

PDR copy

MAR 19 1993

MEMORANDUM TO: Louis M. Shotkin, Chief
Reactor and Plant Systems Branch
Division of Systems Research

THRU: Ralph O. Meyer, Section Leader
Reactor and Plant Systems Branch
Division of Systems Research

FROM: Andrew J. Szukiewicz
Reactor and Plant Systems Branch
Division of Systems Research

SUBJECT: SUMMARY OF MEETING WITH ORNL ON CANDU 3 SYSTEMS
RESEARCH (FIN #2015)

A public meeting was held in the Nicholson Lane Building/South, Rockville, with Oak Ridge National Laboratory (ORNL), the NRC staff, AECL-CANDU, and AECL Technologies on February 10, 1993. The purpose of the meeting was to: 1) have ORNL present a summary of the CANDU systems research findings and insights that were developed as a result of the ORNL study, 2) solicit comments, and 3) obtain additional information from AECL and AECL Technologies in a number of different areas of the plant design. A List of attendees is attached. Copies of the view graphs are available on request. Highlights of the meeting are summarized below.

Mark Linn, Jeff Wolfgang, and Anthony Wright of ORNL summarized the CANDU 3 review activities and described the methodology and the selection criteria used to categorize the important initiating event sequences into Abnormal Operating Occurrences (AOOs), Design Basis Accidents (DBAs), Severe Accidents (SAs) and into events having residual risk. ORNL also presented their conclusions and insights regarding the plant design, described important event sequences and failure modes, and identified additional analysis and information that might be needed for future reviews.

Following the ORNL presentation and discussions, Mike Fletcher (AECL Technologies) described the CANDU 3 philosophy regarding Safety-Related and Non-Safety-Related systems and how they are implemented in their Group 1 and Group 2 classification. It was pointed out that although Group 2 contains only safety-related equipment, Group 1 also contains some safety-related equipment.

A.C. Wright and D. Pendergast from AECL-CANDU completed the prepared presentations with a discussion on the Crash Cooling system, the

PL-13

9304050199 930319
PDR PROJ
679 A

RETURN TO REGULATORY CENTRAL FILES

PDR

111
x Proj #679

MAR 19 1993

2

Emergency Core Cooling system and, the Safe Shutdown system. Comments from AECL and AECL Technologies and follow-up action items are described below:

1. AECL indicated that the ORNL estimated value of 10^{-3} for the event probability of back flow in the ECCS is high. AECL estimates 10^{-6} for this event. This estimate is based on the failure of three separate and independent valves. AECL stated that the TTR-409 report describes the design and identifies the three valves. ORNL agreed to re-evaluate their estimates and amend their report as necessary.
2. AECL-Technologies stated that the ECCS logic has been changed, but the new design has not yet been submitted to the NRC. The system has been modified to allow the ECCS to refill the core much faster during a LBLOCA. The heat removal function of the Heat Transfer System (HTS) is a qualified system. A revised Technical Description document will provide the details on the new HTS. This document has not yet been submitted to the NRC.
3. The MSSVs and the Liquid Relief Valves (LRV) are classified as category Group 2 systems.
4. ORNL was requested to use the term "failure to shutdown" instead of the term ATWS in the event sequence diagrams.
5. AECL-Technologies stated that a loss of power may require two (2) system failures instead of one (1) as was assumed by ORNL. M. Fletcher agreed to provide a DC power supply diagram which would identify inter-system dependencies.
6. AECL-Technologies stated that during a Loss of Feedwater event (i.e., break in the Reactor Building) the shutdown control system would not be available because it is not currently qualified for accident environment conditions. AECL is currently re-evaluating this design. The auxiliary feedwater system will be available for this type of event. AECL-Technologies indicated that on a loss of feedwater, if SDS1 or SDS2 is not available, timely operator action is very important. AECL stated that the SDS2 system is a faster shutdown system than SDS1. L.Rib (AECL-Technologies) agreed to provide the design schematic showing the SDS2 helium line vent valves.
7. AECL-Technologies stated that in general operator action for the CANDU 3 design is not needed for at least 10 hours, except: 1) during a steam generator tube failure when the operator needs to initiate shutdown cooling and isolate the steam generator and, 2) when the operator is needed to stop feedwater flow in the broken line to minimize flow between the steam generator and the check valve.
8. Additional information requests and AECL responses [in brackets] discussed after the meeting adjourned are summarized below:

- a) AECL was requested to provide information regarding the mechanical configuration of barriers that prevent backflow to the ECCS. [Refer to Fig. 2-3.12-8, "Emergency Core Cooling System"]
- b) AECL was requested to provide additional information regarding the need for HTS to function during A LBLOCA to accomplish rapid refill. [Refer to Pt. Lapreau LBLOCA and Loss of Power analysis].
- c) AECL was requested to provide documentation regarding the new conditioning signal logic for the ECCS. [Provided in the viewgraphs in the meeting].
- d) AECL was requested to provide a reference document which documents the fact that the MSSV's on each steam generator are Group 2 category components. [AECL will respond in a letter].
- e) AECL was requested to define shutdown requirements for SDS1. What conditions or events required both banks of rods and what events require only 1 of the 2 banks to provide sufficient shutdown margin. [This is an open issue pending the completion of AECL analysis].
- f) For loss of class IV power, what parameters cause automatic initiation of the reactor regulating system (RRS). [AECL will respond in a letter].
- g) AECL was requested to provide a reference that documents that condenser steam discharge valves are required to have class IV power. [AECL will respond in a letter].
- h) AECL was requested to provide additional information regarding qualification of the shutdown cooling system. [AECL will respond in a letter].
- i) AECL was requested to provide documentation that shows that the D₂O system is not required to maintain zero power hot shutdown conditions. [AECL will respond in a letter].
- j) AECL was requested to provide more information on the hardware configuration and support systems (e.g., power supplies) for crash cooling - and provide clarification between the ECCS and SDS2 signals.
- k) AECL was requested to provide information on the SDS1 trip logic (in sufficient detail to show the relay configuration). [AECL will respond in a letter].
- l) AECL was requested to provide information on the clutch control modules. [AECL will respond in a letter].

MAR 19 1993

4

- m) AECL was requested to submit the new documentation on the new design for the HTS. [AECL will determine if the new design information can be provided at this time].
- n) In a previous meeting AECL indicated that there was some inter-dependence between SDS1 and SDS2 power supplies. AECL was requested to identify these dependencies. [AECL will determine if the information can be provided at this time].
- o) AECL was requested to provide information on the vent valves for SDS2 and ECCS accumulator tanks. [AECL will determine if this information can be provided at this time]

5
Andrew J. Szukiewicz
Reactor and Plant Systems Branch
Division of Systems Research

Attachment:
As stated

Distribution:
RES Circ/Chron
DSR Chron
PDR
RPSB r/f
ASzukiewicz r/f
ASzukiewicz
ROMeyer
LMShotkin
TLKing
BWSheron
Attendees
a:\shotkin.mem\AS

RPSB/DSR *AS*
ASzukiewicz/clc
3/19/93

LS/rm
RPSB/DSR
ROMeyer
3/19/93

LS
RPSB/DSR
LMShotkin
3/19/93

ATTACHMENT 1

LIST OF ATTENDEES
FEBRUARY 10, 1993RES

Zoltan Rosztoczy (DSR)	301/492-3768
Farouk Eltawila (AEB)	301/492-3525
Ralph Meyer (RPSB)	301/492-3732
Andrew Szukiewicz (RPSB)	301/492-3736
John Lane (RPSB)	301/492-3985
David Ebert (RPSB)	301/492-3804
Don Carlson (RPSB)	301/492-0013

NRR

Bob Pierson (PDAR)	301/504-1111
Tom Cox (PDAR)	301/504-1109
Janet Kennedy (PDAR)	301/504-1140
Jack Donohew (PDAR)	301/504-3128
Edward Throm (PDAR)	301/504-3153
Joe Donoghue (PDAR)	301/504-1131

ORNL

Anthony Wright	615/574-6878
Mark Linn	615/574-4617
Jeff Wolfgang	615/574-2056
Wolfgang Barthold	615/690-1237
(Consultant-Barthold Associates)	

AECL TECHNOLOGIES

Mike Fletcher	301/417-0047
Louis Rib	301/417-0047
Robert Ferguson	301/417-0047

AECL CANADA

A.C.D. Wright	416/823-9040
D.R. Pendergast	416/823-9040 (X-4582)
Scott Grant	416/823-9040

AECB

A.M. Morlada Aly	613/995-2983
John Tong	613/995-2983

INEL

W. Arcieri	301/816-7782
Rex Shumway	208/526-9571
Jerry Judd	208/526-7633

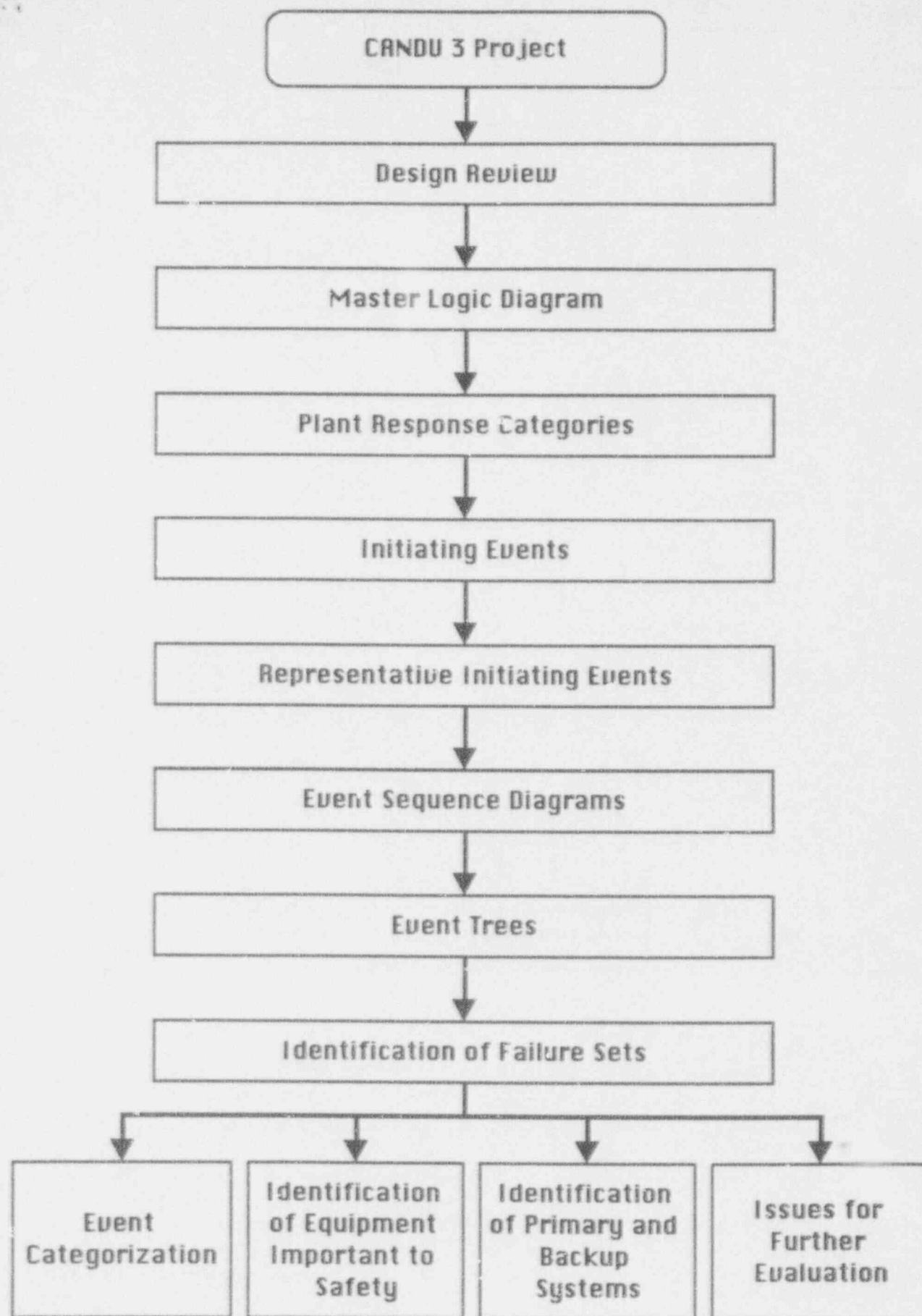
MARK LINN

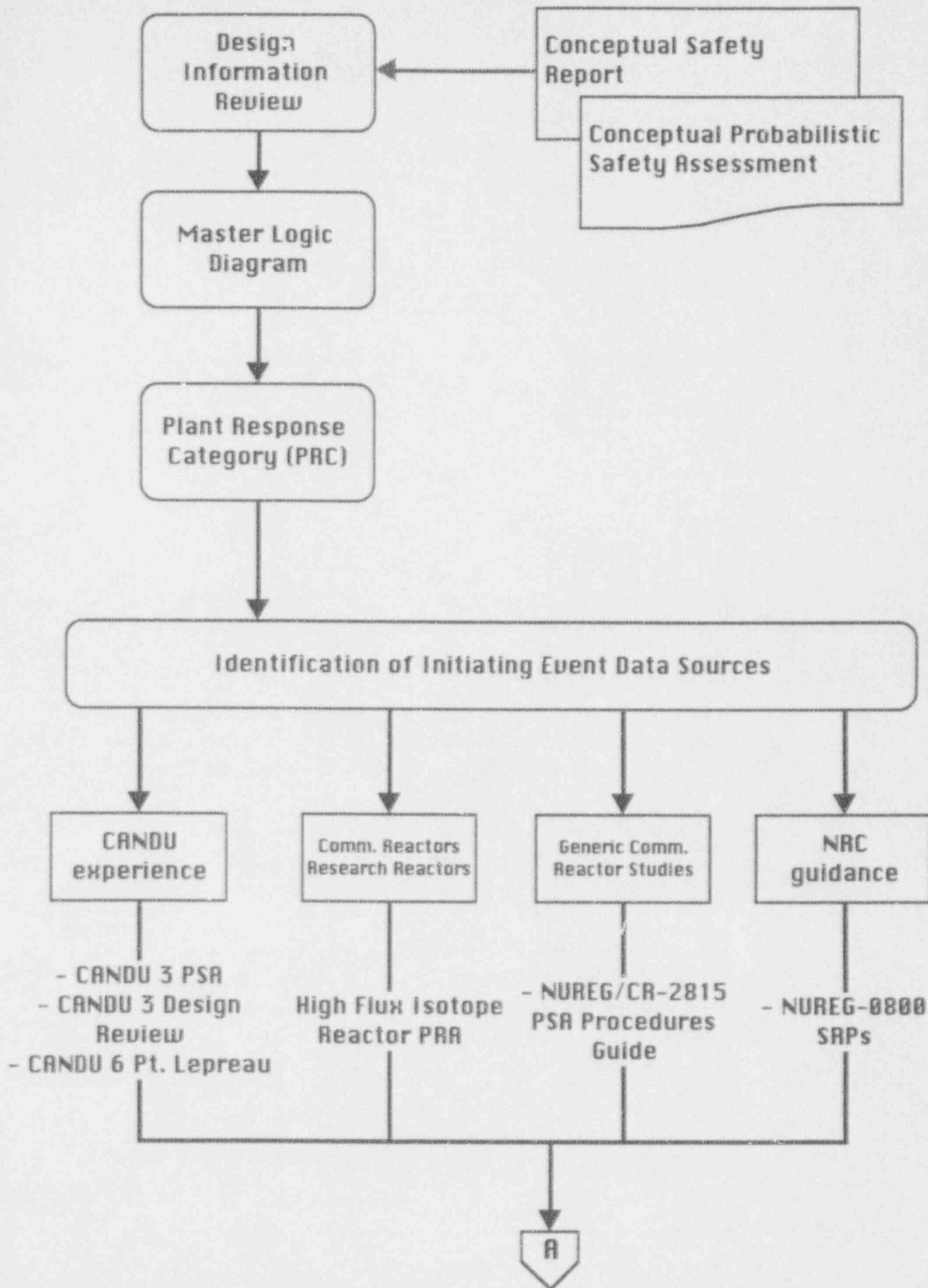
CANDU Systems Research Program
Oak Ridge National Laboratory

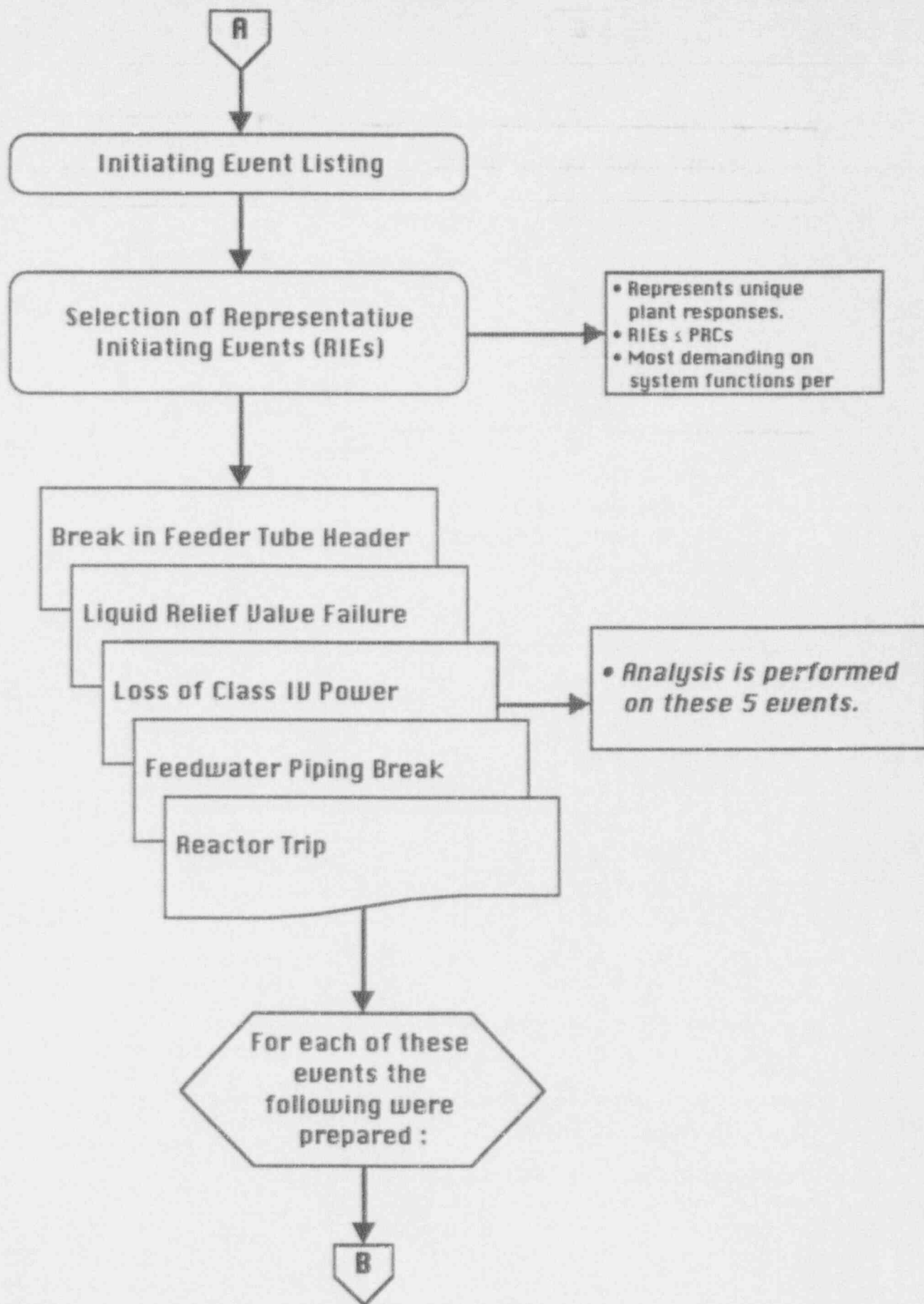
**OVERVIEW OF
CANDU SYSTEMS ANALYSIS EFFORT**

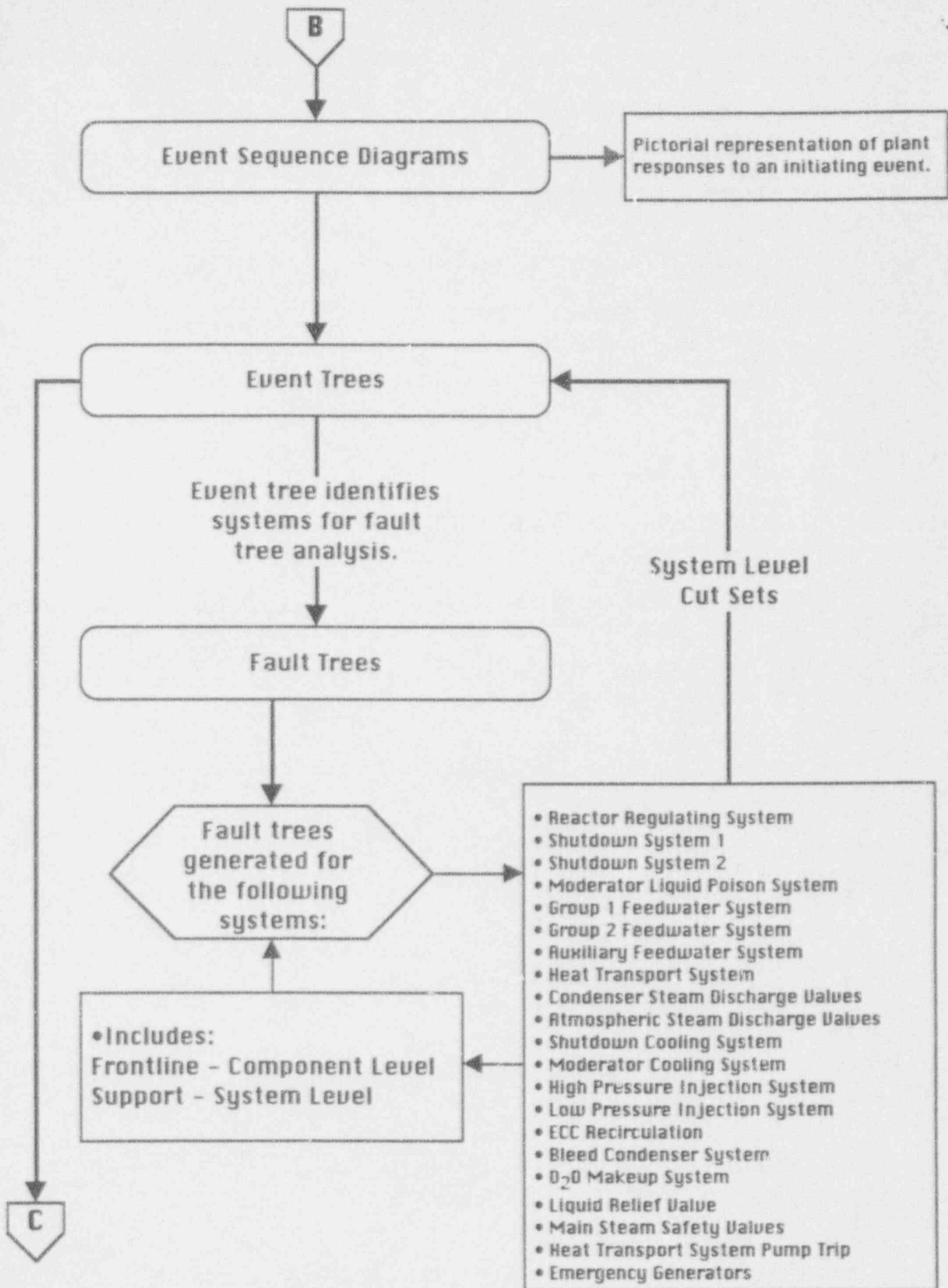
Presented to the NRC/AECL Review Meeting
Systems Analysis of the CANDU 3 Reactor

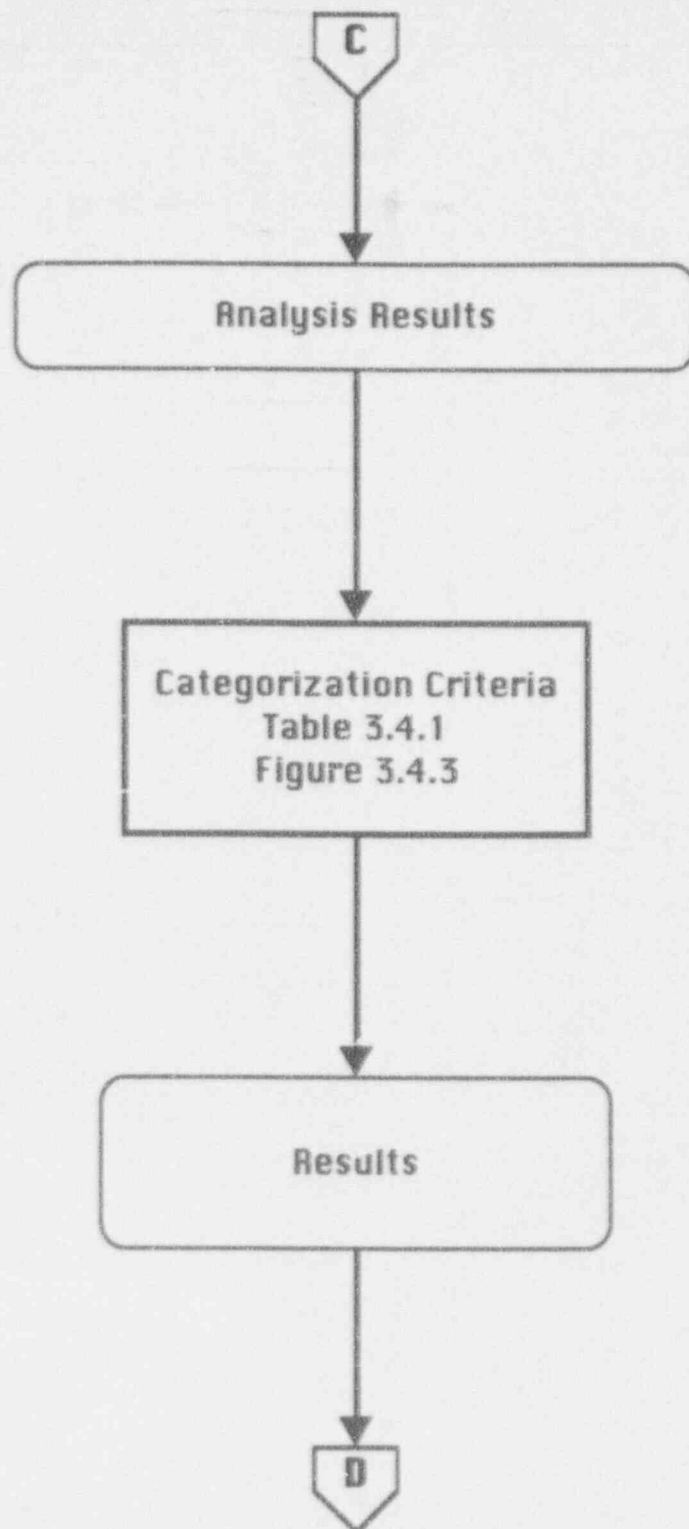
February 10, 1993

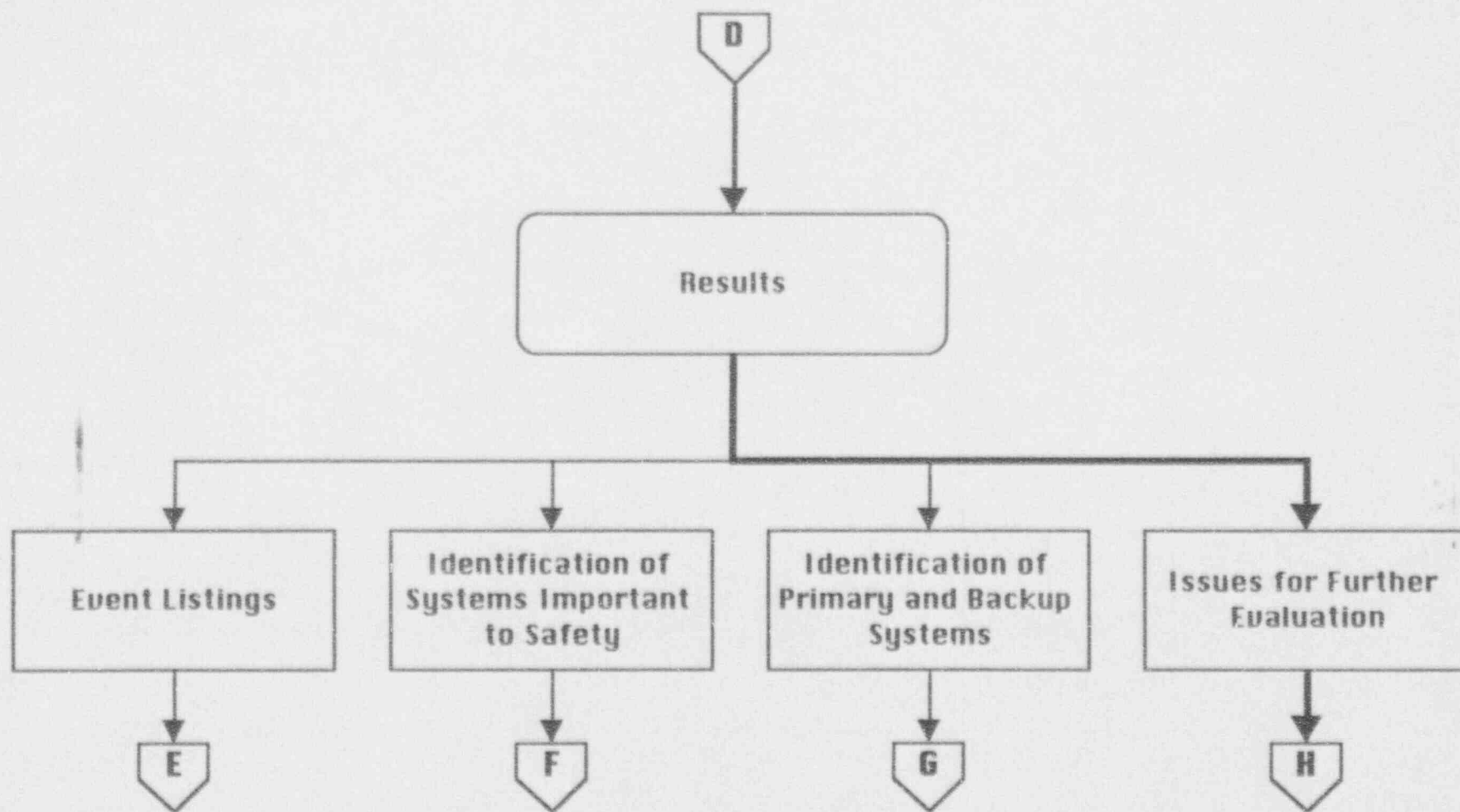


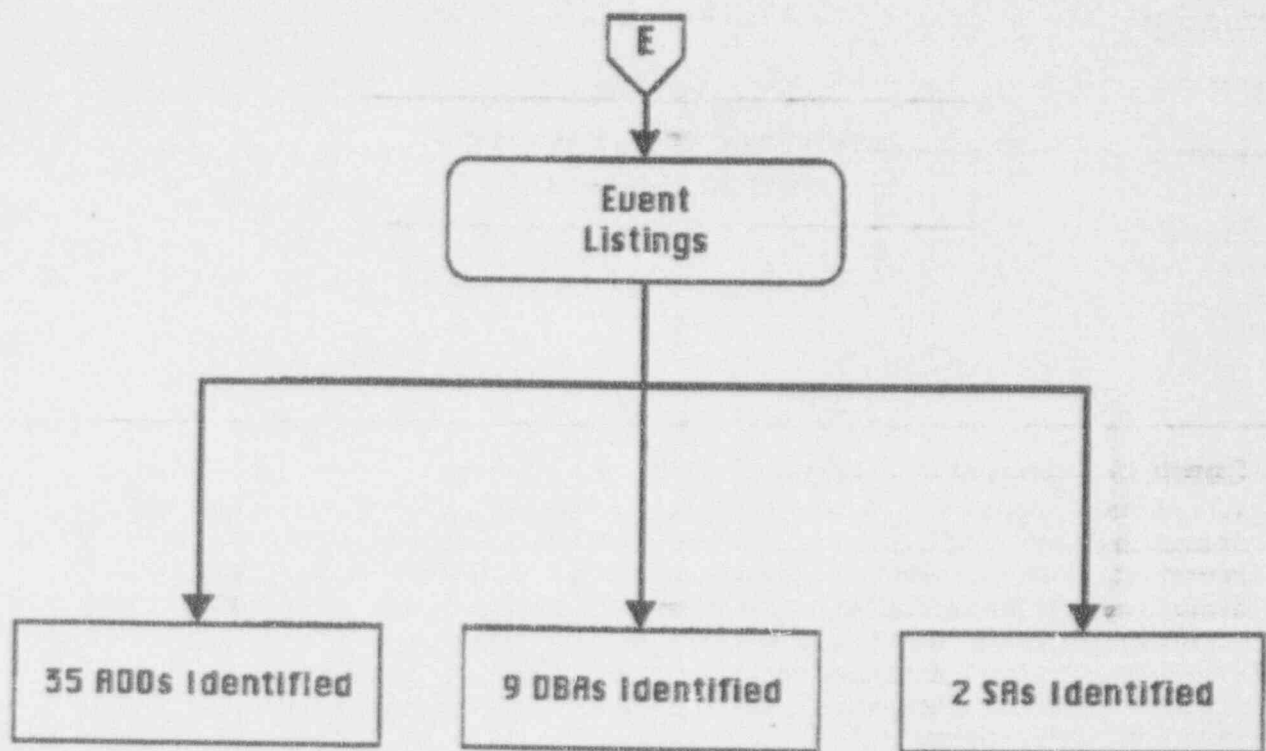














Identification of Systems Important-to-Safety

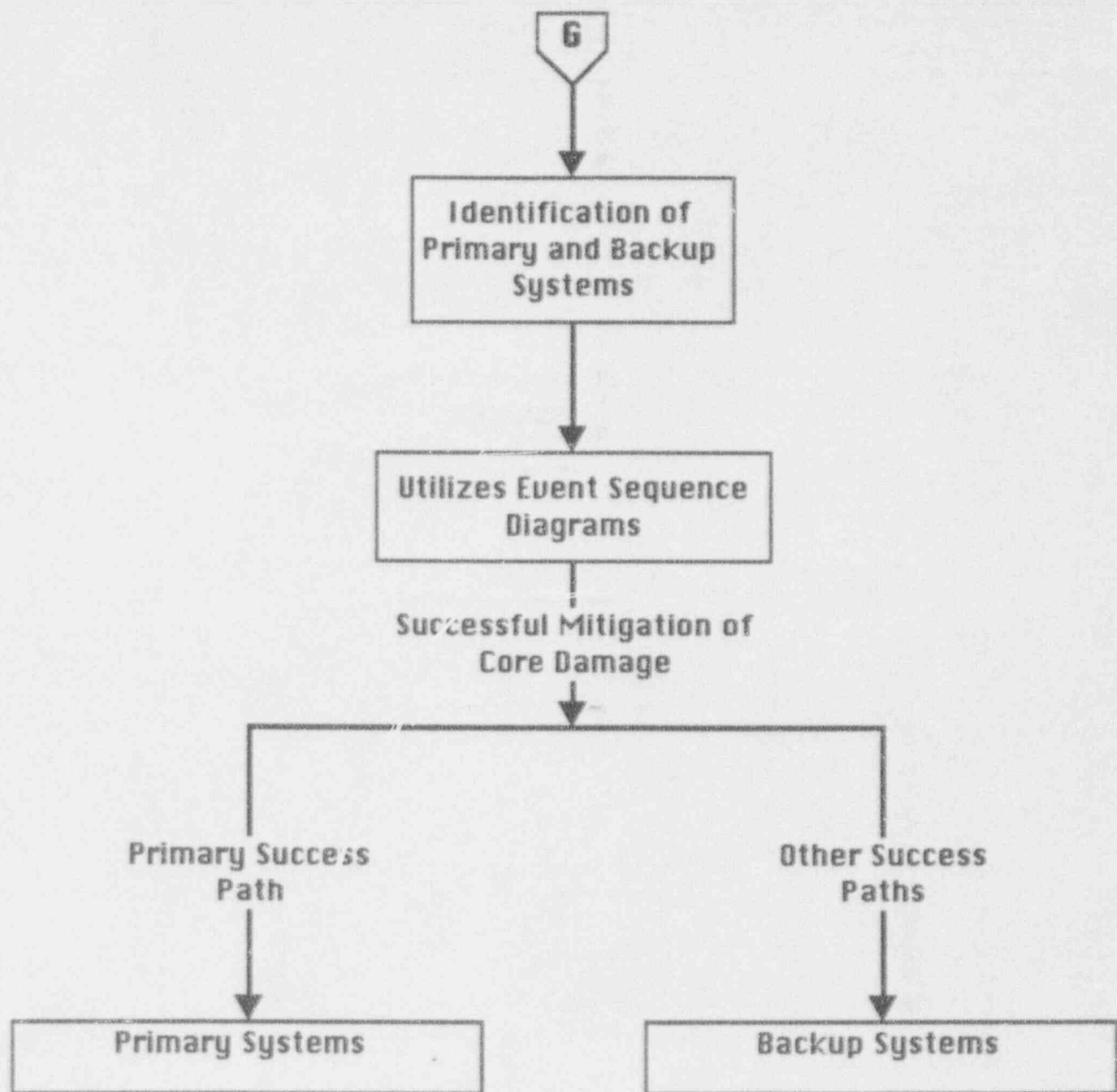
Candidate Systems Criteria:

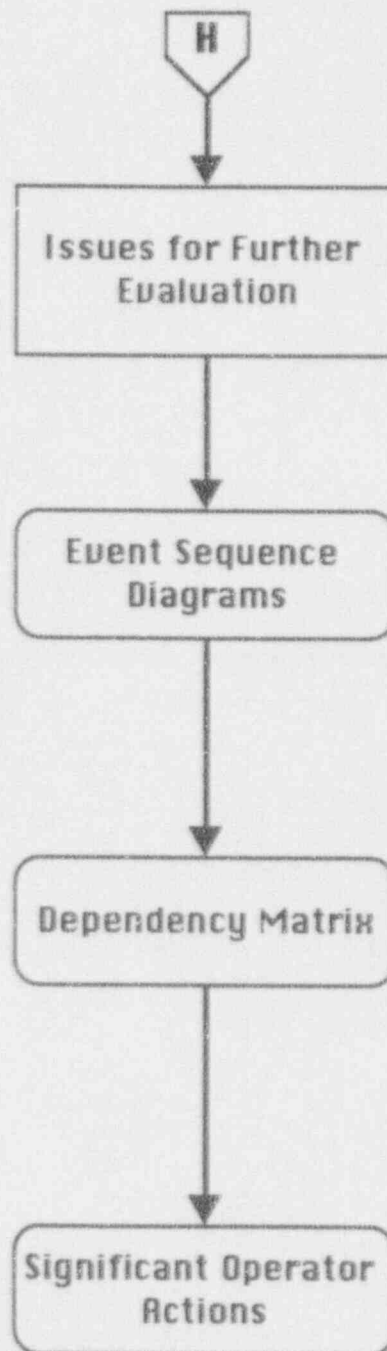
1. Only those systems or components that contribute to successful termination (primary or backup path) of an initiating event are considered candidates for being designated important to safety. Systems on pathways leading to core damage are not considered as being important-to-safety, although such systems could be considered candidates for severe accident management actions.
2. All Group 1 systems or components on successful termination paths are considered as candidates for being designated important-to-safety. This includes frontline systems and their support systems.
3. All safety related systems are designated important-to-safety.

Candidate Systems

Systems Important to Safety Criteria:

1. Any Group 1 system or component whose function is not backed up will be designated as important-to-safety.
2. Any Group 1 system or component with only Group 1 backup will be designated important-to-safety.
3. If a Group 2 candidate system is backed up by a Group 1 system, the Group 1 system will not be designated as important-to-safety.
4. Any Group 1 candidate system or component with at least one Group 2 backup will not be designated as important-to-safety.





**Jeff Wolfgang
CANDU Systems Research Program
Oak Ridge National Laboratory**

CANDU 3 Event Analysis

**Presented to the NRC Review Meeting
Systems Analysis of the CANDU 3 Reactor**

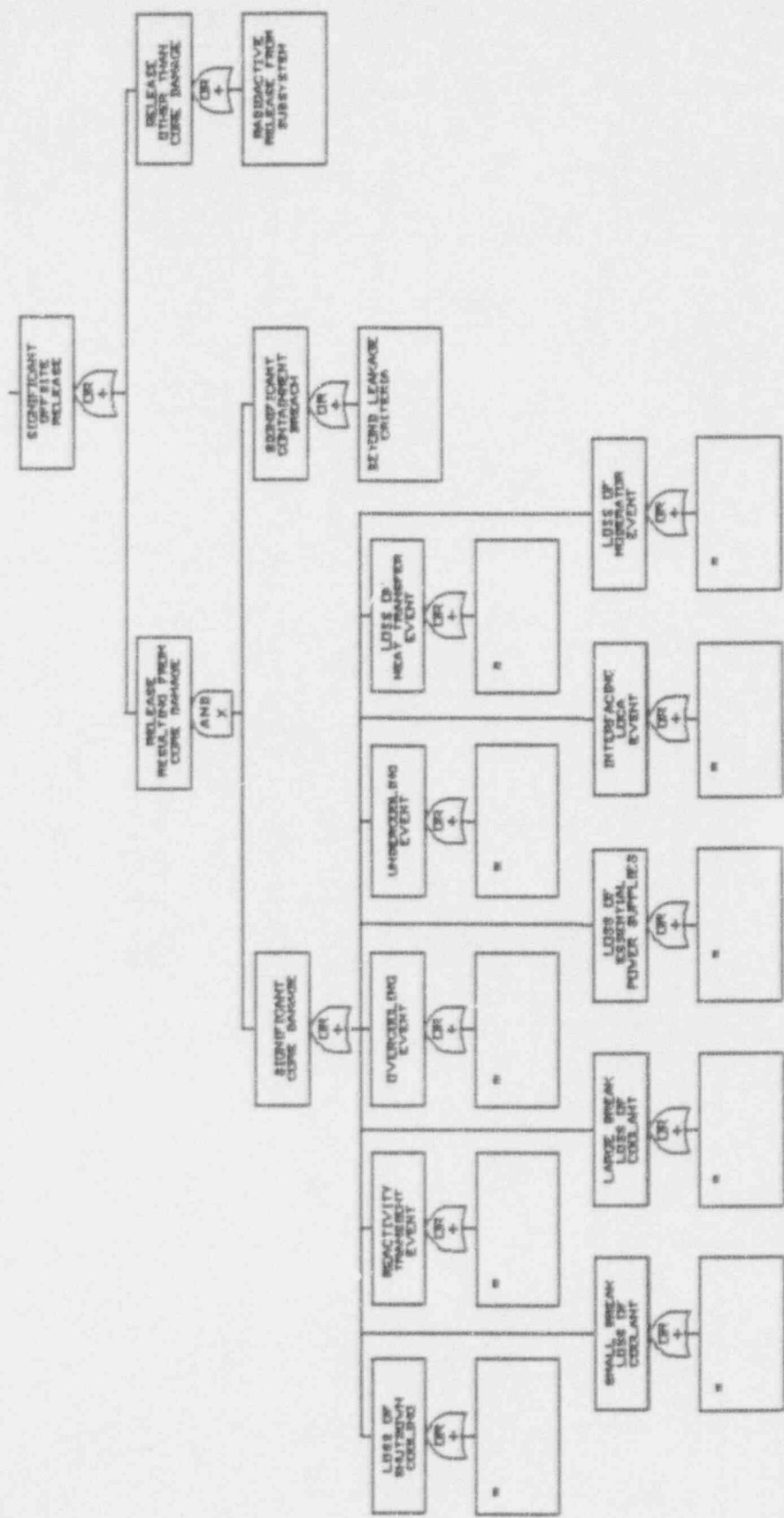
February 10, 1993

EVENT ANALYSIS

- **SELECTION OF EVENTS FOR ANALYSIS**
- **EVENT SEQUENCE DIAGRAMS**
- **EVENT TREES**
- **FAULT TREES**
- **ANALYZE SEQUENCES**
- **CATEGORIZE SEQUENCES**

SELECTION OF EVENTS FOR ANALYSIS

- MASTER LOGIC DIAGRAM
 - PLANT RESPONSE CATEGORIES
 - CONTAINMENT NEEDS FURTHER EVALUATION
 - RELEASES FROM SUBSYSTEMS ELIMINATED
- COMPILE INITIATORS
 - LIGHT WATER REACTOR EXPERIENCE
 - RESEARCH REACTORS EXPERIENCE
 - NUREG STANDARDS
 - NRC SAFETY REVIEW PLANS
 - EXISTING CANDU REACTOR ANALYSES
 - OPERATING HISTORY OF CANDU PLANTS
- CHOOSE REPRESENTATIVE INITIATING EVENTS



W Please refer to following events table

CANDU 3 Master Logic Diagram

Initiating Event Categorization

Plant Response Category (PRC)	Representative IE	Initiating Event (IE)	IE Frequency	Sources	Comments
Loss of Coolant - Large Break > 10 cm	Break in feeder tube header	1. Break in feeder tube headers	1 E-4	1, 2, 3, 5, 6	Frequency obtained from Ref. 2
		2. Backflow into ECC system	1 E-4	6	Requires 2 hardware failures
Loss of Coolant - Small Break < 10 cm	Liquid relief valve failure	1. Pressure tube leak/rupture	1 E-2	2, 5, 6	Frequency obtained from Ref. 2
		2. Inlet and outlet feeder tube leak/break	1 E-2	3, 6	Frequency obtained from Ref. 2
		3. Fuel handling machine breaks end fitting	1 E-2	2, 5, 6	Frequency obtained from Ref. 2
		4. Leakage from fuel handling machine/cooling system	1 E-2	5, 6	Hardware failure
		5. Liquid relief valve failure Pressurizer relief valve failure	1 E-1	2, 5, 6	Frequency obtained from Ref. 2 and 5
		6. Vent line and sample line leaks/breaks, leakage from primary system	1 E-1	1, 4, 5, 6	Frequency obtained from Ref. 2 and 5
		7. Heat transport pump seals fail	1 E-2	6	Hardware failure

		8. Failure of pressure and inventory control system	1 E-2	6	Non-safety system failure
Loss of Essential Power Supplies	Loss of Class IV power	1. Loss of station electric load	1 E-1	1, 2, 4	Frequency obtained from Ref. 5
		2. Offsite power lost	1 E-0	3, 4, 6	Frequency obtained from Ref. 5
		3. Loss of Class IV power	1 E-2	6	Frequency obtained from Ref. 2
Undercooling - Decrease in heat removal by secondary system	Feedwater piping break	1. Turbine trip	1 E-0	1, 4, 6	Frequency obtained from Ref. 5
		2. Loss of condenser vacuum	1 E-1	1, 4, 6	Frequency obtained from Ref. 5
		3. Loss of normal feedwater flow	1 E-0	1, 2, 3, 4, 5, 6	Frequency obtained from Ref. 5
		4. Feedwater piping break	1 E-3	1, 2, 4, 5, 6	Frequency obtained from Ref. 2
		5. Failure of steam generator pressure control resulting in closure of turbine throttle valves	1 E-2	2, 6	Hardware failure

		6. Loss of condensate pumps	1 E-1	4, 6	Frequency obtained from Ref. 5
		7. Failure of steam generator level control	1 E-2	6	Hardware Failure
Reactivity Transient	SCRAM	1. Uncontrolled control rod assembly withdrawal	1 E-2	1, 4, 6	Frequency obtained from Ref. 5
		2. Control rod maloperation (hardware or human error) - includes part length control rods, rod ejection, or rod drop accidents	1 E-0	1, 4, 5, 6	Frequency obtained from Ref. 5
		3. SCRAM - manual or inadvertent	1 E-0	3, 4, 6	Frequency obtained from Ref. 5
		4. Rod reposition error - pressure/temperature/power imbalance	1 E-1	4, 5, 6	Frequency obtained from Ref. 5
		5. moderator anomalies	1 E-2	5, 6	Hardware failure
Overcooling - Increase in heat removal by secondary system	SCRAM	1. Feedwater system malfunctions that result in an increase in feedwater flow or a decrease in feedwater temperature	1 E-0	1, 4, 6	Frequency obtained from Ref. 5
		2. Steam pressure regulator malfunction or failure that results in increasing steam flow (turbine overspeed)	1 E-2	1, 6	Hardware failure

		3. Inadvertent opening of a steam generator relief or safety valve	1 E-2	1, 4, 5, 6	Frequency obtained from Ref. 5
		4. Increased heat transfer flow or inventory	1 E-2	1, 3, 6	Hardware failure
		5. Steamline piping breaks inside or outside of containment	1 E-5	1, 2, 6	Frequency obtained from Ref. 2
		6. Startup of an inactive heat transfer loop or recirculating loop at an incorrect temperature	1 E-3	1, 4, 6	Frequency obtained from Ref. 5
Loss of Heat Transport - Decrease in heat removal by primary system	Loss of Class IV power	1. Loss of flow in one or both heat transfer pump loops	1 E-1	1, 4, 5, 6	Frequency obtained from Ref. 5
		2. Decreased heat transfer flow or inventory or flow blockage through fuel bundle	1 E-2	1, 3, 5, 6	Non-safety system failure
		3. Pressurizer anomalies (high pressure, low pressure, spray failure)	1 E-2	4, 6	Frequency obtained from Ref. 5
		4. Deformation of fuel channel structure that restricts coolant flow	1 E-3	6	Passive component failure
Interfacing LOCA - primary/secondary boundary breached	Feedwater piping break	1. Steam generator tube failure	1 E-3	1, 6	Passive component failure
Loss of Moderator Accident	SCRAM	1. Degradation or loss of moderator flow	1 E-2	2, 6	Non-safety system failure

		2. Degradation or loss of moderator cooling	1 E-2	2, 6	Non-safety system failure
		3. Loss of moderator inventory	1 E-2	2, 6	Non-safety system failure
		4. Failure of the cover gas system	1 E-2	2, 6	Non-safety system failure
		5. Moderator deuterium excursion	1 E-4	2, 6	Requires multiple failures
		6. Loss of calandria structural integrity	1 E-3	6	Passive component failure
Loss of Shutdown Cooling	SCRAM	1. Failure to initiate system	1 E-2	2, 6	Well rehearsed operator action
		2. Shutdown cooling hardware failures	1 E-2	6	Hardware failure
Radioactive Release from Subsystem	This category does not fall within the selected events	1. Leakage from radioactive gas or liquid waste systems	1 E-2	1	Non-safety system failure
		2. Fuel or spent fuel hardware failures or handling accidents	1 E-2	1, 2, 6	Hardware failure
Events not used		Failures of instrument air, service water, plant control data highways, etc. are support system associated and are not included as separate initiating events but are considered contributors to other initiators		2, 3, 4, 5, 6	

	Internal flooding and external events		2, 4, 5, 6	
	Beam tube failure		3	
	Pressurizer pump malfunction		3	
	Reactivity insertion		3	
	Leakage from control rods		4	
	Inadvertent safety injection		4	

1. Standard Review Plan, Table 15-1
2. External Analysis Report, Table 3-1
3. HFIR Internal Initiating Event Categories
4. NUREG/CR - 2815 Probabilistic Safety Analysis Procedures Guide, Table G.3
5. Operating Experience
6. AECL CANDU 3 Systematic Review of the Plant Design for Identification of Initiating Events

Justification for Representative Initiating Events

Plant Response Category (PRC)	Representative IE	Justification
Loss of Coolant - Large Break > 10 cm	Break in feeder tube header	Large volume of coolant inventory loss Requires immediate ECCS response
Loss of Coolant - Small Break < 10 cm	Liquid relief valve failure	Requires elements of other SBLOCAs such as crash cooling Requires isolation of the bleed condenser RRS not credited for reactor shutdown
Loss of Essential Power Supplies	Loss of Class IV power	Plant designed to feed power to itself upon loss of offsite power or station load Requires operation of diesel generators
Undercooling - Decrease in heat removal by secondary system	Feedwater piping break	Loss of coolant supply to the steam generators Potential challenge to the containment Poses a direct challenge upon the Group 2 feedwater system
Reactivity Transient	SCRAM	Requires the reactor to be shut down Other reactivity initiators will result in a SCRAM type situation
Overcooling - Increase in heat removal by the secondary side	SCRAM	Overcooling of the core is not a direct concern except that it forces the reactor to be shut down which then closely follows a SCRAM sequence
Loss of Heat Transport - Decrease in heat removal by the primary system	Loss of Class IV power	The heat transport pumps trip on a loss of Class IV power resulting in loss of forced flow through the core which looks like a loss of Class IV power event except that loss of power implies that other equipment also is unavailable. Simply stated, classifying this event under a loss of Class IV power makes the analysis of the event more conservative.
Interfacing LOCA - primary/secondary boundary breached	Feedwater piping break	The shutdown cooling system would be initiated to bypass the steam generators as would be done in a feedwater piping break
Loss of Moderator Accident	SCRAM	A moderator anomaly would result in a reactivity transient which will result in reactor shutdown
Loss of Shutdown Cooling	SCRAM	The sequence follows a SCRAM sequence progression except that the reactor is most likely already shutdown and the path through the shutdown cooling system would not be available

Initiating Events Chosen for Plant Analysis

Plant Response Category	Representative Initiating Event
Loss of Coolant - Large Break	Break in Feeder Tube Header
Loss of Coolant - Small Break	Liquid Relief Valve Failure
Loss of Essential Power Supplies	Loss of Class IV Power
Undercooling - Decrease in Heat Removal by secondary System	Feedwater piping break
Reactivity Transient	SCRAM

- **THE REPRESENTATIVE INITIATING EVENTS WERE SELECTED AS THE EVENTS JUDGED TO ADEQUATELY ADDRESS THE REMAINING INITIATORS**

EVENT SEQUENCE DIAGRAMS

- ESDs DEVELOPED FOR THE ANALYSIS
 - LBLOCA (BREAK IN FEEDER TUBE HEADER)
 - SBLOCA (LIQUID RELIEF VALVE FAILURE)
 - LOSS OF CLASS IV POWER
 - FEEDWATER PIPING BREAK
 - SCRAM
 - ATWS*
- PICTORIAL DISPLAY OF EVENT PROGRESSIONS
- PRECURSOR TO EVENT TREES
- USER FRIENDLY

* ATWS IS NOT CONSIDERED AN INITIATOR. AN ESD WAS DEVELOPED BECAUSE SOME OF THE SEQUENCES FROM THE OTHER INITIATORS RESULT IN AN ATWS SITUATION

TERMS NEEDING ADDITIONAL CLARIFICATION

- GROUP 1
- GROUP 2
- SPECIAL SAFETY SYSTEMS
- SAFETY SYSTEMS
- SAFETY SUPPORT SYSTEMS
- SAFETY RELATED SYSTEMS
- SYSTEMS IMPORTANT TO SAFETY

GROUP 1

SYSTEMS AND COMPONENTS REQUIRED FOR THE PRODUCTION OF ELECTRICAL POWER WHILE THE PLANT IS IN ITS NORMAL OPERATING MODE. THESE SYSTEMS ARE ALSO REFERRED TO AS *PROCESS SYSTEMS*. (D4-5)

GROUP 2

SYSTEMS AND COMPONENTS REQUIRED FOR THE MITIGATION OF SERIOUS PROCESS FAILURES, INCLUDING THOSE CAUSED BY SITE RELATED EXTERNAL EVENTS SUCH AS EARTHQUAKES AND TORNADOS. GROUP 2 SYSTEMS MUST ENSURE THAT THE SAFETY FUNCTIONS REQUIRED TO MITIGATE A SERIOUS PROCESS FAILURE CAN BE PERFORMED DESPITE THE FAILURE OR UNAVAILABILITY OF THE GROUP1 SYSTEMS OR COMPONENTS. (D4-5)

TABLE 1

GROUP 2 SYSTEMS

GSI	SYSTEM	SUB GROUP	FUNCTION
<u>A. REACTOR SHUTDOWN</u>			
68200 31800	Shutdown System No. 1	2A	Reactor shutdown during accident conditions
68300 34700	Shutdown System No. 2	2B	Reactor shutdown during accident conditions
<u>B. HEAT REMOVAL FROM FUEL</u>			
33400	Shutdown Cooling System	2A	Heat transfer from fuel after a loss of Group 1 support services
34320	Emergency Core Cooling System	2A	Heat transfer from fuel during a loss of coolant accident
43300	Group 2 Feedwater System	2A	Maintains heat transfer from steam generator to atmosphere via Main Steam Safety Valves.
72310	Group 2 Raw Service Water System	2A	Heat transfer from Group 2 components to ultimate heat sink
<u>C. CONTAINMENT OF FISSION PRODUCTS</u>			
68400	Containment Systems	2B	Maintains containment envelope as barrier to fission product release.
<u>D. MONITORING AND CONTROL</u>			
66000	Secondary Control Area	2A/2B	Monitoring and control for Group 2 systems
68700	Safety Systems Computers	2A/2B	As above.
68930	Post Accident Monitoring	2A/2B	Monitoring and control.

TABLE 1 (continued)

GSI	SYSTEM	SUB GROUP	FUNCTION
E. MISCELLANEOUS SAFETY SUPPORT SERVICES			
52000	Group 2 Electrical Supply System	2A/2B	Provides electrical power to Group 2 systems
53000	Group 2 Electrical Distribution System	2A/2B	As above
73400	Group 2 Service Building Heating, Cooling and Ventilation Systems	2A/2B	Provides adequate operating environment for Group 2 systems.
74230	Group 2 Service Building Firewater System	2A/2B	Mitigates effect of fires in the Group 2 area.
75170	Group 2 Instrument Air	2A/2B	Provides instrument air supplies to Group 2 systems, as required

SPECIAL SAFETY SYSTEMS

- SHUTDOWN SYSTEM 1 (SDS1)
- SHUTDOWN SYSTEM 2 (SDS2)
- EMERGENCY CORE COOLING SYSTEM (ECCS)
- CONTAINMNET

(D4-5)

SAFETY SYSTEMS

**SYSTEMS ASSIGNED TO GROUP 2 INCLUDING THE
SPECIAL SAFETY SYSTEMS (3-1, D4-5)**

SAFETY SUPPORT SYSTEMS

**SYSTEMS WHICH PROVIDE ELECTRICAL POWER,
INSTRUMENT AIR AND COOLING WATER TO
MITIGATE SERIOUS PROCESS FAILURES (D4-3)**

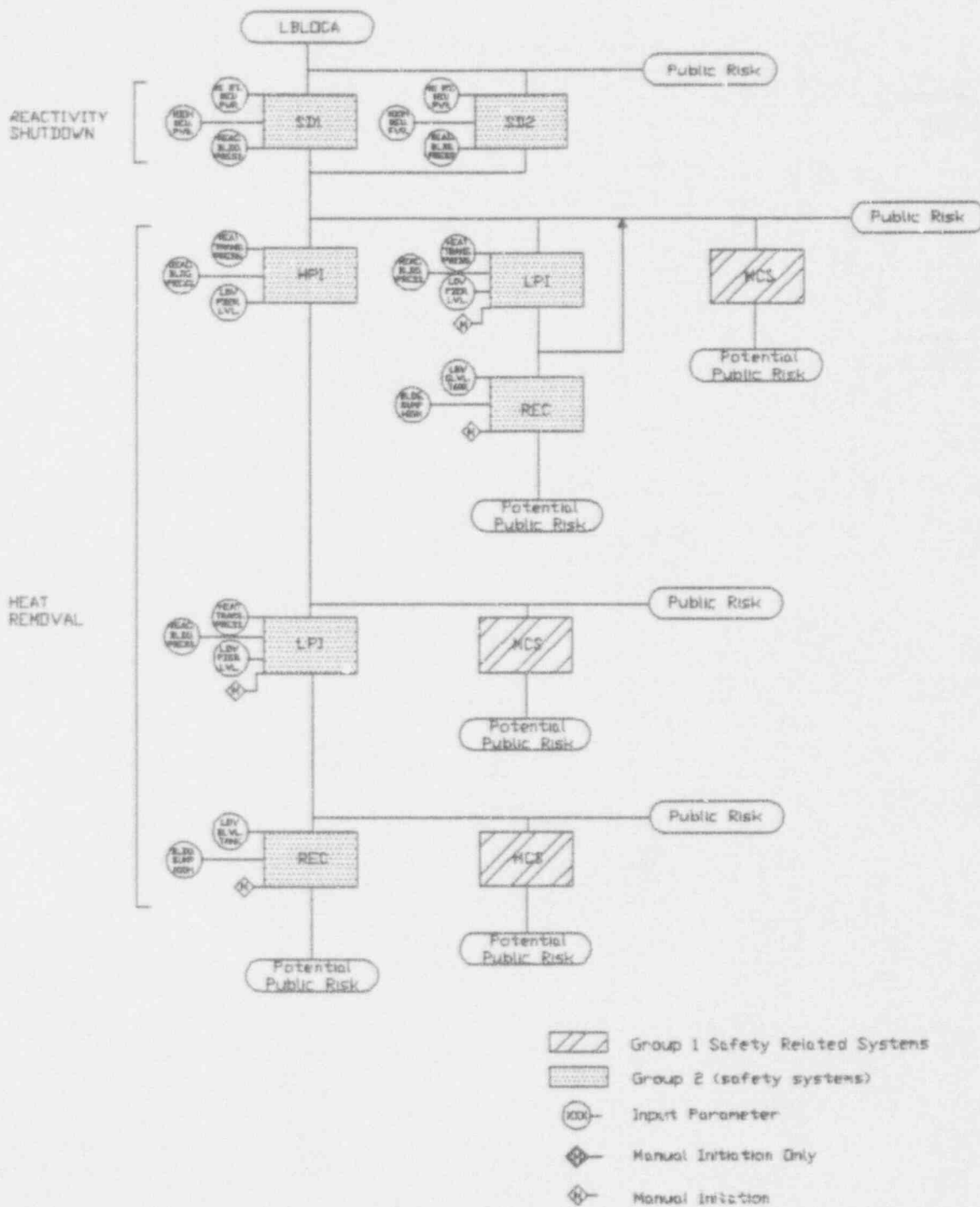
SAFETY RELATED SYSTEMS

SYSTEMS AND STRUCTURES THAT PERFORM THE GENERAL SAFETY FUNCTIONS WHICH MUST BE PERFORMED DURING NORMAL PLANT OPERATION AND DURING ACCIDENT CONDITIONS TO PROTECT THE PLANT WORKERS AND THE PUBLIC FROM ADVERSE HEALTH EFFECTS DUE TO THE RELEASE OF RADIOACTIVE MATERIALS. THE SAFETY FUNCTIONS ARE:

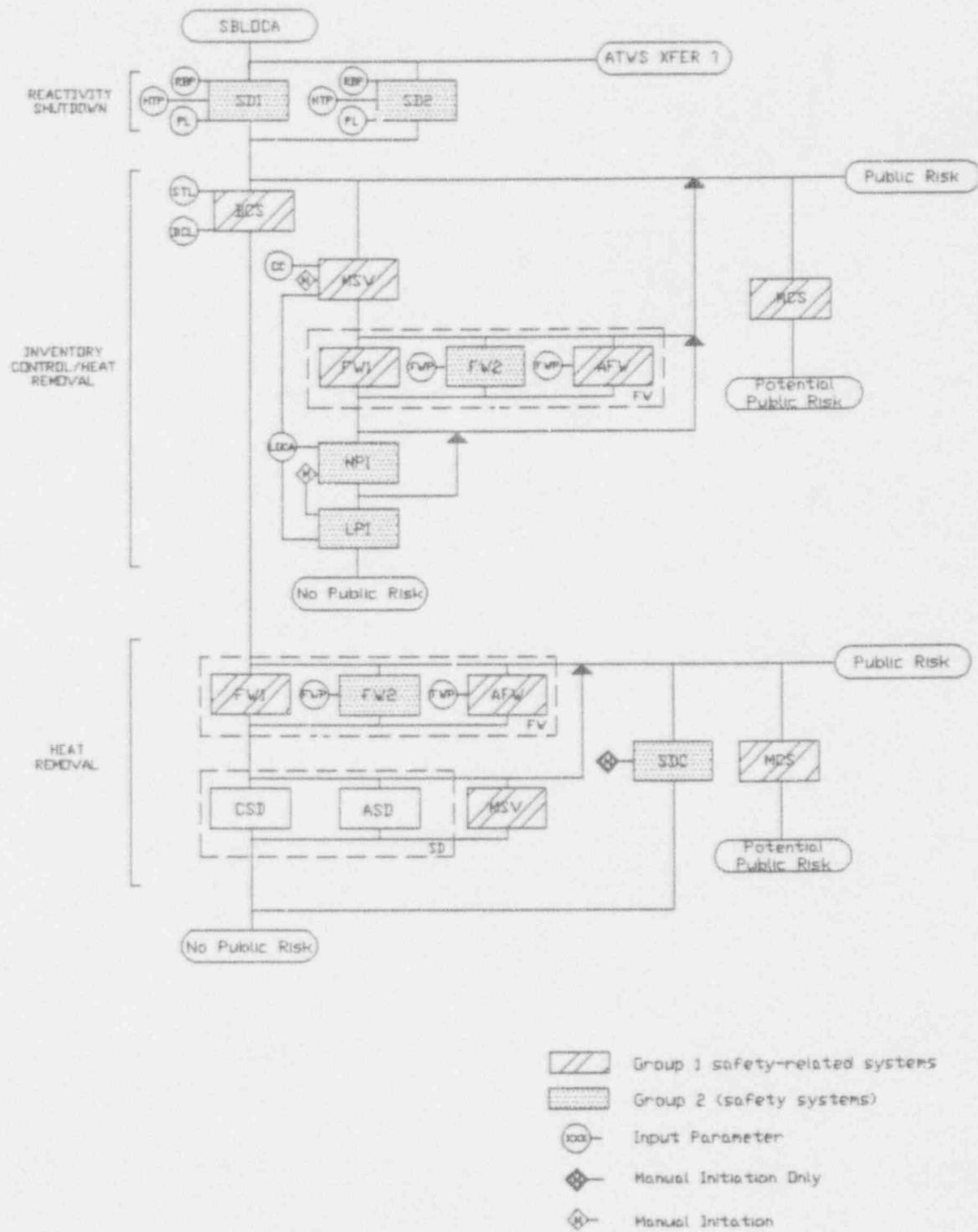
1. SHUT THE REACTOR DOWN AND MAINTAIN IT IN A SAFE SHUTDOWN CONDITION
2. REMOVE HEAT FROM THE FUEL
3. LIMIT THE RELEASE OF RADIOACTIVE MATERIAL BY MAINTAINING A BARRIER
4. MONITOR THE CONDITIONS OF THE PLANT AND PERFORM ACTIONS NECESARY TO MAINTAIN THE ABOVE SAFETY FUNCTIONS
(D1-3-1)

SYSTEMS IMPORTANT TO SAFETY

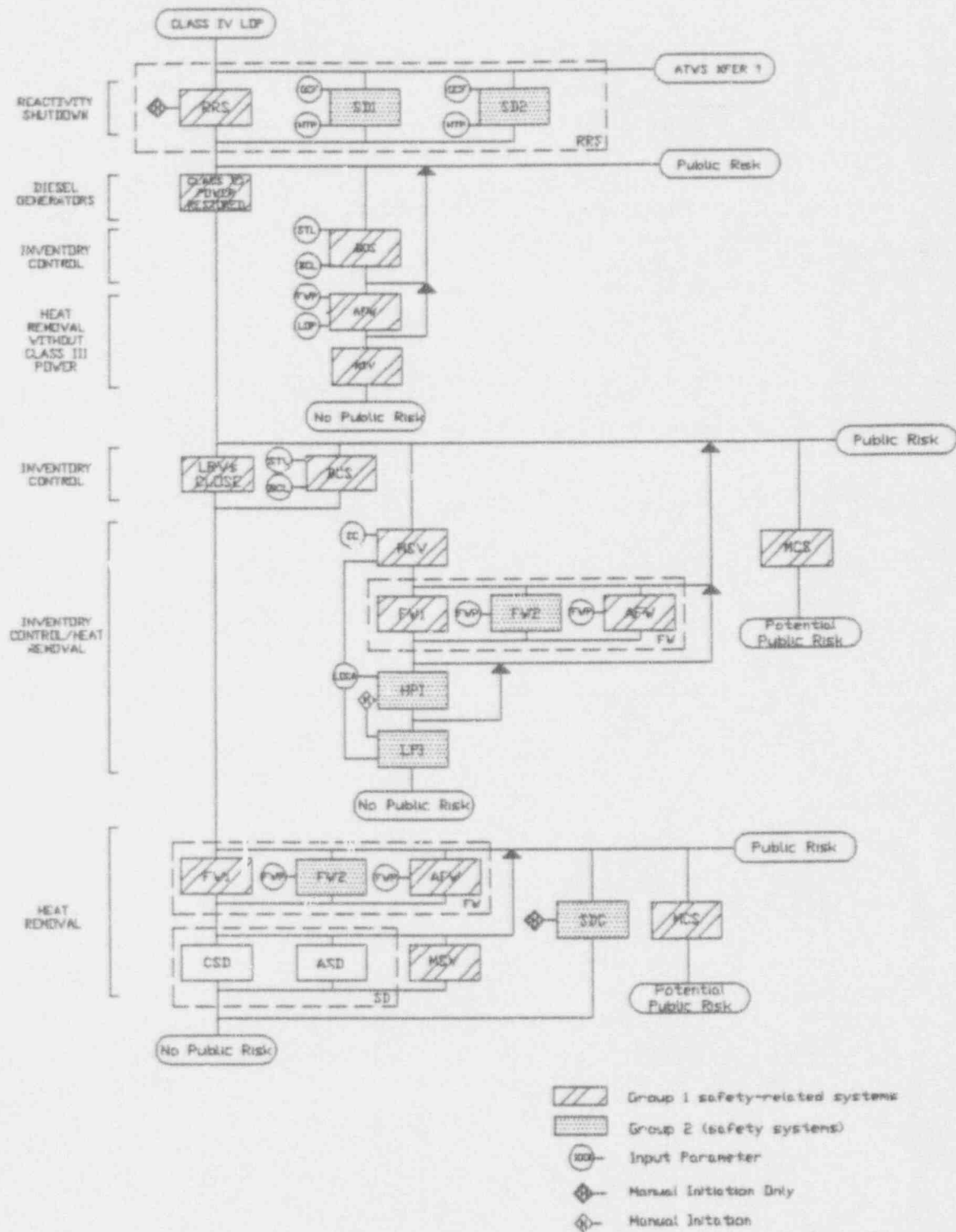
SYSTEMS HAVING A SIGNIFICANT IMPACT ON THE SUCCESSFUL RESPONSE OF THE PLANT TO AN INITIATING EVENT. (A SYSTEM IN ANY OF THE CATEGORIES DEFINED PREVIOUSLY MAY BE A *SYSTEM IMPORTANT TO SAFETY* PROVIDED IT MEETS THE CRITERIA SPECIFIED IN THE *CANDU 3 SYSTEMS ANALYSIS REPORT*.)



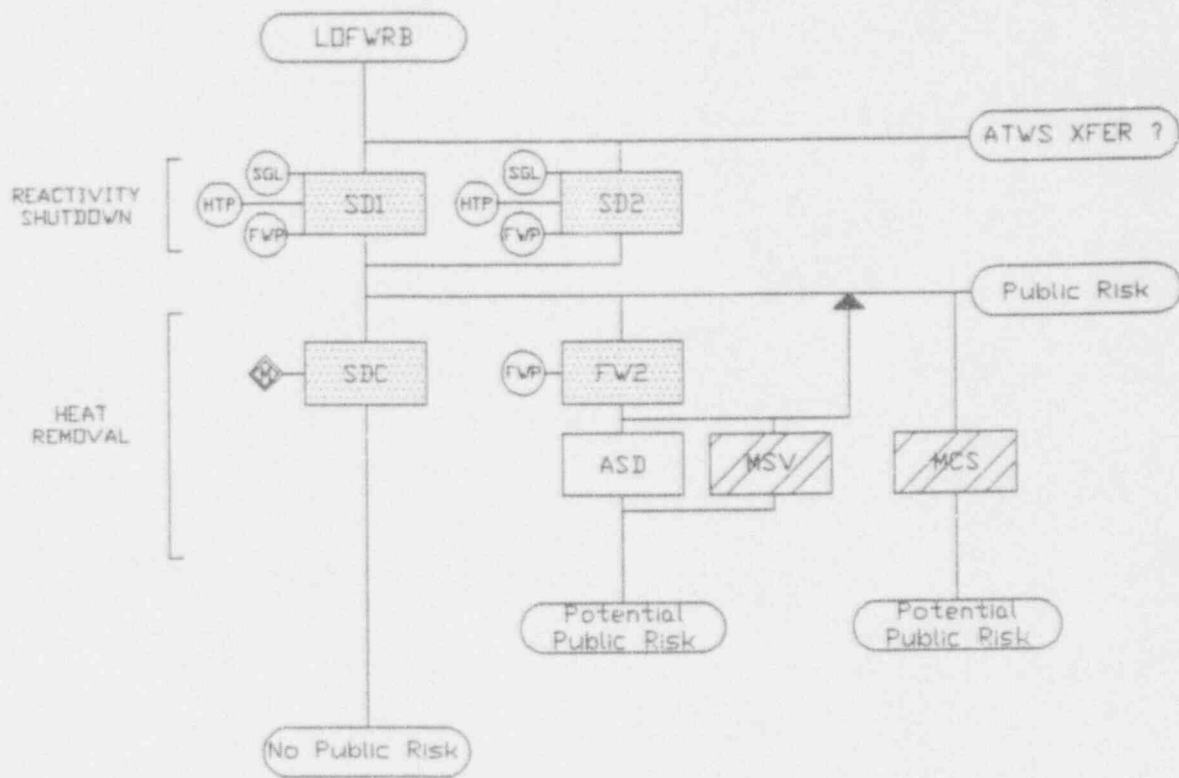
Large Break LOCA Event Sequence Diagram



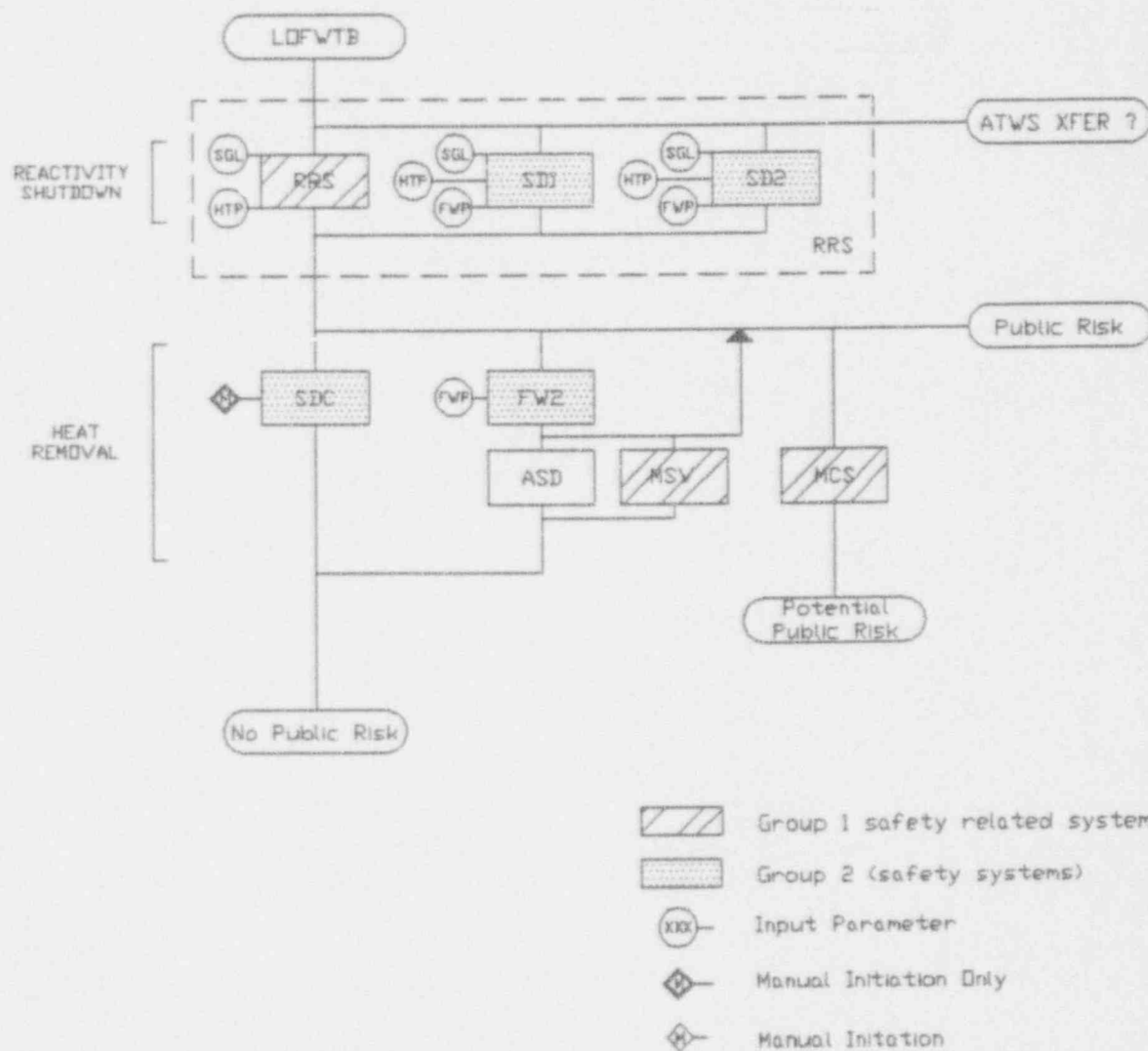
Small Break LOCA Event Sequence Diagram



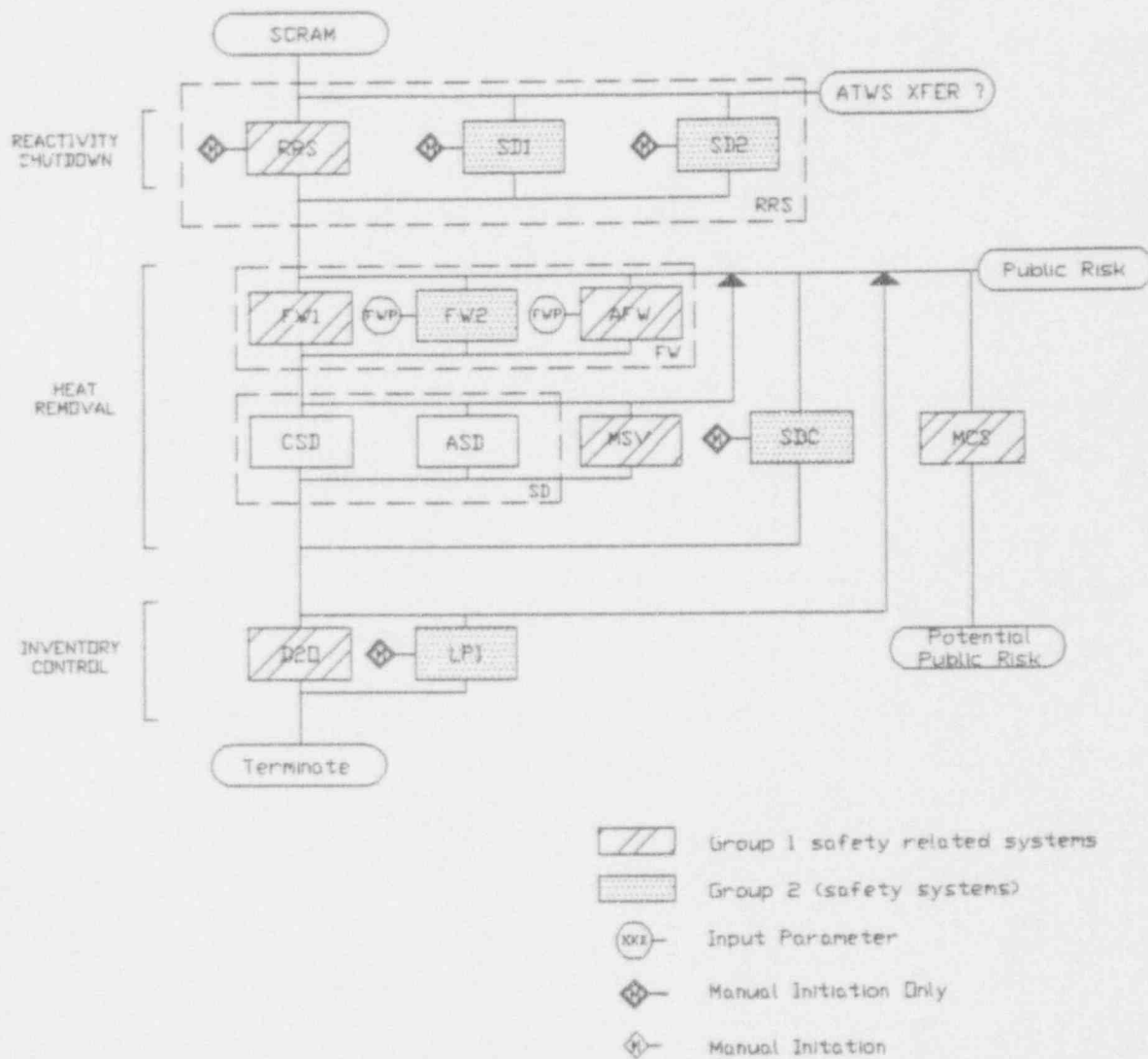
Loss of Class IV Power Event Sequence Diagram



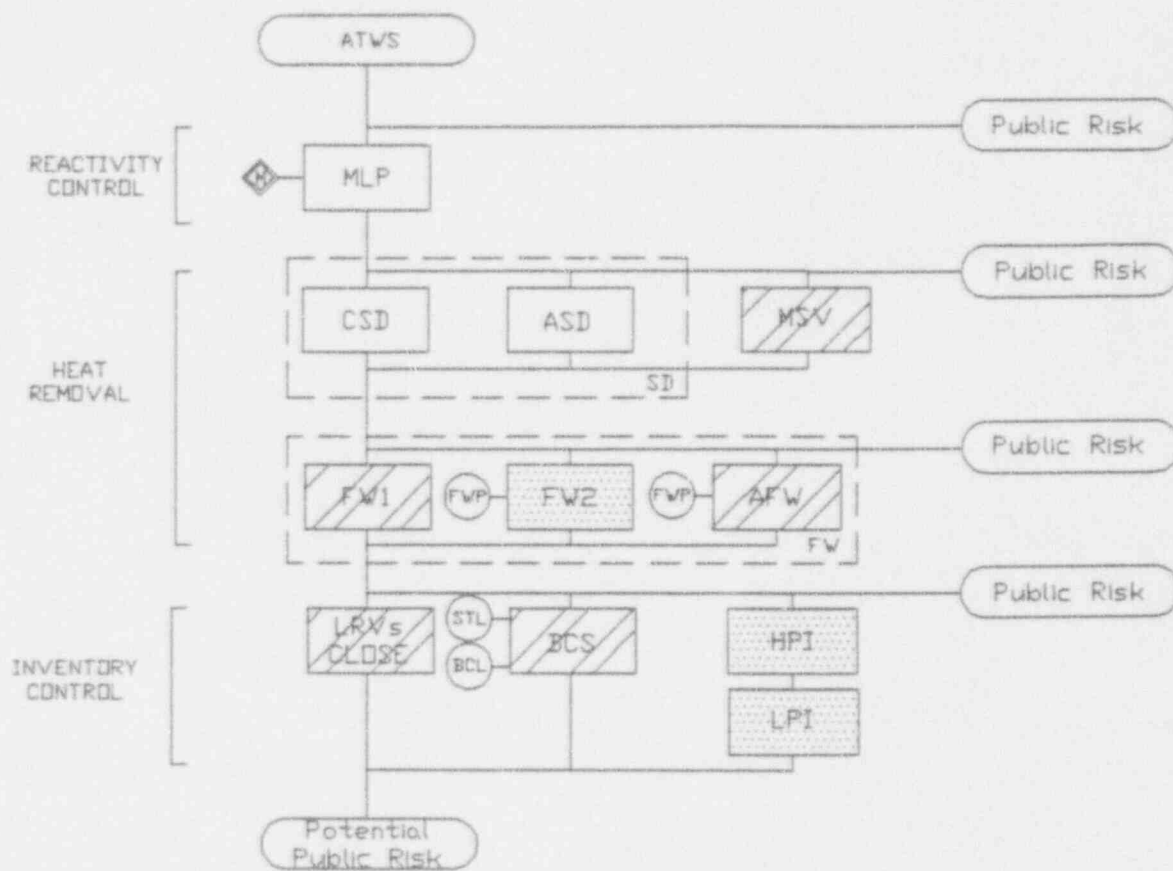
Loss of Feedwater (reactor building) Event Sequence Diagram

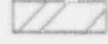






Loss of Feedwater (turbine building) Event Sequence Diagram



SCRAM Event Sequence Diagram



-  Group 1 safety related systems
-  Group 2 (safety systems)
-  Input Parameter
-  Manual Initiation Only
-  Manual Initiation

ATWS Event Sequence Diagram

**Jeff Wolfgang
CANDU Systems Research Program
Oak Ridge National Laboratory**

Sequences Identified for Further Evaluation

**Presented to the NRC Review Meeting
Systems Analysis of the CANDU 3 Reactor**

February 10, 1993

SEQUENCES REQUIRING FURTHER EVALUATION

CRITERIA

- SEQUENCES CLASSIFIED AS AOOs, DBAs, or SAs NOT EVALUATED IN THE CONCEPTUAL SAFETY REPORT IN ANY WAY

OR

- SEQUENCES WHOSE CATEGORIZATION IS UNCERTAIN DUE TO LACK OF INFORMATION OR WHOSE FAILURE SETS REFLECTED POSSIBLY UNACCEPTABLE SYSTEM PERFORMANCE

Justification for Sequences Requiring Further Evaluation

	SEQUENCE DESCRIPTION	JUSTIFICATION
1.	LBLOCA with failure of SDS1	Information needed about the SDS1 trip logic design to assure it does not contain any single failures. More information may allow better categorization of this sequence.
2.	LBLOCA with failure of SDS1 and SDS2	Potential single failure of SDS1 combined with a single failure of SDS2. The SDS2 single failure involves human error associated with reclosure of the helium vent lines.
3.	SBLOCA with failure to remove steam from the steam generators	Indications are that failure of the plant air system may disable all three methods of steam removal. More information needed regarding the supports for these valves.
4.	SBLOCA with failure to isolate the bleed condenser	More information needed regarding bleed condenser isolation valve supports to determine if failure of a single power support can cause the bleed condenser to not be isolated.

	SEQUENCE DESCRIPTION	JUSTIFICATION
5.	Failure of a liquid relief valve to reclose following restoration of power	Single failure following loss of Class IV power results in a SBLOCA type event.
6.	Liquid relief valve fails to reclose after restoration of power followed by failure to remove steam from the steam generators	Same discussions as for 3 and 5.
7.	Liquid relief valve fails to reclose after restoration of power followed by failure to isolate the bleed condenser	The discussion about failure of a single power supply possibly causing failure to isolate the bleed condenser in 4 also applies for this sequence.
8.	Failure to restore onsite power following LOP	Restoration of onsite power needs to be analyzed in more detail.

	SEQUENCE DESCRIPTION	JUSTIFICATION
9.	LOFW with failure of the shutdown cooling system	Single failure involving human error in failing to initiate the shutdown cooling system
10.	Failure of the D ₂ O makeup system following reactor shutdown	A single valve failure in the D ₂ O makeup system can cause this system to be unavailable. Evaluation of the adequacy of the pressurizer inventory may be required.
11.	Failure to remove steam from the steam generators following reactor shutdown along with failure of the D ₂ O makeup system	Same discussion as for 3 and 10.

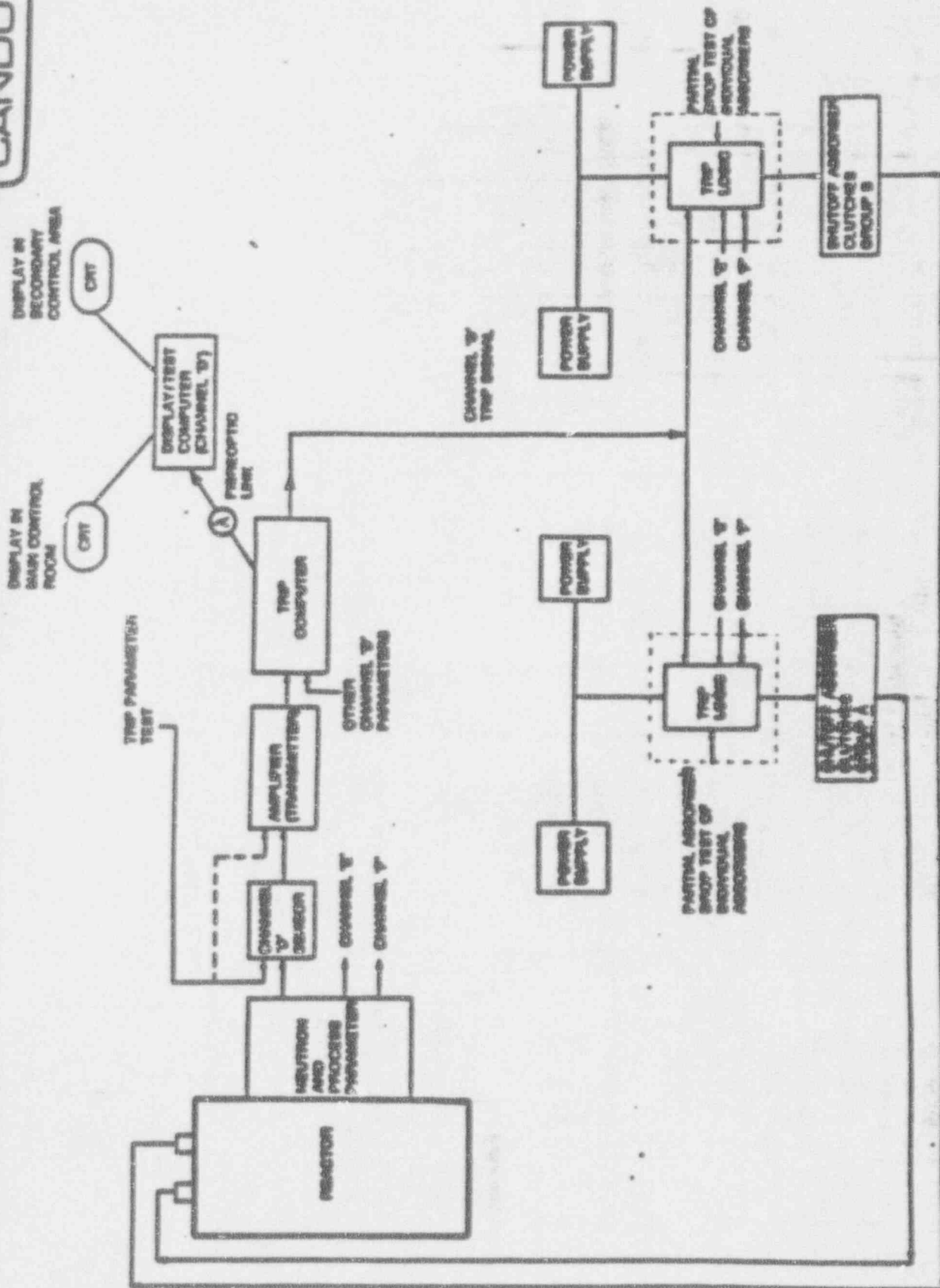
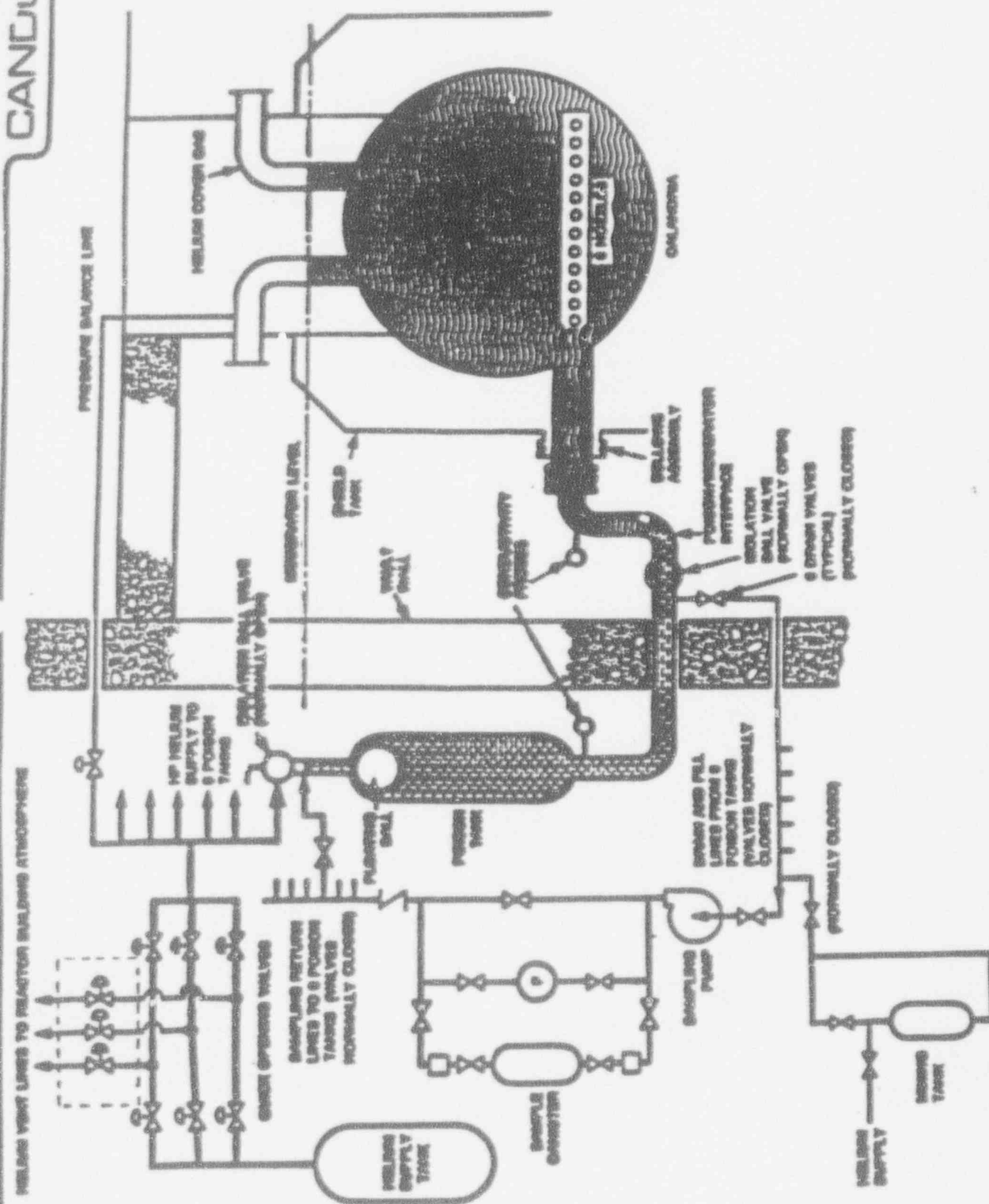
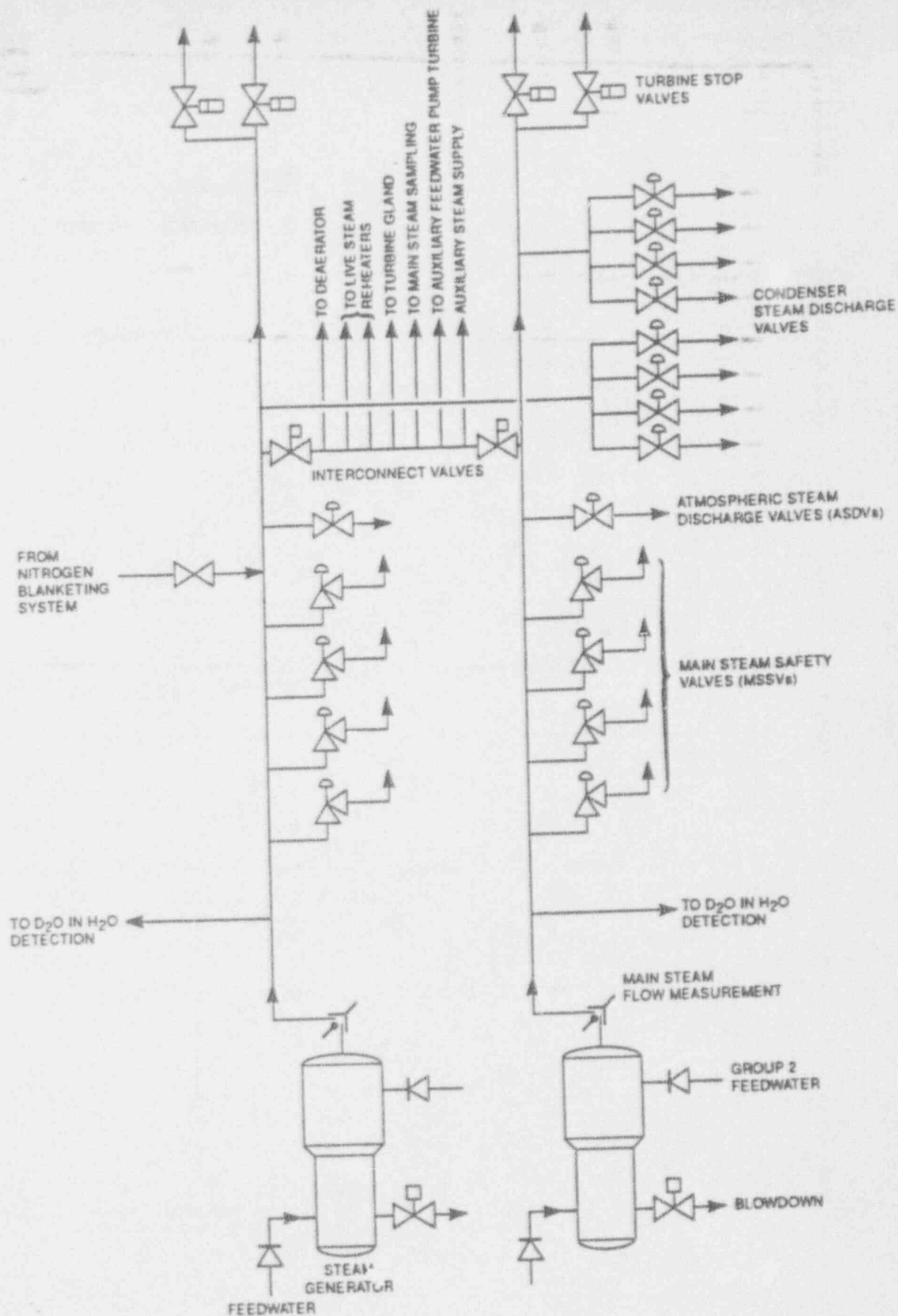


FIGURE 3.2.3 SHUTDOWN SYSTEM NO.1 -- BLOCK DIAGRAM





920396

FIGURE 3.9-1 STEAM SYSTEM

CANDU

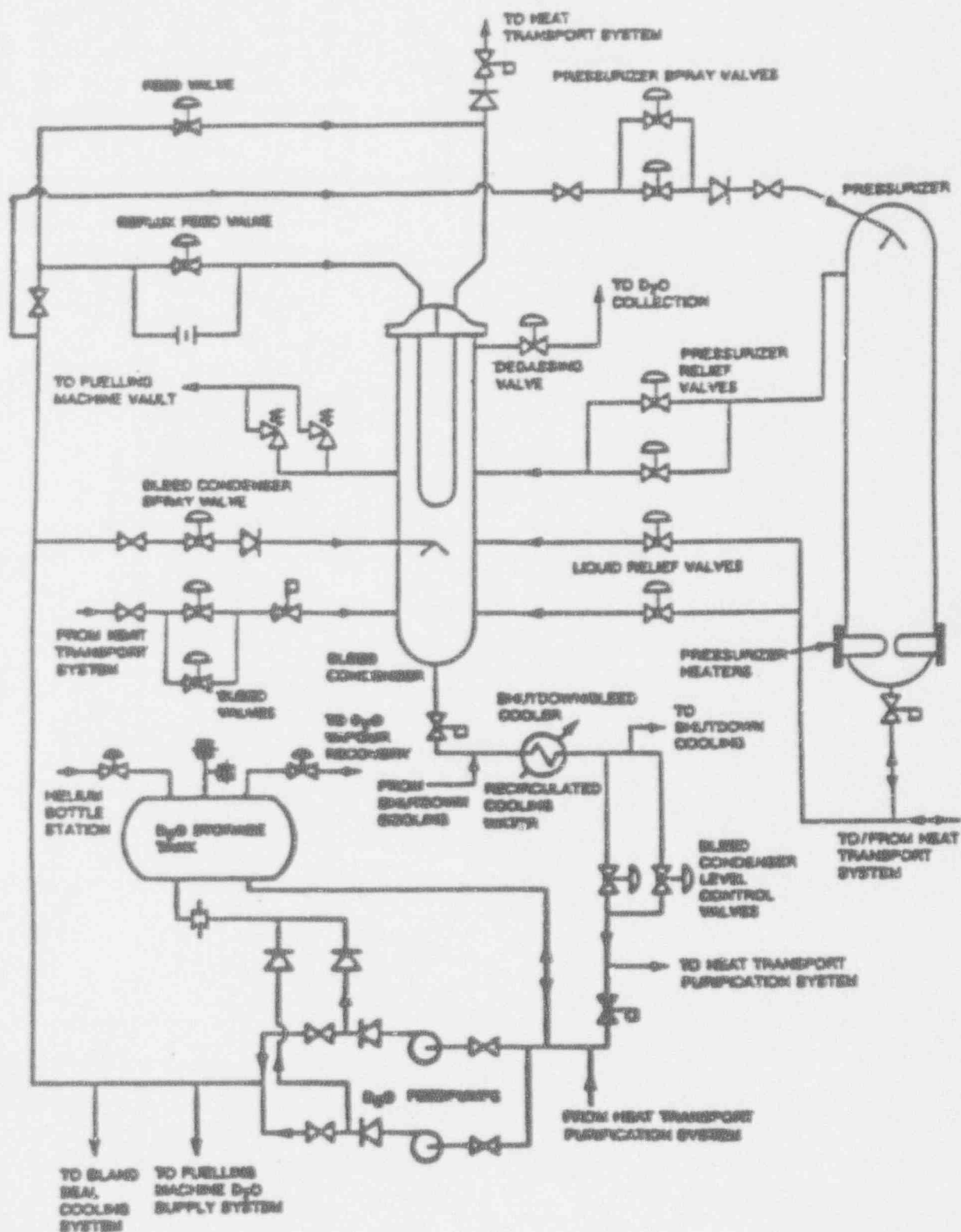


FIGURE 5.2.22 HEAT TRANSPORT PRESSURE AND INVENTORY CONTROL SYSTEM

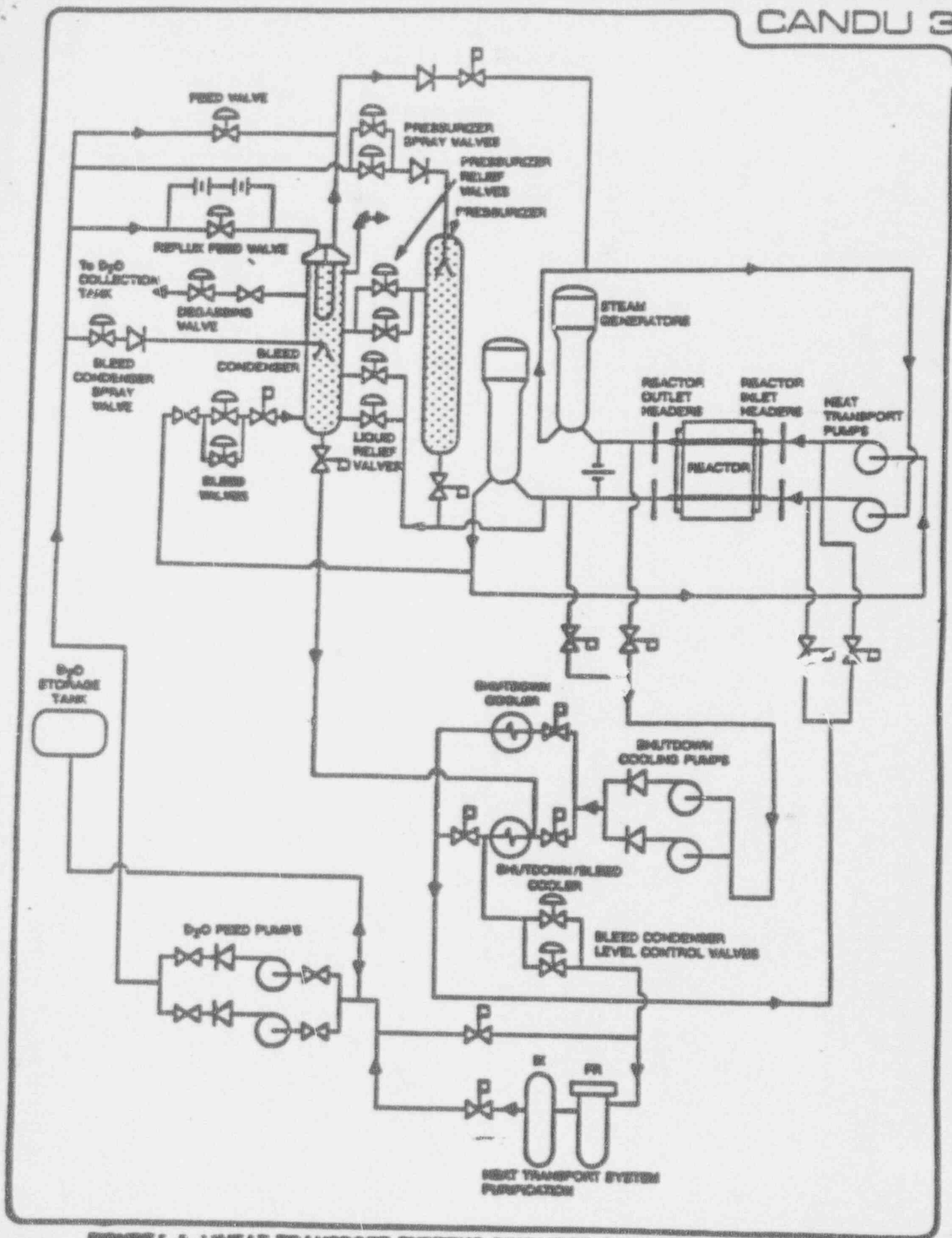


FIGURE 5.2.1 HEAT TRANSPORT SYSTEMS SIMPLIFIED COMPOSITE FLOW DIAGRAM

Jeff Wolfgong
CANDU Systems Research Program
Oak Ridge National Laboratory

Significant Operator Actions

Presented to the NRC Review Meeting
Systems Analysis of the CANDU 3 Reactor

February 10, 1993

SOURCES OF INFORMATION

- SYSTEMS DESCRIPTIONS IN CSR
 - INSIGHTS GAINED FROM FAULT TREE AND EVENT TREE EVALUATION
- * NO OPERATING OR MAINTENANCE PROCEDURES WERE AVAILABLE*

SIGNIFICANT OPERATOR ACTIONS

- REACTOR SHUTDOWN
 - SCRAM INITIATORS
- POSSIBLE ECCS INITIATION AFTER SBLOCA
- REFILL OF GROUP 2 FEEDWATER SUPPLY TANK
- INITIATION OF THE SHUTDOWN COOLING SYSTEM
- POISON ADDITION IN ATWS SEQUENCES

**Jeff Wolfgang
CANDU Systems Research Program
Oak Ridge National Laboratory**

Dependency Matrix

**Presented to the NRC Review Meeting
Systems Analysis of the CANDU 3 Reactor**

February 10, 1993

1. All electrical valves required for high pressure injection are supplied from Class II Group 2 power. These valves fail as is.
2. Separately channeled Group 2a Class I and Class II power supplies are provided for each channel of shutdown system 1. The logic is arranged so that any loss of power to a channel results in a channel trip. The direct current clutches operated from rectified redundant Class II power release on loss of power.
3. The quick opening valves in SDS2 are air-to-close, spring-to-open on loss air or electric power.
4. Separately channeled Group 2b Class I and Class II power supplies are connected to each SDS2 channel. The logic and instrumentation have been designed so that a channel trips on loss of power.
5. The ECCS pumps are energized by Group 2 Class III power. This power is also supplied to electrical valves required for operation. These valves fail as is.
6. Supplies normal cooling water for the ECCS heat exchangers.
7. Supplies backup cooling water for the ECCS heat exchangers.
8. Moderator cooling pumps supplied with Group 1 Class III power.
9. Moderator cooling pumps and heat exchangers are cooled by the Recirculation cooling water system.
10. Recirculation cooling water pumps are supplied from Group 1 Class III power.
11. The recirculation cooling water heat exchangers have the heat removed by the raw service water system.
12. The raw service water pumps are supplied from group 1 Class III power.
13. The Group 2 service water pumps are supplied from Group 2 Class III power.
14. The plant air compressors are supplied from Group 1 Class III power.
15. Heat transport system pumps supplied by Class IV power.
16. Group 1 feedwater pumps and valves supplied by Group 2 Class III power.
17. Group 2 feedwater pumps and valves supplied by Group 2 Class II power.
18. Shutdown cooling system pumps and valves supplied by Group 2 Class II power.
19. MSSVs, SDVs, and ASDs supplied by Group 2 Class II power.
20. Liquid relief valves fail open on loss of Group 2 Class II power.
21. D₂O pumps supplied by Group 1 Class III power. Valves supplied by Group 1 Class II.
22. Valves supplied by Group 1 Class II power.
23. Group 1 Feedwater backup cooling supplied by RCW and Fire Water systems.
24. Shutdown cooling heat exchangers (heat removal side) fed by RCW and Group 2 FW.
25. Level control valves fail closed 1.5 hours after loss of air.
26. Air dependancy assumed. Valves may be self-actuated.
27. Air required to open ASDs and SDVs.
28. LRVs fail open on loss of air.
29. Feed control valves require air to open.
30. Assumed that bleed condenser LCV requires air to close.

Mark Linn

CANDU Systems Research Program
Oak Ridge National Laboratory

**Preliminary Listing of Events and
Event Categorizations**

Presented to NRC/AECL Review Meeting
Systems Analysis of the CANDU 3 Reactor

February 10, 1993

DRAFT

CANDU Table 1
(Preliminary Listing)

Anticipated Operating Occurances (AOOs)

1. Loss of station electrical load
2. Offsite power lost
3. Loss of Class IV power
4. Loss of flow in one or both heat transport loops
5. Decreased heat transport system flow through fuel or flow blockage
6. Pressurizer anomalies (high/low pressure, spray failure)
7. Uncontrolled control rod assembly withdrawal
8. Control rod misoperation
9. Manual or inadvertent SCRAM
10. Rod reposition error
11. Moderator anomalies
12. Feedwater malfunctions resulting in feed flow increase or feed temperature decrease
13. Steam pressure regulator failure resulting in increased steam flow
14. Inadvertent opening of SG relief or safety valve
15. Increased heat transfer flow or inventory
16. Degradation or loss of moderator cooling
17. Degradation or loss of moderator flow
18. Loss of moderator inventory
19. Failure of cover gas system
20. Pressure tube leak/break
21. Inlet or outlet feeder tube leak/break
22. Fuel handling machine breaks end fitting
23. Leakage from fuel handling machine/cooling system
24. Liquid relief valve/pressurizer relief valve failure
25. Heat transport pump seal failure
26. Primary leakage (sample and vent lines)
27. Failure of pressure and inventory control system
28. Turbine trip
29. Loss of condenser vacuum
30. Loss of normal feedwater flow
31. SG pressure control failure closes turbine throttle valves
32. Loss of condensate pumps
33. Failure of steam generator level control system
34. Failure to initiate shutdown cooling
35. Shutdown cooling failure

DRAFT

CANDU Table 2
(Preliminary Listing)

Design Basis Accidents (DBAs)

1. Break in feeder tube headers
2. Backflow to ECCS
3. Steam generator fails to transfer heat to feedwater
4. Loss of calandria structural integrity
5. Startup of inactive heat transfer loop at incorrect temperature
6. Moderator deuterium excursion
7. Feedwater piping break (outside containment)
8. Steam generator tube failure
9. Deformation of fuel channel structure that restricts coolant flow.

DRAFT

CANDU Table 3
(Preliminary Listing)

Severe Accidents (SAs)

1. Steam line break inside or outside containment
2. Feedwater line break inside containment

**AECL****EACL****AECL CANDU****EACL CANDU**

EMERGENCY CORE COOLING SYSTEM

- Key Design Parameters
 - 150 m³ gas tank, 2x150 m³ water tanks for accumulator
 - 6.5 MPa (950 psi) initial gas pressure
 - 1200 m³ grade level tank
 - 2x100% pumps for grade level tank and recirculation
 - pumps rated at about 110 m head and 600 l/s flow
- Initiation Signals
 - low HTS pressure (6.2 MPa) AND high containment pressure
OR
sustained low HTS pressure (5.6 MPa) for 4 minutes

**AECL****EACL****AECL CANDU****EACL CANDU**

EMERGENCY CORE COOLING SYSTEM

- Key Design Requirements (reference AECB R-9)
 - meet dose limits
 - no fuel failures for small breaks
 - maintain coolable geometry for large breaks
 - maintain long term cooling
 - 1E-3 availability target
 - single failure proof for active components
 - independent of off-site power

CANDU 3

**AECL****EACL****AECL CANDU****EACL CANDU**

CRASH COOLDOWN

- Initiation Signals
 - Low HTS Pressure AND High Containment Pressure OR Sustained Low HTS Pressure
- Main Steam Safety Valves Opened By:
 - System Overpressure (spring loaded)
 - ECCS Initiation Signal
 - SDS #2 Signal (half of valves only)

Case 1: 0.76% RIH Break

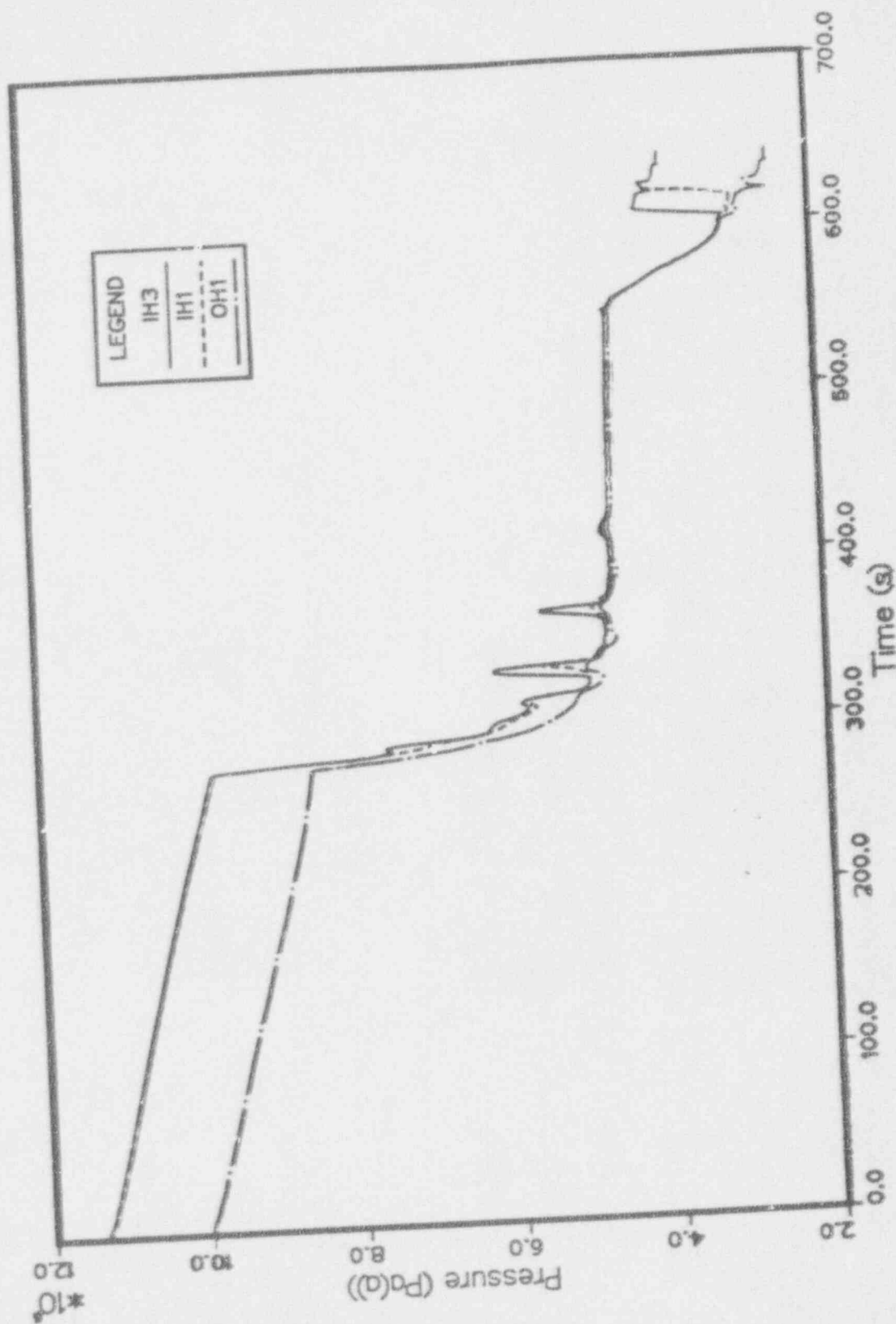


Figure 6.1-15: Core Passes 3 and 1 Reactor Header Pressures

**AECL****EACL**

AECL CANDU

EACL CANDU

OPERATOR ACTIONS

- overall target to have first mitigating operator actions be at 10 hours if mitigating systems work.
- one exception is feedwater break between boiler and check valve (operator must stop feedwater flow to broken boiler to minimize water loss)
- second exception is initiation of Shutdown Cooling and boiler isolation following S/G tube failure in order to limit release.
- action at 10 hours is initiation of Shutdown Cooling or Group 2 Feedwater Tank makeup
- most operator actions are initiation of backups to primary mitigating systems. Backups include:
 - Shutdown Cooling

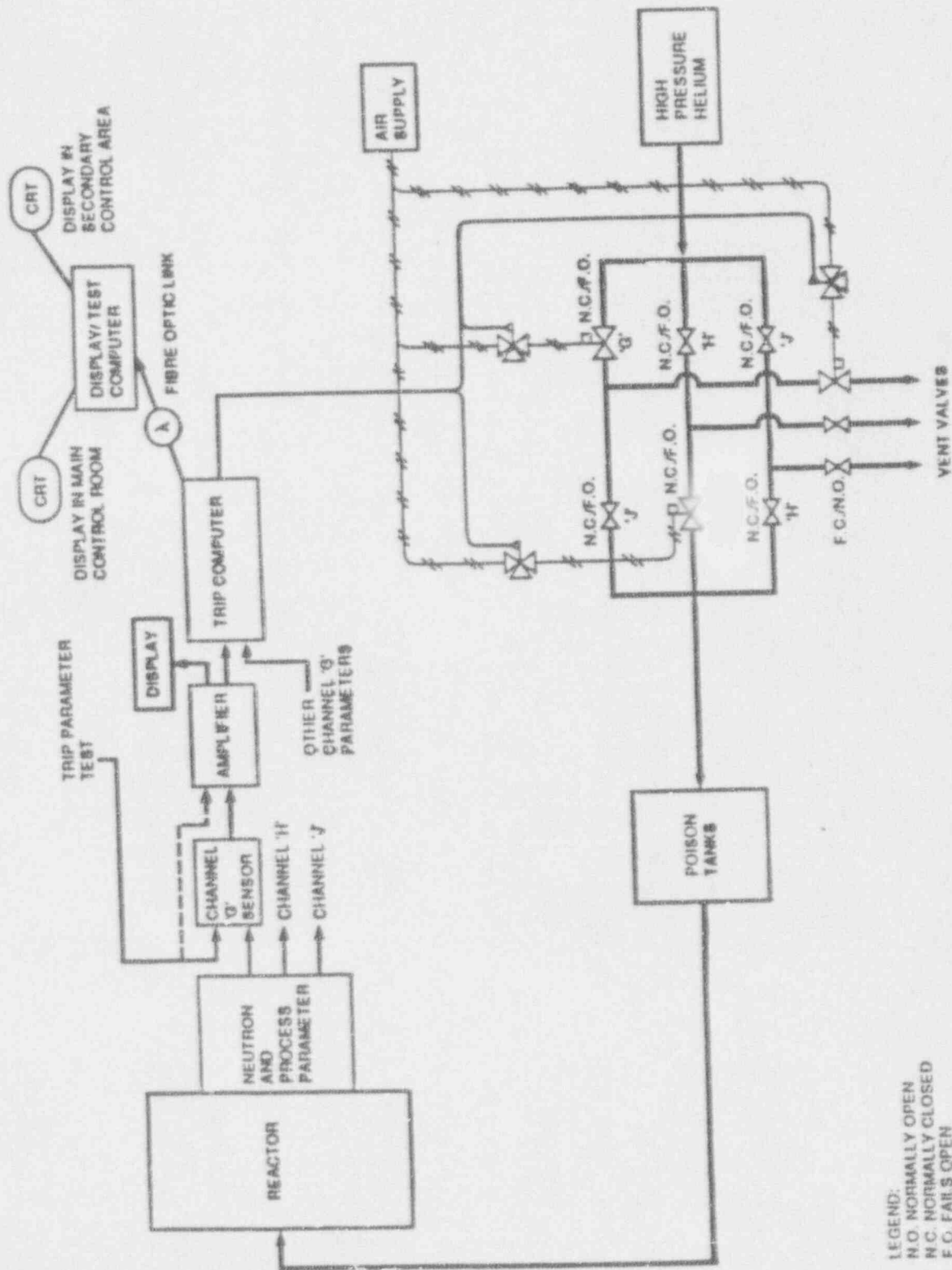
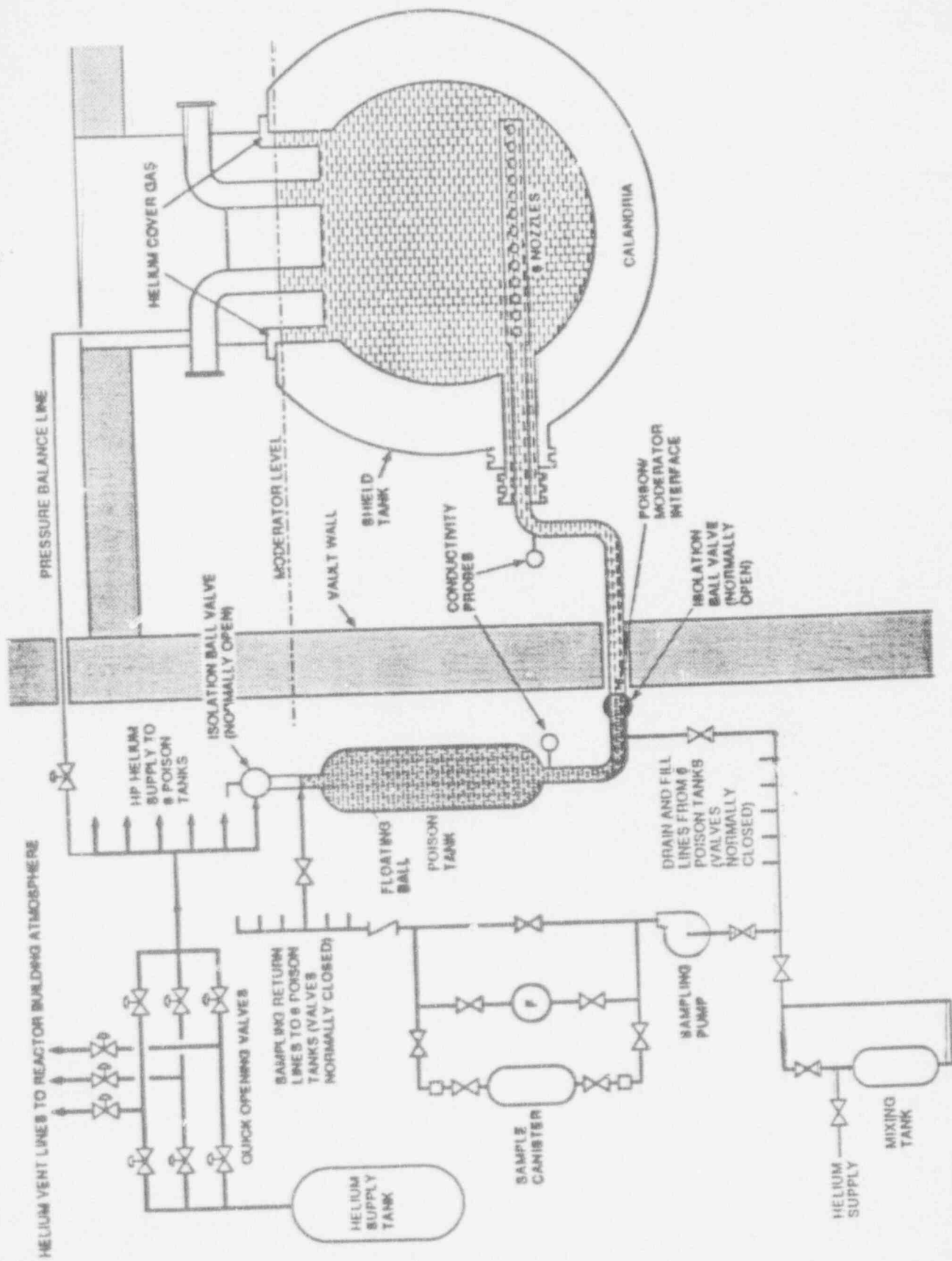


FIGURE 2.3.12-5 SHUTDOWN SYSTEM NO. 2 - BLOCK DIAGRAM



920386

FIGURE 2.3.12-6 SCHEMATIC DIAGRAM OF THE LIQUID INJECTION SYSTEM USED FOR SHUTDOWN SYSTEM NO. 2
CANDU 3

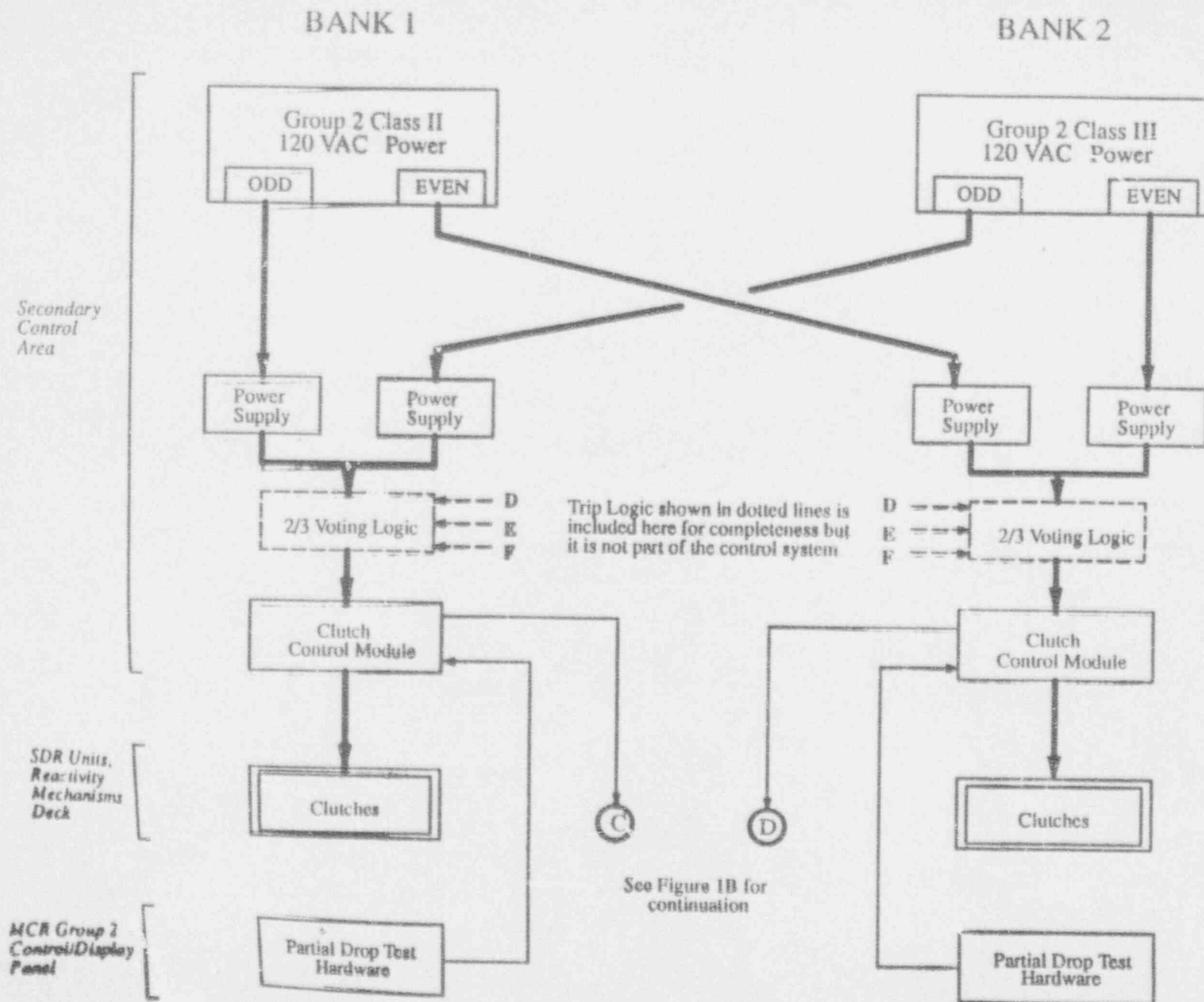


FIGURE 1A

SYSTEMS IMPORTANT TO SAFETY

- o Safety - Related - Functional definition essentially same for US and Canada
- o Safety - Grade (U.S.) - "Pedigree" definition: Category I, Quality Group C or better and I&C per IEEE-279.
- o U.S. Practice
 - 1. Important to Safety synonymous with Safety Related.
 - 2. Safety Related SSC must be Safety Grade
 - 3. In general, no credit for non-safety-related SSC. However, significant exceptions have been allowed.
- o Canadian Practice
 - 1. Graded pedigree requirements applied to SSC commensurate with the safety function to be performed.
 - 2. Credit given for function if SSC is appropriately qualified for the event in question.

QUALIFICATION OF SAFETY-RELATED SSC

o SDG-001 IDENTIFIES REQUIREMENTS

- Events
- Safety function to be performed
- Design requirements
- Requirements for
 1. Seismic
 2. Environmental
 3. Separation
 4. Fire Protection
 5. Code Classification
 6. Periodic inspection (pressure retaining)
 7. Tornado
 8. Pipe rupture effects