UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 31, 1994

Project No. 679

APPLICANT: ATOMIC ENERGY OF CANADA LIMITED TECHNOLOGIES

PROJECT: PREAPPLICATION REVIEW OF THE CANDU 3 REACTOR DESIGN

SUBJECT: SUMMARY OF MEETING HELD WITH AECLT TO DISCUSS TOPICS RELATED TO THE CANDU 3 REACTIVITY CHARACTERISTICS AND THE PENDING DESIGN CERTIFICATION APPLICATION

On March 15, 1994, the staff met with representatives of Atomic Energy of Canada Limited Technologies (AECLT) and AECL to discuss the CANDU 3 reactivity characteristics. The purpose of the meeting was to allow the staff to become more familiar with critical aspects of the design such as the reactivity characteristics, severe accident responses, and to discuss the pending design certification application.

Following the introductions, D. Hink, President AECLT opened up the presentation. Mr. Hink discussed the CANDU 3 program and background indicating that AECLT was on a ten year plan relating to design certification resources and schedules. Funding existed for NRC fees, design changes resulting from the review, as well as other support services. Mr. Hink stated that AECLT could support a 3- 5-year design certification review. Mr. Russell indicated that the NRC would be looking toward the longer end of the schedule range to plan its resource allocations. Mr. Russell ask for a specific date for the design certification application in order that NRC make the necessary plans to review the application. Presently, there were no resources allocated for the design certification only the preapplication review. Mr. Hink indicated that AECLT would send a letter by April 15, 1994, detailing the application date. He though that date would be August 1994.

Asked about the EPRI Requirements, AECLT indicated that the EPRI Requirements would be decoupled from the CANDU 3 application although they realized that they must address the EPRI Requrements Document related to appropriate CANDU 3 issues. They also understand the need to address operating experience, and plan to do so from a world-wide experience stand point.

Victor Snell discussed the evolution of the CANDU design. Stating that some of the reasons for the evolution of the CANDU reactors were the involvement in the 1940's with natural uranium, heavy water experimental facilities, the ability to alter the size of a CANDU reactor by changing the number of pressure tubes in the reactor, and the capability for on line refueling. One of the drawbacks of the CANDU technology is the positive coolant void reactivity. Reactor shut down must be accomplished in approximately 2 seconds for a worst case LOCA. To counter act the positive coolant void reactivity and accomplish a safe shut down in LOCA conditions, CANDU 3 has 2 fast acting independent and diverse shutdown systems; one mechanical and one liquid

poison. Each of these shutdown systems is independently capable of shutting the reactor down. Both systems measure core power and actuate at different power levels. The mechanical system (rods) would actuate first at some preset core power level then if the core power continues to increase the next set point is reached and the liquid poison system actuates.

The need for 2 shutdown systems came about as a result of the NRX accident in 1952. A series of operator errors resulted in extensive damage; fuel melting and hydrogen burning. The lesson learned from NRX was the need for a fast acting, independent, and reliable shut down system. Also, the reactivity control must be separate from the shutdown control.

The CANDU 3 physics and severe accidents were also discussed. Most of the severe accident effort on CANDU is a result of the CANDU 6 design development. AECL discussed the inherent cooling capability of the CANDU design. When a pressure tube is voided of its coolant, inherent cooling occurs as the pressure tube heats up, expands, and contacts the calandria tube: cooling is then effected through the moderator. AECL discussed the large break loss-of-coolant (LB LOCA) without scram accident previously assessed by the staff. If this accident were to occur, AECL expects early failure of a number of fuel channels, and significant fuel melting; however, failure of the first channel will create a steam bubble in the moderator and quickly shut the reactor down. AECL expects the frequency of this LB LOCA accident to be less than 10^{-9}/year. Presently, there has been no PRA done for CANDU 3.

Following the notification from AECLT of the application date, NRC plans to meet with the Atomic Energy Control Board and to visit a CANDU 6 facility. Enclosure 1 is a copy of the presentation view graphs and Enclosure 2 is a copy of the meeting attendees. The meeting was very informative to the staff and its consultants and went a long way to enhance the staff's knowledge of the design.

Original signed by:

Dino Scaletti, Sr. Project Manager
Advanced Reactors Project Directorate
Division of Advanced Reactor
and Special Project

Enclosures:
As stated

cc w/enclosures:
See next page

DISTRIBUTION:

Central File	PDR	PDAR R/F
WRussell/FMiraglia	ADPR/NRR	DCrutchfield
WTravers	GMarcus	DScaletti
EThrom	PShea	OGC
EJordan	NRC Participants	ACRS (10)

* See previous concurrence

OFFICE	LA:PDAR:ADAR*	PM:PDAR:ADAR	PD:PADR:ADAR
NAME	PShea	DScaletti	GMarcus
DATE	03/31/94	3/31/94	4/1/94

Document Name: CANDUSUM.315

poison. Each of these shutdown systems is independently capable of shutting the reactor down. Both systems measure core power and actuate at different power levels. The mechanical system (rods) would actuate first at some preset core power level then if the core power continues to increase the next set point is reached and the liquid poison system actuates.

The need for 2 shutdown systems came about as a result of the NRX accident in 1952. A series of operator errors resulted in extensive damage; fuel melting and hydrogen burning. The lesson learned from NRX was the need for a fast acting, independent, and reliable shut down system. Also, the reactivity control must be separate from the shutdown control.

The CANDU 3 physics and severe accidents were also discussed. Most of the severe accident effort on CANDU is a result of the CANDU 6 design development. AECL discussed the inherent cooling capability of the CANDU design. When a pressure tube is voided of its coolant, inherent cooling occurs as the pressure tube heats up, expands, and contacts the calandria tube: cooling is then effected through the moderator. AECL discussed the large break loss-of-coolant (LB LOCA) without scram accident previously assessed by the staff. If this accident were to occur, AECL expects early failure of a number of fuel channels, and significant fuel melting; however, failure of the first channel will create a steam bubble in the moderator and quickly shut the reactor down. AECL expects the frequency of this LB LOCA accident to be less than 10^{-9}/year. Presently, there has been no PRA done for CANDU 3.

Following the notification from AECLT of the application date, NRC plans to meet with the Atomic Energy Control Board and to visit a CANDU 6 facility. Enclosure 1 is a copy of the presentation view graphs and Enclosure 2 is a copy of the meeting attendees. The meeting was very informative to the staff and its consultants and went a long way to enhance the staff's knowledge of the design.

Original signed by:

Dino Scaletti, Sr. Project Manager
Advanced Reactors Project Directorate
Division of Advanced Reactor
and Special Project

Enclosures:
As stated

cc w/enclosures:
See next page

DISTRIBUTION:

Central File	PDR	PDAR R/F
WRussell/FMiraglia	ADPR/NRR	DCrutchfield
WTravers	GMarcus	DScaletti
EThrom	PShea	OGC
EJordan	NRC Participants	ACRS (10)

* See previous concurrence

OFFICE	LA:PDAR:ADAR*	PM:PDAR:ADAR	PD:PADR:ADAR
NAME	PShea	DScaletti	GMarcus
DATE	03/31/94	3/31/94	2/1/94

Document Name: CANDUSUM.315

poison. Each of these shutdown systems is independently capable of shutting the reactor down. Both systems measure core power and actuate at different power levels. The mechanical system (rods) would actuate first at some preset core power level then if the core power continues to increase the next set point is reached and the liquid poison system actuates.

The need for 2 shutdown systems came about as a result of the NRX accident in 1952. A series of operator errors resulted in extensive damage; fuel melting and hydrogen burning. The lesson learned from NRX was the need for a fast acting, independent, and reliable shut down system. Also, the reactivity control must be separate from the shutdown control.

The CANDU 3 physics and severe accidents were also discussed. Most of the severe accident effort on CANDU is a result of the CANDU 6 design development. AECL discussed the inherent cooling capability of the CANDU design. When a pressure tube is voided of its coolant, inherent cooling occurs as the pressure tube heats up, expands, and contacts the calandria tube: cooling is then effected through the moderator. AECL discussed the large break loss-of-coolant (LB LOCA) without scram accident previously assessed by the staff. If this accident were to occur, AECL expects early failure of a number of fuel channels, and significant fuel melting; however, failure of the first channel will create a steam bubble in the moderator and quickly shut the reactor down. AECL expects the frequency of this LB LOCA accident to be less than 10^{-9}/year. Presently, there has been no PRA done for CANDU 3.

Following the notification from AECLT of the application date, NRC plans to meet with the Atomic Energy Control Board and to visit a CANDU 6 facility. Enclosure 1 is a copy of the presentation view graphs and Enclosure 2 is a copy of the meeting attendees. The meeting was very informative to the staff and its consultants and went a long way to enhance the staff's knowledge of the design.

Dino Scaletti

Dino Scaletti, Sr. Project Manager
Advanced Reactors Project Directorate
Division of Advanced Reactor
and Special Project

Enclosures:
As stated

cc w/enclosures:
See next page

CANDU
Project No. 679

cc: Louis N. Rib, Licensing Consultant
AECL Technologies
9210 Corporate Boulevard, Suite 410
Rockville, Maryland 20850

Bernie Ewing, Manager
Studies and Codification Division
Atomic Energy Control Board
P.O. Box 1046, Station B
270 Albert Street
Ottawa, Ontario, Canada K1P 5S9

A.M. Mortada Aly, Senior Project Officer
Advanced Projects Licensing Group
Studies and Codification Division
Atomic Energy Control Board
P.O. Box 1046, Station B
270 Albert Street
Ottawa, Ontario, Canada K1P 5S9

Project Director - CANDU-3
AECL CANDU
2251 Speakman Drive
Mississaugua, Ontario, Canada L5K 1B2

L. Manning Muntzing
Newman & Holtzinger, P.C.
1615 L Street, N.W., Suite 1000
Washington, D.C. 20036

Steve Goldberg, Budget Examiner
Office of Management and Budget
725 17th Street, NW.
Washington, D.C. 20503

A.D. Hink
Vice President/General Manager
AECL Technologies
9210 Corporate Boulevard, Suite 410
Rockville, Maryland 20850

Enclosure 1

MEETING NRC/AECLT ATTENDEES LIST
March 15, 1994

NAME	ORGANIZATION
D. Scaletti	NRR/ADAR/PDAR
P. Chan	AECL/CANDU
D. Wright	AECL/CANDU
L. A. Simpson	AECL/RESEARCH
E. Throm	NRR/ADAR/PDAR
V. Snell	AECL-T
S. Hink	AECL-T
L. Rib	AECLT
R. Meyer	NRC/RES
M. Fletcher	AECLT
N. Ichiyen	AECL/CANDU
P. Kohut	BNL
D. Dill	NRC/SRXB
R. Landry	NRR/ADAR/PDAR
C. Slovik	BNL
[illegible]. King	NRC/RES
G. Thomes	NRC/NRR
D. Carlson	NRC/RES
M. Virgilio	NRC/NRR
C. McCracken	NRC/NRR
C. Carpenter	NRCC/NRR/DSSA
R. Durante	AECL-T
D. Ebert	NRC/RES
H. Richines	NRC/SRXB
D. Desaulniers	NRC/HHFB
R. Eckenrode	NRC/HHFB
D. Crutchfield	NRC/NRR
W. Travers	NRC/NRR
F. Eltawila	NRC/RES
D. McPherson	NRC/NRR
M. Chiramak	NRR/HICB
K. Mortensen	NRR/HICB
M. Case	NRR/ADAR
L. Shotkin	NRC/RES/DSR
R. Kirkwood	AECL-T
F. Talbot	NRC/NRR/RPEB
P. Wigfull	AGCR
G. Marcus	NRR/PDAR
P. Allen	AECL/CANDU
S. Grant	AECL/CANDU
R. K. McCardell	EGG/INEL
D. M. M. Aly	AECB/DRR
R. L. Ferguson	AECL-T
F. W. Sciacca	SEA
N. Saltos	NRC/NRR/SPSB

CANDU REACTIVITY CHARACTERISTICS

Presentation by
AECL-Technologies Inc.
March 1994

ATOMIC ENERGY
OF CANADA, LTD.

BOARD OF DIRECTORS
AECL TECHNOLOGIES INC.

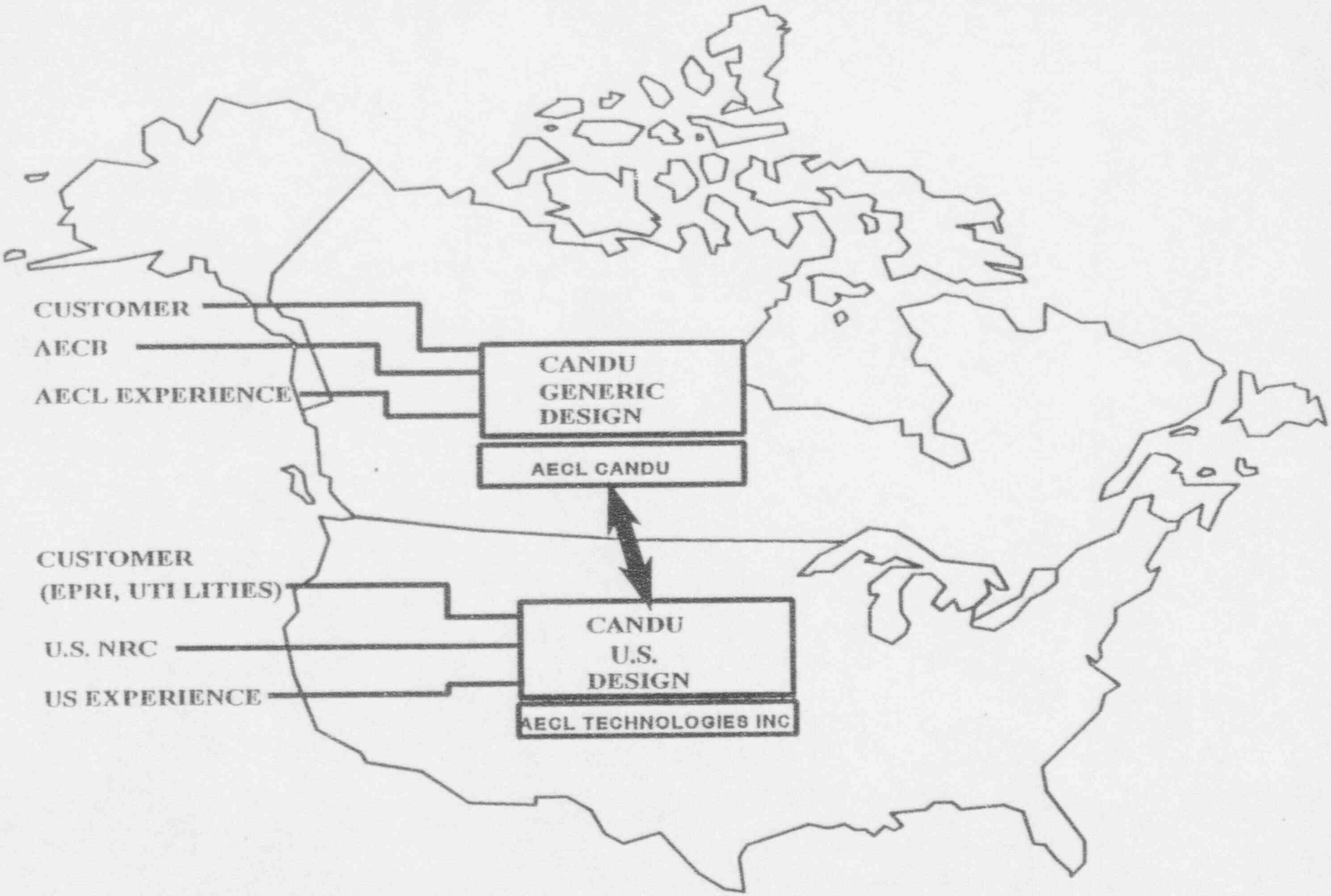
AECL TECHNOLOGIES INC.
A.D. HINK, PRESIDENT

- USCANDU
- MARKETING & SALES
- PROJECT & OPERATIONS

CANDU 3 PROGRAM BACKGROUND

- BEGAN 1987
- BASED ON SUCCESSFUL CANDU 6
- TARGETED AT MARKET FOR SMALLER PLANTS
- ANTICIPATES SECOND PHASE OF COMMERCIALIZATION

AECL Technologies Inc.



BENEFIT & CHALLENGES

- CANDU INCORPORATED TECHNOLOGIES MAY HAVE A BROADER USE
  - CADDS DESIGN & DOCUMENT CONTROL
  - AUTOMATED DIGITAL SAFETY SYSTEM ACTIVATION
  - ON-LINE RELIABILITY TEST CAPABILITY
- REVIEW CANDU 3 SPD vs NRC PWR REQUIREMENTS
- DESIGN CHANGES vs EQUIVALENT SAFETY LOGIC

BACKGROUND

- Application for SDC for CANDU 3
  - Evolutionary Design (27 Larger CANDUs Operating)
- Continues Dialogue with NRC
  - Letter of Intent May 25, 1989
  - Meetings with NRR, RES, ACRS on Pre-Application Process & Policy Issues
  - Submittal of Equivalent Safety Reviews
- Policy Issues Identified by NRC Staff & Commission, Some Concurrence, Some Outstanding
- One of the Key Issues: Reactivity Characteristics

PURPOSE OF THE MEETING

- To Provide an Integrated Set of Information to Help NRC Review
- To Initiate Dialogue on Requirements for Resolving this Policy Issue

AECL Technologies Inc.

AGENDA
CANDU REACTIVITY CHARACTERISTICS
Washington, 1994

ITEM	SPEAKER	TIME (questions additional)
Purpose and Introduction of Speakers	A.D. Hink	25 mins
Evolution of CANDU design	V.G. Snell	45 mins
CANDU physics	P. Chan	1.5 hours
Shutdown systems concept & design	N. Ichiyen	1 hour
Severe accidents	P. Allen	1 hour

EVOLUTION OF CANDU DESIGN

CONCEPT BASIS

IMPLICATIONS OF CONCEPT BASIS

SAFETY DESIGN APPROACH

SEVERE ACCIDENTS

CONCEPT BASIS

- natural uranium, heavy-water
  - ZEEP (1945)
  - NRX (1947)
    - * heavy-water moderated, light-water cooled
  - independence in fuel supply

- heavy-water coolant

- pressure tubes
  - scale-up to larger size
  - on-power refuelling
  - NPD (1962)

IMPLICATIONS OF CONCEPT BASIS

- limited reactivity holdup due to on-power refuelling
  - total short-term movable reactivity ~ 3$
  - max. reactivity in any one device ~ 0.3$
  - core geometry near reactivity maximum
  - no changes in core state after initial operation

IMPLICATIONS OF CONCEPT BASIS - cont'd

- reactivity devices in moderator, not coolant
  - no pressure-assisted ejection
  - no hydraulic forces on shutdown systems for large LOCA
- long prompt neutron lifetime
  - 0.9 ms or 20X larger than LWRs
  - no abrupt change in behaviour for hypothetical reactivity insertions above prompt critical

IMPLICATIONS OF CONCEPT BASIS - cont'd

- decoupling of moderator reactivity coefficients
    - negative feedback in certain severe accidents

- no poison in the coolant

- relatively large core, spatial control

- prompt negative feedback from Doppler effect
    - simple mechanical reactivity control

IMPLICATIONS OF CONCEPT BASIS - cont'd

- positive coolant void coefficient
  - rate limited by hydraulics (< 0.6 $ in 0.3 sec. for worst LOCA)
  - slower for loss of RCS pumps, loss of pressure control
  - requires shutdown within ~ 2 sec. for worst LOCA
  - can use mechanical or hydraulic devices

IMPLICATIONS OF CONCEPT BASIS - cont'd

- inherent negative feedback for:

  1. cold or light water injection
     - no need to borate ECC

  2. steam-line break

  3. turbine stop-valve closure

SAFETY DESIGN APPROACH

- NRX accident (1952)
    - complex shutdown system & common-cause failure of several rods
    - terminated by rupture of a few channels and "dumping the polymer"
- tolerate DBA + unavailability of special safety system (ECCS, shutdown system, active part of containment)

SAFETY DESIGN APPROACH - cont'd

- options:

  1. analyze DBA's without shutdown

  2. provide redundant & diverse shutdown systems

- modern CANDUs use option 2

  - increases real safety
  - avoids speculative analysis
  - now regulatory requirement

SAFETY DESIGN APPROACH - cont'd

- shutdown system requirements:
  - diverse in design, operation, maintenance
  - independent of each other and control system
  - tested regularly at power to demonstrate availability of 0.999
  - each system fully effective for all DBAs (to cold shutdown)

SAFETY DESIGN APPROACH - cont'd

- control system independently capable of shutdown for Anticipated Transients & some DBAs

- two lines of defense for low-frequency DBAs (e.g., LOCA)

- three lines of defense for Anticipated Transients (e.g., loss of RCS pumps)

SEVERE ACCIDENTS

- some severe accidents part of Canadian design basis, e.g.:
  - LOCA plus failure of containment isolation
  - LOCA plus unavailability of ECC injection

- core melt precluded by moderator

SEVERE ACCIDENTS

- some severe accidents part of Canadian design basis, e.g.:
  - LOCA plus failure of containment isolation
  - LOCA plus unavailability of ECC injection

- core melt precluded by moderator

SEVERE ACCIDENTS - cont'd

- combined failure approach forces redundancy in safety function at system level
  - Group 1 & Group 2 feedwater
  - Group 1 & Group 2 diesels

SEVERE ACCIDENTS - cont'd

- for reactivity accidents, relevant combination is:

Initiating event

+

Failure of RRS (if otherwise effective)

+

Failure of SDS1

+

Failure of SDS2

SEVERE ACCIDENTS - cont'd

- most demanding initiating event is large LOCA with NO shutdown

- incoherent failure of individual channels due to local overheating

- terminated by moderator void & loss of lattice geometry (SDS3!)

SEVERE ACCIDENTS - cont'd

- design inherently:
  - precludes coherent failure of pressure boundary consequent to unterminated overpower accident
  - does not require fuel movement for shutdown
  - contains a "fuse" which limits the energy generation

CONCLUSIONS

- as in all reactors, uncompensated reactivity accidents can lead to core damage

- time scale relatively slow in CANDU

- design approach has been to prevent with dual demonstrably reliable shutdown systems

- CANDU "fuse" inherently limits the energy available

AECL EACL

AECL CANDU EACL CANDU

CANDU PHYSICS

Peter Chan

- Reactivity Coefficients
- Reactivity Perturbations
- Effect of D_2O on Neutronic Transients

Reactivity Coefficients

- Fuel Temperature
- Coolant Temperature
- Coolant Void
- Moderator Temperature
- Power

Definition of Some Terms Used in CANDU Physics

- Reactivity is expressed in milli–k (mk)

  6 mk ≈ \$1 for CANDU 3

- Fuel Irradiation is expressed in n/kb

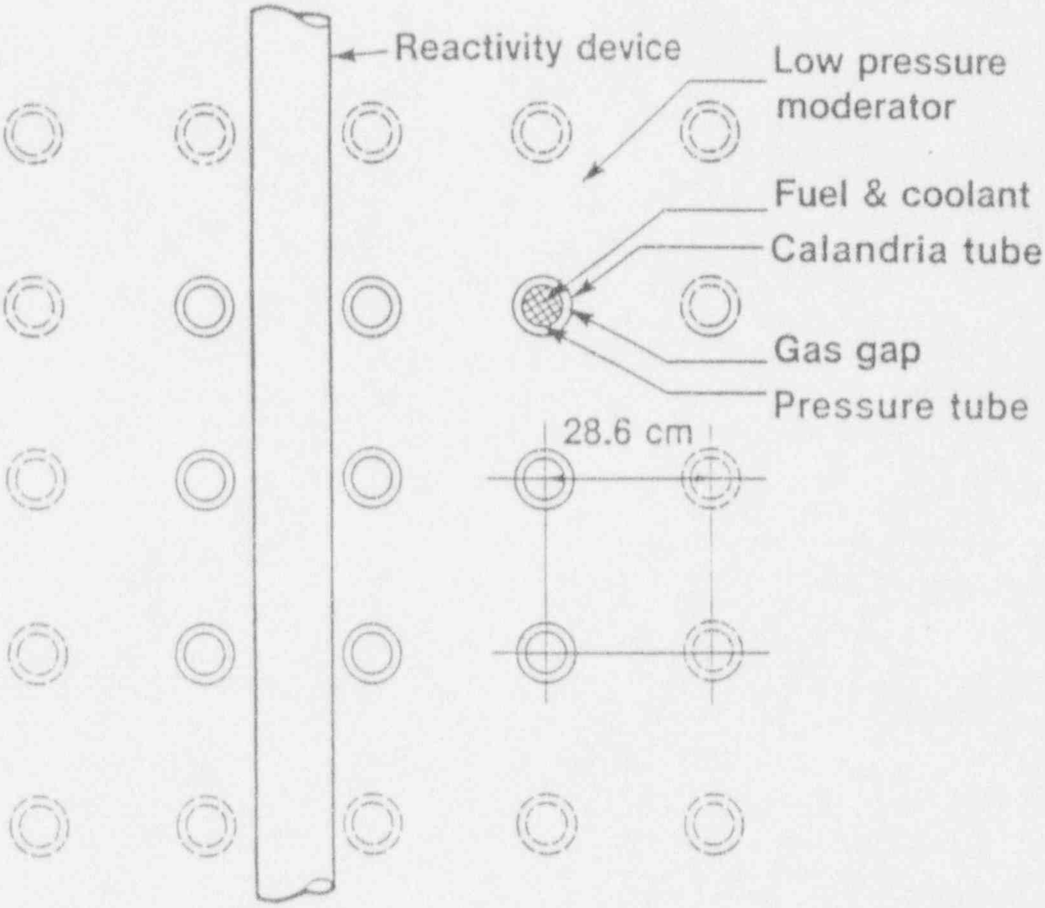
  1 n/kb ≈ 4100 MWD/tU

EFFECT OF D_2O AND H_2O ON REACTOR SIZE

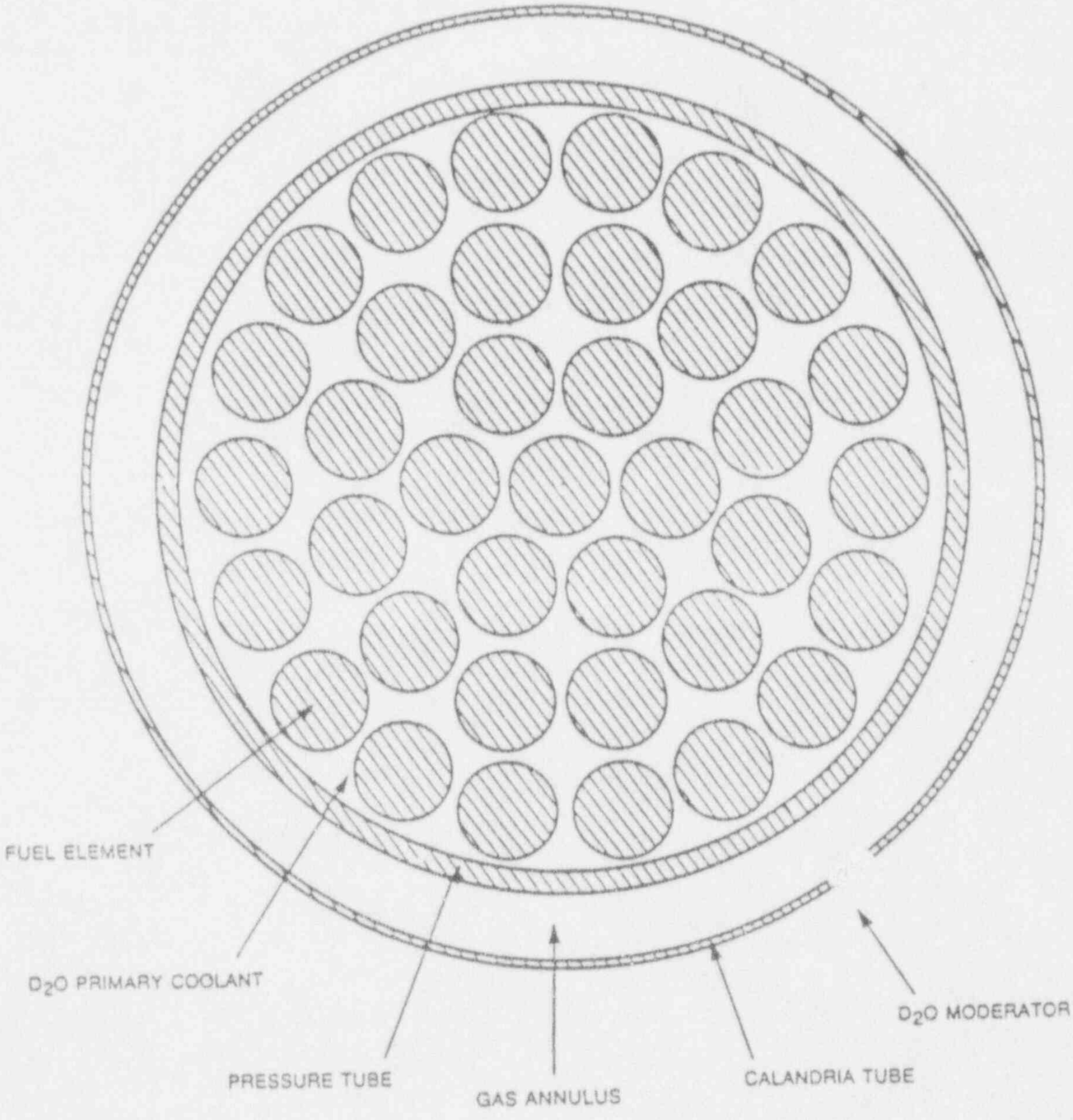
	D_2O	H_2O
Migration Length (Core)	20 cm.	6 cm.
Migration Length (Reflector)	100 cm.	6.5 cm.

Effects of Large Migration Length in D_2O Lattice

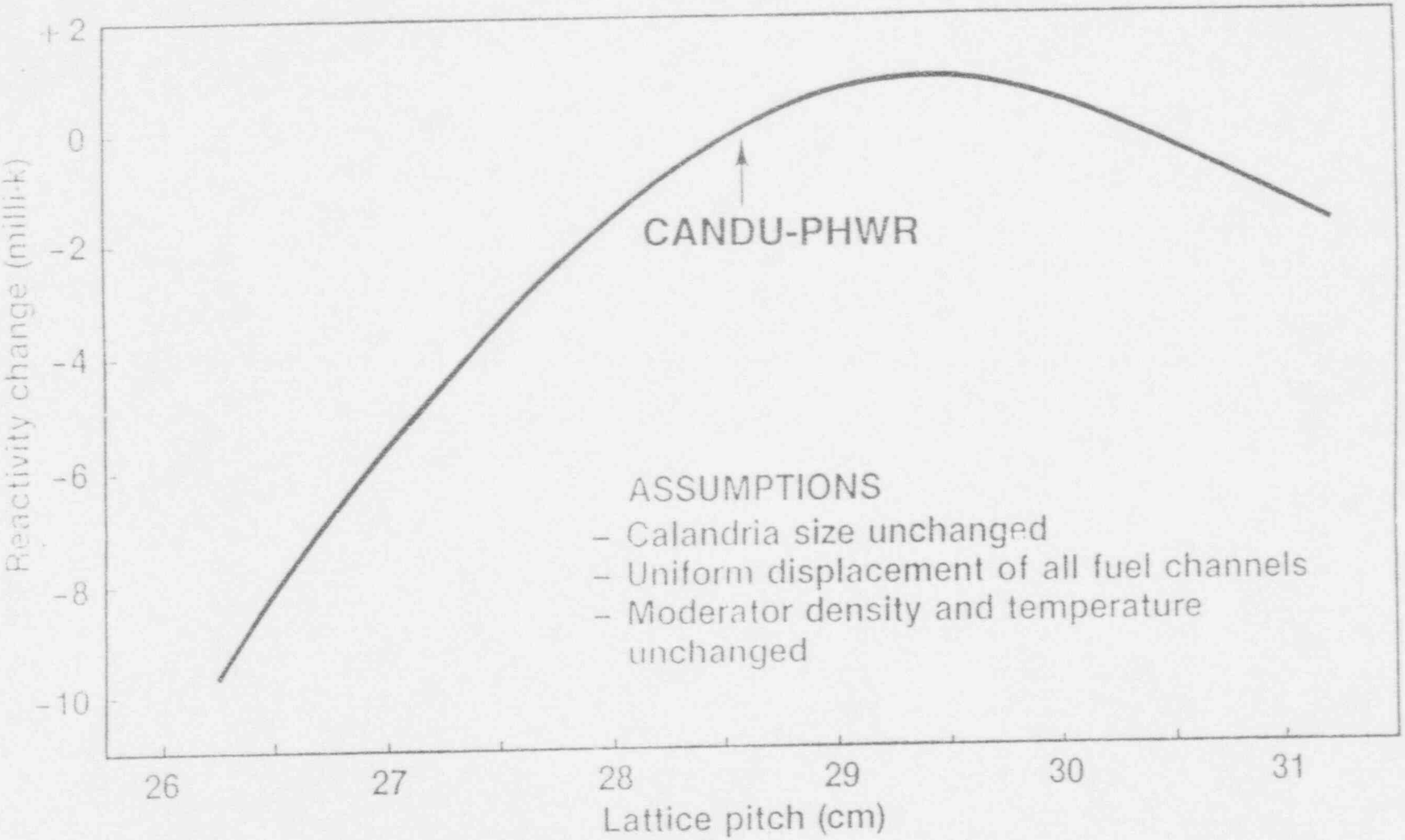
- Pressure tube design
- Separation of high temperature and high pressure coolant from low temperature and low pressure moderator
- Reactivity control devices are placed in the moderator environment between fuel channels
- Insensitive to rod ejection and crash cooling scenarios



Schematic of CANDU–PHW Lattice

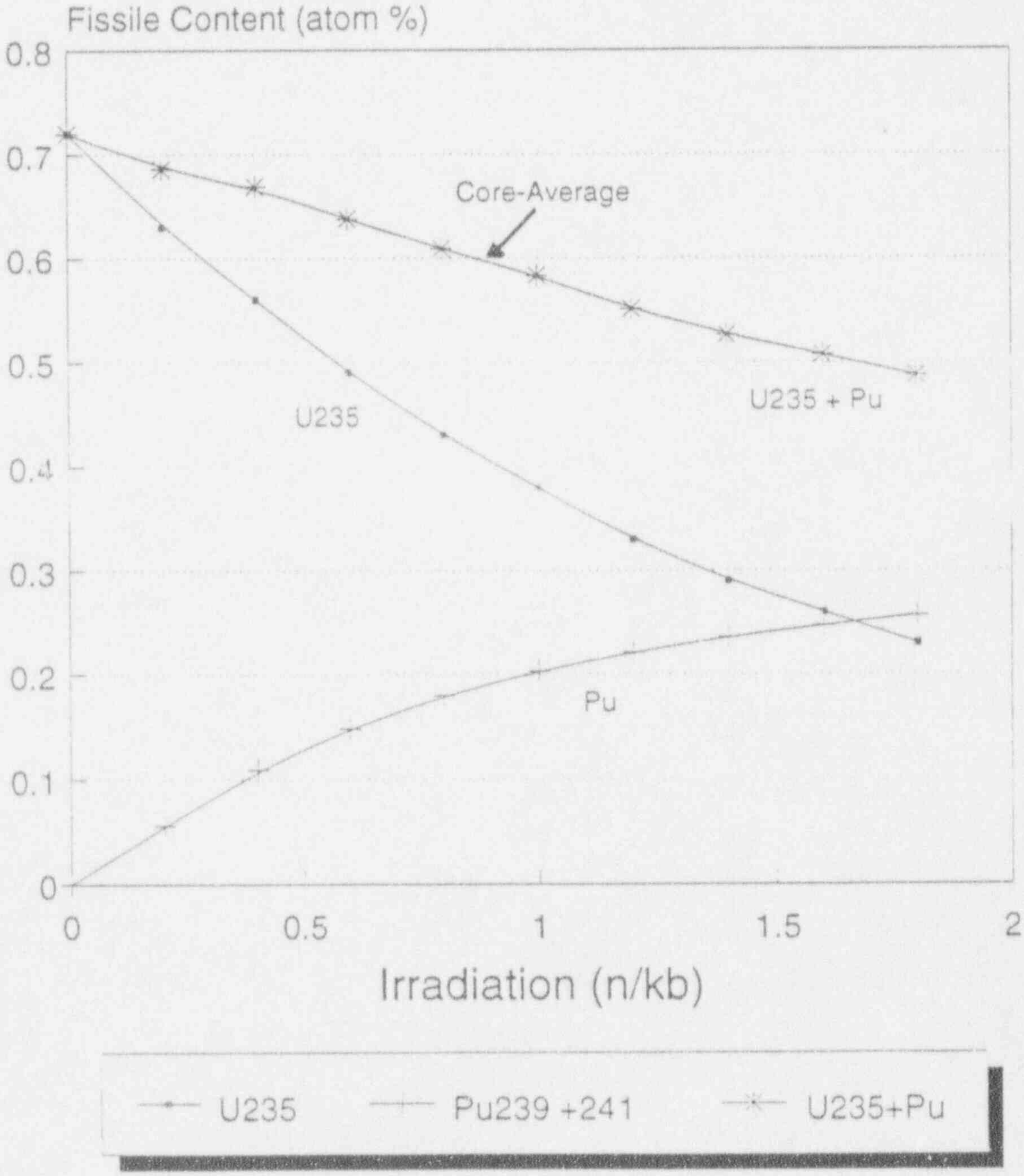


37 Element Fuel Lattice



Variation of Reactivity with Lattice Pitch for CANDU–PHW Lattice

Fissile Content In CANDU Fuel vs. Irradiation



AECL EACL

AECL CANDU EACL CANDU

FEEDBACK REACTIVITY COEFFICIENTS IN CANDU AND LWR

	CANDU	LWR
Fuel Temperature Coefficient	–4.1 μk/°C	–18 μk/°C
Coolant Temperature "	+37.5 μk/°C	
Coolant Void "	+12.7 mk/(gm/cc)	
Moderator Temperature "	+100 μk/°C*	–630 μk/°C

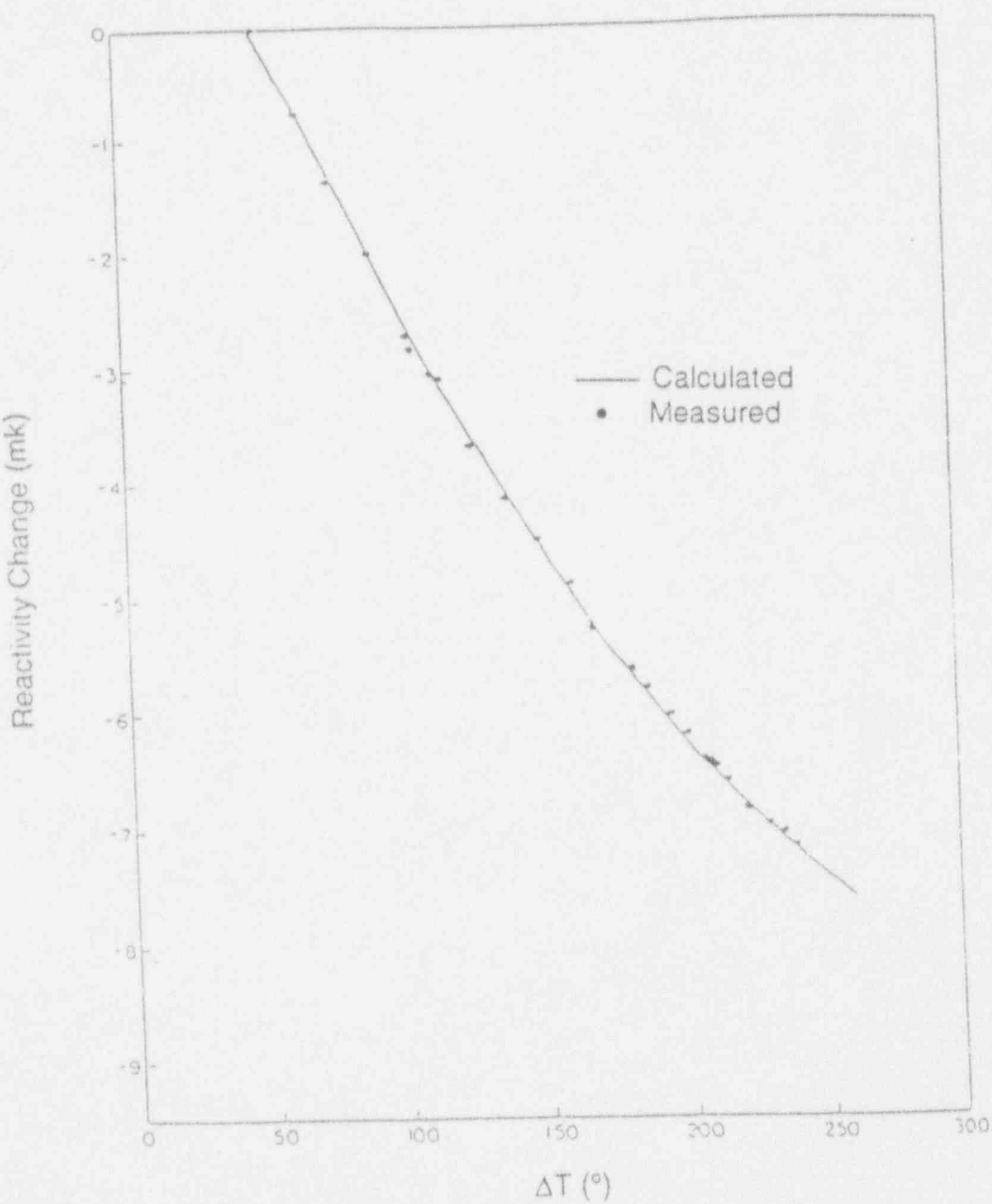
* Insensitive to crash cooling

AECL EACL

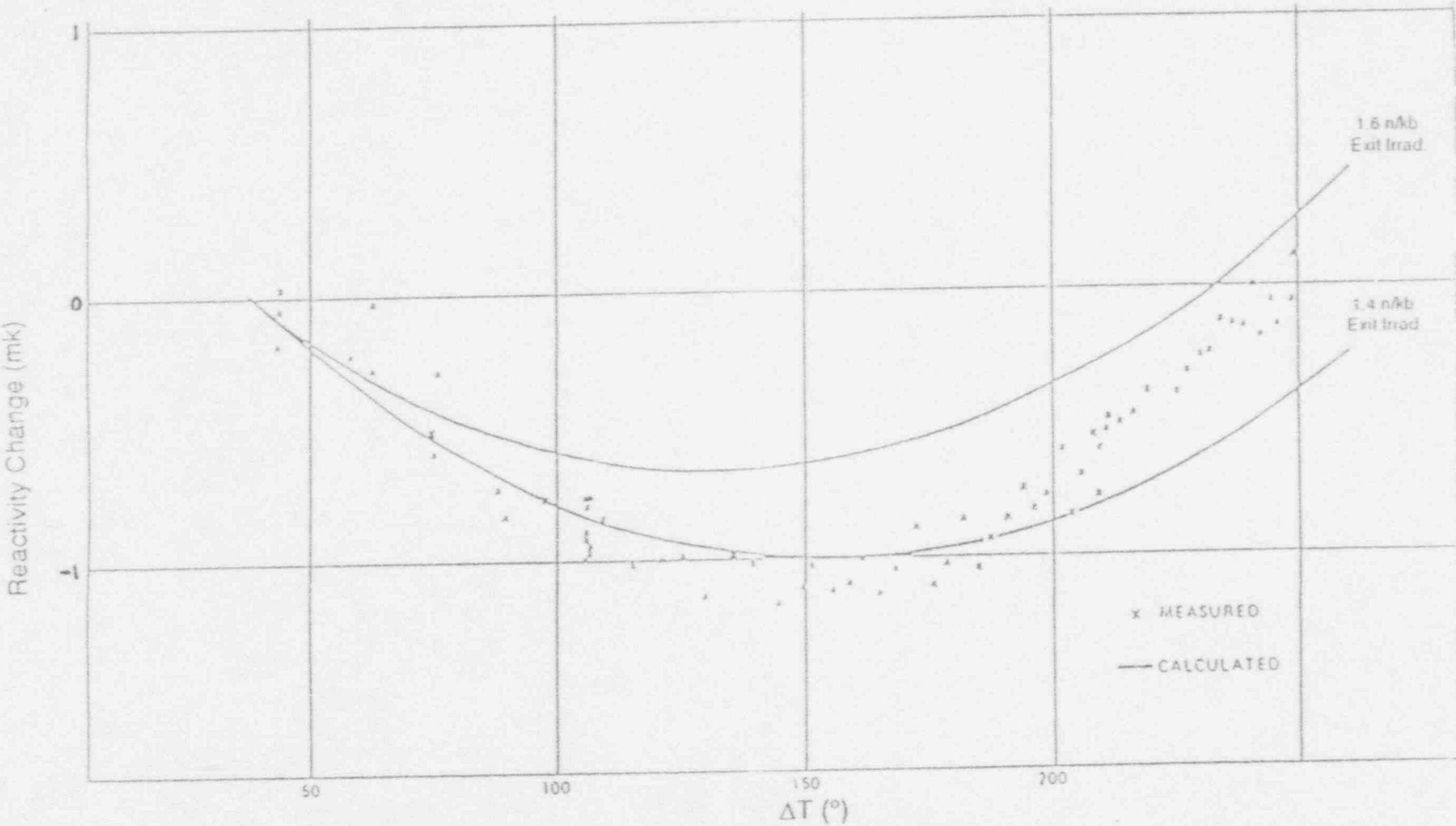
AECL CANDU EACL CANDU

POWER COEFFICIENT

- Negative Fuel Temperature Feedback
- Positive Coolant Temperature (density) Feedback
- Redistribution of Flux/Power Shapes
- Change In Leakage Due to Change in Flux Shape
- Near Zero Under Nominal Conditions
- Supported by Measurements In Operating Stations



Bruce–A Unit 2 Initial Startup, Measured and Calculated Reactivity Change Due to Heat Transport System Temperature Change



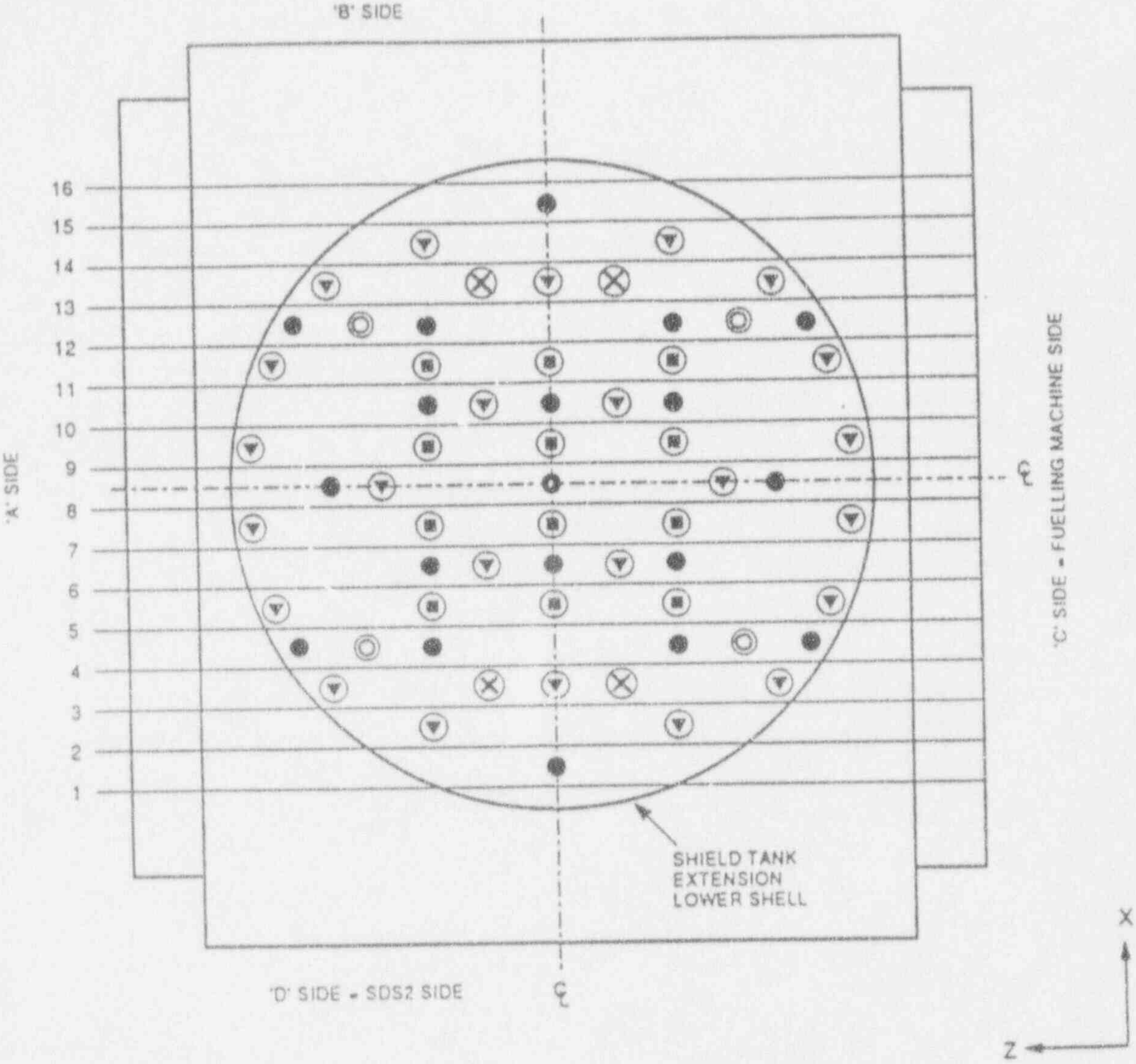
Comparison of Measured and Calculated Reactivity Changes Due to Fuel and Coolant Temperature in Pickering 'A', Unit 4 (Irradiated Fuel)

AECL EACL

AECL CANDU EACL CANDU

Reactivity Perturbations

- Reactivity Devices
- On-Power Fuelling
- Spatial Control and Xenon Effects



MECHANICAL ZONE CONTROL (MZC) (4)

ADJUSTER (ADJ) (12)

MECHANICAL CONTROL ABSORBER (MCA) (4)

VERTICAL FLUX DETECTOR (VFD) (19)

MECHANICAL SHUTDOWN ROD (SDR) (24)

General Arrangement of Reactivity Control Devices

AECL EACL

AECL CANDU EACL CANDU

REACTIVITY DEVICES, WORTHS AND MAXIMUM RATES

Function	Device	Total Reactivity Worth (mk)	Maximum Reactivity Rate (mk/s)
Control	8 Mech. Zone Controllers	5	±0.12
Control	12 Adjuster Rods	12	±0.08
Control	4 Mechanical Control Absorbers	10	±0.075(driving) –3.5 (dropping)
Control	Moderator Poison	–	–0.01(adding) +0.001(extracting)
Safety	24 Shutoff Rods	–94	–50
Safety	6 Poison Injection nozzles	–200	–50

General Features of On-Power Fuelling

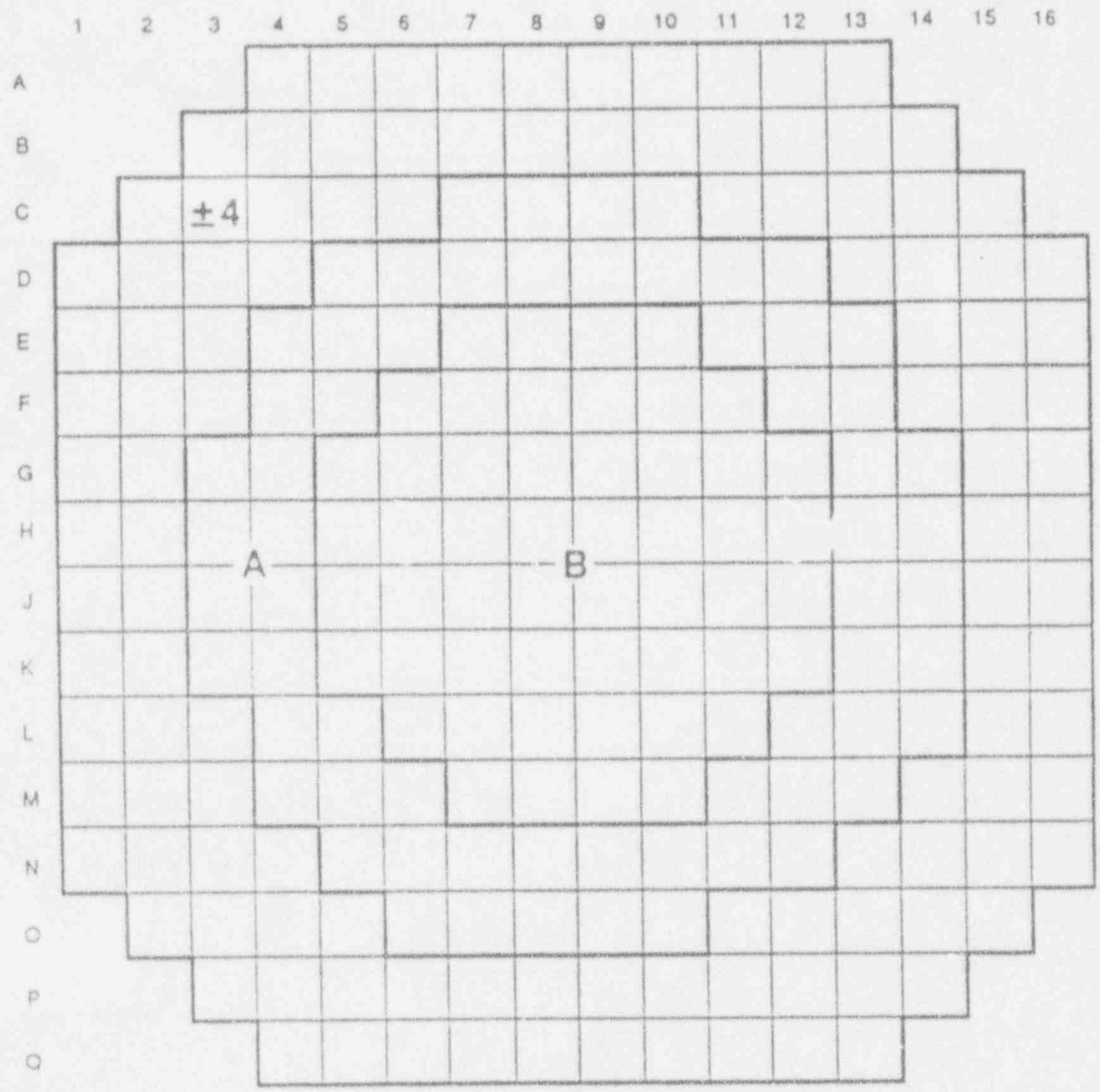
- Global power distribution is predictable
- Local deviations from the global power shape is small
- Small built-in excess reactivity
- Small reactivity perturbations

AECL EACL

AECL CANDU EACL CANDU

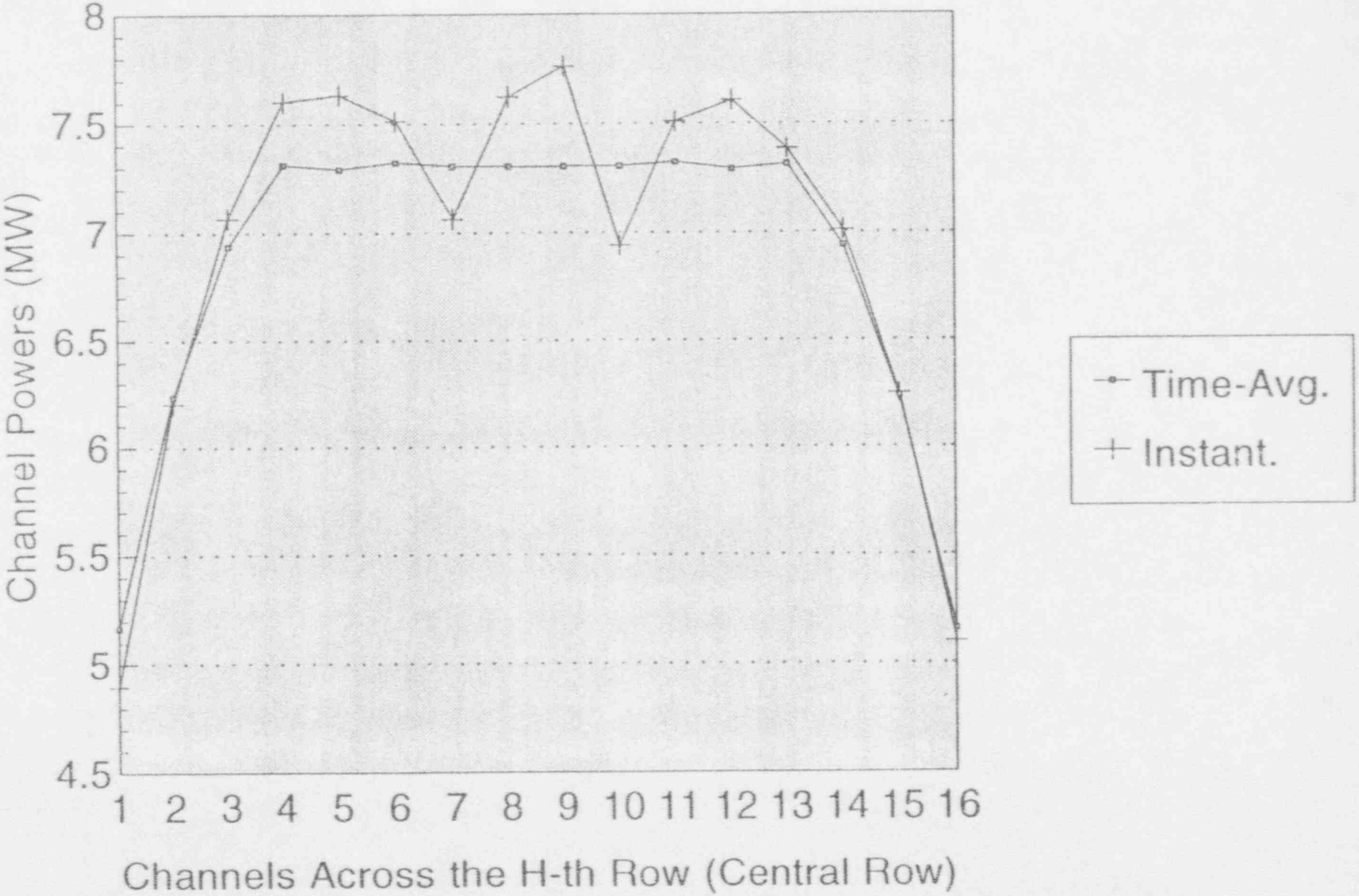
Reactivity Effect of Refuelling in CANDU 3

Total Thermal Power (MW)	1370.4
Average Discharge Burnup (MWd/tU)	6167.
Average Refuelling Rate	
Channels/FPD	3.
Bundles/FPD	12.1
% of Fuel in Core	0.4
Average Reactivity Decay Rate (mk/FPD)	–0.44
Average Reactivity Increase per Channel Refuelled (mk)	0.15

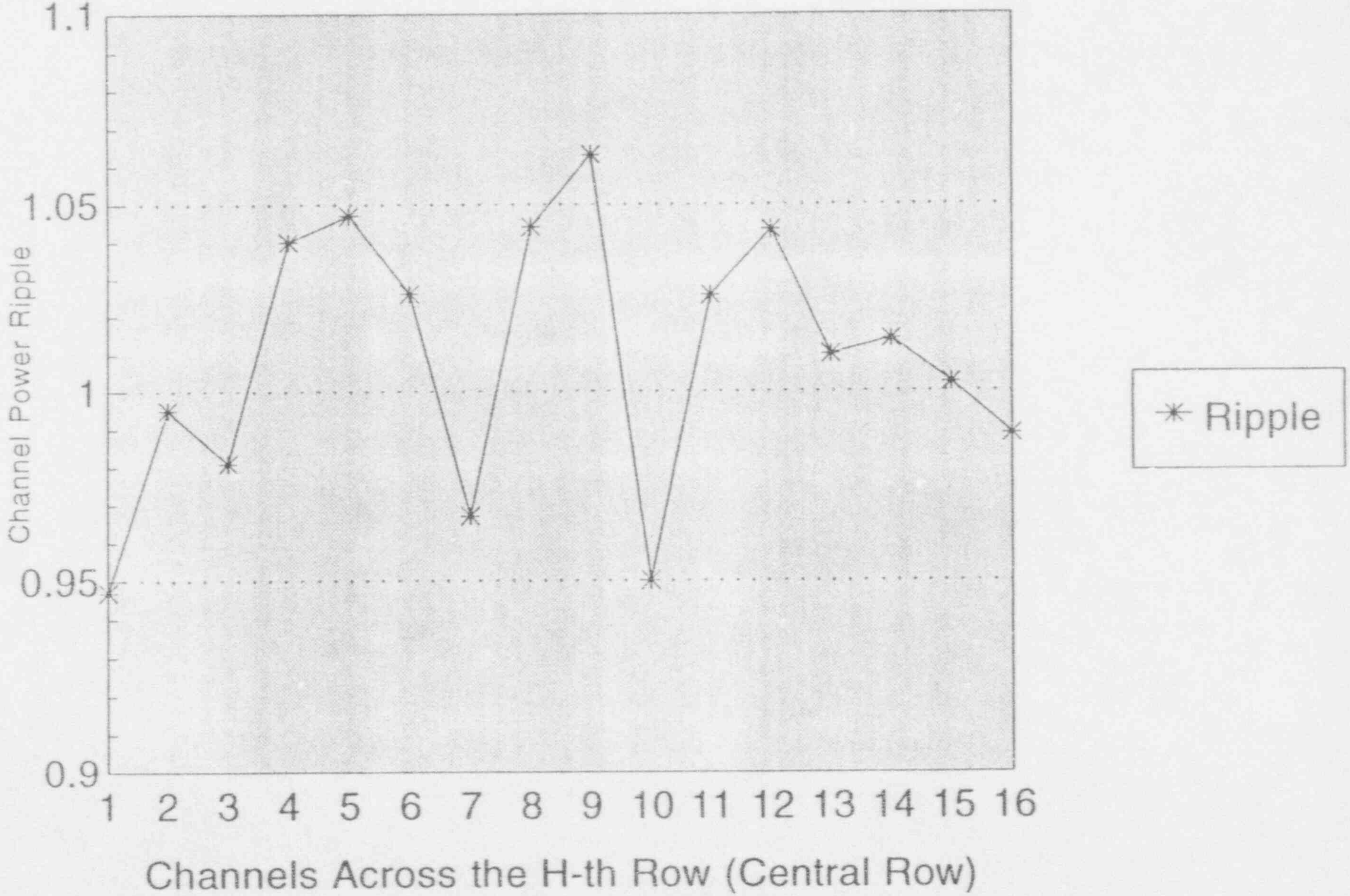


Refuelling Zones and Schemes

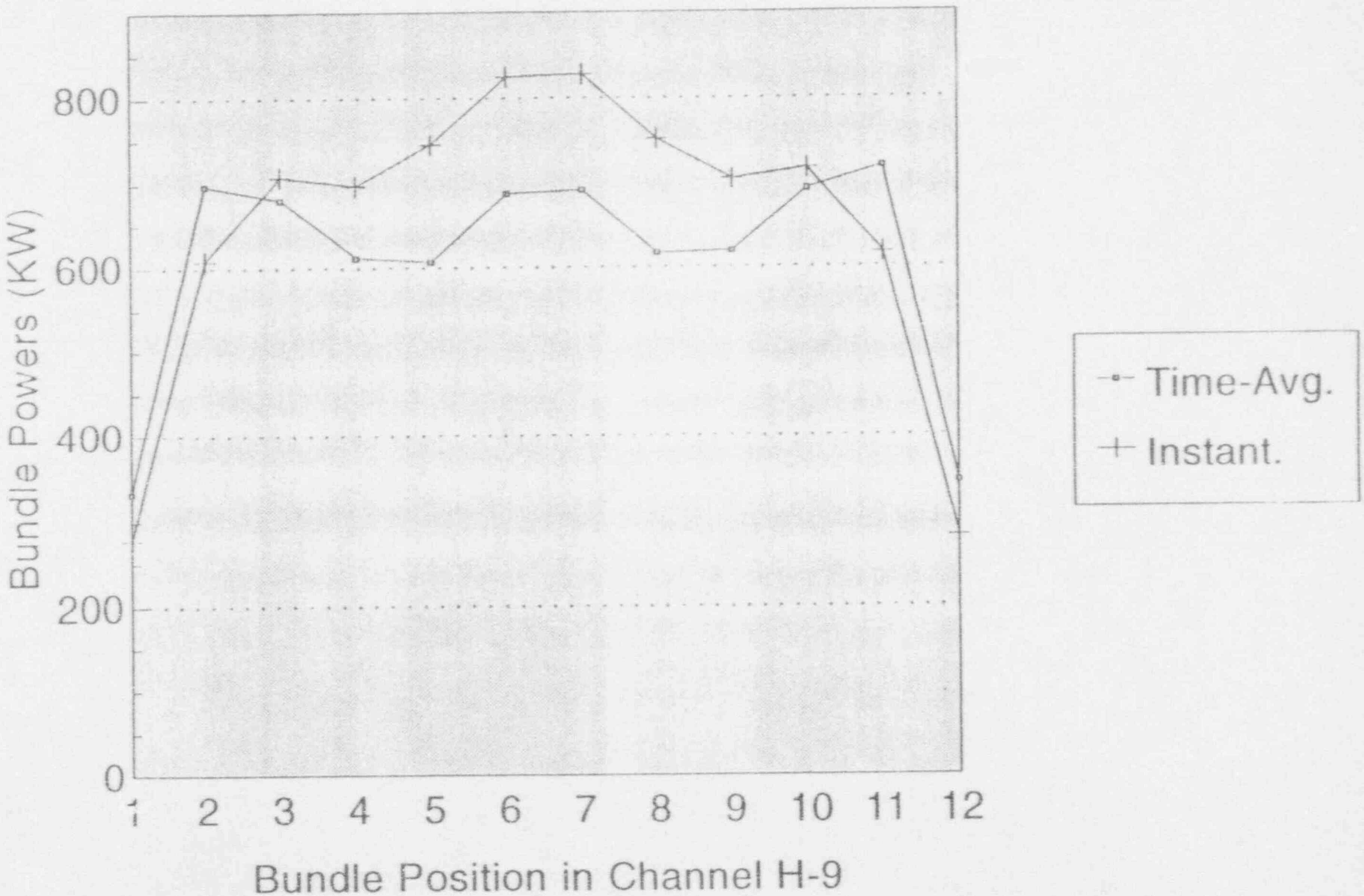
Radial Power Distribution in CANDU 3



Channel Power Ripples in CANDU 3



Bundle Power Distribution in CANDU 3

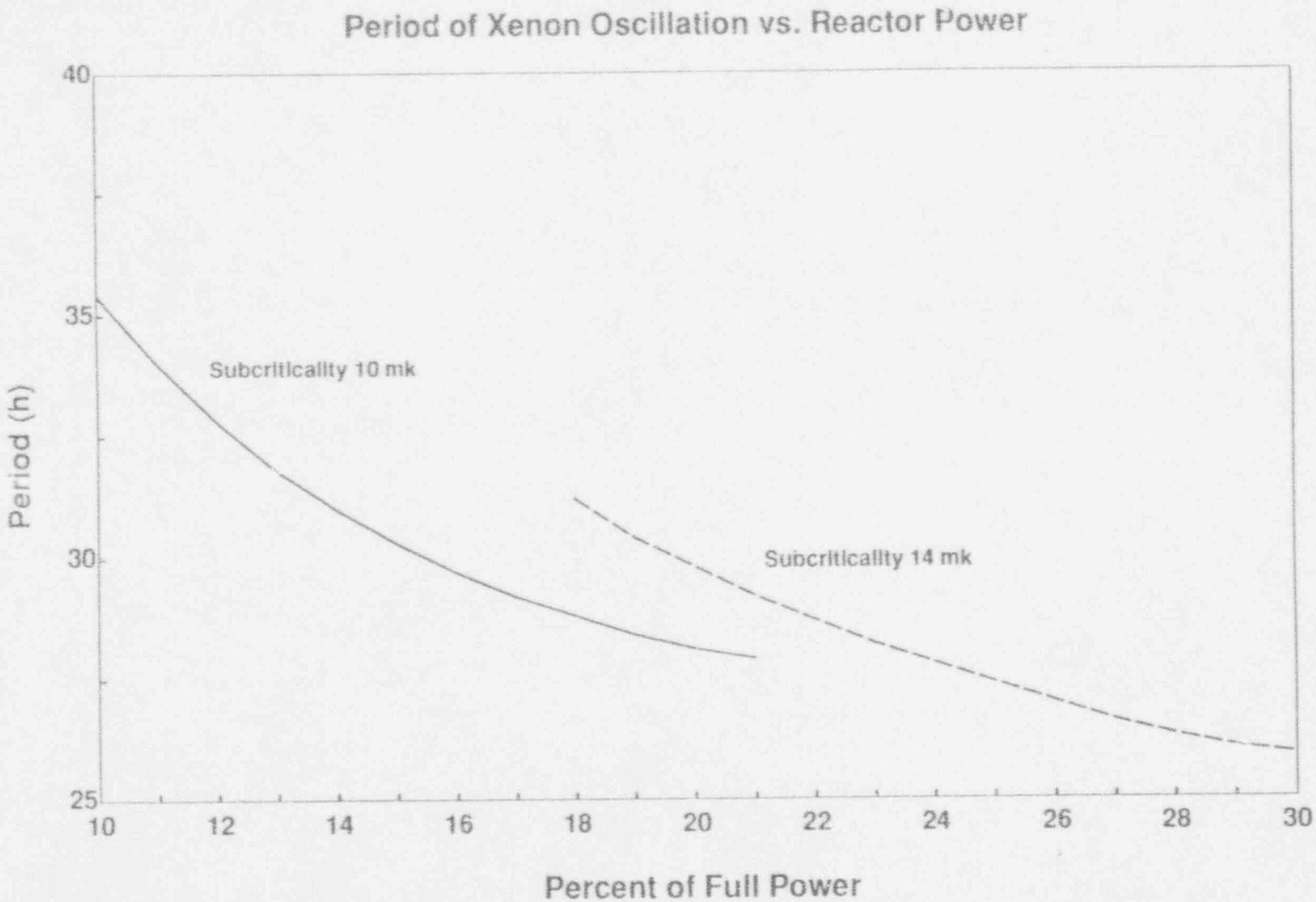


Xenon Effects

- Caused by power perturbations

- Most likely modes of xenon-induced power oscillations are:
  - First azimuthal (top to bottom)
  - First axial (front to back)

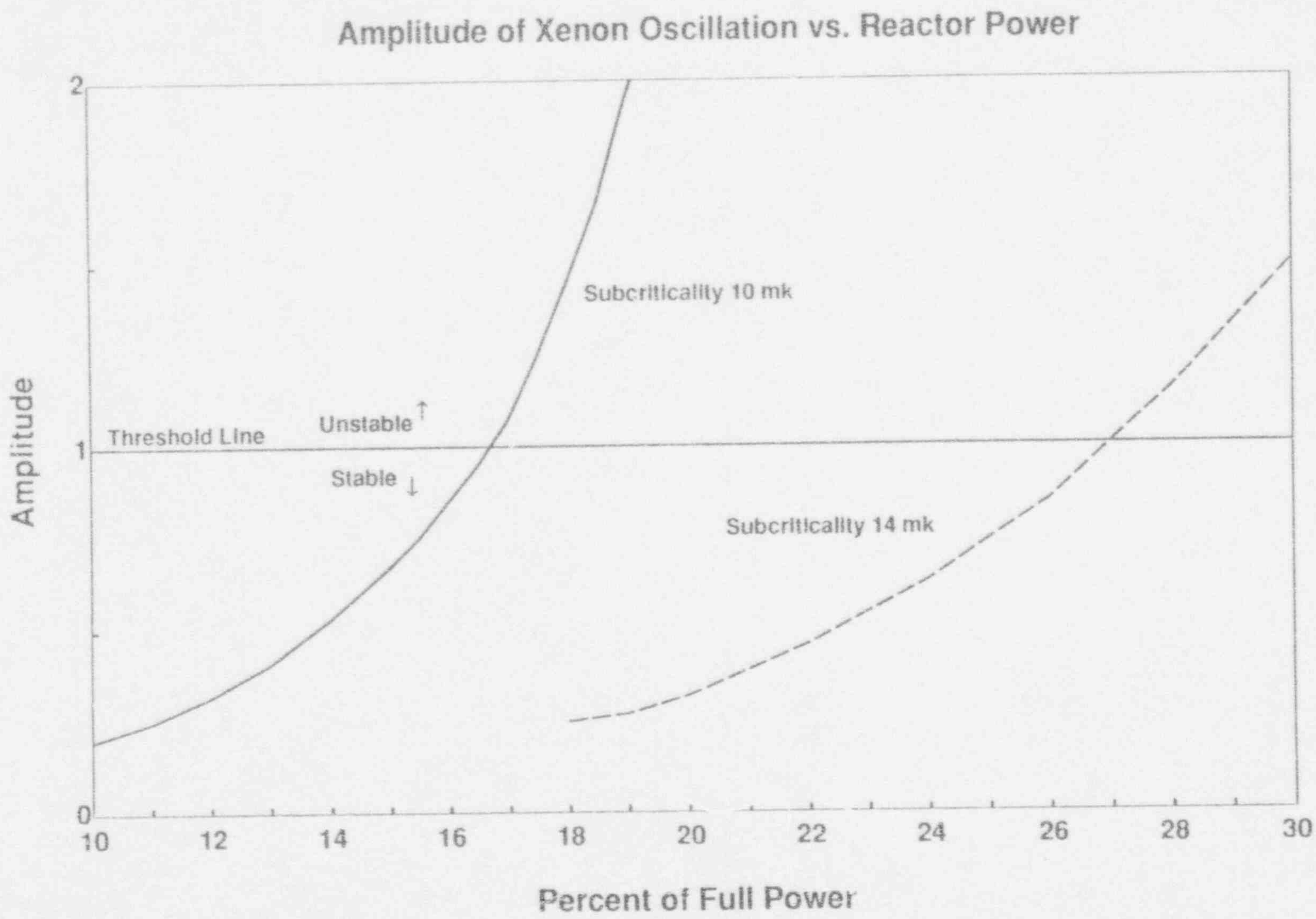
- Period of oscillation is in excess of 24 hours



Period of Xenon Oscillation vs. Reactor Power
Period (h)
40
35
30
25
Subcriticality 10 mk
Subcriticality 14 mk
10
12
14
16
18
20
22
24
26
28
30
Percent of Full Power

Effect of Reactor Size on Subcriticality (mk) of Harmonic Flux Modes

Harmonic Mode	CANDU 3	CANDU 6	Bruce B
First Azimuthal	–35	–16	–13
First Axial	–24	–24	–26


Amplitude of Xenon Oscillation vs. Reactor Power
Subcriticality 10 mk
Unstable
Threshold Line
Stable
Subcriticality 14 mk
Amplitude
0
1
2
10
12
14
16
18
20
22
24
26
28
30
Percent of Full Power

AECL EACL

AECL CANDU EACL CANDU

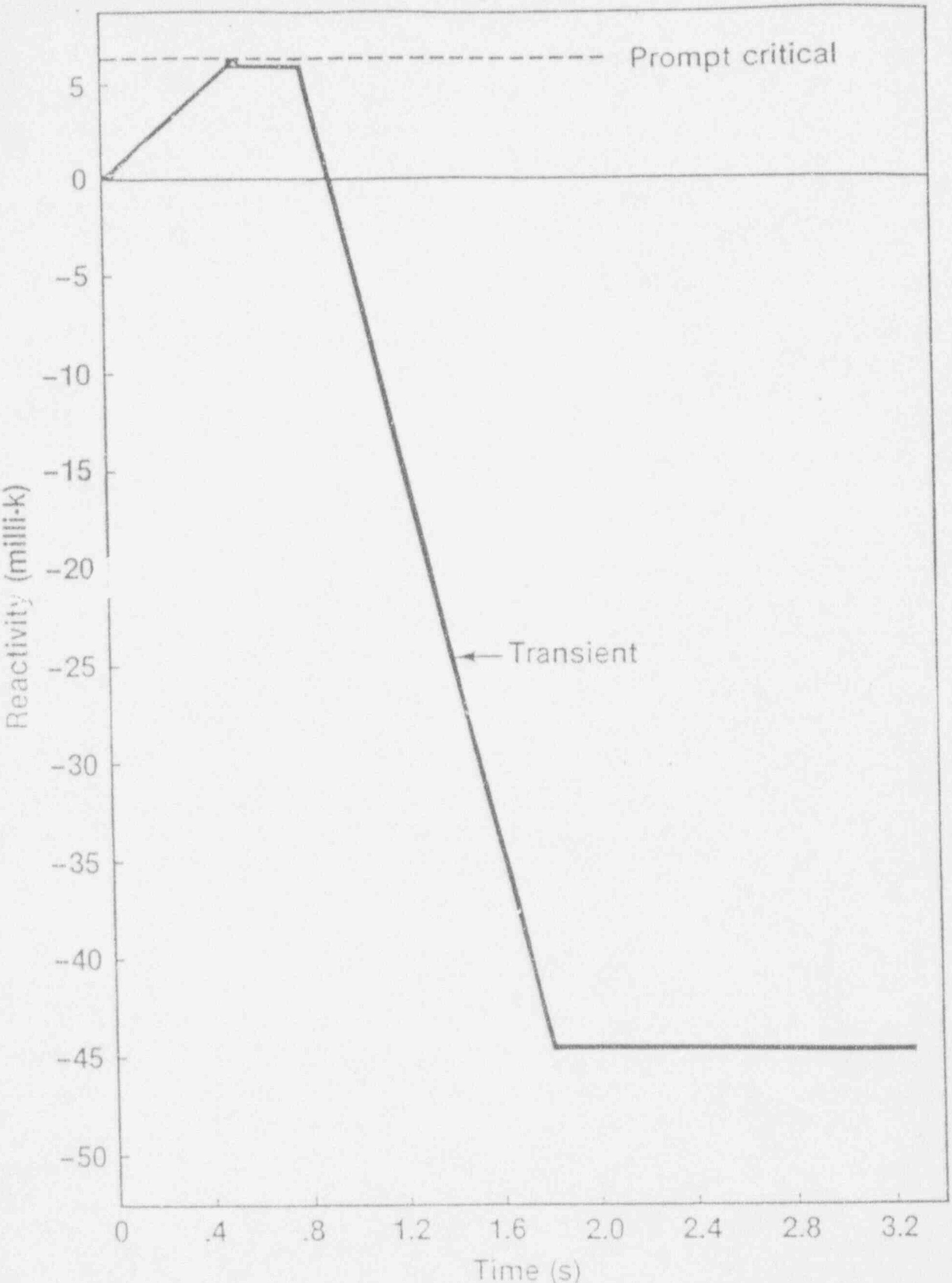
EFFECT OF D_2O ON NEUTRONIC TRANSIENTS

- Long Neutron Lifetime :
  0.9 ms for D_2O Lattice
  vs. 0.03 ms for H_2O Lattice
- Large Delayed Neutron Fraction (beta)
  0.8 mk from Photo-neutrons in D_2O
- Retardation of Neutronic Growth During Transient

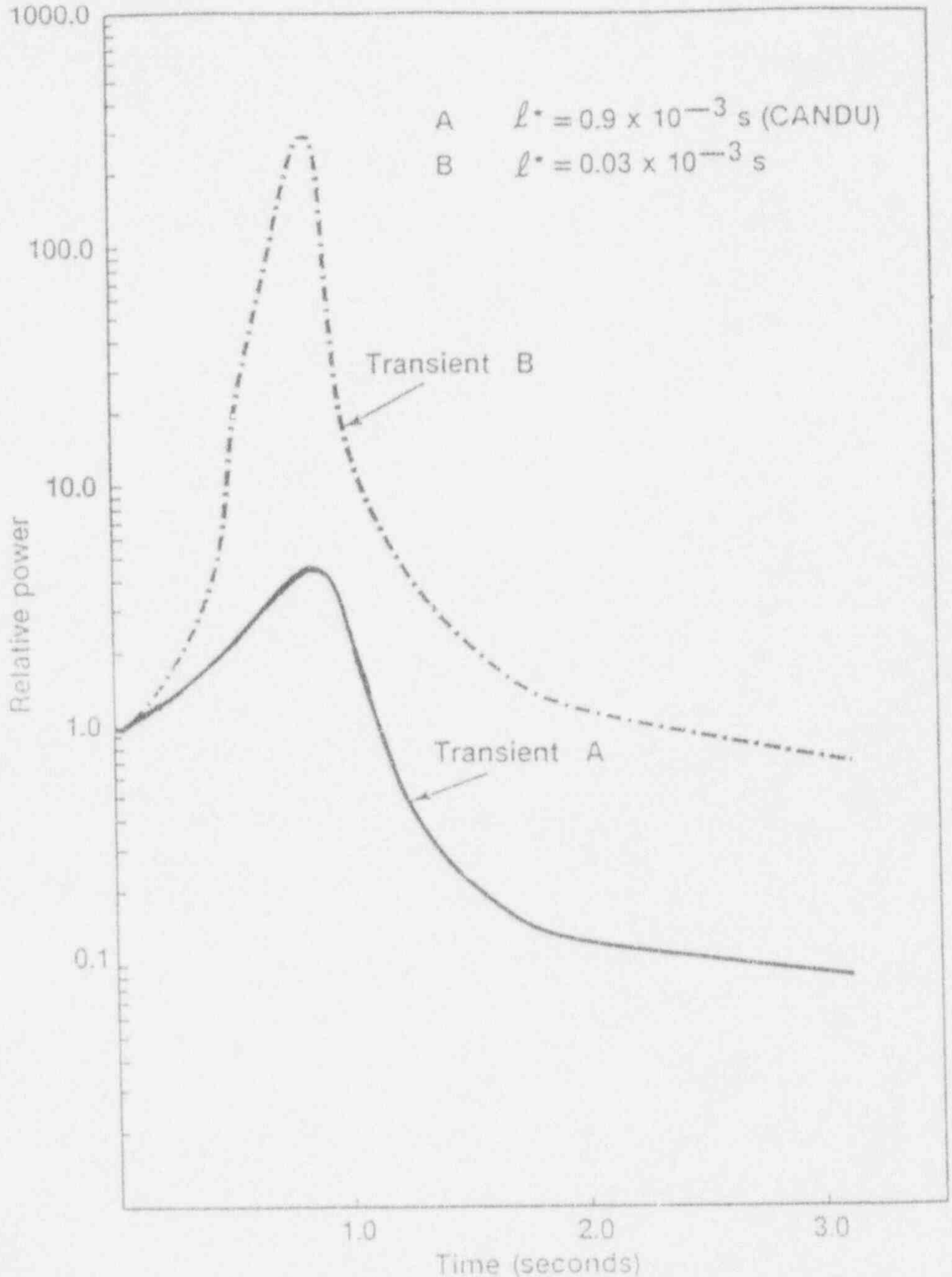
DELAYED NEUTRON DATA FOR EQUILIBRIUM FUEL

Group	Delayed Neutron Fraction β	Time Constant λ (s^{-1})
1	0.00030	0.001
2	0.00120	0.032
3	0.00107	0.121
4	0.00244	0.317
5	0.00081	1.390
6	0.00020	3.803
Total	0.00603	

Prompt neutron lifetime: 9.6×10^{-4} s



HYPOTHETICAL REACTIVITY EXCURSIONS



Sensitivity of Power Excursion to ℓ^*

Summary

- Good neutron economy
- Efficient conversion of U238 to plutonium
- Small change in fissile content over fuel life
- Small change in lattice properties over fuel life
- Small excess reactivity due to on-power fuelling
- Predictable global flux and power shapes
- All reactivity perturbations, except LOCA, are small and can be easily controlled by the regulating system
- LOCA can be terminated by either one of the two independent shutdown systems
- Long neutron lifetime of D_2O lattice retards neutronic growth during transient

CANDU 3 SHUTDOWN SYSTEMS

by

Norman M. Ichiyen

OUTLINE

- Historical perspective
  - Early lessons learned
  - Historical development of SDS concepts
- Description of 2 SDSs
  - Overview
  - Basic requirements
- Use of computers for SDSs
- Conclusions

LESSONS LEARNED

- NRX Incident (1952) set the basic requirements for a shutdown system
- Background:
  - low power experiment to measure burnup
  - 12 control and shutdown rods (dual functionality)
  - 6 SORs to remain in the core (part of experiment)
  - history of SOR malfunctions and spurious trips

COURSE OF THE ACCIDENT

- Errors made during adjustments to 6 SOR air supply
  - resulted in SORs rising out of the core
- Operator closed bypass valves - but rods did not go all the way in
- Operator mistakenly caused safeguard bank to drive out
- Extensive damage
  - fuel melting in 22 places
  - hydrogen burn postulated

LESSONS LEARNED

- Fast shutdown capacity should always be available (SDS poised)
- Shutdown must be independent of control arrangements
- SDS must be reliable (simple) but not over-sensitive to the extent that it frustrates operators

SDS POISED

- Counter-intuitive - contemporary thinking that reactor safest with all possible neutron absorbing material in core
- "... in any operation it is possible that the reactivity of the pile will be changed .. In the normal shutdown state if all the shutoff rods are in, then the monitoring instruments have no control and cannot guard against the unintended reactivity changes." [Lewis, 1953]
- Implies requirement for rapid withdrawal and repoising of SOR after trip

INDEPENDENCE

- Reactivity control must be absolutely separated from shutdown provisions
- At NRX seven out of twelve SORs had been converted to act as "control" elements
- SDS must protect against control system failure

RELIABILITY OF SDS ELEMENTS

- Simplification of SOR insertion mechanism to spring-assisted gravity drop (1956)
- Triplicated shutdown circuits
  - increased reliability of instrumentation
  - decreased systems' sensitivity to spurious actuation
- Regular on-line testing of SDS

HISTORICAL DEVELOPMENT OF SDS CONCEPTS

- 2 SDS
  - serious process failure frequency 10^{-1} to 10^{-3}
  - classification of systems into process or special safety systems
  - no significant release following failure of a process system combined with a failure of a SSS
  - all above led to concept of 2 independent SDSs
  - requires each SDS to fully meet the requirements for any serious failure
    - » requires the SDSs be independent in design and operation and free from any operational connection with any of the process systems including the Regulating System

HISTORICAL DEVELOPMENT OF SDS CONCEPTS

- Impact on licensing
  - "For those plant designs incorporating two independent reactor protective shutdown systems of suitable design amongst the special safety systems, it is accepted that at least one of them will operate as designed when protective shutdown action is required".
  - "Each system must be capable of limiting both the rate of energy production and the total energy production to the extent that the integrity of the containment system is not jeopardized".

HISTORICAL DEVELOPMENT OF SDS CONCEPTS

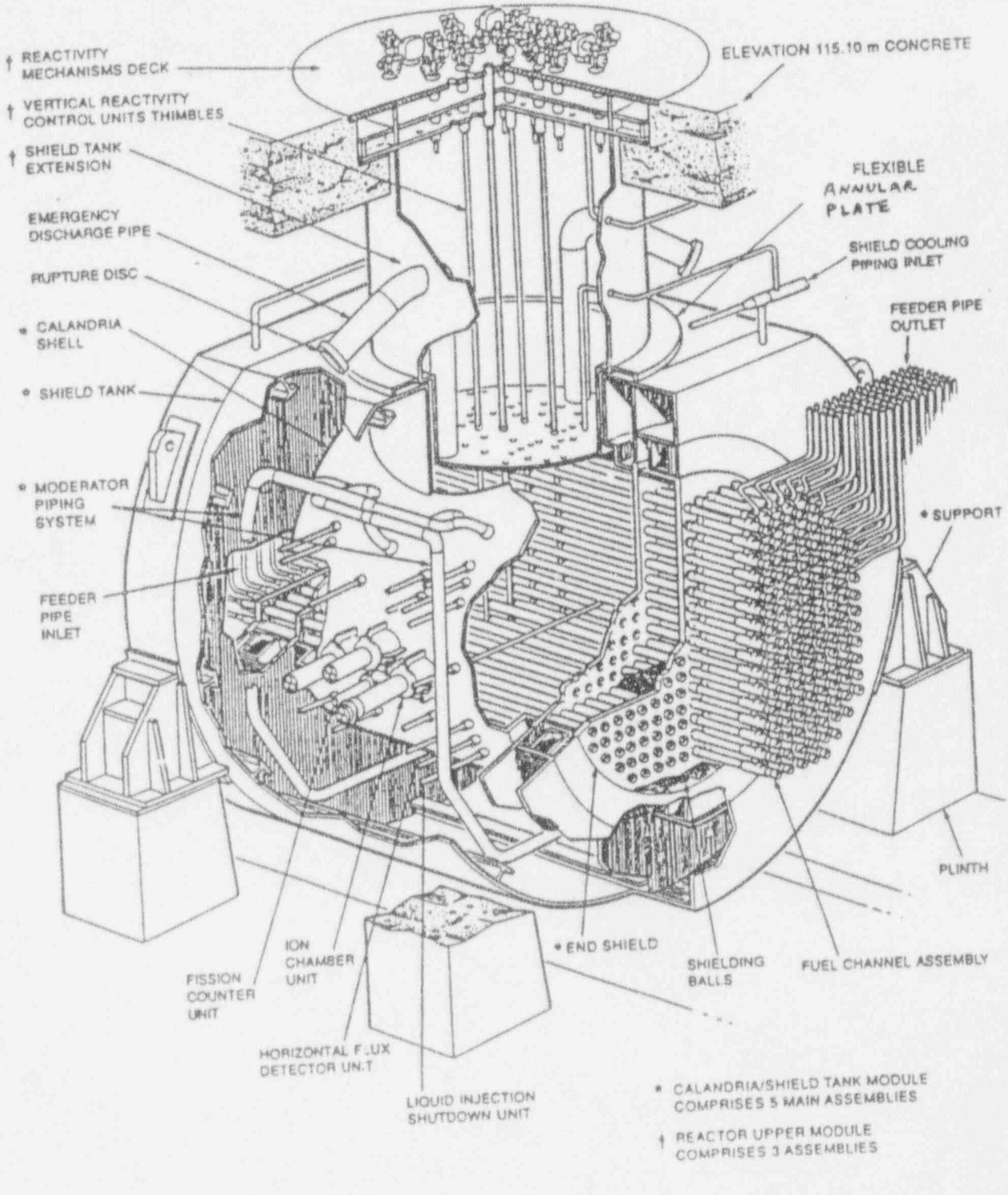
- 2 trip parameters rule
  - "Where practicable, two diverse trip parameters shall be incorporated into the sensing and control logic of each protective shutdown system for each of the serious process failures requiring shutdown action. Manual action is creditable if adequate information and time are available".
  - Rationale: unforeseen circumstances, efficacy of the analysis; hence another layer of protection was added

DESIGN REQUIREMENTS

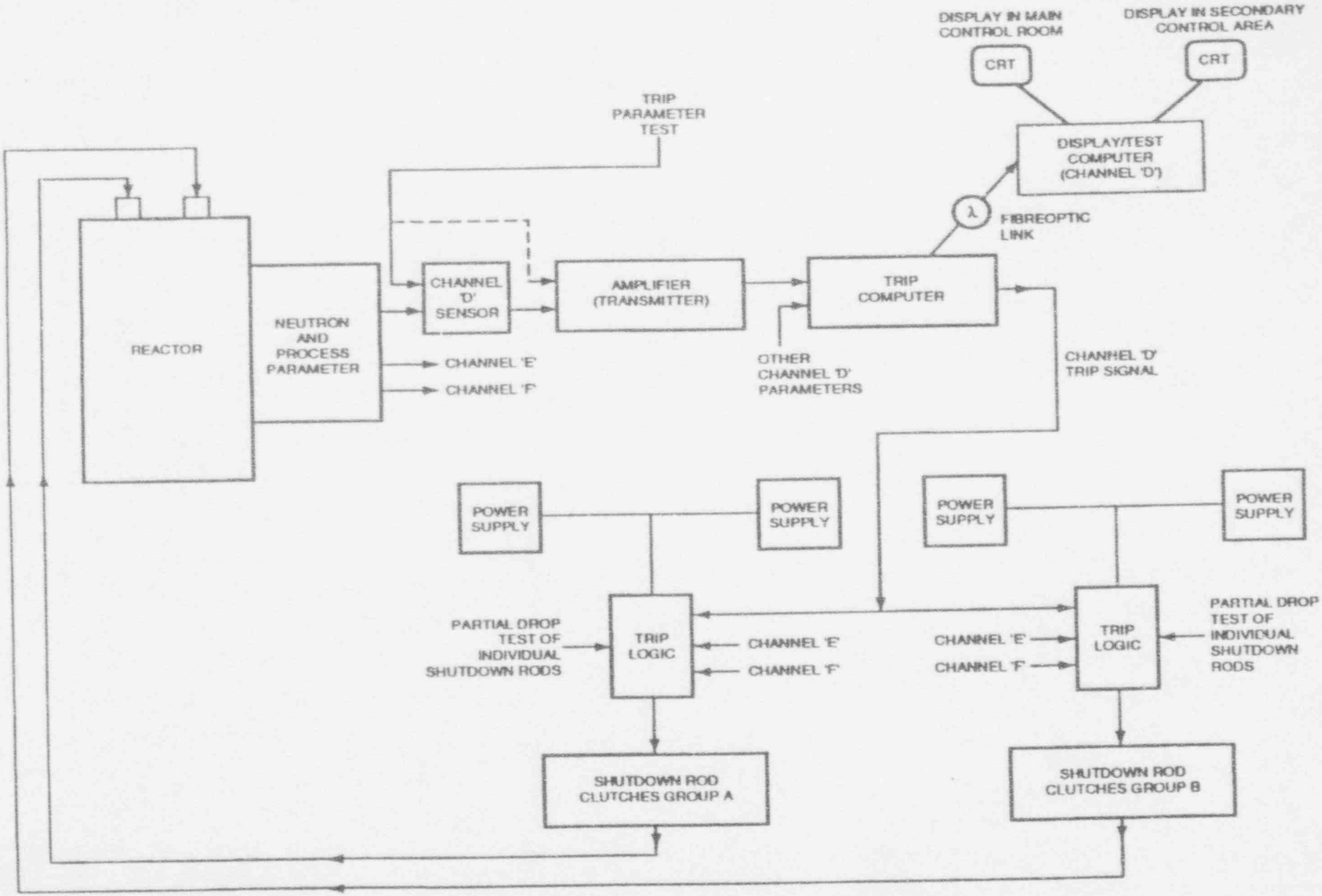
- 2 SDSs
- Separation and independence requirements
- Actuation instrumentation requirements (2 trip parameters)
- Availability requirements
- Testing requirements
- Status monitoring requirements

DESCRIPTION OF 2 SDSs

SDS1 CONCEPT

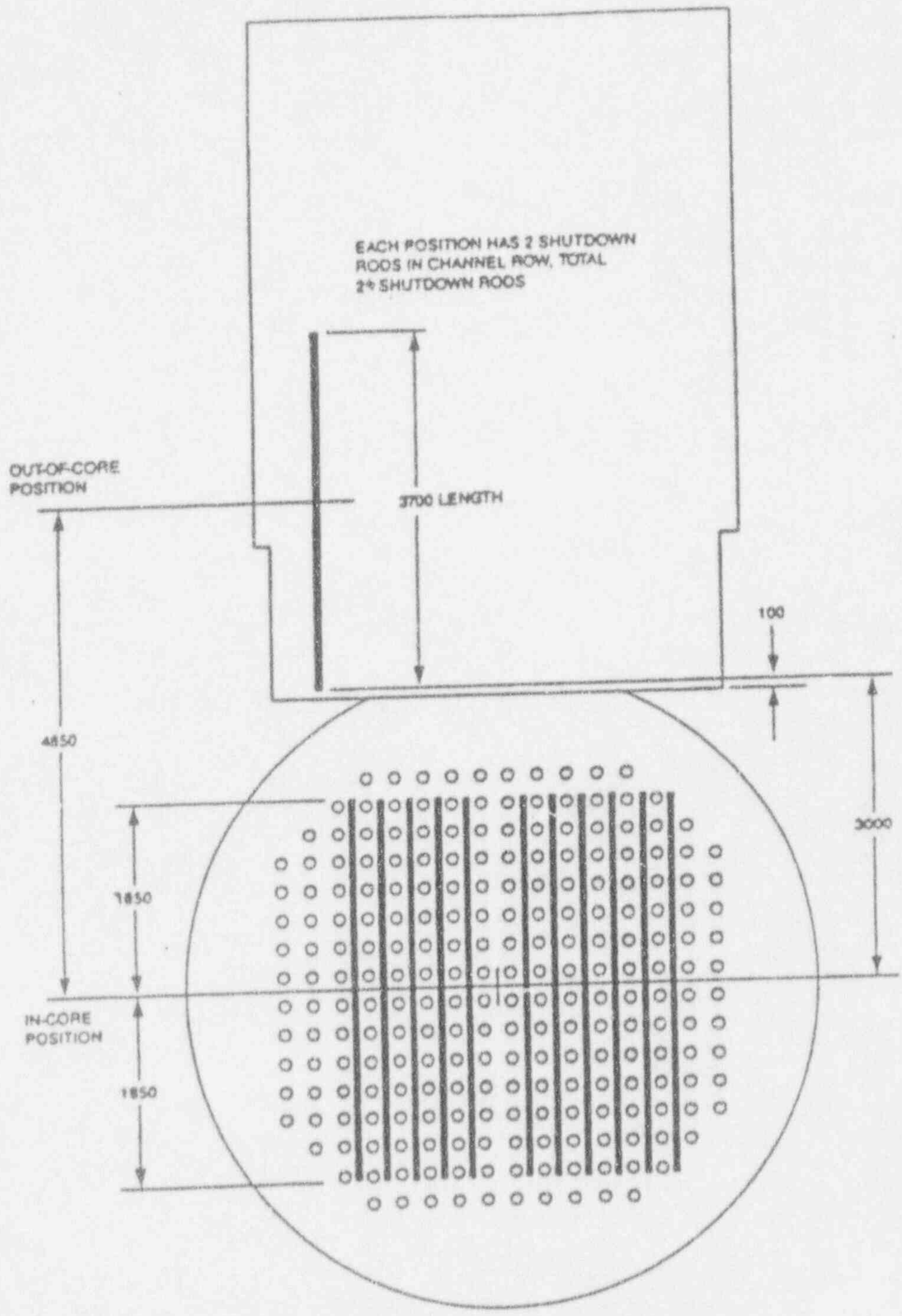


REACTOR ASSEMBLY



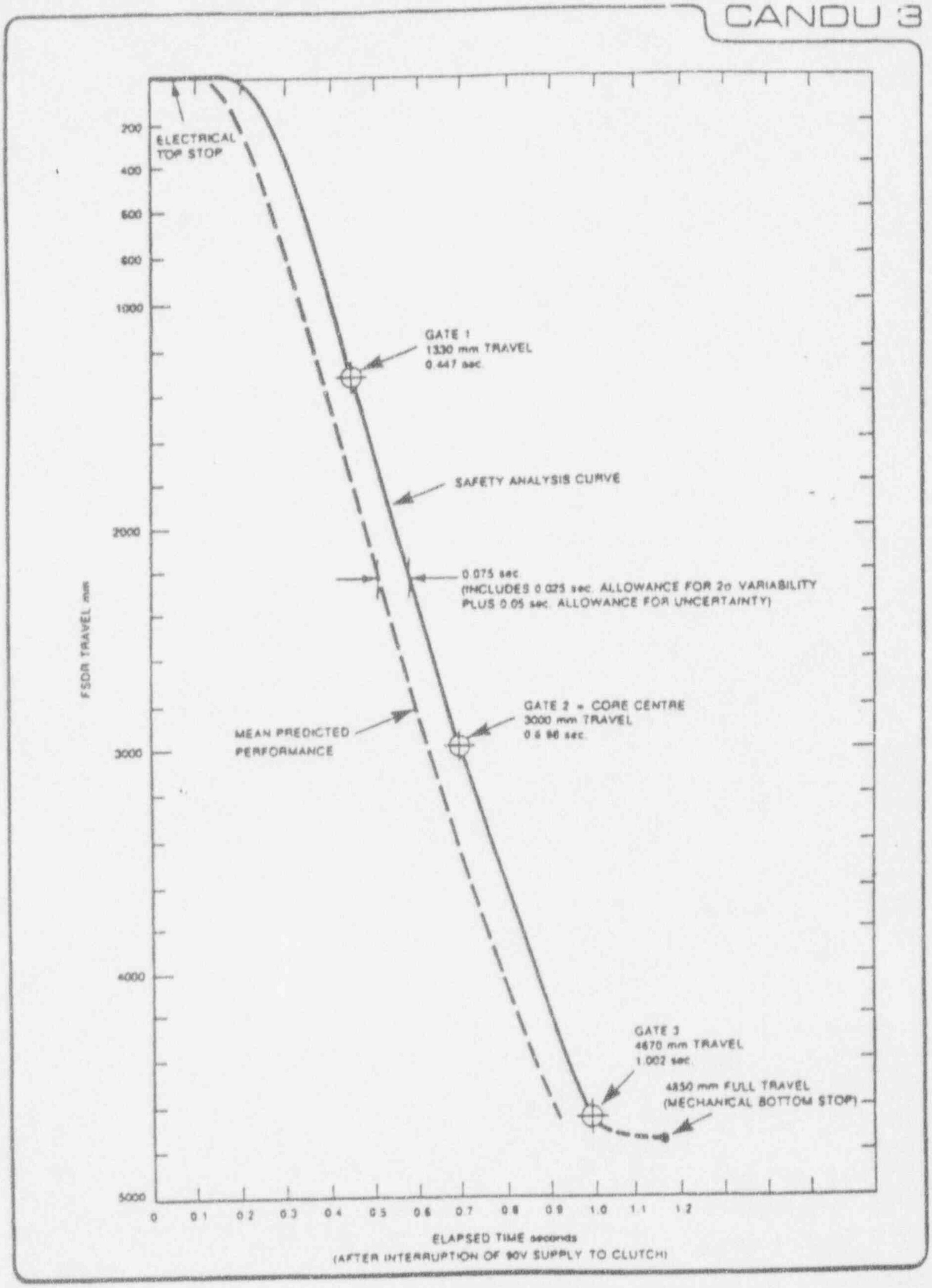
SHUTDOWN SYSTEM NO. 1 – BLOCK DIAGRAM

CANDU 3



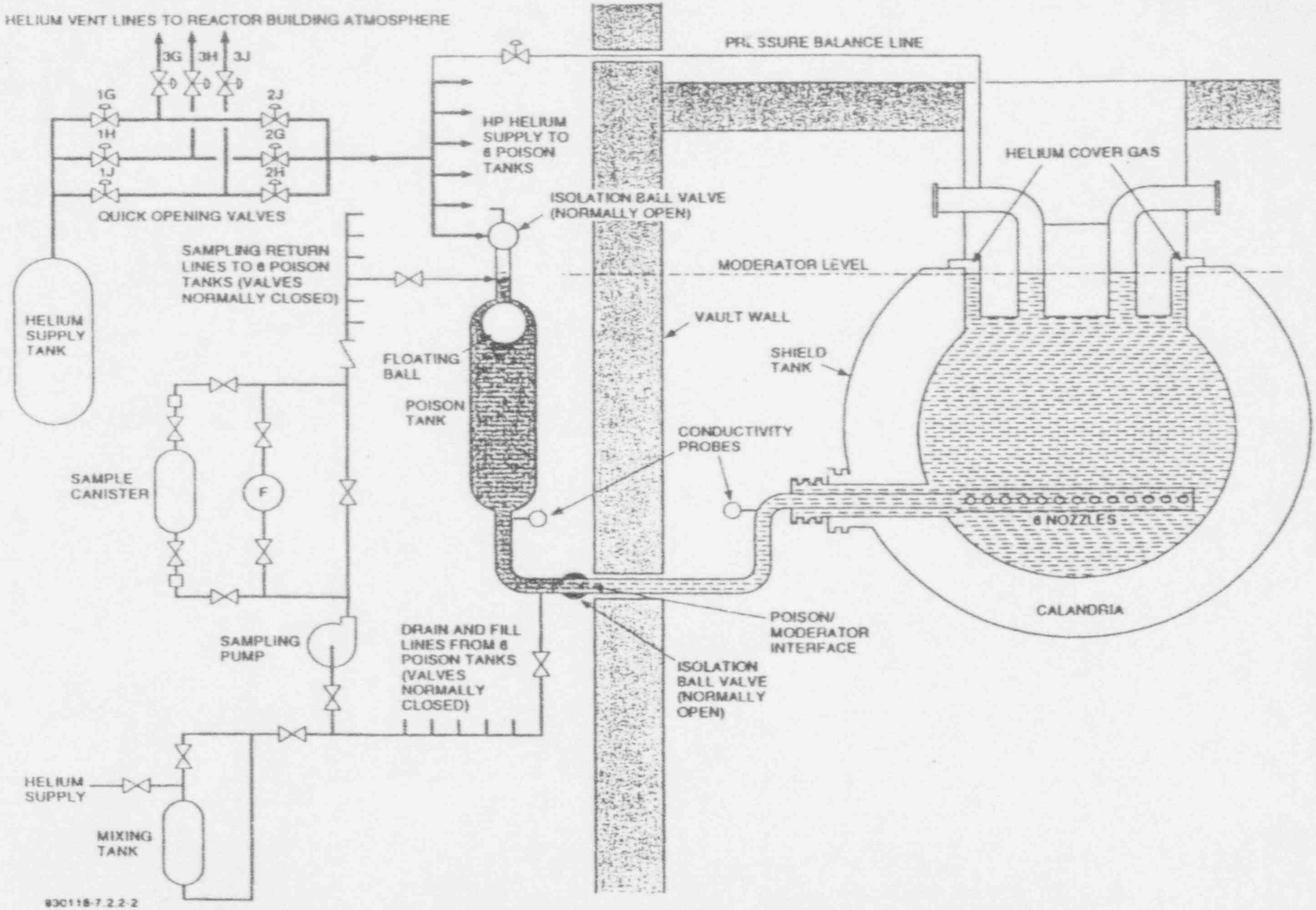
INSERTION — BY SPRING AND GRAVITY
TIME FOR WITHDRAWAL AT 60 Hz — 102s ± 12s

SHUTDOWN RODS (SDR)

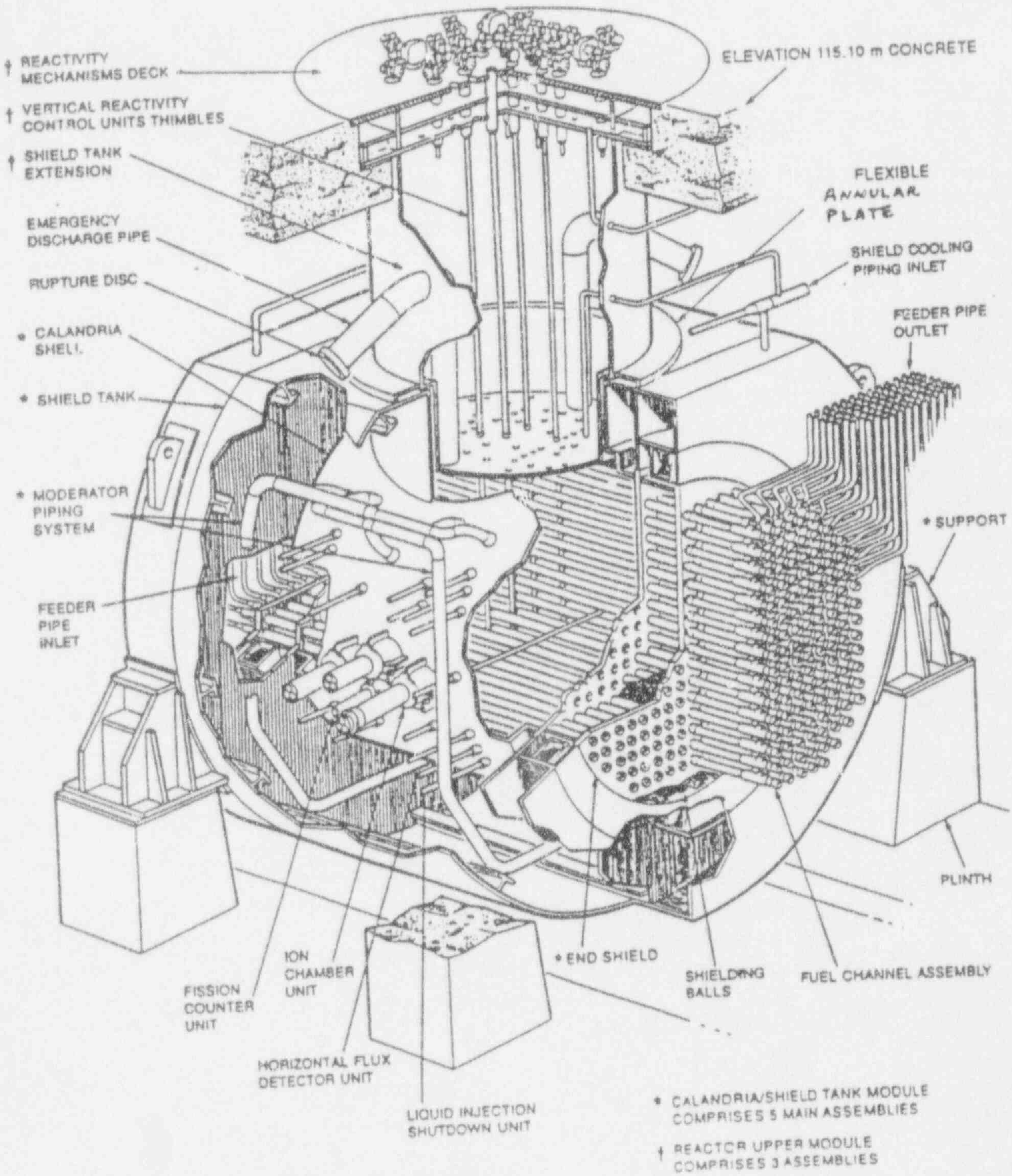


CANDU 3 FAST SHUTDOWN ROD (FSDR)
INSERTION PERFORMANCE

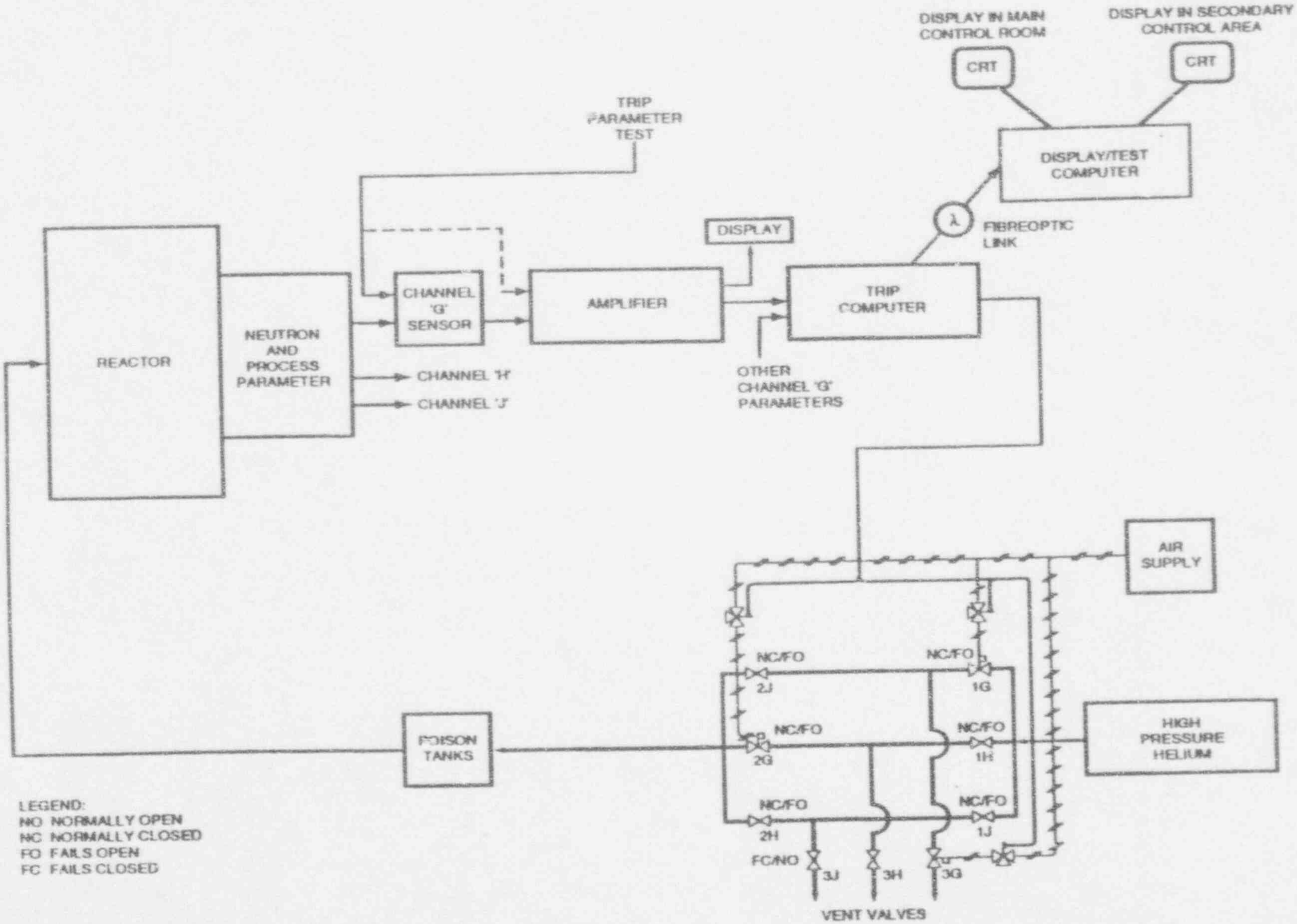
SDS2 CONCEPT



SCHEMATIC DIAGRAM OF THE LIQUID INJECTION SYSTEM USED FOR SHUTDOWN SYSTEM NO. 2



REACTOR ASSEMBLY



930116-7.2.2-1

SHUTDOWN SYSTEM NO. 2 – BLOCK DIAGRAM

2 SDSs - BASIC REQUIREMENTS

SEPARATION AND INDEPENDENCE REQUIREMENTS

- "As far as practicable, the shutdown systems shall be of diverse designs and shall be physically and operationally independent from each other, from process systems and from other special safety systems"
  - Diversity of shutdown method
  - Physical independence
    - » geographic separation
    - » different instrumentation (different suppliers, etc)
    - » separate power supplies, etc

ACTUATION INSTRUMENTATION REQMTS (2 TRIP PARAMETERS)

- "For each event specified in the following table there shall be at least 2 diverse trip parameters on each shutdown system, each designed to detect the need for and automatically initiate shutdown action ...."

Events Requiring Two Parameters on Each Shutdown Systems Table 1

1. Failure of reactor control systems.
2. Failure of normal electric power.
3. Seizure of a primary heat transport system main pump.
4. Failure of any feeder pipe in the primary heat transport system.
5. Failure of an end fitting.
6. Failure of a pressure tube and its associated calandria tube.

Events Requiring Two Parameters on Each Shutdown Systems Table 1 (continued)

7. Blockage of a fuel channel.
8. Failure of a fuelling machine to replace a closure plug.
9. Inadvertent opening of pressure relief or control valves on the primary heat transport system or associated systems.
10. Failure of steam generator tubes.
11. Failure of feedwater/steam system.
12. Failure of moderator system.
13. Failure of service water system.

Events Requiring Two Parameters on Each Shutdown Systems Table 1 (continued)

14. Failure of any other equipment in reactor systems which, in the absence of shutdown action, could result in damage to fuel in the reactor.

TABLE 2

1. Failure of any pipe or header in any fuel cooling system.

Shutdown System Number One Trip Parameters and Setpoints Sheet 1 of 3

Trip Parameter	Detector Type	Setpoint	Conditioning Parameters
High Neutron Power	Vertical In-core Detectors	122% nominal 114% effective (after uncertainties)	Setpoints adjusted by pushbuttons for some abnormal flux shapes.
High Rate Log Neutron Power	Fission Chambers On Both Sides	10% per second	-
High Heat Transport System Pressure	Pressure Transmitters On Both Outlet Headers	Immediate Trip - 10.45 MPa (g) (1515 psig) Delayed Trip - 10.24 MPa (g)	Delayed trip conditioned out when flux detector signal ϕ_{AVEC} < 70%
Low Gross Coolant Flow	ΔP Transmitters	~80% of nominal flow at full power in instrumented channels	Conditioned out when ion chamber log-N <0.1% FP.
High Reactor Building Pressure	ΔP Transmitters	ΔP of 4 kPa(g) (0.58 psig)	-

Shutdown System Number One Trip Parameters and Setpoints Sheet 2 of 3

Trip Parameters	Detector Type	Setpoint	Conditioning Parameters
Low Pressurizer Level	Level Transmitters	Function of reactor power (10.3 m at full power)	1. Setpoint determined by flux detector signals ϕ_{AVEC} 2. Conditioned out when: a. Log-N < 1% FP, and b. ϕ_{AVEC} < 10% FP.
Low Steam Generator Level	Level Transmitters	Function of reactor power	1. Setpoint determined by flux detector signals ϕ_{AVEC} 2. Conditioned out when: a. Log-N < 5% FP, and b. ϕ_{AVEC} < 10% FP.

Shutdown System Number One Trip Parameters and Setpoints Sheet 3 of 3

Trip Parameter	Detector Type	Setpoint	Conditioning Parameters
High Moderator Level	ΔP Transmitters	TBD	-
Low Moderator Level	ΔP Transmitters	TBD	-
Low Heat Transport Pressure	Pressure Transmitters On Both Outlet Headers	Function of Reactor Power (8.4 MPa (g) at full Power)	1. Conditioned out when Log-N <0.1% FP 2. Setpoint is function of ϕ_{AVEC}
Low S/G Feedline Pressure	Pressure Transmitters	3.9 MPa (g)	1. Conditioned out when Log-N <10% FP
Manual	-	-	-
Watchdog Timers	-	-	-
Start-up Count Rate	BF_3	5% / sec	-

Shutdown System Number Two Trip Parameters and Setpoints Sheet 1 of 3

Trip Parameters	Detector Type	Setpoint	Conditioning Parameters
High Neutron Power	Horizontal In-core Detectors	122% nominal 114% effective after uncertainties	Setpoints adjusted by handswitches for some abnormal fluxshapes.
High Rate Log Neutron Power	Ion Chambers on both Sides	15% per second	-
Low Core Flow	Differential Pressure Transmitter	80% in instrumented channels	1. Log-N from ion chambers ϕ <0.3% (pushbotton, for long shutdowns) ϕ <5% (normal operation) 2. Power Rundown Discriminator
High Heat Transport System Pressure	Pressure Transmitter	10.55 MPa (g) immediate (1530 psig)	Power Rundown Discriminator

Shutdown System Number Two Trip Parameters and Setpoints Sheet 2 of 3

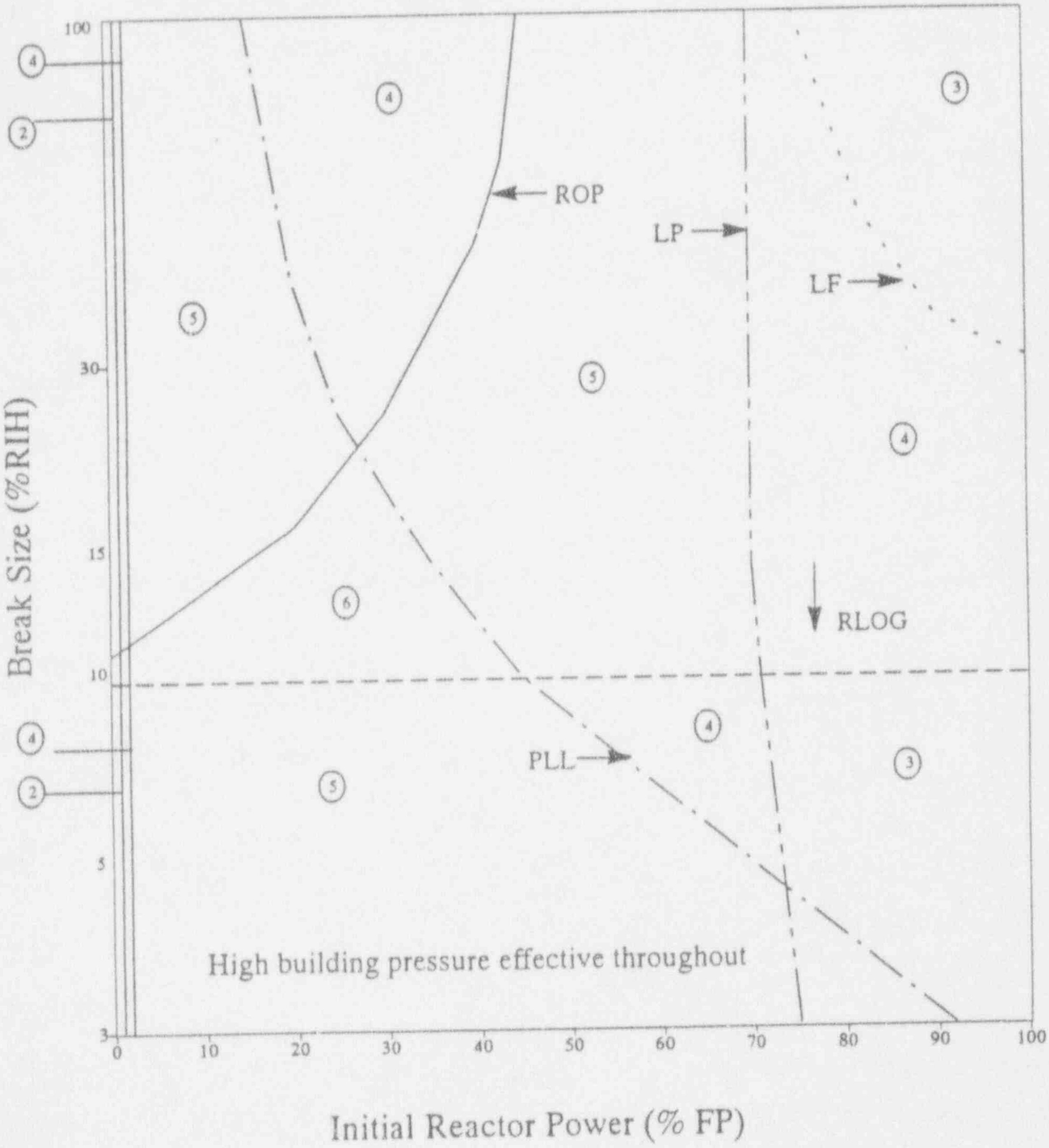
Trip Parameters	Detector Type	Setpoint	Conditioning Parameters
Low Steam Generator Level	Differential Pressure Transmitter	Function of reactor power	1. Conditioned on Log -N < 5% FP or ϕ_{AVEC} < 10% FP 2. Setpoint is a function of reactor power (ϕ_{AVEC})
Low Pressure Level	Differential Pressure Transmitter	Function of reactor power (10.3 m at full power)	1. Setpoint is a function of in-core flux detector signals (ϕ_{AVEC}) 2. Conditioned out on Log-N < 1%

Shutdown System Number Two Trip Parameters and Setpoints Sheet 3 of 3

Trip Parameters	Detector Type	Setpoint	Conditioning Parameters
Low Heat Transport System Pressure	Pressure Transmitter	Function of reactor power (8.4 MPa (g) at full power)	1. Conditioned out on Log-N < 0.3% FP 2. Setpoint is function of (ϕ_{AVEC})
High Reactor Building Pressure	Differential Pressure Transmitter	4 KPa (g) (0.58 psig)	-
Low Steam Generator Feedline Pressure	Pressure Transmitter	3.9 MPa (g)	Conditioned out on Log -N < 10% FP
High Moderator Level	Differential Pressure Transmitter	TBD	-
Low Moderator Level	Differential Pressure Transmitter	TBD	-
Manual	-	-	-
Watchdogs	-	-	-

ACTUATION INSTRUMENTATION REQMTS (2 TRIP PARAMETERS)

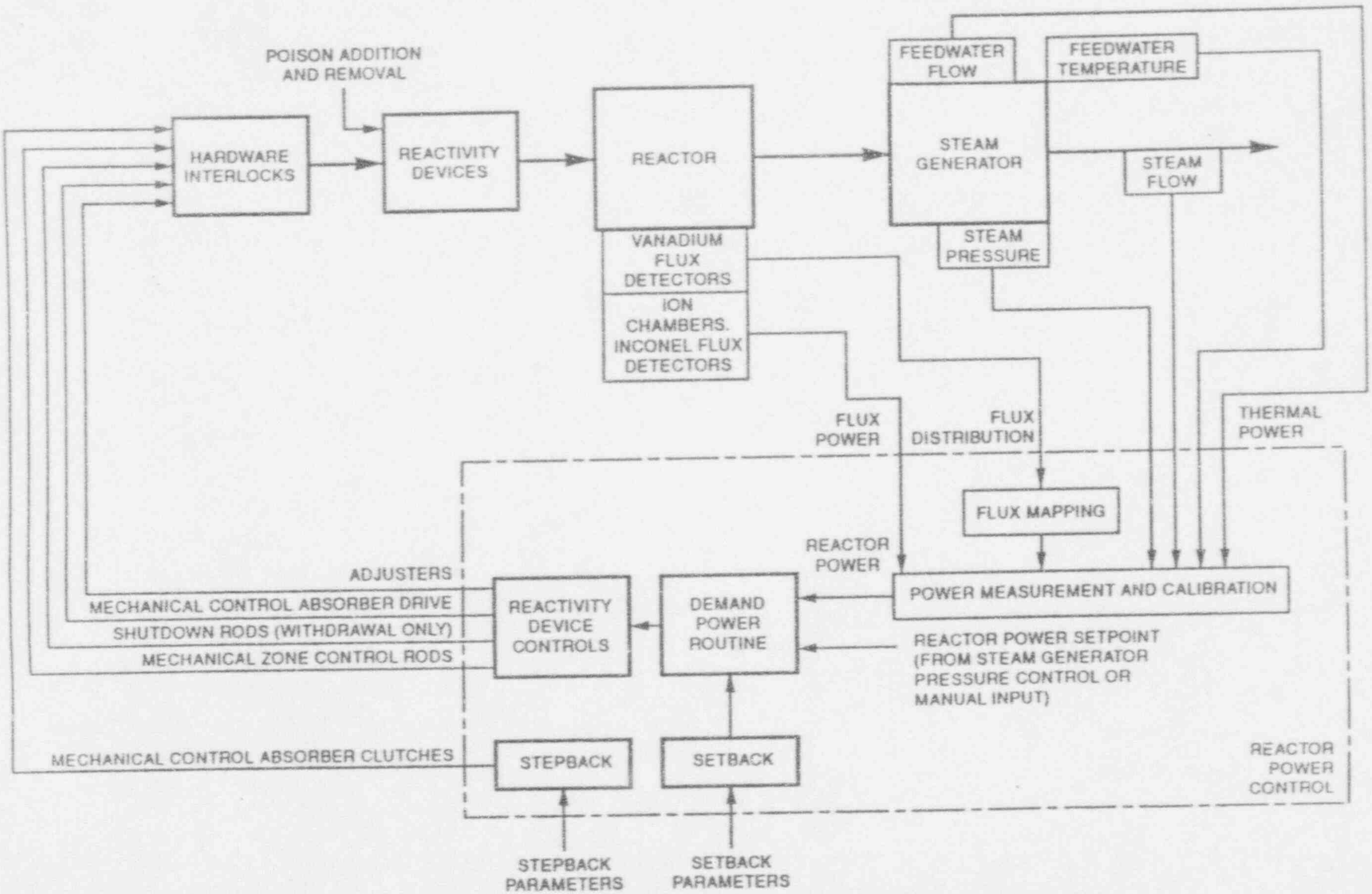
- Design assist analysis - use of trip coverage maps
- Final safety analysis is confirmatory analysis



SDS1 Trip Coverage Map for Large LOCA

DEFENSE-IN-DEPTH (REACTOR SHUTDOWN)

- Reactor Control
  - RRS (Reactor Regulating System)
  - Setbacks
  - Stepbacks (separate instrumentation and logic from RRS)
    - MCAs (Mechanical Control Absorbers) - devices only for setback and stepback
- SDS1
- SDS2



Reactor Regulating System – Block Diagram

TYPICAL REACTOR SETBACK CONDITIONS

- Zone controller system failure
- Spatial control off normal
- High local neutron flux
- Turbine trip
- Loss of line
- High steam pressure
- Low de-aerator level
- High moderator level
- Manual

TYPICAL REACTOR STEPBACK CONDITIONS

- Reactor Trip
- Main coolant pump trip
- High heat transport pressure
- High flux power
- High rate log
- Low steam generator level
- Low moderator level

AVAILABILITY REQUIREMENTS

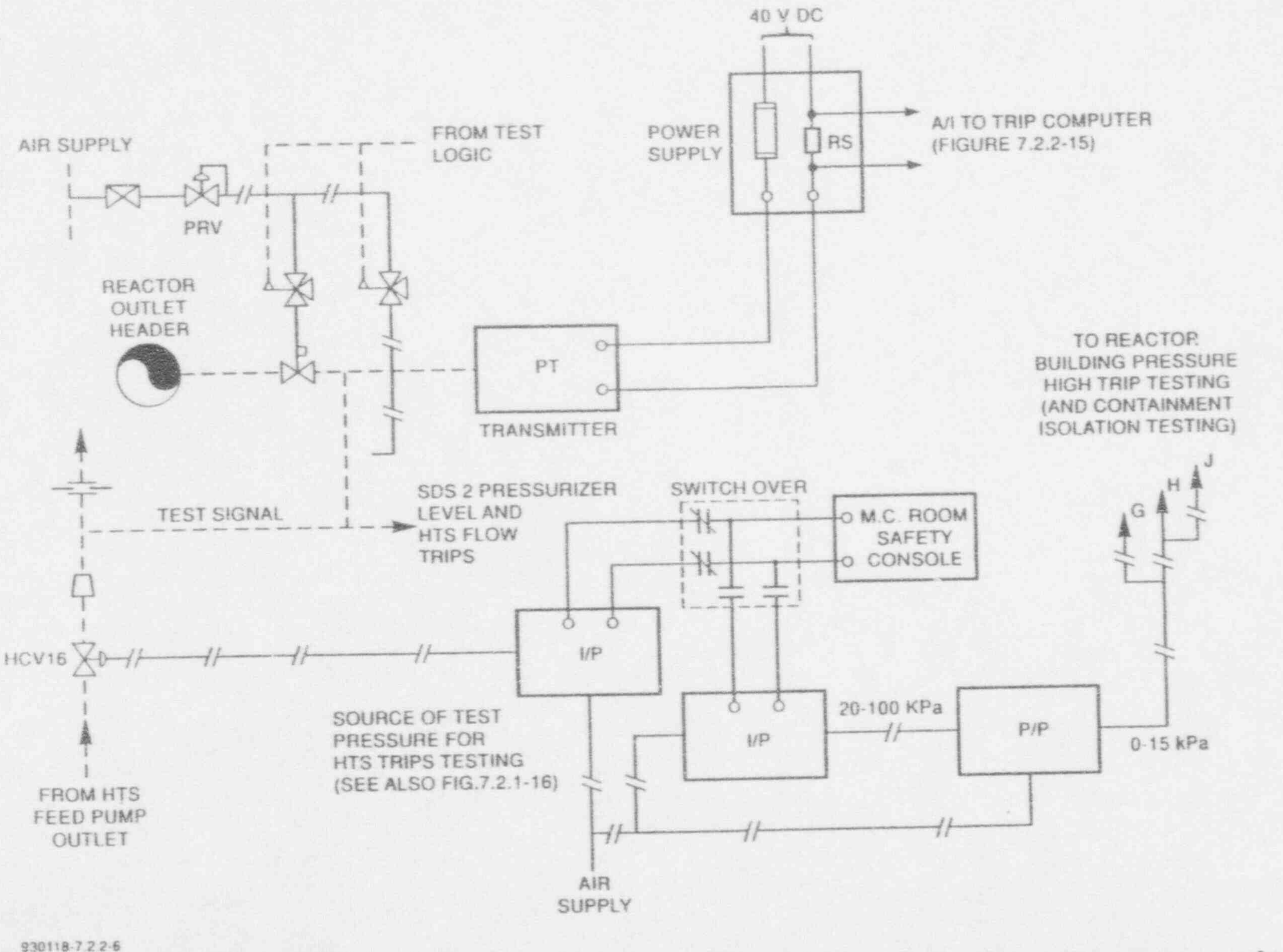
- "Each shutdown system shall be designed such that the fraction of time for which it is unavailable can be <u>demonstrated</u> to be less than 10^{-3}."
  - In other words, the probability the system works on demand is >999/1000 challenges.
  - Demonstration is accomplished through a combination of overlapping tests with predicted future unavailability using fault tree techniques

AVAILABILITY REQUIREMENTS (DESIGN TARGET)

- For design purposes, the system availability requirement is used as a target on an individual trip parameter basis
  - This means that although we have ≥2 trip parameter coverage for each accident condition, we only require each parameter acting alone to meet the unavailability requirement.

AVAILABILITY TESTING REQUIREMENTS

- "All shutdown system equipment shall be monitored or tested at a frequency which is adequate to demonstrate compliance with the availability requirement."



HTS Pressure Trips Measurement Loop (Typical) and Testing Arrangements

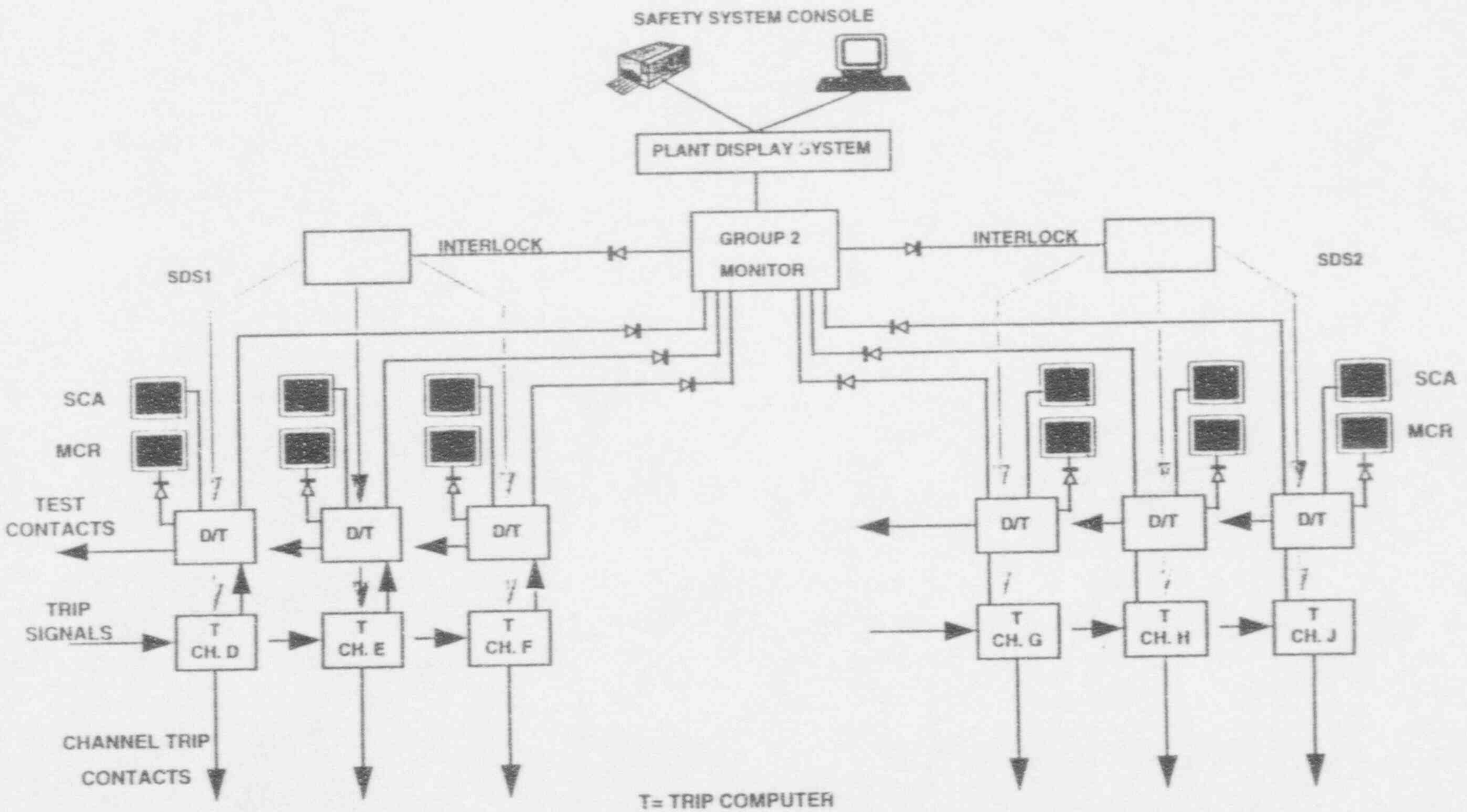
Safety System Faults

Type	Definition
0	A Type 0 fault totally incapacitated the system, such that it would not have provided any protection under any conditions.
1	A Type 1 fault significantly reduced the effectiveness of the system, such that it would have been of little or no benefit if the worst possible process system failure had occurred.
2	A Type 2 fault reduced the effectiveness of the system, such that it would have failed to satisfy the design intent. However, the system would still have operated and significant benefit would have been gained from its operation.
3	A Type 3 fault reduced the level of redundancy that is built into the system. The effectiveness of the system was not significantly reduced and the design intent could still be satisfied.
4	A Type 4 fault reduced the effectiveness of the system, or a single component, such that it was outside normal operating limits. However, the design intent could still be satisfied.
5	A Type 5 fault had no negative effect on the system.

STATUS MONITORING REQUIREMENTS

- "The design of a shutdown system shall be such that the status of all important equipment required for its actuation can be monitored from or inferred from the control room."

CONFIGURATION OF FULLY COMPUTERIZED SHUTDOWN SYSTEMS



T= TRIP COMPUTER

D/T= DISPLAY TEST COMPUTER

USE OF COMPUTERS FOR CANDU SDSs

- Long history of computer usage in SDSs - C-6 plants
  - The three CANDU 600 stations (Wolsong 1, Gentilly 2 and Pt. Lepreau) have over 300 unit-years of operating history without a single unsafe failure reported.
- Darlington NGS fully computerized SDS design
  - Trip decision logic
  - Operator displays
  - Operator-assisted testing
  - Monitoring
    - » signal spreadchecks
    - » margin to trip annunciation

REASONS FOR USING COMPUTERS IN SDSs

- Fail safe nature (ability to convert unsafe failures into safe failures)
- Greater production reliability

SOFTWARE ENGINEERING PRACTICE

- AECL and Ontario Hydro have developed 2 highly rigorous methodologies whose distinctive characteristics are:
  - Use of mathematical functions for software requirements specification and design description (sometimes referred to as "formal" methods)
  - The design description is mathematically verified against the requirements specification and the code is mathematically verified against the design description.

ANALYSIS OF RESULTS TO-DATE

- AECL is using these 2 methodologies for SDS1 and SDS2 for Wolsong 2/3/4
- Nearing completion of unit testing
  - Results to date are exceptional
    - » No errors in the code for the "formal" part
    - » A few errors found with respect to the hardware interfaces

ANALYSIS OF RESULTS TO-DATE

- AECL is using these 2 methodologies for SDS1 and SDS2 for Wolsong 2/3/4
- Nearing completion of unit testing
  - Results to date are exceptional
    - » No errors in the code for the "formal" part
    - » A few errors found with respect to the hardware interfaces

CONCLUSION

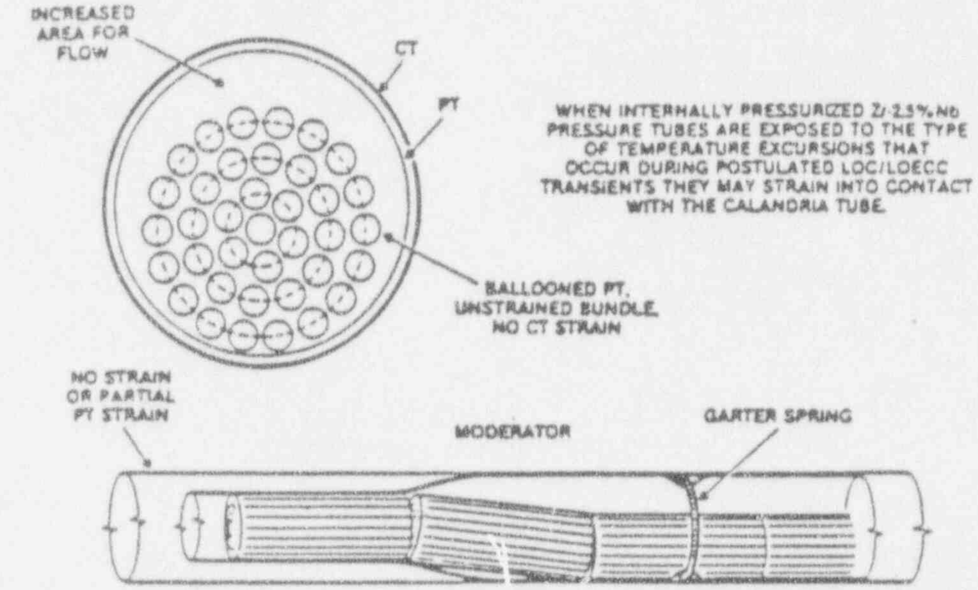
- CANDU SDS philosophy has been shaped through long years of experience (NRX incident, etc)
- simplicity
- diversity, independence
- availability requirements demonstrated "continuously"
- result is a design that provides us with a high degree of assurance that the SDSs will perform as required

CANADIAN DESIGN APPROACH

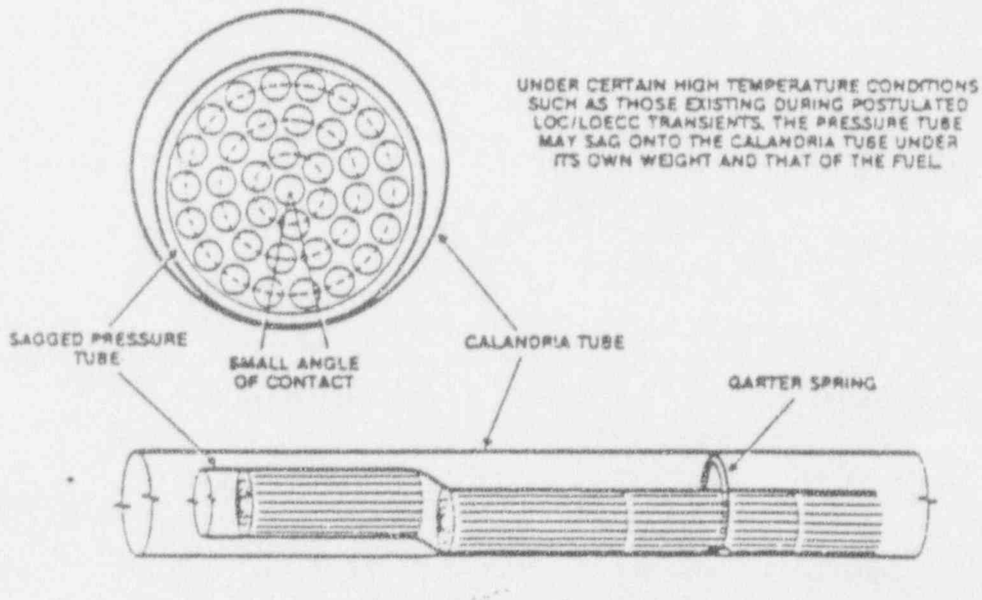
- design for single initiating events that could release radioactivity
- also include design basis events with complete failure of:
    - a shutdown system
    - the emergency core cooling system
    - a containment system

IMPACT ON DESIGN

- second diverse equally effective shutdown system
- moderator designed to provide ECCS backup
- safety systems optimized to limit doses even with containment system failures
- emphasis on reliable safety systems with in–service testing feedback



DIAMETRAL STRAIN TO CONTACT



CONTACT DUE TO PRESSURE TUBE SAG

MODES OF PRESSURE TUBE DEFORMATION FOR LARGE LOSS OF COOLANT WITH FAILURE OF EMERGENCY COOLANT INJECTION

EVENTS BEYOND CANADIAN DESIGN BASIS

- studies include
  - probabilistic evaluations
    - Darlington PSE
    - AECL/KEMA CANDU 600 study
  - consequence evaluations
    - AECL/KEMA CANDU 600 study
    - MAAP/CANDU
    - Pickering failure of shutdown

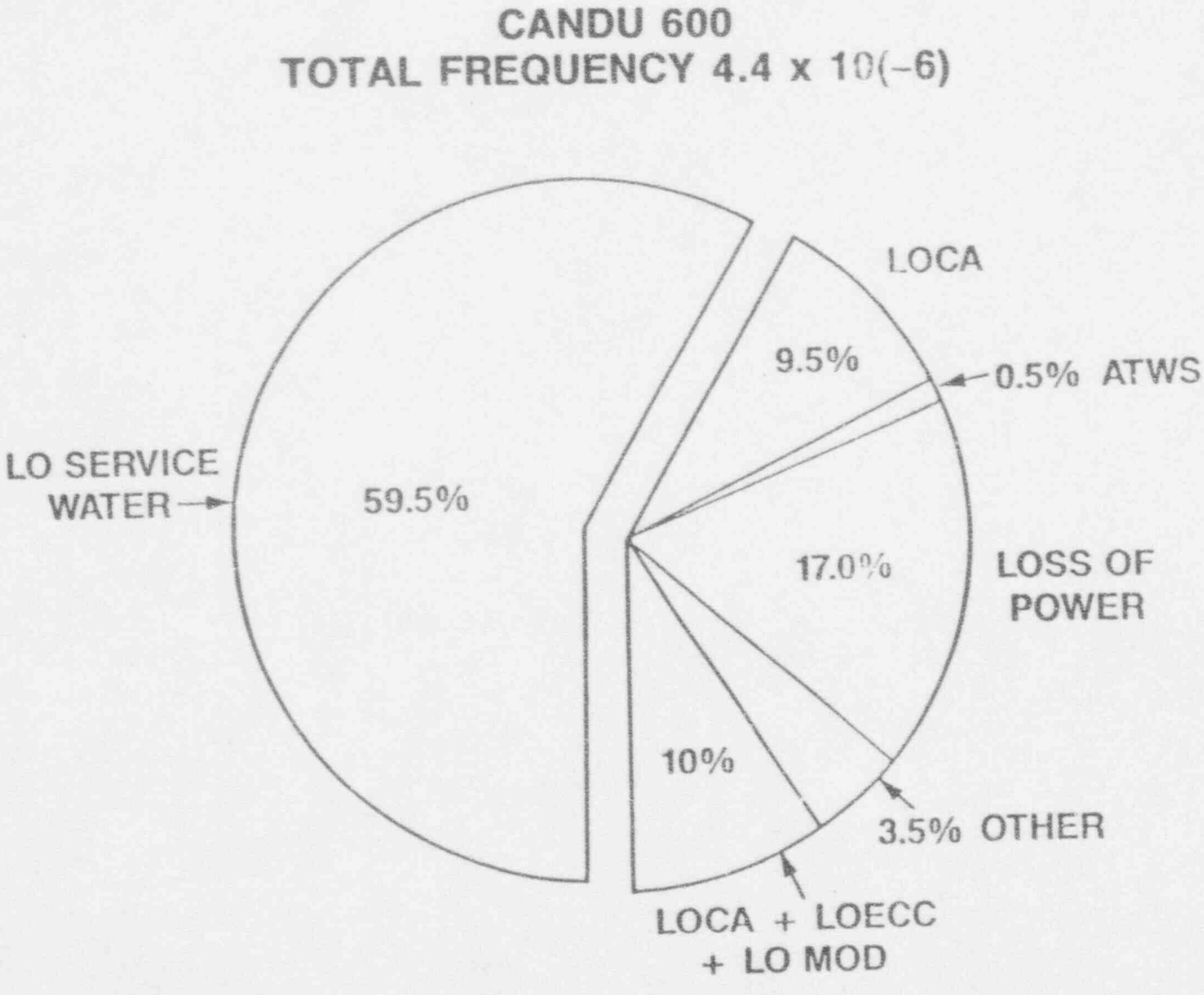


FIGURE 2.1 CORE MELT FREQUENCY

1 HOUR

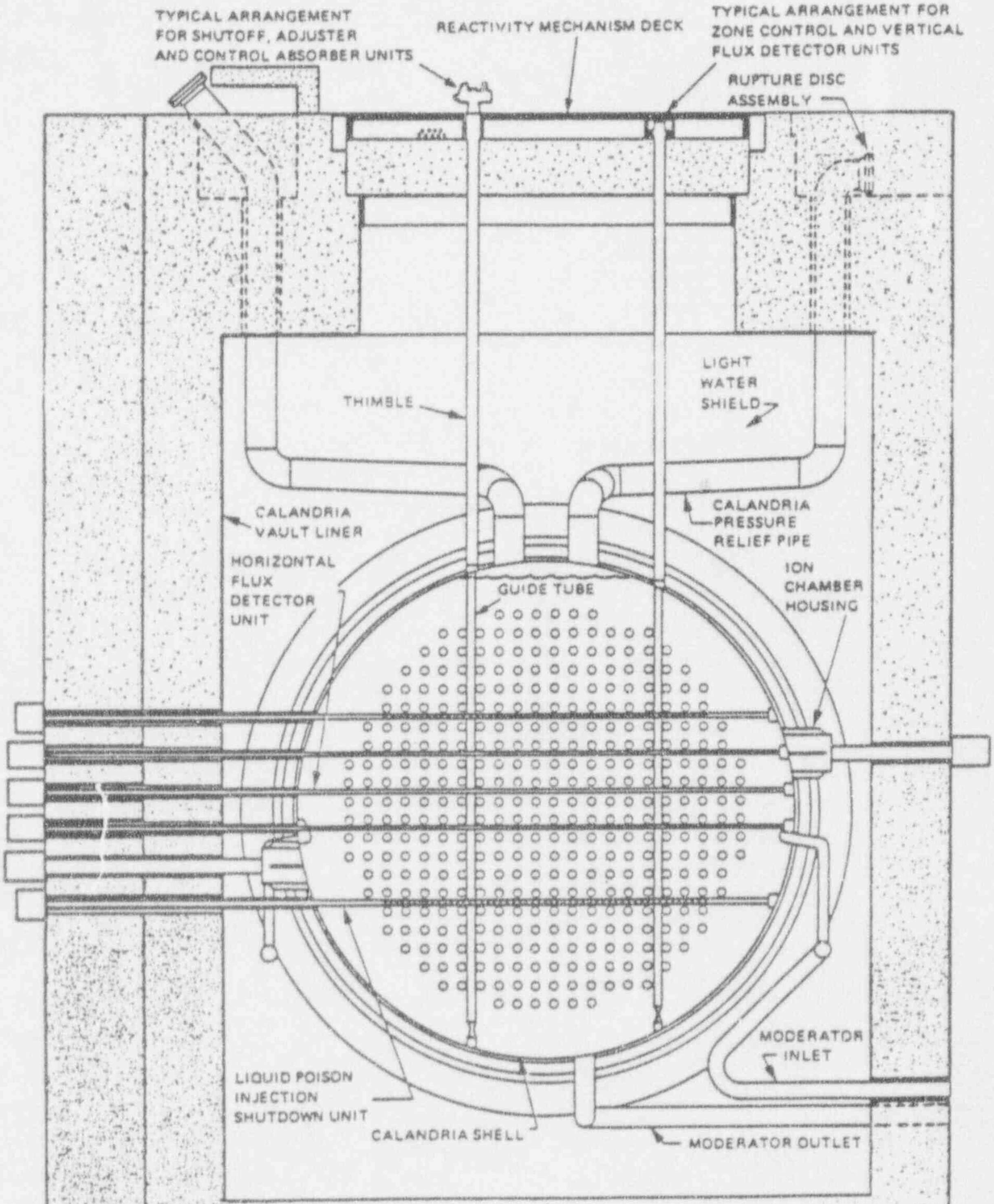


FIGURE 3.3 LATE CORE DISASSEMBLY - 1 HOUR

1-2 HOURS

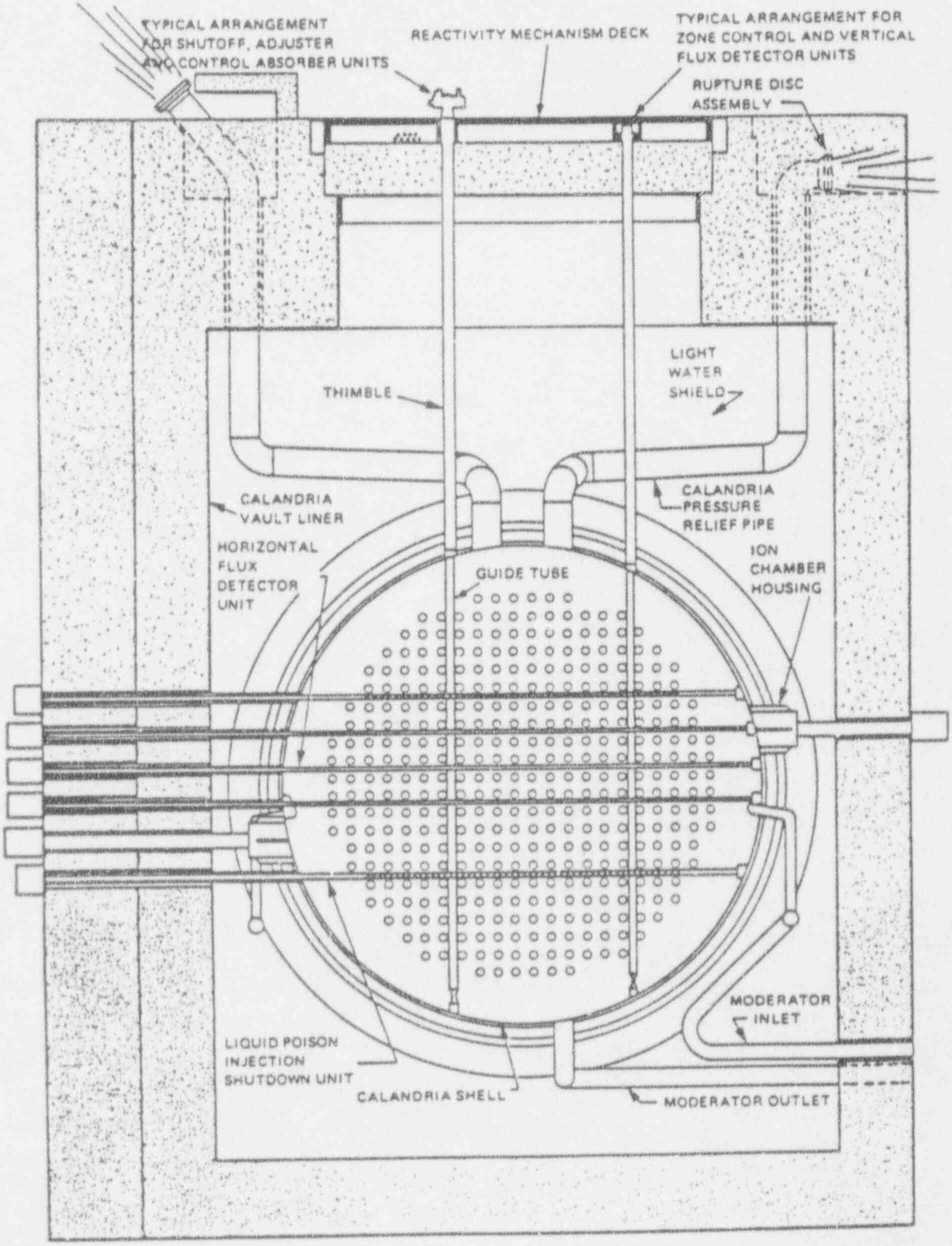


FIGURE 3.4 LATE CORE DISASSEMBLY – 1 TO 2 HOURS

3 HOURS

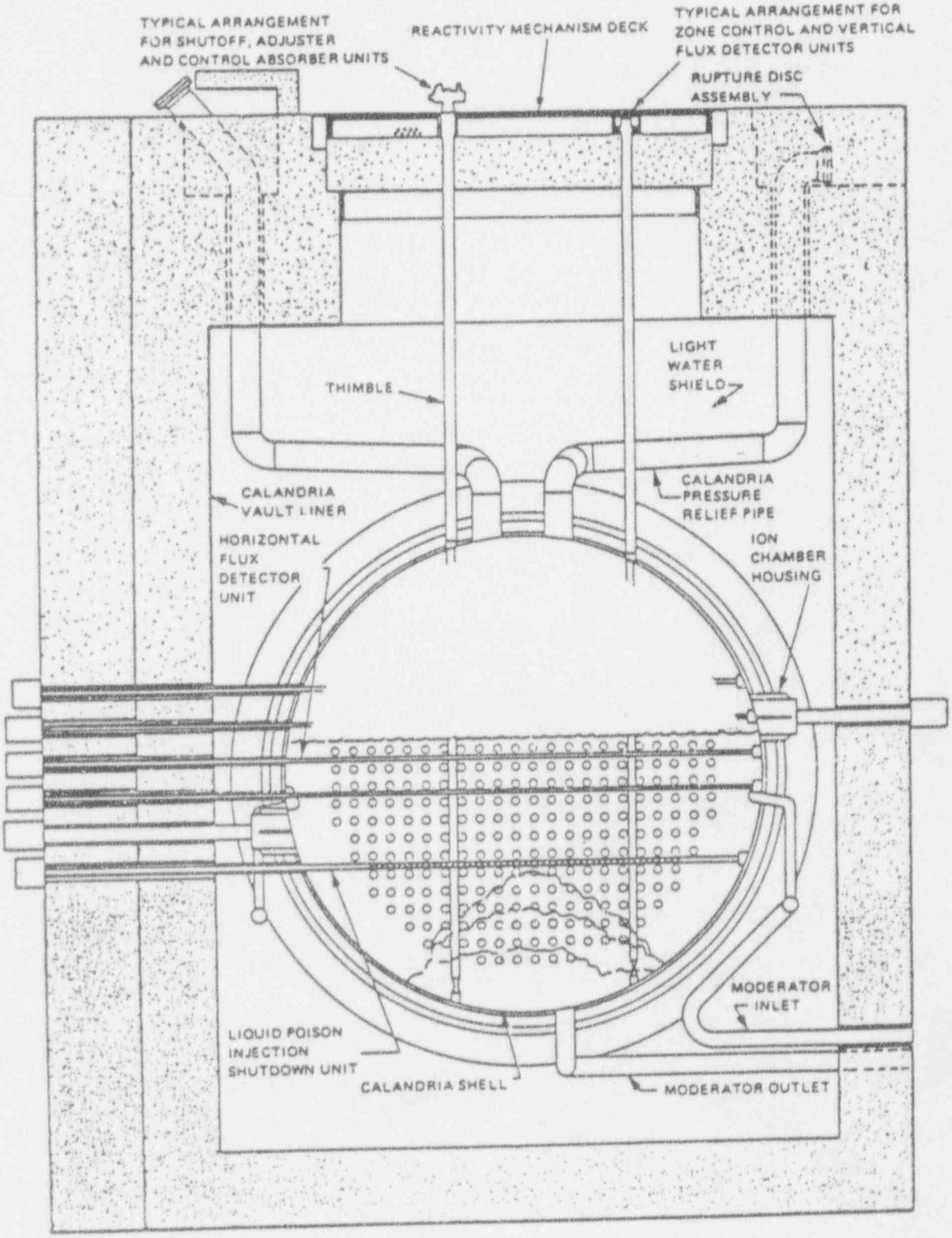


FIGURE 3.5 LATE CORE DISASSEMBLY - 3 HOURS

25 HOURS

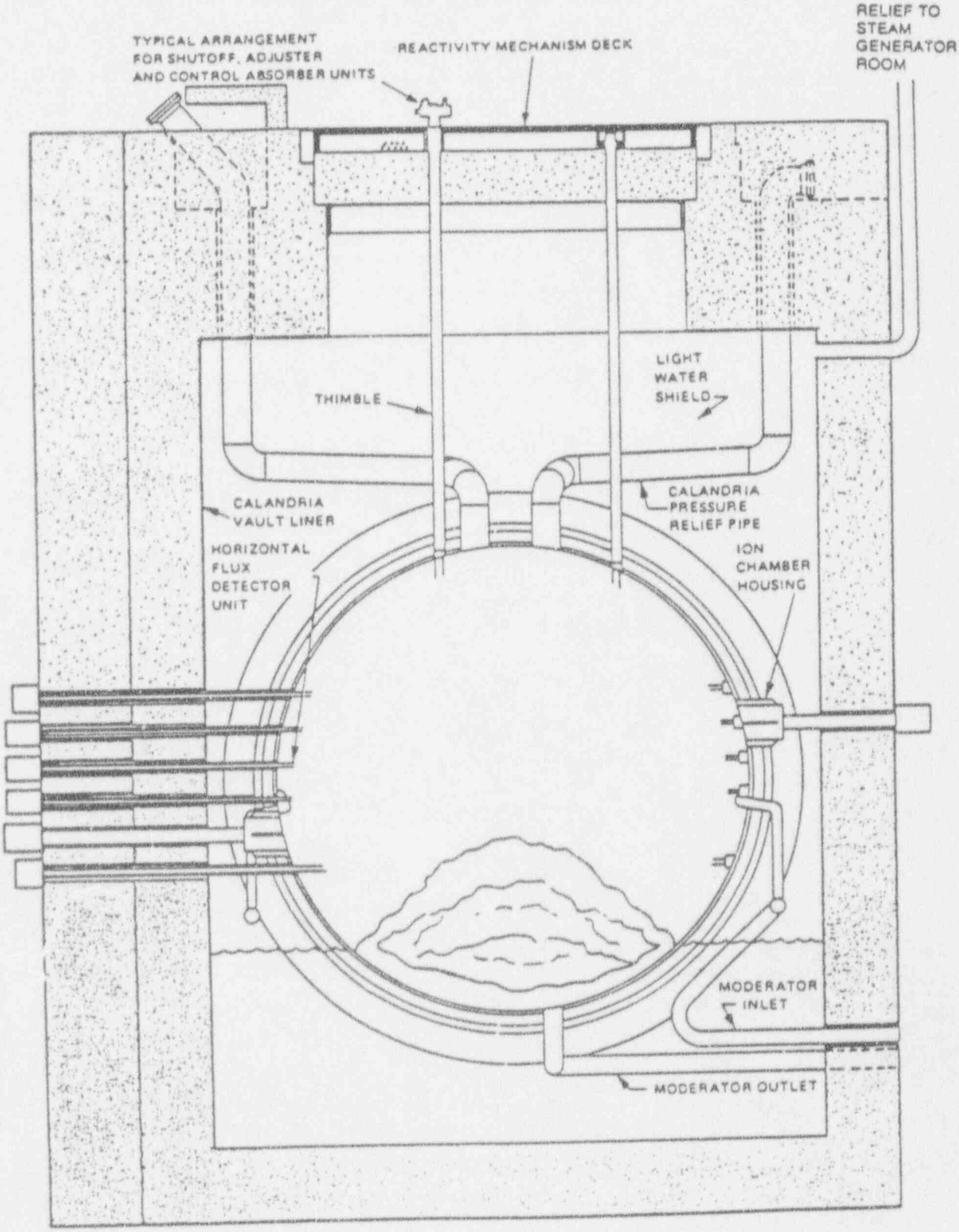


FIGURE 3.6 LATE CORE DISASSEMBLY – 25 HOURS

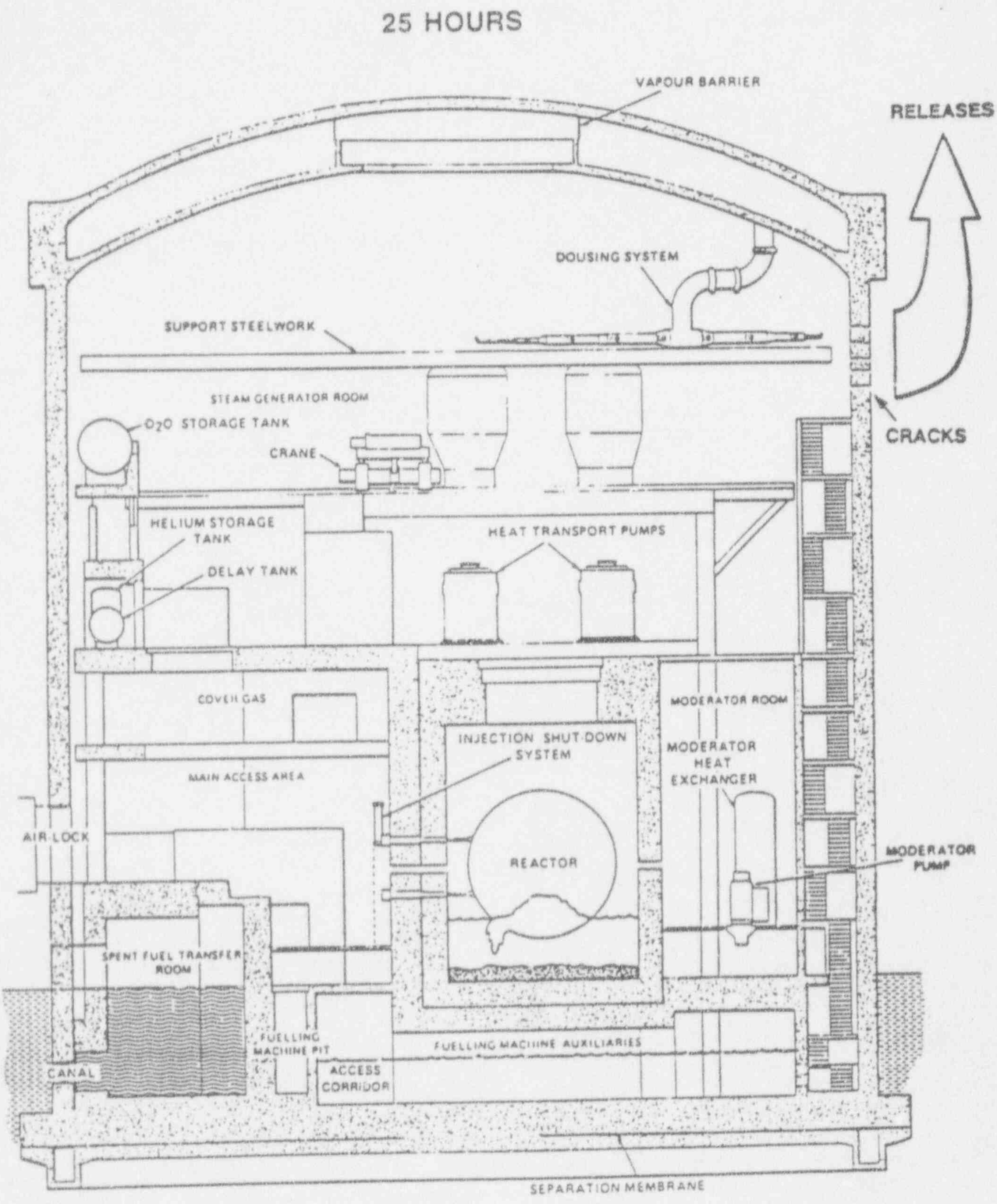


FIGURE 3.7 LATE CORE DISASSEMBLY - REACTOR BUILDING - 25 HOURS

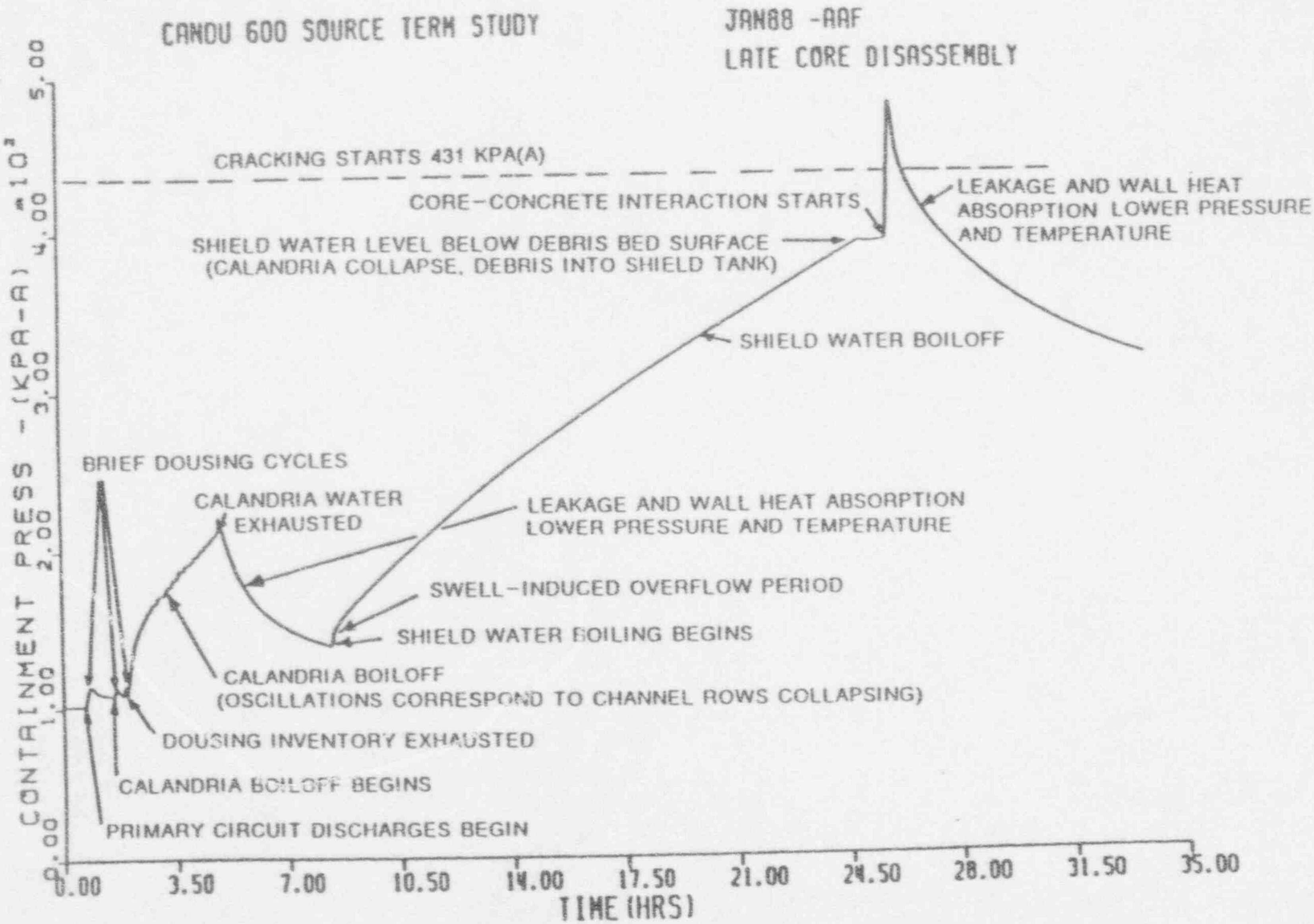
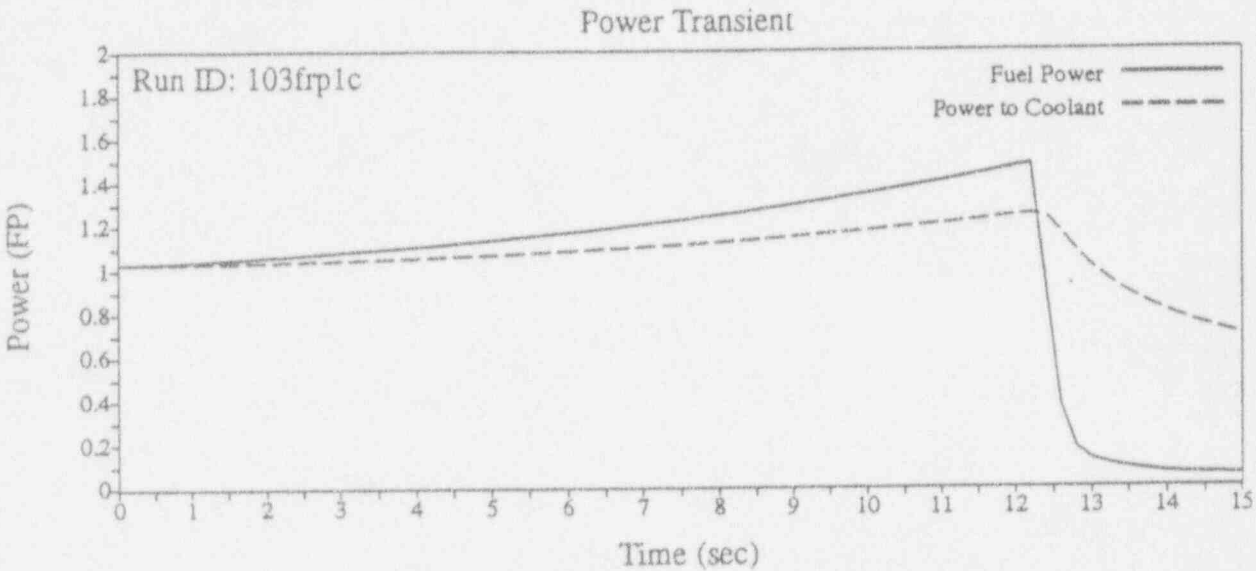
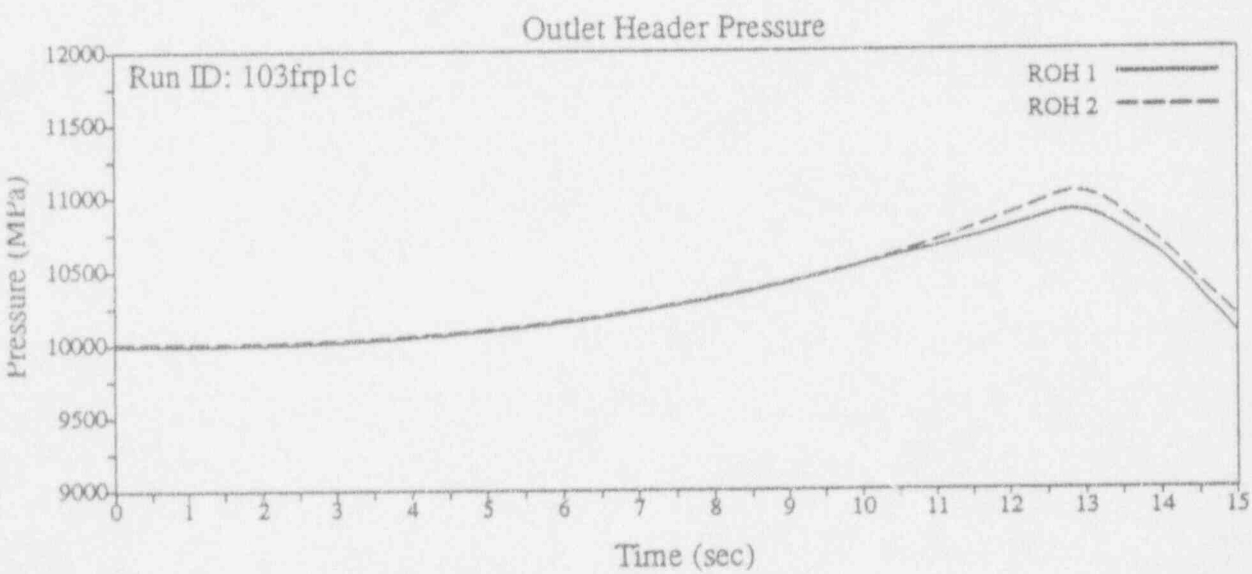


FIG. C.4-5 CONTAINMENT PRESSURE RESPONSE

CANDU 3 ACCIDENTS W/O SCRAM

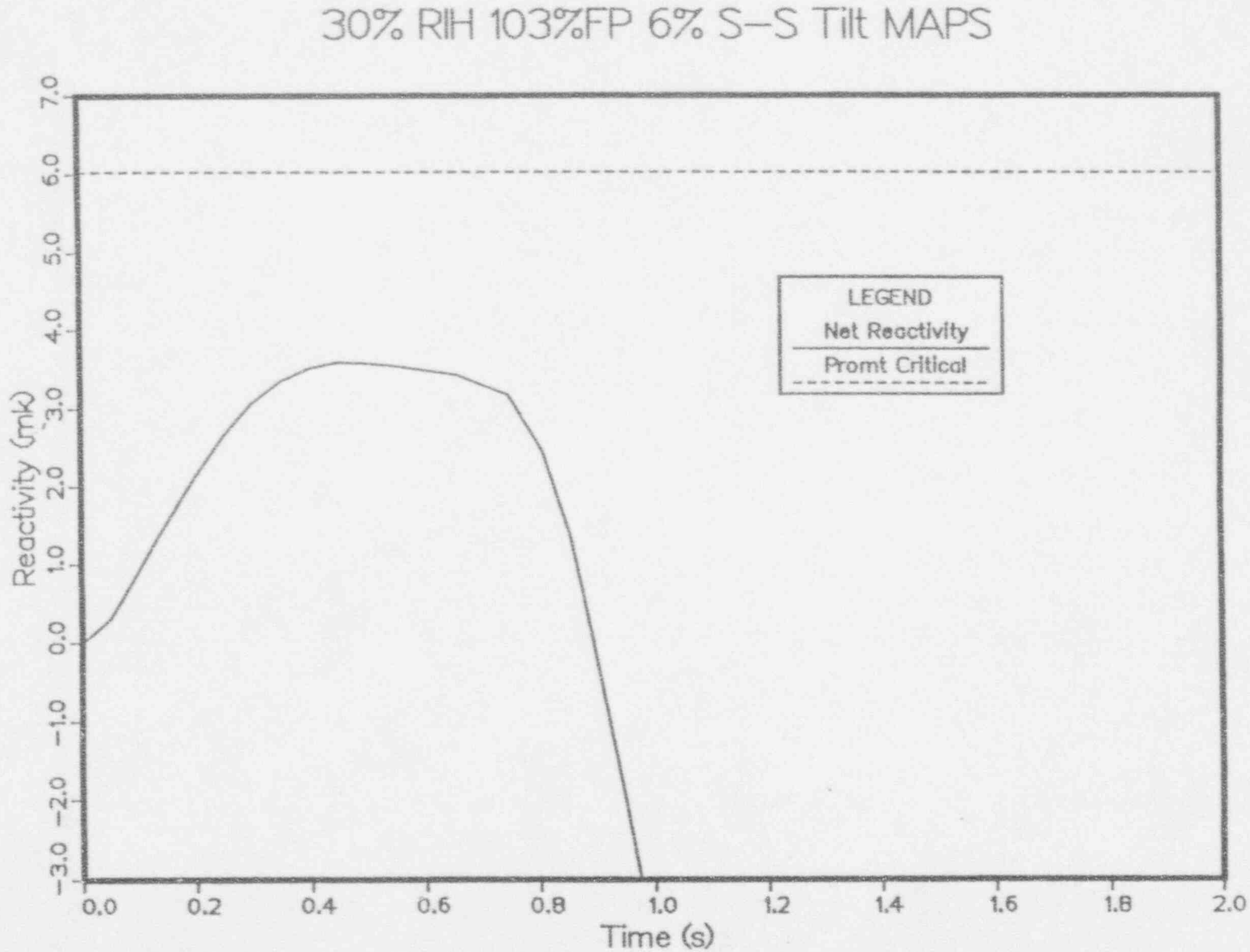
- probability dominated by loss of power regulation
  <3E–8 per year
- 1E–3 used for SDS unavailable includes failure of any one trip and loss of more than two rods or one poison tank
- large LOCA (<1E–9) gives faster transient and probably more coherent fuel heating – maximizes containment challenge



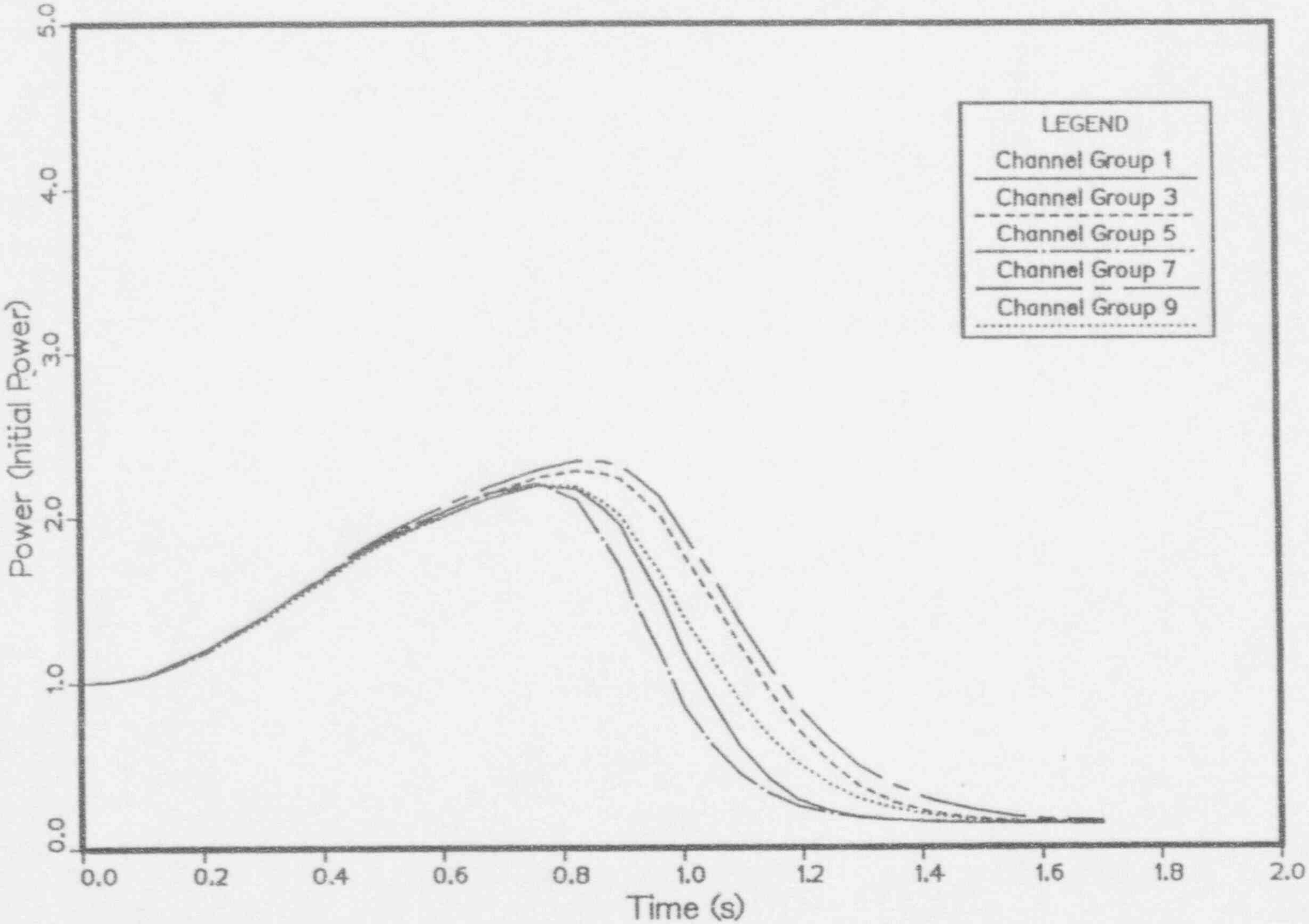


0.1mk/s from 103% FP, SDS2 Second Trip

Figure 11.1-3


30% RIH 103%FP 6% S-S Tilt MAPS
Reactivity (mk)
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1.8
2.0
Time (s)
LEGEND
Net Reactivity
Promt Critical

30% RIH 103%FP 6% S-S Tilt MAPS



LARGE LOCA W/O SCRAM

- rise in power leads to fuel melting
- large number of channels (20–100) fail within a few seconds
- steam bubble created in moderator shuts reactor down quickly after first channel failures
- energy in pulse is about 40 FPS, 60 GJ for CANDU 3
- energy transfer rates to containment will be a function of amount of moiten fuel and rate of coolant discharge (number of channel failures)

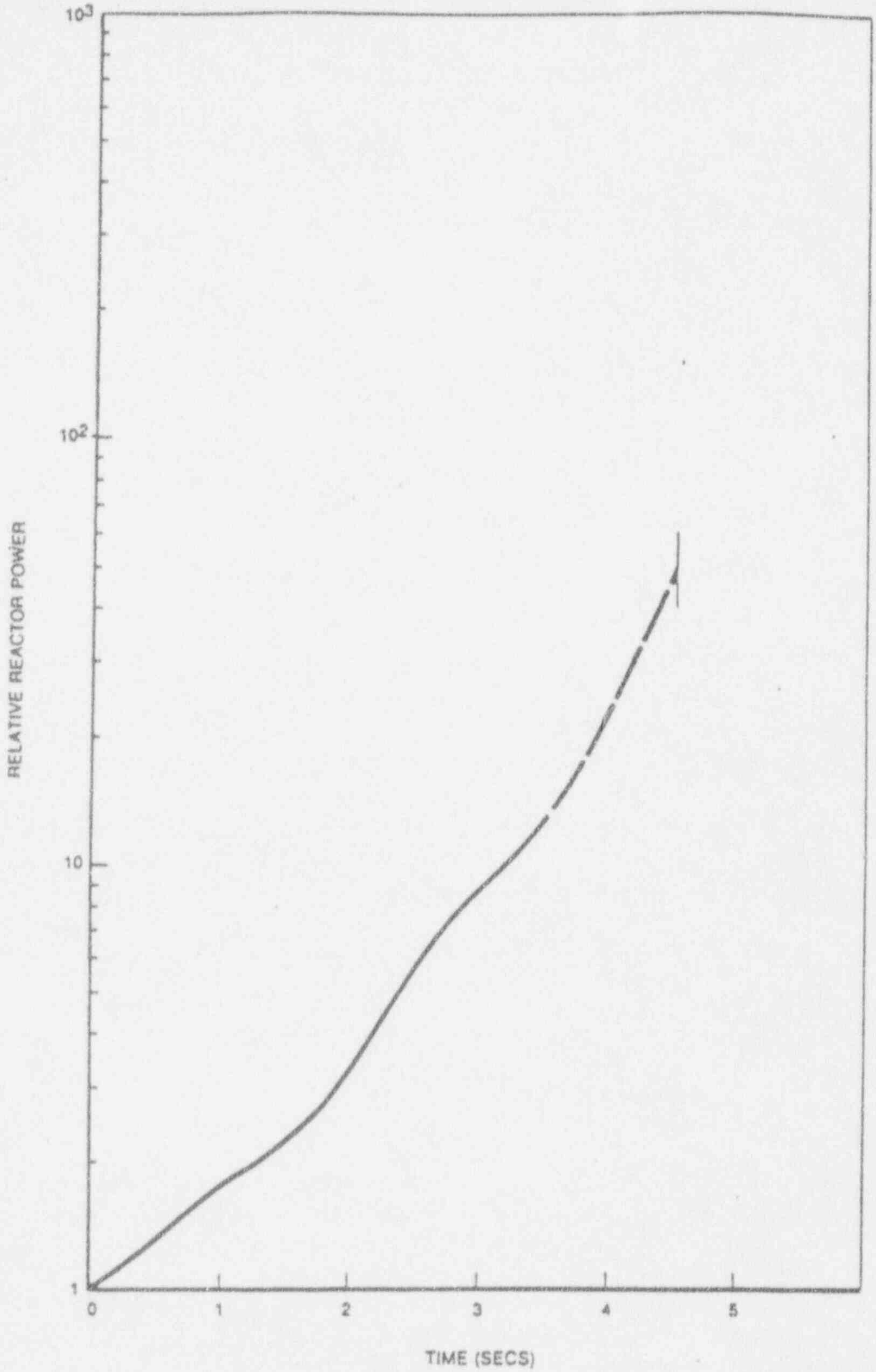


FIGURE 3.13 REACTOR POWER TRANSIENT - EARLY CORE DISASSEMBLY

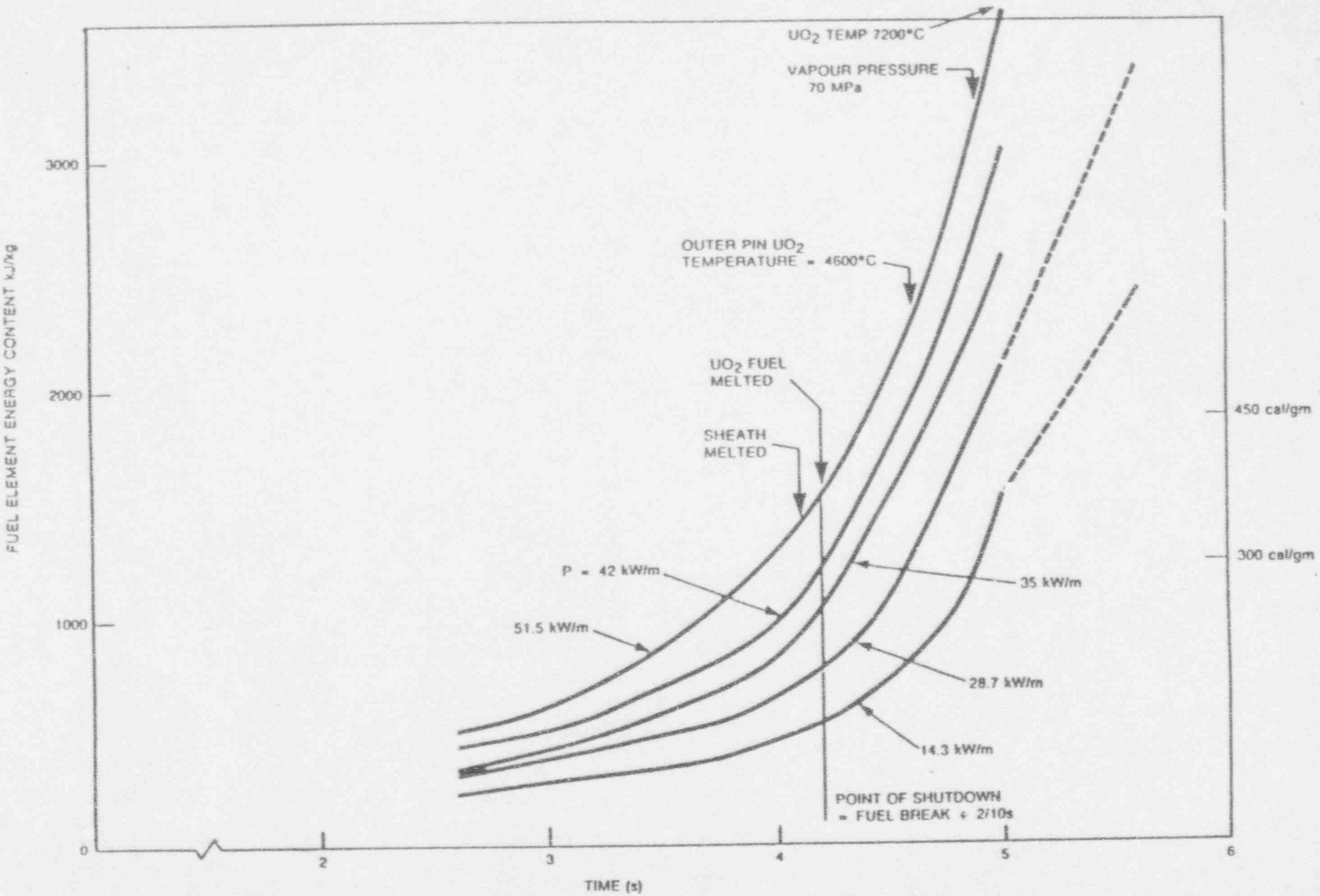
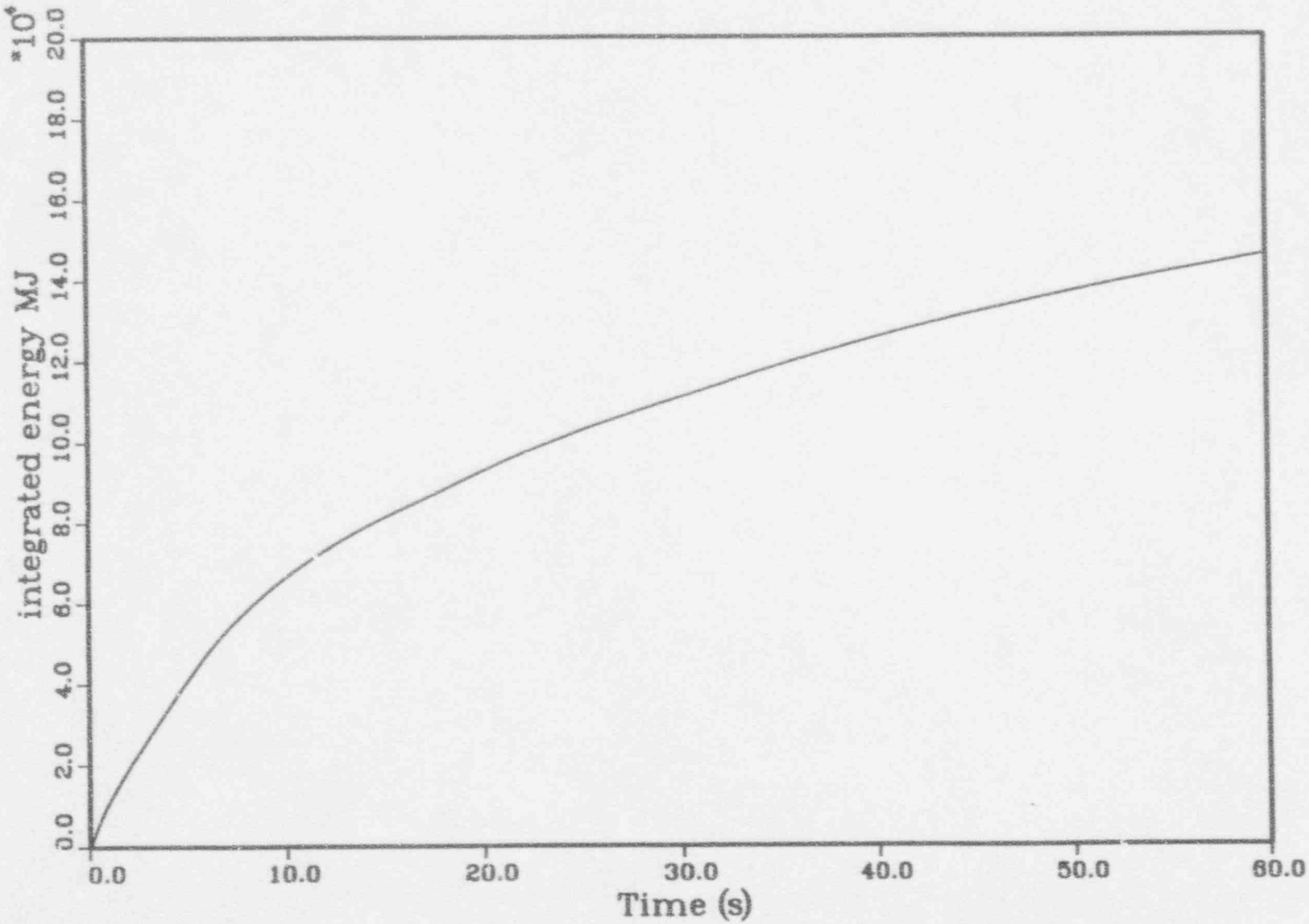


FIGURE 3.14 EARLY CORE DISASSEMBLY – FUEL ELEMENT ENERGY CONTENT VERSUS TIME FOR VARIOUS ELEMENT POWERS

100%ROH break



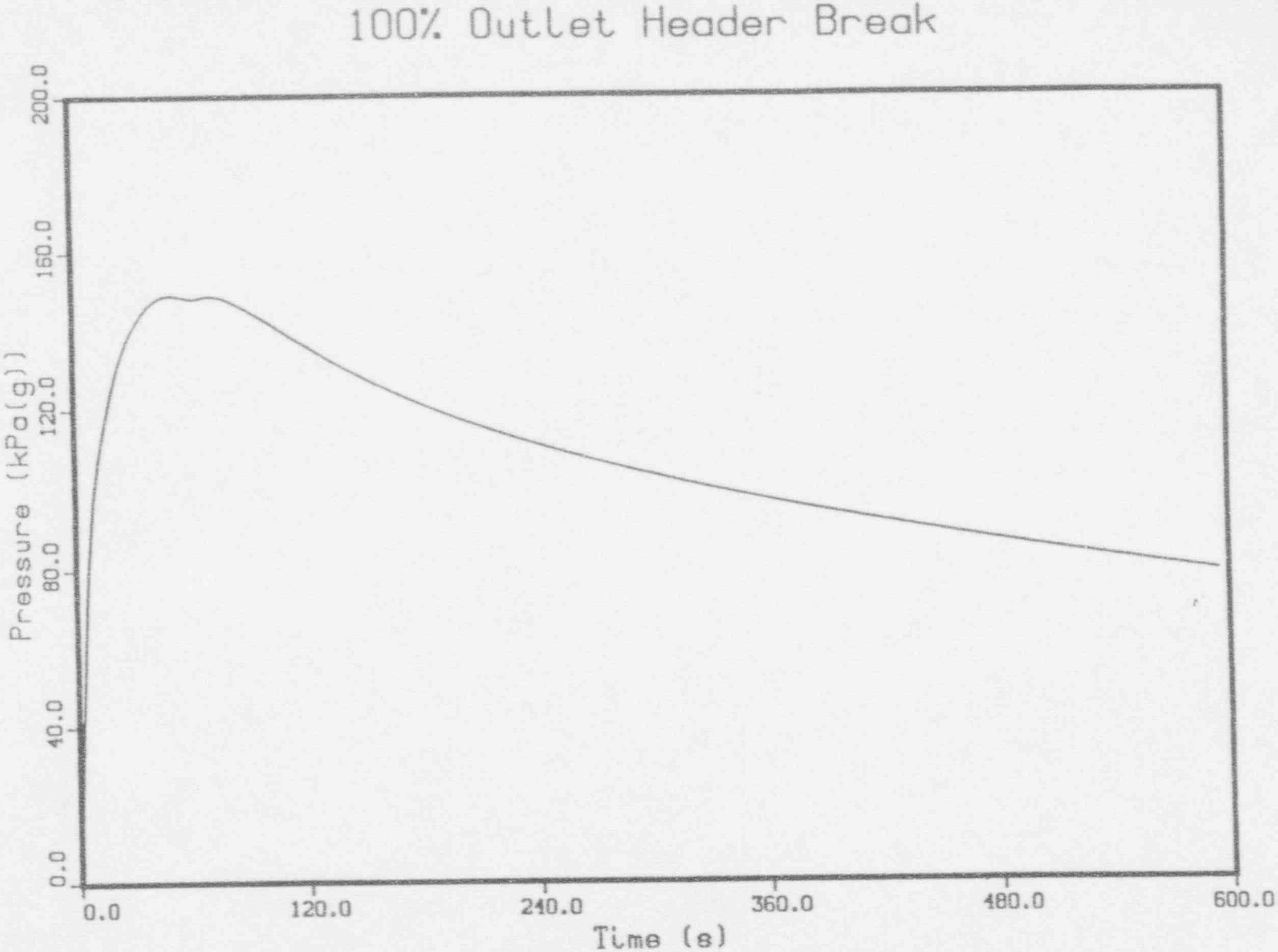
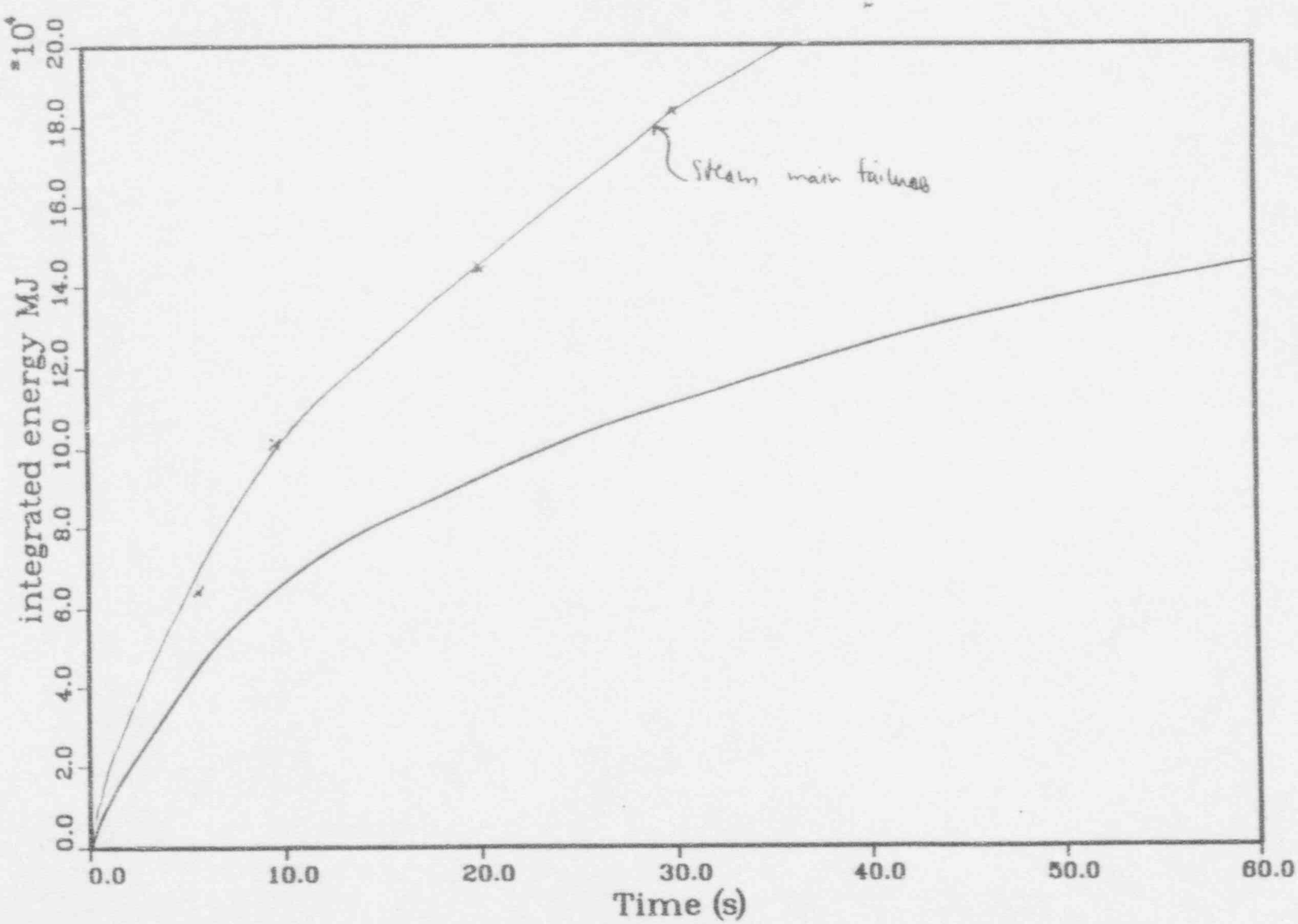


Figure 2.1-280: Accessible Area Pressure Transient
100% Outlet Header Break
Short Term

a30041/970-74
74-er
93/04/01

100%ROH break



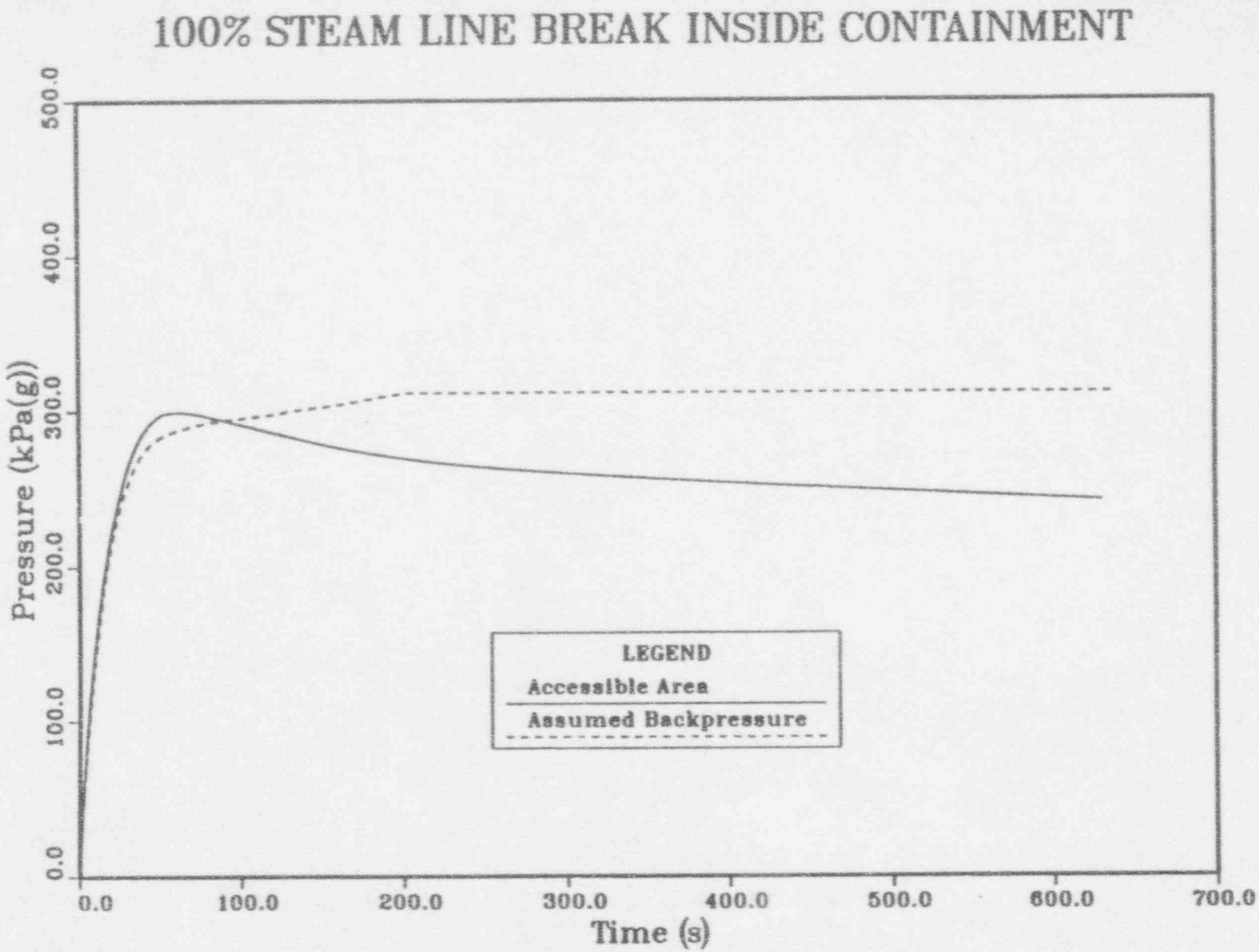
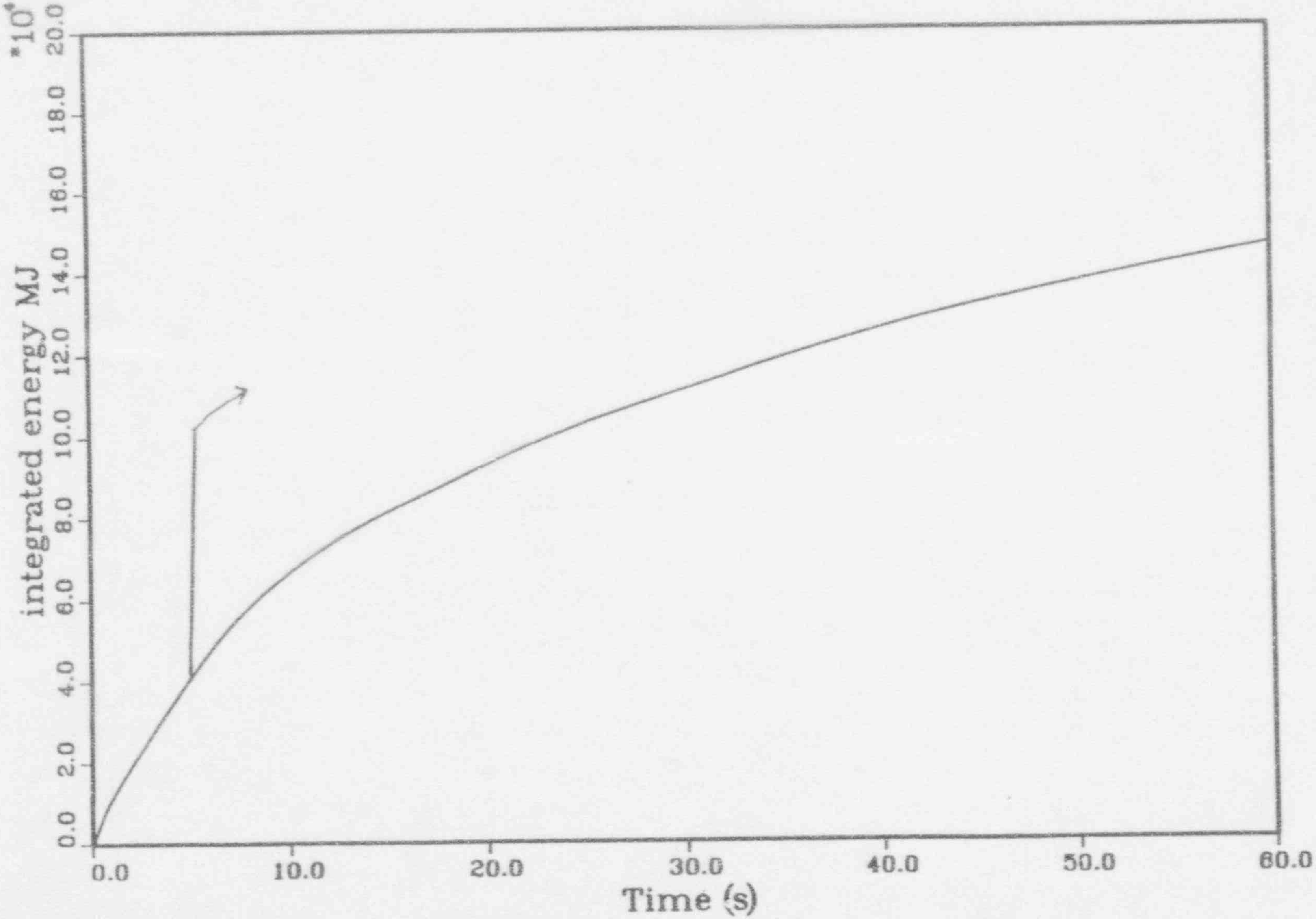
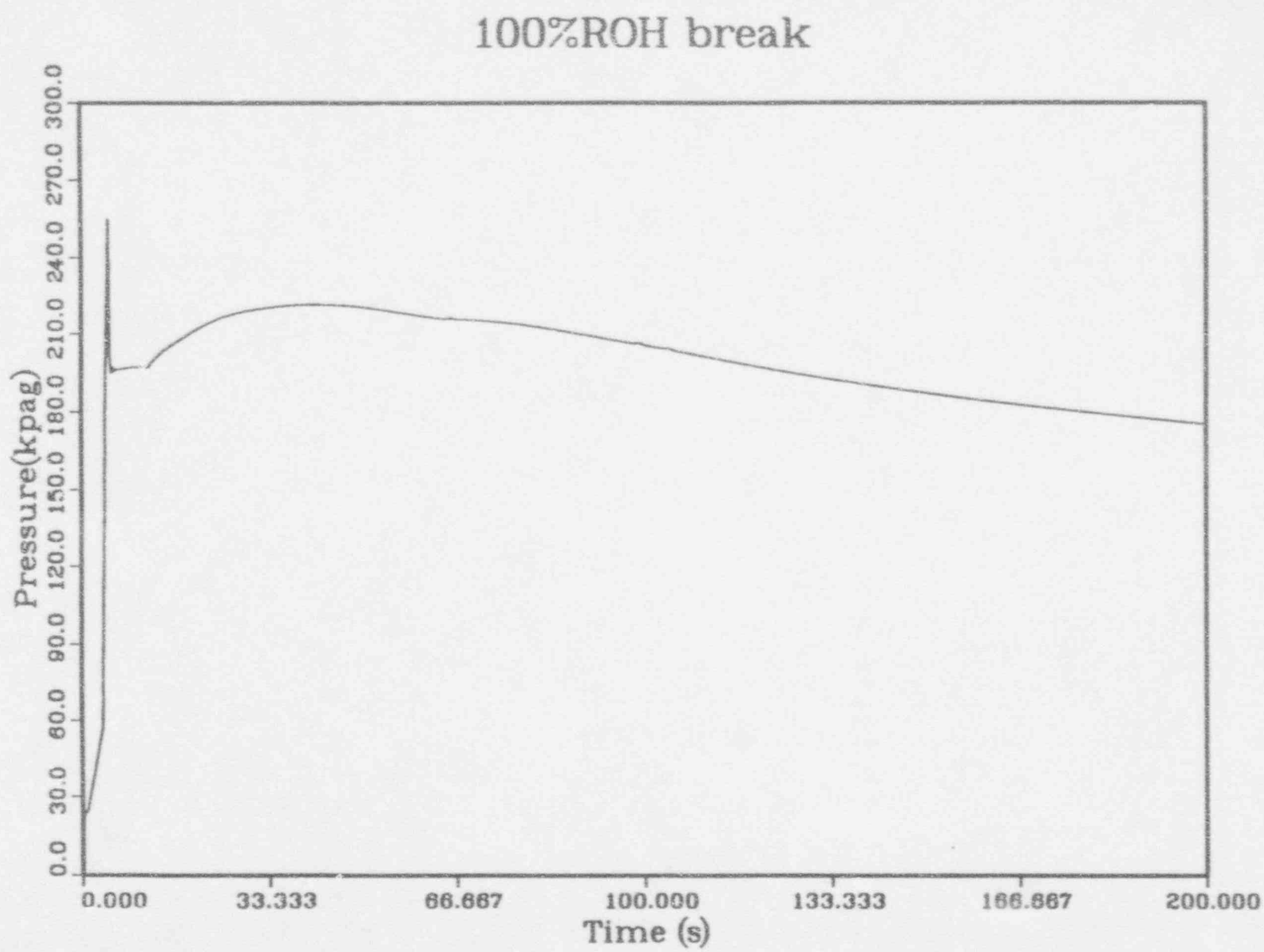


Figure 6.4-13: Case 4
Reactor Building Pressure

100%ROH break




100%ROH break
Pressure(kpag)
0.0
30.0
60.0
90.0
120.0
150.0
180.0
210.0
240.0
270.0
300.0
0.000
33.333
66.667
100.000
133.333
166.667
200.000
Time (s)

ACCIDENTS W/O SCRAM SUMMARY

- frequency consistent with residual risk (<1E–7)
- energy available for rapid transfer to containment atmosphere is limited

CONCLUSIONS

- as in all reactors, uncompensated reactivity accidents can lead to core damage
- time scale relatively slow in CANDU
- design approach has been to prevent with dual demonstrably reliable shutdown systems
- CANDU "fuse" inherently limits the energy available