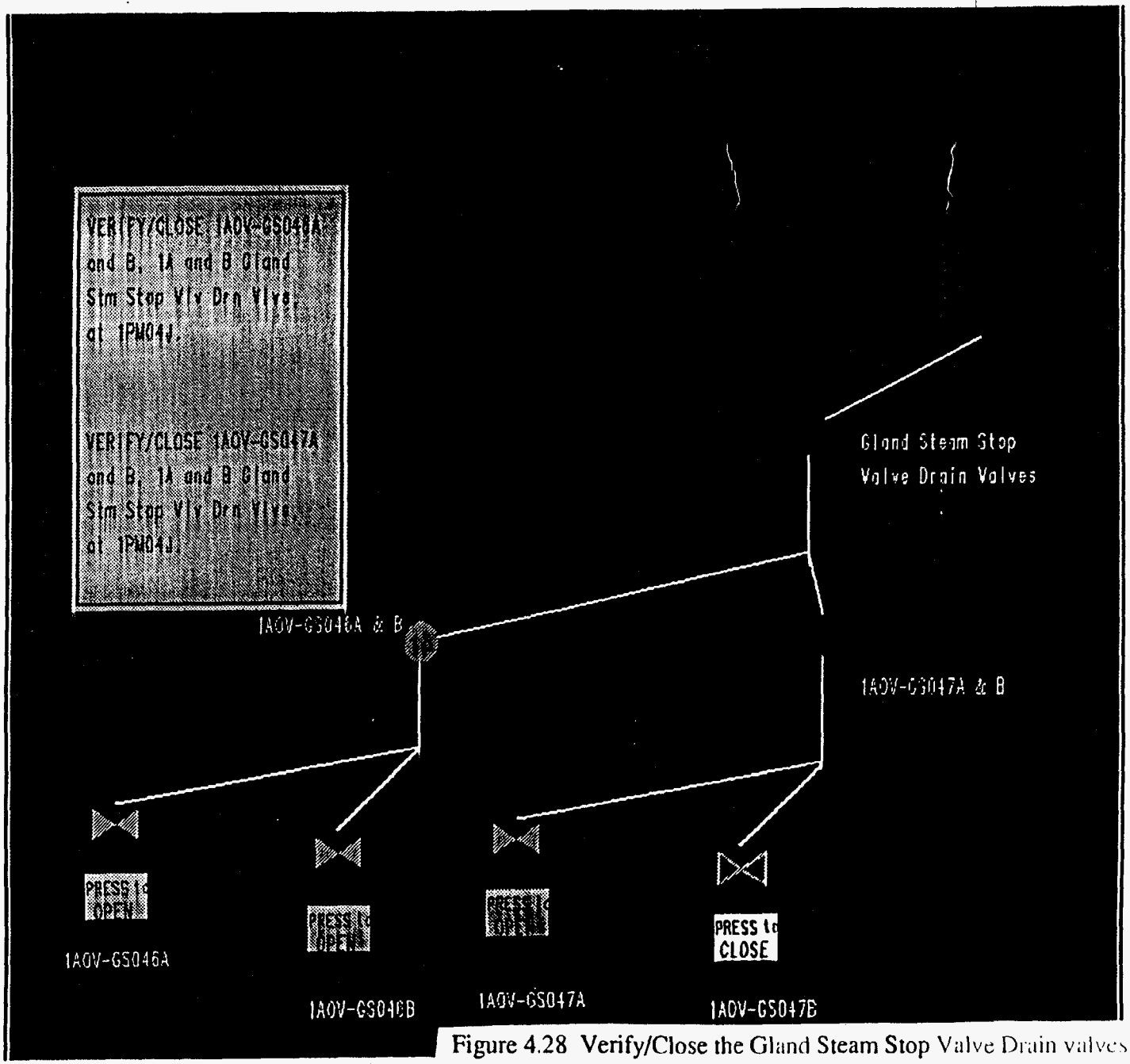


Figure 4.28 Verify/Close the Gland Steam Stop Valve Drain valves

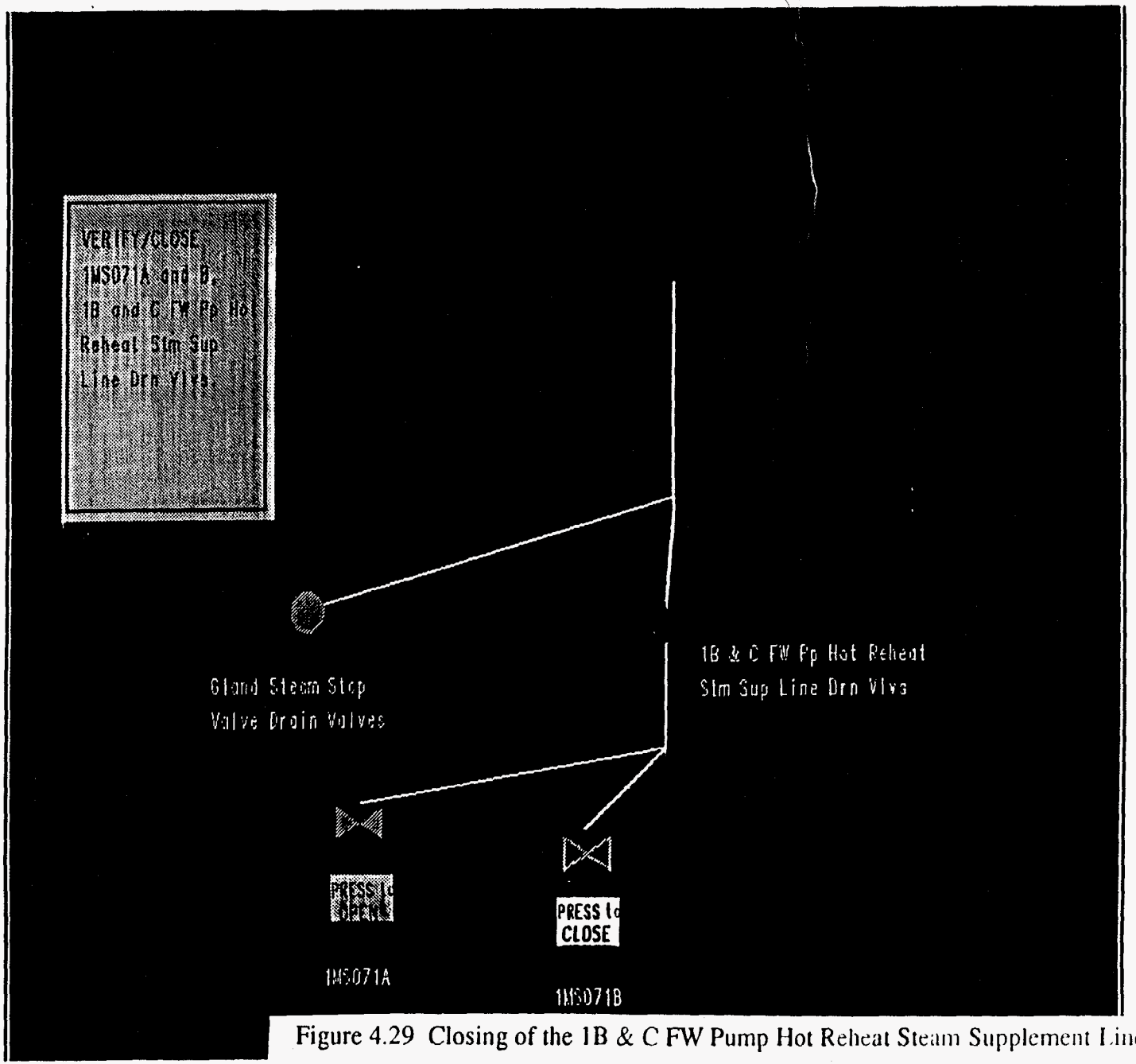


Figure 4.29 Closing of the 1B & C FW Pump Hot Reheat Steam Supplement Line Drain valves

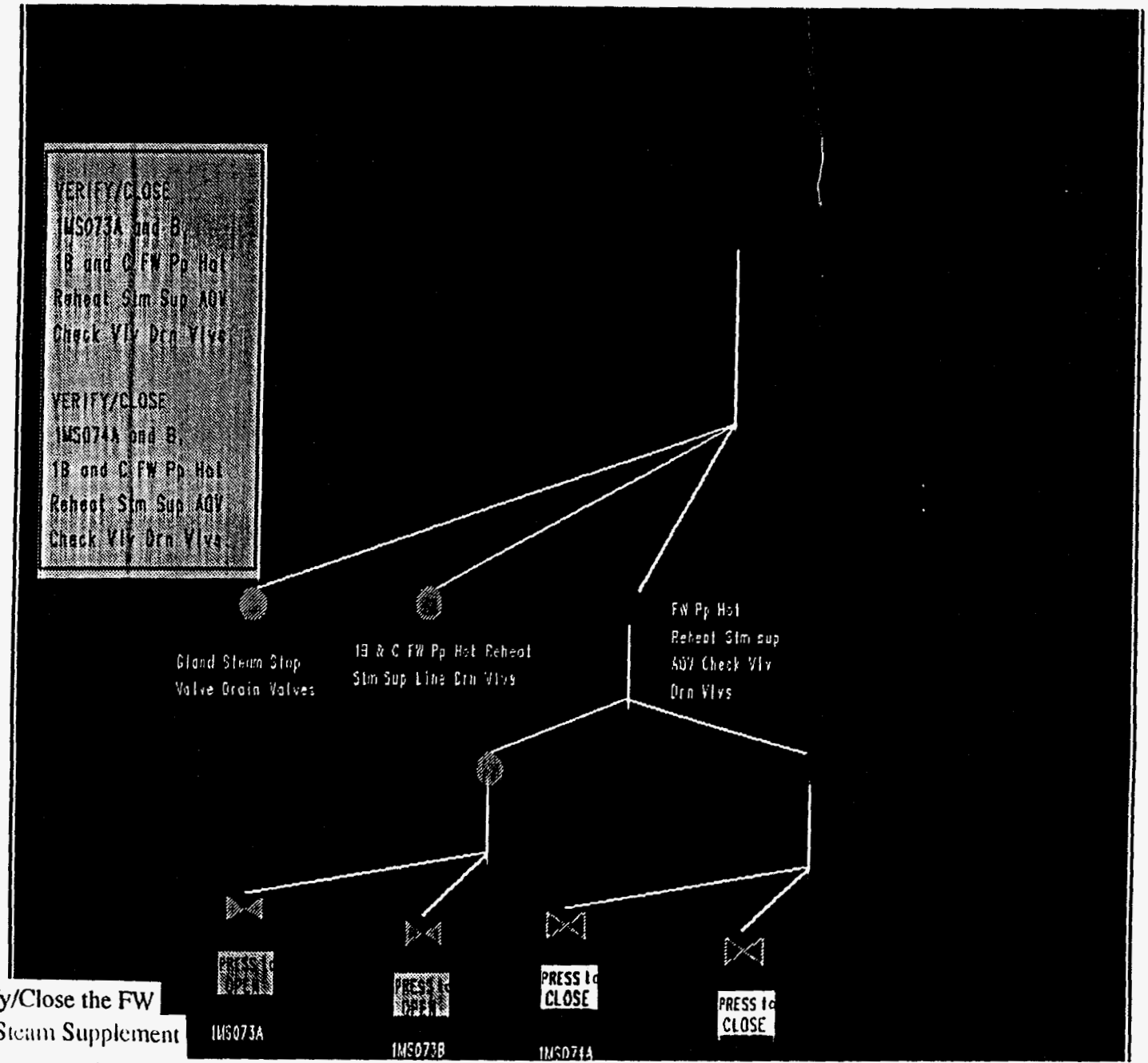


Figure 4.30 Verify/Close the FW Pump Hot Reheat Steam Supplement AOV Check Valve Drain valves

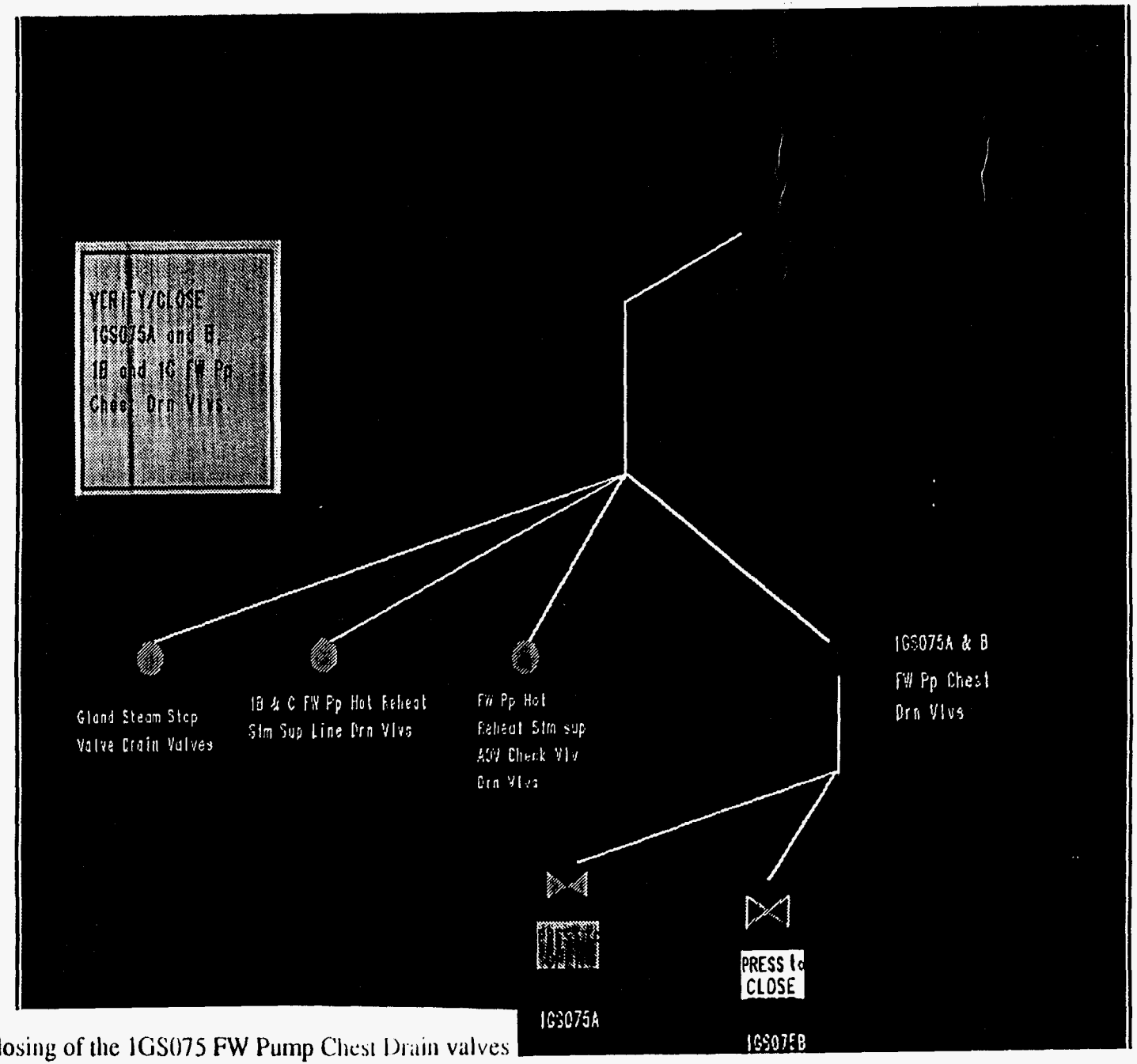


Figure 4.31 Closing of the 1GS075 FW Pump Chest Drain valves

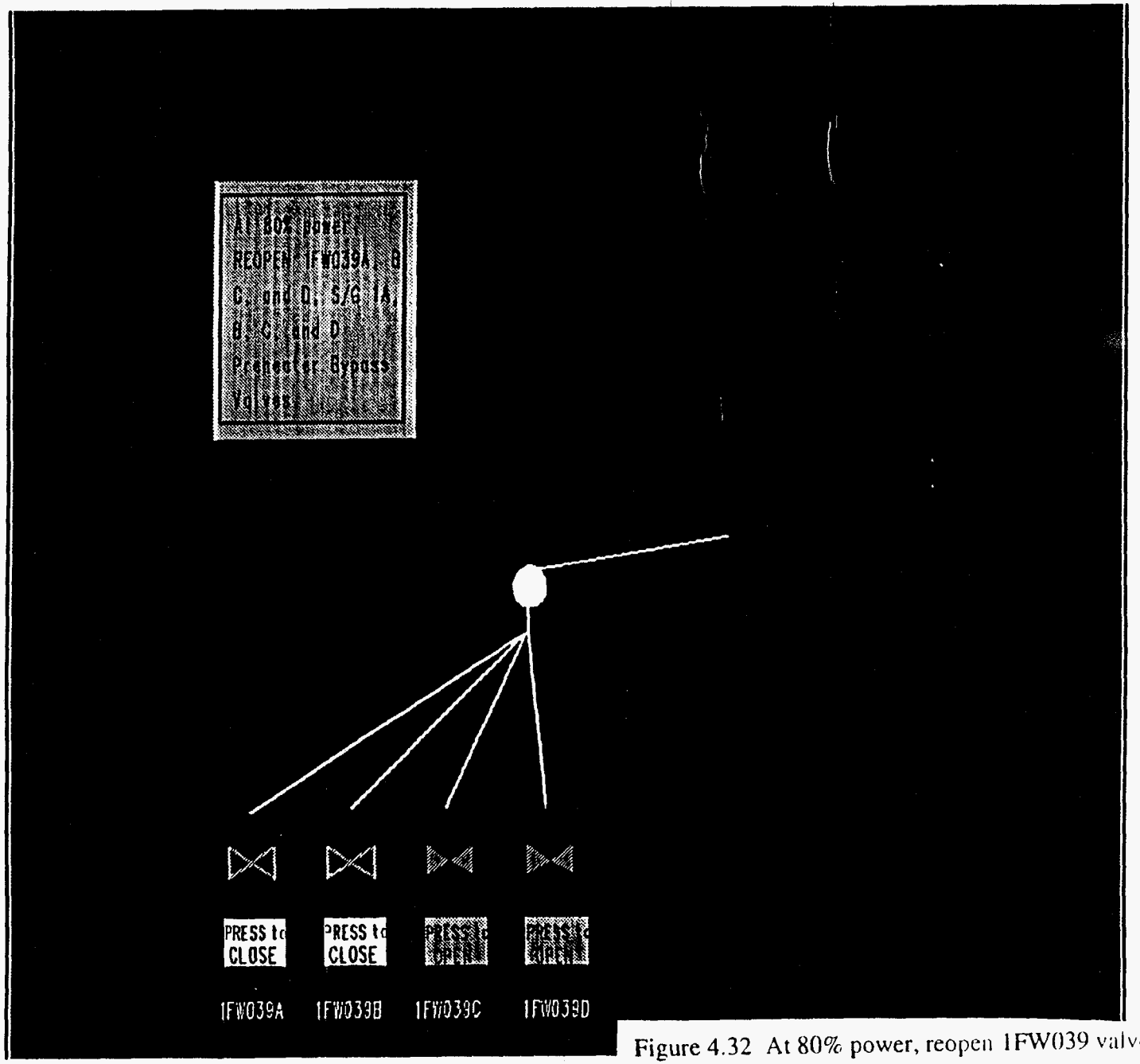


Figure 4.32 At 80% power, reopen 1FW039 valves

CHAPTER 6
EVALUATION

6.1 Introduction

Often new displays and interfaces are built without evaluation as "proofs of principle." This not only could be costly if modifications are needed later but could also affect safe operation of the plant. As part of the overall interface system design cycle, evaluation of the system may be the most challenging task to perform. Woods et al (Woods, O'Brain, & Hanes, 1987) stated the following regarding the importance of evaluation studies of new interface designs: "Evaluation studies are needed to identify weak points where a human-machine system can be improved, to provide design feedback during the development of new concepts, and to determine the ultimate effectiveness of new or modified interface systems." (p. 1758)

Rasmussen and Goodstein (1988) and Woods et al. (1987) suggested that comprehensive evaluation studies must distinguish between interface system goals (what is to be achieved) and the means of achieving them (design features). They also agreed about the importance of conducting evaluation studies in the context of work situations, i. e., real tasks, and of applying user performance measures as evaluation criteria.

Furthermore, a workshop was held in 1989 by the USNRC on nuclear power plant man-machine interface issues and it resulted in a list of proposed evaluation criteria for assessment of man-machine interface design for advanced technical systems in areas such as function allocation, decision aiding, system evaluation, and system maintenance. Based on the ideas for evaluation of interface designs in complex systems of Woods et al. (1987), Rasmussen and Goodstein (1988), and the guidelines and research issues suggested at the USNRC workshop (1989), a proposed plan for the evaluation of the "Bird's foot displays" EID interface has being designed. This thesis only provides a theoretical evaluation proposal, the actual evaluation with a full-scope NPP simulator is left for a future project.

6.2 Evaluation criteria

The first issue for this proposed evaluation is to determine a set of criteria that is suitable for these displays. Both Woods et al. (1987) and Rasmussen and Goodstein (1988) stressed the importance of clear definitions of system goals and the need for performance measurements. From the above and suggestions made at the USNRC workshop, the following general criteria are established and are considered to be appropriate in evaluating this EID interface design in complex systems.

1. Interface system design goals and design features need to be identified.
2. Categories of work situations to be evaluated need to be decided to produce the design problems of interest.
3. Performance needs to be defined and measured.

The following paragraphs will elaborate these three criteria, and hence attempt to provide an evaluation structure for the "Bird's foot displays" interface system. In addition, two scenarios will be used to illustrate the function and behavior of the interface.

6.2.1 Design goals and design features

The first part of the evaluation is to determine if the interface displays represent the design goals and provide design features to achieve them. As mentioned in the introduction chapter, the goal of this interface design is to develop a comprehensive set of interactive displays which are based on the ecological interface design theory. In addition, when possible, direct manipulations are included in the displays to provide users with timely feedback. These design goals are achieved through the "Bird's foot displays", which include the abstraction hierarchy and configural displays of states and constraints. These design features attempt to make the deep relationships among variables visible to the operators and to support operators' skill-based behavior (SBB), rule-based behavior RBB), and knowledge-based behavior (KBB) controls.

The displays are designed based on the abstraction hierarchy address appropriate levels of plant functions and tasks. These displays are categorized into three levels, functions processes, and parts and components. At the lowest level of the abstraction hierarchy (also the bird's toes), mimics of the physical components are presented for manipulations and SBB cognitive controls. As the hierarchical level gets higher, more configural displays are presented showing the underlying processes to support RBB and KBB.

The interface reveals the structure of the work domain in the form of an abstraction hierarchy through several design features. Essential information regarding plant states and variables constraints are shown in configural diagrams accompanying interface displays. These are dynamic displays and are designed to emphasize the presentation of all relevant information for each specific operational task without unnecessary information to distract operators. Also, affordances and constraints are embedded in the displays to support the RBB and KBB cognitive control needs.

Furthermore, a direct manipulation interface is provided to allow the users to act directly on the representations of the system. Timely feedback of users' actions is also provided on the representations for a direct engagement feeling. This reduces the distance of gulf of execution and gulf of evaluation, thus eliminates the translation and calculation usually required

6.2.2 Work situations

Due to resource constraints, new interface designs are often evaluated in a laboratory setting. However, in this case, it is recommended that the interface displays are to be evaluated in a full-scope NPP simulator. If a group of operators is available, it will be possible to use it to measure the effectiveness of a new interface. Because the operators are known to be skilled, any change in their performance compared with their performance before the introduction of the new display can be ascribed to changes in the design of the interface. and the efficiency of the operators can be measured for a particular interface.

A start up process of the NPP should be used for both the EID displays and the conventional displays. However, due to the nature of these particular displays, there are several difficulties in conducting the evaluation. It is best to compare the EID displays with the conventional displays, which consist of meters, switches, and charts. In order to preserve the authenticity of a control room, either a detailed simulation of the control room design is needed or the evaluation need to be conducted in a full scope NPP simulator facility, which may not allow non-expert subjects to participate in the evaluation.

It is also recommended that the interface is to be evaluated for both normal and emergency operations. Later in this section, the loss of feedwater transient scenario will be implemented for evaluation, .

6.2.3 Performance indicators

Lastly, evaluation is needed to determine if this EID interface is better than the conventional control room interface and in what way. Woods et al. (1987) suggested that it is insufficient simply to evaluate one system or display against another or against a set of design principles or standards because that does not address how the interface affects the operator's performance. That illustrates that even though the "Bird's foot displays" utilize the EID theory while the traditional single-sensor-single-indicator interface lacks a strong theoretical basis, it does not necessary imply one system is more advanced than the other. Some forms of performance indicators are needed to determine if the new EID design does indeed improve user's performance.

Follow the idea presented in the evaluation for the Rankine cycle display (NUREG/CR-5977), performance can be defined and measured through a diagnosis test.

Diagnosis test

One major aspect of this interface design is that it should facilitate in recognizing abnormal changes in the plant data. One way to determine if the interface does indeed provide operators with the ability to recognize abnormal changes is through a diagnosis test or a fault detection test. During a diagnosis test, some planned faults are injected into the programming and the outcomes of these faults are displayed through the state of components or through the configural diagrams or both. Since the interface provides trend information, component status, operating ranges, Technical Specifications, and physical limits, it should not only assist operators in detecting errors, but also in deciding actions needed.

A diagnosis test for fault detection can be constructed so that it may be either a single fault or multiple faults. An example of a single fault situation is that if there is a power supply failure to one of the four valves, that particular valve would fail to a close position while others remain open. In this case, the fault detection test can be designed so that operators need to recognize the status change in the main display and trace the fault back down the hierarchy to determine the causes and to take corrective actions. In the case of a multiple fault situation, a single cause may contribute to many components failures. For instance, a valve closes and trips off the pump to which it supplies water and that may cause components downstream to be overheated and trip. For situations such as this, the interface design should support operators with adequate information from the configural displays and the "Bird's foot displays" to deal with the fault.

6.3 Evaluation scenario

6.3.1 Introduction

A set of displays for the feedwater (FW) system is constructed using the EID approach for the PWR operation. These interface displays are generated for the cold start up procedures, i.e., their sequence and conditions are specific to the start up process. However, there are several state space diagrams that are generic in all cases. Examples are the RCS temperature vs. pressure curve, power output diagram, etc.

A theoretical evaluation is conducted for this interface. However, the evaluation of this interface has created some problems. First, NPP operation is very complex and highly coupled. Since only FW systems related to start up procedures are selected, this creates a difficulty because that any scenario chosen for evaluation would involve more than just the

FW system. Secondly, since no actual NPP data are implemented to drive the displays for now, certain plant states and system behaviors may be unpredictable. With these in mind, one scenario is selected to evaluate this interface, the loss of feedwater transient during the cold start up process.

This scenario is chosen for the following reasons. The start up process is a very complex, time consuming, and demanding operation and it is the process based on which the interface is designed. The loss of feedwater transient is selected primarily because FW system displays are available. In addition, a loss of feedwater can have effects anywhere from small significance (a small leak through a valve stem) to large safety risk (all FW pumps stop working). In a loss of feedwater transient, the flow in the secondary subsystem gradually declines due to a leak or drops to zero because of a large pipe rupture or a pump tripped. When this transient occurs, it normally trips both the reactor and the turbine-generator. Descriptions of the scenario and a "walk-through" of the interface for this transient will be discussed in the following section. The diagrams provided to facilitate in understanding this process do not represent the actual values in any way.

6.3.2 Loss of feedwater transient during start-up process

As mentioned in Chapter 1, the purpose of the feedwater system is to remove heat from the primary coolant (RCS system) and to generator power. Hence, one can image that without sufficient feedwater, the reactor would overheat and that would initiate a scram (shut down). For the worst case, if all other emergency cooling systems fail, a loss of feedwater might cause the reactor core to uncover due to the boiling away of the primary coolant and thus cause the release of radioactivity. There are two possible cases of a loss of feedwater scenario: gradual and abrupt. A gradual loss of feedwater refers to a small leak of coolant through valves and an abrupt loss implies that there is a large break somewhere in the FW system.

Gradual loss of feedwater transient

During the start up process, when a procedure is performed and the plant status is within normal range, the system nodes of completed steps in the main FW system display should indicate normal (green light). Often when a gradual loss of feedwater occurs, valves and pumps may not trip immediately due to their limit settings, therefore the system nodes may still indicate normal. However, there are several signs showing the possibility of a gradual loss of feedwater.

First, if the loss is through valves, the configural diagram for valve temperatures would provide some indications due to a rise in temperatures, see Figure 6.1. Secondly, operators may be alerted from the S/G level graph. The S/G level diagram provides a time history of feedwater level. When there is a small leak through the valve and no additional FW is added, there will be a slight drop in the actual level over time, see Figure 6.2. Third, the RCS temperature vs. pressure graph used for start up is a dynamic diagram that constantly provides crucial information to the operators. With less feedwater to remove the heat from the RCS system there will be a slight increase in RCS temperature. Because of the coupled relation between temperature and pressure in a closed space (the Ideal gas law), the RCS pressure will also rise. This information should be easy to see from the history curve provided by the temperature vs. pressure plot. The fourth indication comes from the power output graphs. With less feedwater, there are less steams to drive the turbine-generator, hence less electricity (MWe) will be produced. However, the reactor power output (MWt) may not be affected or only slightly lower due to the effect of the power coefficient (Figure 6.3), but the efficiency of converting energy from thermal to electric would be much less than ideal.

From the above descriptions, it can be seen that if a gradual loss of feedwater transient occurs anytime during the start up process, the configural displays would provide operators with sufficient information for the RBB and the KBB cognitive controls. This particular transient situation may not be obvious due to the small and gradual loss, but the design features of crucial information and history trend should alert and help operators in detecting faults.

Abrupt loss of feedwater transient.

The second case is more severe than the previous example. An abrupt loss of feedwater may occur if there is a break in the FW pipe line or a FW pump failure. The FW pumps are designed to trip to prevent any physical damage when there is little or no water. If a sudden loss of feedwater transient occurs during start up process, the FW pumps will trip. When the FW pumps stop delivering water to the S/G, heat from the reactor core cannot be removed and no steam is sent to the turbine-generator. The NPP is designed to automatically shutdown if there is any condition that might compromise the integrity of the core. Therefore the next event is a reactor scram and a turbine trip.

In this case, when the feed pumps stop working, the FW system node will indicate abnormal (red light) and so will the subsystems involved. Thus operators can select the abnormal node in order to access the displays for the subsystems, then select whichever

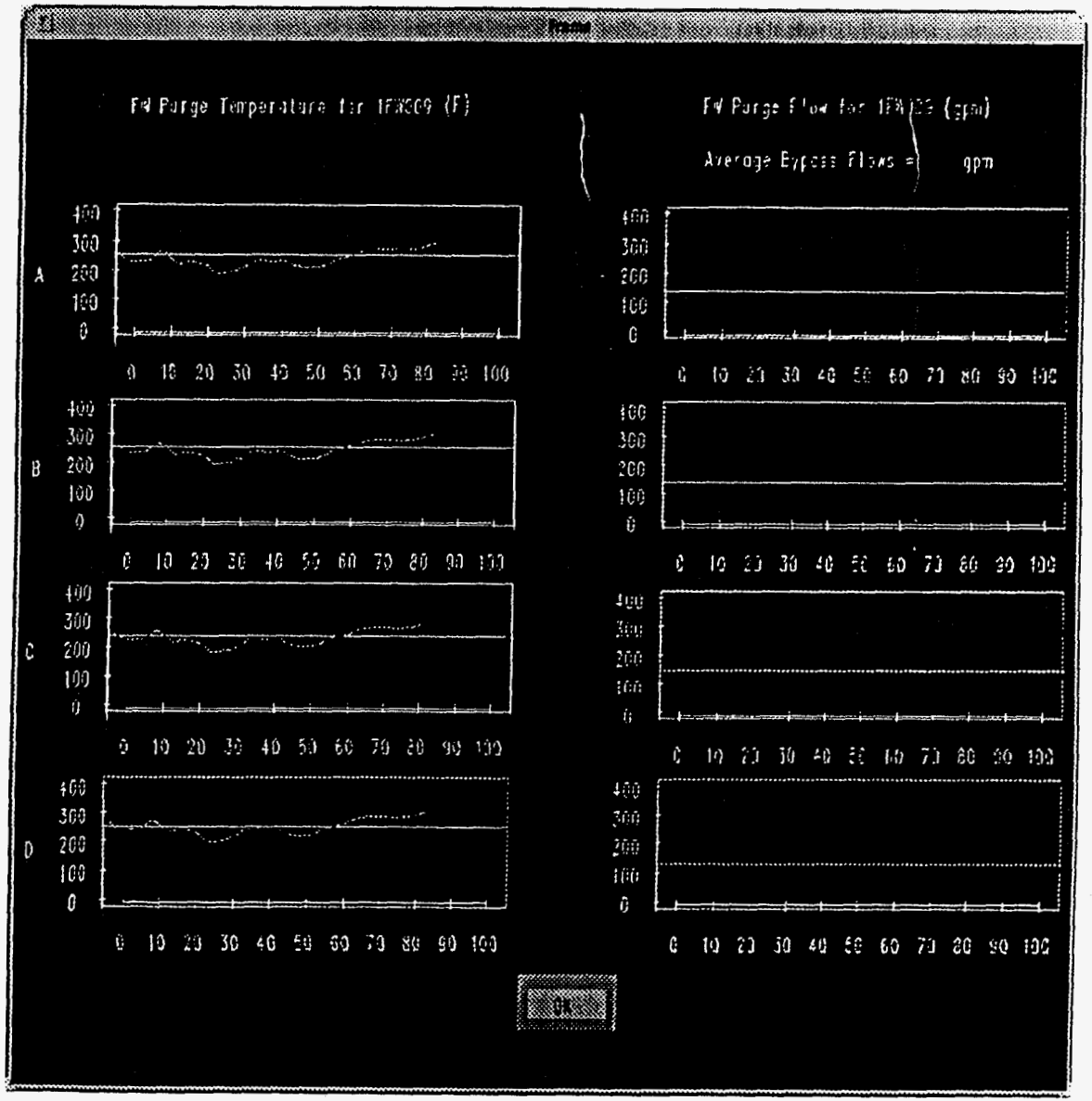


Figure 6.1 Slight increase in 1FW009 FW purge temperature

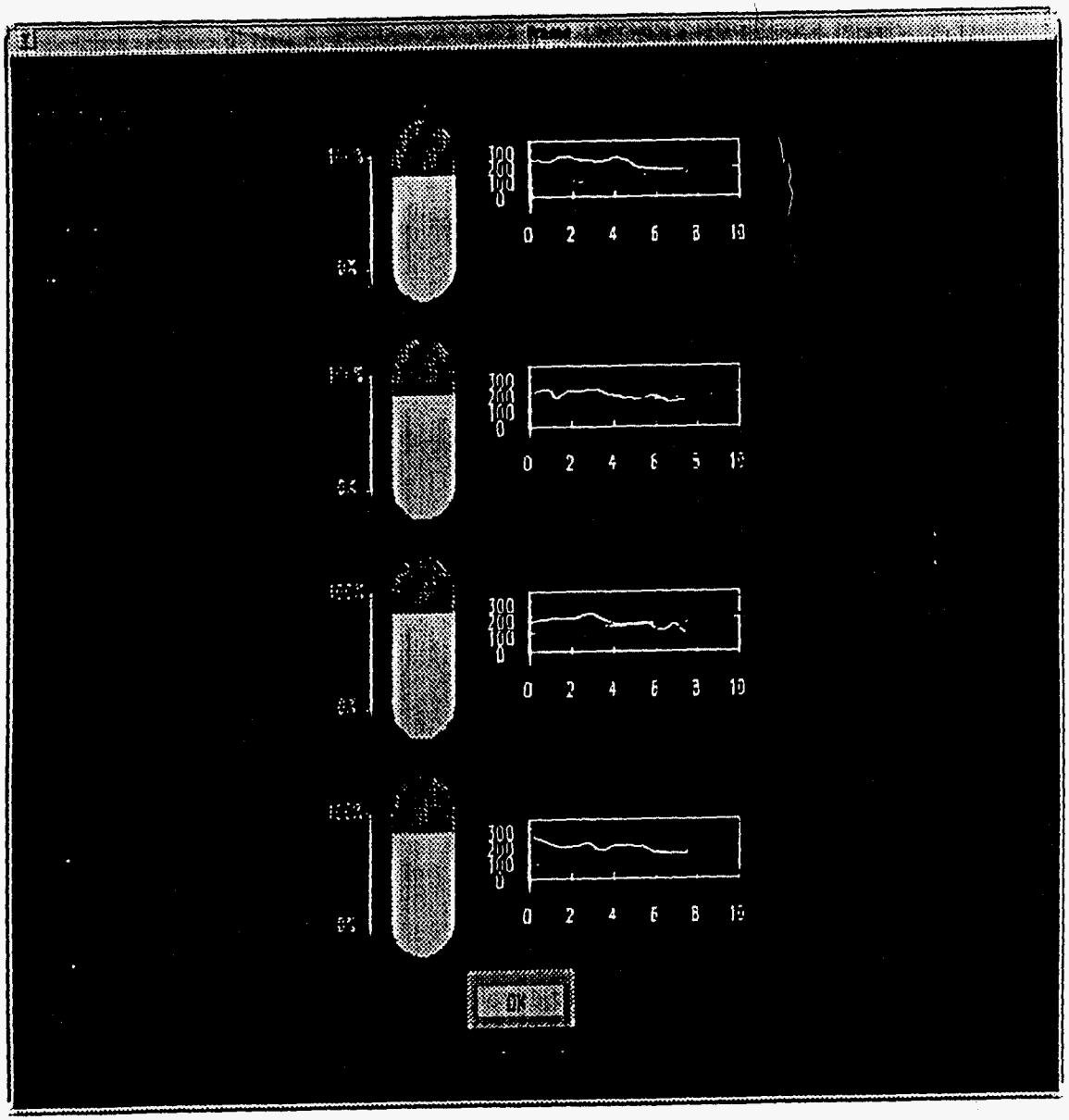


Figure 6.2 Slight decrease in the S/G levels

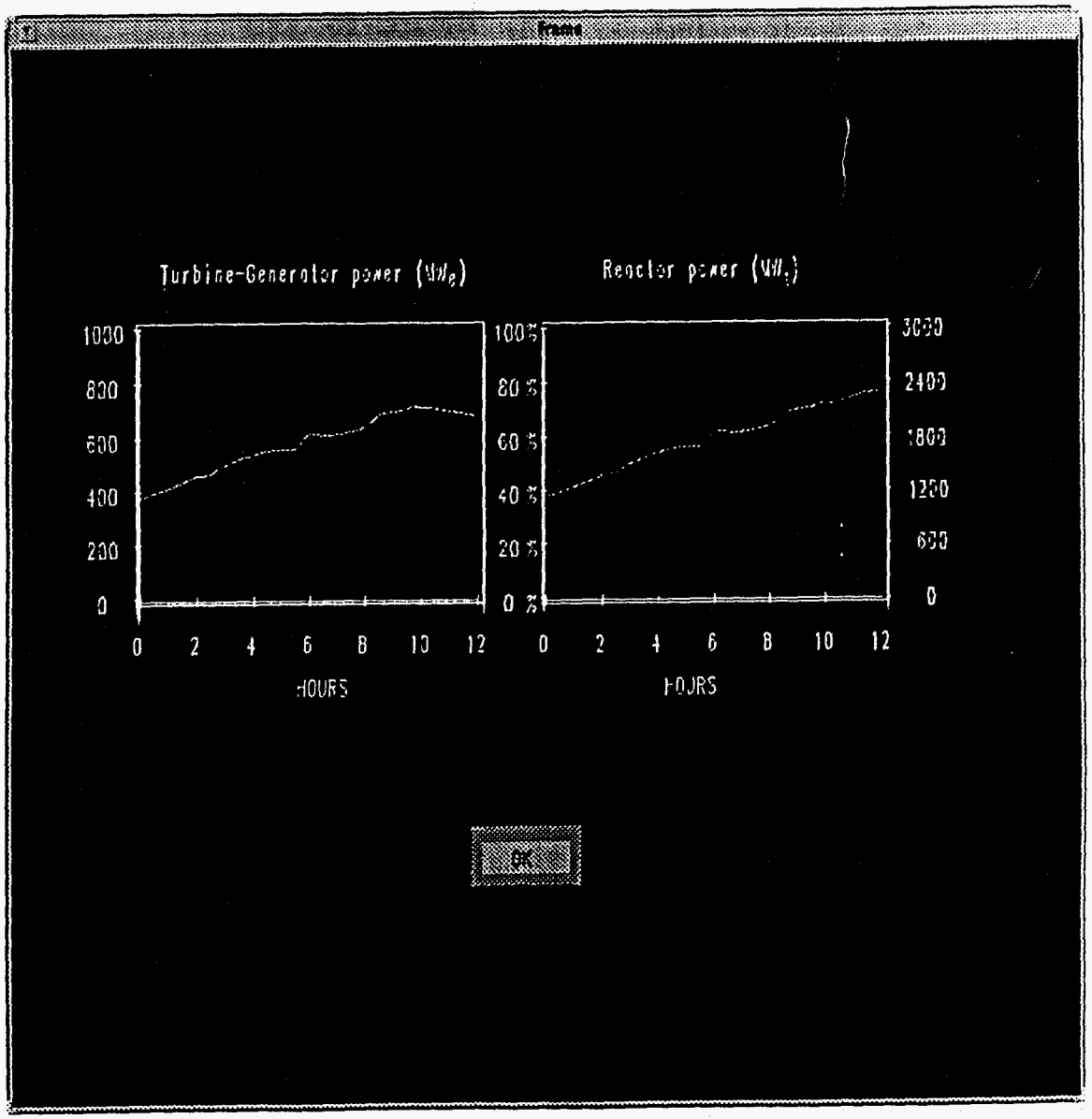


Figure 6.3 Decreasing efficiency in converting thermal power to electrical

subsystem node that indicates abnormality to see the components in question. This interface provides operators with the capability of tracing the faults just by going down the red lights. In addition, a mimic diagram of the entire FW system is provided in the main display. This provides operators with the option of reconfigure the system or redirecting FW flow, for instance to avoid the break in a line, when and if allowed. Again, as in the gradual loss of feedwater transient case, at each functional level, applicable integrated state space diagrams are given to support operators' SRK - based controls. These configural displays and the "Bird's foot displays" interface contain necessary information for the specific task not only for normal operation but also applicable during emergencies.

6.4 Limitations and Weaknesses

In the previous sections, details of the unique characteristics and advantages of the "Bird's foot displays" and the configural displays were discussed. However, all human-computer interaction interface designs have some short comings and the "Bird's foot displays" interface is definitely not without limitations and disadvantages. In this section, some of the limitations and weak points of this interface will be discussed and some suggestions for future improvements are provided.

First, the interface does not provide operators with more than one frame at a time. In other words, unless numerous computer monitors are utilized, operators would only be able to view few subsystems, such as the four 1FW006 valves, at a given time. This may pose a problem if a multiple fault situation occurs in a system and many components and subsystems are effected. Operators may lose a total perspective of the system and situation because only limited displays are present. This could reduce operators' RBB cognitive controls.

Secondly, this particular interface is very proceduralized. Because the structure of this interface is based on the start up procedures, conditions are set up in that sequence to prevent operating errors. However, in some cases operation procedures do not apply to transient situations. Consider the following example, assuming that Valves A are opened before Valves B for start up. When a fault occurs both sets of valves are closed automatically. In order to restore the pre-fault configuration, it is possible that Valves B need to be opened prior to Valves A. However, this interface does not provide specific information regarding transient procedures thus the attempt to restore may either be prevented or shown as an abnormal signal.

Third, because this interface is proceduralized, it creates some difficulties in accessing certain components. For instance, during the start up process, if operators wish to see the 1FW035 FW Tempering Line Isolation valves, they need to know that this set of valves is under the procedure for FW Main Nozzle Purge. This is not only impractical but could also raise some frustration under stress.

In addition, the accessibility of displays is also compromised due to the functional hierarchical structure. The start up process and other operational procedures usually involve more than just the FW system. When several systems are implemented, an easy way to get to desired frames is unquestionably necessary. It would not be efficient if operators need to travel through several functional levels up to the top level, select the next desired system, then travel down to the lowest level to perform tasks and repeat this process to reach next desired display. A better method of accessing lower level parts and components is definitely needed to improve this interface.

6.5 Summary and future work recommendations

The EID design principles have demonstrated the relevance of affordances and direct perception in the design of interface systems (Vicente, 1991; Moray et al., 1992). Overall, the "Bird's foot displays" interface illustrates some promising features based on the theoretical evaluations conducted in the earlier sections. This interface system for NPP operations reveals the underlying structure through dynamic configural displays of basic variables such as temperature, pressure, and the safety limits. It is also constructed in an hierarchical order to support operators at different levels of cognitive controls. Furthermore, the control and display relationships are compatible with required operations. The direct manipulation capability eliminates some mental translations required of the operators for executing tasks through an interface.

As an outcome of this thesis, some work recommendations are suggested for future development. These suggestion include the need for better "visual momentum" for going from display to display with minimal disruption. Also, an easier way of accessing lower level subsystems and components and getting back to the higher level displays requires further development. On the configural displays side, more research is need to include all necessary variables for operation in a good hierarchical fashion.

Furthermore, the future plans for NPP evaluations of the interface system are needed. A full scope NPP simulator should be used with actual start up data. Experiments

may be conducted based on the guidelines provided above in order to evaluate the effectiveness of this interface comparing with the conventional displays.