490

KSC-1037-2

ANALYSIS OF EFFECT OF HUMAN INTERACTIONS ON HTGR SAFETY AND RELIABILITY

Final Report

By
N. J. Becar
D. E. Wood

Date Published—April 5, 1976

Kaman Sciences Corporation
Colorado Springs, Colorado

TECHNICAL INFORMATION CENTER
ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION

DISCLAIMER

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

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

This report has been reproduced directly from the best available copy.

Available from the National Technical Information Service, U. S. Department of Commerce, Springfield, Virginia 22161

Price: Paper Copy $7.50 (domestic)
$10.00 (foreign)
Microfiche $2.25 (domestic)
$3.75 (foreign)

Printed in the United States of America
USERDA Technical Information Center, Oak Ridge, Tennessee

KSC-1037-2
Distribution Category UC-77

ANALYSIS OF EFFECT OF HUMAN INTERACTIONS ON HTGR SAFETY AND RELIABILITY

Final Report

Revised April 5, 1976

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Prepared for the U.S. Energy Research and Development Administration, Division of Reactor Research and Development, under Contract No. AT(04-3)-1037.

ABSTRACT

This study was undertaken to provide a numerical measure of the impact of operator actions on the shutdown of an HTGR plant similar to Fort St. Vrain during specified accident sequences. The study also provides a similar kind of measure for the impact of current procedures and practices during normal surveillance and calibration testing on the Fort St. Vrain Plant Protection System.

It is concluded that the Fort St. Vrain shutdown and Plant Protection Systems appear to be relatively safe from any significant effects due to operator error during a high stress situation. However, the amount of public exposure during any credible accident can be significantly reduced by modifying administrative procedures and/or by training the operators to develop proper reflex actions during emergencies. It is concluded that operator errors during low stress surveillance and calibration exercises contribute negligibly to overall PPS failures at Fort St. Vrain as long as specified recovery factors are able to operate.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SUMMARY

The impact of operator actions on an HTGR plant similar to Fort St. Vrain during specified accident sequences has been evaluated in this study. Concurrent with the above study, a review was conducted of the impact of current procedures and practices as drawn up for normal surveillance testing and systems maintenance on systems similar to the Fort St. Vrain SCRAM Protection System.

The Fort St. Vrain Nuclear Power Station was used as a model for each of the tasks described above. The study was intended to provide information useful in improving the design and operation of future gas cooled reactor plants. The necessary drawings, documents, and manuals were made available through the cooperation of the General Atomic Corporation (GAC) and the Public Service Company of Colorado, (PSCC).

Interim reports on the GAC conducted Accident Initiation and Progression Analysis* (AIPA) were reviewed to identify a typical set of credible incidents to serve as a set of basic scenarios on which a sequence of operator actions could be based. The incidents selected were relatively high on a total risk basis, i.e., low probability with high consequence, or, high probability with low consequences.

The planned emergency actions for each incident were identified on an Event Flow diagram and expanded to include a probable set of unplanned actions. Each set of human actions was then configured into a table identified as the Human Interaction Matrix Table (HIM).

* Not directly applicable to Fort St. Vrain, but used to select reasonable types of incidents.

The Human Interaction Matrix was in turn simplified by transposing it into an Emergency Decision Chart, (EDC). On this chart each decision point or point of identified action serves as a focal point for the assignment of estimated probabilities which define the possibility of the action proceeding along one of two possible paths. High stress human error probabilities as suggested in the WASH 1400 report were developed for emergency action on Light Water Nuclear Steam Plants. These values were modified slightly to be more compatible with HTGR operations. At this point, a "GO" model was constructed to simulate all events on the EDC. This "GO" model was identified as Human Decision Model, (HDM-1).

The HDM was run in a parametric mode to provide inputs for a Shutdown Model of the St. Vrain Plant. The FSAR for Fort St. Vrain, Reference 7 specifies a list of equipment which is required for Safe Shutdown of the Fort St. Vrain Plant. This equipment was included in the Shutdown Model, hence the model is called a Safe Shutdown Model (SDM-1). The Safe Shutdown Model is a top level model containing only equipment redundancy and no functional relationships or subsystem detail. Since the accident sequences studied are similar after the first response, maximum attention was directed to the Reheater Tube Leak incident. This incident has a relatively high probability of occurrence, but is of extremely low consequence to the public. Since the steam is contaminated in this kind of incident, the emergency action plans indicate that it is preferable to not SCRAM the HTGR while at high power. Hence, the probability of getting an unanticipated SCRAM becomes more significant. The results of this study indicate that the probability of getting such an unanticipated SCRAM is directly dependent on the amount of operator error assumed at the start of the incident, e.g.:

Assumed Operator Error at Start of Accident	Probability of Unanticipated SCRAM
0.50	.406
0.17	.170
0.05	.057
0.03	.032
.004	.007

It is immediately apparent that if one desires to have the probability of unanticipated SCRAMS to be in the order of .01 or less, the estimated operator error at the start of the incident must be of about the same magnitude. Human Factors experts (References 6, 10, 11) in this field indicate that a value of .01 to .001 most likely represents a normal unstressed error level for human operations of all types. If it is desirable to have a lower value for operator errors during high stress conditions,* there are at least two alternatives:

(1) When at all feasible, all operator actions should be delayed until at least two operators concur in the decisions, and one operator monitors the other carefully to insure that the correct action is being implemented. This will help to lower the probability of operator error during high stress conditions, to a value somewhere between .03-.05.

(2) Expose the Nuclear Power Plant operators to normative exercising techniques or specially designed simulators to develop trained reflex actions for emergency situation. Simulators are expensive but could also be used to train, requalify operators, and check out desired changes in emergency procedures.

* This report does not address the need for reducing error levels. Instead the values are estimated and reasonable methods for reduction are proposed.

In the area of normal surveillance testing and SCRAM Protective System maintenance, specific selection criteria were postulated to screen the many Plant Protective System (PPS) Surveillance and Calibration procedures and identify those procedures which might be considered to be most significant in their possible impact on successful PPS action. Each of the selected procedures was then reviewed to identify additional points of human interface not included in the previous SCRAM Protection System Study. (Reference 1). To evaluate potential system impact, specific test procedures were selected for observation. Among those selected were pulse tests, pressure tests, and temperature tests. These observations were made possible by the cooperation of staff and supervision at St. Vrain. The observations considered items such as procedural adequacy, adherence to procedure, and recovery factors that could be identified such as post maintenance test, support by control room personnel, lights, meters, alarms, etc., indicating correct or anamalous performance. Failure values assigned to various steps in the procedures were estimated using the non-stress values suggested in the WASH 1400 Report (Reference 5).

Recovery factor values were postulated so as to be in reasonable consonance with the estimated error departures, i.e., a complete recovery may be realizable if each event listed in the series of steps leading to such a recovery is initiated or executed. Some identifiable common mode failures were evaluated along with methods to recover or minimize the effect of these errors.

As a final step in this task, the maximum Human Interface failure probabilities were compared with the probabilities for hardware failure as obtained from the previous study on the PPS system. In the previous study all human interfaces were set at a minimal value.

In this comparison, all recovery factors were assumed to be operative. Under these conditions, the maximum contribution from Human Interfaces exceeded the hardware failures only in the 10^{-6} or 10^{-7} ranges. To help increase the probability of these recovery factors being operative, suggestions have been prepared to improve the PPS surveillance and calibration procedures for future HTGR's.

In general it appears that human errors in the PPS have only a small affect on SCRAM reliability, at least for the actions available for examination in this study (actual power operations and annual calibrations were not observed since they were not in progress at the time). There appear to be at least two major reasons for the above conclusion:

1. The slow response and large thermal capacity of the HTGR allows the operator a reasonable amount of time to consider problems and consult with senior staff to improve the probability of correct action.

2. Redundancy and diversity are effectively used throughout the St. Vrain Plant to minimize the impact of equipment or human failures. Modelling at the basic event level was quite helpful for including these factors in a natural way.

I. INTRODUCTION

In March of 1975, Kaman Sciences completed a "Reliability Analysis of An HTGR SCRAM System Including Human Interaces" (Reference 1). This was an exploratory analysis conducted on the HTGR Nuclear Power Plant at Fort St. Vrain to define system reliability and to identify the areas or system elements that might be major contributors to a SCRAM failure. Human interfaces were identified in the reference study but, were not studied in depth.

On May 1, 1975, a study was initiated to more fully explore the impact of human interfaces on an HTGR plant similar to Fort St. Vrain. Work performed on that study forms the basis for this report. This study was conducted in two parallel tasks.

Task 1 was initiated to estimate the effects of significant human action during postulated accident sequences and its resulting impact on HTGR safety.

Task 2 was closely related and consisted of a detailed review of current practices for normal surveillance and test procedures and their respective impact on HTGR safety.

Both of the above tasks make use of appropriate portions of the 'GO' analysis model developed during the work in reference 1 to measure the impact of revised human factors on the response of the Fort St. Vrain Plant Protective System.

The postulated accident sequences evaluated in Task 1 were defined to be the three most significant incidents identified in the on-going Accident Initiation and Progression Analysis (Reference 9), by the General Atomic Company. The AIPA does not apply specifically to Fort St. Vrain but these three sequences appeared to provide a suitable range of operator interactions.

Both Task 1 and Task 2 refer to procedures such as The System Operating Procedures (SOP), Overall Plant Operating Procedures (OPOP), and Surveillance Procedures (SP). These are procedures which have been prepared by Public Service Company for operation and maintenance of the Fort St. Vrain Nuclear Power Plant, during both normal and emergency conditions.

II. Fort St. Vrain Nuclear Power Station Description

The Fort St. Vrain Nuclear Generating Station near Platteville, Colorado was built by the General Atomic Company (GAC) for the Public Service Company of Colorado (PSCC). The station is a load following central station power plant using a high temperature gas cooled reactor (HTCR) to produce steam for the generation of electric power. Heat is produced by fission in an HTGR utilizing a uranium-thorium fuel cycle. Graphite is used for the moderator, fuel cladding, core structure, and reflector, with helium as the primary coolant.

The high total thermal capacity of the core provides a very slow rate of fuel temperature rise in the event of an accident. The materials of core construction permit a temperature rise to extend for a significant time without core damage.

The helium coolant transfers heat from the reactor core to the secondary coolant system. Helium is particularly desirable as a reactor coolant since it is chemically inert, is stable, has excellent heat transfer characteristics, does not undergo phase change and has zero neutron capture cross section. The coolant flow from the reactor core divides equally between two identical coolant loops; each loop consists of a six-module steam generator, a steam generator outlet plenum, and two helium circulators.

The helium coolant, at a pressure of about 700 psia, flows downward through the reactor core where it is heated to a mean temperature of about 1403°F. The helium is then directed to the steam generators beneath the reactor core to produce superheated and reheated steam.

After passing through the steam generators, the coolant is returned to the reactor at about 760 F by four steam-turbine-driven circulators, operating on steam from the exhaust of the high-pressure element of the main plant turbine. Auxiliary water-turbine drives provide power to the circulators when steam supply is not available.

During periods when the plant is shut down and the primary coolant system depressurized for refueling or other maintenance, two circulators will be operated to remove after-heat from the reactor at relatively low helium temperatures, although one is sufficient for after heat removal.

The prestressed concrete reactor vessel (PCRV) acts as a shielding for the reactor and contains the entire helium coolant system. It is constructed of concrete reinforced with reinforcement steel and prestressed with steel tendons. Enclosing the entire system in the PCRV prevents sudden loss of primary coolant, provides for efficient cooling of the core, and permits any radiation leakage to be collected by conventional means, filtered, and discharged at roof level.

A core support floor is provided within the PCRV in the form of a water-cooled structre of steel and reinforced concrete supported by 12 water-cooled steel columns from the bottom of the PCRV cavity.

The reactor plant design does not require a separate system reserved solely for emergency cooling. Instead, the reactor cooling system normally used for operations is also used as an emergency cooling system. Necessary safety provisions include a steam turbine drive, and an independent water turbine drive on a common shaft for each circulator, two separate coolant loops each with two circulators, two separate steam generators with six modules in each loop, and each with two independent heat transfer sections, multiple cooling water supplies, and multiple power sources. The advantage of these provisions for emergency cooling over the usual "emergency cooling system" lies mainly in the fact that all parts of the system are continuously, or frequently, operated in the course of normal plant operations. This feature eliminates the question associated with seldom or never used systems as to adequate performance on demand.

A steam/water dump system is provided to minimize the amount of water that could leak into the primary coolant as a result of a steam generator tube or subheader rupture. On indication of high moisture level in the primary coolant, the plant protective system will act to scram the reactor, stop the helium circulators and the feedwater flow to the affected loop, dump water and steam from the leaking steam generator into a dump tank, and rapidly cool the core utilizing the intact primary coolant loop.

In order to limit the amount of water that could leak into the primary coolant system from steam generator failures before the steam/water dump system terminates the leakage, each steam generator is provided with feedwater flow limiters.

The turbine plant design is conventional utilizing 1000°F superheated and 1000°F reheated steam.

The reactor is controlled by the selective movement of 37 control rod pairs. Interlocks are provided to prohibit rod withdrawal in the event of inadequate source neutron flux indication, short reactor period, high neutron flux level, or incorrect operator action regarding the sequencing of certain safety functions.

When the reactor is scrammed by a signal from the Plant Protection System *or by the operator, all 37 control rod pairs are driven into the core by gravity.

In addition, a reserve shutdown system for emergency use is provided which is completely independent of the control rods and drives. It utilizes neutron absorbing material consisting of boron in spherical form. The approximately 1/2 inch diameter spheres are stored in a hopper in each refueling penetration from which they can be released, if required, by the operator and allowed to fall into channels in the core. This system can shut down the reactor from any credible operating condition and hold the reactor subcritical without any control rod insertion.

Fourteen channels of nuclear instrumentation are provided for neutron flux monitoring and control. Redundant channels are provided with individual indication and alarm. The Plant Protection System uses redundant nuclear and process inputs in coincidence and includes SCRAM and automatic coolant loop shutdown.

* The Plant Protection System includes the SCRAM Protection System which is described in more detail in Appendix E.

The electrical system for an HTGR plant shares, along with similar systems of other nuclear power reactor concepts, the provision of an assured and adequate electric power supply to vital loads and instrument systems in the event of equipment malfunction or accident. Accordingly, the system has the following independent dependable sources of electricity physically isolated so that any phenomenon causing one source to fail will not cause failure of other sources:

1. Main generator via a unit auxiliary transformer.
2. Four 230-kv transmission lines via a reserve auxiliary transformer.
3. Two standby generator sets.
4. Two DC batteries.

A number of auxiliary and emergency systems and facilities are provided to perform certain functions necessary for the operation and maintenance of the plant. Among these are the fuel handling and storage system, auxiliary handling equipment and facilities, the decontamination system, the helium purification system, the helium storage system, the nitrogen system, the reactor plant cooling water system, service water, domestic water, fire protection systems, the instrument and service air systems, and the building heating system.

III. PLANT OPERATION

During operations of the Fort St. Vrain Nuclear Power Plant, the Technical Specifications (Reference 3) indicate that the following type people will be involved in all human interfaces considered during this study.

Administrative Personnel

[1]Plant Superintendent

[1]Assistant Superintendent

Operating Personnel

[1]Shift Supervisor (1/Shift)

[2]Reactor Operator (1/Shift)

[2]Equipment Operator (1/Shift)
Equipment Operator (1/Shift)
Auxiliary Tender (1/Shift)

Senior Results Engineer
Maintenance Supervisor
Senior Health Physicist and Chemist

The Technical Specifications also indicate that:

1. A licensed senior operator shall be present on-site at all times when there is fuel in the reactor.

2. A licensed operator must be in the control room at all times when fuel is in the reactor.

3. During reactor startup, shutdown or recovery from reactor trip, two licensed operators must be in the control room. Note: Since the plant controls at Fort St.

(1) Senior Licensed Operator
(2) Licensed Operator

Vrain are not consolidated but spread out over a considerable number of consoles, credit has not been given for operator backup during the initial phases of an incident.

4. A senior licensed operator, or special "fuel handling" senior operator shall be in charge of any refueling operation.

5. An operator, or technician, qualified in radiation protection procedures, shall be present at the facility at all times that there is fuel on site.

Replacement or training of plant operatórs will normally be in accordance with the American National Standards Institute, Document No. N18.1-1971 (Reference 4), entitled, "Selection and Training of Personnel for Nuclear Power Plants."

NRC examiners administer both written and operating examinations to test the knowledge of applicants for granting the initial licenses (Reference 8). The operating tests normally consist of both an oral examination during a plant walk-through and an actual demonstration at the reactor console during a reactor startup. The scope of both portions of the operating test is the same for both operators and senior operators except that the senior operator is expected to answer questions as if he were the operator's supervisor. The scope of the oral and operating test consist of (1) reading and interpretation of control instrumentation (2) manipulation of the control equipment (3) ability to operate other facility equipment and (4) knowledge of radiological safety practices and radiation-monitoring equipment. An operator would be expected to recognize abnormal reactor/plant behavior and notify his shift supervisor, whereas the senior operator would be expected to know what to do.

The written examination for an operator consists of seven categories:

1. Principles of reactor operation
2. Features of facility design
3. General operating characteristics
4. Instrumentation and controls
5. Safety and emergency systems
6. Standard and emergency operating procedures
7. Radiation control and safety.

The written examination for the senior operator consists of the seven categories mentioned above, plus the following:

1. Reactor theory
2. Radioactive materials handling, disposal and hazards
3. Specific operating characteristics
4. Fuel handling and core parameters
5. Administrative procedures, conditions and limitations.

Recent NRC regulations require that licensed individuals participate in requalification programs as a condition for license renewal <u>without</u> examination. One requirement of the program is that a licensee must have manipulated the reactor controls or the controls of approved simulators through at least 10 reactivity changes during the 2-year tenure of his license.

IV. TASK 1. EFFECTS OF HUMAN ACTION DURING ACCIDENT SEQUENCES AND IMPACT ON HTGR SAFETY

A. Review of Accident Initiation and Progression Study

There exists a low probability that, because of various accidents and component failures, small amounts of radioactive material may escape from High Temperature Gas Cooled Reactors (HTGR's). This radioactive material may result in some exposure to the general public.

The General Atomic Company, San Diego, California, has analyzed the risk to the public for a number of such accident scenarios (Reference 2). This analysis was conducted for advanced HTGR's and not for the Fort St. Vrain plant. The dispersion calculations were taken from the Reactor Safety Study (Reference 5) (WASH-1400) and represent an average of 39 locations in the United States. This analysis is identified as the Accident Initiation and Progression Analysis (AIPA).

Three relatively high risk incidents (seven scenarios) were chosen by ERDA from the AIPA list of incidents for evaluation during this study. The incident types are:

1. Leak in the reheat steam plumbing within the PCRV (prestressed concrete reactor vessel);
2. Earthquake greater than safe shutdown, (0.1g acceleration), and
3. Loss of all off-site power.

These specific scenarios with their probabilities of occurrence are shown in Table 1. It was assumed for this study that scenarios similar to those in Table 1 may apply to the

Fort St. Vrain Nuclear Power Plant (HTGR) located 40 miles north of Denver, Colorado.

Due to differences between the Fort St. Vrain Plant and the advanced HTGR designs considered in the AIPA evaluations, it should be understood that the accident consequences and risks associated with these accidents as listed in Reference 2 apply only to the AIPA studies and not to Fort St. Vrain. The current study is not a risk analysis so the differences do not affect the conclusions. The accidents chosen appear to be suitable because they cover the range from high probability to high consequences (earthquakes) and include loss of forced cooling.

SECTION IV. TABLE 1

OCCURRENCE PROBABILITIES FOR AIPA ACCIDENTS

			Probability/Year
1.	Reheater Leaks		
	a)	Small	$4\cdot10^{-2}$
	b)	Intermediate	$1\cdot10^{-2}$
	c)	Intermediate (Delayed Ident.)	$1\cdot10^{-5}$
	d)	Large	$2\cdot10^{-3}$
2.	Earthquake		
	a)	$1.0 < \alpha < 1.2$	$1\cdot10^{-8}$
		$1.8 < \alpha < 2.0$	$2\cdot10^{-10}$
		$\left[\alpha = \left(\dfrac{\text{Earthquake Mag. of Interest}}{\text{SSE Magnitude}}\right)\right]$	
3.	Loss of Offsite Power		
	a)	Normal Loss Occurrence	$9\cdot10^{-2}$
	b)	Loss of Offsite Power and Loss of Forced Cooling (PCRV Safety Valves Open)	$1\cdot10^{-6}$

SSE - Safe Shutdown Earthquake

Table 1 indicates that small reheater leaks may occur in HTGR plants about 1.6 times in the plant's expected 40 year lifetime. Similarly, loss of offsite power, with normal ramp down and associated steam dump (radioactivity assumed below technical specification limit) is calculated to occur about 3.6 times in the plant's expected lifetime.

An intermediate reheater leak followed by normal cooldown is expected only 0.40 times in the 40 year plant life with the probability of all other postulated events being considerably lower.

It can be seen from these estimates that the risk to the general public is extremely low. However, this study was undertaken to determine the probabilities that each incident can be correctly identified by the operators and that appropriate action is subsequently undertaken. Concurrent with these evaluations, it is desirable to try to anticipate what might be the impact on systems operations during an accident progression due to errors on the part of plant operators. To initiate these studies, a knowledge of how the accident makes itself evident, and its subsequent progress is necessary along with an understanding of the planned emergency procedures and some of the more probable unplanned actions.

B. Accident Descriptions

Each accident/incident described in Table 1, its cause and possible consequences are described in this section.

1. LEAK IN REHEAT LINES WITHIN PCRV

Assumptions: Plant operating at 100% power, all parameters at nominal values:
Primary coolant 686 psia.
Reheat steam pressure inlet 638 psia.
Reheat steam pressure outlet 567 psia.

Incident: A leak develops in the reheater where reheat steam is inside the pipe. Primary coolant (He) is in contact with the outside of the pipe.

Consequences: Because of the pressure gradient, contaminated Helium leaks into the reheat steam. Steam for each loop goes to the Intermediate Pressure Turbine and to the Low Pressure Turbine. There are 3 radiation monitors in each loop which monitor the hot reheat loop headers. A trip is set at 5mr/hr on these monitors. If 2 out of 3 of these monitors trip, a large leak is indicated which initiates automatic loop shutdown in about 3 seconds by the Plant Protective System. A small leak does not actuate the trips. However, some steam from the reheat header is sampled periodically, condensed, cooled and monitored for radioactivity. There are two of these loop header condensate monitors, one in each loop. These instruments are connected to alarms and are used to help identify which loop is contributing to the small leak rates. The major portion of the steam is directed to the condenser. After the steam leaves the condenser it goes to the air ejector and demineralizer before returning to the system. The gas exhaust of the common loop air ejector also has a low level radioactivity monitor, before the gas is routed to filters then discharged to the atmosphere. Because discharge of radioactive gas may cause public exposure, it is desirable to shut down the loop which is leaking in a safe and controlled manner as soon as the leak is detected. A SCRAM while operating near full power is to be avoided if possible, since the main steam lines and steam dump components can only handle about 80% of a full steam load without causing the main line relief valves and atmospheric vent valves to open, and release contaminated steam to the atmosphere.

Case 1a - Small Reheat Leak

The automatic radiation monitors in the reheat header are not tripped. Detection of this incident is dependent upon operator recognition of an increase of radioactivity in the condensate monitor of the proper loop. Assuming this has been recognized, the operator shuts down the affected loop and reduces power to 50%. Eventually, the reactor will have to be shut down and the leaking pipe in the reheat section will be plugged.

Case lb - Intermediate Reheat Leak - Normal Cool Down

This case is the same as la except that more radioactive gas has excaped.

Case lc - Intermediate Reheat Leak - Delayed Identification

When the leak is not enough to trip the automatic radiation monitors, the radioactivity in the steam may be distributed through both loops because of mixing in the feedwater. If the monitors on the sampled condensate of both loops are not equally calibrated, equally sensitive and subject to equal background radiation, it may be difficult to determine which loop has the leak. Both loops will show increased radiation but the determination of which loop has more may be difficult. Manual purging and sampling procedures are used under these conditions to attempt to identify which loop if faulty. The delay in identification may be several hours, or for a very small leak it may be days.

Case ld - Large Reheat Leak

This leak is large enough to trip the automatic radioactivity monitors on the Loop Reheat Header. Detection and automatic initiation of a safe loop shutdown is begun within about 3 seconds.

2. EARTHQUAKE AND LOSS OF FORCED COOLING

Assumptions: The plant is operating at 100% power.

Accident: An earthquake with accelerations greater than 1.0 times SSE but less than 2.0 times SSE occurs, all off-site power is lost, the Main Turbine is tripped, and all 4 Helium Circulators fail. This is a very low probability combination of coincident failures. The earthquake could cause a loss of all off-site power. The turbine trip and the temporary loss of the Helium Circulators are independent of the loss of off site power.

Consequences: The reactor is SCRAMMED and a steam/water dump is initiated on high primary coolant temperature detection. This dump would not be serious unless reheater tubes in the PCRV have been cracked or the PCRV itself has suffered damage. Auxiliary generators are started to operate at least one helium circulator.

3. LOSS OF ALL OFF-SITE POWER

Assumptions: Plant is operated at 100% power.

Incident: Simultaneous loss of all 4 sources of off-site power.

Consequences: Two emergency diesel generators are started automatically to provide power for cooling in case the Main Generator should trip. The Main Generator is ramped down to auxiliary power requirements at the rate of approximately 1%

per minute. Excess steam is routed automatically to a desuperheater in each loop, then to a common flash tank. If off-site power is restored within 10 minutes the Main Generator may be returned to power. Otherwise, the reactor may be reduced to 1% standby power. This accident is not considered serious unless it is simultaneous with a leak in the Reheat Tubes.

Case 3a - Loss of Off-Site Power, Normal Cool Down

This incident proceeds as outlined above.

Case 3b - Loss of Off-Site Power, Loss of Forced Circulation

The consequences of the incident are the same as those for an earthquake greater than safe shutdown. Loss of forced cooling has already been discussed in Section B-2.

C. Emergency Action (Planned)

1. Reheat Steam Leaks

   a. For a large leak, the loop will shut down automatically when radioactivity in the Reheat header exceeds 5mr/hr.

   b. For small or intermediate leaks, operator action is required to identify the leaking loop, initiate loop shutdown and attempt to prevent SCRAM.

      (1) For an intermediate leak, the radioactivity monitor of sampled condensate may trip alarms which, together with the Reheat header monitors, enable the operator to determine the leaking loop.

(2) For small leaks, the radioactivity may be mixed throughout both loops before being detected. When this occurs, detailed analysis of the steam in each loop is normally required to identify the leaking loop.

c. Automatic shutdown of one loop includes the following functions:

Tripping of both circulator turbines.

Closing of the inlet and outlet valves to the circulator turbines.

Reducing main turbine generator to 50% of previous load.

Closing of the feedwater valves.

Closing of the Reheat stop-check valves.

Opening of the Main Steam By-Pass valve to direct steam to the desuperheater and then to the by-pass flash tank.

Opening of the Reheat Steam By-Pass valves to direct steam to the desuperheater and then to the main steam condenser.

d. Loop shutdown may be initiated by:
Closing the appropriate Reheat outlet stop-check valve (HS2253-Loop 1 or HS2254-Loop 2) on the control panel, and/or preferably by
tripping of the two circulator turbines in one loop.

e. System SCRAM or manual SCRAM which is to be avoided to prevent the possible release of contaminated steam, includes: Tripping of an automatic SCRAM parameter, such as Reheat Header activity, or the actuation of the Manual SCRAM button by the Operator.

Opening of main steam and reheat steam by-pass valves to direct water/steam into desuperheaters and reheat attemperators and from there to the flash tank and main steam condenser.

Opening of main steam and reheat steam relief valves and release of about 20% of the contaminated steam to atmosphere.

Closing of feedwater valves.

Closing of Reheat stop-check valves.

2. Earthquake

a. If there have been no breaks in pipes, no loss of off-site power, no turbine trip or other results which initiate SCRAM or automatic shutdown, the operator must check all seismoscopes and process all accelerographs as soon as possible. Any indication of horizontal accelerations $\geq$0.1g requires immediate initiation of plant shutdown. Any indication of horizontal accelerations $\geq$0.05g requires visual inspection of Class I pipes and equipment.

b. If the earthquake is accompanied by loss of all off-site power and/or main turbine trip, required actions are as outlined in the section describing those incidents, except that complete plant shutdown is necessary if the accelerations exceed 0.1g. If forced circulation is to be maintained after an earthquake, the operator must maintain the electrical, steam and water supplies until safe shutdown has been accomplished.

c. The worst situation is the Loss of Forced Circulation plus loss of off-site power. In this situation, all four of the Helium circulators are inoperable by either the normal steam turbines or the emergency water turbines, and the main turbine must be tripped.

In this situation the reactor must be SCRAMMED, if not already in that state.

The reserve shutdown system may be operated after about 5 hours, when it becomes apparent that the loss of forced circulation is permanent.

The primary coolant (Helium) system must be gradually depressurized to slightly less than atmospheric pressure through the Helium purification system.

The PCRV water coolant system must continue to operate to insure integrity of the PCRV.

The reactor building ventilation system must continue to operate to filter any leakage before venting to the atmosphere.

The core will heat to a maximum of 5400°F after 83 hours, destroying most of the metal components within the PCRV and much of the fuel coating. The reactor must continue to be cooled by the PCRV water coolant system until the reactor is cool enough for repairs. This may take a year. The operator must insure a supply of PCRV cooling water and electricity for the reactor building ventilation system.

3. Loss of All Off-Site Power

a. Without Main Turbine Trip, the operator may choose to initiate automatic shutdown or standby for return to power.

If he chooses to initiate shutdown, the main turbine load will be reduced to auxiliary requirements.

The standby diesel generators will be started automatically and manually synchronized to the main generator. At this point, the auxiliary load must be transferred to the diesel generators.

The main turbine must be manually tripped during automatic load shedding, superheated steam will be by-passed to the desuperheater and then to the by-pass flash tank. Reheat steam will be by-passed to the attemperator, then to the main condenser. Steam will still be available to operate the auxiliary steam turbines. However, most of the steam operated equipment will be shut down as listed in Table 2 and reactor power will be reduced to less than 1%.

b. Loss of off-site power with Main Turbine Trip: The operator must immediately initiate automatic shutdown as above. If outside power is not restored within approximately 10 minutes, the operator must SCRAM the reactor. During these 10 minutes some steam is being released to the atmosphere. Between the time the Main Turbine trips and the availability of auxiliary power from the diesel generators there is a 15 second delay when emergency auxiliary systems must rely on the DC batteries.

SECTION IV - TABLE 2

INITIATING SEQUENCE OF SAFE SHUTDOWN EQUIPMENT

SEQUENCE	HORSE POWER	TWO STANDBY GENERATORS AVAILABLE EQUIPMENT STARTED	ONE STANDBY GENERATOR AVAILABLE EQUIPMENT STARTED
1	150	Service Water Pump	Service Water Pump
2	50	Service Water Return Pump	Service Water Return Pump
3	7-1/2	Purification Cooling Water Pump	Purification Cooling Water Pump
	7-1/2	Purification Cooling Water Pump	
4	125	Helium Circulator Bearing Water Pump	Helium Circulator Bearing Water Pump
[a]	125	Helium Circulator Bearing Water Pump	
5	125	Helium Circulator Bearing Water Pump	Helium Circulator Bearing Water Pump
[a]	125	Helium Circulator Bearing Water Pump	Helium Circulator Bearing Water Pump
6	20	Bearing Water Removal Pump	Bearing Water Removal Pump
[a]	7-1/2	Buffer Helium Recirculator	Buffer Helium Recirculator
	7-1/2	Buffer Helium Recirculator	
7	250	Circulating Water Pump	
8	100	Reactor Plant Cooling Water Pump	Reactor Plant Cooling Water Pump
[a]	100	Reactor Plant Cooling Water Pump	
9	60	EHC Fluid Pump[b]	EHC Fluid Pump[b]
10	20	Hydraulic Pump (for valve actuator)	Hydraulic Pump (for valve actuator)
[a]	20	Hydraulic Pump (for valve actuator)	Hydraulic Pump (for valve actuator)
11	150	Condensate Pump	Condensate Pump
13	60	Instrument Air Compressor	Instrument Air Compressor
14	5 kw	Reactor Plant Valve Actuators	Reactor Plant Valve Actuators
	5 kw	Turbine Plant Valve Actuators	Turbine Plant Valve Actuators
15	60	Helium Purification Comp. M-G Set	Helium Purification Comp. M-G Set
16	20	Helium Recovery Compressor	

[a] Operated on other Standby generator.
[b] Not on Safe Shutdown List (Reference 9).

SECTION IV - TABLE 2 (Continued)

INITIATING SEQUENCE OF SAFE SHUTDOWN EQUIPMENT

SEQUENCE	HORSE POWER	TWO STANDBY GENERATORS AVAILABLE EQUIPMENT STARTED	ONE STANDBY GENERATOR AVAILABLE EQUIPMENT STARTED
17	30	Gas Waste Compressor	Purification Cooling Water Pump
	1-1/2	Gas Waste Blower	Gas Waste Blower
18	50	Reactor Plant Exhaust Fan[b]	Reactor Plant Exhaust Fan[b]
[a]	50	Reactor Plant Exhaust Fan[b]	
20	37-1/2	Main Cooling Tower Fan[b]	
[a]	37-1/2	Main Cooling Tower Fan[b]	
[a]	7-1/2	Service Water Cooling Tower Fan[b]	Service Water Cooling Tower Fan[b]
	1/2	Battery Room Exhaust Fan[b]	Battery Room Exhaust Fan[b]
	1/2	Battery Room Exhaust Fan[b]	Battery Room Exhaust Fan[b]
	25	Control Room Supply Fan	
22	50	Control Room Water Chill	
[a]	15	Control Room Return Fan	
23	7-1/2	Gland Seal Steam Exhaust[b]	
	3	Standby Generator - Air Compressor	Standby Generator - Air Compressor
	3	Standby Generator - Air Compressor	Standby Generator - Air Compressor
	10	H_2 Seal Oil Pump[b]	H_2 Seal Oil Pump[b]
	5	Service Water Booster Pump	Service Water Booster Pump
24	25	Turbine Turning Gear Oil Pump[b]	Turbine Turning Gear Oil Pump[b]
	3	BFP 1B Auxiliary Lube Oil Pump[b]	BFP 1B Auxiliary Lube Oil Pump
25	150	Bearing Water Makeup Pump	Bearing Water Makeup Pump
26	3	Reactor Building Sump Pump	Reactor Building Sump Pump[b]
	7-1/2	Liquid Waste Sump Pump	Liquid Waste Sump Pump[b]
	25	BFP 1A Auxiliary Lube Oil Pump	BFP 1A Auxiliary Lube Oil Pump
[a]	25	BFP 1C Auxiliary Lube Oil Pump	BFP 1C Auxiliary Lube Oil Pump

[a] Operated on other Standby generator.

[b] Not on Safe Shutdown List (reference 9).

SECTION IV - TABLE 2 (Continued)

INITIATING SEQUENCE OF SAFE SHUTDOWN EQUIPMENT

SEQUENCE	HORSE POWER	TWO STANDBY GENERATORS AVAILABLE EQUIPMENT STARTED	ONE STANDBY GENERATOR AVAILABLE EQUIPMENT STARTED
27	150	Circ. Water Makeup Pump	Circ. Water Makeup Pump
	150	Turbine Water Removal Pump	Turbine Water Removal Pump
		Instrument Air Dryer Package Unit	
28	10	Control Room Emergency Filter Fan	Control Room Emergency Filter Fan
29	200	Reactor Plant Water Chiller	Reactor Plant Water Chiller
30	100	Auxiliary Boiler Feedpump	Auxiliary Boiler Feedpump
31	200	Miscellaneous	Miscellaneous

a Operated on other standby generator.

b Not on Safe Shutdown List (Reference 9).

D. Emergency Action (Unplanned)

Under high stress conditions there exists a significant potential for inappropriate or wrong decisions to be made by human operators. Some of these decisions could result in aggravating the accident progression.

A multi-level appraoch has been used to identify the most probable choices in the spectrum of operator decisions for each of the major incidents in question.

The first item in the approach has been the construction of a set of Event Flow Diagrams which give an overview of the top level events which may be encountered during each of the postulated incidents. From these charts, a set of Human Interaction Matrices can be generated which itemize the gross spectrum of operator actions which might be realized for each incident. The Event Flow Diagrams are depicted in Figures 3A through 3C. The Human Interaction Matrices are given in Tables 3, 4 and 5.

The events in the Human Interaction Matrix are indicative of both expected responses from the operator and some of the more probable unexpected responses which he might make. It is not intended to be all inclusive, but all inappropriate responses will generally bring about an unanticipated SCRAM or an automatic loop shutdown depending upon whether one loop was previously locked out or not prior to the operator's action.

The HIM Table is read in the folowing manner:

> The events preceded by item number 1 constitute the first action branch and should be read in successive order, i.e., Events 1-1, 1-2. 1-3,...1-7: This should be followed by action branch 2 which is read in the same manner. It is not necessary for any action branch that the first event start with x-1, x-2, etc.; it may well start and end as with branch 2 in Table 3 with 2-5, and 2-7. The remainder of the action branches are read in a similar manner.

Most actions which might be performed by the operator involve the operation or non-operation of various plant controls located on the operator console. There are a multiplicity of controls which are available to operators in the Fort St. Vrain control room. Under high stress conditions, it is quite probable that at certain times the operator can inadvertently select the wrong control. Some of the consequences of this action are discussed under System Impact, Section I. To assign the probabilities for operator action, an Emergency Decision Chart (EDC-1), Figure 4A, was drawn up for the Reheat Steam Leak Accident.

Figure 4A of the EDC-1 contains each important operator action depicted in the Human Interaction Matrix (Table 3).

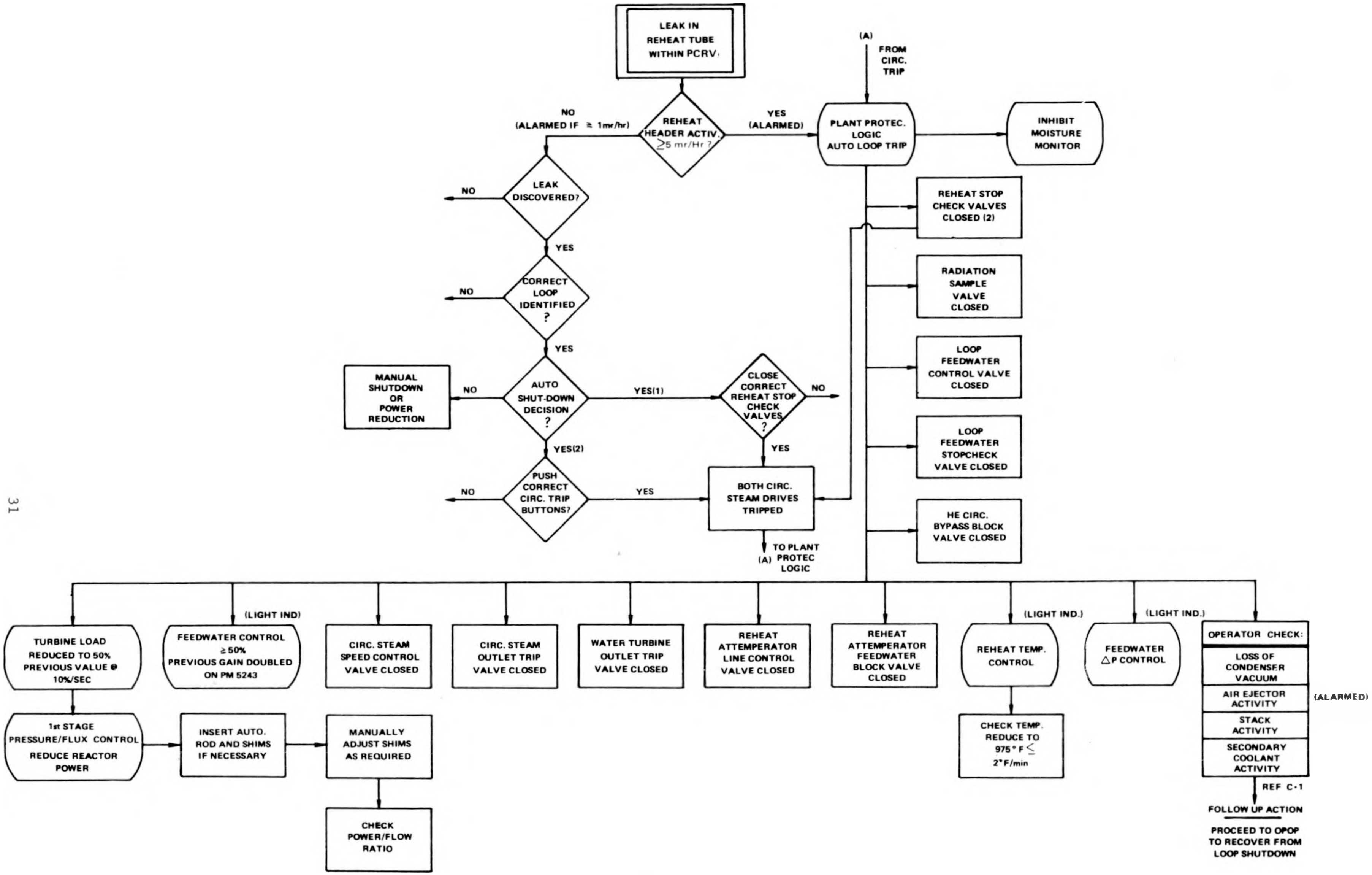

LEAK IN REHEAT TUBE WITHIN PCRV
REHEAT HEADER ACTIV. ≥5 mr/Hr ?
NO (ALARMED IF ≥ 1mr/hr)
YES (ALARMED)
(A) FROM CIRC. TRIP
PLANT PROTEC. LOGIC AUTO LOOP TRIP
INHIBIT MOISTURE MONITOR
LEAK DISCOVERED?
NO
YES
CORRECT LOOP IDENTIFIED ?
NO
YES
AUTO SHUT-DOWN DECISION ?
NO
MANUAL SHUTDOWN OR POWER REDUCTION
YES(1)
CLOSE CORRECT REHEAT STOP CHECK VALVES ?
NO
YES
YES(2)
PUSH CORRECT CIRC. TRIP BUTTONS?
NO
YES
BOTH CIRC. STEAM DRIVES TRIPPED
(A) TO PLANT PROTEC LOGIC
REHEAT STOP CHECK VALVES CLOSED (2)
RADIATION SAMPLE VALVE CLOSED
LOOP FEEDWATER CONTROL VALVE CLOSED
LOOP FEEDWATER STOPCHECK VALVE CLOSED
HE CIRC. BYPASS BLOCK VALVE CLOSED
TURBINE LOAD REDUCED TO 50% PREVIOUS VALUE @ 10%/SEC
(LIGHT IND)
FEEDWATER CONTROL ≥ 50% PREVIOUS GAIN DOUBLED ON PM 5243
CIRC. STEAM SPEED CONTROL VALVE CLOSED
CIRC. STEAM OUTLET TRIP VALVE CLOSED
WATER TURBINE OUTLET TRIP VALVE CLOSED
REHEAT ATTEMPERATOR LINE CONTROL VALVE CLOSED
REHEAT ATTEMPERATOR FEEDWATER BLOCK VALVE CLOSED
(LIGHT IND.)
REHEAT TEMP. CONTROL
(LIGHT IND.)
FEEDWATER ΔP CONTROL
OPERATOR CHECK:
LOSS OF CONDENSER VACUUM
AIR EJECTOR ACTIVITY
(ALARMED)
STACK ACTIVITY
SECONDARY COOLANT ACTIVITY
REF C-1
FOLLOW UP ACTION
PROCEED TO OPOP TO RECOVER FROM LOOP SHUTDOWN
1st STAGE PRESSURE/FLUX CONTROL REDUCE REACTOR POWER
INSERT AUTO. ROD AND SHIMS IF NECESSARY
MANUALLY ADJUST SHIMS AS REQUIRED
CHECK POWER/FLOW RATIO
CHECK TEMP. REDUCE TO 975° F ≤ 2° F/min

FIGURE 3-A

EVENT FLOW DIAGRAM
REHEATER LEAK ACCIDENT

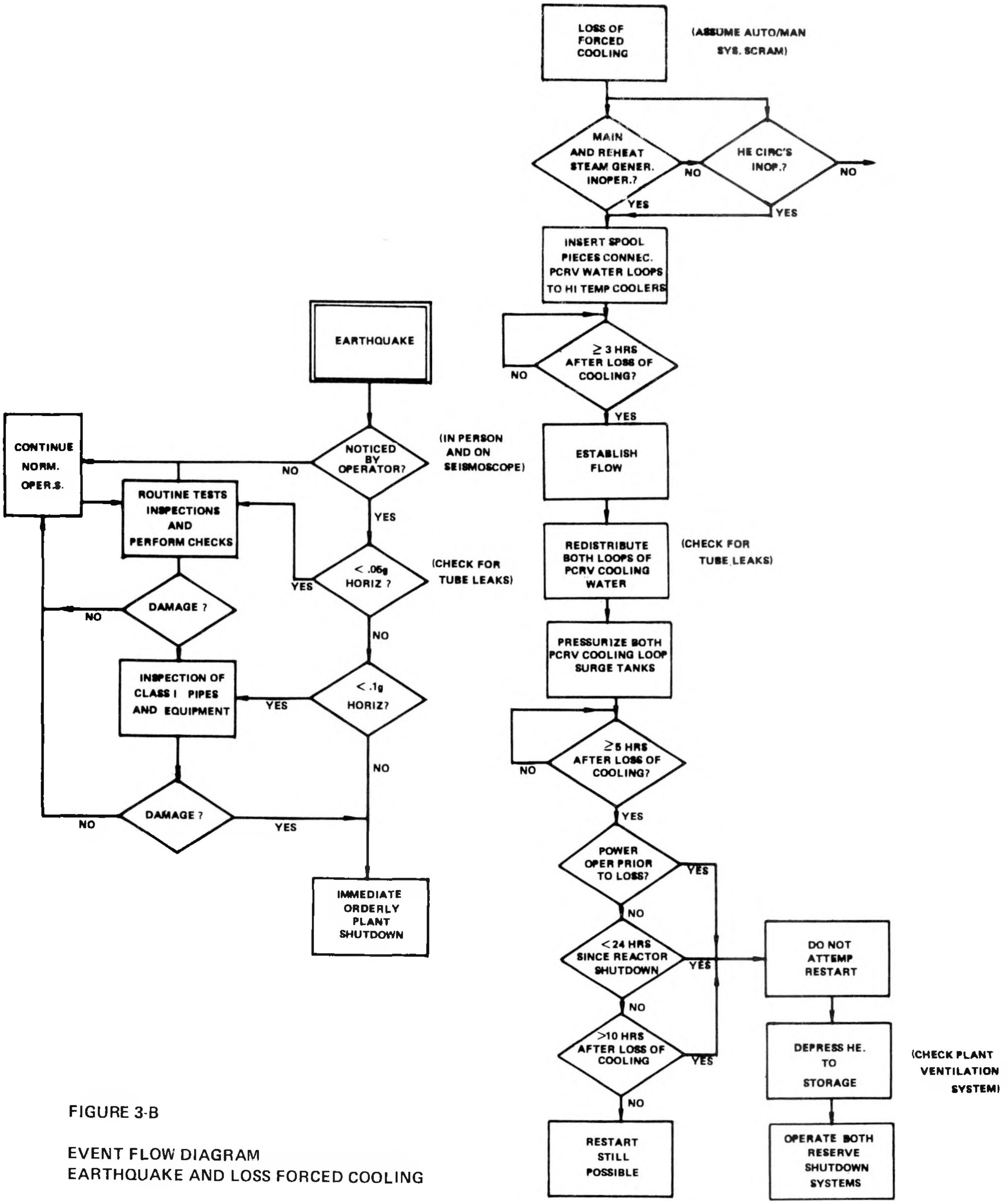

LOSS OF FORCED COOLING
(ASSUME AUTO/MAN SYS. SCRAM)
MAIN AND REHEAT STEAM GENER. INOPER.?
NO
HE CIRC'S INOP.?
NO
YES
YES
INSERT SPOOL PIECES CONNEC. PCRV WATER LOOPS TO HI TEMP COOLERS
≥ 3 HRS AFTER LOSS OF COOLING?
NO
YES
ESTABLISH FLOW
REDISTRIBUTE BOTH LOOPS OF PCRV COOLING WATER
(CHECK FOR TUBE LEAKS)
PRESSURIZE BOTH PCRV COOLING LOOP SURGE TANKS
≥5 HRS AFTER LOSS OF COOLING?
NO
YES
POWER OPER PRIOR TO LOSS?
YES
NO
<24 HRS SINCE REACTOR SHUTDOWN
YES
NO
>10 HRS AFTER LOSS OF COOLING
YES
NO
RESTART STILL POSSIBLE
DO NOT ATTEMP RESTART
DEPRESS HE. TO STORAGE
(CHECK PLANT VENTILATION SYSTEM)
OPERATE BOTH RESERVE SHUTDOWN SYSTEMS
EARTHQUAKE
NOTICED BY OPERATOR?
(IN PERSON AND ON SEISMOSCOPE)
NO
CONTINUE NORM. OPER.S.
YES
ROUTINE TESTS INSPECTIONS AND PERFORM CHECKS
< .05g HORIZ ?
(CHECK FOR TUBE LEAKS)
YES
NO
DAMAGE ?
NO
< .1g HORIZ?
YES
INSPECTION OF CLASS I PIPES AND EQUIPMENT
NO
DAMAGE ?
NO
YES
IMMEDIATE ORDERLY PLANT SHUTDOWN

FIGURE 3-B

EVENT FLOW DIAGRAM
EARTHQUAKE AND LOSS FORCED COOLING

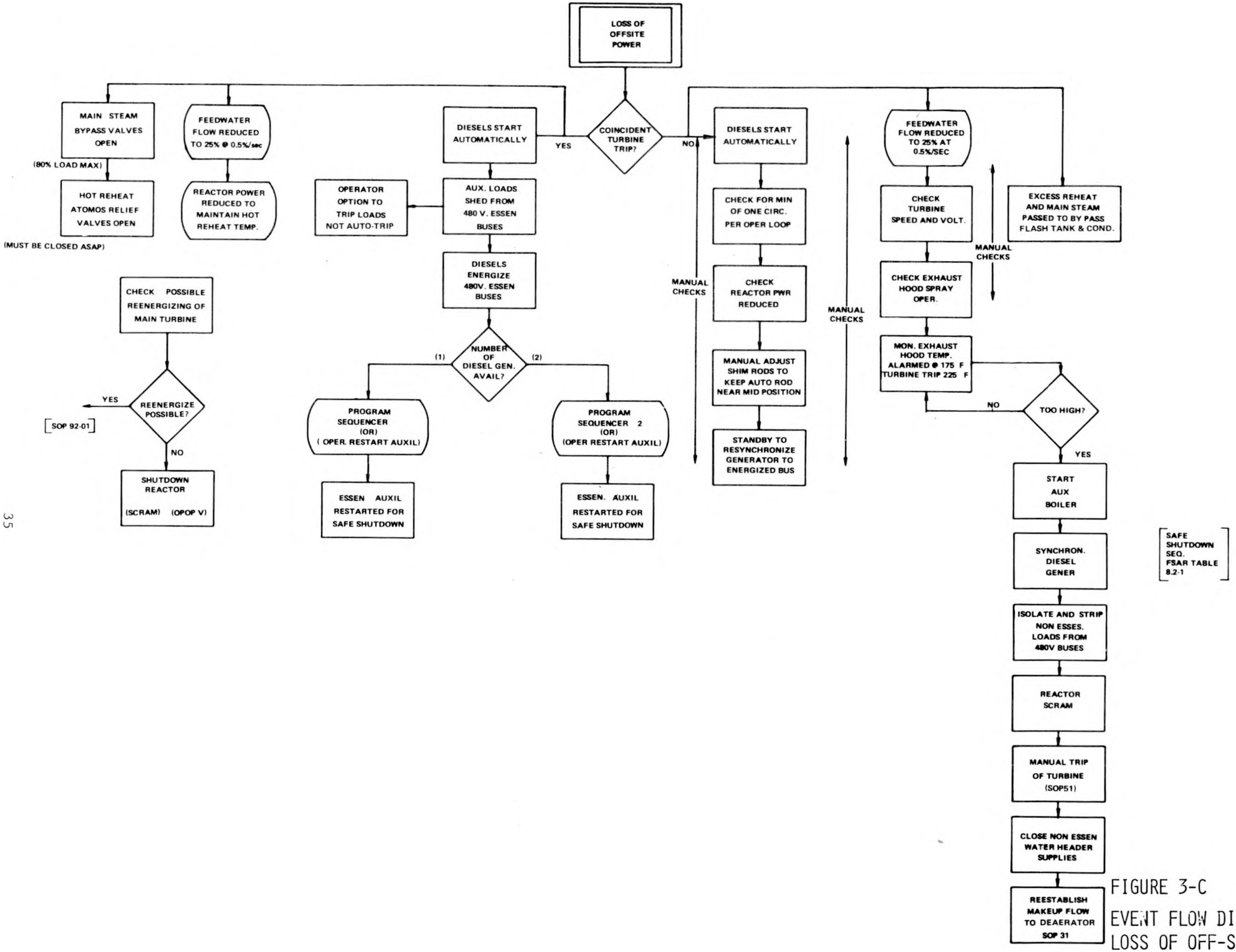

LOSS OF OFFSITE POWER
COINCIDENT TURBINE TRIP?
YES
NO
MAIN STEAM BYPASS VALVES OPEN
(80% LOAD MAX)
HOT REHEAT ATOMOS RELIEF VALVES OPEN
(MUST BE CLOSED ASAP)
FEEDWATER FLOW REDUCED TO 25% @ 0.5%/sec
REACTOR POWER REDUCED TO MAINTAIN HOT REHEAT TEMP.
CHECK POSSIBLE REENERGIZING OF MAIN TURBINE
REENERGIZE POSSIBLE?
YES
[SOP 92-01]
NO
SHUTDOWN REACTOR (SCRAM) (OPOP V)
DIESELS START AUTOMATICALLY
AUX. LOADS SHED FROM 480 V. ESSEN BUSES
OPERATOR OPTION TO TRIP LOADS NOT AUTO-TRIP
DIESELS ENERGIZE 480V. ESSEN BUSES
NUMBER OF DIESEL GEN. AVAIL?
(1)
(2)
PROGRAM SEQUENCER (OR) (OPER. RESTART AUXIL)
PROGRAM SEQUENCER 2 (OR) (OPER RESTART AUXIL)
ESSEN AUXIL RESTARTED FOR SAFE SHUTDOWN
ESSEN. AUXIL RESTARTED FOR SAFE SHUTDOWN
MANUAL CHECKS
DIESELS START AUTOMATICALLY
CHECK FOR MIN OF ONE CIRC. PER OPER LOOP
CHECK REACTOR PWR REDUCED
MANUAL ADJUST SHIM RODS TO KEEP AUTO ROD NEAR MID POSITION
STANDBY TO RESYNCHRONIZE GENERATOR TO ENERGIZED BUS
MANUAL CHECKS
FEEDWATER FLOW REDUCED TO 25% AT 0.5%/SEC
CHECK TURBINE SPEED AND VOLT.
CHECK EXHAUST HOOD SPRAY OPER.
MON. EXHAUST HOOD TEMP. ALARMED @ 175 F TURBINE TRIP 225 F
MANUAL CHECKS
EXCESS REHEAT AND MAIN STEAM PASSED TO BY PASS FLASH TANK & COND.
TOO HIGH?
NO
YES
START AUX BOILER
SYNCHRON. DIESEL GENER
ISOLATE AND STRIP NON ESSES. LOADS FROM 480V BUSES
REACTOR SCRAM
MANUAL TRIP OF TURBINE (SOP51)
CLOSE NON ESSEN WATER HEADER SUPPLIES
REESTABLISH MAKEUP FLOW TO DEAERATOR SOP 31
[SAFE SHUTDOWN SEQ. FSAR TABLE 8.2-1]

FIGURE 3-C

EVENT FLOW DIAGRAM
LOSS OF OFF-SITE POWER ACCIDENT

SECTION IV - TABLE 3

HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1 Initiating Event	2 Indications	3 Operator Action (1)	4 Operator Action (2)	5 Operator Action (3)	6 Operator Action (4)	7 Physical Results
1-1 Radioactive primary coolant mixes with reheat steam.	1-2 Monitors in Loop Sample condensate or air ejector show increase in activity.	1-3 Operator notes increase in condensate monitor.	1-4 Operator decides to shutdown affected loop.	1-5 Operator pushes correct circulator trip switches (CA)		*1-7 Automatic loop shutdown initiated.
				2-5 Operator pushes incorrect C/T switches.		*2-7 Wrong loop shutdown initiated.
				3-5 Operator turns correct Reheat Stop Check valve switch (RSC).		3-7 Automatic loop shutdown initiated.
				4-5 Operator turns incorrect RSC valve switch.		*4-7 Wrong loop shutdown initiated.
			5-4 Operator decides not to act			5-7 Loop shutdown initiated by RHA activity monitors.
		6-3 Operator does not notice increase in condensate monitor.				*6-7 Activity begins to increase in air ejector monitor.
7-1 Wrong loop shutdown in process.	7-2 Activity monitors continue to increase rather than decrease	7-3 Operator notes increasing activity levels.	7-4 Operator decides to reverse operating loop.	7-5 Operator shuts down plant and restarts on good loop.		7-7 One loop down; other loop brought up to 50% power.
			8-4 Operator decides not to act.			8-7 Plant SCRAM by RHA activity monitors.
		9-3 Operator does not notice increase in activity monitors.				9-7 Plant SCRAM by RHA activity monitors.

*Denotes Initiating Events

SECTION IV - TABLE 3 (Continued)

HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1	2	3	4	5	6	7
Initiating Event	Indications	Operator Action (1)	Operator Action (2)	Operator Action (3)	Operator Action (4)	Physical Results
10-1 Air ejector increasing in activity.	10-2 Air ejector monitors continue to show increase in activity.	10-3 Operator notes increase in air ejector monitor.	10-4 Operator starts faulty loop identification tests.	10-5 Operator correctly identifies faulty loop.	10-6 Operator decides to shut-down affected loop.(See 1-4)	10-7* Loop shut-down initiated.
					11-6 Operator decides to not act. (See 5-4)	11-7 Loop shutdown initiated auto. by RHA monitors
				12-5 Operator does not identify faulty loop.		12-7 Loop shutdown initiated auto. by RHA monitors.
			13-4 Operator decides to reduce overall Plant power.			13-7 Power reduction without loop shutdown.
			14-4 Operator decides to not act.			14-7 Loop shutdown initiated auto. by RHA monitors.
		15-3 Operator does not notice increase in air ejector monitors.				15-7 Loop shutdown initiated auto. by RHA monitors.

*Denotes Initiating Events

SECTION IV - TABLE 3 (Continued)

HUMAN INTERACTION MATIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1 Initiating Event	2 Indications	3 Operator Action (1)	4 Operator Action (2)	5 Operator Action (3)	6 Operator Action (4)	7 Physical Results
1-1 Automatic loop or Plant shutdown.		1-3 Reheat stop check valve closes.	1-4 (None)			1-7 Loop shutdown continues.
	2-2 Valve light incorrect.	2-3 (RSC valve does not close).	2-4 Manual closure			2-7 Loop shutdown continues.
		3-3 Radiation sampling valve closes	3-4 (None)			3-7 Loop snutdown continues.
	4-2 Valve light incorrect.	4-3 (Does not close).	4-4 Manual closure			4-7 Loop shutdown continues.
		5-3 Loop feedwater control valve closes.	5-4 (None)			5-7 Loop shutdown continues.
	6-2 Valve light incorrect.	6-3 (Does not close.	6-4 Manual closure			6-7 Loop shutdown continues.
		7-3 Loop feedwater stop/check valve closes.	7-4 (None)			7-7 Loop shutdown continues.
	8-2 Valve light incorrect.	8-3 (Does not close).	8-4 Manual closure			8-7 Loop shutdown continues.
		9-3 Circulator bypass block valve closes.	9-4 (None)			9-7 Loop shutdown continues.
	10-2 Valve light incorrect.	10-3 (Does not close).	10-4 Manual closure			10-7 Loop shutdown continues.
		11-3 Turbine load reduction by 50%	11-4 (None)			11-7 Loop shutdown continues.
	12-2 Valve light incorrect.	12-3 (Does not shed load)	12-4 Manual load reduction.			12-7 Loop shutdown continues.

SECTION IV - TABLE 3 (Continued)
HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1 Initiating Event	2 Indications	3 Automatic Action	4 Operator Action (1)	5 Operator Action (2)	6 Physical Results
(Automatic Loop or Plant shutdown continued)					
13-1 Programmed reactor pressure and flux reduction.	13-2 Rates of change of nuclear flux and primary coolant pressure nominal.	13-3 Shim rod insertion.			
	14-2 Flux or pressure not nominal	-	14-4 Operator notes need for shim rod correction.	14-5 Operator adjusts shim rod correctly.	14-6 Loop shutdown continues.
				15-5 Operator causes incorrect shim rod adjustment.	15-6 *Reactor power increases, or,
					16-6 *Reactor power drop rate exceeds specification.
			17-4 Operator does not notice need for shim rod adjustment.		17-6 *Automatic shutdown stops, or,
					18-6 Turbine trip, Main SCRAM.
19-1 Automatic shutdown stops.	19-2 Activity monitors show no change.		19-4 Operator switches to manual control.		19-6 Manual Plant shutdown.
			20-4 Operator does not act.		20-6 System SCRAM on RHA monitors.
21-1 Reactor Power Increases.	21-2 Flux and pressure monitors show rise.	21-3 Rod Inhibit on flux level	21-4 Operator notes increasing power.	21-5 Operator inserts shim rods.	21-6 Power levels off and starts to drop, shutdown continues.
			22-4 Operator does not notice increasing power.		22-6 SCRAM on overflux level.
23-1 Power drop rate exceeds specification.	23-2 Flux and pressure rate of change too fast.		23-4 Operator notes rate of change too fast.	23-5 Operator withdraws shim rods.	23-6 Power drop slows and reverses, shutdown continues.
			24-4 Operator does not notice rate of change.		24-6 Turbine trip, manual SCRAM.

SECTION IV - TABLE 3 (Continued)

HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

Initiating Event 1	Indications 2	Automatic Action 3	Operator Action (1) 4	Operator Action (2) 5	Physical Results 6
(Automatic loop or Plant shutdown continued)					
		25-3 Feedwater flow valve adjusted.	25-4 (None)		25-6 Loop shutdown continues.
	26-2 Feedwater flow rate outside spec.	26-3 (Not adjusted corrected).	26-4 Manual adjustment.		26-6 Loop shutdown continues.
		27-3 Circulator steam speed control valve closes.	27-4 (None)		27-6 Loop shutdown continues.
	28-2 Valve light incorrect.	28-3 (Does not close).	28-4 Manual closure		28-6 Loop shutdown continues.
		29-3 Circulator steam outlet trip valve closed.	29-4 (None)		29-6 Loop shutdown continues.
	30-2 Valve light incorrect.	30-3 (Does not close).	30-4 Manual closure.		30-6 Loop shutdown continues.
		31-3 Water turbine outlet steam trip valve closed.	31-4 (None)		31-6 Loop shutdown continues.
	32-2 Valve light incorrect.	32-3 (Does not close).	32-4 Manual closure		32-6 Loop shutdown continues.
		33-3 Reheat header attemperator line control valve close.	33-4 (None)		33-6 Loop shutdown continues.
	34-2 Valve light incorrect.	34-3 (Does not close).	34-4 Manual closure.		34-6 Loop shutdown continues.
		35-3 Rehat header attemperator feed water block valve closed.	35-4 (None)		35-6 Loop shutdown continues.
	36-2 Valve light incorrect.	36-3 (Does not close).	36-4 Manual closure.		36-6 Loop shutdown continues.

SECTION IV - TABLE 3 (Continued)

HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1 Initiating Event	2 Indications	3 Automatic Action	4 Operator Action (1)	5 Operator Action (2)	6 Physical Results
(Automatic loop or Plant shutdown continued)					
37-1 Reheat header temperature reduction abnormal	37-2 Rate change RH temperature outside specification.		37-4 Operator notes temperature rate change too fast.	37-5 Operator readjusts feedwater flow correctly.	37-6 Loop shutdown continues.
				38-5 Operator readjusts feedwater flow incorrectly.	38-6 Turbine Trip, Manual SCRAM
			39-4 Operator does not notice rate of temperature change.		39-6 Turbine Trip, Manual SCRAM
40-1 Condenser vacuum incorrect.	40-2 Condenser pressure monitors show abnormal readings.		40-4 Operator notes incorrect condenser pressure.	40-5 Operator isolators condenser.	40-6 Loop shutdown continues.
				41-5 Operator fails to isolate condenser.	41-6 Turbine Trip, Manual SCRAM
			42-4 Operator does not note incorrect pressure.		42-6 Turbine Trip, Manual SCRAM
43-1 Abnormal Stack activity.	43-2 Stack monitors show abnormal activity.		43-4 Operator notes abnormal stack activity.	43-5 Operator reduces overall Plant power.	43-6 Power reduction initiated. Loop shutdown continues.
				44-5 Operator does not act immediately.	44-6 Delayed RHA or Manual SCRAM
			45-4 Operator does not notice stack activity.		45-6 Delayed RHA or Manual SCRAM

SECTION IV - Table 3 (Continued)

HUMAN INTERACTION MATRIX (HIM)

SLOW LEAK IN REHEAT STEAM PIPE WITHIN STEAM GENERATOR

1 Initiating Event	2 Indications	3 Automatic Action	4 Operator Action (1)	5 Operator Action (2)	6 Physical Results
46-1 Abnormal AIR ejector activity.	46-2 Air ejectors show abnormal activity.		46-4 Operator notes abnormal air ejector activity.	46-5 Operator reduces overall Plant power.	46-6 Power reduction initiated. Loop shutdown continues.
				47-5 Operator does not act immediately.	47-6 Delayed RHA or Manual SCRAM
			48-4 Operator does not notice air ejector activity.		48-6 Delayed RHA or Manual SCRAM
49-1 Abnormal activity in Primary Coolant	49-2 RHA monitor show increase in activity.		49-4 Operator notes increase in steam activity at RHA monitors.	49-5 Operator acts to reduce overall plant power.	49-6 Power reduction initiated. Loop shutdown continues.
				50-5 Operator does not immediately act.	50-6 Delayed RHA or Manual SCRAM.
			51-4 Operator does not notice increase in RHA monitors.		51-6 Delayed RHA or Manual SCRAM.
52-1 Automatic Loop shutdown complete.					52-6 One Loop down. Other loop at 50% power.

SECTION IV- TABLE 4

HUMAN INTERACTION MATRIX (HIM)

1. EARTHQUAKE

1 Initiating Event	2 Indications	3 Operator Action (1)	4 Operator Action (2)	5 Operator Action (3)	6 Operator Action (4)	7 Physical Results
1-1 Earthquake near site.	1-2 Earthquake alarm triggered.	1-3 Alarm noticed by operator.	1-4 Seismic amplitude check initiated.	1-5 Amplitude >SSE.	1-6 Initiate normal Plant shutdown.	1-7 (See Plant Shutdown).
					2-6 Decide for emergency shutdown	2-7 Manual SCRAM.
				3-5 Amplitude >DBE <SSE.	3-6 Inspect for major damage.	3-7 Possible shutdown.
					4-6 Decide for orderly shutdown.	4-7 Plant shutdown.
				5-5 Amplitude <DBE.	5-6 Institute routine inspection and tests.	5-7 Continue operating.
			6-4 Amplitude check not initiated.			6-7 Manual SCRAM
		7-3 Alarm not noticed by operator.				7-7 Delayed Manual SCRAM.
	8-2 Earthquake alarm <u>not</u> triggered.	8-3 Shock felt by operator.	8-4 (Go to 1-4)			
		9-3 Shock not felt by operator.				9-7 Delayed Manual SCRAM.

SECTION IV- TABLE 4 (Continued)

HUMAN INTERACTION MATRIX (HIM)

2. LOSS OF FORCED COOLING

1 Initiating Event	2 Indications	3 Operator Action (1)	4 Operator Action (2)	5 Operator Action (3)	6 Operator Action (4)	7 Physical Results
10-1 Earthquake	10-2 Loss of Primary Coolant pressure (one loop).	10-3 Low reactor pressure (TLT) channel triggered.				10-7 Automatic loop shutdown initiated.
		11-3 TLT action fails.	11-4 Manual initiation of loop shutdown (Go to automatic loop shutdown)			11-7 Loop shutdown initiated.
	12-2 Loss of Primary Coolant pressure (Both loops)	12-3 High reactor pressure SCRAM action.				12-7 System SCRAM.
			13-4 Checks steam generators and circulators to see if operable.	13-5 Attempts to reestablish flow.	13-6 Flow successful.	13-7 Normal Plant shutdown.
			14-4 If not operable-	14-5 Manual SCRAM and connect PCRV water loops to HT coolers		14-7 Manual SCRAM
			15-4 (Loss cooling > 3 hours).	15-5 Distribute flow in both loops	15-6 Check for tube leaks.	15-7(Go to 17-5)
			16-4 No leaks	16-5 Pressurize cooling loop and surge tanks.		
			17-4 (Loss cooling > 10 hours)	17-5 Depress helium to storage	17-6 Operate both reserve shutdown systems and check plant ventilation systems.	17-7 Reserve System shutdown.

SECTION IV- TABLE 5

HUMAN INTERACTION MATRIX (HIM)

LOSS OF OFFSITE POWER

Initiating Event 1	Indications 2	Operator Action (1) 3	Operator Action (2) 4	Operator Action (3) 5	Operator Action (4) 6	Physical Results 7
1-1 Loss of offsite power	1-2 Offsite power meters null and panel alarms					
2-1 Main turbine trips.	2-2 Turbine console lights	2-3 Operator checks diesel startup.	2-4 Operator checks Non-essential loads shed.	2-5 Operator checks automatic Prog. sequencers.	2-6 Operator initiates safe shutdown.	2-7 Normal Plant shutdown.
					3-6 No operator action.	3-7 Delayed Manual SCRAM.
				4-5 Sequencers fail.	4-6 Operator starts essential auxiliaries (Go to 2-6.)	
			5-4 Loads not shed.	5-5 Operator sheds non-essential loads. (GO to 2-5.)		
		6-3 No diesel startup.	6-4 Operator manually starts diesels. (go to 2-4.)			
7-1 Feedwater flow automatically reduced to 25%.	7-2 RH steam pressure drops 25%. Automatic control drops out.	7-3 Operator inserts rods to reduce RH temperature.				7-7 Power reduction.
		8-3 No operator action.				8-7 System SCRAM on low SH pressure.
9-1 Main steam bypass valves open.	9-2 console lights on.	9-3 Operator closes RH relief valves.				9-7 Nominal power reduction, some venting.
		10-3 No operator action.				10-7 System SCRAM on Low SH pressure. Major venting.
		11-3 Operator tries to restart turbine.				11-7 Continue normal power reduction.
		12-3 Turbine doesn't start.				12-7 Manual SCRAM.

SECTION IV- TABLE 5 (Continued)

HUMAN INTERACTION MATRIX (HIM)

LOSS OF OFFSITE POWER

1 Initiating Event	2 Indications	3 Operator Action (1)	4 Operator Action (2)	5 Operator Action (3)	6 Operator Action (4)	7 Physical Results
13-1 Main turbine does not trip out.	13-2 Turbine console lights.	13-3 Operator checks: diesel startup.	13-4 Operator checks: for min of one operating circulator in one loop. Yes.	13-5 Operator checks: Reactor power is reducing Yes.	13-6 (None)	13-7 Normal power reduction.
				14-5 No.	14-6 Operator inserts rods to reduce power.	14-7 Power reduction starts
		15-3 Yes.	(None) 15-4 (Go to 13-7). No.			15-7 Manual SCRAM.
		16-3 No.	16-4 Operator manually starts diesels. (Go to 13-4).			
		17-3 Operator adjusts shim rods Yes.	17-4(None-Go to 13-5).			
		18-3 No.				18-7 Power reduction stops.
		19-3 Operator resynchronizes generator to "Bus" Yes.	19-4(None-Go to 13-5).			
		20-3 No				20-7 Turbine trip and Manual SCRAM
21-1 Feedwater flow automatically reduced to 25%.	21-2 RH Steam pressure drops 25% automatic control drops outs.	21-3 Operator checks turbine speed and voltage. Good.	21-4 (None-Go to 13-5).			
		22-3 No good.	22-4 Operator reduces power with rods.	22-5 (Go to 13-5).		
			23-4 No operator action.			23-7 System SCRAM on Low SH pressure.

SECTION IV - TABLE 5 (Continued)

HUMAN INTERACTION MATRIX (HIM)

LOSS OF OFFSITE POWER

Initiating Event 1	Indications 2	Operator Action (1) 3	Operator Action (2) 4	Operator Action (3) 5	Operator Action (4) 6	Physical Results 7
		24-3 Operator checks turbine exhaust hood spray operation.Good.	24-4 (None-Go to 13-5)			
		25-3 No Good.	25-4 Start safe shutdown sequence.			*25-7 Safe shutdown started.
		26-3 Operator monitors exhaust hood temperature normal.	26-4 (None-Go to 13-5).			
		27-3 High.	27-4 Start Safe shutdown sequence.			*27-5 Safe shutdown started.
Safe Shutdown Sequence		28-3 Operator starts auxiliary boiler.				
		29-3 No Start.				29-7 Manual SCRAM.
		30-3 Operator synchronizes diesel generator.				
		31-3 No Start				31-7 Turbine trip and Manual SCRAM.
		32-3 Operator sheds non-essential loads				
		33-3 Operator manually SCRAMS reactor.				33-7 Manual SCRAM.
		34-3 Turbine manually tripped.				
		35-3 Non-essential water feeds deleted by operator.				
		36-3 Make-up flow to deaerator established.				36-7 Shutdown accomplished.

At action point (1-1) on this chart, the operator may or may not observe a higher than normal activity in the Loop Condensate Sample Monitor. If he notices the increased activity (a yes, indicated by the upper path "y"), he must make the next decision (1-2), which is to shut down the leaking loop or ignore it temporarily. If the decision is to shut down the loop, he then has an alternative (indicated by "br" for branch path) on how he initiates loop shutdown. He may elect to take the preferred path which is to push the two red circulator trip buttons associated with the faulty loop or, for various reasons he may decide to turn the Reheat Stop Check Valve (RSC) off. Either action will initiate loop shutdown. Since the RSC valve is not prominently marked in red and is nested with a whole group of similar switches, this option is probably less apt to be taken and is more prone to error if it is selected. For these reasons the branch selection ratio has been arbitrarily set at 80:20 to favor the selection of the circulator trip buttons. At action point (1-3), the operator may or may not have actuated the right pair of circulator trip buttons. If his actions were correct, a loop shutdown will be initiated culminating in the proper loop being shutdown. (Terminal point 1-4). If however, the operator has pushed the wrong two circulator trip buttons, a loop shutdown will be initiated on the wrong loop. The operator's first indication of this may be to observe that the condensate monitor activity is not decreasing as rapidly as it should and that the wrong set of loop valve lights are being actuated as the shutdown proceeds. Under these conditions point (1-5), the operator can choose to manually SCRAM the system or to wait for loop shutdown to be completed. He may then attempt to shut down the plant and bring it back up with only the good loop operational (Point 1-7). If he does not observe that the wrong

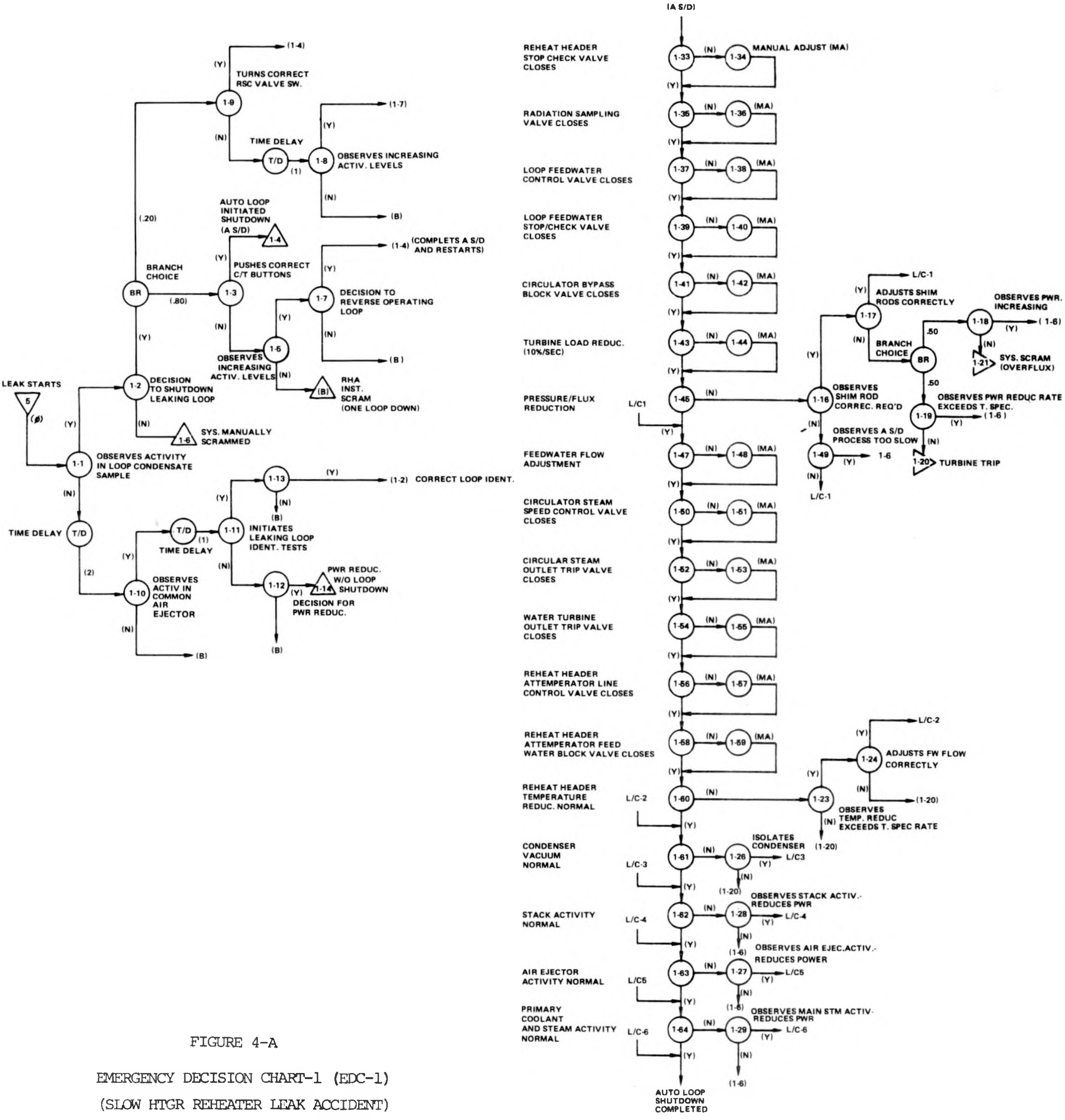

LEAK STARTS
5
(ø)
1-1
OBSERVES ACTIVITY IN LOOP CONDENSATE SAMPLE
(Y)
(N)
TIME DELAY
T/D
(2)
1-2
DECISION TO SHUTDOWN LEAKING LOOP
(N)
1-6
SYS. MANUALLY SCRAMMED
(Y)
BR
BRANCH CHOICE
(.20)
(.80)
1-9
TURNS CORRECT RSC VALVE SW.
(1-4)
TIME DELAY
T/D
(1)
1-8
OBSERVES INCREASING ACTIV. LEVELS
(1-7)
(B)
1-3
PUSHES CORRECT C/T BUTTONS
AUTO LOOP INITIATED SHUTDOWN (A S/D)
1-4
1-5
OBSERVES INCREASING ACTIV. LEVELS
1-7
DECISION TO REVERSE OPERATING LOOP
(1-4) (COMPLETS A S/D AND RESTARTS)
(B)
RHA INST. SCRAM (ONE LOOP DOWN)
1-10
OBSERVES ACTIV IN COMMON AIR EJECTOR
T/D
TIME DELAY
1-11
INITIATES LEAKING LOOP IDENT. TESTS
1-13
(1-2) CORRECT LOOP IDENT.
1-12
DECISION FOR PWR REDUC.
1-14
PWR REDUC. W/O LOOP SHUTDOWN
(A S/D)
REHEAT HEADER STOP CHECK VALVE CLOSES
1-33
1-34
MANUAL ADJUST (MA)
RADIATION SAMPLING VALVE CLOSES
1-35
1-36
(MA)
LOOP FEEDWATER CONTROL VALVE CLOSES
1-37
1-38
LOOP FEEDWATER STOP/CHECK VALVE CLOSES
1-39
1-40
CIRCULATOR BYPASS BLOCK VALVE CLOSES
1-41
1-42
TURBINE LOAD REDUC. (10%/SEC)
1-43
1-44
PRESSURE/FLUX REDUCTION
L/C1
1-45
1-16
OBSERVES SHIM ROD CORREC. REQ'D
1-17
ADJUSTS SHIM RODS CORRECTLY
L/C-1
BRANCH CHOICE
BR
.50
.50
1-18
OBSERVES PWR. INCREASING
(1-6)
1-21
SYS. SCRAM (OVERFLUX)
1-19
OBSERVES PWR REDUC RATE EXCEEDS T. SPEC.
(1-6)
1-20
TURBINE TRIP
1-49
OBSERVES A S/D PROCESS TOO SLOW
1-6
L/C-1
FEEDWATER FLOW ADJUSTMENT
1-47
1-48
CIRCULATOR STEAM SPEED CONTROL VALVE CLOSES
1-50
1-51
CIRCULAR STEAM OUTLET TRIP VALVE CLOSES
1-52
1-53
WATER TURBINE OUTLET TRIP VALVE CLOSES
1-54
1-55
REHEAT HEADER ATTEMPERATOR LINE CONTROL VALVE CLOSES
1-56
1-57
REHEAT HEADER ATTEMPERATOR FEED WATER BLOCK VALVE CLOSES
1-58
1-59
REHEAT HEADER TEMPERATURE REDUC. NORMAL
L/C-2
1-60
1-23
OBSERVES TEMP. REDUC EXCEEDS T. SPEC RATE
1-24
ADJUSTS FW FLOW CORRECTLY
L/C-2
(1-20)
CONDENSER VACUUM NORMAL
L/C-3
1-61
1-26
ISOLATES CONDENSER
L/C3
(1-20)
STACK ACTIVITY NORMAL
L/C-4
1-62
1-28
OBSERVES STACK ACTIV.- REDUCES PWR
L/C-4
(1-6)
AIR EJECTOR ACTIVITY NORMAL
L/C5
1-63
1-27
OBSERVES AIR EJEC.ACTIV.- REDUCES POWER
L/C5
PRIMARY COOLANT AND STEAM ACTIVITY NORMAL
L/C-6
1-64
1-29
OBSERVES MAIN STM ACTIV- REDUCES PWR
L/C-6
(1-6)
AUTO LOOP SHUTDOWN COMPLETED

FIGURE 4-A

EMERGENCY DECISION CHART-1 (EDC-1)
(SLOW HTGR REHEATER LEAK ACCIDENT)
]

loop is being shut down, or that the activity level in the supposedly good loop is still increasing, it has been assumed that the activity may build-up to the point where either the RHA monitors trip and SCRAM the system, or the senior operator may point out the discrepancies and a decision made to manually SCRAM the system. (The "no" paths, indicated by "n" indicates an erroneous action or lack of action or decision).

If at the initial event (1-1), the operator did not notice abnormal activity in the condensate sample, his subsequent action will follow the "no" action path (n) to action point (1-10). After some time has passed, indicated by the time delay block (T/D), the operator may observe that the air ejector is showing abnormal activity levels. Since this monitor is common to both loops, it indicates that the activity resulting from reheater leak has gradually infiltrated through both operating loops and the condensate monitors may not at this time be too useful in positively indicating which loop is the source of the original trouble. The operator must then initiate a series of leaking loop identification tests by decreasing power, purging the loops, and then drawing samples off from both loops to monitor the relative activity levels. (Point 1-11). If these tests are successful, the correct loop has been identified and the operator can then proceed to shutdown the bad loop (action point 1-2).

If he cannot positively identify which loop is bad, he may take the lower branch (action point 1-12) which leads to a normal power reduction (NPR) without loop shutdown (terminal point 1-14) and if things do not change he would be expected to shut down the plant.

Once a loop shutdown is initiated by the operator, the plant is placed into an automatic shutdown sequence. This sequence is is monitored by the operator who acts only to override certain items in the shutdown sequence if they fail to occur, or to make some slight adjustment if it is required, such as adjusting shim rods to keep the automatic control rod at its most effective position in the reactor core, or slowing down temperature and power reduction rates to protect the plant from thermal shock. These actions are indicated in action points 1-33 through 1-64 on the right hand side of EDC-1. The decision points and manual actions (MA) are self-explanatory. Each time a manual adjustment is made, the Loop Shutdown is allowed to continue in normal fashion. The probability that a manual adjustment may be required for each of the valve actions in the shutdown sequence was arbitrarily set a one time in a thousand shutdowns.

A comparison of the critical events in each of the three accident scenarios reveals that the most important element of safety is the exposure to the general public of small amounts of radioactive effluent. Almost all of this release occurs when the HTGR is subjected to emergency shutdown or SCRAM from full power. Under these conditions, the steam by-pass valves can only handle about 80% of the system steam load. This means that about 15-20% of the steam load may be vented to the atmosphere. Venting at the air ejector is filtered, but not the output of steam relief valves. If a reheater tube leaks or ruptures due to earthquake or structural fatigue, it is possible for small amounts of radioactivity to be mixed with the primary steam. Under these conditions, present plant emergency procedures are cognizant of the need to avoid emergency shutdown or system SCRAM and an attempt is made to shut down the plant or leaking loop in a safe and orderly fashion.

Examination of EDC-1 indicates that the probability of an unanticipated SCRAM is directly dependent on the efficiency of the operator in detecting the incident at its inception, and in his subsequent response to the incident. Because of this dependency, the safety problem under study is not dependent on how reliable the HTGR SCRAM system is in performing its function. Rather, the questions are, how reliable is the normal plant or loop shutdown system and what are the probabilities of having contaminated steam and initiating an inadvertent or premature SCRAM before the contaminated steam is reduced to a safe pressure which can be handled without additional venting.

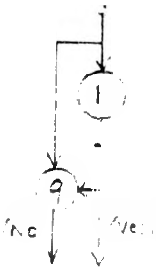
An earthquake greater than the design basis value may become serious from a public safety standpoint only if the seismic shock is great enough to rupture the PCRV wall and crack some of the reheater leak transfer tubes. Loss of off-site power may be critical only if it occurs at the time of such an earthquake or during a reheater tube leak accident. For these reasons, it seemed expedient to choose the reheater leak accident scenario as a reference case and vary the dependent operator error parametrically to simulate the effect of this parameter during other accident scenarios where attempts are made to achieve safe shutdown.

The EDC provides a convenient base from which two important determinations can be made:

1. Processing of the input decision data with a given set of probabilities will provide a rough estimate of how likely each of the possible end event may be, i.e., the probability of the operator attempting loop shutdown, the probability of a power reduction without loop shutdown, the probability that the operator may choose the wrong loop to shut down, the probability of an instrument SCRAM due to error or delayed operator decisions, and the probability that the operator may have to manually adjust or perform various shutdown functions, such as primary and secondary system valve closures, turbine load shedding, shim rod adjustments, etc.

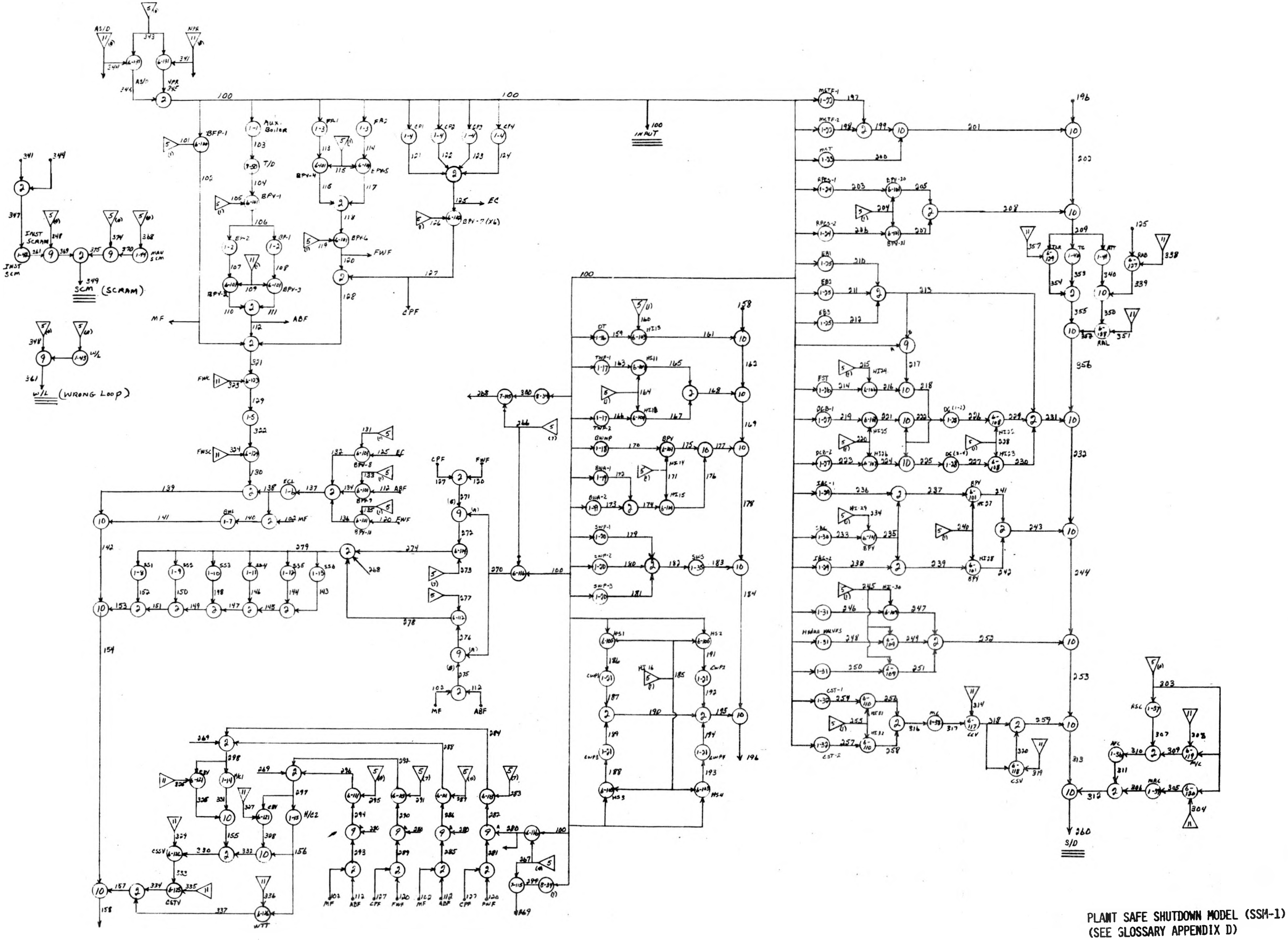
2. By combining the possible events described above with a top level model of the redundancy available in those plant elements required for safe shutdown, a preliminary estimate can be obtained of the probability of achieving a safe shutdown.

This combining of events is most efficiently accomplished by converting the EDC to a Human Decision 'GO' model. The EDC was constructed during this analysis so that a one-to-one conversion algorithm would suffice to transform the EDC to a GO model. In the resulting GO model, each decision point in the EDC is modeled by a type 1 element with the success probability representing a yes decision and failure representing a 'no'. A type 9 element in parallel acts as a gate to provide a disjoint output for the 'no' decision. If a perfect input is provided to the type 1 at time T, and the success probability of the type 1 is P, the output probability from the type 1 will be P at T and 1 - P at time 7 (never). Conversely, the output probabilities from the type 9 will be 1 - P at T and P at time 7. This algorithm is used at each nodal point in the decision tree depicted on the EDC, e.g., if the operator has an 80% probability of choosing a given course, the above algorithm will yield a value of .80 for the yes path and .20 for the no path. The resulting Human Decision Model (HDM-1) is depicted in Figure 4B. The output of the HDM-1 was subsequently used as input to the Plant Safe Shutdown Model (SSM-1) which is depicted in Figure 5. The SSM-1 is discussed further in Sections F and G.

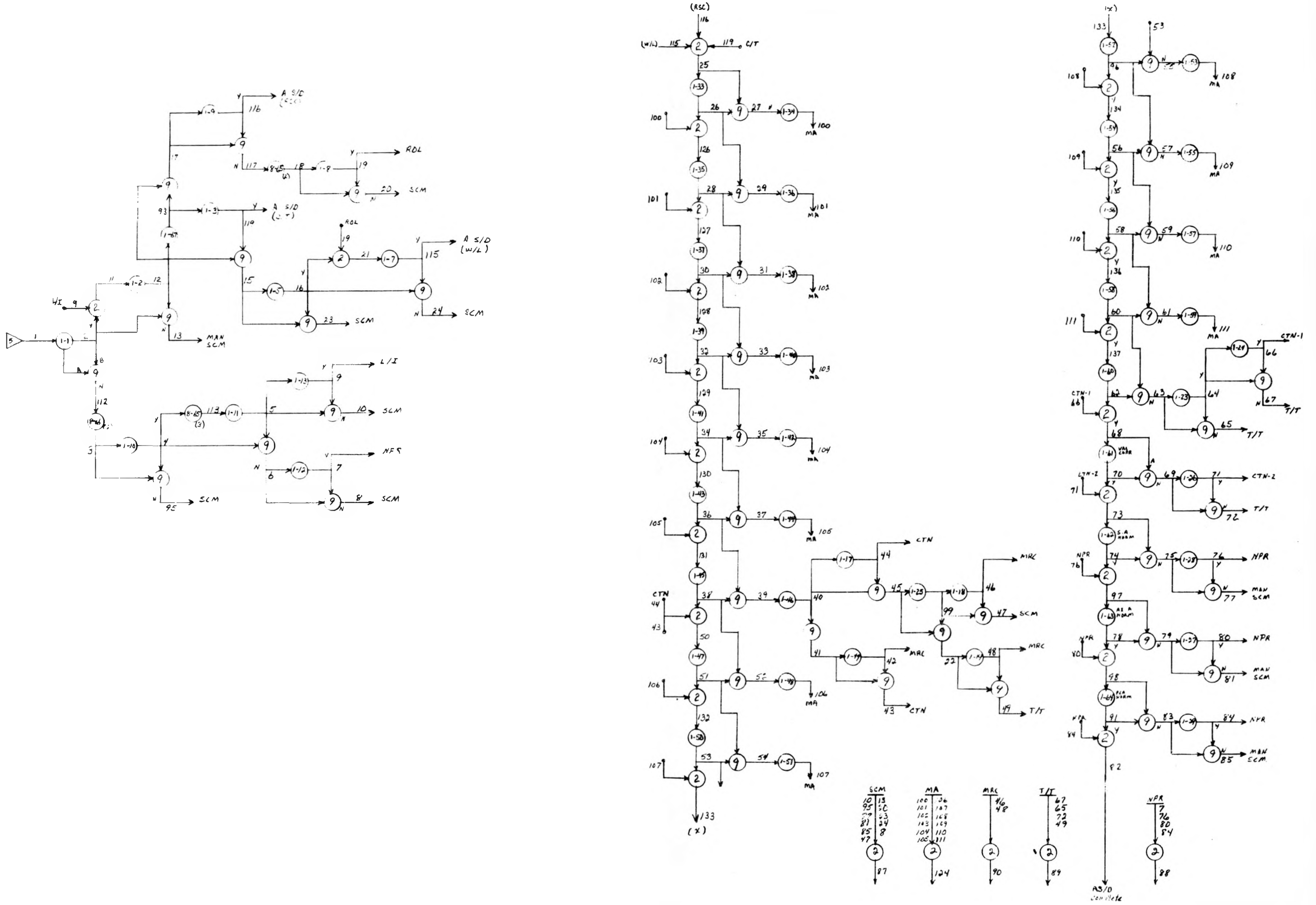


E. Human Reliability Analysis

Once the Emergency Decision Charts have been defined, it becomes necessary to assign expected error values to each action initiated by the human operator. WASH-1400 (Reference 3) gives a possible range of nominal values for various human activities in a typical Nuclear Power Plant. The values quoted in the WASH-1400 report and the various weighting factors considered in their derivation are given for reference purposes in Appendix C.



PLANT SAFE SHUTDOWN MODEL (SSM-1)
(SEE GLOSSARY APPENDIX D)



HUMAN DECISION MODEL -1(HDM-1)
(SLOW REHEATER LEAK ACCIDENT)

F. Modified Human Error Rates for HTGR Incidents

Due to the relatively slow response of an HTGR to serious incidents including loss of forced cooling, the end point error values suggested in the WASH-1400 report have been modified to reflect the faster rate of recovery which might be expected of HTGR operators following a high stress situation. Since accidents in LWR reactors tend to progress at a much faster rate, the operator stress factors reach a peak value much quicker than for HTGR operators and require a much longer time for recovery.

It was assumed for this analysis that a maximum initial human error rate of 0.50 should be assigned for the response of nuclear power plant operators during the first few minutes of a recognized reheater leak incident, followed by a fairly fast recovery during the later time intervals. The normal human error rate for nuclear power plant operators under low stress situations was assumed to vary from .01 to .001, depending on the particular diligence and alertness of the operator in question. It was further assumed in serious HTGR incidents, that the response of most normal operators would have progressed from high stress to low stress values in a time interval of 14 hours or about two shifts.

The actual value for human error under stress is the subject of considerable discussion and disagreement. To accomodate this range of opinions, the results here are presented as a function of a human error rate (HER) correction factor (CF) which ranges downward from 1.0. The actual HER is the product of the initial value (0.5) and the HER-CF. An improvement in HER can occur if human action is delayed after an incident. Thus the HER-CF can also be used as an improvement factor due to delayed initiation of operator action.

The range of possible time variations assumed for this correction factor is given in Table 7 and Figure 6. These time delays may be used to select an appropriate HER-CF for the initial error rate and subsequent times of action after a given incident.

The Plant Shutdown model has numerous valves in the system which are used to connect or disconnect alternate back-up system elements for safe shutdown. Prior to the arrival of a major incident, it is assumed that all of these valves have been preset to a desired configuration. The probability that each of these valves has been correctly set has been treated parametrically, i.e., it was assumed that each valve in the shutdown model has the following probabilities of being correctly set - .999, .99, and 0.90. After the incident has been recognized and while the operator is attempting to shut down a given loop or the entire plant, it was assumed that some of the valves in question might have to be manually adjusted due to an incorrect presetting or due to a system operational failure. The probability values for these minor valve adjustments in the associated computer runs are given in Appendix B.

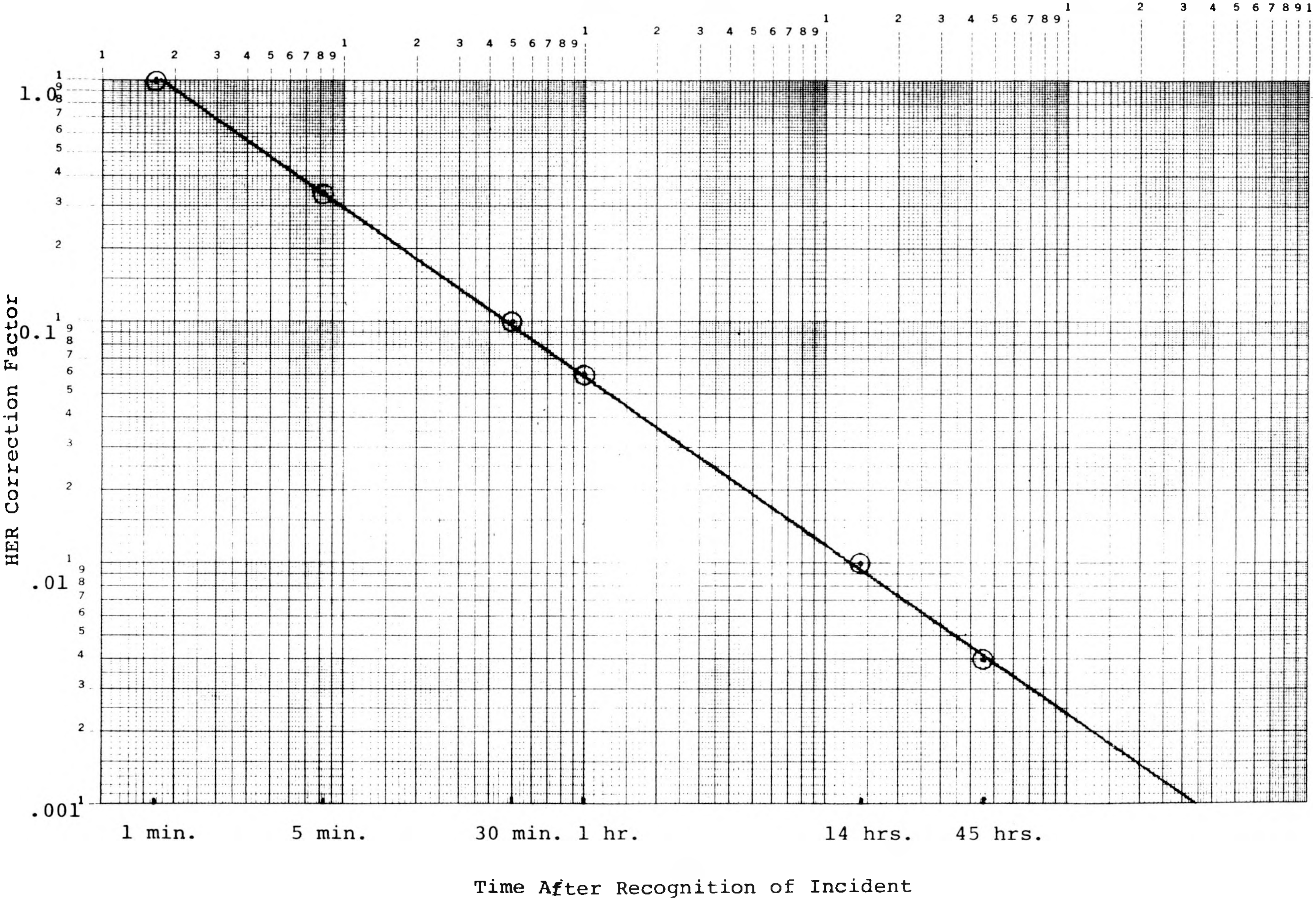
SECTION IV- TABLE 7

HTGR HUMAN ERROR RATE CORRECTION FACTOR AS A FUNCTION OF TIME

Time After Recognition of a Major Incident	Human Error Rate Correction Factor
1 minute	1.00
5 minutes	.34
30 minutes	.10
1 hour	.06
14 hours	.01
45 hours	.004

Appendix B lists the estimated error rates that were used in this study. These values were used in both the Human Decision Model and the Safe Shutdown Model to obtain system response as a function of time after the incident.

SECTION IV. FIGURE 6. HUMAN ERROR RATE CORRECTION FACTOR VERSUS TIME AFTER RECOGNITION OF A SLOW REHEATER LEAK ACCIDENT



G. Safe Shutdown Model - Sensitivity

The FSAR (Reference 7) gives a list of the minimum number of HTGR plant hardware systems and components which must be properly working to achieve a safe plant or loop shutdown. These system elements were used to make up a top level Safe Shutdown Model which reflects the redundancy depicted in the FSAR listing and not the order of flow. This list with minor modifications has been reproduced in Table 8 for convenience. Schematic drawings depicting the actual flow interconnections and functional redundancy were abstracted from the FSAR and are included in Appendix A. Since this part of the analysis is primarily directed toward an evaluation of the impact of human interfaces, it was assumed that the bulk of the plant hardware was perfect in its operation. The only exception to this was for plant valves, control rods, turbine controls, etc., that might require occasional manual adjustments. The probability of these system elements failing and requiring manual adjustment are given in Appendix B.

SECTION IV - TABLE 8

MINIMUM LIST OF SYSTEMS AND COMPONENTS REQUIRED FOR SAFE OPERATION OF PLANT

1. SCRAM system (including control rod drives), and/or the reserve shutdown system.

2. The economizer-evaporator superheater in one out of six steam generators plus, one out of two helium circulators in a given loop.

3. Helium circulator auxiliary system, including:
   water turbine drive supply,
   emergency condensate line leading to water turbines and steam generators,
   return lines to turbine water drain tank and associated water removal pumps.

4. Helium circulator bearing water system, including:
   bearing water make-up pump,
   pressurized bearing water accumulator system, and/or the service water piping to bearing water heat exchangers (coolers).

5. One of three service water pumps and pump pit, plus service water piping to PCRV liner cooling system.

6. Inlet and outlet secondary coolant system piping from the PCRV up to and including the first isolation valves.

7. One of three auxiliary Boiler Feed pumps, and/or one of four condensate pumps, plus all discharge connections to the emergency condensate line, and/or one of two firewater pumps, plus connections to emergency condensate line, for helium circulator steam or water turbine drive operations.

8. Condensate storage tanks and suction lines to small condensate pumps and auxiliary boiler feedpumps, if condensate pumps or boiler feed pumps are used.

TABLE 8 (Continued)

9. Firewater system, including one electric and/or gasoline operated driving engine for pumps, pump pit, storage tank, and associated piping.

10. One of four circulating water pumps in the water makeup system and connections to service water pump pit, and/or connections to fire pump pit if firewater system is used.

11. One loop of reactor plant cooling water system, including the PCRV closed loop cooling system and the fuel storage cooling water system.

12. Three essential electrical buses and applicable control systems, and/or two of four standby electric generators with associated diesel fuel storage tanks, plus one of two D.C. station batteries.

13. Plant cooling tower (two cells) plus one of two tower cooling fans.

14. Instrument or service air system for pneumatic valve operation, plus hydraulic valve operating system, including all interconnections with the control room.

Those components having human interfaces in the safe shutdown model were evaluated in a typical GO computer run to determine those interfaces which would have the most impact on system performance. The ratio of change in the total system probability of failure to a small change in a given component's probability of failure is defined in this study as the system sensitivity to failure for the given component. An analogous system sensitivity can be defined for a change in a component's probability of prematuring or acting spuriously.

Table 9 lists the system sensitivity values for each significant interface in the safe shutdown model.

It is noticeable that of the 29 valves requiring possible adjustment, only nine appear to have a significant effect on the shutdown function.

H. System Impact, General

At the beginning of an incident which requires loop shutdown the operator has several options depending on whether he recognizes that an accident is in progress or not, i.e., he may decide to perform a loop shutdown, reduce power, SCRAM, or do nothing. If he decides to perform a loop shutdown, he must recognize which loop is bad and identify the correct set of Circulator Trip buttons or the correct Reheat Stop Check valve to operate and thus signal the plant to initiate an automatic loop shutdown. The Human Decision Model (HDM-1) was employed to determine the probabilities that a given operator would obtain each of these possible results, dependent either on his initial error or, if the Correction Factor of Figure 6 is used, on the time after recognition of the accident when he responds. Several sets of estimated probabilities were generated for the sequence of human decisions or actions depicted in the HDM. These are tabulated in Appendix B. Each probability set is based on the general stress-time conditions given in Figure 6 and represents probability of operator error as a function of time after the initial recognition of the accident. The first set of probabilities represents operator response during the first minute after recognition of an accident, with an assumed probability of initial operator error set at 0.50.

SECTION IV-TABLE 9

SENSITIVITY OF HUMAN INTERFACES ON SAFE SHUTDOWN MODEL

Item	*Component ID Number	Component Description	Relative Sensitivity
1	100	Boiler feed pump (motor drive) Bp valve or BPF turbine S/O valve (#105) or FWF S/O Valve (#119) or E/C S/O Valve (#126)	1.0
2	101	Bearing water accum. & make up pump S/O valves	2.0
3	102		Neg
4	103	Turbine water drain tank S/O Valve	1.0
5	104		Neg
6	105		Neg
7	106		Neg
8	107		Neg
9	108		Neg
10	109		Neg
11	110		Neg
12	111		Neg
13	112		Neg
14	113		Neg
15	114		Neg
16	115		Neg
17	116	Reheat stop check valve switch (#115)	1.0
18	117	Condensate control valve	1.0
19	118		Neg
20	119		Neg
21	120		Neg
22	121		Neg
23	122	Circulator steam speed valve	1.0

*Component numbers represent 'type' numbers for 'kind' 6 components shown on Plant Safe Shutdown GO Model, Figure 4b, (Page 59), i.e., Component ID# 100 = Element 6-100.

SECTION IV -TABLE 9 (Continued)

Item	Component ID Number	Component Description	Relative Sensitivity
24	123		Neg
25	124		Neg
26	125	Circulator Steam trip valve or (water turbine trip valve #126)	1.0
27	126		Neg
28	127	Reheat Attemp. F/W Block Valve	1.0
29	128	Reheat Attemp. Line Valve	1.0

Since the entire spectrum of actions required by the operator to successfully accomplish a loop or plant shutdown requires his actions be distributed over an extended time interval, it should be expected that the operator error rate will drop off with time. This is reflected in Appendix B as one scans the sequence of actions in each vertical column. It should be noted, however, that the order in which the actions are listed is not always in time sequence. The time sequencing can be better followed by correlating the function numbers in Appendix B with the same decision numbers shown on either the Emergency Decision Chart EDC-1 (Figure 4A), or the GO Model (HDM-1) (Figure 4B). Since the operator may not immediately react after recognizing a possible accident, e.g., he may call in his supervisor to verify the anomalous situation and decide on a unified plan of action, different initial error probabilities have been assigned to cover the range of possible human errors in a parametric fashion. Each new initial error gives rise to a new set of operator action probabilities. Five different sets of such human action probabilities are depicted in Appendix B. Each of these five decision sets were run in the GO Model (HDM-1) to derive conditional probabilities of the operator doing the following:

Actuating the correct circulator trip buttons to initiate loop shutdown;
Selecting the correct Reheat Stop Check valves to initiate loop shutdown;
Deliberately or inadvertently initiating a power reduction instead of loop shutdown;
Precipitating or inadvertently causing an unanticipated SCRAM.

The Human Errors listed in Appendix B were used as inputs to the Safe Shutdown Model (SSM-1). The results of the runs on both the HDM and the SSM have been plotted versus the human error rate correction factor at the start of the time sequence. These error values have been normalized to an initial operator error of 0.50 to allow more convenient interpolation in terms of system response when shutdown is initiated for either a given time after recognition of the accident, or for any assumed initial error the user wishes to apply.

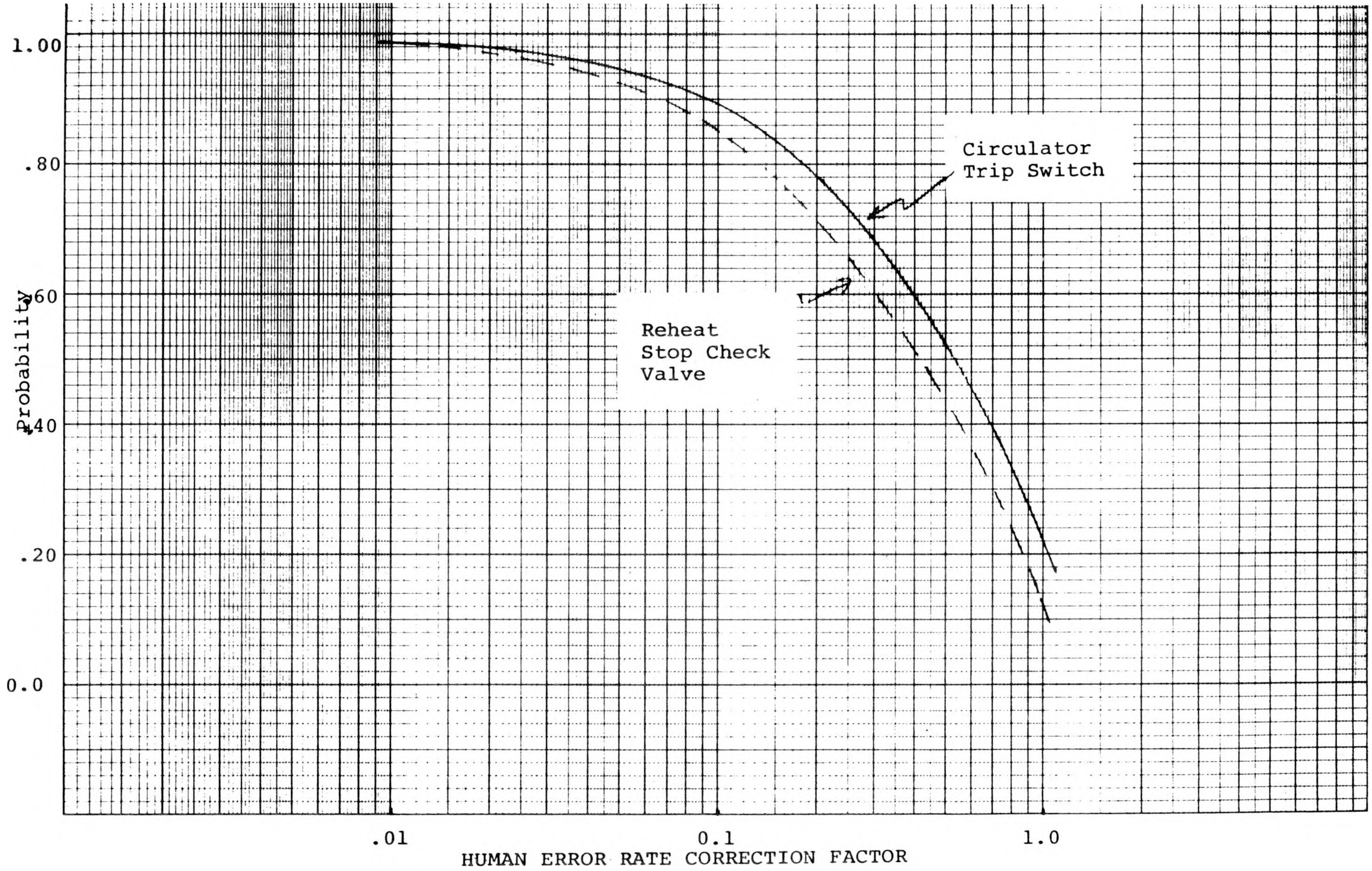
The first set of these results is listed in Table 10. It will be noted from Table 10 that if the operator has an initial error rate as high as 0.50, he has approximately a 0.21 probability of selecting the right set of circulator trip switches or about 0.12 probability of selecting the right reheater stop check valve. If, on the other hand, the operator's response is ten times better, i.e., error of about 0.05, he has a probability of 0.89 of getting to the right set of circulator trip switches and a probability of 0.85 of getting the right reheater stop check valve. The probabilities for selecting the right loop shutdown controls are also depicted in Figure 7.

SECTION IV. TABLE 10

HUMAN DECISION MODEL (HDM-1)
REHEATER LEAK ACCIDENT

	Probability Of	Probability of Several END Events			Probability of Selecting Proper Controls		
Time After Accident Recognition	Initial Operator Error	Safe Shutdown	Normal Power Reduction	Instrument SCRAM	Circulator Trip	Reheat Stop Check	Wrong Loop
1 min.	.50	.2343	.3600	.4057	.212	.122	.0404
2.9 min.							.0484
3.9 min.							.0507
5 min.	.17	.6774	.1529	.1697	.653	.566	.0417
30 min.	.05	.8985	.0441	.0574	.893	.849	.0141
1 hour	.03	.9385	.0291	.0324	.935	.910	.0084
14 hours	.005	.9873	.0060	.0067	.986	.985	.0012

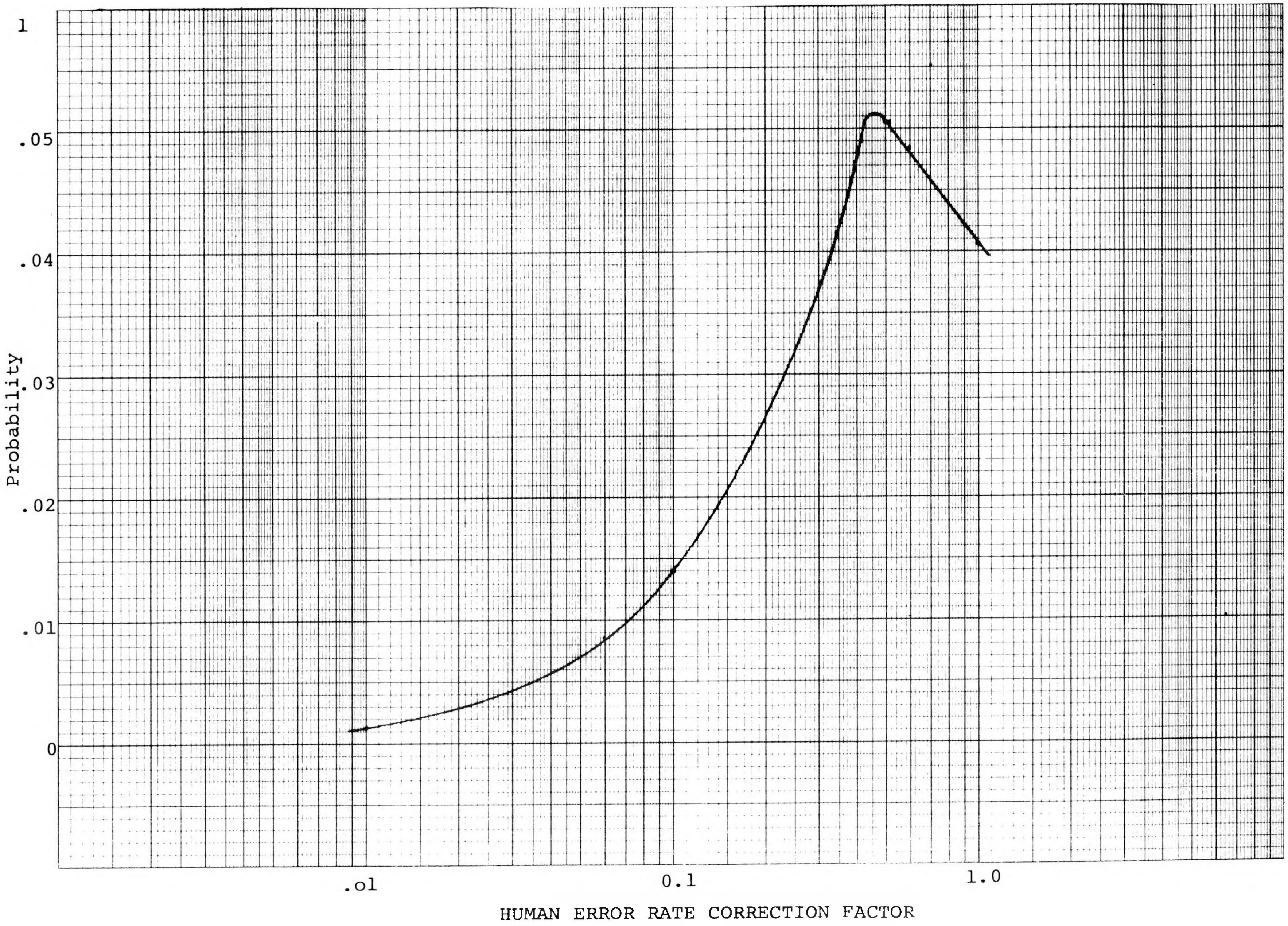
SECTION IV. FIGURE 7. PROBABILITY OF OPERATOR SELECTING PROPER LOOP SHUTDOWN CONTROL VERSUS OPERATOR ERROR CORRECTION FACTOR



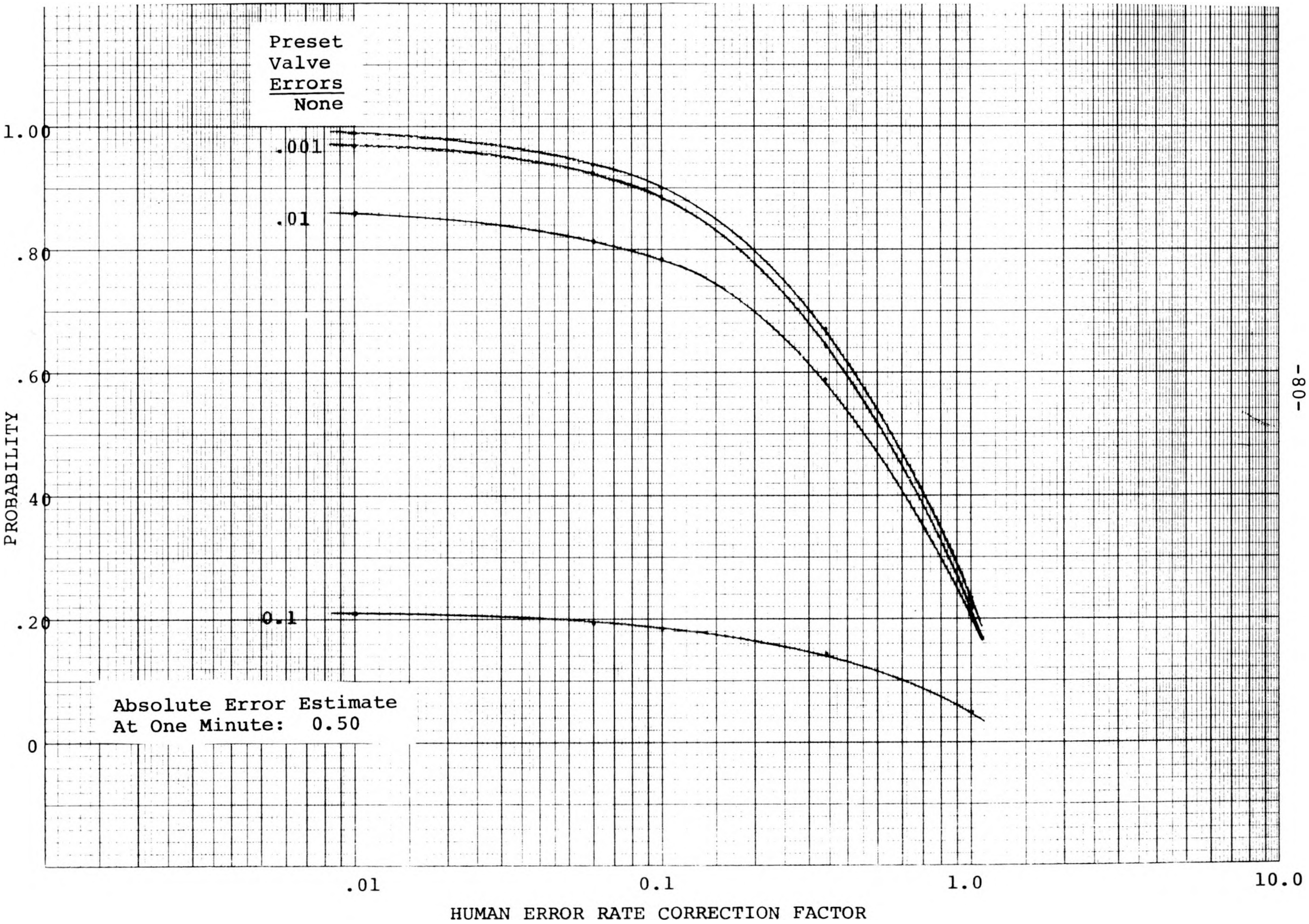
If the operator selects the wrong loop the automatic shutdown process must continue until the loop is down, thereupon, the operator must shut the plant down and start up with the good loop. If he has managed to shut the plant down without an instrument SCRAM or premature SCRAM occurring, the operator then has a fairly good chance of bringing the plant back up on the good operating loop. The probability of the operator selecting the wrong loop is plotted in Figure 8. The falling off of this curve in the region of HER Correction Factor values from 0.5 to 1.0 indicates that as the operator becomes more disoriented, the probability of achieving any shutdown process (wrong loop or right loop) also becomes lower.

The probability that the operator will successfully achieve a loop or plant shutdown without a failure in the equipment required for safe shutdown is strongly dependent on the accuracy with which all the preset valves have been set when the last start up to power was made and the normal failure rate of the equipment. Figure 9 shows this reliance parametrically for preset valve errors of 0.0, .001, .01, and 0.1, e.g., if there exists a 10% probability that some of the valves required for shutdown are not set properly, the probability of achieving a successful shutdown without failure drops from a possible 0.99 to 0.21. However, the consequences of such a shutdown failure are not serious unless the delay exists over a fairly long time period. If the component causing the failure can be quickly located and repaired, or redundant system elements can be brought into operation, the shutdown process can be continued. However, if the plant cannot be shut down in a reasonable time, the reheater leakage which initiated the accident may result in a system SCRAM which the shutdown operation had tried to avoid.

SECTION IV. FIGURE 8. PROBABILITY OF OPERATOR SELECTING WRONG LOOP FOR SHUTDOWN VERSUS OPERATOR ERROR CORRECTION FACTOR



SECTION IV. FIGURE 9. PROBABILITY OF LOOP OR PLANT SHUTDOWN WITHOUT FAILURE VERSUS OPERATOR ERROR CORRECTION FACTOR AND PRESET VALVE ERRORS



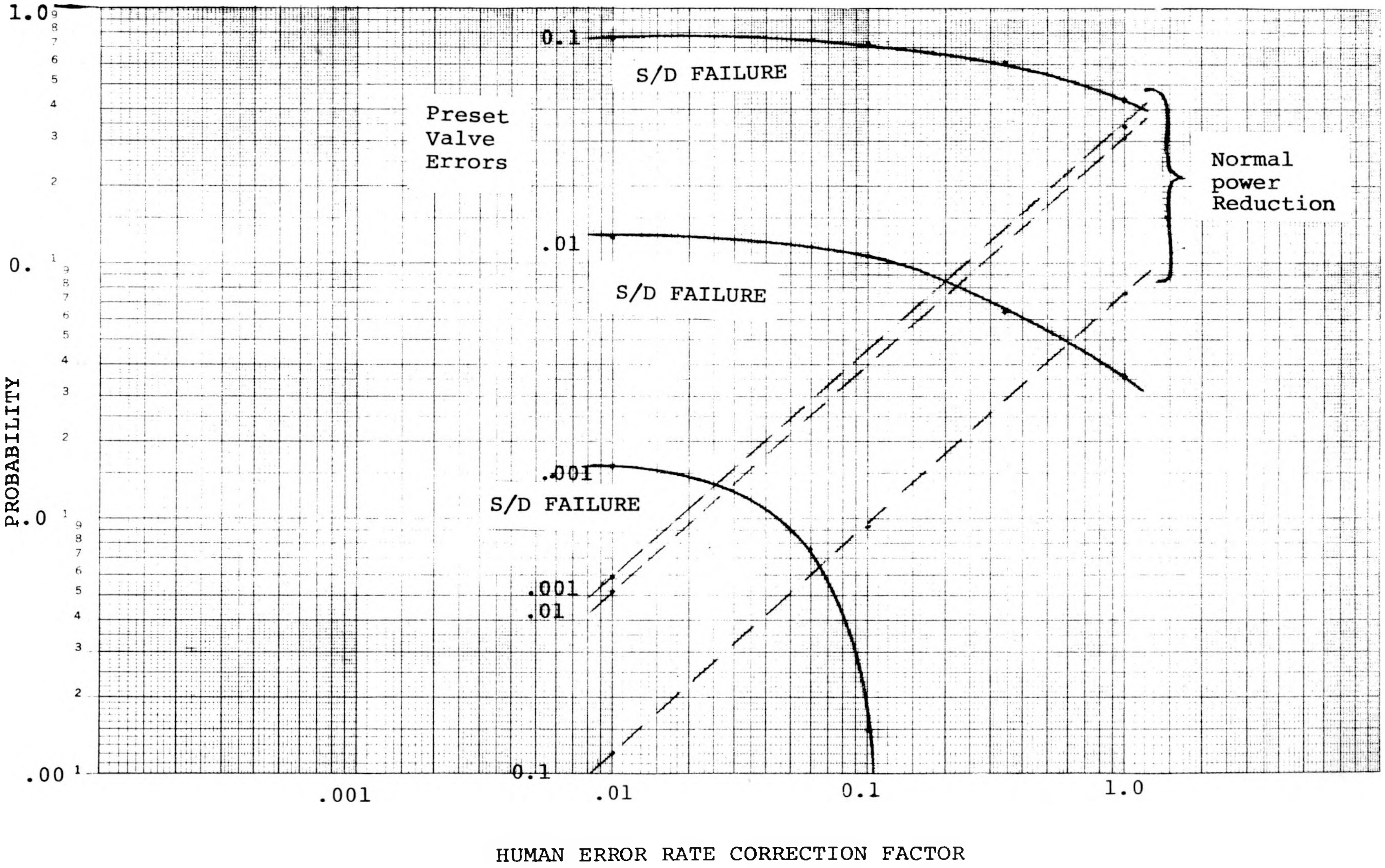
The probability of encountering such a shutdown failure is depicted in Figure 10. It will be noticed that the probability of a shutdown failure appears to drop off with increasing operator error. This merely reflects the same situation discussed earlier; that the more disoriented the operator is, the less apt he is to correctly initiate a loop shutdown, and hence there is less chance for a shutdown failure. Figure 10 also shows the probability of the operator getting a normal power reduction without loop shutdown plotted against the error correction factor. A normal power reduction or plant shutdown will generally act to reduce the amount of radioactive leakage coming into the affected primary loop, and hence appear to heal the incident. However, any subsequent attempts to start up with both loops on would quickly reveal the real situation.

The data plotted in Figures 9 and 10 is tabulated in Table 11. The probability of the operator getting an unanticipated SCRAM is also contained in this table. If the initial operator error of 0.5 is assumed, the probability of getting an unanticipated SCRAM is extremely high (about 0.40) immediately at the start of the incident and falls off rapidly with delayin initial operator response so that thirty minutes later the probability of an unanticipated SCRAM has dropped to about 0.06. Figure 11 depicts the same data.

It can be seen from this curve that if it is desirable to get the probability of an unanticipated SCRAM down to the order of 0.01, then the operator error at the start of the accident must also be in the order of 0.01 (initial error of 0.5 times 0.02 Correction Factor). This low error rate may be achieved in several ways, i.e.:

(1) Depending on the urgency of the situation, the operators response could be delayed until recovery from the high stress situation is nearly normal (about 14 hours).

SECTION IV. FIGURE 10. PROBABILITY OF FAILURE DURING SHUTDOWN AND POWER REDUCTION WITHOUT LOOP SHUTDOWN VERSUS OPERATOR ERROR CORRECTION FACTOR AND PRESET VALVE ERRORS

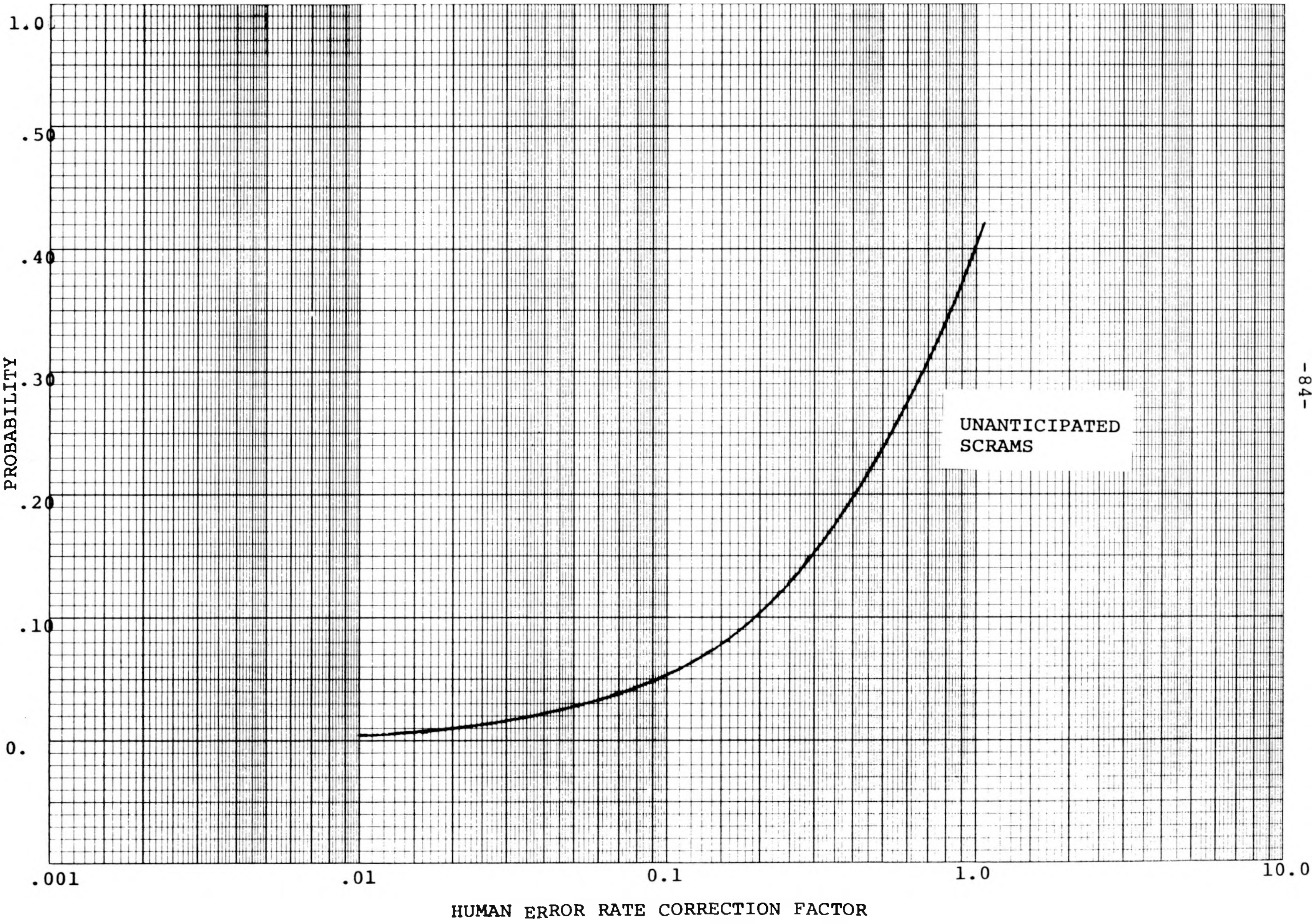


SECTION IV. TABLE 11

SAFE SHUTDOWN MODEL RESPONSE TO REHEATER LEAK ACCIDENT

Absolute Operator Error	Time After Recognition of Accident	Safe Shutdown				Normalized Power Reduction				SCRAM	Wrong Loop Shutdown	Fail Shutdown			
		Preset Valve Errors				Preset Valve Errors						Preset Valve Errors			
		.1	.01	.001	Perfect	.1	.01	.001	Perfect	(All)	(All)	.1	.01	.001	Perfect
.50	1 min	.0493	.2040	.2184	.2343	.0760	.3135	.3355	.3600	.4057	.0404	.4286	.0364	0.0	0.0
.17	5 min	.1424	.5899	.6418	.6774	.0319	.1332	.1468	.1529	.1697	.0417	.6143	.0655	0.0	0.0
.05	30 min	.1895	.7826	.8836	.8985	.0093	.0384	.0434	.0441	.0574	.0141	.7297	.1075	.0015	0.0
.03	1 hr	.1975	.8175	.9229	.9385	.0061	.0253	.0286	.0291	.0324	.0084	.7556	.1164	.0077	0.0
.005	14 hr	.2073	.8600	.9709	.9873	.0012	.0052	.0059	.0060	.0067	.0012	.7836	.1269	.0153	0.0

SECTION IV. FIGURE 11. PROBABILITY OF UNANTICIPATED SCRAMS VERSUS OPERATOR CORRECTION FACTOR



(2) If possible, the operator could wait about 30 minutes after recognition of the incident and review action to be taken with the senior operator, who will observe and monitor that proper controls are being actuated. (If loose coupling is assumed, we may assume that the joint error might approach a value of .03 to .05).

(3) Train operators to automatically respond properly for a variety of possible incidents. There are several possible techniques that make this kind of training feasible. One of the most positive methods is one identified as Automated Normative Exercising.

In this technique, a computer is used to analyze the operator's response to a given situation and present a printout or visual screen display of the impact of his action on the accident progression and the subsequent plant response. The methodology can be automated in whole or in part depending on the financial desires of the user. It can be tied into existing plant equipment or made completely independent.

(4) An HTGR Simulator could be used to condition the operators to make proper responses during high stress situations and in addition could be used for new operator training, operator requalification, and for checking out desired changes in procedures for emergency situations.

I. System Impact, Wrong Control Selection

The control room of the Fort St. Vrain Nuclear Power Plant is filled with control panels containing several hundred control switches, buttons, programmers, recorders, panel warning lights, etc. Figures I-1, 2, 3, show only about 1/10 of the total set of St. Vrain control room panels. The field of view encompassed by these figures overlap each other by about 30%. These three figures were selected for illustration in this report because they include the majority of the controls for initiating and monitoring a normal loop or Plant Shutdown. Figure I-1 shows the initiating loop shutdown controls for loop 1. In the upper left two pairs of push button controls are mounted on the vertical panel. The first pair of buttons represent the Circulator Trip buttons for water turbine drive on Circulator A and Circulator B respectively. The second set represents the same function for steam turbine drive on these two circulators. The Circulator Trip buttons are the only large red buttons on the vertical panel and are almost impossible to miss. However, it is quite possible that the water turbine drive buttons might be selected by error instead of the steam drive buttons, or alternatively, the wrong loop might be selected for shutdown.

Under the very improbable circumstances, that the circulator trips do not operate as planned, i.e.; no loop shutdown is initiated, the operator has the option of initiating a loop shutdown by using the Hot Reheat Stop Check valve, or the steam turbine trips. The operating manual specifies that normal plant shutdown will be initiated using the circulator trip or the steam turbine trip.

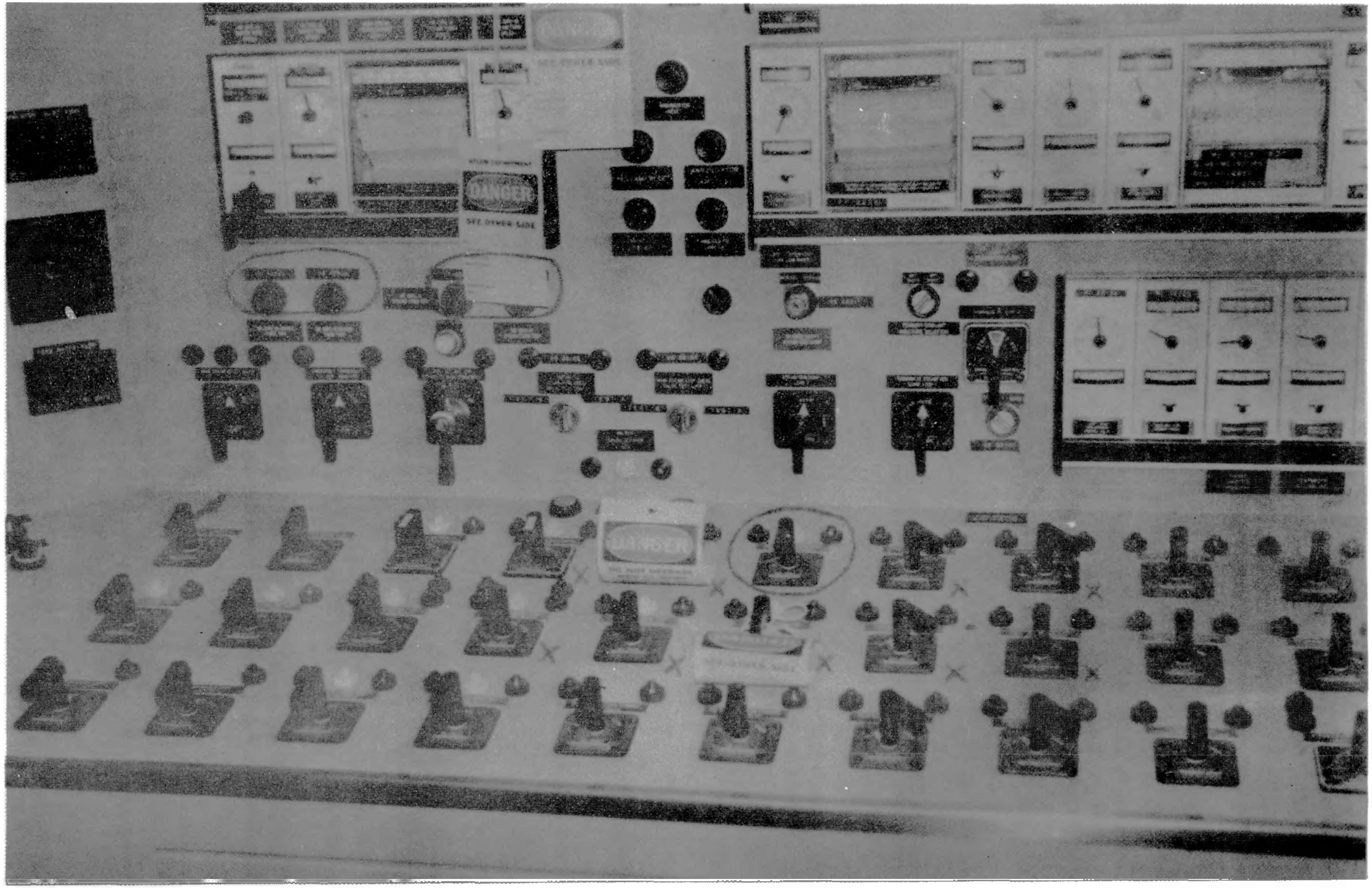


FIGURE I-1
FORT ST. VRAIN CONTROL PANELS (Loop 1)

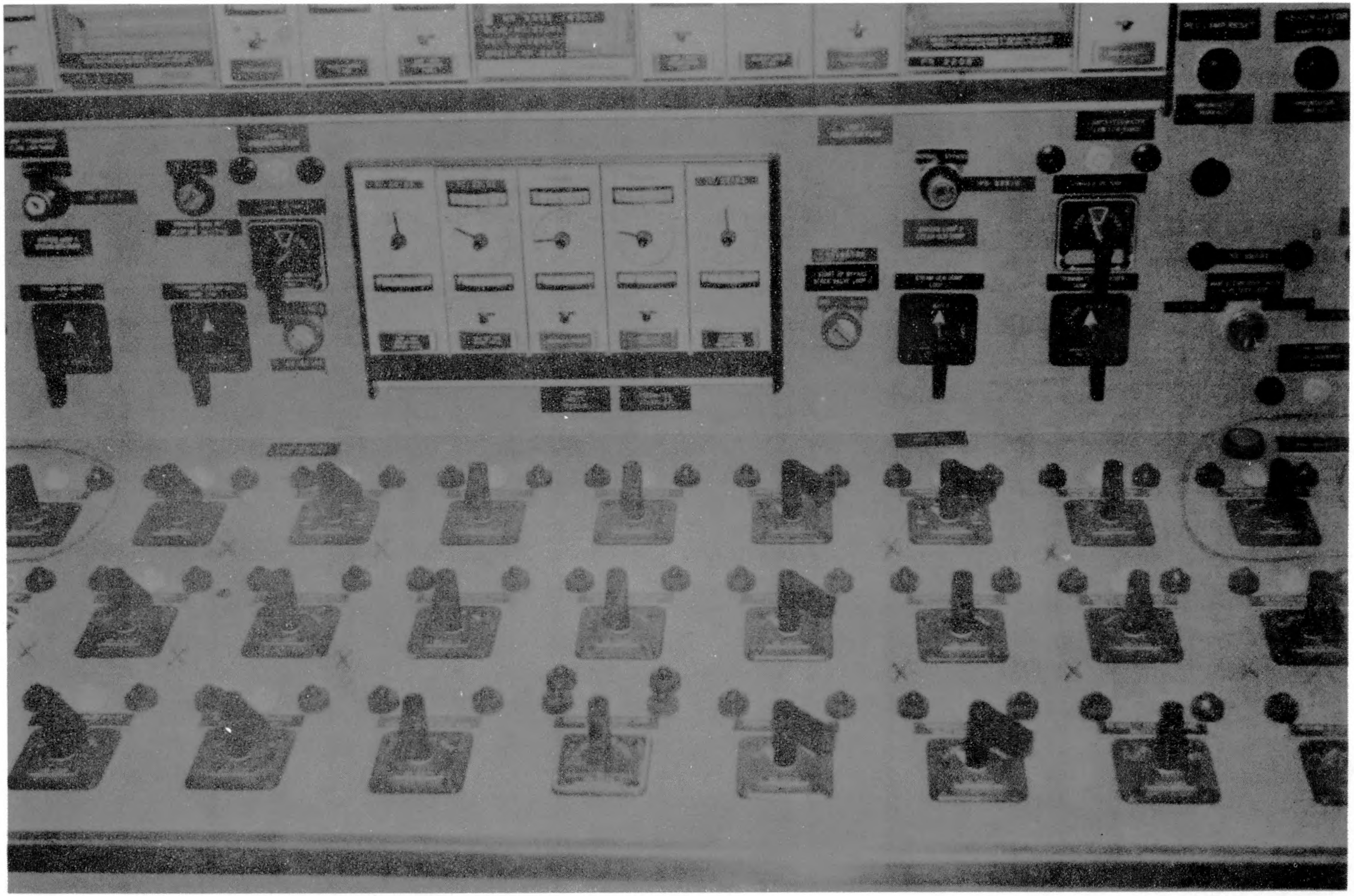


FIGURE I-2
FORT ST. VRAIN CONTROL PANELS (Loop 1 & Loop 2)

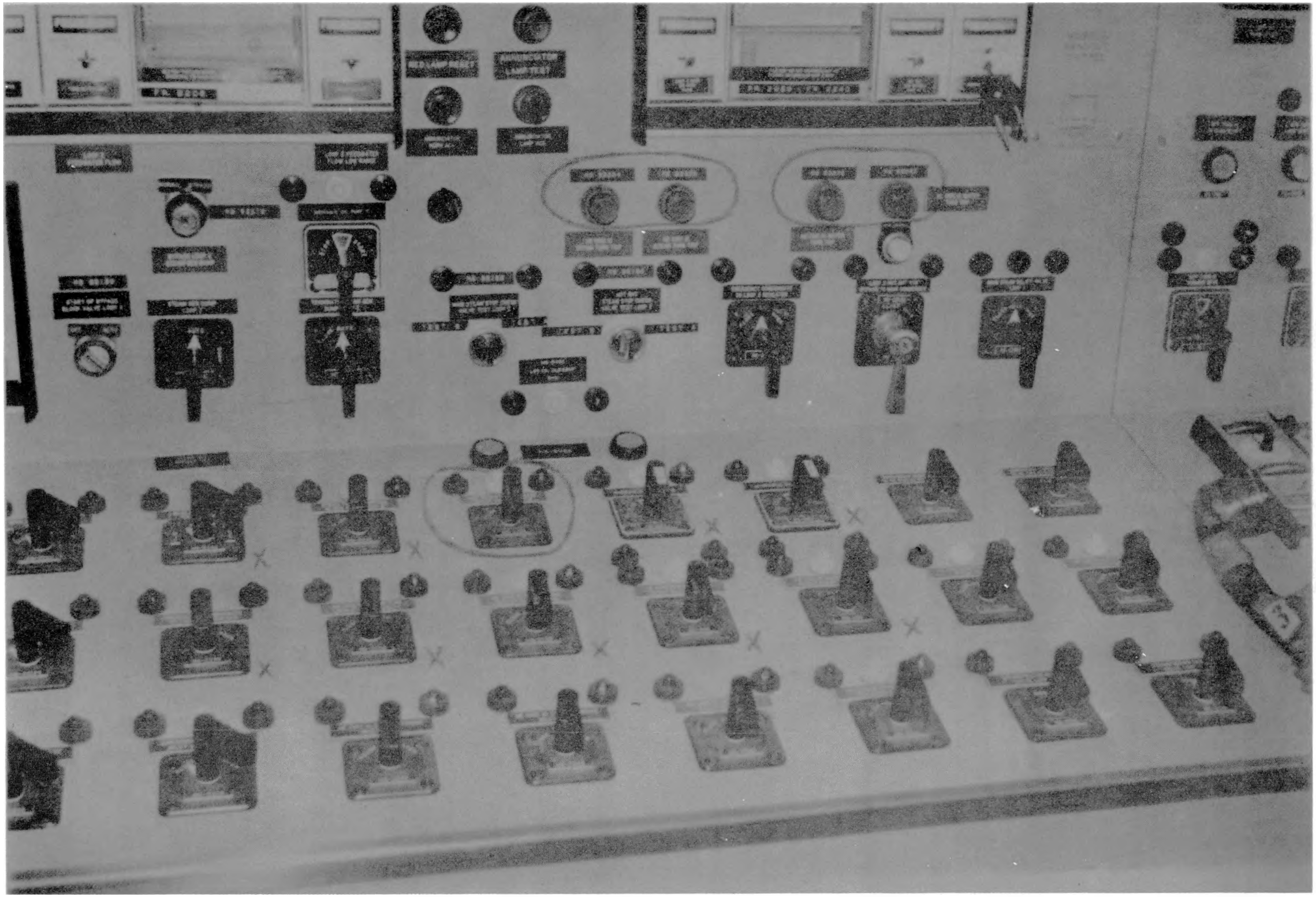


FIGURE I-3
FORT ST. VRAIN CONTROL PANELS (Loop 2)

The front horizontal panel shows a circled hand switch (6th switch from left back row) representing the control switch for the Hot Reheat Stop Check valve in Loop 1. Nine switches surrounding the Hot Reheat Stop Check valve are marked with an "X". These are the switches which were considered in this analysis to have the highest probability of being selected in error if the operator tried to effect an immediate loop shutdown by searching for the *Hot Reheat Stop Check valve. The Hot Reheat Stop Check valve switch has a red name plate but so do about 15 other surrounding switches. The control handle is black as are all the surrounding switch control handles.

Figure I-3 shows an almost identical arrangement for Loop 2 except that the Hot Reheat Stop Check valve control switch is located 5 switches from the right side instead of being the 6th switch.

Figure I-2 shows the same Reheat Stop Check switches for both loop 1 and loop 2 but does not quite catch the Circulator Trip buttons which are located on both sides just outside the field of view covered by this picture.

Figure I-4 has been included to help identify the various hand switches of interest.

Circulator Trip Selection

If the wrong trip mode is selected when attempting to shut down the circulators, i.e., water drive vs steam drive, no shutdown action will occur until the proper mode is reselected. In addition, the PPS system will indicate by alarms and lights which specific circuit has been tripped.

* Initiation of loop shutdown by means of the Hot Reheat Stop Check valve is classed as an abnormal shutdown procedure. However, this is an alternative shutdown mode recognized by the plant operators as a possible emergency mode if the circulator trip or steam turbine trip actions appear to have no effect.

FIGURE I-4

SWITCH IDENTIFICATION CHART

Loop 1

Switch Location

Back Row	(1)	(2)	(X)	(3)	(4)
Mid Row	(5)	(6)	(7)	(8)	(9)

(X) Represents Hot Reheat Stop Check Valve Switch

1. Hydraulic Oil Pump 1B (HS-9103-1)
2. Steam Turbine Bypass Block Valve (HS2241
3. Main Steam Block Valve (HS-2223)
4. Main Steam Bypass Valve (HS-2293)
5. Helium Circulator 1B Water Turbine In/Out Block Valve (HS-2115)
6. Helium Circulator 1A Steam Turbine Outlet Block Valve (HS-2249)
7. Helium Circulator 1B Steam Turbine Outlet Block Valve (HS-2251)
8. Feedwater to Attemperator (HS-22133)
9. Emergency Condensate to Steam Generator (HS-2237)

Loop 2

Switch Location

(4)	(3)	(X)	(2)	(1)	Back Row
(9)	(8)	(7)	(6)	(5)	Mid Row

1. Hydraulic Oil Pump 1D (HS-9104-1)
2. Hydraulic Oil Pump 1C (HS-9102-1)
3. Steam Turbine Bypass Block Valve (HS-2242)
4. Main Steam Block Valve (HS-2224)
5. Helium Circulator 1D Water Turbine In/Out Block Valve (HS-2118)
6. Helium Circulator 1C Water Turbine In/Out Block Valve (HS-2110)
7. Helium Circulator 1D Steam Turbine Outlet Block Valve (HS-2252)
8. Helium Circulator 1C Steam Turbine Outlet Block Valve (HS-2250)
9. Emergency Condensate to Steam Generator (HS-2238)

If the wrong loop is selected, shutdown will be indicated but the operator will soon notice that the wrong loop is shutting down. Since a loop shutdown is accomplished in about 5 seconds, the operator may immediately restart the loop that was shut down, and proceed to shut down the correct loop.

Reheat Stop Check Valve Selection

If the operator chooses to effect an emergency loop shutdown with the Reheat Stop Check valve, there is a finite probability, depending on the degree of stress present in the operator, that he may select the wrong switch to initiate shutdown. The most probable switches which might be selected in error are listed below in Table 12.

SECTION IV-TABLE 12

HAND SWITCHES SURROUNDING HOT REHEAT STOP CHECK VALVE - LOOP 1

VALVE FUNCTION	Loop 2	Loop 1
Hydraulic Oil Pump (1B, 1C, 1D), (Hyd)	HS-9104-1, 9102-1	HS-9103-1
Steam Turbine Bypass Block Valve, (Hyd)	HS-2242	HS-2241
Main Steam Block Valve, (Hyd)	HS-2224	HS-2223
Main Steam Bypass Valve, (Hyd)	HS-2292	HS-2293
Circ (1B, 1C, 1D) Water Turbine In/Out Block Valve, (Hyd)	HS-2118, 2110	HS-2115
Circ (1A, 1C) Steam Turbine Outlet Block Valve,(Hyd)	HS-2252	HS-2249
Circ (1B, 1D) Steam Turbine Outlet Block Valve, (Hyd)	HS-2250	HS-2251
Feedwater to Attemperator	HS-22134	HS-22133
Emergency Condensate to Steam Generator	HS-2238	HS-2237

The following sections describe the most probable system impact resulting from operation by mistake of each one of the above valve controls.

RESULTS

(1) Hydraulic Oil Pump (HS9102-1, 9103-1, 9104-1)

Turning off any one of the three hydraulic pump switches will shut down either a standby hydraulic pump or the main hydraulic pump. If the main hydraulic pump is shut off, the standby pump in loop 1 will come on automatically. If the hydraulic pressure in loop 1 or loop 2 drops to a critical value when on the standby pump, a Low Pressure Alarm will annunciate and inform the operator that the Emergency Hydraulic pump should be switched on.

In all cases, the hydraulic accumulators in each of the loop hydraulic systems will supply sufficient oil under pressure to accomplish an orderly loop or plant shutdown.

(2) Steam Turbine Bypass Block Valve

This block valve is normally open. If it is accidently shut off, the turbine speed control loop will react very quickly to maintain circulator speed and Helium flow constant. The loops would operate for a period of time in an unbalanced condition and the loop with the reduced reheat flow would initiate a high-reheat-steam trip SCRAM when the reheat temperature reached or exceeded 1075°F. Based on reaction to reheat temperature alarms, the operator would likely reopen the steam turbine bypass block valve and retry for loop shutdown.

(3) Main Steam Block Valve (HS-2223,2224)(Hydraulic)

This block valve is normally open. If it is accidentally shut off the main steam pressure will rapidly rise in that loop. The loop is protected by the Main Steam bypass valves which will detect the pressure rise and pass desuperheated steam to the flash tank. If these valves should fail there are 4 safety relief valves upstream of the block valve which will blow to atmosphere when the line pressure reaches 2670 PSIG, 2720 PSIG, and 2790 PSIG respectively. This will relieve the pressure in that loop.

(4) Main Steam Bypass Valve (HS-2293, 2292) (Hydraulic)

Normally this valve is closed and cannot be opened until main steam temperature falls below 800°F due to interlocks. However, if the interlock should fail and this valve is accidentally opened the main steam in the affected loop will be dumped into the flash tank. At the same time, the main turbine-generator will trip out due to sudden loss of pressure and/or the reheat line will initiate a low pressure SCRAM on sensing the sudden pressure drop.

(5) Circulator 1B Water Turbine In/Out Block Valves (HS-2115, 2116) (Pneumatic)

Normally these valves are closed and the circulators are driven by cold reheat steam. If the hand switch for one of these valves is accidently opened there would be no noticeable effect as the speed control valves would maintain the water turbine drive in a deenergized state. If the circulators are being driven by the water turbine when this switch is operated and the valve is accidentally closed, the circulator controlled by that valve will trip out upon sensing low speed.

(6) Circulator 1A or 1B Steam Turbine Outlet Block Valves (HS-2249, 2252, 2251, 2250) (Hydraulic)

These valves are normally open to pass steam to the reheater section of the steam generators. If one of these valves is accidently closed, the affected circulator will slow down and a low speed trip will be initiated taking it off line. The circulator bypass valve will maintain normal pressure and no shutdown action will be initiated. Given these conditions, the operator may decide to manually SCRAM.

(7) Feed Water to Cold Reheat Desuperheaters (HS-22133, 22134) (Pneumatic)

Normally these valves are open to allow control of reheat steam temperature prior to going to the reheater section of the steam generators. If the switch to one of these valves is closed, while over 50% power, the temperature of the reheat steam in all six steam generator modules in the affected loop will start to increase. This will cause the reheat temperature controller to compensate by reducing overall power. The probability of a manual SCRAM is fairly high.

(8) Emergency Condensate to Steam Generator (HS-2237, 2238) (Hydraulic)

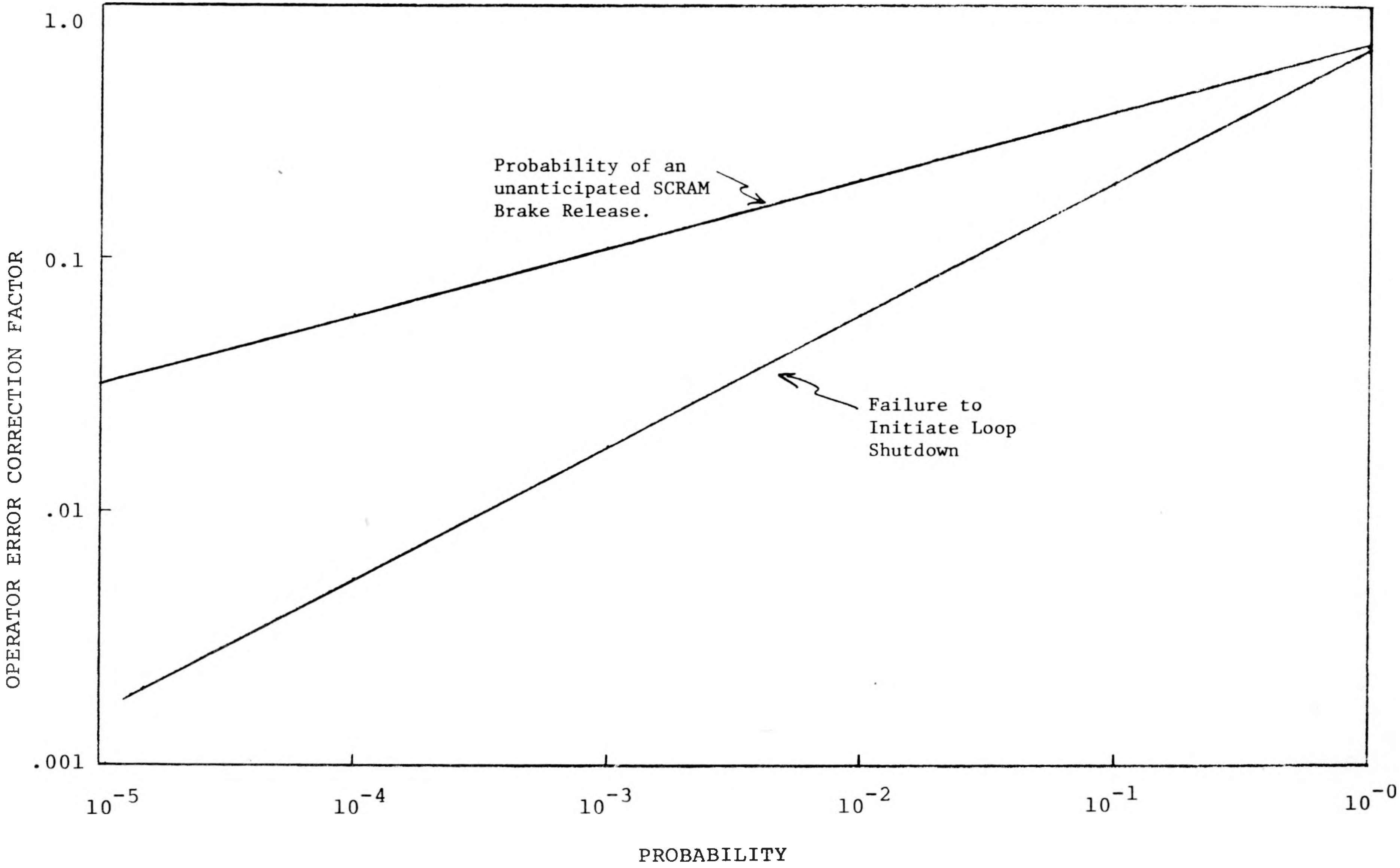
This valve is normally closed and interlocked when the plant is using normal feedwater supply. If this valve were accidently opened, the interlock would insure that there would be no effect on the system. If the plant were operating on emergency condensate and the valve was accidently shut off, flow alarms would annunciate, informing the operator to switch to alternate feedwater supplies. The pressure in the main steam generators would rapidly drop as well as circulator speed. These events trigger multiple system SCRAMS unless the feedwater source is immediately supplemented.

J. PLANT PROTECTIVE SYSTEM RESPONSE

The SCRAM Protective System Model constructed during the previous study (Reference 1) was modified slightly to allow the incorporation of Loop Shutdown circuits which are initiated by the Reheat Header Activity Monitors (RHA). The model was then run assuming that for each operator error correction factor there is a corresponding probability for the Plant Protection System to attempt to either shut down one of the two operating loops if they are both operating or to cause an unanticipated system SCRAM if one loop is already down. The results are shown in Figure 12.

If both loops are operating, it is apparent from Figure 12 that the probability of initiating a loop shutdown is strongly correlated with the degree of operator error. However, the loop that is shut down may not be the right loop. In a similar manner, the probability of getting an unanticipated SCRAM is closely correlated to operator error values. Figures 12 also indicates that an operator error correction factor of .03 (absolute error probability of .015) will result in negligible probability of an unanticipated SCRAM.

FIGURE 12. SCRAM PROTECTIVE SYSTEM RESPONSE TO OPERATOR ERROR CORRECTION FACTOR



K. Manual SCRAM Response

The most obvious point of human interface with the PPS system is Manual SCRAM. This interaction is an important element in the functional diversity of the plant protection system. In the previous study the probability of SCRAM equipment failure for various accident sequences was calculated at 10^{-5} or less, before credit for operator intervention. For accidents other than a Reheater Leak accident, an automatic SCRAM backed up by Manual SCRAM is the usual shutdown mode.

WASH-1400 gives estimates of the probability of correct action for the first half hour after a major accident as 0.9 to 0.1. However, this estimate refers to a wide variety of actions requiring some thought and analysis. Manual SCRAM is a simple, direct action which is a major element in operator education and training. Also, operators are usually trained to back up an automatic SCRAM with an immediate manual SCRAM, which helps to condition their responses toward the SCRAM action. Furthermore, a second operator or supervisor would be present at the console very quickly after an accident to make his own evaluation of the situation. Thus, the probability of initiating a manual SCRAM should be at least 0.99 after the first minute or two. For an HTGR this is fast enough due to the high thermal capacity of the core and relatively slow reactivity effects characteristic of a graphite reactor. Thus, the probability of SCRAM failure for the accidents considered becomes 10^{-7} or less, including operator intervention. The Reserve Shutdown System is not included because it is primarily an alternate or backup system. The reliability gain from the RSS would be in the event of failure of more than one control rod to insert during an otherwise successful SCRAM. If multiple rod failures (probably common mode) occur with a probability of 10^{-5} or less, and the operator unreliability to actuate the RSS is 10^{-2} or less, the RSS contribution to SCRAM failure is 10^{-7} or less (assuming the RSS failure probability is less than 10^{-2} which is certainly reasonable.)

L. Conclusions and Recommendations

1. Conclusions

(A) The three accident scenarios evaluated in this task become a safety problem only if the secondary coolant becomes radioactive, a normal loop or plant shutdown cannot be initiated and/or post shutdown cooling becomes impossible. When Reheater leaks exist, premature SCRAMS or an operator initiated SCRAM may result in the release of small amounts of radioactive steam to the atmosphere through steam relief valves, air ejectors and deaerator vents. However, the consequent mixing and dilution with the upper atmosphere at Fort St. Vrain prior to public exposure reduces even this small hazard to almost negligible proportions.

(B) The probability of an operator safely initiating loop shutdown or plant shutdown at the inception of an accident is directly dependent on the stability, training and reliability of the operator during the accident situation. If we assume an initial high stress error rate of .10 for the human operator (correction factor of .2), the probability of his initiating a safe loop/plant shutdown action will vary from about 0.71 to 0.78 depending on the mode of shutdown (Figure 7). At this level of error, his probability of selecting the wrong loop for shutdown is about .027 (Figure 8). If all critical plant valves were preset with a nominal error of (0.01) prior to the accident, the probability that the operator will encounter a failure during the shutdown process is of the order of about 0.083 (Figure 10). If such a failure occurs, this event is postulated to disorient the operator even more so that the subsequent probability of his detecting and rectifying the plant anomaly for a second try at plant shutdown is estimated to drop an amount proportional to double his previous error rate, i.e., the operator error correction factor will probably change from 0.2 to 0.4 (See Appendix Table C-1, Item 15). The probability of the operator achieving a successful loop shutdown at this point has now dropped to 0.54 (Figure 9). Simultaneous with this probability, the expectation that the operator will experience an unanticipated SCRAM which he is trying to avoid is about 0.20 (Figure 11). To maintain the probability of an unanticipated SCRAM below 0.01, it is evident that the human error rate during the initial course of an incident should be less than 0.01 (Figure 11). It is unrealistic to expect that operator errors during the beginning stages of an incident, such as those evaluated in this study, can approach a value like 0.01 without using administrative procedures to inhibit immediate undesired responses and working closely with a second operator, or by developing trained operator reflex actions for such emergency situations.

2. Recommendations

(A) The existing operator certification and requalification programs provide a basis for safe operation of the Fort St. Vrain Nuclear Power Plant. However, under high operator stress conditions, some errors can occur which may result in the release of small amounts of radioactive effluent to the atmosphere. While the amount that can be released in this manner is acceptable insofar as public risk is concerned it is desirable to reduce the possibility of these occurrences to a minimum. To achieve this, it would appear that operator response to accident stimuli should be a trained reflex type response. This response is only partly developed by accident talk-throughs and/or walk-throughs.

The implementation of normative exercising training techniques would be a feasible and efficient way to fill this void in the conditioning of nuclear power plant operator responses to emergency situations. It is recommended that the use of these techniques and possible variations of these be evaluated for application to the operating staff at Fort St. Vrain.

Another possible solution to the problem of training operators to respond correctly, might be the development of a full scale, interactive simulator. The simulator can be used not only for emergency response training, but to train new operators, qualify current operators for license renewal and to study the impact of changes in procedures when handling specified accidents.

It is recognized that such simulators are expensive ($3-5 million) and a cost-effect analysis would be needed before implementing this suggestion.

(B) It is recommended that the procedure for presetting plant valves and the valve line up inspection procedures be reviewed internally by plant management to maintain the probability of safe shutdown failures to as low a value as practicable. This might include such items as an easily visible and readable identification tag for each critical valve, consistent color codes for valves normally closed, versus valves normally open, prestartup checkoff of valve positions on a single list, and periodic operating checks of valve positions.

(C) It is recommended that a more detailed study of the reliability of the plant shutdown system be initiated to verify the assumptions used in this study. This is particularly important with regard to the reliability of hand operated and automatic valves used in the shutdown system.

V. TASK 2. CURRENT PRACTICE IN SURVEILLANCE AND TEST PROCEDURES

Maintenance, test and calibration procedures can have an affect on SCRAM system reliability through the possibility of human error in performing these procedures. The written procedures were examined to determine the degree and nature of human interfaces and potential system impact.

A. Selection Criteria

Specific criteria were established to guide selection of the appropriate procedures to be examined, since the total number of procedures is large and many give evidence of having little impact on system performance. There are 12 SCRAM parameters in the main SCRAM System, 7 in loop shutdown and 10 in circulator trip. Most of the sensors have 3 procedures; daily shift checks or readouts of a selected parameter response, monthly channel testing and annual calibrations. If multiplicity of sensors is counted, the shift checks alone (on the Weekly PPS Log) include 191 entries.

The earlier study (Reference 1) had identified redundancy, functional diversity and shift checks of redundant readouts as important contributors to overall reliability. Thus, the absence of these factors was considered to be one of the criteria for selecting the interfaces to be examined.

The selection criteria chosen were:

1. Any human interface beyond the two-out-of three SCRAM gate relay matrix (no benefit from redundancy).

2. Inspection/test frequency monthly (no benefit from shift checks).

3. No visual readout (not checked each shift).
4. Identified in earlier study as important.
5. Surveillance procedures for all main SCRAM channels.

The test and calibration procedures and test frequencies are listed in Tables 5.4.1, 5.4.2 and 5.4.3, of the Fort St. Vrain Technical Specification (Reference 3). These tables do not correspond exactly to the individual parameter channels (nor do they need to) due to necessary overlapping of tests and rearrangement for test convenience. For example, the SCRAM tests include Primary Coolant Pressure and Core Inlet Temperature as separate tests while the SCRAM Parameters are Reactor Pressure High or Low (programmed by Core Inlet Temperature). Since the current study emphasizes procedures, the selected list is itemized to correspond with the procedure list rather than the channel parameter list used in the previous report. After identification of human interfaces, the operator effects were then entered into the appropriate channel in the existing GO model for quantitative analysis.

From the selection criteria and procedure list, a number of procedures and subsystems were chosen for analysis. These were:

1. Top Level
    a. Control Rods and Drives,
    b. Rod Control System,
    c. SCRAM Brake Control System.
2. Main SCRAM Parameter Tests
    a. High Ambient Temperature,
    b. 480V Surge Undervoltage,
    c. Core Inlet Temperature,

   d. Primary Coolant Pressure,
   e. Reheat Steam Temperature,
   f. Main Steam Pressure,
   g. Hot Reheat Header Pressure,
   h. Two Loop Trouble Inputs (including moisture),
   i. Linear Power Channels,
   j. Wide Range Channels,
   k. Startup Channels.

3. Loop Shutdown Parameter Tests
   a. Steam Pipe Rupture (Pipe Cavity),
   b. Steam Pipe Rupture (under PCRV)
   c. Circulator Trip Inputs,
   d. Moisture Monitors,
   e. Steam Generator Penetration Pressure,
   f. Two Loop Trouble Output Logic (included in 2-h).

4. Circulator Trip Parameter Tests
   a. Circulator Penetration Pressure,
   b. Circulator Trip Output Logic (included in 3-c).

B. Procedure Review

Test and calibration surveillance procedures for the items listed above were obtained and analyzed where available. Non-routine repair operations are usually not known in advance so few procedures are available for these activities.

Each procedure was examined to determine whether the previous points of human interface with the system needed expansion or revision, and if any changes could be expected in the potential system performance. Some of the expanded interfaces included Test/Operate switches not previously included, valves, cables, basic test equipment (temporarily applied), and type and nature of sensor manipulation (direct or indirect).

Test frequencies and short descriptions of the tests are given in Table 5* for the SCRAM system. Loop Shutdown System and Circulator Trip System. Those channels with readouts in the control room are recorded and checked against redundant channels daily. (Current practice is to record during every shift on the Weekly PPS Log, although the Technical Specification requirement is daily only.) Channel tests are performed monthly. In cases where the sensor is accessible, the sensor is exercised during the test (e.g., heat or pressure applied to temperature or pressure switches) and trip is verified in the control room. For others, test signals are introduced into the electronics to trip the channel. Pulse tests are used for dependent signals which feed more than one channel wherever a d.c. test signal would cause a SCRAM or loop shutdown. One channel is pulsed at a low enough duty cycle to avoid energizing the output relay while the second channel is tripped. A pulse transformer in series with the output relay coil provides a signal to indicate that the pulse reached the relay. Then the relays are individually checked in various combinations.

The SCRAM contactors are checked one channel at a time with annunciation from one set of contacts. This test checks everything except the contacts in the dual 2-out-of-3 matrix which interrupt rod brake power. These contacts could be checked by meters across the dual matrix which read non-zero only when one channel is tripped.

Items beyond the 2/3 matrix include the manual SCRAM switch, fuses, in/out relays, rod brakes and the control rods.

*From Fort St. Vrain FSAR, Tables 5.4.1, 5.4.2 and 5.4.3

SECTION V-TABLE 5

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS, AND TESTING OF SCRAM SYSTEM

Channel Description	Function	Frequency (1)	Method
1. Manual (Control Room)	a. Test	R	a. Manually trip system
2. Manual (I-49)	a. Test	M	a. Manually trip each channel
3. Start-Up Channel	a. Check	D	a. Comparison of two separate channel indicators
	b. Test	P	b. Internal test signal to verify trips, and alarms
	c. Calibrate	R	c. Internal test signal to verify indication and set trip point
4. Linear Power Channel	a. Check	D	a. Comparison of 6 separate channel indicators
	b. Test	M	b. Internal test signal to verify trips, and alarms
	c. Calibrate	D	c. Channel adjusted to agree with heat balance calculation
5. Wide Range Power Channel	a. Check	D	a. Comparison of three separate indicators
	b. Test	P	b. Internal Test signals to verify trips and alarms
	c. Calibrate	M	c. Channel adjusted to agree with heat balance calculation
	d. Calibrate	P	d. Internal Test signals to adjust trips and indications
6. Primary Coolant Moisture (all channels)	a. Check	D	a. Comparison of two separate high level channel mirror temperature indications
	b. Check	D	b. Comparison of six separate low level channel mirror temperature indications

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS, AND TESTING OF SCRAM SYSTEM (continued)

Channel Description	Function	Frequency (1)	Method
6. Continued	c. Calibrate	R	c. Inject moisture laden gas into sample lines
7. Primary Coolant Moisture (High Level Channels)	a. Test	M	a. Trip one high level, one low level channel, pulse another low level channel.
8. Reheat Steam Temperature	a. Check	D	a. Comparison of the averaged thermocouple channel input indications
	b. Test	M	b. Trip channel, verify alarms and indications. Internal test signal to verify trips and alarms.
	c. Calibrate	R	c. Compare each thermocouple output with calibrated RTD. Internal test signal to adjust trips and indicators.
9. Primary Coolant Pressure	a. Check	D	a. Comparison of six separate channel indicators.
	b. Test	M	b. Trip channel, internal test signal to verify trips and alarms.
	c. Calibrate	R	c. Known pressure applied to sensor. Internal test signal to adjust trips and indicators.
10. Circulator Inlet Temperature	a. Check	D	a. Comparison of eight separate indicators.
	b. Test	M	b. Trip channel, internal test signal to verify trips and alarms.
	c. Calibrate	R	c. Compare thermocouple with calibrated RTD. Internal test signal to adjust trips and indicators.

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS, AND TESTING OF SCRAM SYSTEM (continued)

Channel Description	Function	Frequency (1)	Method
11. Hot Reheat Header Pressure	a. Test	M	a. Reduce pressure at sensor to trip channel, verify alarms and indications.
	b. Calibrate	R	b. Known pressure applied at sensor to adjust trips.
12. Main Steam Pressure	a. Test	M	a. Reduce pressure at sensor to trip channel, verify alarms and indications.
	b. Calibrate	R	b. Known pressure applied at sensor to adjust trips.
13. Two Loop Trouble	a. Test	M	a. Special test module used to trip channel by energizing each of four appropriate pairs of two-loop trouble relays.
	b. Test	R	b. Trip logic to cause two loop trouble scram.
14. Plant 480 V Power Loss	a. Test	M	a. Trip channel by applying 40% of rated voltage; verify alarms and indications.
15. High Ambient Temperature (Pipe Cavity)	a. Check	D	a. Comparison of three separate channel indicators.
	b. Test	M	b. Trip channel, verify alarms and indications. Internal test signal to verify trips and alarms.
	c. Calibrate	R	c. Calibrated RTD to adjust temperature trip point.

NOTE 1: D - Daily when in use
M - Monthly
R - Once per refueling cycle
P - Prior to each start-up if not done previous week

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS AND TESTING OF LOOP SHUTDOWN SYSTEM

Channel Description	Function	Frequency (1)	Method
1. Steam Pipe Rupture (Pipe cavity)	a. Check	D	a. Comparison of separate ultrasonic channel indicators/loop.
	b. Test	M	b. Pulse test one temperature channel with another temperature channel tripped, while simultaneously having two ultrasonic channels tripped.
	c. Test	M	c. Pulse test one ultrasonic channel with another ultrasonic channel tripped while simultaneously having two pressure channels tripped.
	d. Test	M	d. Pressure switch actuated by pressure applied at sensor.
	e. Test	M	e. Temperature switch actuated by heat applied at sensor.
	f. Calibrate	M	f. Internal test signal to adjust ultrasonic trip.
	g. Calibrate	R	g. Known pressure applied at sensor to adjust trip.
	h. Calibrate	R	h. Calibrate to adjust temperature trip point.
	i. Calibrate	R	i. Known sound applied at detector to adjust trip.
2. Steam Pipe Rupture (Under PCRV)	a. Check	D	a. Comparison of separate ultrasonic channel indicators/loop
	b. Test	M	b. Pulse test one temperature channel with another temperature channel tripped, while simultaneously having two ultrasonic channels tripped.
	c. Test	M	c. Pulse test one ultrasonic channel with another ultrasonic channel tripped, while simultaneously having two pressure channels tripped.

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS AND TESTING OF LOOP SHUTDOWN SYSTEM (continued)

Channel Description	Function	Frequency (1)	Method
	d. Test	M	d. Pressure switch actuated by pressure applied at sensor.
	e. Test	M	e. Temperature switch actuated by heat applied at sensor.
	f. Calibrate	M	f. Internal test signal to adjust ultrasonic trip.
	g. Calibrate	R	g. Known pressure applied at sensor to adjust trip.
	h. Calibrate	R	h. Calibrate to adjust temperature trip point.
	i. Calibrate	R	i. Known sound applied at detector to adjust trip.
3. Circulator 1A and 1B tripped	a. Test	M	a. Pulse test and verify proper indications.
	b. Test	R	b. Trip both circulators to test loop shutdown.
4. Circulator 1C and 1D tripped	a. Test	M	a. Pulse test and verify proper indications.
	b. Test	R	b. Trip both circulators to test loop shutdown.
5. Steam Generator Penetration pressure	a. Test	M	a. Pressure switches actuated by pressure applied.
	b. Test	M	b. Pulse test each channel with another channel tripped and verify proper indications.
	c. Calibrate	R	c. Known pressure applied at sensor to adjust trip.
6. Reheat Header Activity	a. Check	D	a. Comparison of six separate channel indicators.
	b. Test	M	b. Pulse test each channel with another channel tripped and verify proper indications.
	c. Calibrate	R	c. Expose sensor to known radiation source and adjust trips and indicators.

SECTION V-TABLE 5) (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS AND TESTING OF LOOP SHUTDOWN SYSTEM (continued)

Channel Description	Function	Frequency (1)	Method
7. Superheat Header Temperature	a. Check	D	a. Comparison of 3 separate temperature indicators per loop.
	b. Check	D	b. Comparison of 3 separate temperature differential indicators.
	c. Test	M	c. Pulse test one channel with another channel tripped and verify proper indications.
	d. Calibrate	R	d. Compare thermocouple with calibrated RTD. Internal test signal to adjust trips and indicators.
8. Primary Coolant Moisture (Low Level Channels)	a. Test	M	a. Trip each channel, verify proper indications.
	b. Test	M	b. Trip each channel, pulse test other loop to check loop identification.
9. Primary Coolant Pressure	a. Test	M	a. Pulse test one channel with another channel tripped and verify proper indications, both channels.

NOTE 1: D - Daily when in use
M - Monthly
R - Once per refueling cycle
P - Prior to each start-up if not done previous week

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS AND TESTING OF CIRCULATOR TRIP SYSTEM

Channel Description	Function	Frequency	Method
1. Circulator Speed-Steam and Water	a. Check	D	a. Comparison of 6 separate speed indications per circulator.
	b. Test	M	b. Internal test signal to verify trip setting and indicators.
	c. Test	M	c. Pulse test one channel with another channel tripped, and verify proper indications.
	d. Calibrate	R	d. Known pulse frequency applied at sensor to adjust trips and indicators.
2. Feedwater Flow	a. Check	D	a. Comparison of 6 separate indicators per loop.
	b. Test	M	b. Internal test signal to verify trip setting and indications.
	c. Test	M	c. Pulse test one channel with another channel tripped, and verify proper indications.
	d. Calibrate	R	d. Apply known ΔP at flow transmitter. Internal test signal to adjust trips and indicators.
3. Circulator Bearing Water Pressure	a. Check	D	a. Comparison of 3 separate indicators/circulator
	b. Test	M	b. Pulse test one channel with another channel tripped, and verify proper indications.
	c. Calibrate	R	b. Known pressure applied to adjust trip setting.

SECTION V-TABLE 5 (Continued)

MINIMUM FREQUENCIES FOR CHECKS, CALIBRATIONS AND TESTING OF CIRCULATOR TRIP SYSTEM (continued)

Channel Description	Function	Frequency	Method
4. Circulator Penetration Pressure	a. Test	M	a. Pressure switches actuated by pressure applied.
	b. Test	M	b. Pulse test one channel with another channel tripped, and verify proper indications.
	c. Calibrate	R	c. Known pressure applied at sensor to adjust trip setting.
5. Circulator drain Pressure	a. Check	D	a. Comparison of 3 separate indicators/Circulator.
	b. Test	M	b. Pulse test one channel with another channel tripped and verify proper indications.
	c. Calibrate	R	c. Known pressure applied at sensor to adjust trip setting.
6. Circulator Seal Malfunction	a. Check	D	a. Comparison of 3 separate indicators/circulator.
	b. Test	M	b. Pulse test one channel with another channel tripped and verify proper indications.
	c. Calibrate	R	c. Known pressure applied at sensor to adjust trip setting.
7. Circulator Trip (Manual)	a. Test	R	a. Trip steam turbine drives. Verify water turbine automatic start.

NOTE 1: D - Daily when in use
M - Monthly
R - Once per refueling cycle
P - Prior to each start-up if not done previous week

Sticking contacts and relay shorts to power are the unsafe failure modes. The control room manual SCRAM is tested anually. Control rod in/out limit switches are tested annually. Control rod in/out relays and brakes are tested by small motions (a few inches) monthly, and full SCRAM (single rod unpowered drop with drop time measured) annually.

C. Procedure Observations

Observation of the procedures was considered to be the best way to evaluate possible system impact. However, calibration exercises are not scheduled again until first refueling at Fort St. Vrain, so there were no calibrations available for observation. In addition, some of the monthly tests involve parameters that can be tested only during power operation, which was not scheduled during the time period encompassed by this study. Of the remaining monthly tests, a representative sample was chosen to be observed since many are repetitive and it was desirable to minimize interference with daily plant functions. Those selected included pulse tests, pressure tests and temperature tests.

With the cooperation of staff and supervision at Fort St. Vrain, arrangements were made to observe the selected tests at the regularly scheduled times. The observations considered such items as adequacy of procedures, adherence to procedures, and backup or recovery factors such as support by control room personnel, quality of communication, and availability of indicators (lights, meteres, alarms) to indicate correct performance.

D. Human Reliability Evaluation

The tasks involved in the various procedures were analyzed for the reliability of the various operations. Table 6 provides a summary of this analysis. It includes the equipment locations, names, Human Interfaces, representative signal numbers in the

(Text Continued on Page 125)

LOCATION OR CHANNEL	PROCEDURE	FREQUENCY	COMPONENT AFFECTED	SIGNAL NUMBER	FAILURE MECHANISM	SYSTEM EFFECT	INITIAL FAILURE PROBABILITY	RECOVERY FACTORS	IMPROVEMENT FACTORS	OVERALL FAILURE PROBABILITY
I. TOP LEVEL		A	Rod or Drive		Improper Repair	Single Rod Failure	10^{-2}	Test before and after installation	10^{-3}	10^{-5}
A. Control Rods and Drives	Control Rod Repair									
	Install Rod	A	Rod or Drive		Installation Damage	Single Rod Failure	10^{-3}	Test after installation	10^{-2}	10^{-5}
	Replace Cover	A	Rod or Drive		Cover Loose	Cover blown-possible rod ejection	10^{-2}	Multiple seals, bolts torqued, Leak Test.	10^{-3}	10^{-5}
B. Rod Control System	Test breakers		Circuit Breakers		Left off	No brake power				
	Select bus		Power		Wrong Position	No brake power				
	Select Rod		Rod		Select wrong rod	None				
	In/Out Select		Rod		Out instead of in	Minor transient				
	Maintenance		Rod Power	210	Shorts allowing multiple Rod Withdrawal	Possible power increase	10^{-3}	Multiple rod withdrawal test	10^{-3}	10^{-6}
C. SCRAM Brake Control System	Rod Withdrawal		Rod Power	6446,6452	Not Powered	None				
	Reset SCRAM Relay		Rod Power	163	Not Reset	Channel Trip				
	Manual SCRAM		Rod Power	162	Inadvertent Operation	SCRAM				
	AER SCRAM		Rod Power	160	Inadvertent Operation	SCRAM				
	Maintenance		Beyond 2/3		Short to Rod Brake Power	SCRAM failure	10^{-3}	SCRAM test by dropping at least 1 rod-each half	10^{-3}	10^{-6}
	Maintenance		Before 2/3		Short to Rod Brake Power	Channel failure	10^{-3}	Test single channel SCRAM	10^{-3}	10^{-6}
	Mode Switch		Rod Power	106	Wrong Position	Possible SCRAM RWP				
					Low Power during Power Operation					
II. MAIN SCRAM Parameters										
A. Reactor Bldg. Temp. High (Daily Check)	Test	M	T/O Switch	36	Wrong Position	Single Channel SCRAM				
	Calibration	A	Sensor	327,328	None-not manipulated					
			Input		Test Leads Not Removed	Temp. error	10^{-3}	Channel Comparison	10^{-3}	10^{-6}
			Channel		Miscalibration-all 3 channels	SCRAM failure	$5x10^{-4}$	Reactor Operator sees wrong temperature	10^{-3}	$5x10^{-7}$
			Trip Settings		Set wrong-all 3 channels	SCRAM failure	$5x10^{-4}$	Maximum setting still may allow SCRAM	10^{-2}	$5x10^{-6}$
	Maintenance		Most		Channel Open	Channel failure	10^{-2}	Calibrate and test on installation	10^{-2}	10^{-4}
B. 480V Surge Undervoltage	Test	M	T/O Switch	44	T/O in Test	Single channel SCRAM		Alarms obvious		
	Maintenance		Most		Channel Open	Channel failure	10^{-2}	Calibrate and test	10^{-2}	10^{-4}
C. Circulator Inlet Temperature (Daily Check)	Test	M	T/O Switches	27,29	T/O in Test	Single channel SCRAM		Alarms obvious		
	Calibration	A	Channel trip Setting		Miscalibration-all 3 channels	SCRAM failure	$5x10^{-4}$	5 more channels wrong	10^{-3}	$5x10^{-7}$
	Maintenance		TC	331,334	Failure to replace in position	Single channel SCRAM failure	10^{-3}	Calibrate and test	10^{-2}	10^{-5}
D. Reactor (Primary Coolant) Pressure (Daily Check)	Test	M	T/O Switches	27,29,38 41,40	T/O in Test	Single channel SCRAM		Alarms obvious		
	Calibration	A	Valves	325,326	Pressure Sensor valved off	Channel failure	10^{-2}	Reactor operator sees low pressure	10^{-3}	10^{-5}
			Penetration Cover		Not Replaced	PCRV safety factor reduced	not modeled			
	Maintenance		Most		Channel Open	Single channel SCRAM failure	10^{-2}	Calibration and Test	10^{-2}	10^{-4}

M-Monthly
A-Annual

TABLE 6

RELIABILITY AND RECOVERY FACTORS FOR TEST AND MAINTINANCE PROCEDURES

LOCATION OR CHANNEL	PROCEDURE	FREQUENCY	COMPONENT AFFECTED	SIGNAL NUMBER	FAILURE MECHANISM	SYSTEM EFFECT	INITIAL FAILURE PROBABILITY	RECOVERY FACTORS	IMPROVEMENT FACTORS	OVERALL FAILURE PROBABILITY
E. Reheat Steam Temperature High (Daily Check)	Test	M	T/O Switch	45	T/O in Test	Single channel SCRAM		Alarms obvious		
	Calibration	A	ATC-3A gain	45,46,47	Millivolt calculation error	Single channel SCRAM failure	$3x10^{-2}$	Reactor operator sees wrong temp.	10^{-3}	$3x10^{-5}$
			Trip Setting		Trip setting error	Single channel SCRAM failure	10^{-3}			10^{-3}
	Maintenance		Thermocouple		TC damaged	Single channel SCRAM failure	10^{-2}	Cal., test and wrong temperature indications	10^{-3}	10^{-5}
F. Main (Superheat) Steam Low Pressure	Test	M	Valves, Pipe Cap	321,42, 163	Failure to restore	Single channel SCRAM		Alarms obvious		
	Calibration	A	Pressure Switch		Set too low	Single channel SCRAM failure	10^{-3}	Not tripped during startup	10^{-2}	10^{-5}
			All 3 channels		Identical miscalibration	Parameter SCRAM failure	$5x10^{-4}$	Reheat Palso wrong and absence of trip during startup	10^{-2}	$5x10^{-6}$
	Maintenance	-	Most		Channel open	Single channel SCRAM failure	10^{-2}	Calibration and test	10^{-2}	10^{-4}
G. Hot Reheat Steam Low Pressure	Test	M	Sensor	324	Valves not restored	Channel remains tripped				
	Calibration	A	Switch	43	Left on	Channel trip				
			All 3 channels	324	Identical miscalibration	Parameter SCRAM failure	$5x10^{-4}$	Superheat P also wrong and absence of trip condition during startup	10^{-2}	$5x10^{-6}$
	Maintenance	-	Channel	1797	Signal line open	Channel failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
H. Two Loop Trouble	SCRAM Test	A	Switch (reset)		Not restored	Remains tripped				
	Relay Test	M	TLT Trip Relays	7206	Left on test	Remains tripped				
	Maintenance	-	A or B logic	5282	Left open	Single Logic failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
			Trip Relays	5338,etc.	Left stuck	Single SCRAM channel failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
I. Moisture Monitors (Daily check on mirror temperature)	Test	M	Switches	222,226, 230, etc.	Not restored	Trip				
	Calibration	A	Valves	1819 etc.	Not restored	Possible channel failure	$3x10^{-2}$	7 more monitors	In Model	
			Penetration Cover		Left off	Possible Depressurization	Not modeled			
			2 high channels		Identical miscalibration	SCRAM failure	10^{-3}	Lows also wrong and disagreement with weekly sample	10^{-2}	10^{-5}
	Maintenance	-	Single channel		Left open	Channel failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
			Output logic		Open	Single logic failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
J. Linear Power Channels (Daily check)	Test	M	Switches	50,61,63, etc.	Wrong position	Possible trip				
	Calibration	A	3 Channels		Identical miscalibration	Possible SCRAM failure	$5x10^{-4}$	3 other channels wrong, alpha test, downscale RWP, power calibration	10^{-4}	$5x10^{-8}$
	Maintenance	-	Channel		Channel Open	Single channel failure	10^{-2}	Test on installation and downscale RWP	10^{-3}	10^{-5}
K. Wide Range Channels (Period Trip)	Test	M	Switches	49	Wrong position	Possible trip				
	Calibration	A	Channel	54	Wrong position	Possible trip				
			3 Channels		Identical miscalibration of 5 dpm SCRAM	Possible SCRAM failure	$5x10^{-4}$	2DPM RWP also wrong and operator observes fast level change	10^{-3}	$5x10^{-7}$
	Maintenance	-	Channel		Channel Open	Single channel failure	10^{-2}	Test on installation	10^{-2}	10^{-4}
L. Startup Channels	Not used for SCRAM in "RUN"									

TABLE 6

RELIABILITY AND RECOVERY FACTORS FOR TEST AND MAINTINANCE PROCEDURES

LOCATION OR CHANNEL	PROCEDURE	FREQUENCY	COMPONENT AFFECTED	SIGNAL NUMBER	FAILURE MECHANISM	SYSTEM EFFECT	INITIAL FAILURE PROBABILITY	RECOVERY FACTORS	IMPROVEMENT FACTORS	OVERALL FAILURE PROBABILITY
III. LOOP SHUTDOWN Parameters										
A. Steam Pipe Rupture-Pipe Cavity	Pressure Test	M	Valves, Pipe Cap	-	Fail to restore valve or cap	Sensor inoperative, fails to trip	10^{-1}	Other parameters	In Model	
	Pressure Calibration	A	Valves, Pipe Cap	-	Fail to restore valves or cap	Sensor inoperative	10^{-2}	Other parameters	In Model	
	Maintenance	-	Valves		Fail to restore valves	Sensor inoperative	10^{-1}	Run test after maintenance	10^{-1}	10^{-2}
(Daily check on ultrasonic)	Temperature Test	M	Sensor	-	Trip point mis-set	Fail to trip	10^{-3}	Max. setting is ~200°F.	10^{-2}	10^{-5}
	Temperature Calibration	A	Sensor	-	Trip point misadjusted	Fail to trip	10^{-4}	Max. setting is ~200°F.	10^{-2}	10^{-6}
	Maintenance	-	Sensor	-	Damage sensor	Fail to trip	10^{-3}	Run test after maintenance	10^{-2}	10^{-5}
B. Steam Pipe Rupture-under PCRV	System is identical to Steam Pipe Rupture-Pipe Cavity (above)									
C. Circulator 1A & 1B Tripped	Test	M	Switches	-	Switches held in TEST Mode	Negligible (Pulse Test)	-	-	-	-
	Maintenance	-	Modules Channel	-	Modules removed Channel open	Removal trips Channel failure	- 10^{-3}	- Test after installation	- 10^{-2}	- 10^{-5}
D. Steam Generator Penetration Overpressure	Pressure Test	M	Valves	-	Fail to restore valves	Sensor inoperative	$3x10^{-2}$			$3x10^{-2}$
	Pressure Calibration	A	Valves	-	Fail to restore valve	Sensor inoperative	$3x10^{-2}$			$3x10^{-2}$
				-	Identical miscalibration	Parameter failure	$5x10^{-4}$			$5x10^{-4}$
	Pulse Test	M	Switches	-	Switches held in TEST mode	Negligible (Pulse Test)	-	-	-	-
	Maintenance	-	Valves, etc.	-	Fail to restore valves or channel open	Channel inoperative	10^{-2}	Run test after maintenance	$3x10^{-2}$	$3x10^{-4}$
IV. CIRCULATOR TRIP Parameter	System is the same as Steam Generator Penetration Pressure (III-D).									

TABLE 6
RELIABILITY AND RECOVERY FACTORS FOR TEST AND MAINTINANCE PROCEDURES

GO model, failure modes, system effects, values for the initial failure estimates associated recovery factors, and the final failure estimates.

The procedures generally involve test, calibration and maintenance, as discussed earlier. Failure mode and system effects are determined from an examination of system drawings and the GO logic model developed in the earlier report. Safe failure modes are not considered further.

Error rate estimates are taken from WASH-1400*, Appendix III, as well as references to that report. Error rates given for routine activities range from .03 to .003 depending on the task. For this study, a value of .01 is used unless there are obvious reasons for choosing a different value. Recovery factors which tend to improve reliability are then considered. These include personnel redundancy during the test, later functional tests, independent inspections, improper readings obvious to another operation, annunciation of incorrect state, diverse equipment or operations showing obvious error, and similar items of backup by operator and equipment. Lack of full independence is included by taking a value between full coupling and complete independence. For example, if two operations affecting the same system are considered, the nominal unreliability range would be 10^{-2} (full coupling) to 10^{-4} (independent). For the moderate coupling of 2 operators together (not performing the test separately and independently) a value of 10^{-3} is used. A final reliability value is then estimated as the product of initial reliability and recovery factors.

(*See Appendix C of this Report.)

Final system values below 10^{-6} are not used since they would have no affect on the overall system. Common mode failures (assumed to be 10^{-5} in the earlier study) will probably dominate if the random probability is as low as 10^{-6}. Channel values below 10^{-4} are not used because the hardware values are usually 10^{-3} or higher for a single channel. The search for recovery factors ends if the final value drops below 10^{-6} or 10^{-4} for the system or channel values respectively. Thus the final values quoted in Table 6 are upper limits. In many cases the actual values would be much lower, but there is no need to determine these values.

In the various channel tests the usual failure modes are failure to restore the channel to operation (valves or switches left in wrong position) and failure to perform the test properly. The procedures are quite detailed on actual test performance, training is extensive, and a control room operator checks trips and indications, so performing this part of the test should have a failure probability of .001 or less. However, the restore step varies in detail among the tests. The failure probability of this step is estimated as:

.001	if procedure calls out the step and an independent check is performed;
.003	if the procedure requires restoration and details the items by number and individual steps on a check-off list;
.01	if the restore step is not detailed
.03	if the restore step is missing (the operator is credited with remembering the step).
.1	if the restore step is missing and 3 or more items (valves, covers, etc.) must be restored (the high value arises from the confusion factor even though the operator remembers the step).

Common mode failures include miscalibration of three coincident channels due to using incorrect settings (of either equipment to be calibrated or calibration equipment itself) or deficiences in the calibration equipment. For miscalibration, the probability of the first failure is taken as .01. There is some carryover to the others, so the probabilities are estimated as .1 for the second and .5 for the third. Thus the estimate for all 3 is .0005. Recovery factors to improve this estimate include:

1. Continuation to more calibrations of the same parameter (e.g., more pressure tests after the first set) on a different SCRAM input (perhaps Main Steam Pressure after Hot Reheat Header Pressure).
2. Operating range of variable unreasonable when compared to other variables (pressure-temperature combination not the same as before, neutron flux disagrees with heat balance, ambient temperature reads high compared to operator's perception, etc.).
3. More than 3 identical monitors of same variable (6 Reheat Header Activity monitors, 6 moisture monitors, 6 circulator speed monitors on each of 4 circulators, etc.).
4. Diverse equipment disagrees (e.g., RHA monitors and moisture monitors may be the only parameters of their kind used, but in both cases weekly samples are taken for laboratory analysis, so the disagreement should be recognized at this point.)

The possibility of calibration equipment failure can be controlled by a systematic program of inspection and test of this equipment, as well as the recovery factors.

In Table 6, "Top Level" refers to equipment and interfaces below the channel inputs to the main SCRAM "OR" gate. This includes the SCRAM Brake Control System, Rod Control System, and the control rods and drives.

E. ERROR EVALUATION (TABLE 6)

1. Control Rod Drives

For control rods and drives the monthly testing is the same as the normal operation of the rod and should contribute little to the unreliability. Control rod repair is performed between refuelings with the absorber material replaced and drives reconditioned. This procedure is given a nominal reliability of 0.99. The recovery factors are functional tests and unpowered drops before and after installation, which are also given a nominal reliability of 0.99. These values are expected to be conservative estimates in the sense that actual reliability should be higher. Recovery factors are not completely independent because the tests are performed in approximately the same way. Thus the improvement factor is given a partially coupled value of 10^{-3}. The final value for the failure probability is then 10^{-5} or less, which is smaller than the hardware value of 10^{-4} determined in the previous study. Thus no further consideration is needed unless the hardware is improved. The remaining consideration is a possible failure mode which is not apparent during functional tests, since this could be a common mode failure for several rods as well as including the factor of not being tested. A detailed examination of the design would be needed to develop confidence that such failure modes are unlikely. Installation damage is given a lower probability value of 10^{-3}, because it is likely that the damage would be apparent from a rod being stuck or inoperable even before the test is performed. Replacement of the control rod refueling penetration cover is considered because multiple failures here could result in a possible ejection of the control rod and orificing assembly. However, there are several recovery factors here including three seals the the operations of torquing down all the bolts which tie down the assembly to the refueling penetration, and leak testing after installation.

In the Rod Control System most of the operator interfaces shown have little effect except for possible premature SCRAM. Even the choice of moving a rod out instead of in results in a minor transient which would be terminated by the operator if he sees that the neutron flux is going up, or by the automatic rod withdrawal prohibit or SCRAM if he does not. For the maintenance procedures any failure leaving the circuit open results in a premature SCRAM, so only possible shorts allowing multiple rod withdrawal could have a possible safety effect. Shorts from maintenance operations are considered less probable than open circuits or normal failures so that shorting failure probability is chosen at 10^{-3}. The first recovery factor is a mandatory multiple rod withdrawal test which is given an improvement factor of 10^{-3}. Since this gives a final value of 10^{-6}, additional improvement factors are not sought although there are others.

In the SCRAM brake control system the normal operational interfaces and maintenance operations leaving the system open either have no effect or result in premature SCRAMS. Again the only possible maintenance failure would be a short to rod brake power. The recovery factor is the SCRAM test before startup. However, this test should involve dropping at least 1 rod in each half of the total rod system, since otherwise an undetected short might be present in the half that was not tested.

The next section of table 6 includes all of the main SCRAM parameters. For each channel the procedures of interest are test, calibration and maintenance.

2. Main Scram Parameters

For Reactor Building Temperature High the test procedure might leave the test/operate switch in the wrong position. However, these switches are always designed so that the wrong position will either trip the channel or add a signal to the normal signal causing a premature trip. For the calibration procedure the sensor is not manipulated so this is not a source of failure. Test leads or other instrumentation could be left attached to the input but this would be noticed on comparison of the channel readouts. When calibrating the temperature readout it is possible to miscalibrate all three channels, but this would be noticed during the shift checks when the operator would see the wrong temperature on the channel readout. The trip settings could also be set wrong for all three channels. In this case the normal setting is close to the full scale available on the instrument. Thus even improper setting of all three channels would still allow a SCRAM although slightly delayed due to the higher settings for the trips. Maintenance affecting most of the components could lead to a channel failure if the channel were left open. Calibration and test on installation provides the recovery factor for this error.

The 480 Volt Surge Undervoltage channel is similar to the above in that mistakes in the test procedure lead to a premature SCRAM, and maintenance operations leaving the channel open would lead to a channel failure with the recovery factor being calibration and test on reinstallation.

For the Circulator Inlet Temperature the primary mistake of interest would be miscalibration of three identical channels. However, there are 5 additional channels to be calibrated so the recovery factor would be discovery that additional channels were also wrong. For maintenance procedures, failure to replace a thermocouple or leaving the channel open would lead to a single channel SCRAM failure which would be detected by calibration and testing after completion of maintenance. It would also be possible to conceive that the thermocouple was placed in the wrong location and reads some different temperature. This error would be noticed during the shift check of temperatures against all other channels as well as during power calibration.

The Reactor Pressure calibration involves manipulation of several valves which could be left in the wrong position and cause a single channel failure. This error would become apparent on checking the pressure readings during the shift checks. Maintenance results are similar to those on the other channels except for the fact that the penetration cover is removed for this procedure. If the cover is not replaced the PCRV integrity is threatened. The effect is not further modeled since it is not connected to the Plant Protection System. However, the procedure should be very explicit about replacing the penetration cover and performing the leak test appropriately. The use of an independent operator to perform the leak test would help to improve the reliability of this operation. Identical miscalibration is unlikely since the data are plotted independently for each channel and used for the settings.

For Reheat Steam Temperature High the gain of the amplifier could be set wrong leading to a single channel failure. This would also lead to an improper temperature reading which would be seen by the reactor operator during comparisons with other channels and power calibration.

Improper trip setting is chosen as the failure mode since the procedures make this appear to be the most likely possibility for error. The maximum possible channel setting is sufficiently high so that it does not provide a recovery factor. Identical miscalibration is not likely because calculations are performed independently for the individual channels during the calibration. These are expected to be reasonably independent. Multiple trip setting errors for several channels should be noticed since there are so many temperature calibrations and trip settings to be made. The probability of multiple trip setting errors could be reduced by using personnel redundancy for the calibration procedures. Maintenance errors involving thermocouple damage or improper temperature settings in the channel would be detected by calibration, tests and observations of the wrong temperature indication.

Superheat Steam Low Pressure testing involves several valves and pipe caps which could be left unrestored. This error leads to annunciation or alarms and is not considered further. During calibration the pressure switch could be set too low leading to a single channel failure. This error would be noticed because the channel would not be tripped as expected during startup. Improper maintenance leading to a single channel failure would be detected during calibration and test.

Hot Reheat Steam Low Pressure is quite similar to Superheat Steam Low Pressure. Slightly different failure modes are considered although most of these apply to both channels.

The Two Loop Trouble SCRAM input involves the A and B logics and the TLT trip relays which are tested separately from the logics. Maintenance could leave the logics open or the relays stuck, but these would be tested on installation.

Among the various parameters which feed the Two Loop Trouble input, there are possibilities for miscalibration or improper trip settings. This will not be of much importance for parameters like temperature and pressure which have many sensors. In these cases the continuation to calibration of more of the sensors should lead to discovery of the error. Considerations of identical miscalibration are more important when involved with parameters with a minimum number of sensors. If the number of sensors for a unique parameter were as low as three the possibility of identical miscalibration of 5 x 10^{-4} could be higher than the equipment failure probability. However, the existence of two cooling loops generally means the existence of at least six sensors of any type since there are at least three for each loop. This includes such items as Reheat Header Activity (6 sensors) and Moisture Monitors (8 sensors). The nuclear channels involve at least six channels (not counting the automatic control channel) except at very low power where only the two Startup Channels are active. Even here the Wide Range Channels provide a backup many decades below full power.

The Moisture Monitor channels involve calibrations where valves could be left not restored. This could lead to a possible single channel failure with the recovery factor consisting of seven more monitors. A final failure probability is not listed because the total system is included in the overall model. The PCRV penetration cover must be removed for calibration and could be left off leading to a possible PCRV leak. This failure is not modeled, but explicit procedural requirements for replacement, bolt torquing and leak testing could minimize the possibility of this failure. Identical miscalibration of the two high level moisture channels could lead to a SCRAM failure. Recovery factors include the possibility that the low level channels would also be discovered to be wrong. Also, weekly samples of moisture are taken for chemical analysis. If the moisture channels disagree with these samples the miscalibration should be discovered. Maintenance errors leading to a single channel failure or output logic left open leading to a single logic failure should be discovered during the test on installation.

The Nuclear Channels have similar possibilities for identical miscalibration or channels left open, however, additional recovery factors are available for these channels. For example, the Linear Power Channels have fission chambers as detectors, and these have a switch to increase sensitivity so that alpha particles can be detected from the chambers, thus giving a test of channel integrity with no reactor input. Downscale failure of these channels will cause a Rod Withdrawal Prohibit. Finally the power level shown by these channels is checked by a power calibration against physical parameters. The period trips on the Wide Range Channel are checked by trips set at 2 decades per minutes and 5 decades per minute. Also the operator can observe the rate of level change and intuitively estimate whether this is too fast, thus indicating the possibility that the period trip may have failed.

For the above discussion of SCRAM inputs all parameters were included since they are primary inputs to the SCRAM logic. For the following considerations of loop shutdown parameters and circulator trip parameters, only parameters that do not have daily checking are considered since these are secondary SCRAM requirements. The loop shutdown parameters could cause a SCRAM only if one of the two loops was already down or if simultaneous trouble occurred in the second loop.

3. Loop Shutdown and Circulator Trip

Steam Pipe Rupture has 3 parameters available to cause loop shutdown or SCRAM if the other loop were already down. These include high pressure or high temperature with ultrasonic noise independently in the pipe cavity or under the PCRV. Failure to restore the pressure channel to operation is an important failure mode, but the functional diversity of additional parameters reduces the impact. Identical miscalibration of the temperature channel is less likely because of a local readout which is used in the calibration procedure.

For Steam Generation Penetration Pressure all test and calibration errors work in a safe direction escept for failure to restore the valves to their proper condition. Identical miscalibration of all three channels could lead to a parameter failure. Continuation to another set of similar calibrations could provide a recovery factor except that the only similar parameter (Circulator Penetration Pressure) is normally calibrated a week later.

Table 5-7 compares maximum human interface failure probabilities with the hardware results obtained in the previous report for each parameter. In the previous report the value for human interfaces was set at a minimal value. In the parameter column the failure probability is taken from Table 6 for those parameters where redundant channels are affected. For those values shown by an asterisk, a multiple effect due to redundant channels was not found so the value was computed from appropriate combination of the input channels. In general this is a combination of two out of three channels. For the Moisture Monitors the value given is the failure probability for both high level channels failing.

Steam pipe rupture is the combination not only of several channels but of all three parameters involved. Circulator Trip and Two Loop Trouble include the effects of dual logics as well as fanning of outputs to all three SCRAM channels. For the latter parameters a specific result is not available from the previous study because their effect was included as part of more complete calculations.

The purpose of this comparison is to determine whether the human interfaces alone can increase the failure probability above the hardware value obtained in the previous report. The only cases in which this occurs are in the 10^{-6} to 10^{-7} range so it is concluded that the human interfaces for test, maintenance, and calibration do not affect the system failure probability significantly. This result assumes that the recovery factors are actually operating consistently. Since some of the recovery factors are applied by administrative controls only, it is essential that these controls be rigidly enforced.

SECTION V-TABLE 5-7

COMPARISON OF FAILURE PROBABILITIES WITH PREVIOUS STUDY

Channel	Highest Human Interface Failure Probability Assuming all Recovery Factors are Operative		Previous Report Parameter Failure Probability
	Channel	Parameter	
I. Top Level:			
Rod System Failure		10^{-5}	10^{-5}
Single Rod Failure		10^{-5}	10^{-4}
II. Main SCRAM			
RBTH	10^{-4}	$5x10^{-6}$	$2x10^{-7}$
480V SUV	10^{-4}	10^{-8}*	$7x10^{-4}$
CIT	10^{-5}	$5x10^{-7}$	$2x10^{-7}$
RPH	10^{-4}	10^{-8}*	$2x10^{-7}$
RSTH	10^{-3}	10^{-6}*	$4x10^{-7}$
SSLP	10^{-4}	$5x10^{-6}$	10^{-4}
TLT	10^{-4}	10^{-8}*	Not available
MM	$3x10^{-2}$	10^{-3}*	10^{-3}
Linear Power	10^{-5}	$5x10^{-8}$	10^{-6}
Wide Range	10^{-4}	$5x10^{-7}$	10^{-6}
III. Loop Shutdown			
SPR-Pressure	10^{-1}	10^{-6}*	10^{-4}
-Temperature	10^{-5}		
CT	10^{-5}	$<10^{-6}$*	Not available
SGPO	$3x10^{-2}$	$3x10^{-4}$	$4x10^{-4}$
IV. Circulator Trip			
CPP	$3x10^{-2}$	$3x10^{-4}$	10^{-3}

*From combination of channels.

F. Procedural Considerations and Conclusions

Although the human interface effects have been shown to have little impact on system safety, there could easily be a substantial impact on system availability which has not been specifically considered in this study. Some of the interfaces that contribute to premature trips could easily cause reactor down time of a day or more. The cost of down time is in the range of $\$10^5$/day. Thus substantial incentive exists to improve test, calibration and maintenance procedures in order to avoid downtime. The avoidance of a single day per year in down time could easily pay for the cost of 5 people working for a year toward upgrading test and maintenance procedures and practices. Another incentive for improving human interfaces is the possibility of unrecognized common mode failures. Even after the most detailed analysis there will always remain some unexpected failure probabilities, some of which can be common mode. Improvements to individual interface failure probabilities will tend to reduce, although not eliminate, any common mode effect due to coupling between interfaces.

Reactor operators are selected and trained to a high degree of reliability. However, the reliability required of a single person may exceed human capabilities just as equipment capabilities can be exceeded. The preparation of detailed and thorough procedures is intended to assist the operator in maintaining the highest degree of reliability. The degree of detail is sometimes burdensome, but it is essential if the highest standards are to be maintained. In the current study several features of the procedures were identified as contributing to the initial reliability or for recovery factors. Although these are usually included in existing procedures it seems useful to emphasize these here as an aid to those writing future procedures or rewriting existing ones.

Equipment needed for specified procedures and auxiliary calibration procedures should be listed. Such things as heat sources for temperature tests and oscilloscopes to verify operation of other equipment may easily be forgotten. Each item (switch, valve, etc.) to be manipulated should be called out by numoer and location. This identification is also necessary when restoring the channel to operation. The restore step itself should be included with each individual item to be restored,listed and identified. This is especially important where the operating status of a channel is not indicated or annunciated, because the channel could be left dead until the next test cycle. In some cases a restore step is necessary for equipment (like penetration covers) not included in the channel instrumentation. These items should be listed and identified because of their possible interaction with other plant systems. Careful identification of all items will also improve personnel efficiency by speeding up the test procedures.

An important recovery factor for maintenance operations is the test and calibration of a piece of equipment after reinstallation. The test should be designed to test all necessary modes of operation and not just those that result in appropriate annunciators being triggered. This is critical in the top level SCRAM logic. Multi-contact relays and switches are used, and all contacts may not be tested by certain types of functional tests. For example, the main SCRAM relays have one set of contacts to turn on a light and another set of contacts to interrupt the SCRAM bus, so that a single channel SCRAM light does not prove that the SCRAM relay contacts actually opened. Even a full SCRAM is not a complete test since the relay contacts are dual and one set of contacts may have stuck. However, meters are provided across the dual SCRAM relay matrix to indicate the direction of current flow during a single channel SCRAM. Recording of these meter readings during a single channel SCRAM test will indicate the conditions of the SCRAM contacts. The manual SCRAM switch has contacts in all three SCRAM channels before the two-out-of-three matrix as well as dual contacts in series after the relay matrix. Thus a successful manual SCRAM test does not indicate that all contacts are working. Continuity or voltage checks would indicate that the contacts are not stuck. Such a test might also be appropriate after a high current surge which might have welded switch or relay contacts. SCRAM capability tests during shutdown are sometimes performed by raising a single rod a small amount and verifying that it drops when the SCRAM is signaled. If the control rod system is divided into sections this test should include dropping one rod in each section to verify that all contacts in various switches and relays are servicable.

The possibility of identical miscalibration of redundant channels often dominates the parameter failure probability since the redundancy reduces the effect of errors in single channels. There are several ways to reduce the possibility of identical miscalibration. One would be the use of two people for the test although this would certainly increase the overall cost. One person would read the procedure and check each step while the other one performed the actual test or calibration. For additional improvement the two could reverse roles and repeat the calibration. Another way would be to have each individual calibrate one channel of a redundant set with the other calibrations done by other people independently. Still another way would be to require reporting and independent rechecking if any channel required recalibration by more than a preselected amount or if more than one channel in a set had to be recalibrated.

One of the frequent recovery factors is comparison of readouts to check calibration and operability of sensor channels. However, trip settings cannot be verified in this fashion. Thus verification of trip setting levels should be included in monthly tests rather than just a simple test for operability of the trip circuit.

It would be useful for each reactor owner to gradually develop a data base for personnel error rates to develop his own.human factors information. Human reliabilities estimated here and in other human factors studies are often based on broad generalizations and extrapolations. The applicability of this data to individual situations could best be determined by actual experimental data accumulated as experience is gained with the reactor system. The number of tests and calibrations performed is sufficiently large so that a reasonable data base could be obtained in a couple of years, especially if data from several reactors were to be combined.

Several recovery factors have been identified to help improve the overall reliability of test, calibration, and maintenance. These include comparison of similar parameters, comparison of diverse parameters, control room readout of parameter values, annunciators, trip conditions changing during startup, and test and calibration after maintenance. If these factors are not active, the human errors could easily dominate the overall failure probability as can be seen from Table 6. Administrative controls are the only way to assure that some of the recovery factors are effective (daily checks, test schedules, required tests after maintenance, periodic calibration of test gear, etc.). Thus overall safety depends on the conscientiousness and capability of the people who apply the controls as well as those who perform the work. This conclusion is neither surprising nor unique, but it emphasizes the recognized need for dependable, dedicated people in the operation and management of nuclear power plants.

VI. REFERENCES

1. Reliability Analysis of An HTGR SCRAM System Including Human Interfaces, KSC-1037-1, March 1975, Kaman Sciences Corporation.

2. HTGR Accident Initiation and Progression Analysis Status Report, Volume IV, General Atomic Company, Dec. 1975, GA-A13617.

3. Technical Specifications, Fort St. Vrain Nuclear Generating Plant, Public Service Company, Denver, Colorado, April, 1972.

4. "Selection and Training of Personnel For Nuclear Power Plants," Document # N18.1-1971, by American National Standards Institute.

5. Reactor Safety Study (WASH-1400), NRC (Formerly AEC) 1975.

6. (a) "Human Reliability Analysis Applied to Nuclear Power," Alan D. Swain, Sandia Laboratories, Proceedings of 1975 Annual Reliability and Maintainability Symposium. EEE.

   (b) Development of a Human Error Rate Data Bank, A.D. Swain, Sandia Laboratories, Document # SC-R-70-4286, July 1970.

7. "Fort St. Vrain Nuclear Generating Station Final Safety Analysis Report" Public Service Company of Colorado, Denver, Colorado, Four volumes, 14 sections, 5 appendices, 1970.

8. "Reactor Operator Training Programs Utilizing Nuclear Power-Plant Simulators", Paul F. Collins, Branch Chief Licensing, NRC, Nuclear Safety, Vol 16, # 4, July-August 1975.

9. "List of Structures, Systems and Components Required for a Safe Shutdown of the Plant", Table 1.4-2, Final Safety Analysis Report, Vol I, Fort St. Vrain Nuclear Generating Station, PSCC, Denver, Colo.

10. "Human Factors Associated With Prescribed Action Links" Alan D. Swain, Sandia Laboratories, SAND-74-0051, July 1974. (See Conclusions)

REFERENCES (Continued)

11. Miscellaneous Human Error Responses

A. "Human Factors In Reliability"
David Meister, Bunker-Ramo Corporation
Reliability Handbook, Section 12, page 24
Quotes in personal communication from
E. T. Klemmer; operator keypunch error
rates with little training are about 10-2
and after a year of training, rates of 10^{-3}.

B. "Human Performance Criteria in Men-Machine Systems", H. G. Williams, MELPAR, Inc. Report from Missile Design and Development, Volume 15, No. 2, February 59, Dial setting tests show untrained operator error rates of 10^{-2}, and trained operator error rates of 10^{-3}.

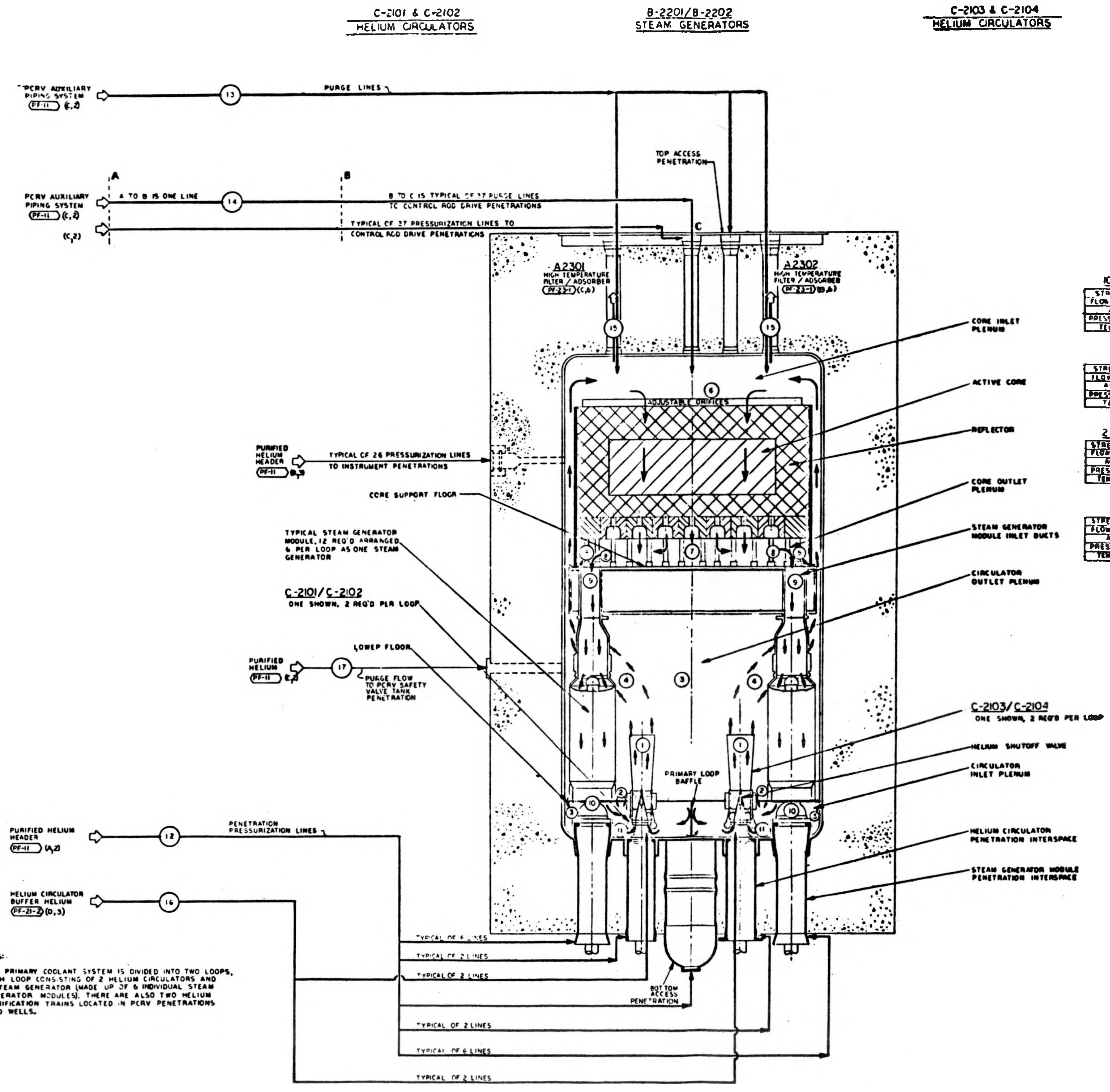
C. "Human Error and Plant Operation"
T. A. Kletz and G. D. Whitaker,
Imperial Chemical Industries, Ltd., U.K.,
9 January 1973
Quotes U.K., AEA estimates of Human Error ranging from 10^{-2} to 10^{-4} per operation; depending on stress, plus pilot error rates in all weather landing system as high as $2x10^{-2}$.

D. "Effect of Human Error and Status Component Failure on Engineered Safety System Reliability." Holmes and Narver, Inc., November 1967. Report #HN-194. Quotes-ranges of human error rates for various tasks in nuclear power plant maintenance from 10^{-2} to 10^{-3}.

APPENDIX A

*PROCESS DRAWINGS

*These drawings are reproduced from the Fort St. Vrain FSAR drawings with permission of General Atomic Company.


C-2101 & C-2102
HELIUM CIRCULATORS
B-2201/B-2202
STEAM GENERATORS
C-2103 & C-2104
HELIUM CIRCULATORS
PCRV AUXILIARY PIPING SYSTEM
PF-11 (C,2)
13
PURGE LINES
TOP ACCESS PENETRATION
A
B
PCRV AUXILIARY PIPING SYSTEM
PF-11 (C,2)
A TO B IS ONE LINE
14
B TO C IS TYPICAL OF 37 PURGE LINES TO CONTROL ROD DRIVE PENETRATIONS
(C,2)
TYPICAL OF 37 PRESSURIZATION LINES TO CONTROL ROD DRIVE PENETRATIONS
C
A2301
HIGH TEMPERATURE FILTER / ADSORBER
PF-23-1 (C,6)
A2302
HIGH TEMPERATURE FILTER / ADSORBER
PF-23-1 (B,6)
15
15
6
CORE INLET PLENUM
ADJUSTABLE ORIFICES
ACTIVE CORE
REFLECTOR
PURIFIED HELIUM HEADER
PF-11 (B,3)
TYPICAL OF 26 PRESSURIZATION LINES TO INSTRUMENT PENETRATIONS
CORE SUPPORT FLOOR
CORE OUTLET PLENUM
TYPICAL STEAM GENERATOR MODULE, 12 REQ'D ARRANGED, 6 PER LOOP AS ONE STEAM GENERATOR
STEAM GENERATOR MODULE INLET DUCTS
7
8
5
5
9
9
C-2101/C-2102
ONE SHOWN, 2 REQ'D PER LOOP
CIRCULATOR OUTLET PLENUM
LOWER FLOOR
PURIFIED HELIUM
PF-11 (C,3)
17
PURGE FLOW TO PCRV SAFETY VALVE TANK PENETRATION
4
3
4
C-2103/C-2104
ONE SHOWN, 2 REQ'D PER LOOP
HELIUM SHUTOFF VALVE
1
1
PRIMARY LOOP BAFFLE
CIRCULATOR INLET PLENUM
10
2
2
10
3
3
11
11
PURIFIED HELIUM HEADER
PF-11 (A,2)
12
PENETRATION PRESSURIZATION LINES
HELIUM CIRCULATOR PENETRATION INTERSPACE
STEAM GENERATOR MODULE PENETRATION INTERSPACE
HELIUM CIRCULATOR BUFFER HELIUM
PF-21-2 (D,3)
16
TYPICAL OF 6 LINES
TYPICAL OF 2 LINES
TYPICAL OF 2 LINES
BOTTOM ACCESS PENETRATION
TYPICAL OF 2 LINES
TYPICAL OF 6 LINES
TYPICAL OF 2 LINES

NOTES:

1. THE PRIMARY COOLANT SYSTEM IS DIVIDED INTO TWO LOOPS, EACH LOOP CONSISTING OF 2 HELIUM CIRCULATORS AND 1 STEAM GENERATOR (MADE UP OF 6 INDIVIDUAL STEAM GENERATOR MODULES). THERE ARE ALSO TWO HELIUM PURIFICATION TRAINS LOCATED IN PCRV PENETRATIONS AND WELLS.

100% STEAM FLOW

STREAM NO	1	2	3	4	5	6	7	8	9	10
FLOW LBS/HR	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ACFM	[illegible]	1380	1270	139000	830	[illegible]	[illegible]	212000	[illegible]	[illegible]
PRESSURE PSIA	720	686	686	699	660	659	650	696	695	[illegible]
TEMP °F	755	755	755	762	762	762	1444	1446	1427	762

STREAM NO.	11	12	13	14	15	16	17			
FLOW LBS/HR	1,145,000	0	[illegible]	26.5	935	433	350			
ACFM	138000	0	13	7.5	73.4	14.4	11.0			
PRESSURE PSIA	686	710	704	704	699	696	704			
TEMP °F	742	105	105	105	759	105	105			

25% STEAM FLOW

STREAM NO.	1	2	3	4	5	6	7	8	9	10
FLOW LBS/HR	498,000	5000	4,200	488,900	[illegible]	[illegible]	[illegible]	488,900	480,900	480,900
ACFM	35200	400	350	[illegible]	245	[illegible]	[illegible]	64,500	63,500	[illegible]
PRESSURE PSIA	551	585	555	551	531	591	590	590	590	590
TEMP °F	571	570	570	560	[illegible]	980	1264	1260	1238	969

STREAM NO.	11	12	13	14	15	16	17			
FLOW LBS/HR	498,000	0	50	173	791	332	256			
ACFM	38,300	0	1.0	7.5	63	14.4	11.0			
PRESSURE PSIA	539	710	704	591	591	588	591			
TEMP °F	569	105	105	105	578	109	109			

Figure A-1 -Simplified process flow diagram primary coolant system

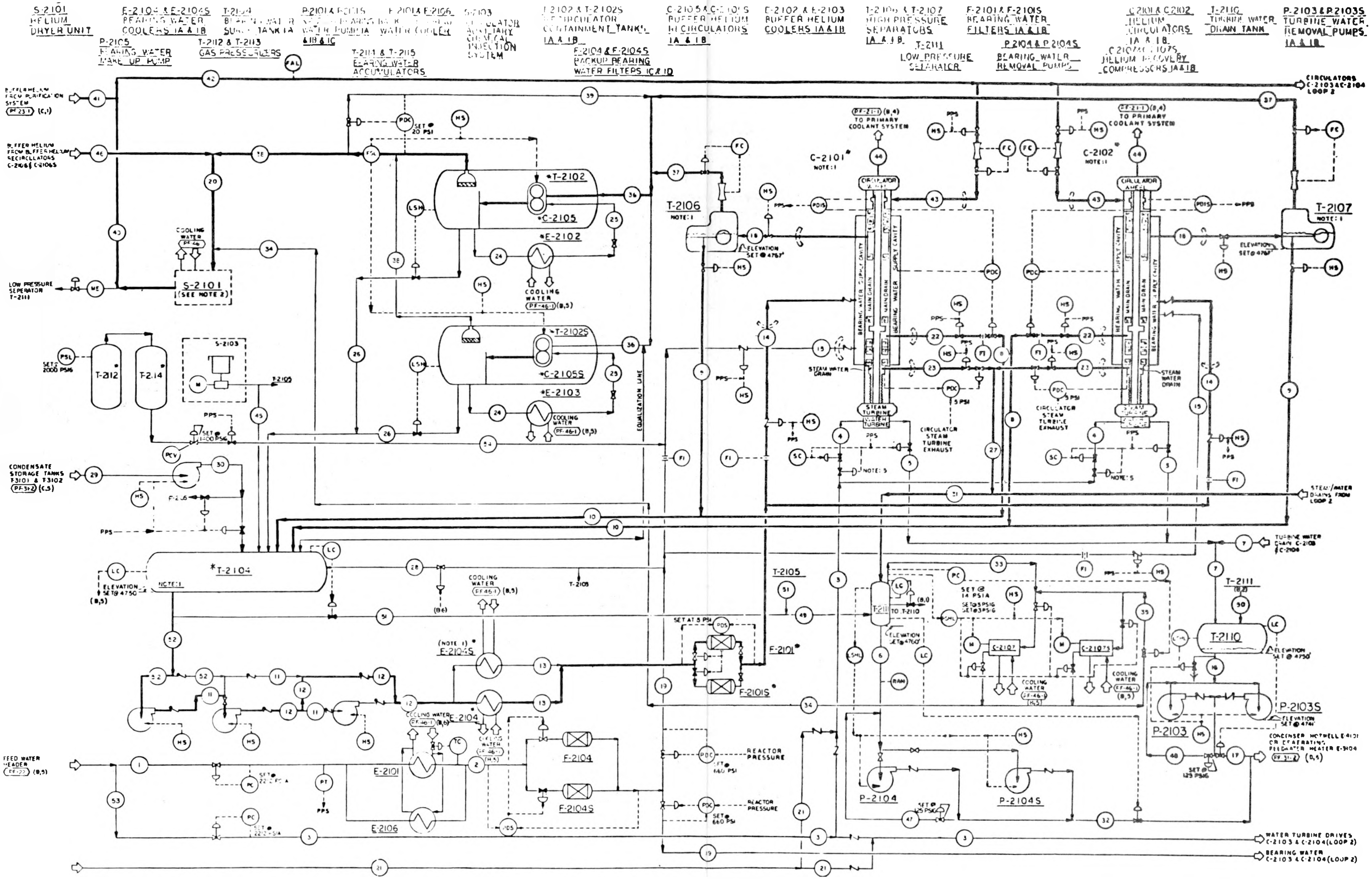

S-2101 HELIUM DRYER UNIT
E-2104 & E-2104S BEARING WATER COOLERS IA & IB
T-2104 BEARING WATER SURGE TANK IA
P-2101 & P-2101S BEARING WATER PUMPS IA & IB & IC
E-2101 & E-2106 WATER COOLER
S-2103 CIRCULATOR AUXILIARY CHEMICAL INJECTION SYSTEM
T-2102 & T-2102S RECIRCULATOR CONTAINMENT TANKS IA & IB
C-2105 & C-2105S BUFFER HELIUM RECIRCULATORS IA & IB
E-2102 & E-2103 BUFFER HELIUM COOLERS IA & IB
T-2106 & T-2107 HIGH PRESSURE SEPARATORS IA & IB
F-2101 & F-2101S BEARING WATER FILTERS IA & IB
C-2101 & C-2102 HELIUM CIRCULATORS IA & IB
T-2110 TURBINE WATER DRAIN TANK
P-2103 & P-2103S TURBINE WATER REMOVAL PUMPS IA & IB
P-2105 BEARING WATER MAKE UP PUMP
T-2112 & T-2113 GAS PRESSURIZERS
T-2114 & T-2115 BEARING WATER ACCUMULATORS
F-2104 & F-2104S BACKUP BEARING WATER FILTERS IC & ID
T-2111 LOW PRESSURE SEPARATOR
P-2104 & P-2104S BEARING WATER REMOVAL PUMPS
C-2107 & C-2107S HELIUM RECOVERY COMPRESSORS IA & IB
BUFFER HELIUM FROM PURIFICATION SYSTEM (PF-23-1) (C,1)
BUFFER HELIUM FROM BUFFER HELIUM RECIRCULATORS C-2105 & C-2105S
LOW PRESSURE SEPERATOR T-2111
CONDENSATE STORAGE TANKS T-3101 & T-3102 (PF-31-2) (C,5)
FEED WATER HEADER (PF-22) (B,5)
CIRCULATORS C-2103 & C-2104 LOOP 2
TO PRIMARY COOLANT SYSTEM (PF-21-1) (B,4)
C-2101 NOTE: 1
C-2102 NOTE: 1
T-2106 NOTE: 1
T-2107 NOTE: 1
ELEVATION SET @ 4767'
CIRCULATOR WHEEL
STEAM TURBINE
WATER TURBINE
BEARING WATER SUPPLY CAVITY
MAIN DRAIN
SUPPLY CAVITY
STEAM WATER DRAIN
CIRCULATOR STEAM TURBINE EXHAUST
NOTE: 5
STEAM/WATER DRAINS FROM LOOP 2
TURBINE WATER DRAIN C-2103 & C-2104
*T-2102
*C-2105
*E-2102
*T-2102S
*C-2105S
*E-2103
COOLING WATER (PF-46-1) (B,5)
S-2101 (SEE NOTE 2)
S-2103
T-2112
T-2.14
SET @ 2000 PSIG
SET @ 20 PSI
SET @ 1400 PSIG
EQUALIZATION LINE
*T-2104
NOTE: 1
ELEVATION SET @ 4750
(NOTE 1) * E-2104S
E-2104
E-2101
E-2106
F-2104
F-2104S
F-2101
F-2101S
SET AT 5 PSI
SET @ 2212 PSIA
T-2105
T-2111
TO T-2110
ELEVATION SET @ 4760'
SET @ 14 PSIA
SET @ 5 PSIG
C-2107
C-2107S
T-2110
ELEVATION SET @ 4750'
P-2103
P-2103S
ELEVATION SET @ 4746'
P-2104
P-2104S
SET @ 125 PSIG
REACTOR PRESSURE
SET @ 660 PSI
CONDENSER HOTWELL E-4101 OR DEAERATING FEEDWATER HEATER E-3104 (PF-31-2) (D,5)
WATER TURBINE DRIVES C-2103 & C-2104 (LOOP 2)
BEARING WATER C-2103 & C-2104 (LOOP 2)
PDC
PDS
PDIS
HS
FC
FI
LC
LSH
TC
PT
PC
PCV
SC
RAM
PPS
FAL
FSL

Figure A-2 -Process flow diagram helium circulators auxiliary system

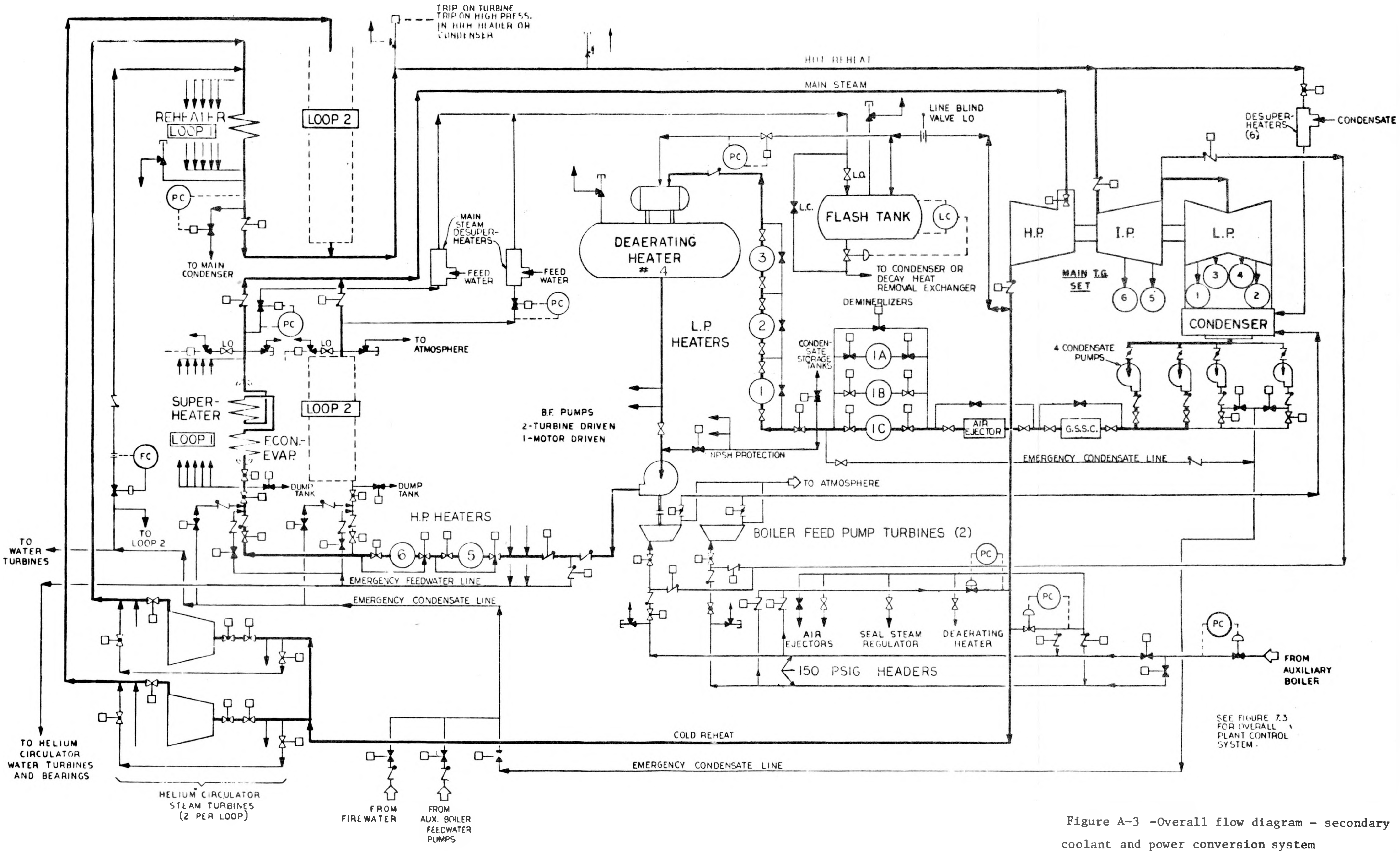


Figure A-3 -Overall flow diagram - secondary coolant and power conversion system

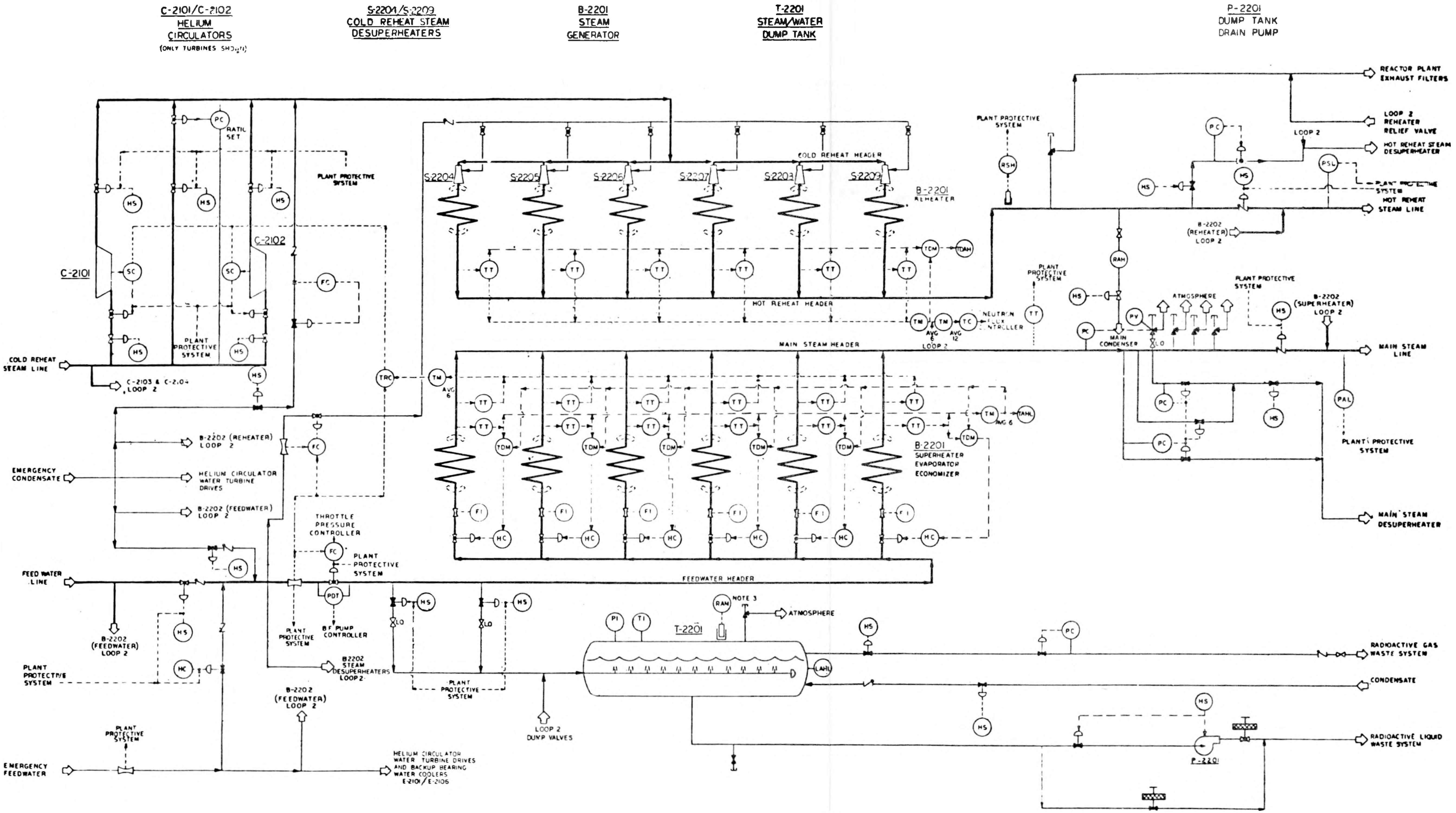


Figure A-4 -Process flow diagram - secondary coolant system

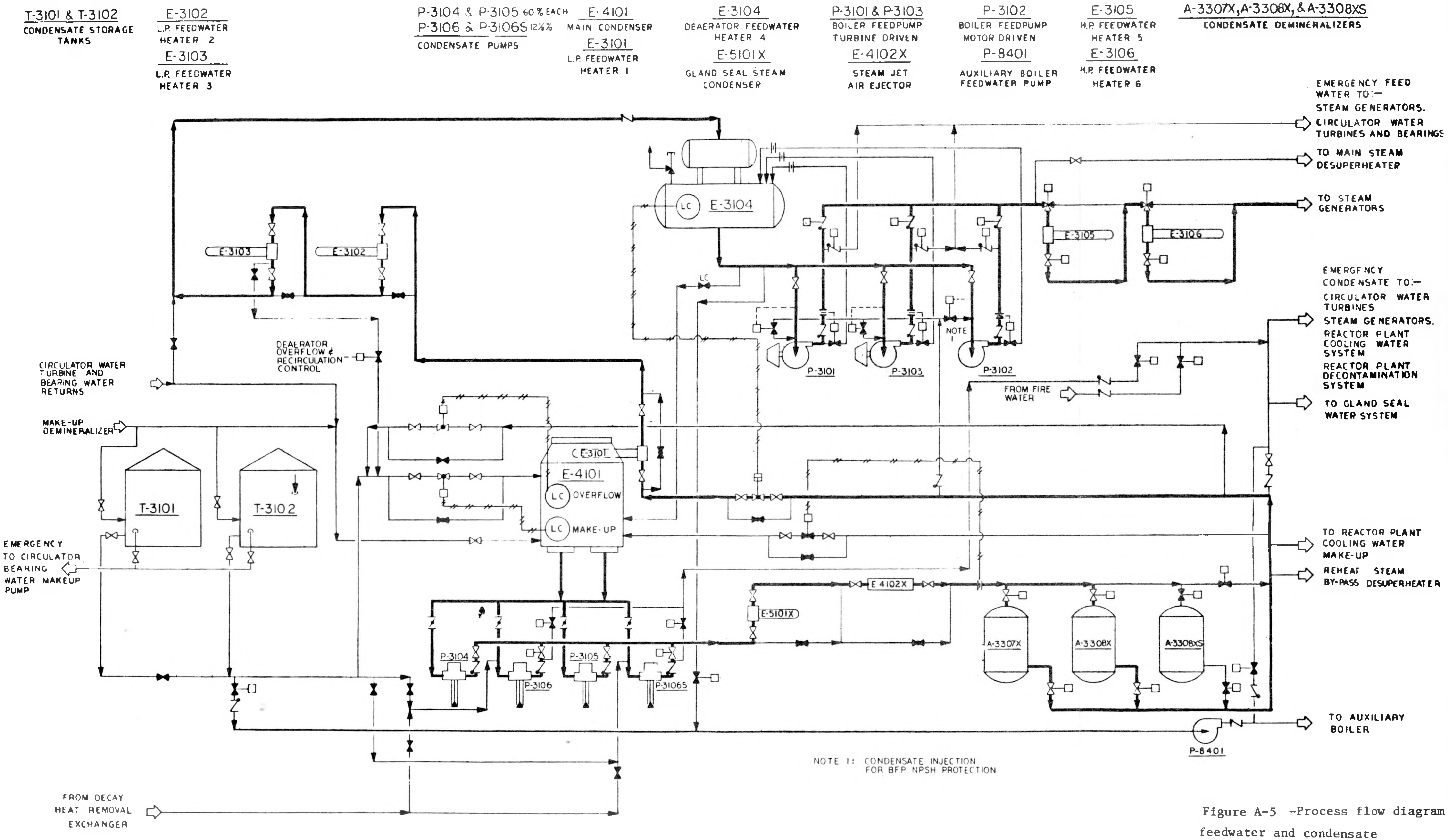

T-3101 & T-3102
CONDENSATE STORAGE TANKS
E-3102
L.P. FEEDWATER HEATER 2
E-3103
L.P. FEEDWATER HEATER 3
P-3104 & P-3105 60% EACH
P-3106 & P-3106S 12½%
CONDENSATE PUMPS
E-4101
MAIN CONDENSER
E-3101
L.P. FEEDWATER HEATER 1
E-3104
DEAERATOR FEEDWATER HEATER 4
E-5101X
GLAND SEAL STEAM CONDENSER
P-3101 & P-3103
BOILER FEEDPUMP TURBINE DRIVEN
E-4102X
STEAM JET AIR EJECTOR
P-3102
BOILER FEEDPUMP MOTOR DRIVEN
P-8401
AUXILIARY BOILER FEEDWATER PUMP
E-3105
H.P. FEEDWATER HEATER 5
E-3106
H.P. FEEDWATER HEATER 6
A-3307X, A-3308X, & A-3308XS
CONDENSATE DEMINERALIZERS
EMERGENCY FEED WATER TO:—
STEAM GENERATORS.
CIRCULATOR WATER TURBINES AND BEARINGS
TO MAIN STEAM DESUPERHEATER
TO STEAM GENERATORS
LC
E-3104
E-3103
E-3102
E-3105
E-3106
LC
DEAERATOR OVERFLOW & RECIRCULATION CONTROL
NOTE 1
P-3101
P-3103
P-3102
FROM FIRE WATER
EMERGENCY CONDENSATE TO:—
CIRCULATOR WATER TURBINES
STEAM GENERATORS.
REACTOR PLANT COOLING WATER SYSTEM
REACTOR PLANT DECONTAMINATION SYSTEM
TO GLAND SEAL WATER SYSTEM
CIRCULATOR WATER TURBINE AND BEARING WATER RETURNS
MAKE-UP DEMINERALIZER
E-3101
E-4101
LC OVERFLOW
LC MAKE-UP
T-3101
T-3102
EMERGENCY TO CIRCULATOR BEARING WATER MAKEUP PUMP
TO REACTOR PLANT COOLING WATER MAKE-UP
REHEAT STEAM BY-PASS DESUPERHEATER
E 4102X
E-5101X
A-3307X
A-3308X
A-3308XS
P-3104
P-3106
P-3105
P-3106S
TO AUXILIARY BOILER
P-8401
NOTE 1: CONDENSATE INJECTION FOR BFP NPSH PROTECTION
FROM DECAY HEAT REMOVAL EXCHANGER

Figure A-5 -Process flow diagram feedwater and condensate

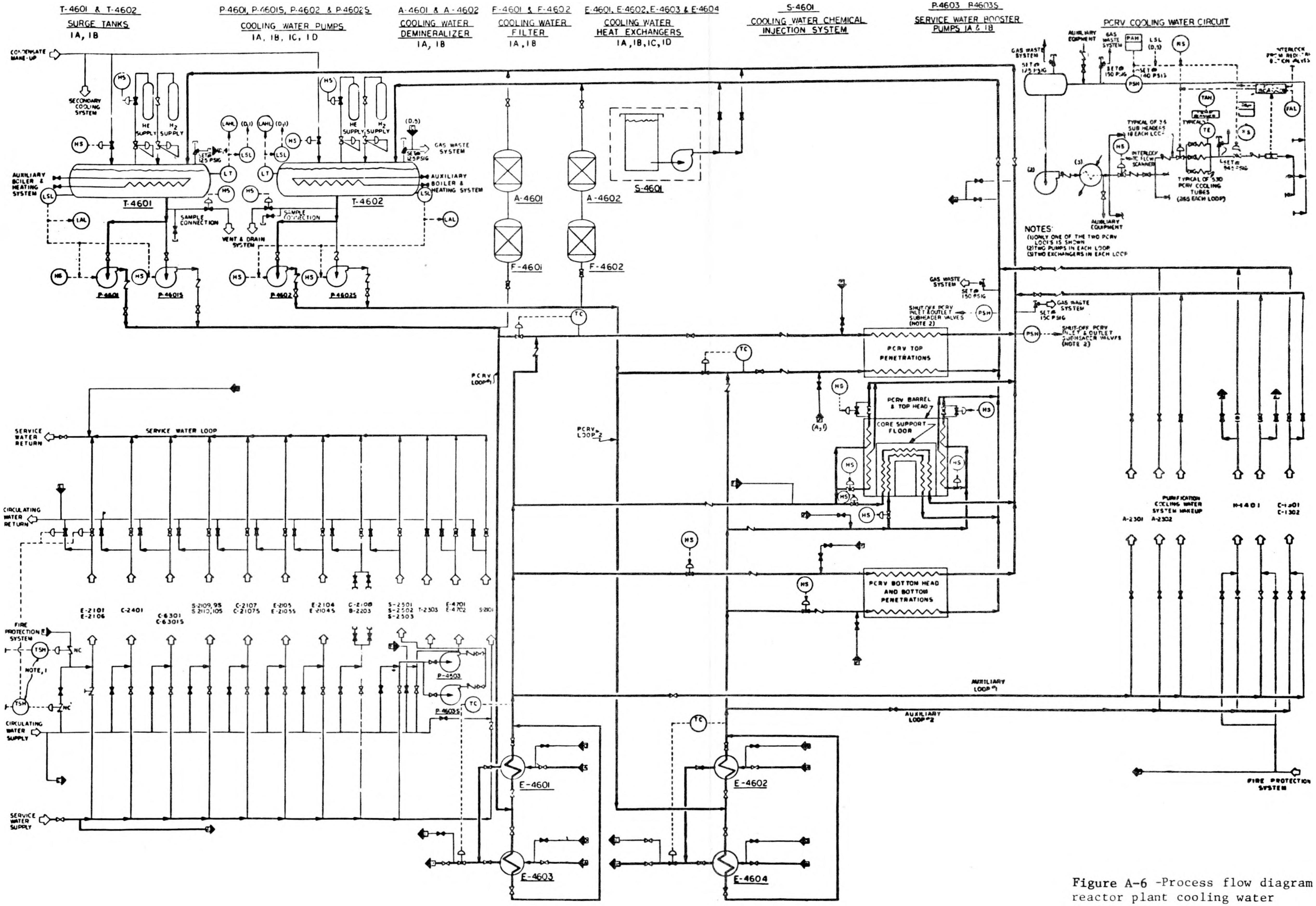


Figure A-6 -Process flow diagram reactor plant cooling water system

E-4101
Main Condenser
C-4101X to
C-4110X
Main Cooling
Tower Fans

E-4103
Main Cooling
Tower
P-4101, P-4102 } 43%
P-4103, R-4104 } 7%
Circulating
Water Pumps

C-8202
Service Air
Compressor

E-8202X
Service Air
Compressor
Aftercooler

E-4202
Decay Heat
Removal Exchanger

C-8201 & C-8201S
Instrument Air
Compressors

E-8201X & E-8201SX
Instrument Air
Compressor
Aftercoolers

K-9201 & K-9202
Standby
Generators

F-4201
Service Water
Strainer

E-4201
Service Water
Cooling Tower

P-4201, P-4202,
P-4202S
Service Water
Pumps

C-4201X& C-4202X
Service Water
Cooling Tower
Fans

T-5101X
Turbine
Lube Oil
Reservoir

E-5106X & E-5106SX
Turbine Lube
Oil Coolers

S-7537
Control Room HVAC
Water Chiller

S-7538
Turbine Bldg.
Service Area HVAC
Water Chiller

T-4201
Service Water
Return Sump

P-4203, P-4204
P-4204S
Service Water
Return Pumps

S-7306
S-7307
S-7307X
Reactor
Plant H.V.A.C.
Water Chiller

E-3107X, E-3108X,
E-3109X
BFP Lube Oil
Coolers

E-5109X
E-5109SX
EHC System
Fluid Coolers

E-5108X & E-5108SX
Generator Stator
Liquid Coolers

E-5102X to E-5105SX
Hydrogen Coolers

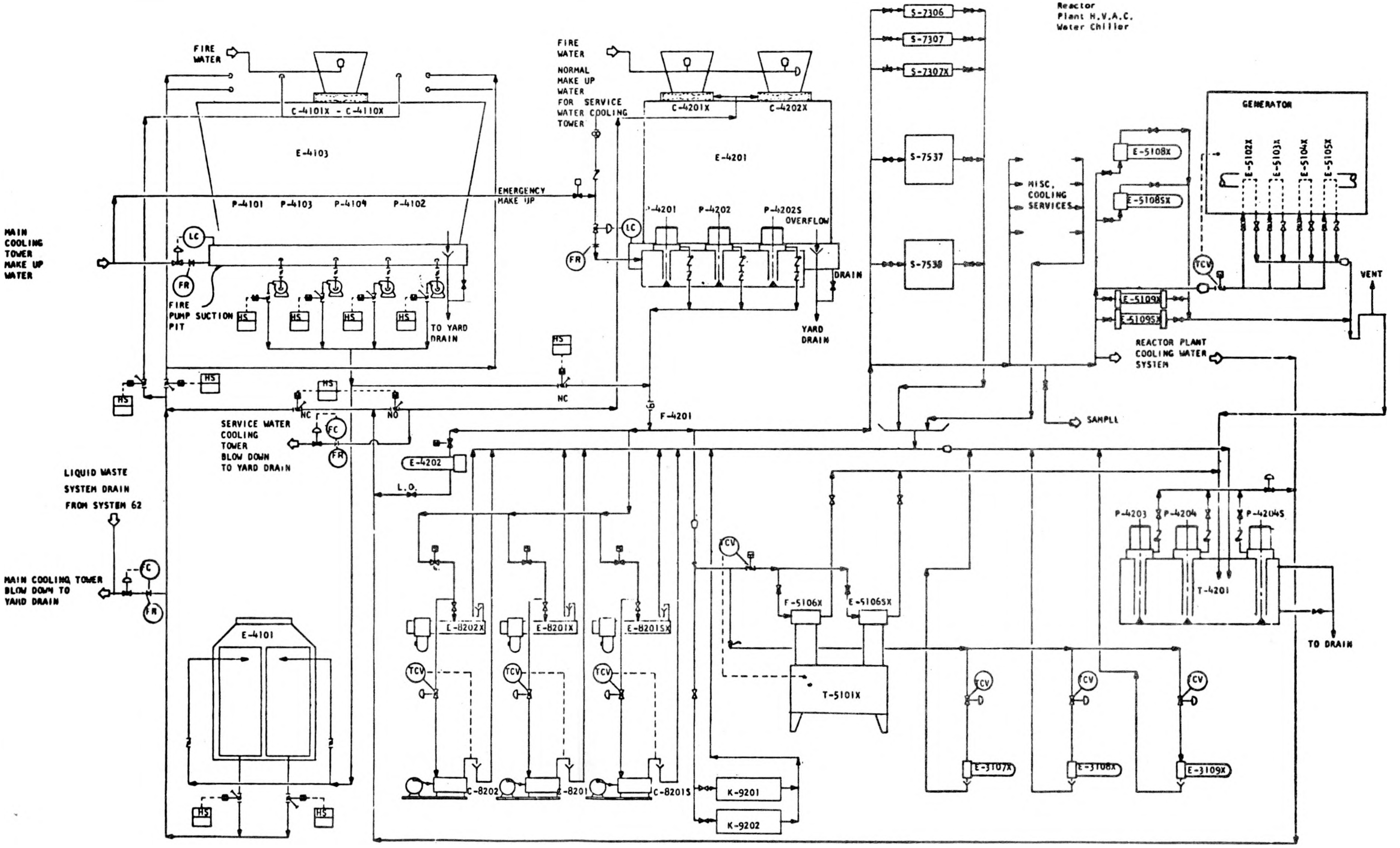
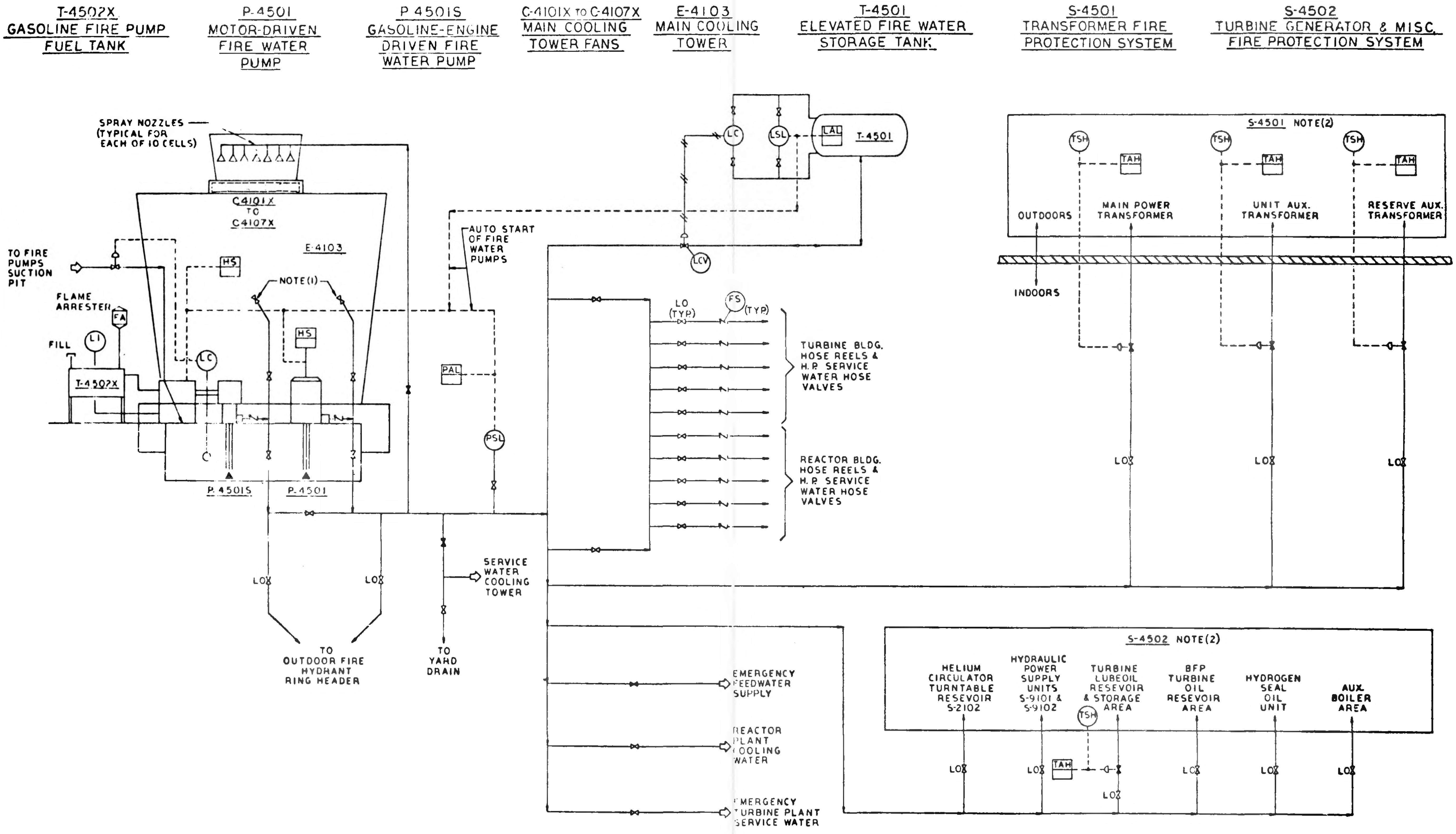


Figure A-7 -Process flow diagram
service water system


T-4502X GASOLINE FIRE PUMP FUEL TANK
P-4501 MOTOR-DRIVEN FIRE WATER PUMP
P 4501S GASOLINE-ENGINE DRIVEN FIRE WATER PUMP
C-4101X TO C-4107X MAIN COOLING TOWER FANS
E-4103 MAIN COOLING TOWER
T-4501 ELEVATED FIRE WATER STORAGE TANK
S-4501 TRANSFORMER FIRE PROTECTION SYSTEM
S-4502 TURBINE GENERATOR & MISC. FIRE PROTECTION SYSTEM
SPRAY NOZZLES (TYPICAL FOR EACH OF 10 CELLS)
C4101X TO C4107X
E-4103
TO FIRE PUMPS SUCTION PIT
FLAME ARRESTER
FA
FILL
LI
T-4502X
HS
HS
NOTE(1)
LC
P-4501S
P-4501
AUTO START OF FIRE WATER PUMPS
PAL
PSL
LC
LSL
LAL
T-4501
LCV
LO (TYP)
FS (TYP)
TURBINE BLDG. HOSE REELS & H.P. SERVICE WATER HOSE VALVES
REACTOR BLDG. HOSE REELS & H.P. SERVICE WATER HOSE VALVES
LO
LO
SERVICE WATER COOLING TOWER
TO OUTDOOR FIRE HYDRANT RING HEADER
TO YARD DRAIN
EMERGENCY FEEDWATER SUPPLY
REACTOR PLANT COOLING WATER
EMERGENCY TURBINE PLANT SERVICE WATER
S-4501 NOTE(2)
TSH
TAH
TSH
TAH
TSH
TAH
OUTDOORS
MAIN POWER TRANSFORMER
UNIT AUX. TRANSFORMER
RESERVE AUX. TRANSFORMER
INDOORS
LO
LO
LO
S-4502 NOTE(2)
HELIUM CIRCULATOR TURNTABLE RESEVOIR S-2102
HYDRAULIC POWER SUPPLY UNITS S-9101 & S-9102
TURBINE LUBEOIL RESEVOIR & STORAGE AREA
TSH
TAH
BFP TURBINE OIL RESEVOIR AREA
HYDROGEN SEAL OIL UNIT
AUX. BOILER AREA
LO
LO
LO
LO
LO
LO
LO

NOTES

(1) REPRESENTS CLUSTER OF FIVE 2½" HOSE CONNECTIONS AT EACH FIRE WATER PUMP.

(2) S-4501 & S-4502 INCLUDE FIXED WATER SPRAY NOZZLES AT LOCATION OF EQUIPMENT WHICH IS PROTECTED. ALL NOZZLES ARE AUTOMATICALLY ACTUATED.

Figure A-8 -Process flow diagram fire water system

APPENDIX B

HUMAN ERROR RATES FOR HDM-1

The first numerical column in this Appendix uses an initial error rate of 0.5 (Human Correction Factor 1.0) with lower values for later actions appropriate to the times before these actions must be taken. The other columns give lower error rates that would be appropriate for either a lower initial HER, or a time delay before the initial sequence begins. The values in Appendix B were used as inputs to the GO model to give the results shown in this report.

HUMAN ERROR RATES FOR HDM-1

OPERATOR		Time After Recognition of Accident Before Initiating Shutdown Procedure				
FUNCTION #	TASK	1 Min	5 Min	30 Min	1 Hr	14 Hr
1	Observe high activity in condensate sample	0.50	0.17	0.05	0.03	.006
2	Decide shutdown bad loop	0.50	0.17	0.05	0.03	.006
.3	Pushes correct C/T buttons (283, 87, 91, 95)	0.15	.051	0.01	.006	.0012
4	Auto. shutdown process starts	-	-	-	-	-
5	Notes increasing R/H levels	0.10	.034	0.01	.006	.0012
6	Auto. SCRAM (RHA sensors)	-	-	-	-	-
7	Decide to reverse oper. loop	0.10	.034	0.01	.006	.0012
8	Notes increasing R/A levels	0.05	.017	0.03	.006	.0012
.9	Turns correct R/H stopcheck valves (273, 77)	0.40	0.12	0.04	0.02	.0012
10	Observe act. in air ejector	0.20	.068	0.10	0.02	.004
.11	Starts faulty loop I/D tests	0.10	.034	0.02	.008	.0016
12	Decides for Power Reduction	0.10	.034	0.02	.008	.0016
13	Correct Loop Identified	0.05	.017	0.01	.004	.008
14	Power Reduced W/O Loop Shutdown	-	-	-	-	-
15	Normal Plant shutdown and restart	-	-	-	-	-

HUMAN ERROR RATES FOR HDM-1 (Continued)

OPERATOR FUNCTION #	TASK	Time After Recognition of Accident Before Initiating Shutdown Procedure 1 Min	5 Min	30 Min	1 Hr	14 Hr
16	Observe shim rod corrections needed	0.05	.017	0.01	.004	.008
.17	Adjust shim rod correctly	0.05	.017	0.01	.004	.008
18	Notes increasing Power Level	0.05	.017	0.01	.004	.008
19	Notes Power Reduced too fast	0.05	.017	0.01	.004	.008
20	Turbine Trip	-	-	-	-	-
21	Auto. SCRAM (over-flux)	-	-	-	-	-
22	Loop Shutdown Proceeds	-	-	-	-	-
23	Observes Temperature reduc. too fast	0.05	.017	0.01	.004	.008
.24	Adjust FW flow correctly	0.05	.017	0.01	.004	.008
25	Branch Path	0.50	0.50	0.50	0.50	0.50
.26	Isolates Conden. Correctly	0.05	.017	0.01	.004	.008
27	Notes abnormal air ejection activity	0.05	.017	0.01	.004	.008
28	Notes abnormal stack activity	0.05	.017	0.01	.004	.008
29	Notes abnormal steam activity	0.05	.017	0.01	.004	.008
30	Concludes Loop S/D finished	-	-	-	-	-
31	End of auto. loop S/D	-	-	-	-	-
32	Normal plant S/D initiated	-	-	-	-	-

HUMAN ERROR RATES FOR HDM-1 (Continued)

OPERATOR FUNCTION #	TASK	Time After Recognition of Accident Before Initiating Shutdown Procedure 1 Min	5 Min	30 Min	1 Hr	14 Hr
33	R/H stopcheck* (VNO) fails to close	.001	.001	.001	.001	.001
.34	Notes and corrects manual adj. (CMA)	0.10	.034	0.02	.008	.0016
35	Rad sample valve (VNO) fails	.001	.001	.001	.001	.001
.36	(CMA)	0.10	.034	0.02	.008	.0016
37	F/W Control valve (VNO) fails	.001	.001	.001	.001	.001
.38	(CMA)	0.10	.034	0.02	.008	.0016
39	F/W Stop/Check valve (VNO) fails	.001	.001	.001	.001	.001
.40	(CMA)	0.10	.034	0.02	.008	.0016
41	Circ. Bypass BLK Valve (VNO) fails	.001	.001	.001	.001	.001
.42	(CMA)	0.10	.034	0.02	.008	.0016
43	Turbine Load Reduct. incorrect	.005	.005	.005	.005	.005
.44	(CMA)	0.10	.034	0.02	.008	.0016
45	Flux control abnormal	.005	.005	.005	.005	.005
46						
47	F/W Flow valve fails (VNO)	.001	.001	.001	.001	.001
.48	(CMA)	0.10	.034	0.02	.008	.0016
49	Notes time to reach 50%	0.10	.034	0.02	.008	.0016
50	Circ. Steam speed valve (VNO) fails	.001	.001	.001	.001	.001

HUMAN ERROR RATES FOR HDM-1 (Continued)

OPERATOR FUNCTION #	TASK	Time After Recognition of Accident Before Initiating Shutdown Procedure 1 Min	5 Min	30 Min	1 Hr	14 Hr
.51	(CMA)	0.10	.034	0.02	.008	.0016
52	Steam Outlet Trip Valve (VNO) fails	.001	.001	.001	.001	.001
.53	(CMA)	0.10	.034	0.02	.008	.0016
54	W/T outlet trip valve (VNO) fails	.001	.001	.001	.001	.001
.55	(CMA)	0.10	.034	0.02	.008	.0016
56	R/H attemp. Line valve (VNO) fails	.001	.001	.001	.001	.001
.57	(CMA)	0.10	.034	0.02	.008	.0016
58	R/H Attempt. F/W BLK valve (VNO) fails	.001	.001	.001	.001	.001
.59	(CMA)	0.10	0.34	0.02	.008	.0016
60	Temp. Reduct. Abnorm.	.001	.001	.001	.001	.001
61	Prob. Cond. Vacuum Incorrect	0.02	.0173	.004	.001	.0002
62	Prob. Stack Activ. Hi	0.01	.0116	0.02	0.05	0.10
63	Prob. Air Eject. Activ. Hi	0.01	.0116	0.02	0.05	0.10
64	Prob. Prim. Coolant Activ. Hi	0.01	.0116	0.02	0.05	0.10
67	Branch Path	.80	.80	.80	.80	.80

VNO = Valve Norm. Open
CMA = Notes Failure and Correctly Adjusts

· Tasks which require operation action or Interface with Plant Safe Shutdown Model)

APPENDIX C

GENERAL HUMAN ERROR RATES

TABLE C-1

GENERAL HUMAN ERROR RATE ESTIMATES*

Item	Conditional Error Rates (Estimates)	Activity
1.	10^{-4}	Selection of a key-operated switch rather than a non-key switch (this value does not include the error of decision where the operator misinterprets situation and believes key switch is correct choice).
2.	10^{-3}	Selection of a switch (or pair of switches) dissimilar in shape or location to the desired switch (or pair of switches), assuming no decision error. For example, operator actuates large handled switch rather than small switch.
3.	$3x10^{-3}$	General human error of commission, e.g., misreading label and therefore selecting wrong switch.
4.	10^{-2}	General human error of omission when there is no display in the control room of the status of the item omitted, e.g., failure to return manually operated test valve to proper configuration after maintenance.
5.	$3x10^{-3}$	Errors of omission, where the items being omitted are embedded in a procedure rather than at the end as above.
6.	$3x10^{-2}$	Simple arithmetic errors with self-checking but without repeating the calculation by redoing it on another piece of paper.
7.	1/N	Given that an operator is reaching for an incorrect switch (or pair of switches), he selects a particular similar appearing switch (or pair of switches), where N = the number of incorrect switches (or pairs of switches) adjacent to the desired switch (or pairs of switches). The 1/N applies up to 5 or 6 items.

*See Reference 5

TABLE C-1 (Continued)

Item	Conditional Error Rates (Estimates)	Activity
		After that point, the error rate would be lower because the operator would take more time to search. With up to 5 or 6 items he doesn't expect to be wrong and therefore is more likely to do less deliberate searching.
8.	10^{-1}	Given that an operator is reaching for a wrong motor operated valve MOV switch (or pair of switches), he fails to note from the indicator lamps that the MOV(s) is (are) already in the desired state and merely changes the status of the MOV(s) without recognizing he had selected the wrong switch(es).
9.	-1.0	Same as above, except that the state(s) of the incorrect switch(es) is (are) not the desired state.
10.	~1.0	If an operator fails to operate correctly one of two closely coupled valves or switches in a procedural step, he also fails to correctly operate the other valve.
11.	10^{-1}	Monitor or inspector fails to recognize initial error by operator. Note: With continuing feedback of the error on the annunciator panel, this high error rate would not apply.
12.	10^{-1}	Personnel on different work shifts fail to check conditions of hardware unless required by check list or written directive.
13.	$5x10^{-1}$	Monitor fails to detect undesired position of valves, etc., during general walk-around inspections, assuming no check list is used.
14.	.2 - .3	General error rate given very high stress levels where dangerous activities are occurring rapidly.

TABLE C-1 (Continued)

Item	Conditional Error Rates (Estimate)	Activity
15.	$2^{(n-1)}x$	Given severe time stress, as in trying to compensate for an error made in an emergency situation, the initial error rate, x, for an activity doubles for each attempt, n, after a previous incorrect attempt, until the limiting condition of an error rate of 1.0 is reached or until time runs out. This limiting condition corresponds to an individual's becoming completely disorganized or ineffective.
16.	x_1x_2	If the first operator reviews each anticipated action with a second operator and the second operator monitors the subsequent actions performed by the first operator, their combined probability of error can be considered to be the joint product of their individual erros, "$x_1^{\cdot}+x_2^{\cdot}$".

	Incident Error Rates (Estimate)	Activity
17.	~1.0	Operator fails to act correctly in the first 60 seconds after the onset of an extremely high stress condition, e.g., a large LOCA.
18.	$9x10^{-1}$	Operator fails to act correctly after the first 5 minutes after the onset of an extremely high stress condition.
19.	10^{-1}	Operator fails to act correctly after the first 30 minutes in an extreme stress condition.
20.	10^{-2}	Operator fails to act correctly after the first several hours in a high stress condition.
21.	x	After 7 days after a large LOCA, there is a complete recovery to the normal error rate, x, for any task.

NOTE 1: Modification of these underlying (basic) probabilities were made on the basis of individual factors pertaining to the tasks evaluated.

NOTE 2: Unless otherwise indicated, estimates of error rates assume no undue time pressures or stresses related to accidents.

APPENDIX D

GLOSSARY FOR SSM-1

APPENDIX D

GLOSSARY FOR ACRONYMS USED IN PLANT SAFE SHUTDOWN MODEL-1 (Figure 5)

ABF	Auxiliary Boiler Feedline
AFC	Auto Flux Controller (Plant)
AS/D	Automatic Shutdown
ATT	Attemperator
Aux	Auxiliary
BP	Boiler Pump
BPF	Boiler Pump Feed
BPV	Bypass valve
BWA	Bearing Water Accumulator
BWL	Bearing Water Line
BWMP	Bearing Water Makeup Pump
CBV	Circulator Bypass Valve
CCV	Condenser Control Valve
CP	Condensate Pump
CPF	Condensate Pump Feedline
CSSV	Circulator Steam Speed Valve
CST	Condenser Storage Tanks
CSTV	Circulator Steam Trip Valve
CSV	Condenser Sample Valve
CWP	Circulating Water Pump
DCB	DC Battery
DG	Diesel Generator
DT	Turbine Water Drain Tank
EB	Essential Electrical Bus
EC	Emergency condensate
ECL	Emergency Condensate Line
FP	Firewater Pump
FST	Diesel Fuel Storage Tank and Lines
FWC	Feedwater Control Valve
FWF	Firewater Feed Line
FWSC	Feedwater Stopcheck Valve
H/C	Helium Circulator
HI	Human Interface
HS	Handswitch
Hydra	Hydraulic valve system
IAC	Instrument Air Compressor
INST	Instrument
MAN	Manual
M/C	Manual (Plant) Control
MCD	Main Condenser

APPENDIX D

GLOSSARY FOR ACRONYMS USED IN PLANT SAFE SHUTDOWN MODEL-1 (Figure 5) (Continued)

MCT	Main Cooling Tower
MCTF	Main Cooling Tower Fan
MF	Main Feed Line
MRC	Manual Rod Control
NPR	Normal Power Reduction
RAB	Reheat Attemperator Feedwater Block Valve
RAL	Reheat Attemperator Line Valve
RPCS	Reactor Plant Cooling System
RSC	Reheater Steam Controller (Plant)
SAC	Service Air Compressor
SCM	SCRAM
SS	Superheater (Steam Generator)
SWP	Service Water Pump
SWS	Service Water Supply Line (piping)
T/D	Time Delay
TG	Turbine Generator
TLR	Turbine Load Reduction
TWP	Turbine Water Removal Pumps
W/L	Wrong Loop
WTT	Water Turbine Trip Valve

APPENDIX E

SCRAM SYSTEM DESCRIPTION

APPENDIX E

SCRAM PROTECTIVE SYSTEM DESCRIPTION

In the Fort St. Vrain HTGR design, a number of subsystems normally used for reactor operations and monitoring are also involved in reactor shutdown. Thus, the SCRAM system includes not only stand-by protective system circuitry, but also substantial portions of the plant operating system. The reactor shutdown system will attempt to perform its function in spite of the failure of any single channel or component. Some of the features designed into the system to aid in achieving this kind of performance involve: two-out-of-three coincidence between sensors, one-out-of-two logic systems, generalized two-out-of-three relay matrix coincidence in the SCRAM brake circuits, and a First-In-With-Lockout (FILO) system for shutdown of either one of two cooling loops. Each of the two coolant loops contain two helium circulators. There are ten different kinds of trouble sensors that will act to trip the circulators if trouble is detected. The circulator trip function is one of seven major parameters which serve to protect the two loop coolant system. Most of the trouble sensors in the two loop system are redundant and are arranged in a local two-out-of-three coincidence to initiate trip or loop shutdown actions. Signals from each loop are then combined in the final output circuit to request SCRAM action whenever trouble is detected in both loops. Trouble in one loop only will usually result in single loop shutdown.

Two loop SCRAM requests coming from any of the seven major inputs are routed through the Two Loop Trouble (TLT) circuits to the Main SCRAM Logic. The TLT input is one of 12 SCRAM parameters which operate in the Main SCRAM Logic. Since a single transmission logic circuit for the TLT system would not satisfy 'single failure criteria,' dual logic circuits are used in each loop to provide positive SCRAM requests.

All inputs to the main SCRAM gate are independent except for (1) the two Nuclear STartup Channels (SUC), and (2) the Two Loop Trouble (TLT) inputs to main SCRAM.

The twelve main SCRAM parameters are as follows:

1. Super-Heat Header Low Pressure
2. Reheat Header Low Pressure
3. Wide Range Flux Rate Change (Period)
4. Reactor Pressure High (Programmed by Core Inlet Temperature)
5. Reactor Pressure Low (Programmed by Core Inlet Temperature)
6. Reheat Steam Temperature
7. Reactor Building Temperature
8. Switch Gear Undervoltage Switch
9. Nuclear Startup Channels
10. Wide Range Flux Level (Power)
11. Linear Range Flux Level (Power)
12. Two Loop Trouble Inputs.

In addition to the twelve main SCRAM inputs defined above, there are two independent manual SCRAM trip circuits and an Emergency Shutdown System consisting of hoppers of Boron balls, which can be dropped into the core with the purpose of making the reactor subcritical.

Whenever trouble develops in one of the two primary coolant loops, the faulty loop is shut down and the plant can be operated on a single coolant loop as long as one of the circulators in the shutdown loop is still operable. If trouble should develop in the second loop an immediate SCRAM is initiated and a second loop shutdown is inhibited. These SCRAM inputs constitute the Two Loop Trouble input parameters for the SCRAM Protective System.

There are seven possible SCRAM inputs feeding the Two Loop Trouble monitoring circuits. They are as follows:

1. Circulator Trip
2. Reheat Header Activity
3. Steam Generator Penetration Overpressure
4. Moisture Monitor and Detection
5. Steam Pipe Rupture
6. Reactor Pressure, Low
7. Superheat Header Temperature, Low

The helium circulators can be tripped by ten possible operational malfunctions. The items which can contribute to a trip condition are as follows:

1. Circulator Penetration Pressure
2. Circulator Overspeed Trip
3. Circulator Speed Trip, Low (Programmed with Feedwater Flow)
4. Circulator Manual Trips
5. Programmed Feedwater Flow, Low (Programmed with Circulator Speed)
6. Reheat Header Activity
7. Loss of Bearing Water
8. Circulator Seal Malfunction
9. Fixed Feedwater Flow Trip, Low
10. Circulator Drain Malfunction

Each of the parameters enumerated above are monitored and tested on a regular schedule. Most, but not all, of the parameters are monitored and logged on a daily basis. The operation of the SCRAM/Trip circuits are tested, usually on a monthly basis.