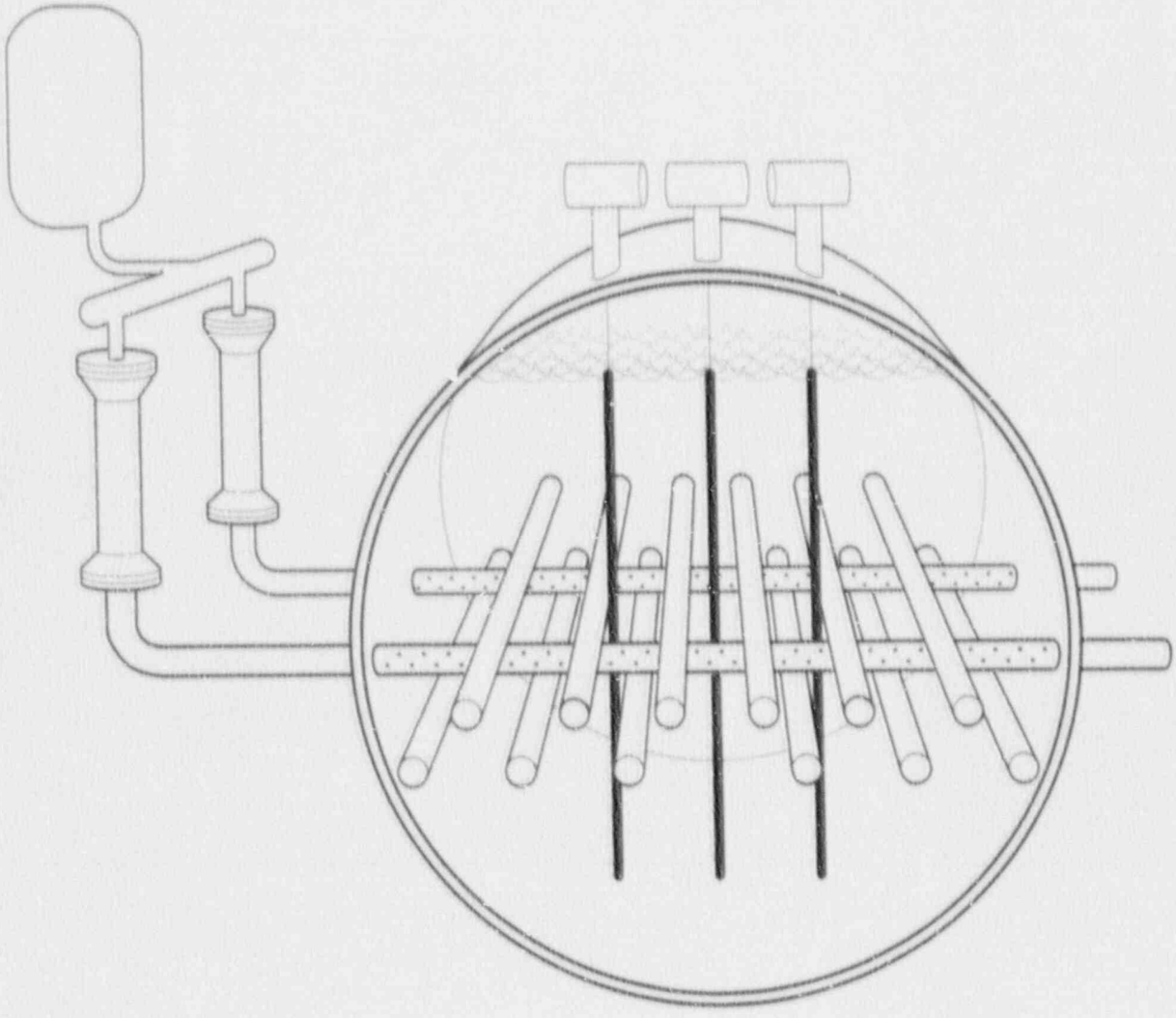
AECL EACL

AECL CANDU EACL CANDU

The Technology of CANDU Shutdown Systems

TTR-306
1991 February



TTR-306

Rev. 0

THE TECHNOLOGY OF CANDU SHUTDOWN SYSTEMS

Prepared by: A.R. Khan / S. Schafer for P. Archer

A.R. Khan/P. Archer
Control and Instrumentation

Reviewed by: N. I. Ichiyen

N.M. Ichiyen
Control and Instrumentation

Approved by: S. Schafer

S. Schafer
Control and Instrumentation

Approved for issuance by:

S.Azeez
Manager, U.S. Initiative

AECL CANDU
Sheridan Park Research Community
Mississauga, Ontario
L5K 1B2

1991 March

THE TECHNOLOGY OF CANDU SHUTDOWN SYSTEMS

CONTRIBUTING AUTHORS

SECTION		
1.	INTRODUCTION	R. Khan
2.	FUNCTIONAL ROLE OF SDS1 AND SDS2 IN CANDU	R. Khan
3.	PRINCIPLES, REQUIREMENTS AND DESIGN	R. Khan
4.	ARCHITECTURE OF FULLY COMPUTERIZED CANDU SHUTDOWN SYSTEMS	R. Khan S. Galbraith
5.	OVERVIEW OF SHUTDOWN SYSTEM DESIGN PROCESS	R. Khan S. Galbraith
6.	SDS COMPUTER SOFTWARE DEVELOPMENT PROCESS	R. Khan S. Galbraith
7.	SDS COMPUTER HARDWARE DEVELOPMENT PROCESS	R. Khan S. Galbraith
8.	SDS COMPUTER SOFTWARE AND HARDWARE PRODUCT CHARACTERISTICS	R. Khan S. Galbraith
9.	CANDU EXPERIENCE WITH COMPUTERS IN CONTROL AND SAFETY SYSTEMS	R. Khan P. Archer
10.	CURRENT ISSUES AND DESIGN DIRECTIONS FOR CANDU 3	R. Khan P. Archer
11.	SUMMARY AND CONCLUSIONS	R. Khan P. Archer

ACKNOWLEDGEMENTS

We thank M. Bonechi for his review and R. Ferguson of AECL Technologies for his extensive comments on the report.

ABSTRACT

CANDU Shutdown Systems (SDS) have a number of unique characteristics. CANDU reactors are equipped with two independent shutdown systems that are fully testable from the control room. In addition they are equipped with a seismically qualified secondary control area for use during emergencies.

The recent shutdown system designs have a high degree of computerization which permits implementation of relatively sophisticated trip logic and provides improved man machine interface. The change from analogue to digital trip determination hardware was gradual and was first introduced on the CANDU 6 reactors.

This report explains the CANDU shutdown system configuration, and the associated design principles and practices. The emphasis is Darlington SDS design which is the first CANDU to use fully computerized shut down systems. However, the report also includes more general information about fundamental CANDU SDS design concepts, including principles of accident coverage, and the manner of usage of sensors.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLES

TABLE OF CONTENTS

SECTION PAGE

APPENDICES

LIST OF FIGURES

1. INTRODUCTION

Safety of CANDU reactor systems is ensured by a variety of devices and systems. Among them are reactor process systems, control systems, service systems, containment system, emergency core cooling systems and shutdown systems. The last three types of systems together are called the Special Safety Systems. This report deals with the functional role, design principles, and the design of shutdown systems in current reactor system designs.

CANDU safety shutdown systems (SDS) have a number of unique characteristics, including:

a. Two separate and independent methods and systems for shutdown of the reactor.

b. A high degree of computerization in recent CANDU SDS designs.

c. Complete testing of the shutdown systems from sensor to final trip of the channel as opposed to only testing the electrical portion of the chain.

d. Testing of the trips is done from the control room. There is no need of intervention within the control cabinets for testing the shutdown system.

e. There is no sharing of the sensors between control and shutdown systems.

f. Trip devices, i.e., the rods and poison injection system are not used for control purposes.

g. On recent designs, neutron overpower (NOP) trip sensors are recalibrated automatically. The operator simply inserts one calibration constant into the shutdown system computers and the rest is done automatically. This process replaces manual calibration of dozens of amplifiers.

h. Independent annunciation windows are provided on the control room panel. These are in addition to the CRT message and data logging by the computer.

The computerized configuration provides means of implementing relatively sophisticated trip logic, including setpoint programming, trip conditioning as a function of measured power and automatic handling of failed sensors. Broad coverage of safety parameters, low probability of spurious trips, and improved man/machine interaction are facilitated. However, because of the safety critical nature of the shutdown system function, special measures must be taken in the design and implementation of the system, in order to ensure the software and hardware is free of latent faults.

This report is to explain the CANDU shutdown system configuration, and the associated design principles and practices. The emphasis is on Darlington design, which is the first CANDU to use fully computerized shutdown systems. However, the report also includes more general information about fundamental CANDU SDS design concepts, including principles of accident coverage, and the manner of usage of sensors, cabling, power supplies, actuators, and reactivity devices. This general information is pertinent to both computerized and conventional CANDU shutdown systems implementation.

The change from conventional to computerized shutdown systems was gradual. Digital equipment was first used on the CANDU 6 reactors. This was followed by fully computerized systems in later designs.

The function of the special safety systems is to limit the magnitude and frequency of releases of radioactivity following failures of the process systems that are required for power production.

Shutdown Systems 1 and 2 are two of the special safety systems that can make the reactor subcritical quickly and shut it down as soon as unsafe conditions are detected. This reduces the probability of further failures and is effective in preventing or limiting the releases of radioactivity from the fuel.

SDS1 relies on mechanical shutoff rods made of neutron absorbing materials. SDS2 is based on liquid poison injection into the moderator. It constitutes the second line of defence. SDS1 is the preferred system for shutdown. This preference is based on economic considerations. Because the dissolved poison cannot be removed from the moderator quickly, the use of SDS2 for shutdown makes the plant inoperable for about 40 hours due to xenon buildup following the shutdown.

The Atomic Energy Control Board (AECB) in Canada sets the requirements that must be met by operating nuclear power plants. For normal operation, the AECB has used ICRP (International Commission on Radiological Protection) recommendations for maximum acceptable dose limits for the public. For normal operation, the target set by utilities is that exposure to radiation is not to exceed 1% of the mandatory dose limits. For accident conditions the AECB specifies dose limits for single and dual failures. A single failure is a serious process system failure that can potentially lead to radioactive releases. A dual failure is a single process failure coincident with unavailability of a special safety system.

The dose limits chosen by the AECB for accident conditions are based on considerations of frequency and release. Thus the higher the frequency of the event the lower is the permissible release. The dose limits for single failures are lower than the limits for dual failure.

In addition, general guidelines are published periodically by the AECB dealing with the release and monitoring of radioactivity during normal operation and following accidents. The guidelines also cover the design of the special safety systems with respect to their reliability, testability and independence. From these reference dose limits and guidelines, the designers establish derived criteria and design requirements for the special safety systems. The relevant AECB documents are listed in Section 3.1. Documents C-8 and R-10 are particularly important.

2. FUNCTIONAL ROLE OF SDS1 AND SDS2 IN CANDU

2.1 BASIC REQUIREMENTS

The reliable and safe operation of a reactor system depends on the design of both the process and safety systems. Though safety considerations are always paramount, the design of the process and the process control systems is chiefly for reliable operation and high availability, and the design of the special safety systems is for limiting the severity and frequency of radiation releases to the public. The overall safety of design depends on the design of all components and systems, and is measured in terms of radiation releases. The Atomic Energy Control Board (AECB) has established limits on the frequency and magnitude of releases.

The limits of radiation dose to the public for the single and dual failures are shown in the table below:

AECB Guidelines for Accident Conditions

Situation	Maximum Frequency	Individual Dose Limit	Total Population Dose Limit
Single Failure	1 per 3 years	0.5 rem whole body 3 rem thyroid	10^4 man–rem whole body 10^5 man–rem thyroid
Dual Failure	1 per 3000 yrs	25 rem whole body 250 rem thyroid	10^6 man–rem whole body 10^6 man–rem thyroid

In addition to the dose limits, the AECB regulations state two requirements of the special safety systems which are basic to the risk frequency approach:

a. The special safety systems must be independent of the process systems and independent of each other. The single and dual failure approach is not valid, for instance, if a special safety system failure occurs as a consequence of the initial process failure.

b. Each special safety system must have a demonstrated availability greater than 0.999. This means that each safety system must be available to function properly not less than 99.9% of the time, i.e. the unavailability must be less than 10^{-3} years/year.

2.2 THE ROLE OF CONTROL SYSTEMS IN REDUCING RISK

The safety of the plant is first ensured by careful and conservative design of the reactor and the associated process systems. As far as possible the systems are designed to be tolerant to system transients due to their own design configuration. For example there are two circulating pumps in series in each heat transport loop so that on loss of a pump, flow through the core is reduced by only about 25%. There are fly wheels on the pump shafts that ensure that this reduction is gradual. There is sufficient volume of steam in the heat transport system and the pressurizer to cushion pressure surges due to expansion and contraction of the heat transport fluid. To maintain a heat sink for the heat transport system a minimum inventory of water is always kept in the boilers. Failure states of the valves are selected to put the system in a safe state in case of failure of the valve actuator. In some cases redundant process components are provided to improve safety and availability of systems. The layout and connections of the process and safety equipment are done to minimize common mode events. This is achieved by dividing the system into two groups. Both Groups 1 and 2 have the capability to shutdown the reactor and prevent release of radioactive material to the environment.

The design of the control system provides a first line of defense in depth to ensure safety. All critical control systems are designed to be tolerant to single and in some cases to multiple failures. This is achieved by use of redundant components in control channels. For example, sensors are triplicated and control programs are designed to detect faulty sensors and select signals from good sensors for determining control action. Most control systems are computerized and control is exercised by a dual computer system with 100% redundancy. Transfer of control from one computer to the other is automatic. For certain degraded conditions that can lead to unsafe status, control systems can automatically reduce power to a safe level, if necessary right down to zero. All power reductions by control systems including shutdown initiated by them, are completely independent of the two shutdown systems. The service systems that support the operation of process and process control systems are also divided into groups which are configured to provide the reliability required for the process systems they support. For example, to avoid common mode events, electrical power, instrument air, and process water supplies are also divided into groups.

Continued operation of process and process control systems is not necessary for safe shutdown of the reactor. No credit is taken for their availability in determining the effectiveness of the shutdown systems.

But since the overall risk to the public is proportional to the frequency of failures in these systems, or frequency of call upon the safety systems, a great deal of effort is spent on making the process and process control systems reliable and fault tolerant.

2.3 WHY TWO SHUTDOWN SYSTEMS

The basic safety requirement is that the release of radiation to the public be kept below the limits specified in section 2.1 and the unavailability of each shutdown system be less than 10^{-3}. The use of two shutdown systems is mandated by AECB. This ensures that the probability of a process system failure combined with a failure to shutdown is reduced to an extremely low number (considerably less than 10^{-6}).

The following measures are taken to ensure that the above conditions are satisfied:

a. Systems are designed to be highly reliable to reduce the calls on the shutdown systems.

b. Reliability of shutdown system components is increased by doing frequent tests on them.

c. Multiple redundant channels are used in shutdown systems.

d. Two separate, independent, and diverse shutdown systems are used.

e. Care is taken to eliminate all possible common mode events between the two shutdown systems.

Shutdown system diversity is an important feature of CANDU design. Special effort is made to design SDS1 and SDS2 to perform equally well, but using different design factors such as principles of operation, location and orientation of equipment, suppliers of components, designers, etc. The principle of diversity provides protection against undetected deficiencies in design, manufacturing and construction and against common mode failures.

The diversity between the design of SDS1 and SDS2 is in the shutdown mechanisms (see Figure 1). SDS1 uses solid rods, dropping from the top of the core under the force of gravity whereas SDS2 injects liquid poison by use of high pressure helium into the side of the core.

2.3.1 INDEPENDENCE

Independence principles are designed into the special safety systems, both within each system and between the four special safety systems. A two-group philosophy is used to maintain physical separation between the special safety systems. For the CANDU 6 design SDS-1 and non-seismically qualified portions of ECC are part of group one. SDS2, containment and seismically qualified portions of ECC are part of group two. Separation is maintained between the redundant channels, within each special safety system. Figure 2 illustrates the separation between groups and channels for the special safety systems of the CANDU 6 design.

In the CANDU 3 design the systems required for normal operation (process systems) are in group 1, while the special safety systems SDS1 and ECCS are in group 2a and SDS2 and containment are in group 2b. See Figure 33 for CANDU 3 layout.

The design philosophy applied to the two shutdown systems is to keep them functionally and geometrically independent of each other and functionally independent of the plant control systems.

Functional independence means lack of commonality in physical principle of operation, design, construction or in sharing of devices. Where possible, all of these properties of functional independence are used.

The functional independence of the shutdown systems is basically achieved by the adoption of two different shutdown principles; metallic shutoff rod drop for the first shutdown system and direct liquid poison injection into the moderator for the second shutdown system. Where the function performed is identical (e.g. use of a pressure transmitter or flux detector, etc.), separate devices are used for each shutdown system and for the regulating system.

Both shutdown systems are environmentally qualified. Accident analysis is performed to determine the limiting environmental conditions in terms of maximum temperature, pressure, radiation dose and humidity. For shutdown systems, the time to operate under harsh environment conditions is relatively short. Once the shutdown system trips, there is no need for the instrumentation to continue operating and it is only necessary to be qualified for the period of time until the trip occurs. Environmental qualification involves type tests on the critical equipment (exposed to harsh environments) which simulate the limiting conditions. Some of the shutdown system equipment is qualified for longer periods to supplement post accident monitoring; however this enhancement is not necessary for the shutdown function.

The geometric independence of the shutdown systems is basically achieved by having the shutoff rods inserted vertically in the top of the reactor and the poison injection tubes inserted horizontally in the side of the reactor. Ancillary mechanical and process equipment is similarly kept apart. The shutoff rod drives are above the reactor whereas the poison supply system is to the side of the reactor. The measurement elements of the two shutdown systems are geometrically separated. In CANDU 6 the active elements of the shutoff rod trip system are located in the control equipment room of the control centre, with the readout devices, manual trip buttons and the trip test facilities located in one main control panel reserved solely for the system. The active elements of the poison injection trip system together with the readout devices and manual trip buttons are located in the secondary control area (SCA) remote from the main control centre. Readout devices for trip parameters, a trip button and the trip test facilities for both shutdown systems are located on separate control panels in the main control room, reserved solely for that system.

Excluding the manual trip buttons and trip test facilities, there are no active elements of the poison injection trip system located in the main control centre. All signals to the main control room panel are isolated by buffering. Any possible common mode faults crosslinking poison injection channel elements to each other or to elements of any other system in the main control room, cannot affect the active automatic tripping elements of the system.

In CANDU 3 the trip logic equipment for SDS1 is located in the safety system control equipment rooms adjacent to the secondary control area. For SDS2 the cubicles containing the trip logic equipment are located in a group 2 control equipment area also adjacent to the secondary control area but separate from the area for SDS1 equipment.

Emphasis has been placed on the independence between the two groups (comprising both safety and process systems), and retaining separation between channels of systems. The same three channelized routes, however, are used for all systems in a group, by coupling similar channels of each system into one routing (see Figure 2). Except for this common routing, all other aspects of independence between safety and process systems are followed.

Each process and nuclear measurement loop essential for the operation of a special safety system is triplicated so that a single loop component or power supply failure will not incapacitate or spuriously invoke the operation of the special safety systems. The design approach emphasizes isolation between loops of different channels and between the different special safety systems. This is achieved by the use of separate transmitter mounting racks, electrical cubicles and power supplies for each channel.

The design aim is that, as far as possible, the instrumentation, logic and mechanical components for each trip parameter path be testable right from the primary transducer to the final reactivity devices. The extent and the chosen method of testing varies from parameter to parameter. It is selected to achieve the desired unavailability.

2.4 TWO GROUP APPROACH

All systems in the CANDU designs are assigned to one of two groups (group 1 or group 2). Group 1 systems are those primarily dedicated to normal plant power production. The group 2 systems include safety and safety support systems. These maintain plant safety in the event of a loss or partial loss of group 1 systems, and mitigate the effects of accidents and design basis earthquake.

To guard against cross–linked and common mode events and to facilitate the comprehensive seismic qualification of the group 2 systems, the group 1 and group 2 systems are, to the greatest extent possible, located in separate areas of the station.

Outside the reactor building separation of group 1 and group 2 systems is complete. Within the reactor building, and particularly close to the reactor, the physical separation between the two groups becomes lesser. If the separation is judged inadequate in some area, additional armour is provided such that equipment belonging to the two groups cannot be damaged in a single accident. The design of such armour is a matter of detailed design. In special cases suspected common mode events may be further analyzed in the safety assessment of the plant.

2.5 TRIP PARAMETERS

Trip parameters are selected to detect all possible failure mechanisms that could lead to a release of radioactivity and to trip the reactor fast enough to avoid further damage. Both shutdown systems generally monitor the same parameters, but in some cases minor variations may be dictated by detailed analysis of transients to achieve full coverage for all possible circumstances by both shutdown systems.

Broadly speaking, each shutdown system acting alone to shutdown the reactor has to be capable of:

a. Maintaining the primary heat transport system intact by preventing failures due to overpressure, excessive fuel temperature, or fuel breakup.

b. Maintaining containment intact by limiting both the rate of energy production and the total energy production.

c. Maintaining the reactor in a suitable sub–critical state for a period sufficient to permit the shutdown system to be supplemented by other means that may be necessary for extended shutdown after a major incident.

Design objectives are obtained by considering which mechanisms may lead to violation of the derived criteria and by setting conservative objectives to meet the criteria. For example if the intent is to prevent rupture of the heat transport system pressure boundary, then the sequence of events selected for simulation and the constants of simulation are chosen to cause maximum possible increase in pressure. The considerations are expressed in terms of design basis initiating events. The major classes of postulated initiating events are:

a. loss of regulation (LOR)

b. loss of coolant accident (LOCA)

c. loss of coolant flow (loss of grid power)

d. loss of secondary heat sinks

By doing extensive numerical dynamic analysis of all possible transients induced by failures, and careful logical analysis of all possible scenarios for many reactor designs it has been established that generally the following nine parameters have to be monitored for trip initiation.

SHUTDOWN SYSTEM TRIP PARAMETER

No	Trip Parameter	Detector Type
1	Neutron Power	Vertical In-core Detector
2	Rate Log Neutron Power	Ion Chambers
3	Heat Transport System Flow	Differential Pressure Transmitters
4	Heat Transport System Pressure	Pressure Transmitters
5	Reactor Building Pressure	Pressure Transmitters
6	Pressurizer Level	Differential Pressure Transmitters
7	Steam Generator Level	Differential Pressure Transmitters on steam generators
8	Steam Generator Pressure	Pressure Transmitters on Individual Feedlines
9	Moderator Level	Differential Pressure Transmitters

Both SDS1 and SDS2 use the same or similar parameters but the SDS2 trip settings are kept slightly different so that SDS1 fires first and SDS2 trip is avoided in most cases. For critical parameters like heat transport system low pressure and low flow both shutdown systems have the same settings but additional means are provided to bias the first trip to SDS1. For example in case of low flow SDS2 trip may be delayed and made conditional on power (as measured by SDS-2 instruments) not going down as expected due to the action of SDS1.

2.5.1 Establishing Adequacy of Trip Coverage

Adequacy of trip coverage is established by two iterative processes. The process starts with the development of a list of all possible failures that may have unsafe consequences. If the initiating process failure has a wide range of magnitude, the total range is split into many smaller ranges for transient analysis. If a fault can develop at variable rates, events involving variable rates are listed. Digital models are developed and run to determine the consequences of each fault scenario and the adequacy of each parameter for shutdown before other damage occurs is established. Depending on the results of analysis the list of scenarios is modified and the cases are further analyzed until it can be proven that all conceivable scenarios of faults have been analyzed and found to be covered by a primary and a back up trip parameter on each shut down system. For cases where purely analytical tools are not reliable enough or where suitable analysis codes are not available, experimental work is done on physical models to supplement analysis for proving the adequacy of the shutdown systems.

Table 1 shows the trip coverage of all postulated events that are analyzed for a typical CANDU reactor system. Minor variations do occur from unit to unit because of small differences in individual designs, but this table is representative of the typical process that is used to demonstrate the adequacy of trip coverage.

The symbols used in Table 1 are defined in Table 2. Table 2 also lists the instrument types normally used for each trip.

TABLE 1

SHUTDOWN SYSTEMS TRIP COVERAGE OF PROCESS FAILURES (CANDU 6)

PROCESS FAILURE		SDS-1 TRIP PARAMETERS		SDS-2 TRIP PARAMETERS	
EVENT	MAGNITUDE	PRIMARY	BACK-UP	PRIMARY	BACK-UP
Loss of Regulation	FAST	HRLOG	NOP/PHT-HP	HRLOG	NOP/PHT-HP
from High Power	SLOW	NOP	PHT-HP/MAN	NOP	PHT-HP/MAN
Loss of Regulation	FAST	HRLOG	PHT-HP	HRLOG	PHT-HP
from Decay Power (Pressurized/ Pumps-on)	SLOW	PHT-HP	NOP/MAN	PHT-HP	NOP/MAN
(Pressurized/Pumps-off)	FAST	HRLOG	PHT-LF	HRLOGL	LDP
	SLOW	PHT-LF	PHT-HP/MAN	DP	PHT-HP/MAN
(Depressurized/Pumps-on)	FAST	HRLOG	PHT-LP	HRLOGP	PHT-LP
	SLOW	PHT-LP	MAN	HT-LP	MAN
(Depressurized/Pumps-off)	FAST	HRLOG	PHT-LF	HRLOGL	LDP
	SLOW	PHT-LF	PHT-LP/MAN	DP	PHT-LP/MAN
Loss of Grid Power	----	PHT-LF	PHT-HP	LDP	PHT-HP
Loss of Coolant into Containment	LARGE	HRLOG	NOP/RB-HP RB-HP	HRLOG	NOP/RB-HP
	MEDIUM	NOP		NOP	RB-HP
(with Power Regulation)	SMALL	RB-HP	PHT-LP/P-LL	RB-HP	PHT-LP/P-LL
(with Power Regulation/ Pressurizer Isolated)	SMALL	PHT-LP	RB-HP	PHT-LP	RB-HP
(without Power Regulation)	SMALL	RB-HP	NOP	RB-HP	NOP
(with Power Regulation)	VERY SMALL	PHT-LP	P-LL/MAN	PHT-LP	P-LL/MAN
(with Power Regulation/ Pressurized Isolated)	VERY SMALL	PHT-LP	MAN	PHT-LP	MAN
(without Power Regulation)	VERY SMALL	NOP	MAN	NOP	MAN
Loss of Coolant into Calandria (with Power Regulation)	ALL	PHT-LP	P-LL/MAN	PHT-LP	P-LL/MAN
(with Power Regulation/ Pressurizer Isolated)	ALL	PHT-LP	MAN	PHT-LP	MAN
(without Power Regulation)	ALL	NOP	MAN	NOP	MAN
Steam Main Break with feed pumps on (inside containment)	ALL	RP-HP	SG-LL/BF-LP/MAN	RB-HP	SG-LL/BF-LP/MAN
(outside containment)	ALL	SG-LL	PHT-LP/BP-LP/ MAN	SG-LL	PHT-LP/BF-LP/MAN
Steam Main Break with feed pumps off (inside containment)	ALL	RB-HP	BF-LP/SG-LL/MAN	RB-HP	BF-LP/SG-LL/MAN
(outside containment)	ALL	BF-LP	SG-LL/PHT-HP/ MAN	BF-LP	SG-LL/PHT-HP/MAN
Feedline Break (Upstream of Check Valves)	ALL	BF-LP	SG-LL/BF-LP/MAN	BF-LP	SG-LL/PHT-HP/MAN
(Downstream of Check Valves)	ALL	RB-HP	SG-LL/BF-LP/PHT-HP/MAN	RB-HP	SG-LL/BF-LP/ PHT-HP/MAN
Loss of Feedwater Control (closure of valves to one steam generator)	----	SG-LL	PHT-HP/MAN	SG-LL	PHT-HP/MAN
Feedwater Pumps Trip	----	SG-LL	PHT-HP/BF-LP/ MAN	SG-LL	PHT-HP/BF-LP/MAN
Loss of Moderator Cooling	ALL	MOD-HT	RB-HP/MAN	RB-HP	MAN

TABLE 2

TYPICAL TRIP PARAMETERS FOR SHUTDOWN SYSTEMS (CANDU 6)

SDS-1 AND SDS-2

PARAMETER AND SYMBOL	SDS-1	SDS-2	DETECTOR TYPE
Neutron Over Power (NOP)	X	X	Self-powered in-core flux detectors
High Rate of Log Neutron Power (HRLOG)	X	X	Ion chambers
Primary Heat Transport High Pressure (PHT-HP)	X	X	Pressure Transmitters
Primary heat Transport Low Pressure (PHT-LP)	X	X	Pressure Transmitters
Primary Heat Transport Low Gross Coolant Flow (PHT-LF)	X		Differential Pressure Transmitters
Low Reactor Core Differential Pressure (LDP)		X	Differential Pressure Transmitters
Reactor Building High Pressure (RB-HP)	X	X	Pressure Transmitters
Pressurizer Low Level (P-LL)	X	X	Differential Pressure Transmitters
Steam Generator Low Level (SG-LL)	X	X	Differential Pressure Transmitters
Boiler Feedline Low Pressure (BF-LP)	X	X	Pressure Transmitters
Moderator High Temperature (MOD-HT)	X		Resistive Temperature Detector
Manual (MAN)	X	X	———

2.5.2 Description of Individual Trips

The selection of parameters is such that there are adequate measurements for all identified process failures. The regulatory requirements specify that all identified process failures must have one trip parameter and a back-up trip parameter on each shutdown system whenever practically possible.

Typical trip parameters and protective coverage were summarized in the previous section. The credited protective coverage for each of these trips is outlined below.

Standard industrial process control instruments are used for reading process parameters like flow, level, pressure etc. Ion chambers and special nuclear sensors of our own design are used to read reactor power. Power rate is derived from power signal by electronic means.

2.5.2.1 Regional or Neutron Overpower Trip

The Regional Overpower (ROP) trip, which is sometimes also known as the Neutron Overpower (NOP) trip is designed to give protection against loss of regulation accidents or localized power peaking which result in overheating of the fuel.

This trip is based on self–powered in–core flux detector measurements, and is meant to protect fuel from the effects of overheating.

In addition to considering loss of regulation accidents from the nominal full power flux shape, normal and perturbed flux shapes are also covered. These perturbed shapes are typically as follows:

a. single zone control compartments drained,

b. flux tilts, whether due to an absence of spatial control or driven by zone controllers draining or filling,

c. control absorbers inserted in their normal sequence,

d. adjusters withdrawn in their normal sequence, whether for reactivity shim or xenon override during a stepback or setback,

e. adjusted startup

The flux detectors require calibration on a periodic basis to ensure that they truly reflect reactor power, flux shape, the reactor CPPF (Channel Power Peaking Factor) and other operating characteristics. The CPPF is the maximum ratio (over all channels) of real channel power to its time–averaged value. This ratio can be as high as 1.15 for a channel near its reactive peak to less than 1.0 for a channel that will soon require refueling. As an example, for a reactor in its normal operating configuration at 100% of full power, with a CPPF of 1.10, the detectors will be calibrated to read 110%. This calibration method ensures that protection is provided for all channels at all times.

For plants prior to Darlington, calibration is performed manually, by modifying the gain on the amplifier associated with each detector. On Darlington, calibration is done automatically by the trip computers based on information about the CPPF and current reactor power entered by the operator.

The trip setpoints are chosen to prevent overheating of on the fuel sheath. The determination of the setpoint takes into account various possible systematic and random errors that may occur due to measurement and analysis.

The overpower trip is also the fast responding trip for large loss of coolant accidents where the induced void reactivity rate and depth exceed the capability of the reactor regulating system to maintain constant power.

2.5.2.2 High Rate of Log Neutron Power Trip

The high rate log power trip is based on out–of–core ion chamber measurements, and is designed to give protection against the following:

a. loss of regulation from low power with the heat transport system pressurized or depressurized

b. large LOCA

For a large LOCA, the induced void reactivity rate and depth exceed the capability of the reactor regulating system to maintain constant power. The high rate of neutron power trip responds quickly to this uncontrolled increase in power.

2.5.2.3 Heat Transport System High Pressure Trip

This trip is designed to give protection against the following upsets:

a. loss of grid power (loss of heat sink through loss of circulation)

b. loss of regulation (power exceeds heat sink capacity)

c. loss of secondary heat sink

This trip protects the heat transport system from damage due to high pressure.

2.5.2.4 Heat Transport System Low Pressure Trip

This trip is designed to provide protection against the following:

a. very small loss of primary coolant accidents,

b. small loss of primary coolant accidents where the reactor regulating system is capable of maintaining power constant.

It also provides limited backup coverage for very large steam main breaks outside containment. It is meant to protect the fuel from dryout and sheath failure.

To allow for heat transport system maintenance, this trip is conditioned out at very low power, typically when the log power signal from the ion chambers is less than 0.3% FP.

This conditioning also makes the trip act as an overpower trip with a set point of 0.3% power when the PHTS is depressurized, whether or not the PHTS pumps are running. Stated another way the logic is: No low pressure trip if power < 0.3%, or in reverse low pressure trip if power >0.3%.

2.5.2.5 Heat Transport System Coolant Low Flow Trip

The coolant low flow trip is designed to give protection against the following:

a. loss of grid power (through loss of circulation)

b. loss of regulation from decay power levels when the PHTS pumps are stopped, but the PHTS is pressurized. The trip occurs because of the automatic low power conditioning described below.

To allow for shutdown and maintenance, this trip is conditioned on the log power signal from the SDS ion chambers. The trip is conditioned out at very low power, typically when the log power signal is less than 0.3% FP.

This conditioning also makes the trip act as an overpower trip when the PHTS pumps are stopped, and thus provides LOR trip coverage from decay power levels with the pumps stopped.

2.5.2.6 Heat Transport System Low Differential Pressure Trip

The low differential pressure trip is used on SDS2 as an alternative to the low flow trip and is designed to give protection against the following:

a. loss of grid power (through loss of circulation)

b. loss of regulation from decay power levels when the PHTS pumps are stopped, but the PHTS is pressurized (see explanation below).

To allow for shutdown and maintenance, this trip is conditioned out at low power, on the log power signal from the SDS2 ion chambers. The trip is typically conditioned out when the log power signal is less than 5% FP (manually switchable to 0.3% FP for extended periods of shutdown).

This conditioning also makes the trip act as an overpower trip when the PHTS pumps are stopped, and this provides LOR trip coverage from decay power levels with the pumps stopped.

2.5.2.7 Reactor Building High Pressure Trip

The reactor building high pressure trip is designed to give protection against the following:

a. loss of primary coolant

b. loss of secondary coolant inside containment.

In both cases, the trip covers the large and intermediate size range of piping breaks. The cutoff point for small break protection is the capacity of building coolers and condensation heat sinks to prevent a pressure rise.

One of the purposes of this trip is to maintain the integrity of the containment.

2.5.2.8 Pressurizer Low Level Trip

The pressurizer low level trip is designed to provide protective coverage in the event of a small LOCA. The loss of inventory due to a small LOCA appears as low level in the pressurizer.

2.5.2.9 Steam Generator Low Level Trip

The steam generator (boiler) low level trip is designed to detect secondary side failures. Loss of secondary side inventory results, in low steam generator level and later degrading or loss of heat sink for the main heat transport system. This trip is to prevent overheating the fuel due to a reduced heat sink and to allow time for the operator to ensure an alternate heat sink.

2.5.2.10 Steam Generator Feedline Low Pressure Trip

This trip (also called BFLP (B=boiler)) is designed to detect secondary side failures. Depressurization of the secondary system occurs as a result of steam main and feed line breaks. A loss of feed pumps for the steam generators also causes a BFLP trip. This trip is also for preventing overheating the fuel due to a reduced heat sink.

2.5.2.11 High Moderator Level Trip

Moderator level can increase due to overheating or due to leakage of heat transport fluid into the calandria.

The moderator high level trip is designed to give protection against loss of moderator cooling either through loss of moderator circulation or through loss of service water. It could also detect a large LOCA in the core.

In earlier reactor designs this trip was implemented as a high moderator outlet temperature trip. It is then only effective against a loss of service water as it might not see the hot spots in the moderator if the circulation is lost.

2.5.2.12 Low Moderator Level Trip

The moderator low level trip is designed to give protection against loss of moderator inventory. One possibility for this to occur is through the rupture of a calandria tube. The concern with reduced moderator inventory is reduced cooling to the top rows of calandria tube and potential deflagration of the hydrogen (D2) accumulating in the increased cover gas space. Note that a reduced moderator level can also be detected by the NOP trip detectors as the neutron flux will distort in such a way as to increase in the lower part of the reactor.

2.5.2.13 Manual Trip

The manual trip provides protective coverage for all events, of small enough magnitude that do not require a trip until 15 minutes after the time the operator is made aware of the event.

3. PRINCIPLES, REQUIREMENTS AND DESIGN

3.1 CODES AND STANDARDS

The following are some of the more important codes and standards currently applicable to the design of the CANDU Shutdown Systems. In addition to documents issued by the Canadian Standard Association (CSA), ASME, and Atomic Energy Control Board (AECB) this list also includes a number of design guides produced by AECL. Design Guides supplement various Standards, clarify their interpretation, and explain the method of application to our designs.

Canadian Standards Association

CAN3-N285.0	General Requirements for Pressure Retaining Systems and Components in CANDU Nuclear Power Plants
CAN3-N285.4-M83	Periodic Inspection of CANDU Nuclear Power Plant Components
CAN3-N286.2-86	Quality Assurance During Design
CAN3-N289.1-M80	General Requirements for Seismic Qualification of CANDU Nuclear Power Plants
CAN3-N289.2-M81	Ground Motion Determination for Seismic Qualification of CANDU Nuclear Power Plants
CAN3-N289.3-M81	Design Procedure for Seismic Qualification of CANDU Nuclear Power Plants
CAN3-N289.4-M86	Testing Procedures for Seismic Qualification of CANDU Nuclear Power Plants
CAN3-N290.1	Requirements for the Shutdown Systems of CANDU Nuclear Power Plants
CAN3-N290.6	Requirements for Monitoring and Display of CANDU Nuclear Power Plant Status in the Event of an Accident

Canadian Standards Association: (Non-Nuclear Specific)

CSA-Q396.1	Canadian Standards Association Software Quality Assurance Program
CSA-Z299.1 to .4	Quality Assurance, Control, Verification and Inspection Program Requirements

AECB Documents:

C-6	Requirements for the Safety Analysis of CANDU Nuclear Power Plants
C-8	Requirements for Shutdown Systems for CANDU Nuclear Power Plants
R-10	The Use of Two Shutdown Systems in Reactors
R-70	The Use of Fault Trees in Licensing Submissions
R-77	Overpressure Protection Requirements for Class I Systems in CANDU Power Reactors Fitted with Two Shutdown Systems

Advisory Council on Nuclear Safety (ACNS) Documents:

ACNS-9	Human Factors in Power Plant Design

ASME Codes:

ASME Boiler and Pressure Vessel Code, Section III

3.2 QUALIFICATION

The SDS equipment is qualified to ensure that any accident requiring shutdown system action, does not incapacitate the SDS equipment needed to provide protection. The two areas of special qualification necessary are vibration due to seismic incidents and harsh environment due to a loss of coolant from the primary or secondary heat transport systems. The SDS equipment is also qualified for the worst conditions expected under normal operation, not necessarily related to a particular accident (examples are electromagnetic interference, radiation level, vibration etc.).

Both shutdown systems are seismically qualified to operate during and after a design basis earthquake. Seismic qualification is achieved through equipment hardening and shake testing at the seismic response levels for the equipment location. Seismic qualification also involves locating equipment in protected areas or areas not affected by failure of non-seismic systems (e.g. heavy equipment falling after a seismic incident).

3.3 MONITORING AND TESTING

Each part of the shutdown systems has a test facility. These facilities are designed to test all the parts of the trip chain, as far as possible, right from the sensing elements to the end mechanical components of the shutdown system.

A shutdown system computerized monitoring facility is also employed on some CANDU reactors to detect early signs of failure as well as aid the operator in maintaining adequate operating margins to avoid spurious trips. The monitoring facility takes advantage of the redundant channels by detecting differences to identify faulty measurements. By use of isolation techniques the independence between channels is maintained, even though the computer obtains information from all channels.

3.4 MAIN CONTROL CENTER

The control center is divided into a number of areas like the main control room, control equipment room, fuelling machine equipment room, and a shift supervisor's office.

The main control room contains the main control panels for the station.

An air conditioning system distributes conditioned air throughout the control centre and maintains a temperature of 24°C (75°F) at 45 per cent relative humidity.

The plant computers and computer ancillaries are located in a separate room inside the control equipment room.

The main control room instrumentation is designed to display sufficient information to allow the plant to be controlled safely from the main control room. To achieve this goal, all indications and controls necessary for operation are located on the main control room panels.

For the convenience of the operators, there are video display units located on their desks, allowing them to view on demand the computer–driven graphics or alpha/numeric display of important plant parameters including those of the safety systems.

Extensive use is made of computer–driven, colour graphic displays, with provision for generating a printed copy on demand. This equipment replaces many of the meters and recorders usually found on conventional panels. Sufficient redundancy is built into the display system to ensure a very high availability comparable to that of the dual computer control system itself. The use of computer–driven displays results in less congested panels and allows easier correlation of information. With greater flexibility, special display requirements can be met, while allowing infrequently used information to be suppressed during normal operation.

The main control room alarm annunciation system consists of a window annunciator, computer–driven video display units for alarm message presentation and a facility to provide a printed record of all alarm conditions with sufficient information to enable them to be arranged in the chronological order of their occurrence. Annunciator windows are illuminated independently of the computers for all alarm conditions which will cause reactor trips, power runbacks, turbine generator trips, high voltage breaker trips and other important system alarms. These windows are provided on the top section of some of the main control room panels.

3.5 SECONDARY CONTROL AREA

The secondary control area concept arises from the requirement for post–accident monitoring and control to perform the basic safety functions following any incident that would render the main control room uninhabitable.

Fire, radiation, seismic events and accidents in the vicinity of the main control room are among the causes of uninhabitability. The overall design is such that it is not necessary to regain access to the main control room soon after any such event. The plant can be maintained in a safe condition from the secondary control area.

The secondary control area (SCA) is seismically qualified for a design basis earthquake (DBE) and environmentally qualified to provide controls and indications that enable the operator to:

a. Shut down the reactors and monitor the shutdown state.

b. Effect removal of reactor decay heat.

c. Monitor necessary neutronic and process parameters, to permit assessment of the nuclear steam supply system.

d. Limit radioactivity releases in excess of allowable limits.

Seismically qualified and environmentally protected egress routes from the main control room to the secondary control areas have been provided. Control devices located in the SCA override the equivalent main control room control. The SCA permits control and monitoring of:

a. Emergency water and power systems.

b. SDS2 safety parameters.

c. Process safety parameters.

In CANDU 3 the secondary control area is located in the group 2 service building remote from the main control room and is seismically qualified. It is accessible from the main control room by several routes, one of which is seismically qualified.

The signals connecting the secondary control area and the main control room are buffered in the secondary control area. The secondary control area and its instrumentation and control equipment are seismically qualified for a design basis earthquake.

Signals from the SDS1 instruments are not taken to the Secondary Control Area and the SDS1 cannot be operated from there. But similar parameters, as read by SDS2 instruments, are displayed in the secondary control area.

3.6 DESIGN DESCRIPTION

3.6.1 SDS1 Shutoff Rods

The SDS1 shutoff rods utilizing cadmium absorber elements are provided to quickly shutdown the reactor under normal and emergency conditions. The rods, being diverse in design principle and orientation from SDS2, hang above the core, suspended from the reactivity mechanisms deck. Typical locations are shown in Figure 3 for CANDU 6 reactors which use 28 rods. The absorber elements fall into the reactor under gravity, inside a perforated zirconium alloy guide tube within the core, in response to a shutdown signal. A helical spring is compressed in the rod's "parked" position, to provide initial acceleration upon release. Typical shutoff rod construction is illustrated in Figure 4.

The stainless steel cable that suspends the cadmium absorber element, is wound on a cable sheave inside the shutoff rod drive mechanism. This mechanism is mounted on top of the reactivity mechanism deck directly above the absorber. The sheave and cable are open to the calandria atmosphere. Shaft seals isolate the sheave cavity from the gearing. The outer housings are also sealed to provide back–up enclosure of the calandria atmosphere. The vertical location of the absorber element is determined from a position indicator, fastened to the sheave shaft.

In addition to the shaft–driven indicator, a set of reed switches, actuated by a magnet in the top of the shutoff element, signal when the element is in the up or "cocked" position. The switches are mounted in a readily replaceable assembly and thus are located in a chamber isolated from the moderator atmosphere.

The cable sheave is driven by an electric motor through a gear train, engaged by an electromagnetic friction clutch. When the clutch is de–energized the sheave is released and the element falls, unwinding the cable. The fall velocity is limited by a rotary oil snubber within the drive unit. When the clutch is energized, the element may be motor–driven in or out. Shutoff rod withdrawal is normally done under control of the reactor regulating system. When the clutch is released, the drive is disconnected from the sheave and the motor driven by the regulating system cannot influence the safe operation of the shutdown system.

3.6.2 SDS2 Liquid Injection Shutdown System

The second shutdown system operates by injection of the neutron absorber, gadolinium, directly into the moderator. Figures 5 and 6 show a schematic of the liquid injection system and location of the injection nozzles respectively for CANDU 6 reactors. The Zircaloy–2 nozzles penetrate the calandria horizontally and at right angles to the fuel channels. A solution of gadolinium nitrate in heavy water is injected from each nozzle. Holes are drilled in the nozzle along its length to form four rows of jets which inject the poison upward, downward, and to the sides.

The poison solution is stored in the cylindrical tanks mounted vertically on the outside wall of the reactor vault. Each tank is connected to its own nozzle by piping which traverses the vault and shield tank.

A small diameter pipe is routed from the top of each poison tank to a helium header and thus to a pressurized helium tank. With a normal operating pressure of 8.27 MPa(g), this tank supplies the energy for a rapid injection. Typically the header is isolated from the helium tank by six quick–opening valves. These are in the usual triplicated array which allows for testing during operation. On recent CANDU reactors such as Darlington, four injection valves are used with different trip logic that allows the use of fewer valves.

A small line with a high–flow check valve connects the helium header to the moderator cover gas. Any small leak from the helium tank to the header cannot influence poison level. It stays equal to that of the moderator in the calandria relief ducts. Poison tank elevation is chosen so that poison finds a level in the small diameter pipe above the poison tank. As a consequence of the small diameter, changes in this level will not cause significant movement at the poison/moderator interface.

A polyethylene ball floats at the top of the poison tank. On firing it is swept to the bottom of the tank where it seats, preventing helium leaking into the calandria. This prevents the calandria relief duct bursting disks from failing. As an added precaution, a volume tank is connected to the calandria and relief ducts to increase the helium volume.

Typically there are six poison tanks. Each poison tank can be isolated for maintenance or sampling using two valves, one on the helium side and one on the liquid side. The former valve protects the operator in case a firing occurs during maintenance. The latter valve prevents loss of heavy water. Both valves require a key for closure; a key that cannot be removed while the valve is closed. A key interlock arrangement provides a warning should more than one poison tank be unavailable at a time.

3.7 TRIP LOGIC AND INSTRUMENTATION

3.7.1 Equipment Layout

The equipment layout for both shutdown systems is designed to maintain separation as shown in Figure 2.

The SDS1 shutoff rod drive mechanisms including clutch, motor, potentiometer, gear box and winch are located above the reactor core on the reactivity mechanisms deck plate. These are accessible during shutdown. Separate cables and junction boxes for the clutch and motor drive circuits are used to maintain separation from the regulating system.

The SDS2 instrumentation used to actuate and monitor the liquid injection system is located at the side of the reactor core. This equipment is accessible on power.

The channelized cable routings for SDS1 and SDS2 are separated within the reactor building, and exit the building at greater than 90 degrees from each other. The SDS1 cabling is routed to the control equipment room of the main control room, where its instrumentation for control logic is located. The SDS2 cabling is routed to the secondary control area, where its control logic instrumentation is located. Buffered ties for SDS2, link display and test equipment from the main control room to the secondary control area so that SDS2 can be monitored and tested from the main control room.

The field measuring devices for the shutdown systems are mounted in a manner which minimizes the possibilities of common mode failure. The connecting cables are routed back via the channelized routes to the main control room and secondary control area for SDS1 and SDS2 respectively.

SDS1 and SDS2 both have a separate control panel in the main control room for monitoring trip variables, annunciations, testing and manual trip. Displays for monitoring and annunciation and a manual trip station are also included in the secondary control area for SDS-2.

3.7.2 Channelization and Trip Logic

A common feature in the shutdown systems of all CANDU reactors, is the use of triplicated instrument channels to measure the input variables. Various schemes of two-out-of-three voting logic are employed to initiate a shutdown system trip. Such schemes use general or local coincidence voting logic.

General coincidence logic votes using the trip status of each channel, without taking into account which parameters caused the trip in each channel. Local coincidence logic votes using the trip status of the three channels for each trip parameter. The voting logic is again triplicated into a final three channels which then use additional voting logic to initiate the shutdown system trip. This additional voting is done to prevent spurious trips on single relay failures. Figures 7, 8, and 9 illustrate the use of general and local coincidence logic.

The decision to use general or local coincidence trip logic depends on considerations of spurious trips, equipment design and life expectancy, over all availability of the system, and the need for diversity in design of the first and second shutdown systems. General coincidence logic is relatively simple, easy to test and has a good degree of separation between the channels, however it has less immunity to spurious trips which represent an economic burden. Local coincidence logic is more complex, has a lower degree of separation between channels and requires more complexity to test and reject failed channels. It is thus more expensive to implement than general coincidence logic. The local coincidence logic is, however, more immune to spurious trips and thus the economic benefits must be balanced against the extra cost when choosing the type of trip logic. Both local and general coincidence logic are used in the various CANDU reactors.

CANDU 6 units used general coincidence logic for both shutdown systems. In more recent designs like CANDU 3 and Darlington general coincidence logic is used for SDS1 and a modified form of local coincidence logic is used for SDS2.

The trip system makes extensive use of relay logic. Relay trip logic is standard in CANDU stations, and has proved on the basis of wide experience to be highly reliable. Use of relays, in trip systems having simple trip parameters, leads to a very simple fail–safe design, capable of being completely tested during operation.

Recent CANDU reactors also use computers to varying extents having some or all of the following features; trip logic, display of parameters, testing and monitoring. These are described in a later section.

3.7.3 Neutronics Instrumentation

The neutronics trips for each shutdown system consist of neutron overpower which is measured using in–core self–powered flux detectors and high rate of log neutron power, measured by out–of–core ion chambers. The flux detector and ion chamber power measurements are also used for some process trips to condition setpoints and inhibit trips at low power. The SDS1 flux detector assemblies (see Figure 10) are located vertically in the reactor core from the reactivity mechanisms deck, whereas the SDS–2 assemblies are located horizontally from the poison injection side of the core. Figures 3 and 6 show typical locations for CANDU 6 reactors.

3.7.3.1 Flux Detectors

The in–core flux detectors used in CANDU reactors are of the self–powered type. This type of detector is essentially a coaxial cable consisting of an inner emitter electrode, and an outer collector electrode, separated from each other by an annular insulator. It is "self–powered" because it does not require an applied bias voltage to separate and collect ionization charge to derive a signal. Exposure to radiation causes the emission of energetic electrons from the emitter, some of which penetrate the solid insulation, reach the collector and cannot return to the emitter to recombine. The deficiency of electrons in the emitter results in a positive charge on the centre electrode. On connection to an amplifier, the electron deficiency in the emitter is made up by a flow of electrons from the collector to the emitter via the amplifier. The electron flow maintains the emitter at reactor ground (collector) potential. Therefore the detector acts as a current source (for small loads), dependent only on radiation intensity.

The current output of the detector goes to a linear amplifier, producing an output covering the range 0% to 150% full power and adding dynamic compensation for delayed components of the detector signal. On recent CANDU designs using trip computers, the dynamic compensation is performed in the computer software.

Dynamic compensation is required because the detector signal is produced by a variety of mechanisms with delayed response. Depending on the materials of construction (both of the detector and the reactor core) certain fractions of the detector signals lag behind reactor power. Lead compensation is provided to compensate for the lagged portion of detector response.

Generally, two types of flux detector assemblies are used in CANDU designs. One design uses a set of detectors wound at various locations on the assembly. These include a number of spare detectors. When the spares are used up, the entire assembly must be replaced. Another design uses straight individually replaceable (SIR) type detectors. These detectors are not wound on an assembly, but are inserted straight into a well tube. The SIR detectors are straight and thus somewhat less sensitive than the wound detectors, because of their shorter active length. The advantage of the SIR detectors is that they can be easily replaced individually.

To reduce interferences, the detectors are located so that they are not too close to adjusters, control absorbers, and zone control units.

Test facilities are provided in the control room to check the trip circuit by injection of a test current on the amplifier input. The detector outputs are displayed in the control room for the purpose of monitoring the signals for correctness, at power and during power maneuvering. There is also a facility for checking the insulation resistance of each detector. The resistance is a measure of detector integrity.

3.8 ION CHAMBERS

Three uncompensated ion chambers, located in separate housings are provided for each shutdown system. For SDS-1 each housing also contains one regulating system ion chamber, but in a separate cavity within the housing. The design minimizes the possibility of ingress of light water from the reactor vault, into the ion chamber cavities. The SDS2 ion chamber housings are located on the poison injection system side of the calandria. The SDS1 housings are usually located on the opposite side of the calandria except for some CANDU designs (such as BRUCE), where they are located at the top. Figure 11 shows a typical housing with three cavities, two for ion chambers and one for a test shutter. Figure 1 shows the location of SDS1 and SDS2 ion chamber housings for CANDU 6 reactors.

A test shutter is provided for each ion chamber housing. The test shutter is a piston-operated boral sleeve and has the capability of increasing the flux at the ion chamber by approximately 25 percent. The piston speed is adjustable to provide the necessary neutron rate signals for testing. Shutter tests for both shutdown systems are initiated from the main control room.

The SDS1 ion chamber, though separate from regulation ion chambers, are mounted in the same housing with them. The shutter or boral sleeve used to change the ion chamber signal for test purposes affects the signal from both ion chambers because they are close to each other. While testing the shutdown system the disturbance to the regulation signal can be observed to confirm that the regulating channel is active. The disturbance of the regulating signal on one channel does not disturb reactor power because the median selector rejects the disturbed signal.

4. ARCHITECTURE OF FULLY COMPUTERIZED CANDU SHUTDOWN SYSTEMS

This section describes the architecture of a fully computerized Shutdown System as exemplified by the Darlington Nuclear Generating Station design. Also discussed are CANDU 3 specific aspects of equipment location, physical separation, and channelization. Figure 12 shows the structure of the computer equipment in the shutdown system.

System separation starts at the sensor side of the Shutdown systems. Separate sensors are used in the two systems to supply information about the neutronic and process activity to the trip computers. Figure 13 shows a typical sensor layout for SDS1. All shutdown system measurements are directly connected to their respective channel computers. The computers are programmed for generating trip signals based on individual trip logic and program for each parameter as discussed in Section 2.4.2. Each shutdown system is normaliy held out of trip by a continuous effort of its three channelized trip computers. Should two or more channels fail to operate, or if they discover a trip condition, the shutdown system is released to perform its function.

Each trip computer sends information about its current state to its related channelized display/test computer. This computer displays the sensor status, for the operator, on a CRT display. It also relays requests from the monitor computer to the trip computers for gain changes, and Watchdog and parameter trip tests for purposes of supporting on–line measurement calibration and testing functions.

The display/test computer also sends data to a non–channelized monitor computer (three channels into one) which further processes the data for trending, spread checking), etc. The monitor computer includes a test interpreter function which implements semi–automatic testing of the trip chain.

Messages and test case results from the shutdown system 1 and 2 are transmitted from the monitor computers to a common higher level Shutdown System Monitor Computer (SSMC) for data archiving.

5. OVERVIEW OF SHUTDOWN SYSTEM DESIGN PROCESS

This section provides an overview of the Shutdown System design process including the high level design of the system and the design of the real–time computer hardware and software. See Figure 14 which shows the hardware and software design process.

Design of the shutdown system begins, at high level, in the process and safety design of the plant as a whole, including the design of the reactor and the associated process equipment. This leads to the definition and analysis of the design basis accident conditions which lead, in turn, to the definition of trip parameters, setpoints, conditioning logic and speed requirements, in accordance with the design standards and principles discussed in Section 3. The shutdown system designs are documented, initially at high level in the system design requirements documents, and then, in increasing detail, in the system overview design description and in detailed subsystem design descriptions, flow sheets, instrument specifications, and drawings. In the case of computerized shutdown systems, the design documentation includes computer system functional specifications, which communicate computer system functional requirements from the shutdown system overview designers to the real–time computer system designers.

Detailed design of the computer based sections of the shutdown systems begins once the functional requirements are known. See Figure 15. Hardware is selected to meet the I/O and time response requirements. For the trip computer, software specifications are created, based on the functional specifications, to define the required action for each input scenario rigorously. The appropriate specification is then used to design and code the software. Tests are performed at various stages of the design process and at various levels of system integration to ensure that the software performs correctly from the individual program module to the complete shutdown system.

After passing all tests the software and hardware is shipped to site, where it undergoes further testing and formal commissioning. Routine testing and maintenance is performed on an ongoing basis at the site, using prescribed maintenance procedures and built in test programs.

6. SDS COMPUTER SOFTWARE DEVELOPMENT PROCESS

The process and neutronic events that occur in an operating reactor are analyzed to provide values for trip setpoints, conditioning values, and response times. This information is used to produce requirements for the shutdown system software as described in this section.

This section provides a more detailed view of the Software development portion of the design process. The development methodology is still evolving. The present discussion is based on Darlington experience and practice. The style and content of the documents produced as a result of the design process is defined by AECL procedures and a programmer's handbook. See Figures 16, 17, and 18 which show the software and documentation life cycle used for Darlington. Figure 19 shows an organization chart that is produced as part of the software QA process.

6.1 DESIGN REQUIREMENT DOCUMENT

This document is produced after sign-off of the Conceptual Design Specification for a program by the Design group. It provides a basis for the verification and review of the system designed. It is required to be produced as part of a package of formal documents for a client, and/or for Quality Assurance.

Design Requirement documents include all known limits and constraints, interfaces and interactions with other systems, jurisdictional and safety requirements, reliability and maintainability requirements and a clear indication of all normal and abnormal modes which the system designer must consider. The technical basis for design requirements is not included as part of the Design Requirement document but, rather, is referenced in supporting documents.

6.2 SOFTWARE DEVELOPMENT PLAN

At the outset of the design, a software development plan is prepared which defines the development process to be followed in the design of the software. The Software Development Plan was introduced to the Darlington Shutdown System in order to provide a systematic approach to software development (and to meet the requirements of CSA-Q396). It's scope was limited to the application software for the shutdown system computers. Previous projects had followed company procedures, past experience and existing guidelines to develop code. Figure 15 shows the resulting procedure/plan that was developed for Darlington.

Software design activity follows the preparation of a Functional Specification for the software, based on higher level technical requirements for the Shutdown System.

6.3 FUNCTIONAL SPECIFICATIONS

Once the required response of the Shutdown system is determined, functional specifications are created for the operation of the computers. The Functional Specification is a requirement of the Software Development Plan. The functional requirements defined in the specification must be sufficient to ensure the system will meet design requirements, and will perform satisfactorily in service. The information necessary for the preparation of a Functional Specification is extracted from the following documents: Design Requirement, Design Description, Design Calculations, Design Reports. The document must specify the general functions of the computer, the Input/Output requirements, algorithms associated with the functions of each computer, setpoints and signal ranges, alarms and displays, signal deadbands, computer initialization, self–testing and external tests, trip timing requirements, treatment of irrationality, and historical trend and other data storage.

6.4 SOFTWARE DESIGN SPECIFICATION

Defining the software function may include an additional step of preparing a software specification, which uses an algebraic like notation, to remove ambiguities. This is required for Trip computers, and optional for the other computers under the Darlington software development plan. During code testing it is possible to use this specification to produce test procedures.

The Software Design Specification is a documented interpretation of the functional requirements specification. It describes what the software must do, but not how the software should do it.

The document must do the following:

a. Describe all the requirements related to functionality,

b. Describe every software response to all possible inputs,

c. Be verifiable against the Functional Specifications and the resulting software,

d. Be unambiguous and free of redundancy.

The Software Design Specification contains notation intended to allow abstraction of data and expressions and yet permit easy identification of the type of mnemonic name by bracketing symbols. This also provides a common formal notation standard that avoids ambiguities. The notation includes relational operators that allow comparison of quantities that result in a boolean result of TRUE or FALSE. Also boolean operators are provided to allow a full range of input conditions to be modelled. Additional time operators allow the notation to describe real time events.

For example /anyname/ indicates that the mnemonic refers to an external input, while !execute! represents an expression that is a combination of data, boolean and relational operators.

Relational Operators consist of =:, =, <, <=, >, >=, <>, while Boolean Operators are AND, OR, NOT.

A conditional expression evaluates to TRUE or FALSE and may be compounded with Boolean Operators. An Event occurs at a moment in time when a condition becomes TRUE (@T) or FALSE (@F). WHEN is also used to refer to the pre-existence of another condition that must exist prior to the current condition in order to take action.

As an example consider the case where a digital output must be opened when a reading is above a setpoint value.

	(A)	(B)
	/reading/ > /setpoint/	/reading/ <= /setpoint/
action	//DigitalContact//= open	//DigitalContact//= closed

Column A is read as: whenever the reading input is greater than the setpoint input then set the Digital Contact output to open. Column B is read as: whenever the reading input is less than or equal to the setpoint input then set the Digital Contact output to closed.

6.5 CODE DESIGN

A high level design of the software is then produced, based on Pseudo-Code and/or Data Flow diagrams. The Pseudo Code allows the use of a structured English-like description (without an undue concern about syntax) to create a description of the prescribed software function. The Data Flow diagrams provide a high level view of the required functions, ordered around the flow of data, which can improve modularization and simplify interfaces. This is formally reviewed by other qualified programmers and by the shutdown system functional designer to ensure that the design meets the specifications intent before coding begins. The results of the code design, along with a module description, are placed in a design description when the design and coding are complete. See Figure 17 which shows the software life cycle and documentation requirements. A Hierarchy diagram is included to provide a map to the program structure from the highest level function to the lowest.

6.5.1 Pseudo Code

Pseudo Code is used to convey the logic of an algorithm without the necessity of computer-correct syntax. The pseudo code key words are chosen to be a high level english-like notation that bridges mathematical notation with the actual language used on the target computer. The following is a sample of some key-words suggested by the programmers handbook (described later in section 6.14) for use with pseudo code:

ACTIVATE "Module Name"

DO

END DO

LOOP WHILE

END LOOP

6.5.2 Data Flow Diagram

Figure 20 is a typical Data Flow Diagram. A data flow diagram is a graphical technique that shows the transformation and movement of data from an input location to an output. It is constructed with layers of abstraction, each layer providing increasing levels of detail of an increasingly narrower scope. The emphasis is on the flow of data rather than the flow of control.

A typical data flow diagram contains up to four basic symbols which are:

processes
- symbolized by rectangles,
- transformation of incoming data flow(s) to outgoing data flow(s).

data flows
- symbolized by arrows,
- data travels along the arrows to the next section.

data stores
- symbolized by a U–shaped symbol on its side,
- a store or repository of data.

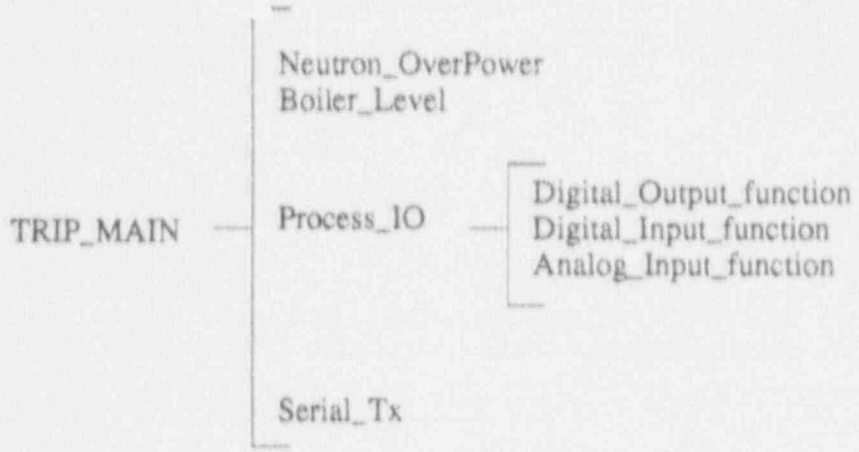
external entity
- symbolized by square boxes,
- a source or sink of data.

The data flow diagram is also created to document the software produced in a design description.

6.5.3 Hierarchy Diagrams

Hierarchy Diagrams are used to assist in the modularization of the code design. It is used to describe the hierarchy of the program with the upper (or left side) layer function calling the functions on the next level below (or to the right).

For example a hierarchy diagram of a simple trip computer might be as follows:



Thus TRIP_MAIN calls Neutron_OverPower, Boiler_level, Process_IO and Serial_Tx to perform its function. Process_IO in turn calls Digital_Output_function, Digital_Input_function and Analog_Input_function.

6.6 UNIT TESTING

As each module of code is created, it is "Unit" tested to ensure that it performs as required (as defined by the design). Performing a unit test ensures that the specific module is problem free before adding other modules. Trying to debug several modules at once makes the identification of the true source of the problem much more complex.

The Unit test is used to detect errors and test for functional completeness. They are performed on new or revised software and include the following checks:

a. Coding standards met,

b. Error free assembly and compilation,

c. Initialization and proper handling of exception conditions,

d. Functional requirements have been met,

e. Test of Data flow across modules (module interface),

f. Test of Local and global data structures,

g. Important paths and statements have been executed,

h. Boundary conditions defined and suitable.

Records of the Unit test are kept and are summarized with a Unit Test Checklist summary. For the trip computers, prior to the start of a test, a test plan must be prepared for all the unit tests, and must be reviewed and approved by an independent reviewer who has not been directly involved in coding the program. A test log is kept for the trip computers and it describes the results of the tests performed. Any special test conditions are included in the log which may also include the test plan.

The test is declared complete by the unit tester (and for the trip computer – the reviewer) when they are satisfied that the software meets the design requirements. The results are filed in AECL's Technical Documentation Service (TDS) to allow audits by clients and the Atomic Energy Control Board (AECB).

Failure of a test may result in modifications to the design and further testing.

6.7 PRELIMINARY INTEGRATION TESTING

Once all modules for a specific computer are created and Unit Tested, they are "Integration"–tested as a whole, by an independent test team against the Software Design Specifications to ensure that they perform correctly together. A test log is kept and filed along with test results in TDS at the successful completion of testing. At this point the software is frozen, and can only be changed by following a strict QA procedure described in section 6.12.

6.8 VALIDATION TESTING

For the trip software the next step is an additional type of test, called the "Validation" test, which is done, by the shutdown system (SDS) functional designer, after the software designer is satisfied with his product (Figure 21). This Validation testing examines the code as a "black–box", which must produce the specified response to the specified stimuli. The validation tests are performed by the SDS designer to ensure that the intent of the design specified in the Functional Spec was conveyed to the Software designer and that the resulting code correctly performs that function. Any problems are corrected in both the functional specification and the code. This is formally documented by raising a Software Change Record (SCR) which records the problem and the solution.

A Validation Computer is used to semi–automatically execute an extensive repertoire of Validation test cases (Figure 22). These test cases are written by the functional designers in a high level interpretive language that is run in a special purpose Validation Computer, which simulates the external environment of the plant to the Trip Computer. Data from the trip computer sent over the communication link may be used to verify that the trip computer has performed a certain action after a specific stimulus. Test requests sent to the trip computer over the communications link are tested during validation. Once the Validation Computer has been programmed with the test cases selected by the Functional Designers and the test is started, the validation process is automatic and self–documenting. There are however, a few supplementary tests that require manual intervention to complete and these are also fully documented.

The following is a sample of a typical interpreter commands:

SET LOGN to –2.04 DEC

CHECK VALVE IS OPEN

WAIT_UNTIL PRESSURE IS > 15

SET DO_1 TO OPEN

Prior to running the validation tests a Test Plan is prepared which cross–references the Functional Specification with the Validation test cases, in order to ensure that all features of the design are tested.

As an example of a typical Test case sequence consider the trip response for a process signal (figure 23 shows a typical signal range). The tester takes the response requirements from the Functional Specification and creates a test procedure that places the trip computer into an untripped initial state. The validation computer verifies this reading and the state of the trip digital outputs. The test then slowly drives the pressure signal up towards the setpoint while monitoring the trip digital outputs for an indication of trip. The time taken to trip, from the point the value exceeds the setpoint, is measured and recorded as part of the test. The signal is then moved back down and a corresponding clearing of the trip digital output is recorded against the signal value. The test results are then compared against those expected in order to determine the success of the test. All test results are collected into a test report after successful completion of testing.

6.9 SYSTEM INTEGRATION TEST

After the code has been tested in the Trip, Display/Test and Monitor computers, the complete computer shutdown system is tested as a whole, in a "System Integration Test" (SIT), in order to ensure that the subsystems perform correctly together. Most of the overall testing is done at AECL but some of the SIT may be performed at site, where there is a full complement of shutdown system hardware.

A complete channel is tested from Trip through Display/Test to the monitor. In order to create the normal loading of the other two channels at the Monitor a simulator feeds typical data into the links.

Prior to running a SIT test a test plan is prepared which outlines the scope of the test and the steps required to complete it. Each step includes a sequence of actions and expected results. Successful completion of a test is declared when the test plan and test results are in agreement, or differences are explainable and acceptable. Any errors or differences are also documented in a SCR.

A SIT test shares some similarities with Validation testing. It does however, require more manual interaction, since the displays and operator inputs must be run as they would be used by an operator.

6.10 COMMISSIONING

After passing all tests, the software is formally issued to site, where it undergoes further testing and formal commissioning.

A commissioning procedure is a formalized document that lists each step to be followed in order to test the item being integrated into the site equipment. Each step indicates an action and the expected result from that action.

In addition to normal CANDU commissioning procedures, for Darlington an additional test was added by Ontario Hydro to perform random testing on the trip computers. To perform this test another computer was connected to the I/O of the Trip Computer. Randomly selected values of all variables were fed into the Trip Computer and the results were checked for correct response.

Over 7000 tests based on postulated accident trajectories selected randomly were performed. A small number of tests were also done manually. Testing was limited to one of the three identical channel computers working alone, This was considered adequate because the three channels are independent of each other, and run identical software.

6.11 PERIODIC TESTING

Routine testing and maintenance is performed on a continuing basis on the operational system using maintenance procedures and built in test programs. Unavailability requirements are used to set the testing frequency. After testing has proceeded for some time the results of the test data may be used to decrease or increase testing.

At the Darlington Nuclear Generating Station the Shutdown System monitor computer also provides a test interpreter program that behaves similarly to the validation test interpreter. These test cases are structured to test the entire system, where practical, from the physical measurement of the process to the signal used to actuate the shutoff device.

For example, one of the reactor trip parameters is a trip on the logarithm of the rate of change of neutron power - a signal derived from an ion chamber mounted at the side of the reactor vessel. To test the log rate trip function, the operator activates the withdrawal of the shutter away from the ion chamber. This causes the ion chamber to sense a high rate of change of neutron flux in the positive direction. This modified signal simulates a power excursion. The trip computer responds by opening its output contacts exactly as in a trip situation and the channel trips. The other two channels remain in an untripped state. Testing cannot be performed if one of the other two channels are in the tripped state. See Figure 24 for a functional block diagramer for one trip parameter.

6.12 DEVELOPMENTAL ADMINISTRATION PROCEDURES

The Darlington software design process included administrative procedure which had the purpose of ensuring that current software was archived, software changes were controlled, and records of changes were kept.

Strict control of software is important on a multiple person software project. Without module control it is quite often common to have concurrent changes being made to a module by different people. Trying to decide which version of the module to use, and how to merge all the changes can become very difficult. This can be solved by allowing only one person at a time to work on a specific module, and to keep the latest version of the module in a centralized location, as was done for the Darlington project. Keeping records of previous versions of software allows for the generation of change lists, and the ability to recover code for study at some future date. These are tasks ideally suited to computers and there are currently several available configuration management packages for various types of computers.

The administrative procedure is as follows:

Each listing, which can consist of one or more code modules, is assigned a unique number. When the code has finished development and has passed testing, a copy is sent to the library as a master. Any changes from this master copy must be documented with a Software Change Record (SCR) which explains the problem and describes a solution to fix it. The problems and changes must be reviewed and approved. When the corrective action has been taken the SCR is updated to document its completion. Though not a requirement for the Darlington Shutdown System the software may also be placed under computer driven Configuration Control which prevents more than one person changing a section of code at a time, and keeps track of the changes made to each module in a way that allows complete recovery of any revision of the software. This was used for development of SDS2 trip software.

The design of CANDU 3 is not far enough advanced yet and the method of administrative control of the design process has not been selected.

6.13 PF TABLES

For Darlington, an additional formal verification technique using Program Function (PF) tables was added for the Trip Computer Software. This approach was first suggested by D.L. Parnas of Queen's University and further developed by Ontario Hydro. This was done to demonstrate to the Atomic Energy Control Board (AECB) that the code matched the software specification. PF tables contain columns of conditional expressions that cover the complete domain of the function and rows that are a program variable. The cells contain an expression that is the terminal value of the variable for the conditional expression. The software specification is also converted to this form and then compared with the code PF tables. This method of static analysis verifies that the software implimentation matches the requirements.

This process results in a large amount of tables and requires an immense manpower effort for a small amount of code. As a result a sub–set of the PF tables was presented to the AECB as a sample to demonstrate that the coding process was producing code that matched the Software specification.

For future designs a modified form of PF tables is being considered. They would become part of the design process which would simplify the verification process and documentation.

6.14 DOCUMENTATION OF SOFTWARE

A certain amount of documentation has been implied by the preceding sections. Typically when a design is completed, and before the designers move onto other things, all of the details that contributed to the design are gathered together and saved as a set of documents for that particular project.

The specification documents have already been described. The design document (DD) is produced prior to validation testing.

6.14.1 Software Design Description

The Design Description is composed of the following main sections:

Hardware Environment – explains the design considerations imposed by the hardware and the effect that the software has on the hardware.

Software Environment – explains the requirements for supporting software (i.e. databases) and the relationship between this software and any other software.

Design Description – gives a general description of the software structure. It contains sub–sections that include data flow diagrams, process descriptions and a data dictionary. Data flow diagrams were introduced in Section 6.4, since they are used in the code design phase. Process descriptions and the data dictionary may be produced at the same time, and are used to preserve the information that the designer uses to create the data flow diagram. The process descriptions summarize the function of each process identified in a data flow diagram. The data dictionary defines all information identified on a data flow diagram as data flows and data stores.

Module Decomposition – contains diagrams and other information to show how the program is decomposed into modules and subroutines.

Module Descriptions – contains sub–sections that document the structure, data and function of modules identified in the decomposition section.

Module Interfaces – describes how the data is supplied to the module.

6.14.2 Programmers Handbook

The Programmers Handbook is a collection of documents that describe the terminology, format, administrative procedures, program development and test guidlines, software tools, and interfaces etc. that are useful to the programmer in coding the software. In general it is not as formalized as the functional specification or design descriptions.

7. SDS COMPUTER HARDWARE DEVELOPMENT PROCESS

This section provides a more detailed view of the hardware development process used for the real-time computer system.

7.1 DESIGN REQUIREMENTS

Based on the system requirements and the design goals, hardware is selected to best meet the requirements. A Technical Specification is prepared that describes the characteristics of the required hardware which is approved before placing an invitation to tender. This specification also states the environmental requirements and the method of testing to demonstrate compliance. Acceptance tests are a combination of type testing of some hardware, often to destruction, and qualification of equipment to be installed. This process is further described in the following sections.

7.2 HARDWARE SELECTION

A tender document is produced specifying the features that the system is to have, including specialized hardware requirements. Bidders are selected by their ability to meet the requirements. Hardware is delivered to site to the Canadian Standards Association CAN3 Z299.1 hardware QA standard. Some of the components of the system may be obtained at a lower QA standard level, Z299.3, if they are vendor components that are widely utilised. AECL's lab will inspect them and test them to the Z299.1 QA level before they are sent to site.

7.3 ACCEPTANCE TESTING

When the vendor delivers hardware to AECL it undergoes acceptance testing to verify that the supplied hardware meets the specifications. The test usually consists of programs that subject the equipment to a pre-determined sequence of operations. Usually these tests use the hardware diagnostics supplied by the manufacturer.

Typical diagnostics test the following: CPU, RAM, ROM, Digital I/O, Analog I/O, Serial Hardware, interrupts, power fail/restart, battery backup, etc. Depending upon the sophistication of these tests a hardware problem can be traced down to within the board level. By running the diagnostic tests as dictated by an acceptance procedure, shortcomings in the hardware with regard to the specification can be identified early in the design. A failure may result in changes to the hardware by the vendor prior to completion of the contract.

7.4 QUALIFICATION (SURVIVAL) TESTING

During or after acceptance testing, the hardware is subjected to Environmental tests consisting of temperature, humidity, Electro-Magnetic Interference (EMI) and Seismic testing. The test levels are chosen to give confidence about the hardware's survival in site operating conditions. Should the hardware fail to pass a test, it is modified to correct the problem and retested.

As a first step a program is prepared to determine the health of the computer hardware as it undergoes testing. The program consists mostly of hardware tests that are as follows:

(1) A RAM test that checks blocks of memory for corruption. This may also include static blocks of RAM that surround variables that are incremented by interrupt or DMA (Direct Memory Access) processes in order to detect runaway RAM update conditions.

(2) A ROM test checks that the ROM is unchanged and still working.

(3) A test of the Watchdog circuitry drop–out and pick–up (this may be fed back to the computer or the result may be sent to a chart recorder).

(4) A Digital Output, Digital Input test where the outputs are fed to the inputs. The DIs may also be set to fixed open or closed contacts in order to test the stability of a fixed condition.

(5) The Analog Outputs are connected to the Analog Inputs and the voltage is ramped up and down at a fixed rate. The AIs may also be connected to fixed voltages to detect drift.

(6) Communication links are connected so that the output is fed back into the input to check that transmitted data can be sent without corruption at various data rates. The communication links used in the shutdown system can be physically disabled by opening a contact relay so that the communication test is extended to expect data when the link is closed, and to report an error if data is received when the link is open.

(7) The status of the computer is printed periodically on a hard copy device.

The tests run while the hardware is exposed to the range of environmental conditions. Generally a chart recorder is also connected to appropriate inputs and outputs to provide an independent record of the test events. Should the hardware fail any of the tests, the cause is determined, Solutions may include design changes and test re–run.

The hardware is tested to the following limits:

Environmental– Normal Ambient operating conditions:

Temperature:	+22.5 ±2.5°C
Relative Humidity:	40%–60% non–condensing

– Ambient range

Temperature:	+10°C to +50°C
Relative Humidity:	5%–95% non–condensing

– Without Applied power

Temperature:	–18°C to ±60°C

Seismic – The equipment is tested to expected site seismic conditions. A typical test would be 1.5g from 1 Hz to 33 Hz.

EMI – Broadband – Ambient noise field of 120 dB /MHz (± 3 dB or 1 V/m/MHz over a frequency range from 14 kHz to 500 MHz) when measured 1 metre from the equipment enclosure. As per SAMA Standard PMC33.1

- Narrowband – RFI of 15 volts/metre at any selected frequency over a range from 35 MHz to 500 MHz.

7.5 COMMISSIONING

Once the hardware is shipped to site it is subjected to a commissioning test prior to acceptance.

A commissioning procedure is a formalized document that lists each step to be followed in order to test the item being integrated into the site equipment. Each step indicates an action and the expected result from that action. Should a test fail the problem is fixed by site and/or AECL and the test is re-run.

7.6 PERIODIC TESTING

Over the life of the plant, periodic tests are performed on the hardware. Any problems are repaired by swapping parts at the circuit board level. Defective components on faulty boards are repaired and the boards are retested later by AECL at the Z299.1 level.

In general, where it can be done, quickly identifying the fault and repairing it by inserting a new board is preferred. This lowers the unavailability of the shutdown system and allows the repair of the fault to be conducted in an environment more suitable for finding component failures. To satisfy the QA requirements replacement of the defective component is performed by AECL.

7.7 DOCUMENTATION OF HARDWARE

As with the software, it is important that the information gathered on the hardware be kept together in a presentable form. Most of the supplied hardware is accompanied by it's own documentation. Other documents concentrate on system assembly, trouble shooting, and operation. Schematics for all hardware are a part of the tender requirements. These are packaged together with the other documentation, registered and issued to site.

7.8 COMPUTER HARDWARE CHANGE NOTICES

Computer Hardware Change Notices (CHCNs) are intended to document any changes to hardware that occur after it has been received from the supplier. This allows a traceable change path from the manufacturer's drawings to the installed site hardware.

7.9 FAILURE MODE AND EFFECT ANALYSIS

For the Darlington shutdown computer selected components were subjected to detailed failure mode analysis. The General Automation CPU and the I/O cables for the DEC computer were analyzed.

8. SDS COMPUTER SOFTWARE AND HARDWARE PRODUCT CHARACTERISTICS

This section describes design features of the SDS software and hardware. Many of the features are concerned with converting abnormal conditions into failsafe actions. The trip computers contain a large number of such failsafe features. They too are discussed in this section.

8.1 SOFTWARE

Experience from previous designs has resulted in some programming guidelines that give a preference to certain features to be present in the code.

8.1.1 Scheduling Algorithm

To avoid the overhead and complexity of an operating system the Trip Computers utilize a simple scheduling algorithm that consists of a successive set of calls to data collection, comparison and data output subroutines contained within a single main program loop. The advantage of this approach is its comprehensible form and deterministic nature. Since the key modules in the trip function are called one after another they can easily accommodate the need to increase the response of one trip function by adding another call to the sequence. Interrupts are only used where necessary, where an asynchronous event requires immediate attention by the CPU and has no buffering mechanism, such as for time functions (where each tick is an interrupt) or data communication links (such as an RS-232 serial link). These interrupt driven events are periodic and since their overhead and frequency is known they can easily be accounted for when calculating the calling sequence. As a result of this approach the variation in loop times is very small and virtually immune to external loading effects.

8.1.2 Software Function

The software is designed according to coding guidelines contained in the Programmers Handbook and Design Principles. These guidelines are provided in order to make the resulting code consistent throughout the system and to provide certain characteristics that are required for safety.

A high level language is used for the majority of the code to increase readability, decrease the development effort and allow portability. Use of a high level language reduces the effort on the programmers part since he/she need no longer be concerned with the peculiarities of the central processor, but rather can concentrate on implementing each algorithm with a language more suited to abstract mathematic and logical operations. One drawback of a high level language is that a compiler must produce code for general situations (special more optimized solutions would have to be anticipated by the compiler writer) and the resulting code is less efficient than hand-coded assembler. In situations where access to a particular piece of hardware is restricted in a high level language, assembler is used.

Compensation of the neutronic detectors for the Darlington Shutdown System is performed in the trip computer. As described in Section 3.8.3.1 the compensator consists of phase lead algorithm that corrects for the delayed components of the detector response. The mathematical formulation is quite complex and will not be described here. Such compensation is not required for any other signals. Computing time considerations led to the compensation of the setpoints rather than the signal (the calculations require a large number of floating point arithmetic operations). The time savings are because the setpoint is relatively fixed compared to the signal and requires less frequent compensation.

The Darlington SDS2 trip computer also features Local Coincidence Logic and Power Rundown Discrimination. In simplest terms, a Power Rundown Discriminator is an algorithm that continuously lowers the SDS2 trip setpoint such that if SDS1 has already taken effect and the reactor power is going down as expected then SDS2 trip cannot be initiated. But if SDS1 fails to take full effect and power is not reduced at the expected rate SDS2 fires immediately because of its lowered setpoint. The Power Rundown Discriminator logic prevents the unnecessary action of SDS2 if SDS1 is effective in shutting down the reactor.

8.1.3 Software Selfchecks

Critical modules, such as trip comparison routines, are checked for proper execution, i.e. in sequence and to completion using a method known as Baton passing. It is important to ensure that the modules operate in proper order since they may depend on a time dependent calculation from a previous routine. Pertinent compiler generated checks are turned on. Compiler generated run-time checks usually are stack limits exceeded, array limits exceeded, and other checks that generally look for the crossing of a boundary. Some of the error detection code is enhanced or extended by hardware. Critical RAM based variables are protected from change either through checksums or by careful assignment of write permission. The checksums are updated when an infrequently updated block is changed. Should the checksum change when there is no expected change then a corruption of the "safe" variable is declared and the area reset to safe values. Assignment of write permission is usually a feature of the hardware that the software can take advantage of in order to limit the update of a variable to selected program procedures.

8.1.4 Software driven Hardware Selfchecks

RAM is tested continually, one location at a time. The value of the current location under test is saved, and some new values stored and read back to test the operation of that memory cell. The original value is then placed back in the test location.

ROM is continually checksummed to ensure that its contents have not changed (since this would affect the code, and its operation). Usually small blocks of data and a very simple checksum algorithm are used to reduce checksum overhead without affecting the checksum error detection accuracy.

CPU instruction tests are performed to gauge the health of the computer. Each time the test is called a new class of instructions is tested. Each step depends on the successful completion of the previous step.

Interrupts are checked for legality and proper frequency. For example a timer-function interrupt should always be invoked a fixed number of times every program pass if the pass time is fixed. Thus by applying a range of acceptable values for the number of timer-function interrupts per pass a failure of the timer-function can be detected. Illegal interrupts can be detected by connecting an illegal interrupt handler to all unused vector locations. This handler is a small section of code that will usually report an error, and perhaps halt the computer if it is serious enough. If interrupt vectors reside in RAM they are checked for corruption. Most CPUs provide more than one level of interrupt and a pointer to an interrupt for all the interrupts supported by the hardware.

8.2 HARDWARE

Maximum use is made of inherent safety features of the hardware. For example the non-volatile nature of ROMs make them ideal for code and constants. They are favoured over a simpler development choice of RAM and a magnetic storage device. The design is such that failures are turned to the largest extent possible into safe failures. For example the watchdog circuit opens the digital outputs resulting in a channel trip, on failure of the computer or loss of power.

8.2.1 Inherent or Introduced Safety Features

ROM is used for code and constants to reduce the likelihood of being corrupted. RAM is used for variables. The CPU must have sufficient speed for the required real time function. Use of interrupts is held to a minimum and unexpected interrupts are trapped to reduce the effects of asynchronous loading during execution of time critical code. The process I/O is read periodically (polled), instead of being input under interrupt control when a change occurs on an input. The chassis and components are designed to withstand environmental (temperature, humidity, EMI and seismic) conditions to ensure that the hardware will function under extreme conditions. Special failsafe hardware, usually referred to as a watchdog circuit, initiates a trip if periodic ("still-awake") impulses fail to arrive from the trip computer. In addition, there exist software self-checks that detect any major failures and will cause the computer to halt, forcing the watchdog to act. I/O is tested through loop-back tests, which function by feeding a signal from an output to an input.

8.2.2 Other Features

For Darlington the trip computers performed detector compensation. The compensator gain values are kept in secure RAM for economic reasons. In the event of a power failure, battery backup can retain the compensation constants for several hours. If the battery backup fails, default gains are loaded from ROM at power-up time.

The computers used are supported by thoroughly tested and proven software. This includes compilers, assemblers, linkers - and any other program that is involved in producing the executable code from a source file. Only those products that have been used by a large number of users over a long period of time are selected for this application.

The hardware is selected for availability over extended periods and upward compatibility with planned future hardware. Though a sufficient number of spares are usually purchased for the planned station lifetime there may be instances where a new part is required, or requirements change that require better hardware response.If available, software compatible hardware upgrades based on technological improvements may also be used.

9. CANDU EXPERIENCE WITH COMPUTERS IN CONTROL AND SAFETY SYSTEMS

AECL has been using computers in CANDU stations since the 1960's. During that time, as operational requirements became more sophisticated, and data available to the operator became more complex, computers were able to save the operator from data over-load and were able to provide automatic response in many complex situations.

This section provides a history of AECL's use of Computers in CANDU for control and monitoring, and illustrates the experience that led to the development of the current Shutdown System designs.

9.1 CONTROL COMPUTERS

AECL introduced computer control into the CANDU plants quite early in their design. The Douglas Point station used a Control Data computer for Turbine Runup, Channel temperature monitoring, and some annunciation. Ontario Hydro's first Nuclear Power Station - Pickering 'A' used an IBM 1800 computer for control and monitoring.

The Ontario Hydro Bruce Power Generating Stations, the 600 MWe (Hydro Quebec G2, New Brunswick Pt. Lepreau, Korea Wolsung) and Pickering 'B' stations use Varian series 70 computers for extensive control and monitoring functions.

The Control algorithms reside in a dual computer system consisting of two identical computers, each with its own set of peripherals and process input-output equipment. The two computer systems are completely independent of each other except for shared display controllers and a computer-to-computer communication data link. A single digital scanner is provided which can be connected by a switch to either computer for annunciation purposes.

All functions essential to the operation of the plant are present in both computers, with one computer being in control and the other in an operating standby role.

The software consists of two main parts, namely the executive as one part, and non-interrupt functions like control, alarm, display, and data logging as the other part. The main function of the executive is to service interrupt requests on a priority basis. Within the executive program structure are numerous sub-routines which control the operation of the various I/O devices in conjunction with the interrupt requests.

The Varian based Control computers consist of process I/O equipment, magnetic storage devices - discs, and a computer. To maintain compatibility with previous projects a paper tape system is available. The original Varians used 8k of magnetic-core memory. Memory restrictions were overcome by using fast Fixed-Head Drives. Current Varian equivalent computers now use a larger amount of solid-state memories.

Many features in current CANDU computers were present in the Varian. One such feature is a Watchdog circuit that detects incorrect program operation. Interrupts are used to respond to system requests and hardware problems. Displays are shown on a CRT driven by a dedicated controller.

Darlington Control Computers are based on DEC PDP–11/70 processors. The software is written in Macro–11 assembler code and was created for this project. This new code is similar in operation to previous designs using Varian Computers. Darlington uses hundreds of programable logic controllers that have substantially replaced traditional relays.

The CANDU 3 design uses a fully distributed control system (DCS) for almost all plant control. The DCS is connected to a PDS (Plant Display System) via data communication links. The PDS performs the man–machine interface functions such as manual control, annuciation, information presentation, data logging and historical data storage.

9.2 MONITOR COMPUTERS

Monitor Computers in CANDU refer to computers used in the safety system that are concerned with relaying information about the state of the reactor with regards to its closeness to trip and some other system conditions. Thus for example a monitor computer provides graphic displays that show the signals and their setpoints, and monitors signal drift, and margin to trip. In general it assists in providing the operator sufficient information to avoid a trip while at the same time allowing efficient operation of the generating station.

9.2.1 Ontario Hydro Bruce Nuclear Power Generation Plant

The Bruce Monitor computers were developed in the early 1980's to provide the operator more information to allow tighter operating margins. The savings due to reduction in spurious trips while running at higher power was the incentive to install a monitor system. The Bruce Monitors were added to an existing system and did not replace existing panel displays. See Figures 25, 26, 27.

The system collected channelized data utilizing Data General MP–100 microcomputers. (The MP–100 is an industrial microcomputer with good price/performance features). Data is collected and transmitted to a central monitor computer. The central monitor computer is a Data General MP–200 (faster than 100) with a 12 Megabyte hard drive. The monitor computer performs spread checks (inter–channel comparisons), margin to trip checks, graphical trend displays and status displays, and alarm message summaries. Alarm messages are also routed to a hardcopy printer.

Testing of the safety systems is done at full power and is performed manually from the main control room using test procedures consisting of checklists. Data from the monitor computer is utilized in safety system testing.

9.2.2 Gentilly 2 600 MWe

The G2 Monitor computer was modelled after the Bruce Monitor computer design and experience at the G2 site (Figure 28). The software is written in HP–Basic and runs on an HP–330. HP–Basic allowed quick development, and was supported by an extensive data collection/manipulation library. The Hewlett Packard 330 is based around the popular Motorola 68000 series CPU and was requested by the client.

Data is collected from the panel display instruments and is routed to a programmable intelligent I/O processor. This processor stores the readings in memory, does some initial data conversion and transfers the data upon request over an IEEE–488 interface to the HP–330. The HP–330 archives important data, does margin to trip comparisons, signal drift, alarm message displays, process and neutronic bar charts, trending and re–calibration data collection.

Testing of the safety systems is done at full power and is performed manually from the main control room using test procedures consisting of checklists. Data from the monitor computer is utilized in the safety system testing.

9.3 PDC (SHUTDOWN SYSTEM TRIP) COMPUTERS

The Programmable Digital Comparators (PDCs) in the CANDU 600 (CANDU 6) plants are the first microcomputers to provide trip functions to the CANDU shutdown systems. These units have been installed in both SDS1 and SDS2 on four CANDU 600 plants. They are Data General MP–100 computers with modifications for seismic and EMI conditions.

For this application the Nucleonic trips used conventional analog instrumentation while the Process trips used the PDCs (see Figure 29). As an initial conservative approach, two PDCs where used in each channel, dividing the process trips between them. The PDCs process seven out of ten trip parameters used in the shutdown system one (refer to Figure 31). The PDCs were added very late in the design of the CANDU 600 MWe shutdown systems in order to respond to more complex safety requirements. Several process trip setpoints were varied according to reactor power and number of circulating pumps in operation.

The PDCs' principal inputs are the process parameter measurements and its major outputs are the trip contacts associated with each parameter. The PDC operates as a sophisticated comparator while the rest of the shutdown system retains the traditional design.

The PDC software was written in assembler and was modularized to model conventional hardware. It was purposely kept simple and did not use an operating system or interrupts.

Reliability data from the Point Lepreau CANDU 600 for the first five years of operation shows that the shutdown systems achieved better than 10^{-4} unavailability (the requirement is 10^{-3}).

The PDCs were subject to a QA process that was a pre–cursor for the current Darlington QA procedure. The steps followed were as follows:

The process and safety design of the plant led to the system design requirement documents which were used to specify the role and function of the PDC in the shutdown system.

A specification was prepared by the system designer that stated the function of the PDC computer. The description used english descriptions, tables and values specifically given in millivolts. The system designer and the programmer worked together as a team, reporting to the same project leader, thus reducing misunderstandings. The system designer, however produced the specification independently and had no knowledge of the detail software.

The code was written in assembler, and had built in selfcheck features to test RAM, ROM, I/O, Module Sequence, and Functional Tests. Many of the features for the current Shutdown System Trip Computer Design originated with the PDCs. The specification was used to create the code and to test the results.

Two MP-10's were cross wired to each other and an interpreter program written in PASCAL (called CROSS) was run on one to test the function of the PDC code running on the other. The test cases consisted of ASCII text files that contained simple commands to open and close DOs, read in DIs, set AOs, and read AIs. The commands were written from the point of view of the PDC. Thus, for example, the Command SP 0 1 5 (SP AI# FROM TO) would slowly move the voltage on the AO attached to the PDC Analog input 0 and move it from 1 volt to 5 volts and back down again.

A formal set of tests were prepared by the system designer to ensure that the code met the intent of the specification. These were used to initially test the code, and for formal acceptance tests in the presence of the client and an AECB representative.

During formal testing, the test cases were run and the results checked by the observers. For involved tests a Chart Recorder would be attached to the PDC to record its response to test cases. The client and or AECB usually requested additional tests as a check of the process. Also, the assembler listings were handmarked to check that the code took the proper path for all input cases as defined by the functional specification. During revisions, a source compare indicated the sections of the code changed and only those parts were hand marked. As a final test the selfcheck logic was checked by intentionally placing errors in the code and making sure the computer caught the error.

When testing was declared complete PROMs were created that contained the same code as that tested. To ensure that the copies were created correctly, each set of PROMs was subjected to a subset of the test cases using the CROSS test program prior to shipment to site.

9.4 DARLINGTON 850 MWE

A Darlington Shutdown System (Figure 12) consists of three channelized Trip Computers and three channelized Display/Test computers and a Monitor Computer. There is also a Safety System Monitor which may be connected to the two SDS computers of each of the 4 Darlington units.

All Display/Test computers and Shutdown System 1 Trip Computers are General Automation 16 bit computers with 60 Kb of EPROM and 64 Kb of RAM. All software is either written in Fortran or assembler and stored in EPROM. The Shutdown System 2 Trip Computer is an LSI-11/73 16 bit processor with 64 Kb of EPROM and 64 Kb of RAM. All software is written in Pascal or assembler and stored in EPROM. The Monitor Computer is a General Automation Computer with 128 Kb of RAM, one 5 Mb removable disk pack and one 5 Mb fixed disk. A multitasking operating system is used and all software is written in assembler or Fortran and is stored on a removable disk pack. The Safety Systems Monitor Computer is an industrial 80286 computer.

The Trip Computer performs all functions that were previously performed by conventional analog instrumentation and relay logic for all trip functions except a Manual trip function. The Trip computer is capable of carrying out its functions regardless of the status of the other computers in the system.

The Display/Test Computer processes data received from its corresponding Trip Computer over fibre optic serial links and displays neutronic trip data, process trip data and status information on two dedicated displays. It routinely transmits its data to the Monitor Computer and processes requests from the Monitor Computer. Requests from the Monitor Computer may be either for transmission of calibration data to the Trip Computer or to manipulate Display/Test field I/O devices used in routine trip testing of the Shutdown System.

The Monitor Computer receives data sent over fibre optic serial links by the three channelized Display/Tests computers. Using this information on the shutdown system the Monitor Computer performs historical data storage, trending, spread checks, margin to trip checks, detection of system impairment, graphical displays, alarm jumpering, and alarm message summaries. Neutron detector calibration in the Trip computer and safety system testing is also performed by the operator from the Monitor Computer. The Monitor Computer also transmits alarm messages and test results to a Safety Systems Monitor Computer for permanent archiving.

The Monitor Computer also has I/O for controlling non-channelized devices used in safety system testing. The testing hardware and software have interlocks to prevent testing of a channel if another channel is in the tripped state or testing is occurring on another Safety System.

The Monitor computer uses an interpreter to execute test programs or test scripts to perform routine shutdown system tests. The test programs are written in a high level language specifically designed to be understandable by operators and are similar to manual test procedures used at other sites. The current philosophy is that the testing is computer-aided rather than fully automated. The test programs are structured in such a way that the operator always initiates test actions which will manipulate field devices or cause trip variables to go into the trip state. The safety system testing programs for Darlington were initially developed by AECL design in consultation with Darlington Operations, however the maintenance of these test programs are solely the responsibilities of Operations. The test interpreter is also used by Commissioning for the commissioning of the Safety Systems.

10. CURRENT ISSUES AND DESIGN DIRECTIONS FOR CANDU 3

The CANDU 3 project has given AECL the opportunity to further evolve the computerized shutdown system concepts developed in previous projects. This section touches on the direction of some of the latest ideas concerning the use of computers in the CANDU 3 shutdown system and beyond.

10.1 COMPUTERS IN CANDU 3

Part of the CANDU 3 plan is to introduce distributed control to the plant along with a centralized data-base that holds data collected plant-wide. Distributed control places the controlling device closer to the process being controlled, which improves response and reduces signal/control cabling requirements. Also moving the control from a centralized computer to many smaller computers increases the reliability of the system, since failure of one part should have little effect on other parts. A centralized data-base provides the operator with a complete picture of plant activity since the data contains information about the status of all systems including the shutdown system. This should allow more meaningful combinations of data that were difficult in previous designs.

The primary focus of the CANDU 3 control room is to provide the operator with the data required to make good decisions quickly and correctly. In order to do this computer driven "Blackboard Displays" are being considered which present schematic diagrams of the plant operation status on large wall surfaces. See Figure 32. Computer assistance for the selection of a proper response from a group of alternative actions during an abnormal plant condition is being considered.

10.2 SHUTDOWN SYSTEM

One of the current directions currently under investigation is realignment of the functional boundary between the trip computers and the display/test and monitoring computers. Currently under consideration is the possibility of putting the trip comparator function onto dedicated hardware, and moving ancillary functions, such as signal validity checks, into other computers in the chain leading to the operator interface. Such realignment may have considerable benefits in terms of simplification of the trip software design and testing.

10.3 DESIGN DIRECTIONS

The main area of evolution is that of software development methodology. We are working towards more "formal" design techniques, including aspects such as mathematical specification and formal verification. Also under consideration are changes to the approach being taken to software structure, including the use of information hiding (between separate software elements), and object oriented design, as a means of enhancing code maintenance, reviewability, and portability from one project to another. Investigations on how to measure software reliability are ongoing.

11. SUMMARY AND CONCLUSIONS

CANDU Shutdown Systems are designed to meet the unavailability target of 10^{-3} yrs./yr. for each of the two shutdown systems. The two shutdown systems are fully independent from each other from sensors to negative reactivity insertion mechanisms. The latest designs take advantage of digital systems to increase their reliability. Regular on line testing is automated through a display/test computer system.

The trip parameters have been selected such that most conceivable incidents are covered by at least 2 parameters on each system. Extensive trip coverage analysis is performed to substantiate these claims. Strict codes and guidelines are adhered to in both the hardware and the software design of the shutdown systems. Multiple levels of testing is performed on the whole system before it is commissioned. This forms part of a comprehensive quality assurance and validation program.

The shutdown systems are designed to fail safe. The computers continuously perform self checks and monitoring of the trip parameters. Abnormalities detected are treated as a tripped parameter on channel in a 2 out of 3 voting logic. This provides a fail safe action while preserving immunity to spurious trips.

The use of computers allows for future changes as new requirements evolve. The present design emphasis is on function allocation between the different computers in the shutdown systems so as to keep the software in the computers performing trip functions as simple as possible.

APPENDIX A

GLOSSARY

APPENDIX A

GLOSSARY

AC	Alternating Current.
ACNS	Advisory Council On Nuclear Safety
AECB	Atomic Energy Control Board of Canada
AECL	Atomic Energy of Canada Limited.
Alarm Jumpering	Jumpering an alarm prevents the alarm from showing up in certain instances where it could unnecessarily distract the operator. An alarm is jumpered when the condition is expected due to maintenance or plant conditions.
Analog I/O	Analog Input or Output (AI, AO). Voltage or Current values in specific ranges (i.e. 0 to 5 Volts) that read or output from/to the field.
Archiving	see Data Archiving.
Battery Back Up	Used in the Darlington Shutdown System trip computers so that they are able to retain data in RAM while the computer is without AC power.
Baton Passing	This is a method of checking that each module has participated in an expected sequence. An array of signatures is created that assigns each module a unique value. As each module is called it enters its value into a sequence table and increments the index into the table to the next location (note: multiple modules result in multiple entries). A selfcheck module then checks the resulting sequence against an expected sequence and the process repeats.
BFLP	Boiler Feedline Low Pressure
Black Box	The inner workings are not revealed. Rather evaluation of the box is restricted to what it shows to the outside world.
Boolean	An expression that can result in a True or False state.
Boundary Condition	A value or state that defines the working limit of the system under test. For example a signal range.
CANDU	CANadian Deuterium Uranium pressurised heavy water reactor nuclear reactors and reactor development program.
CASE	Computer Aided Software Engineering
CHCN	Computer Hardware Change Notice

Chart Recorder	Records the status of Analog I/O and Digital I/O signals over time on paper. Used during testing to capture quickly changing inputs and outputs for later analysis.
Comparator	A device which compares two signals and makes a decision on that comparison.
Computerized	Replacing a design that, did not use computers, or was a manual operation.
Conditioning	Preventing the normal trip action when a signal exceeds a setpoint (used to prevent spurious trips at low power levels where it can be clearly demonstrated that safety is not compromised by neglecting that trip parameter).
CPPF	Channel Power Peaking Factor
CPU	Central Processing Unit. A structured solid state device that allows controlled manipulation of data (Addition, Comparison etc) that is stored in memory accessible to the CPU.
CSA	Canadian Standards Association. It is a not–for–profit, independent, private sector organization that serves the public, governments, and business as a forum for national consensus in the development of standards, and offers them certification, testing, and related services.
CSA CAN3–Z299.1	This Standard specifies minimum requirements for a supplier's quality assurance program. The supplier is responsible for planning and developing a program which assures that each management, design, and technical responsibility for quality is integrated and executed effectively. The program is aimed primarily at being preventive by controlling design and production processes as well as inspection and test verifications which a. assure that products or services will and do conform to specified requirements; and b. readily detect and control the disposition of non–conformances and prevent recurrence. This standard does not apply to computer software. See CSA Q396.
CSA Q396.1	This Standard specifies the Software Quality Assurance Program requirements to be planned, developed, implemented, and maintained by a developer for assuring that software to be developed conforms to customer requirements.
D2	Deuterium

Darlington	Darlington Nuclear Generating Station, an 850 MWe CANDU reactor.
Data Archiving	Data is stored so that it can be retrieved intact at a later time (or until it is not required).
DBE	Design Basis Earthquake
DCC	Digital Control Computer – the computer that controls the nuclear plant.
DD	Design Description. This is a document produced by AECL during the software implementation phase. This is a comprehensive technical document which defines the design as produced as specifically and completely as possible.
Display/Test Computer	Displays show the status of Neutronic and Process readings and setpoints for three channels. Test I/O also allows some computer assisted testing.
Digital I/O	Digital Input or Output (DI, DO). Logic States of 0 or 1 that are translated to/from contact open or closure respectively in the field.
DM	Design Manual. This document is an assemblage of the design documentation produced in support of the system.
DMA	Direct Memory Access
ECCS	Emergency Core Cooling System.
EMI Tests	A test of hardware under Electro–Magnetic Interference conditions.
Environmental Tests	A test of hardware over conditions that it will be exposed to in the field: temperature, humidity, EMI and seismic.
EPROM	Erasable Programmable Read Only Memory. Once programmed, and until erased with an Ultraviolet light the contents of the memory do not change.
Exception Condition	A condition where a value or operation has strayed from its normal range or place. The design of hardware and software includes the consideration of exception conditions and converting them into a safe value or action.
FP	Full Power
Freeze	Software is frozen when it is placed under document control. This means that the code sources are kept in a secure place, and any changes (to copies) are fully documented.

FS	Functional Specification. This document states the requirements of the design.
GA	General Automation. The manufacturer of the computers used for the Darlington Shutdown system except for SDS2 trip computers.
G2	Gentilly 2 Reactor
Gadolinium nitrate	Has a high neutron absorption cross-section. Injection into the moderator rapidly reduces reactivity. It is removed later by filtering the D2O moderator.
Gain changes	The Darlington Shutdown Systems allows the Neutronic detector gains, stored in the trip computer, to be changed from the control room. This is necessary because the signal produced by these self powered flux detectors decreases as they age. Therefore, they must be periodically recalibrated.
I/0	Input/Output
ICRP	International Commission on Radiological Protection
Integration	The process of combining and testing software units to form a unified system product.
Interrupt	A hardware signal that an asynchronous event requires immediate attention. The software being executed is suspended and the CPU branches to a specific software module for that interrupt. After this module is finished the execution of suspended software resumes from the place of suspension.
Kb	Kilobyte. 1024 bytes of memory (memory is produced in multiples of 2, 210 is the closest power of 2).
LOCA	Loss Of Coolant Accident. Represented by a maximum inlet header break. This accident dictates the initial reactivity insertion rate requirements for a shutdown system, including trip delay, and to a lesser degree the final depth of the reactivity insertion.
LOR	Loss Of Regulation. Positive Reactivity insertion due to a LOCA or other causes that exceeds the capability of the reactor regulating system to maintain power constant.
Loss of Flow	Loss of Class IV power causes the Primary Heat Transport pumps to trip and results in a loss of flow event. This can lead to a Primary Heat Transport system rupture due to overpressure.

Loss of Moderator	The moderator is not highly pressurized so this is a slower condition than a LOCA. Though loss of the moderator removes reactivity from the top of the reactor which would decrease power, the resulting flux shape at the bottom, where there is still a moderator, may be difficult for the Reactor Regulating System to control. There is also a concern with overheating in exposed calandria tubes, and accumulation of hydrogen gas in the space created, with a potential for explosions.
Loss of Secondary Side Heat Sinks	The secondary heat sink is provided by the boiler light water system. Its loss is not a serious process failure in the traditional sense, however the consequences can lead to an over–pressurization of the primary heat transport systems, and eventually a serious process failure if the Reactor Regulating System also fails.
LSI–11/xx	A processor produced by Digital Equipment Corporation.
MAD	Maintenance And Development system. Used initially to develop code and later on maintain the hardware at site.
Mb	Megabyte. 1,048,576 bytes of memory.
Module	Refers to one or more software functions/procedures that are grouped together.
Monitor Computer	Monitors process and neutronic signals to provide information in addition to that provided by the shutdown system displays.
MWe	Megawatt Electric
NOP	Neutron Overpower
P–code	Preliminary pseudo code. This pseudo code is a high–level description of main software modules.
PDC	Programmable Digital Comparator.
PHTS	Primary Heat Transport System
PIT	Preliminary Integration Tests. These are tests of a group of software modules to ensure that the these modules work together correctly.
Portability	For software, this refers to the ability to use code (written in a high–level language) created for one computer on a completely different computer by recompiling the source.
Power fail/restart	Process or Hardware that detects failing power and takes action to allow a graceful shutdown of the computer. A corresponding power–up sequence allows an ordered setup of system memory and states.

PROM	Programmable Read Only Memory. Once programmed the contents of the memory do not change.
Q396	See CSA Q396.1
QA	Quality Assurance. A process that provides reasonable assurance that a projected quality is actually met.
RAM	Random Access Memory. Will retain the contents in memory while power is applied, and until overwritten. Random Access because each location can be stored or retrieved individually.
Real Time Software	Software that is structured to respond within a specific time to real world events. This is in contrast to data processing programs which are structured primarily for manipulation of large amounts of data, or simulations where the simulated time is not tied to the computer execution time. In data processing the time response is accommodated by allowances made by the users (i.e. starting a run early).
Response Times	In order for the Shutdown System to be effective key parts of the system must respond to events requiring reactor shutdown within specific time margins. Hardware an[illegible] Software are chosen or created that can provide these margins.
ROM	Read Only Memory. Constructed with fixed data. Once constructed the contents of the memory do not change.
SCA	Secondary Control Area
SCR	Secondary Control Room or Software Change Record.
SDS	Shut Down System.
SDS1	ShutDown System 1. This is the primary shutdown system using insertion of shut–off rods. It is designed to react first to an accident situation.
SDS2	ShutDown System 2. This is the secondary shutdown system which injects neutron poison into the moderator. It is totally independent and as capable as SDS1.
Secure RAM	RAM that is checksummed when it is changed and checked periodically while it is not supposed to change to ensure that the original checksum matches the checksum calculated for the comparison.
Sensor	Instrument that provides a signal that responds to a process or neutronic parameter.

Setpoint	A value used as a boundary condition for an action. In a trip computer a signal exceeding a setpoint would cause a trip.
Serial Hardware	Data communication hardware that sends or receives data one bit (one bit representing a logic level of either 0 or 1) at a time.
Seismic Tests	A test of hardware under a range of typical g forces that the site the hardware is intended for might experience during an earthquake.
Shutoff Rods	Absorb neutrons in a similar manner to gadolinium nitrate in order to shut down the reactor. However, the shutoff rods can be withdrawn to allow an immediate restart of the reactor.
Signal	A voltage or current value that represents the status of a process or neutronic condition.
SIR	Straight Individually Replaceable
Site	A CANDU site.
SIT	System Integration Tests. A set of tests that investigate the response of a representative shutdown system.
Spread Checking	Signals are compared to check for an unreasonable difference in values.
Spurious Trips	Trips that occur when they are not required from a safety point of view, often due to human errors in system testing.
SSMC	Shutdown System Monitor Computer. An overall summary Monitor computer for Darlington that collects data from 4 Units (8 shutdown systems monitors). See figure 2.
Subcritical	The operating state in which the rate of neutron creation in the reactor is less than the rate at which neutrons are absorbed or escape the reactor such that a chain reaction cannot be sustained. In reactivity terms the reactor is subcritical when the overall reactivity balance is negative, independent of what power level the reactor is presently at.
TDS	Technical Documentation System. AECL's filing system for all technical documents.
Trending	A graphical display of one or more signals over time.
Trip Computer	Compares Process (and for Darlington Neutronic) signals against fixed or condition dependent setpoints and will initiate a shutdown sequence if they are exceeded.

Varian	Reference Name for the Digital Control Computer used by AECL. Originally a Varian 70 series machine manufactured by Varian (U.S.A.) it was subsequently sold by Sperry–Univac, and is now a product of Second Source (U.S.A.). The current Second Source product, which runs code developed for the original Varian, uses current hardware technology.
WatchDog	Hardware that takes action if the machine it is watching stops or slows the sending of a periodic "I'm okay" signal.
Xenon Buildup	Xenon 135 buildup can prevent restart of the reactor if present in sufficient quantities (due to its large neutron absorption cross section). When SDS1 trips, the fission by–products continue producing Xenon (with a peak at about 10 hours). For a trip from 100% full power, if the reactor is restarted within 30 minutes the concentration will not be high enough to prevent restart. Any longer and a restart is delayed until the Xenon 135 concentration reaches a level that allows restart (by decaying into less absorbing elements). This takes about 40 hours.
Z299.1	See CSA CAN3–Z299.1

APPENDIX B

REFERENCES

APPENDIX B

REFERENCES

1. AECB Licensing Document No. 13, "The Use of Two Shutdown Systems in Reactors", September 1977.
2. Archinoff G.H., R.J. Hohendorf, A Wassyng, B. Quigley, and M.R. Borsch (Ontario Hydro and Consultants), "Verification of the Shutdown System Software at the Darlington Nuclear Generation Station", INE International Conference on Control and Instrumentation in Nuclear Installations, Glasgow, Scotland, May 1990.
3. Condor A.E., and G.J. Hinton (AECL), "Fault Tolerant and Failsafe Design of CANDU Computerized Shutdown Systems", IAEA Conference, London, England, May 1988.
4. Condor A.E., G.J. Hinton, and S.H. Kendrick (AECL), "Software Design Methodoloy for CANDU Safety Systems", IAEA Conference, London, England.
5. CSA CAN3-Z299, "Quality Assurance Program", Category 1 to 4.
6. CSA Q396.1-1982, "Softward Quality Assurance Program", Part 1.
7. Hinton G.J., S.H. Kendrick, S. Schafer, and T.W. Shiels (AECL), "The Use of Computers in CANDU Shutdown Systems - An Overview", IAEA Conference, London, England, May 1988.
8. Hurst D.G. and F.C. Boyd (Atomic Energy Control Board), "Reactor Licensing and Safety Requirements", Paper 72 CNA 102, Canadian Nuclear Association Conference, June 1972.
9. Ichiyen N.M., W. Fieguth, and R. Gilbert, "Digital Computers in CANDU Safety Systems", Parts 1 and 2, IEEE Transactions on Nuclear Science, Vol. NS-20 No. 3, June 1983.
10. Kendrick S.H., A.A.G. Keates, S.A. Russomanno, and J.G. Sutherland (AECL), "Verification and Validation of the CANDU Safety System Computer Software", IAEA Conferance, London, England, May 1988.
11. Nuclear Regulatory Commission, Washington, D.C., "Defense-in Depth and Diversity Assessment of the RESAR-414 Integrated Protection System", March 1979.
12. Olmstead R.A. (AECL), "Safety Aspects of the CANDU Man/Machine Interface", IAEA Workshop on Safety of Nuclear Installations of the Next Generation and Beyond, Chicago, August 1989.
13. Parnas D.L., A.J. Van Schouwen, and S.P. Kwan, "Evaluation of Safety Critical Software", Volume 33 Number 6 of Communications of ACM, June 1990.
14. Pauksens J., A.E. Condor, J. Popovic, and A. Rosevear. (AECL), "CANDU Experience with Computerized Scram", Third International Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, Korea, November 1988.
15. Popovic J.R., and G.J. Hinton, "CANDU Computerized Safety System", IAEA Workshop on Safety of Nuclear Installations of Next Generation and Beyond, Chicago, August 1989.

APPENDIX C

FIGURES

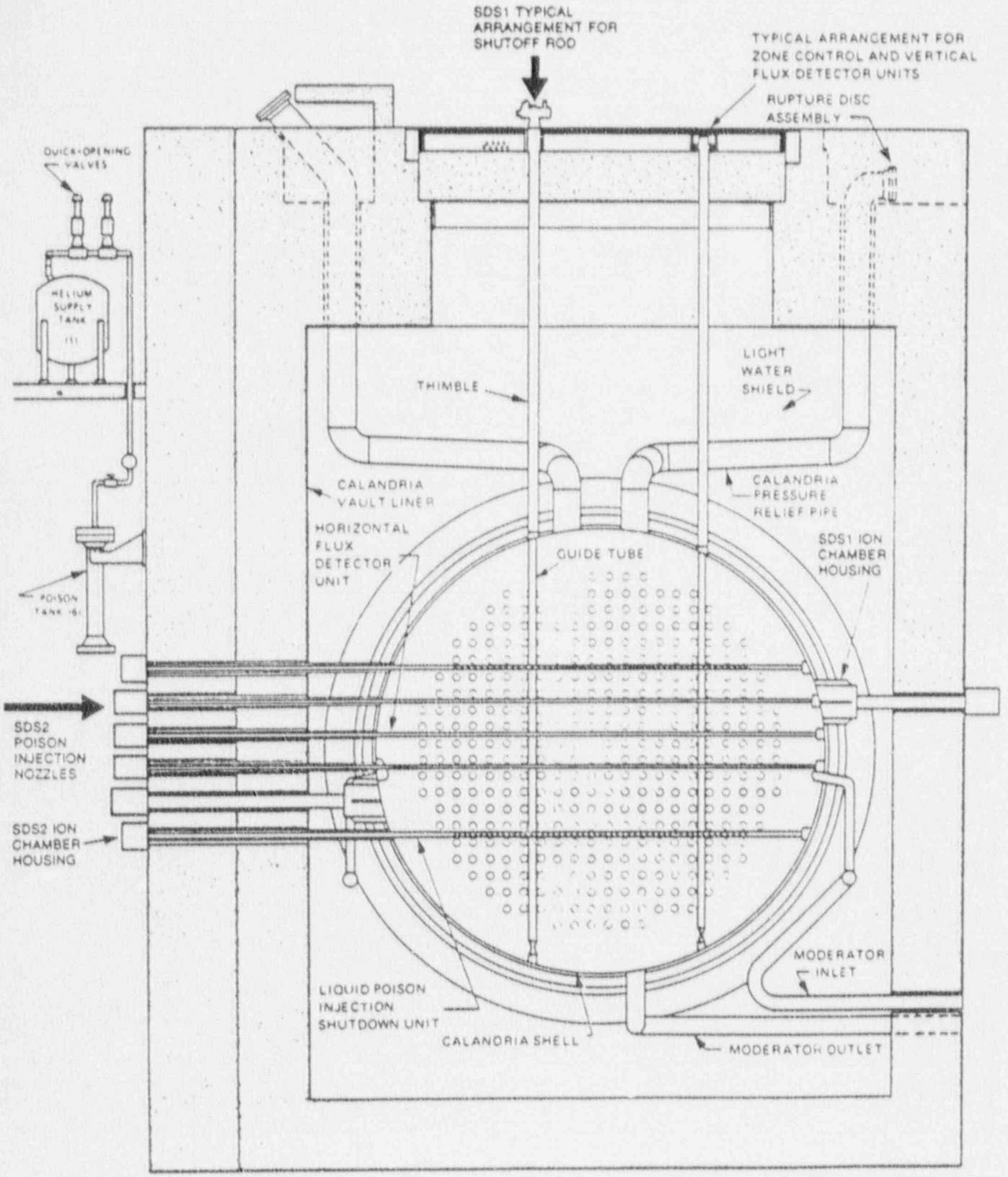


Figure 1 General Layout of SDS1 and SDS2

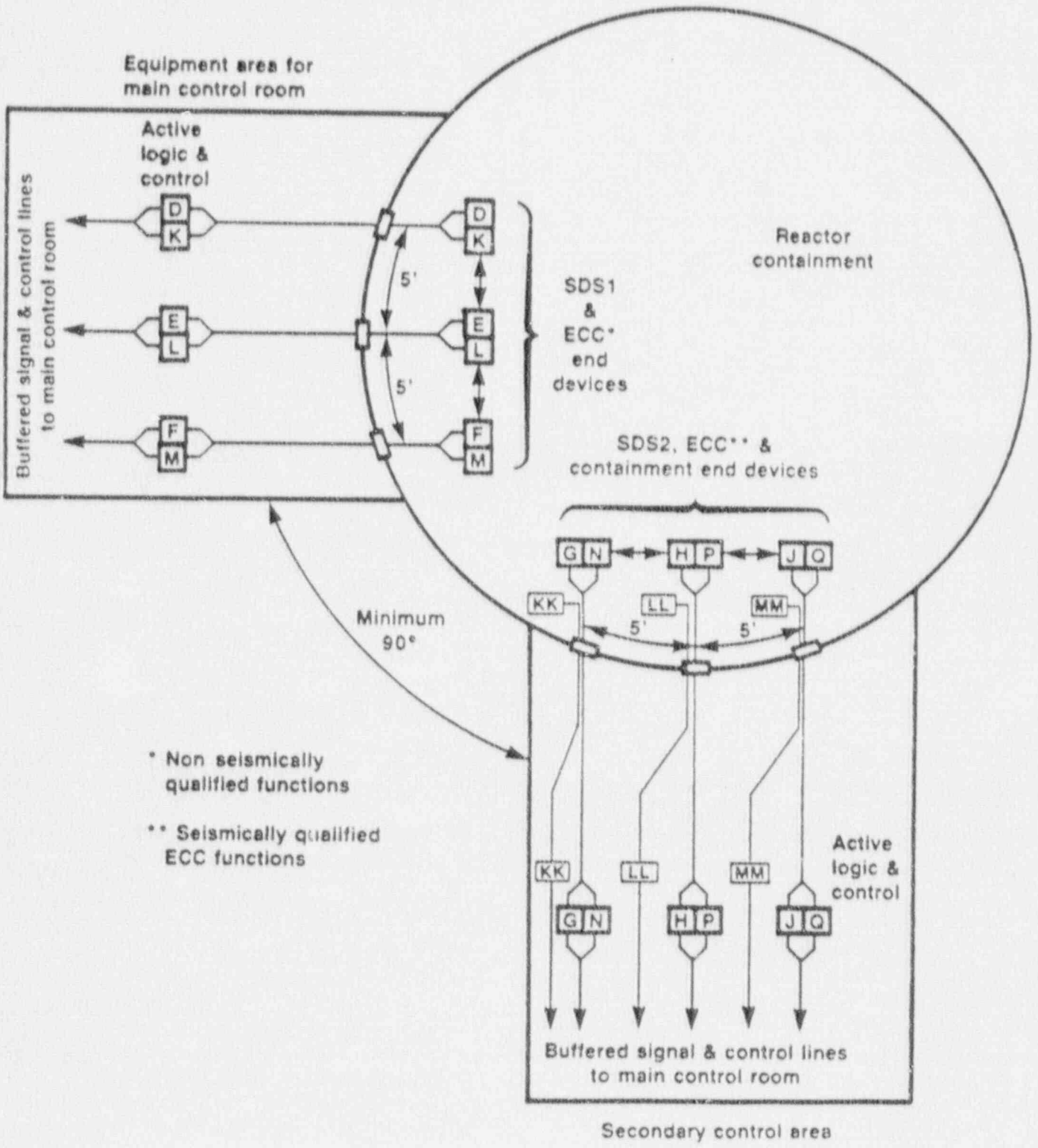


Figure 2 Location and Separation Requirements for Safety Related System (600 MW Stations)

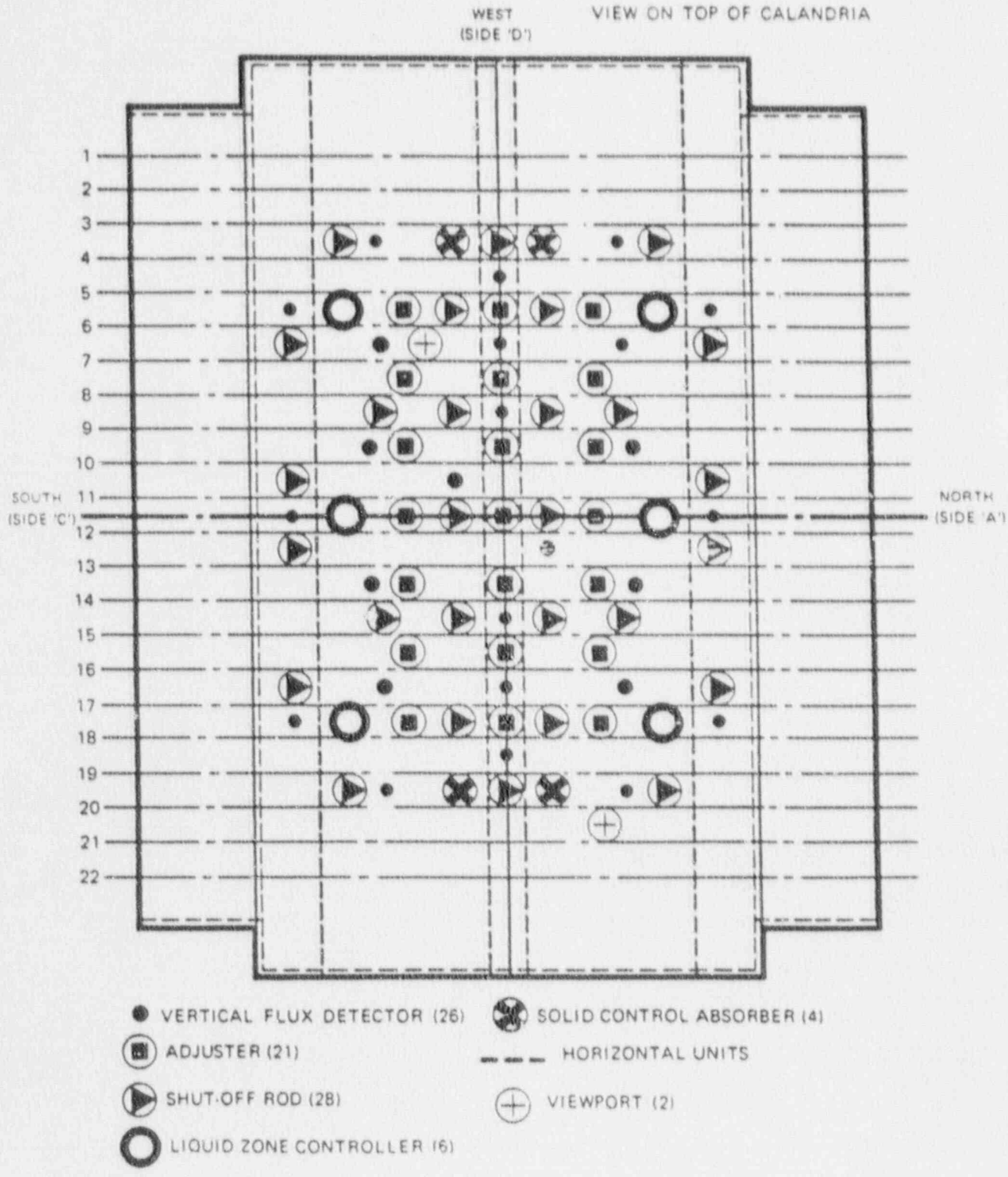


Figure 3 Location of Vertical Reactivity Control Units (600 MW Stations)

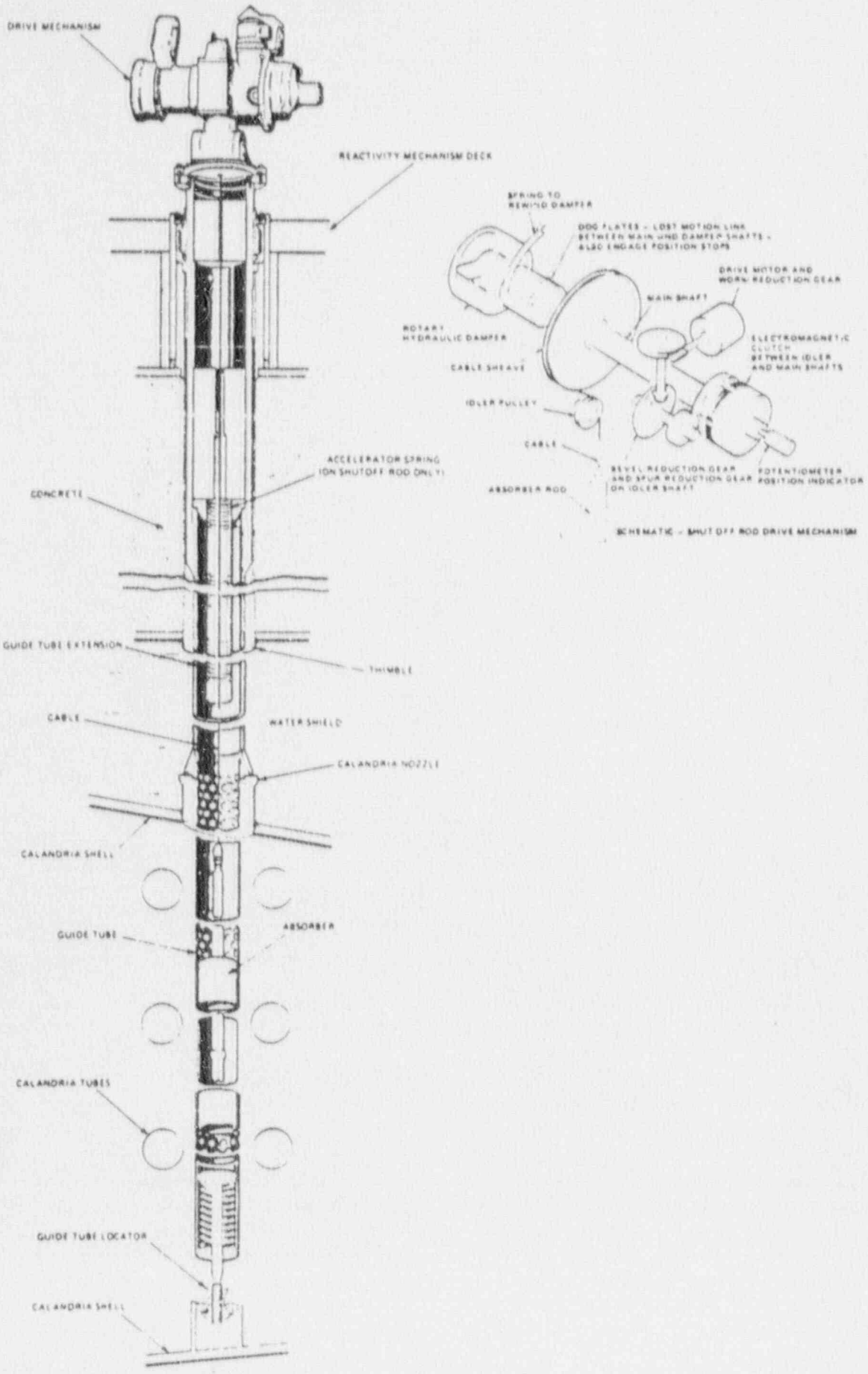


Figure 4 Shutoff and Solid Control Absorber Unit

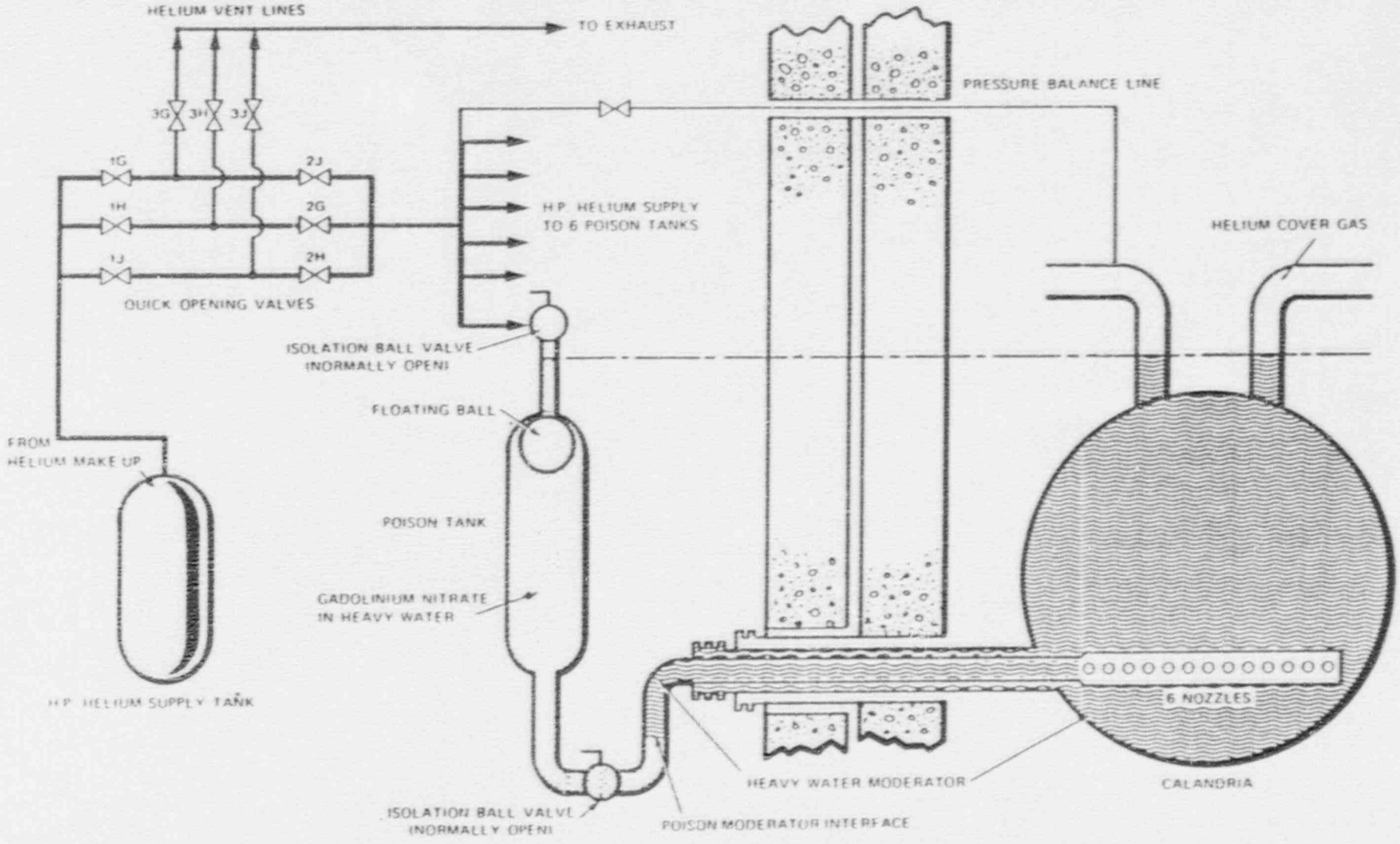


Figure 5 Liquid Injection Shutdown System

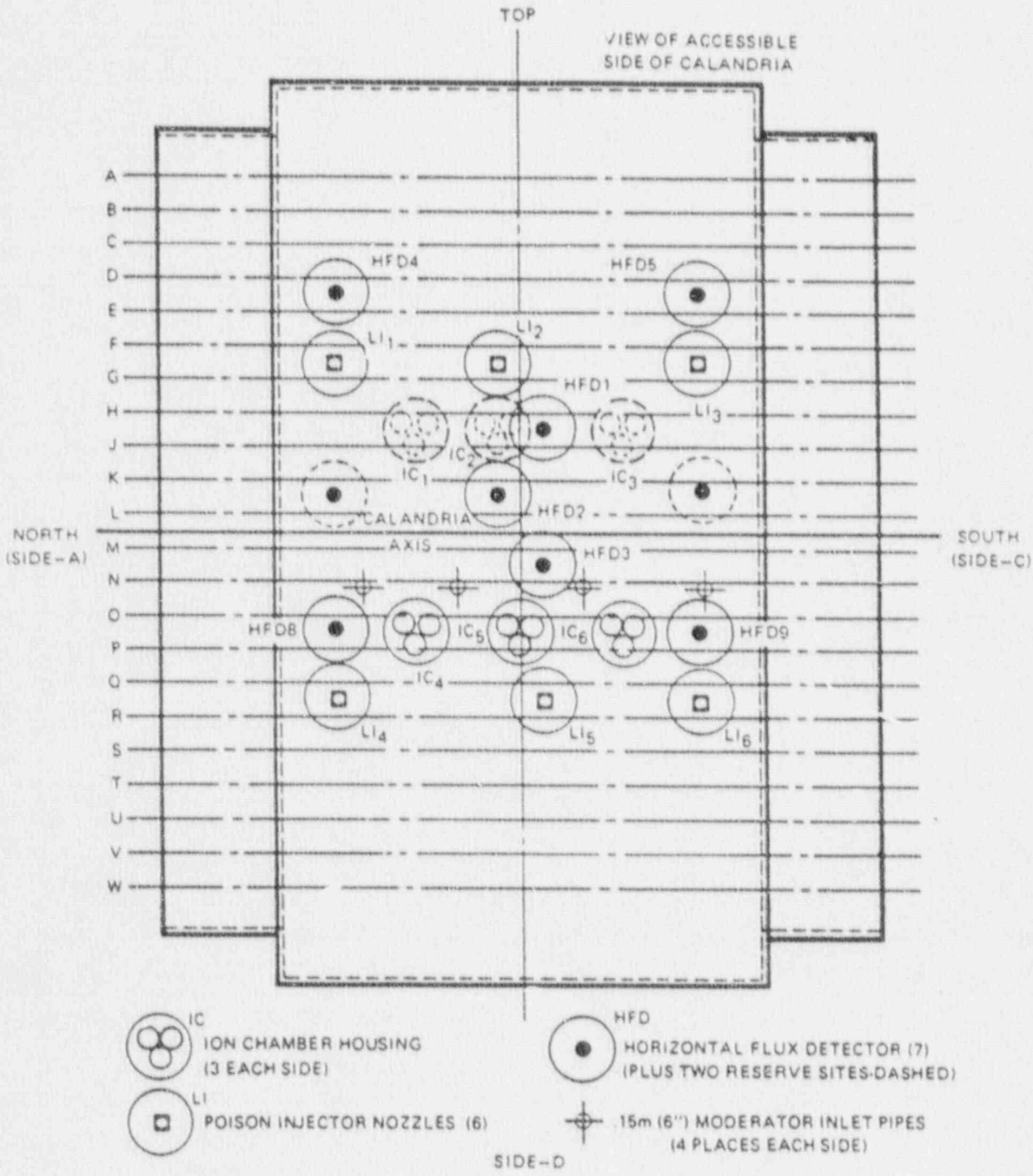


Figure 6 Location of Horizontal Reactivity Devices (600 MW Stations)

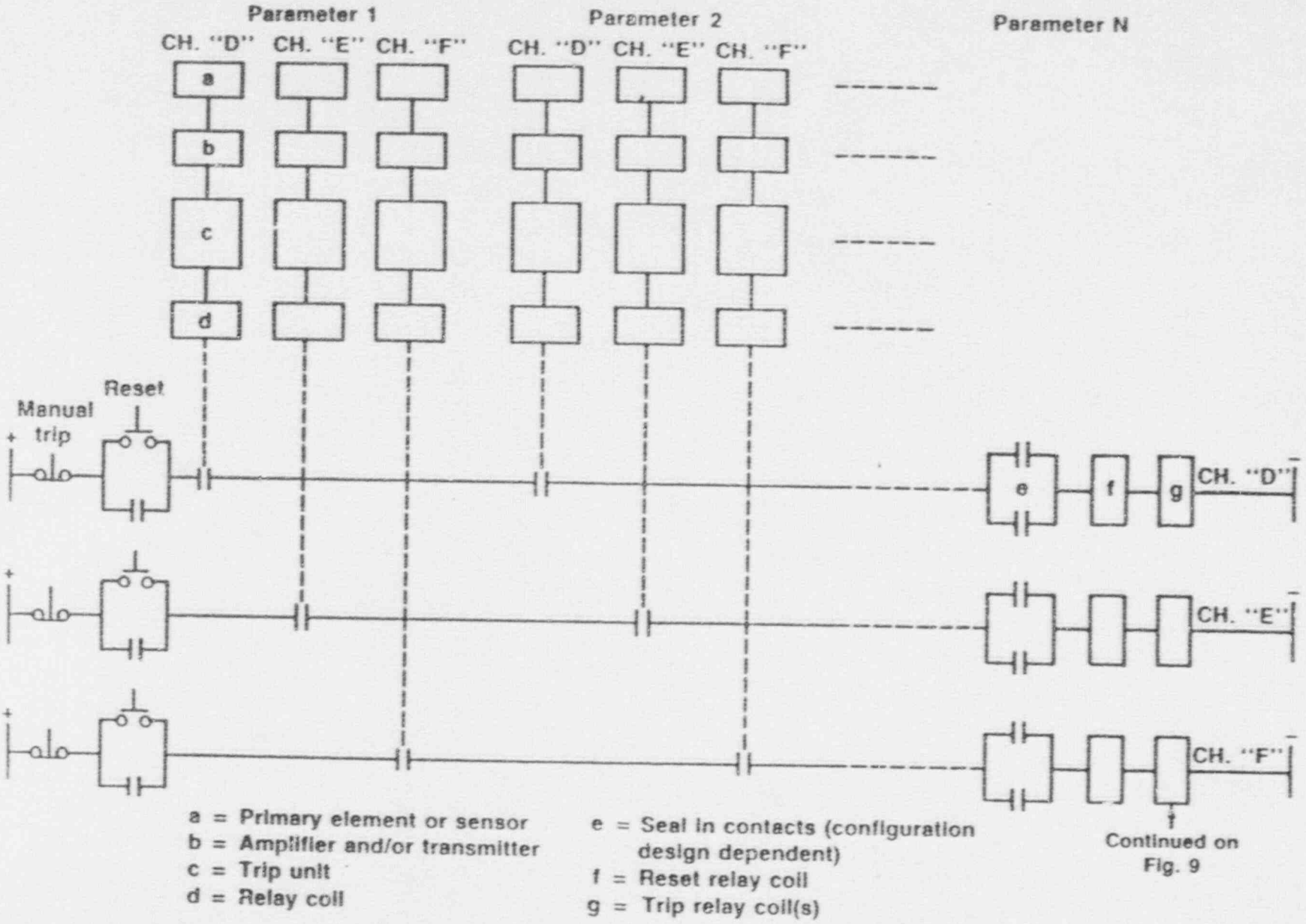


Figure 7 Schematic of General Coincidence Logic

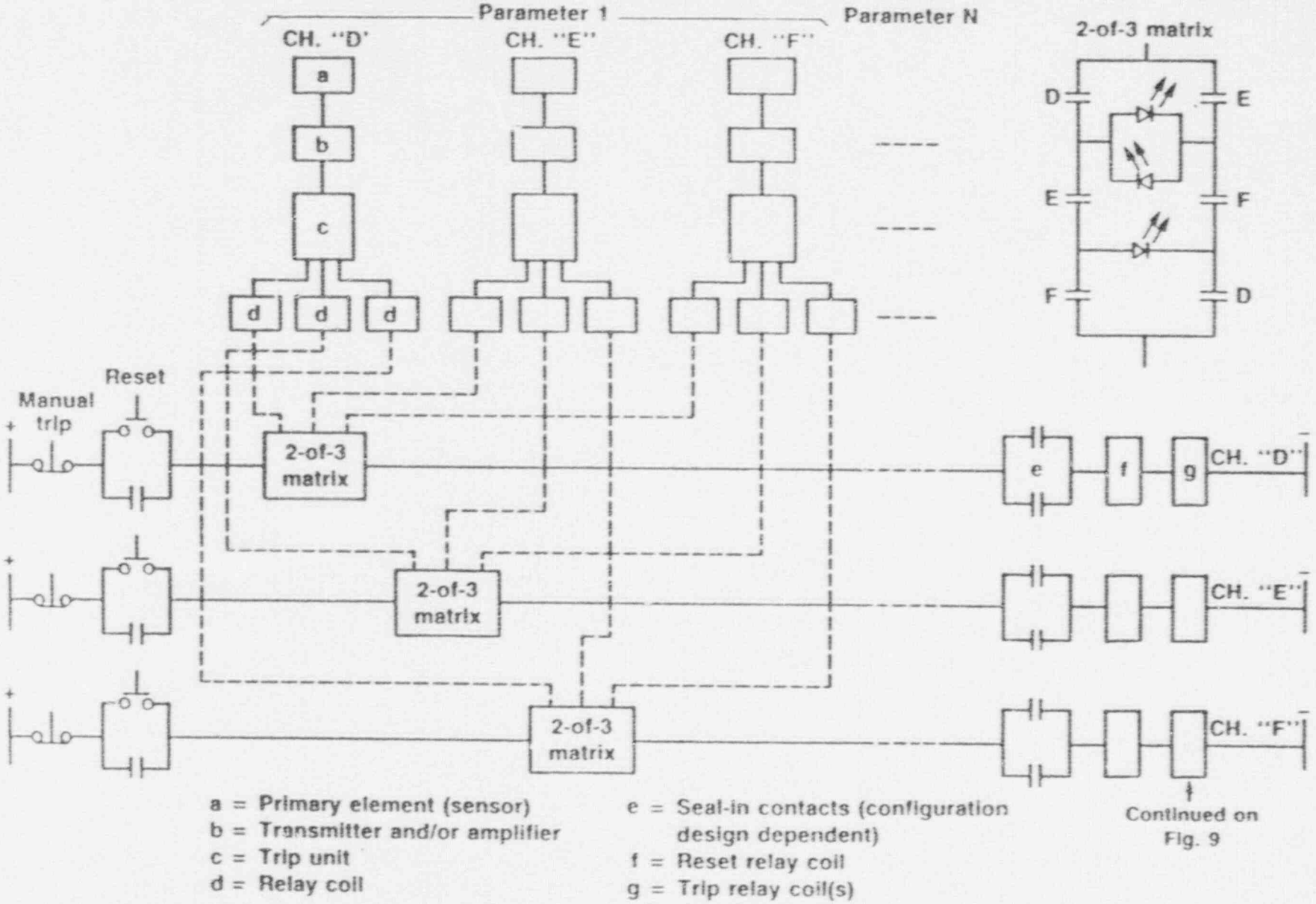
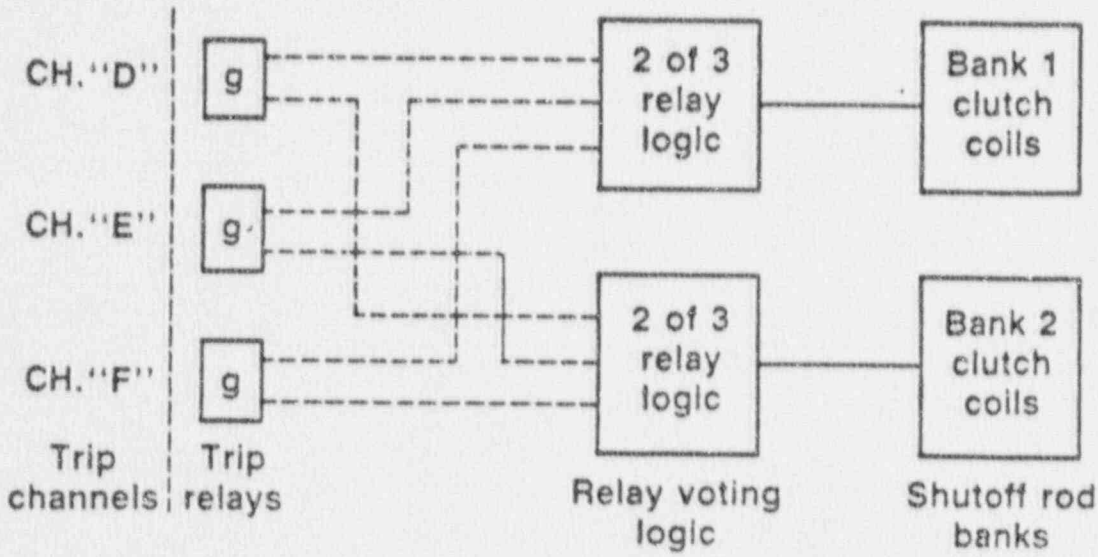
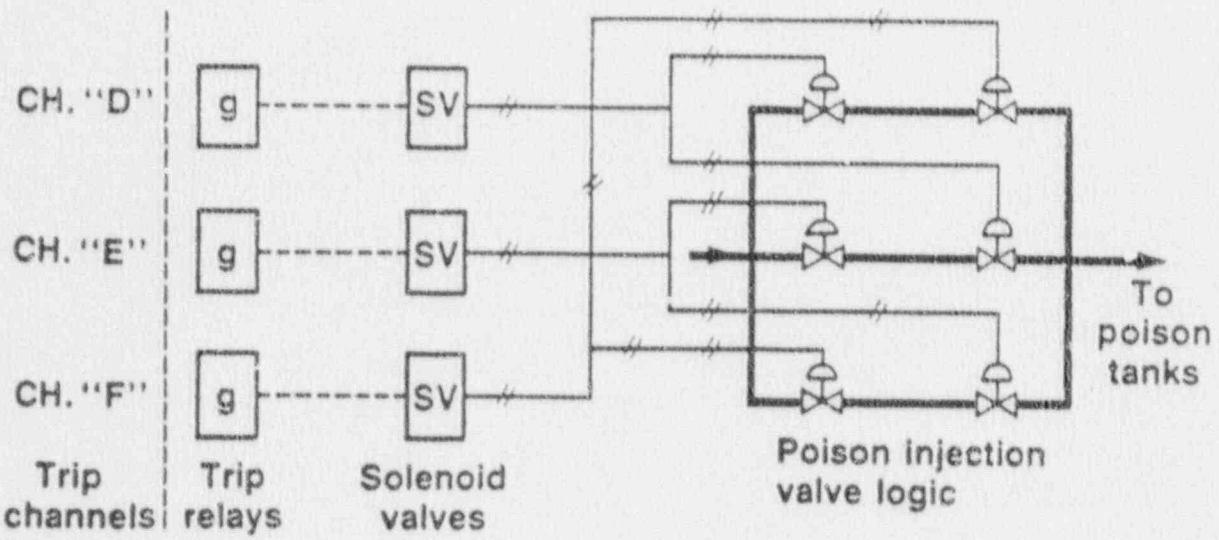


Figure 8 Schematic of Local Coincidence Logic



(a) Typical logic for actuating shutoff rods



(b) Typical logic for actuating poison injection system

Figure 9 Schematics of Logic for Actuating Mechanical Elements of Shutdown Systems

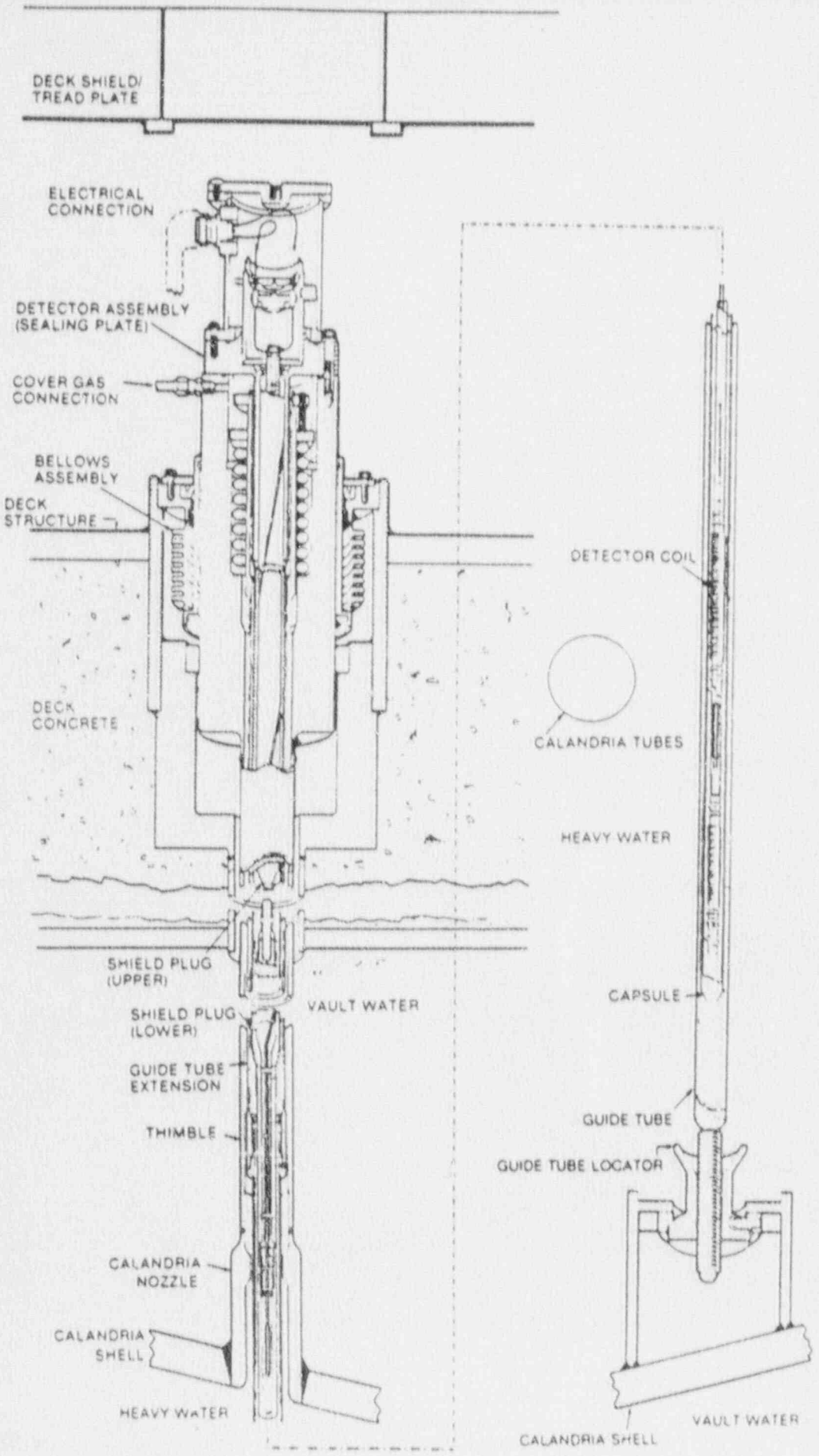


Figure 10 Flux Detector Unit

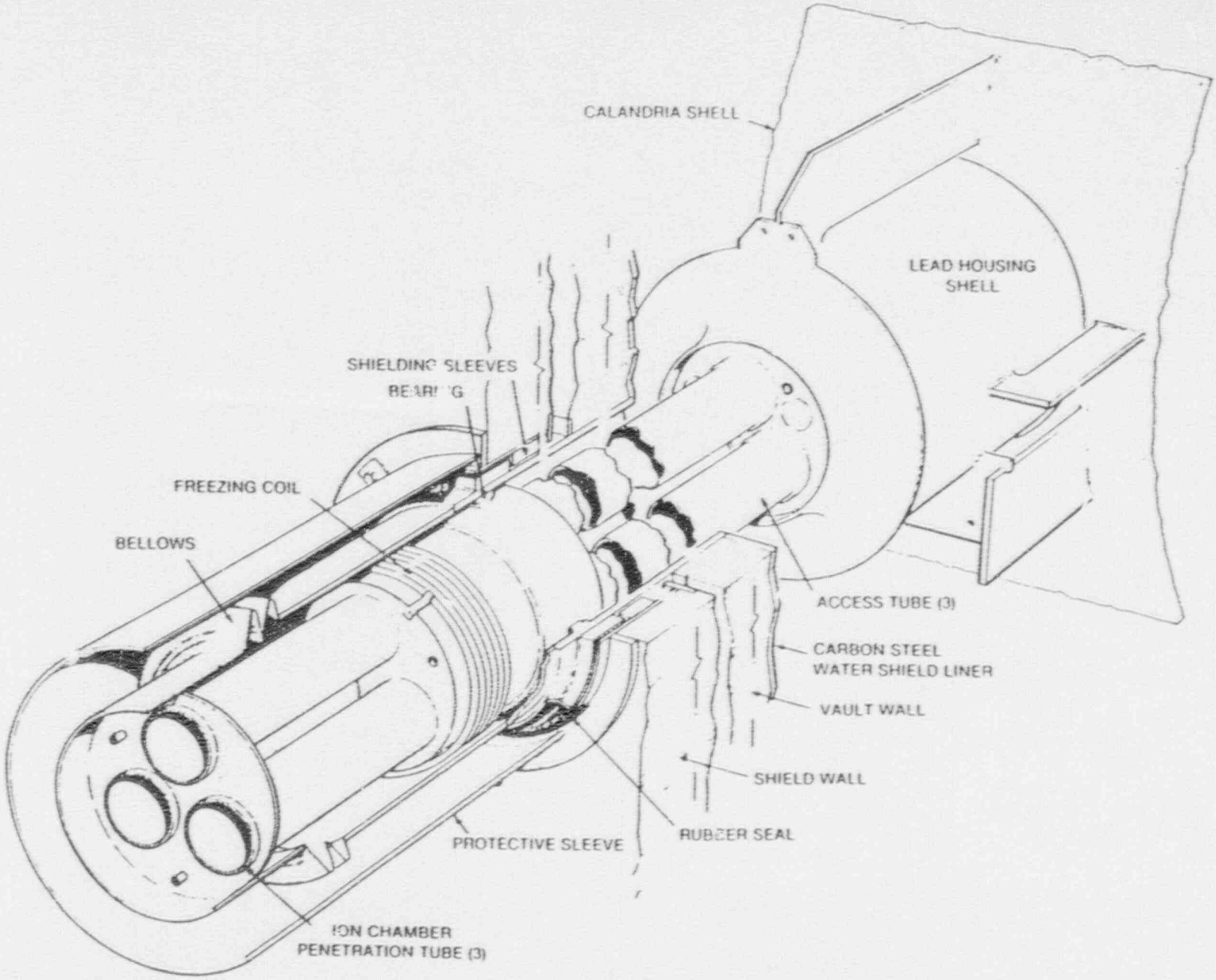


Figure 11 ION Chamber Housing

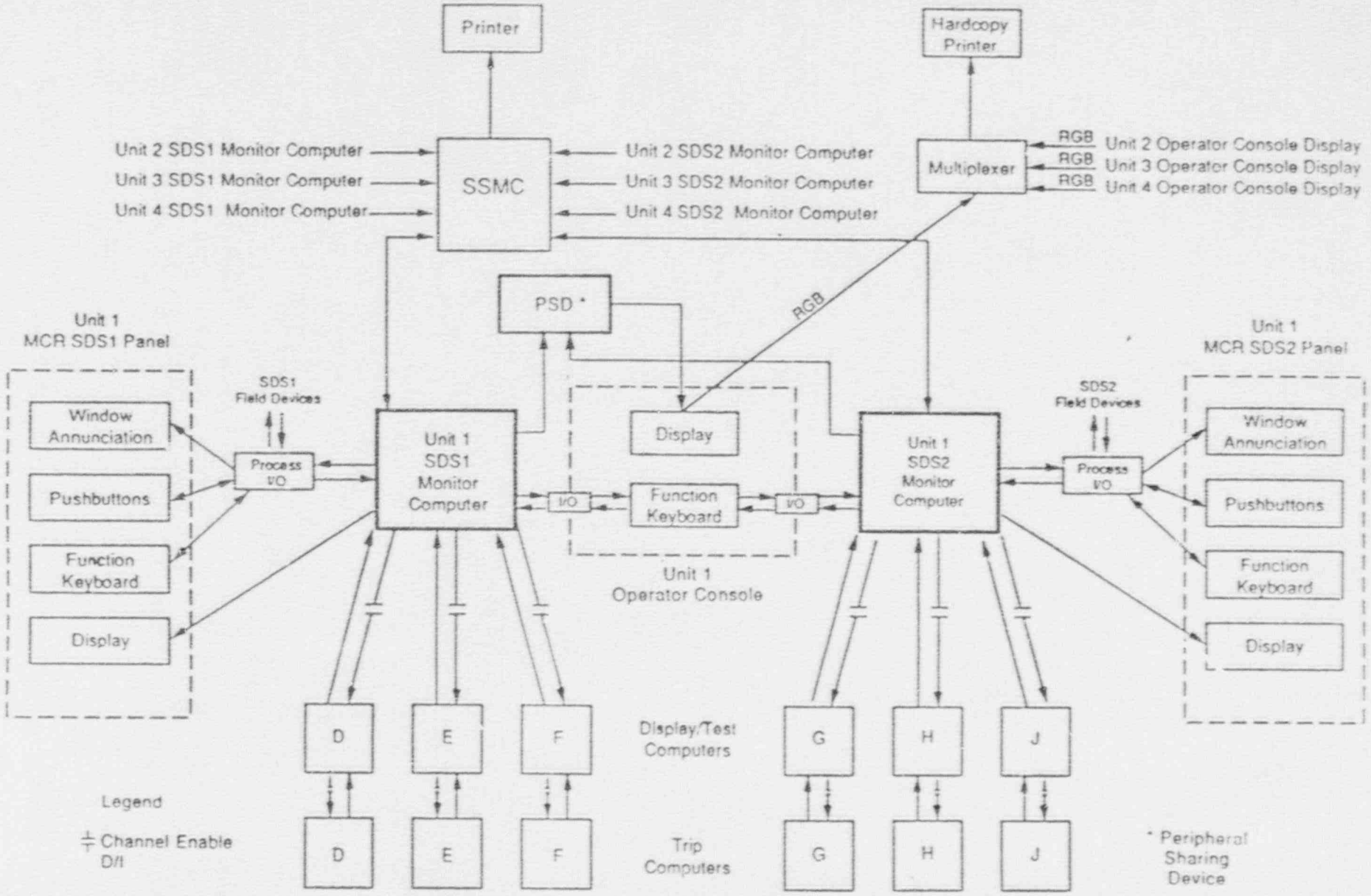


Figure 12 Block Diagram of Darlington Shutdown system Computers

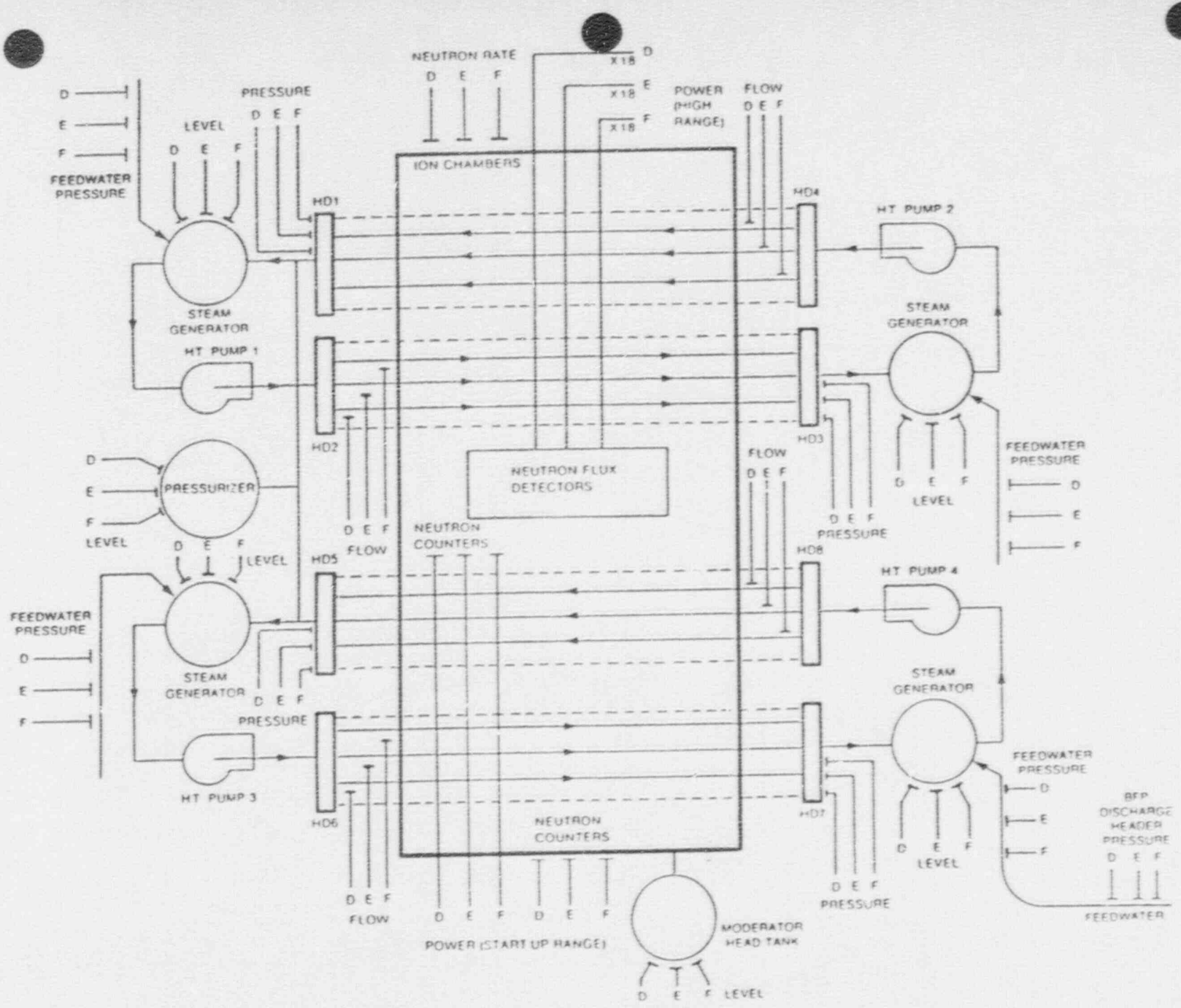


Figure 13 Location of Shutdown System No. 1 Trip Parameter Sensors

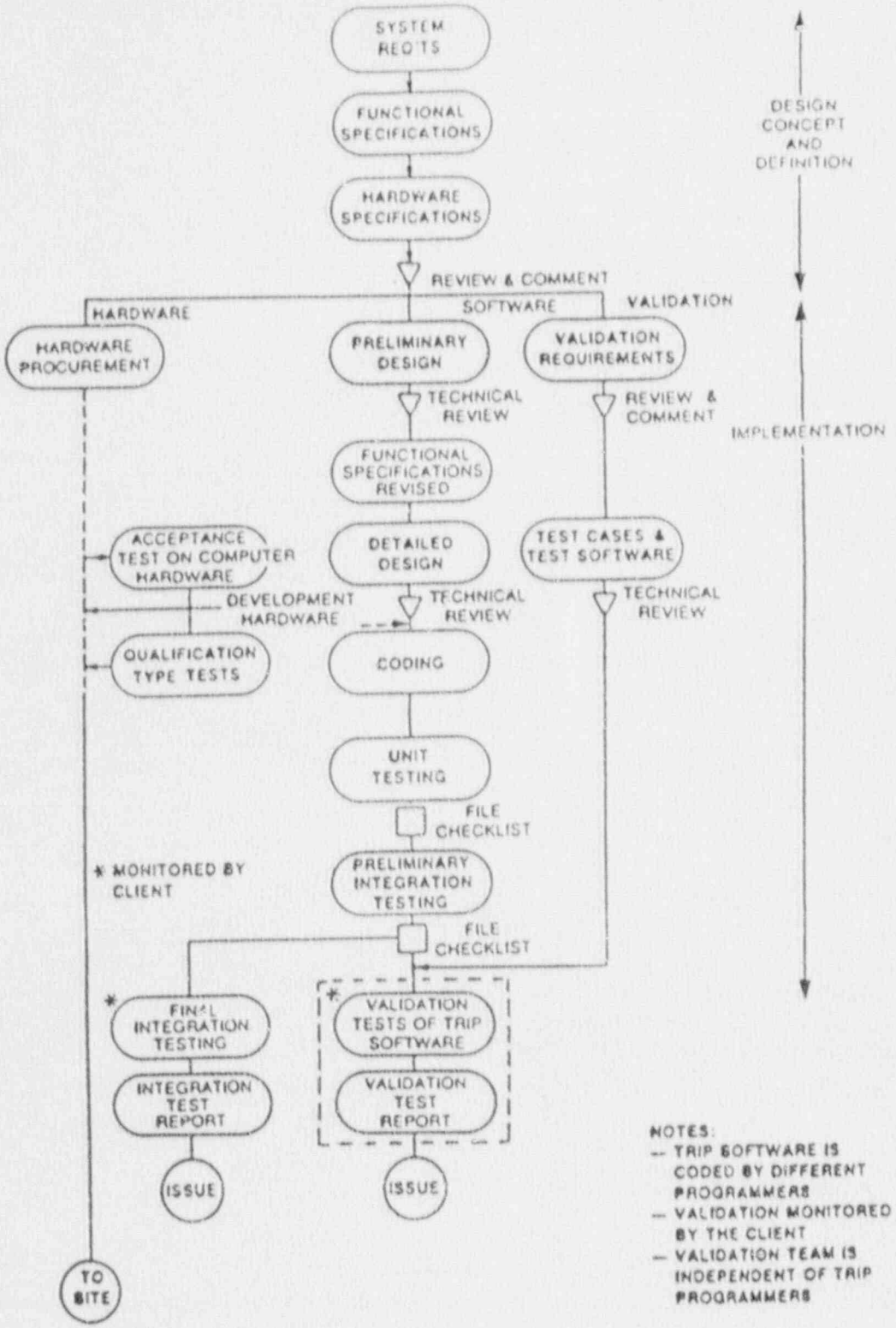


Figure 14 Block Diagram of Design Process for SDS Computer Hardware and Software

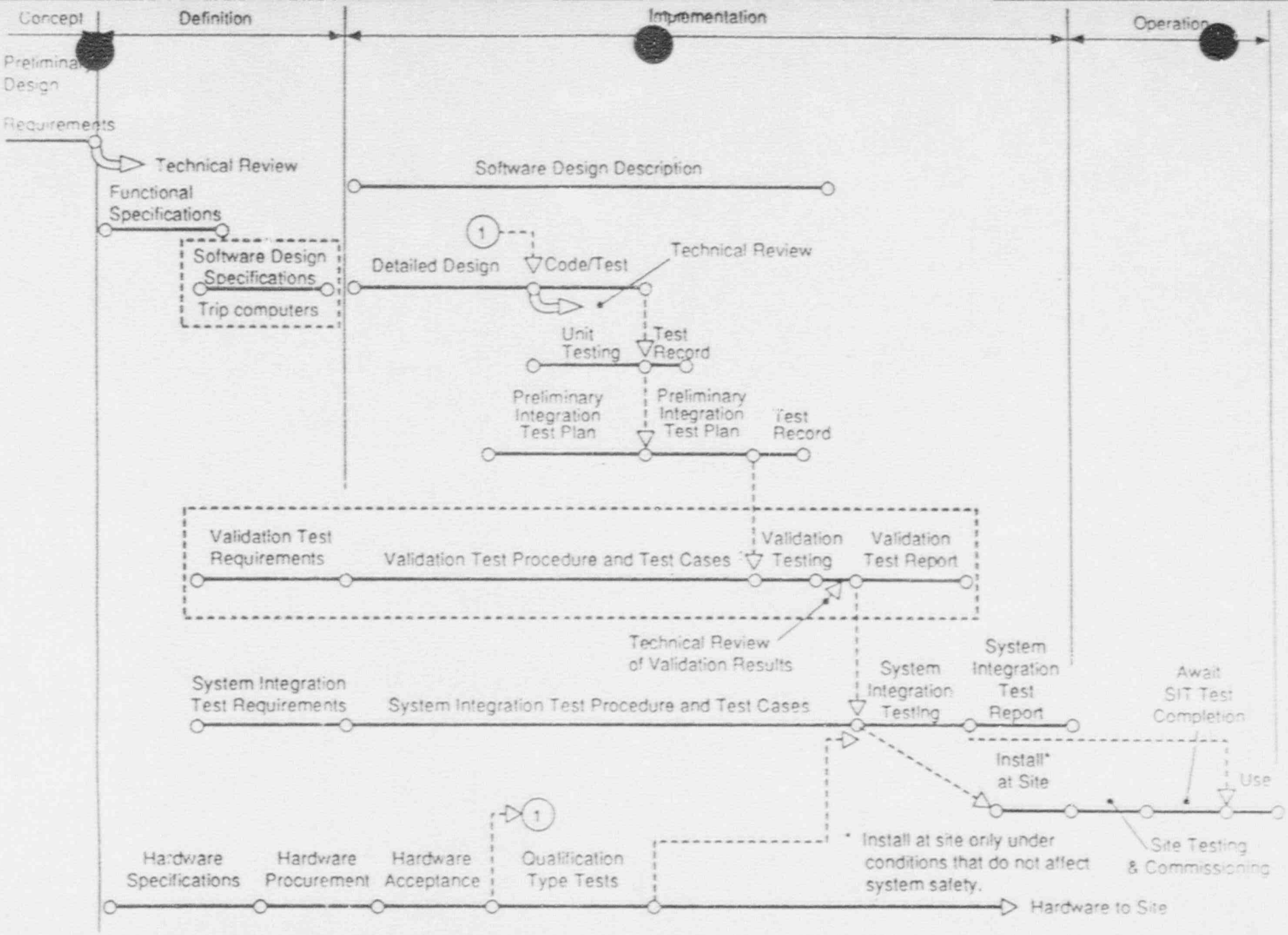


Figure 15 Software Development Process with Hardware Interfaces

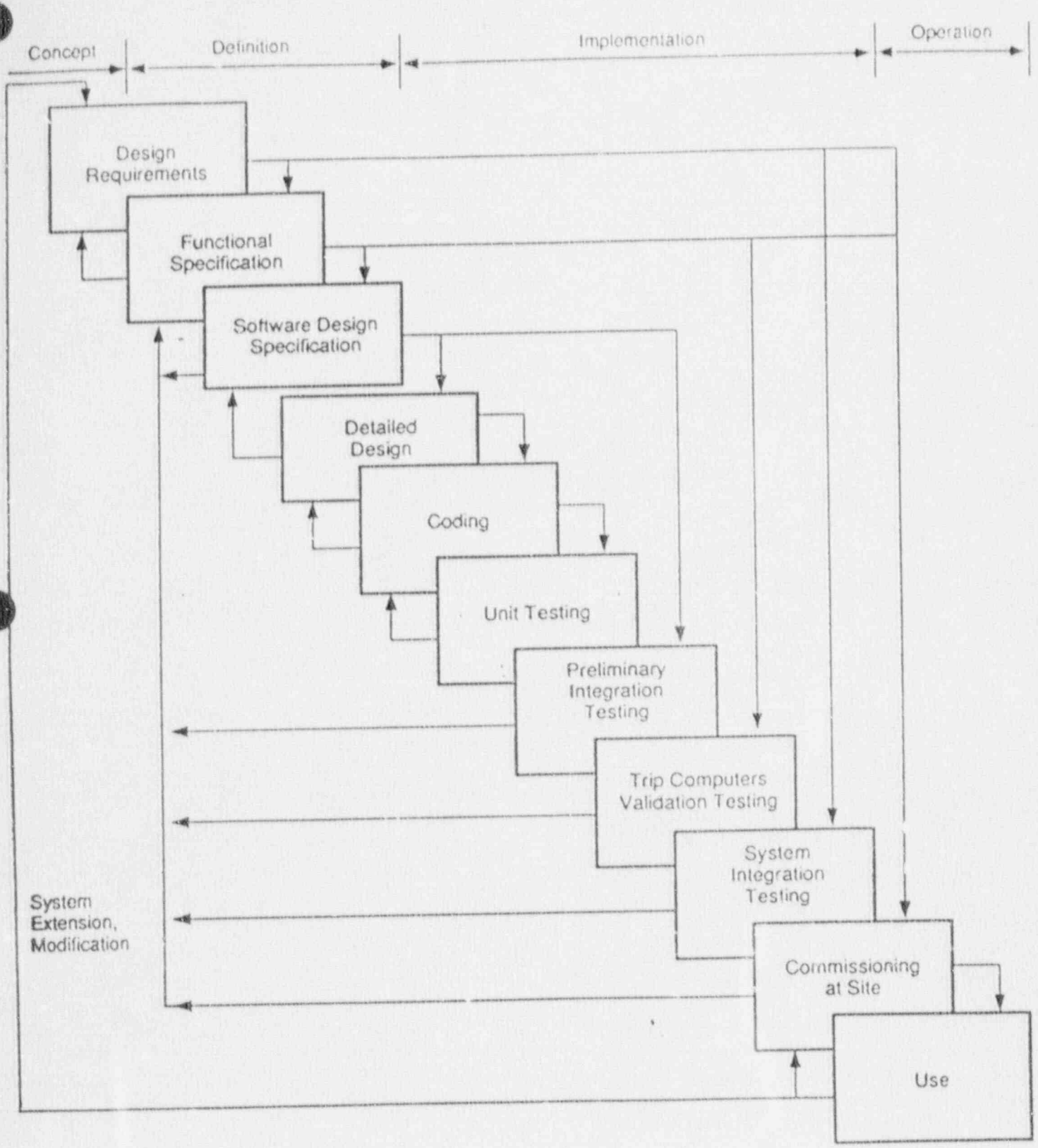


Figure 16 Software Life Cycle

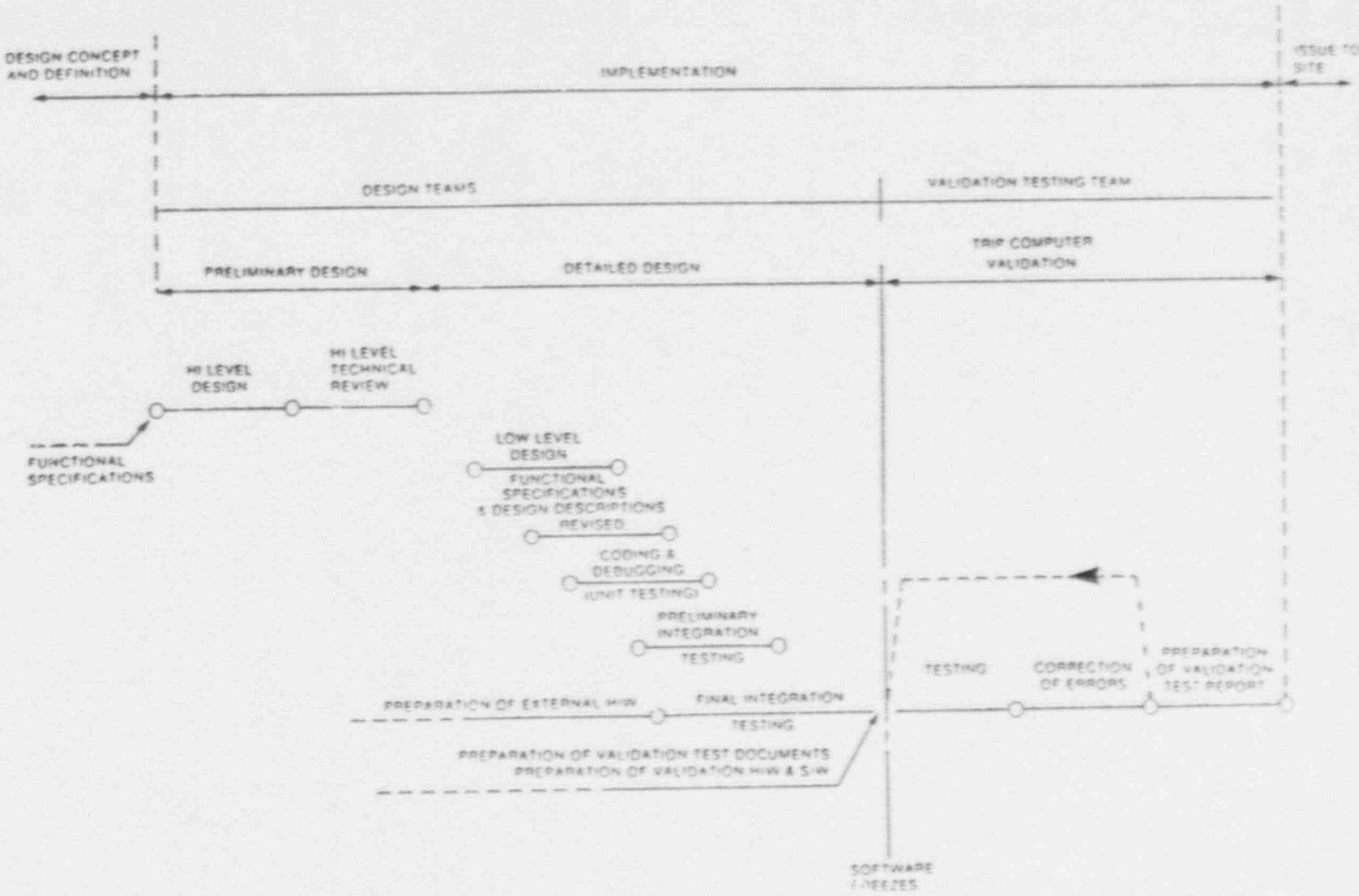


Figure 17 Software Development Life Cycle

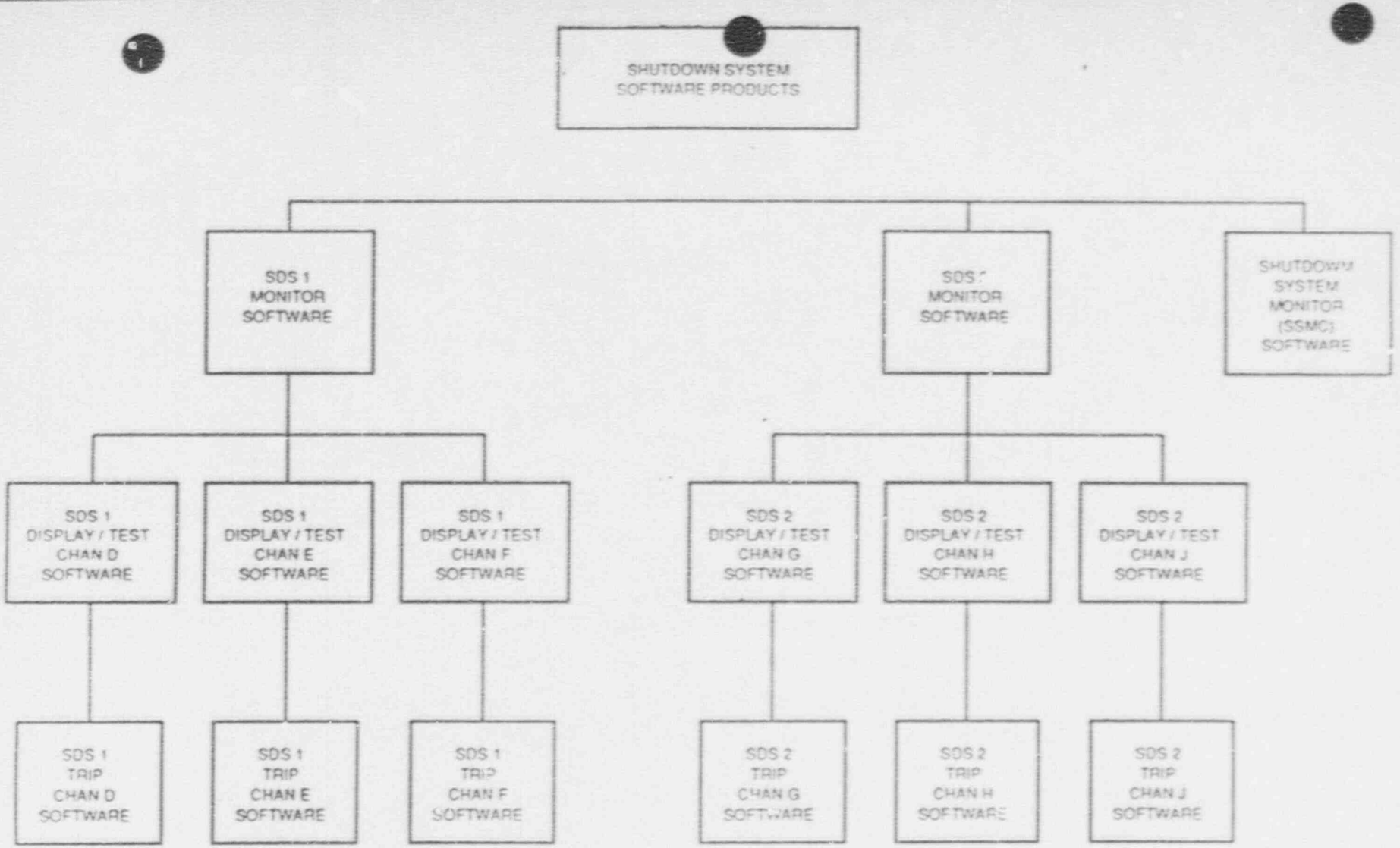


Figure 18 Block Diagram of Shutdown System Software

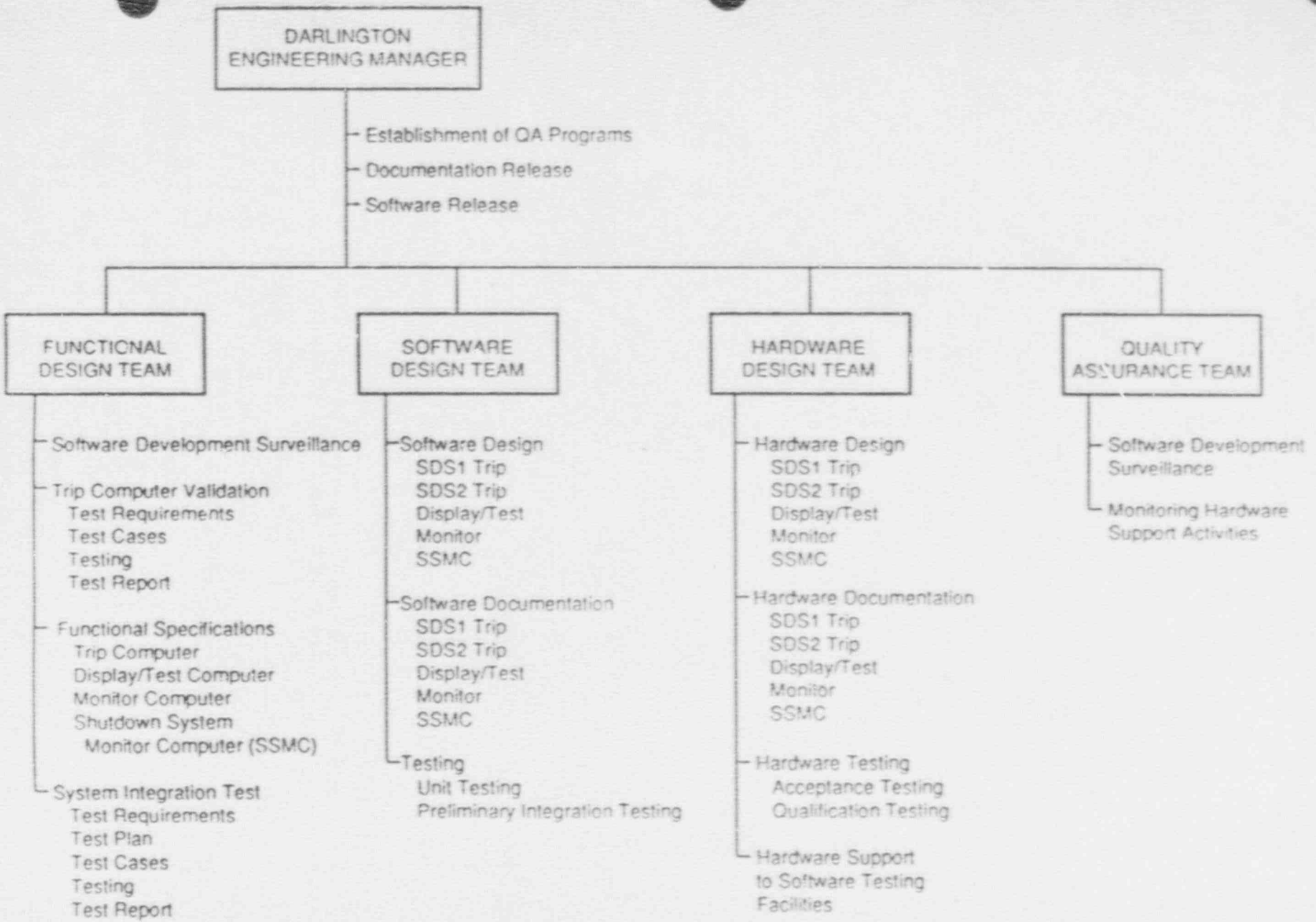


Figure 19 Organization Chart

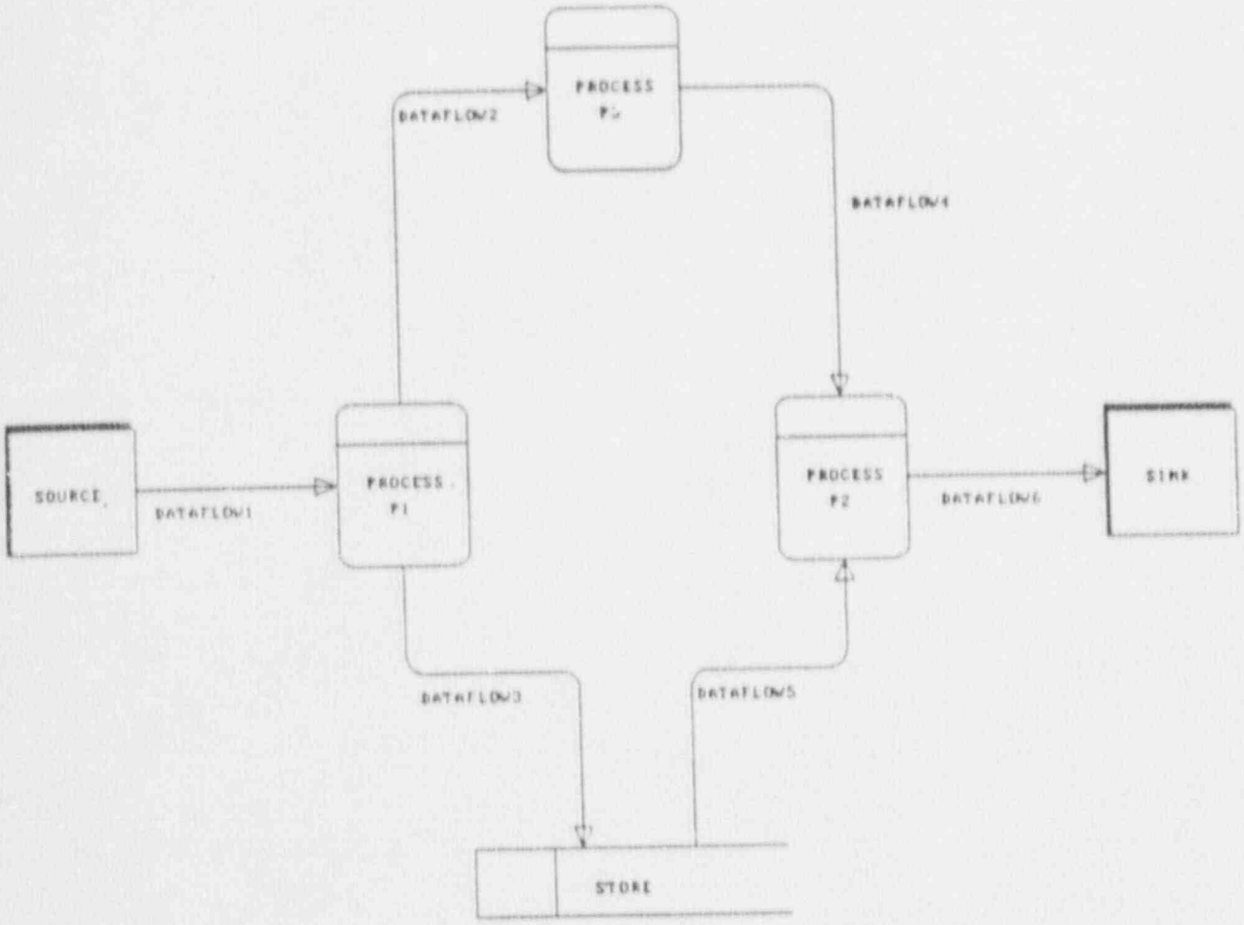


Figure 20 Data Flow

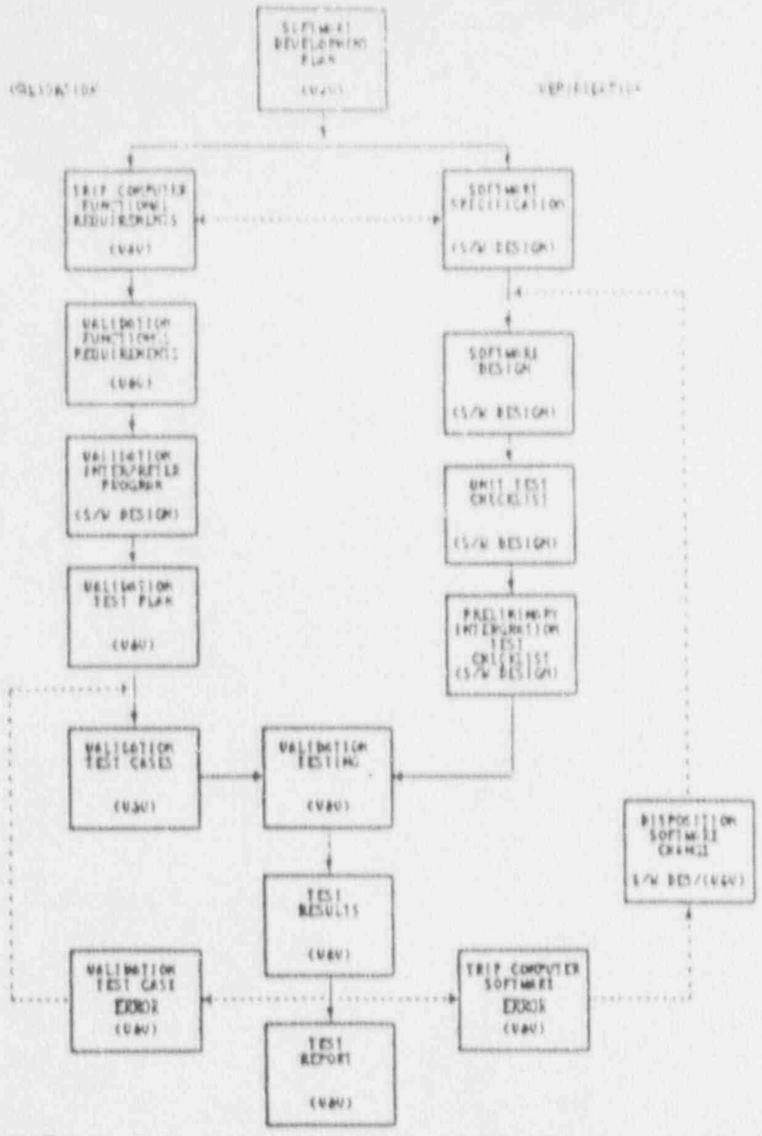
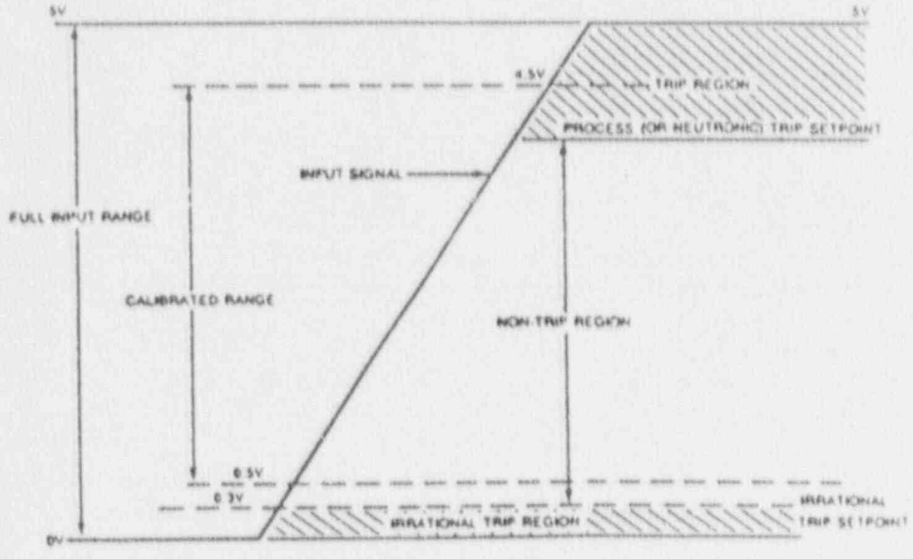


Figure 21 Verification and Validation



NOTE: THE TRIP SETPOINT HAS AN ASSOCIATED DEADBAND (NOT SHOWN)

Figure 23 Required Trip Action for Typical Parameter with High Trip Setpoint and Low Irrational Trip

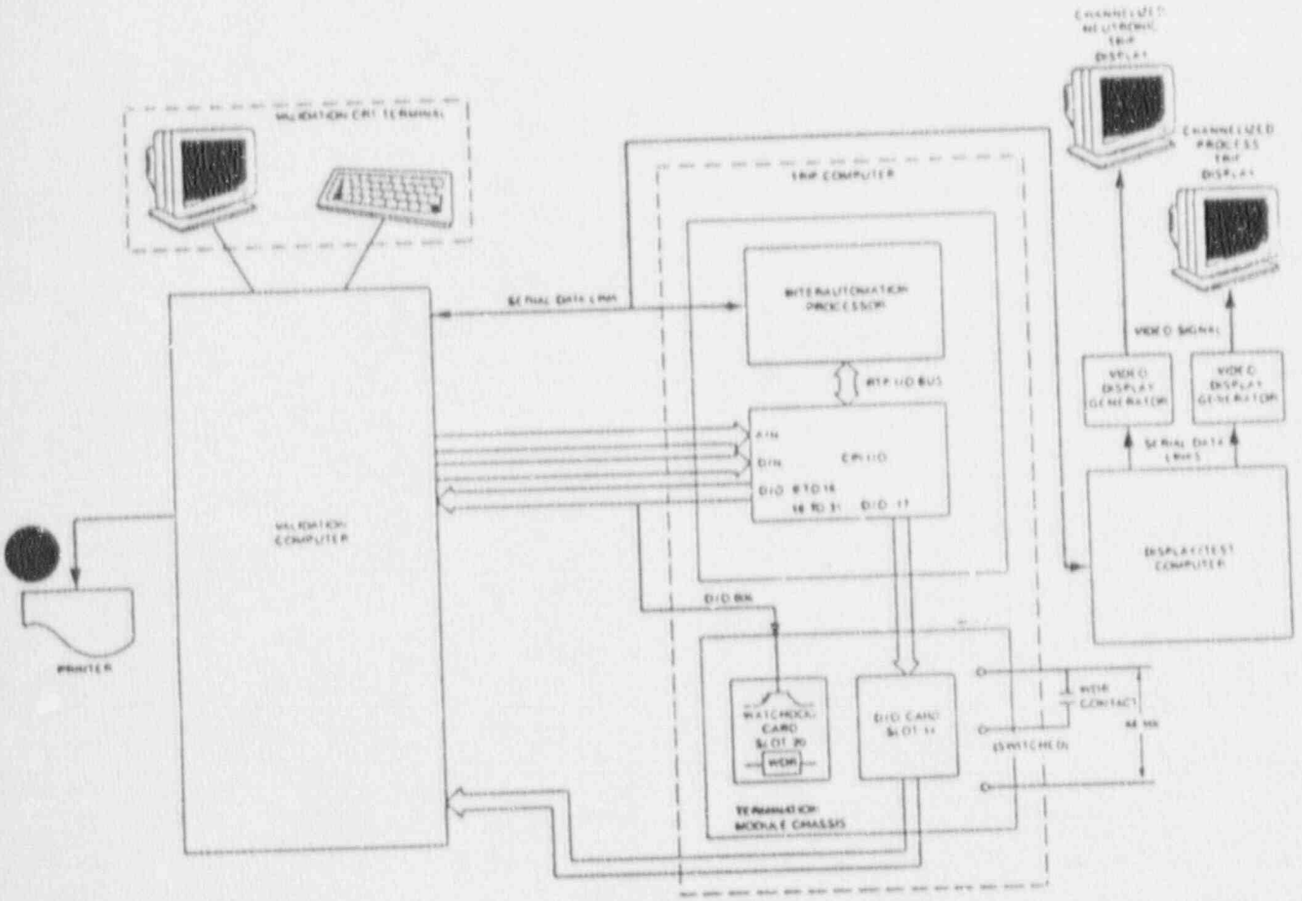


Figure 22 Hardware Configuration for the SDS2 Validation Test Setup

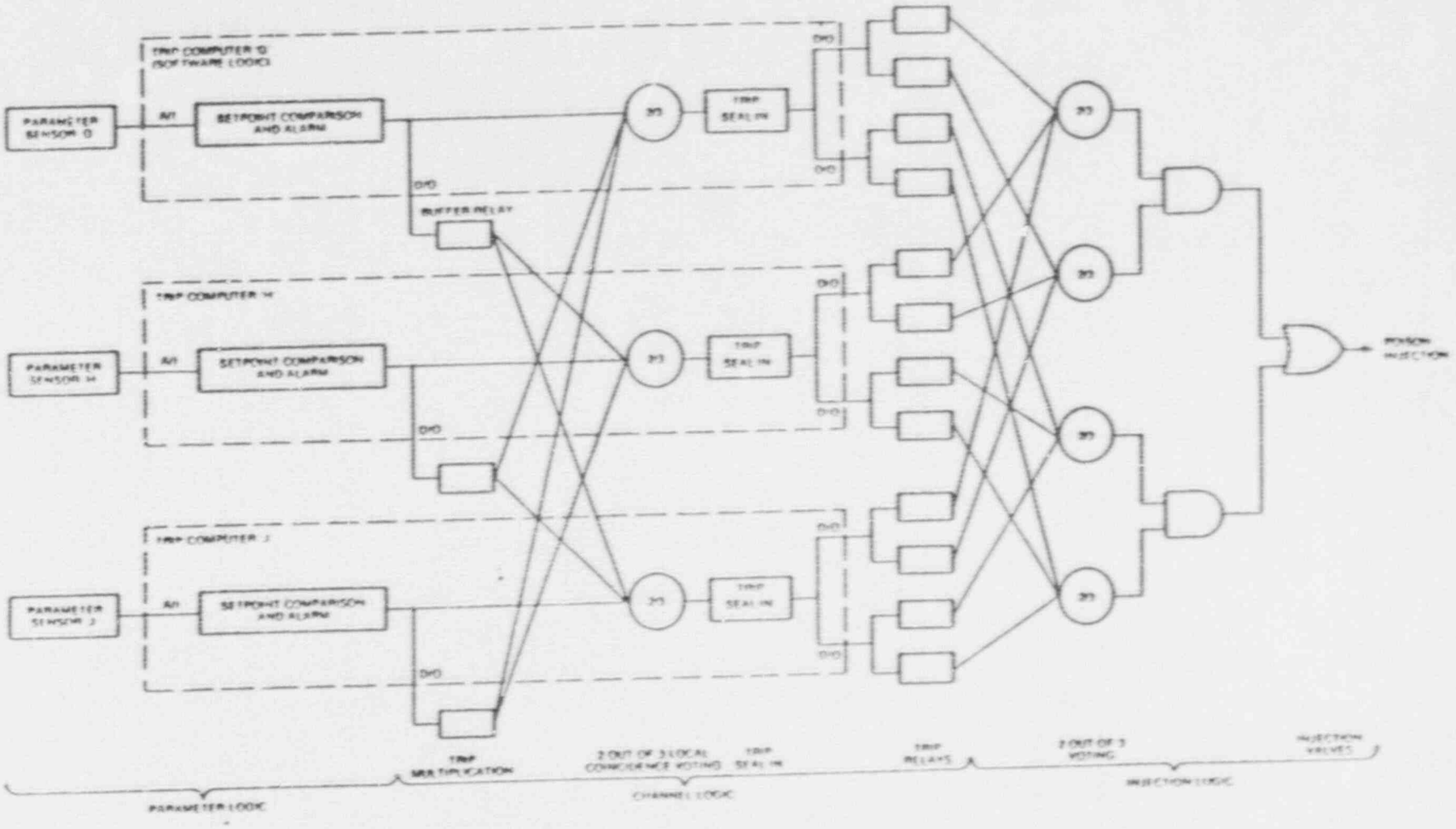


Figure 24 SDS2 Trip Chain Logic Functional Block Diagram for One Trip Parameter

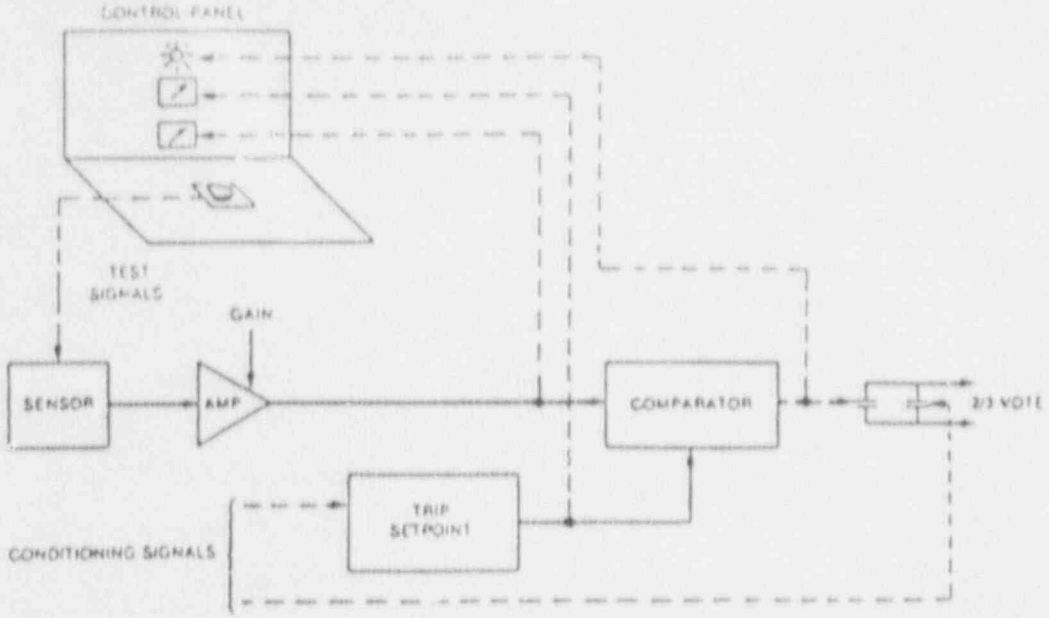


Figure 25 Traditional Shutdown System Design

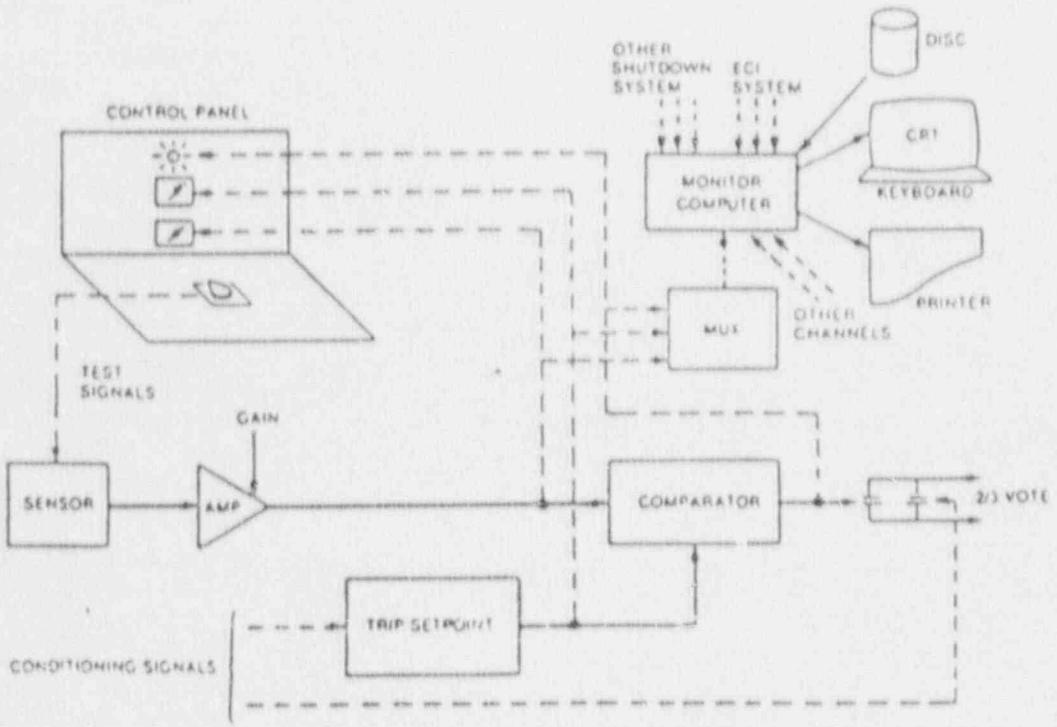


Figure 26 Traditional Shutdown System Design Plus Monitoring Computer (Bruce)

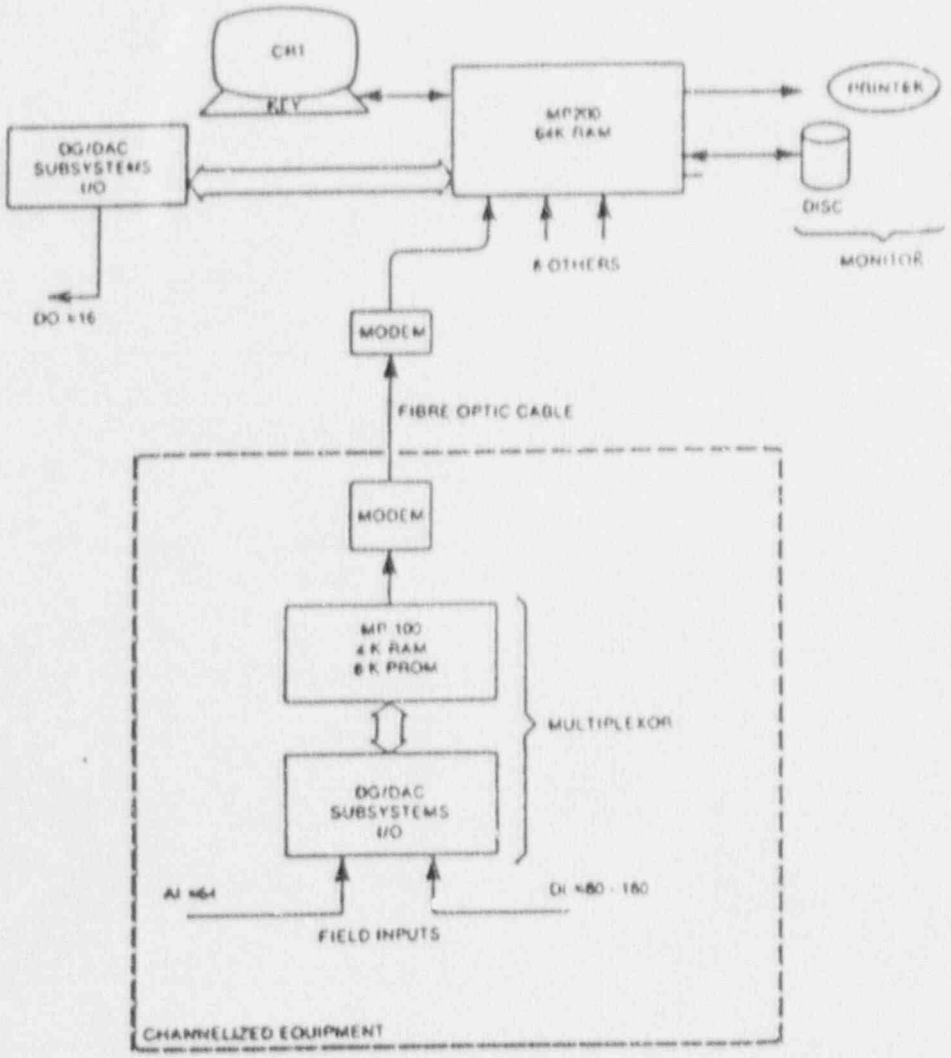


Figure 27 Monitor Computer System (Bruce)

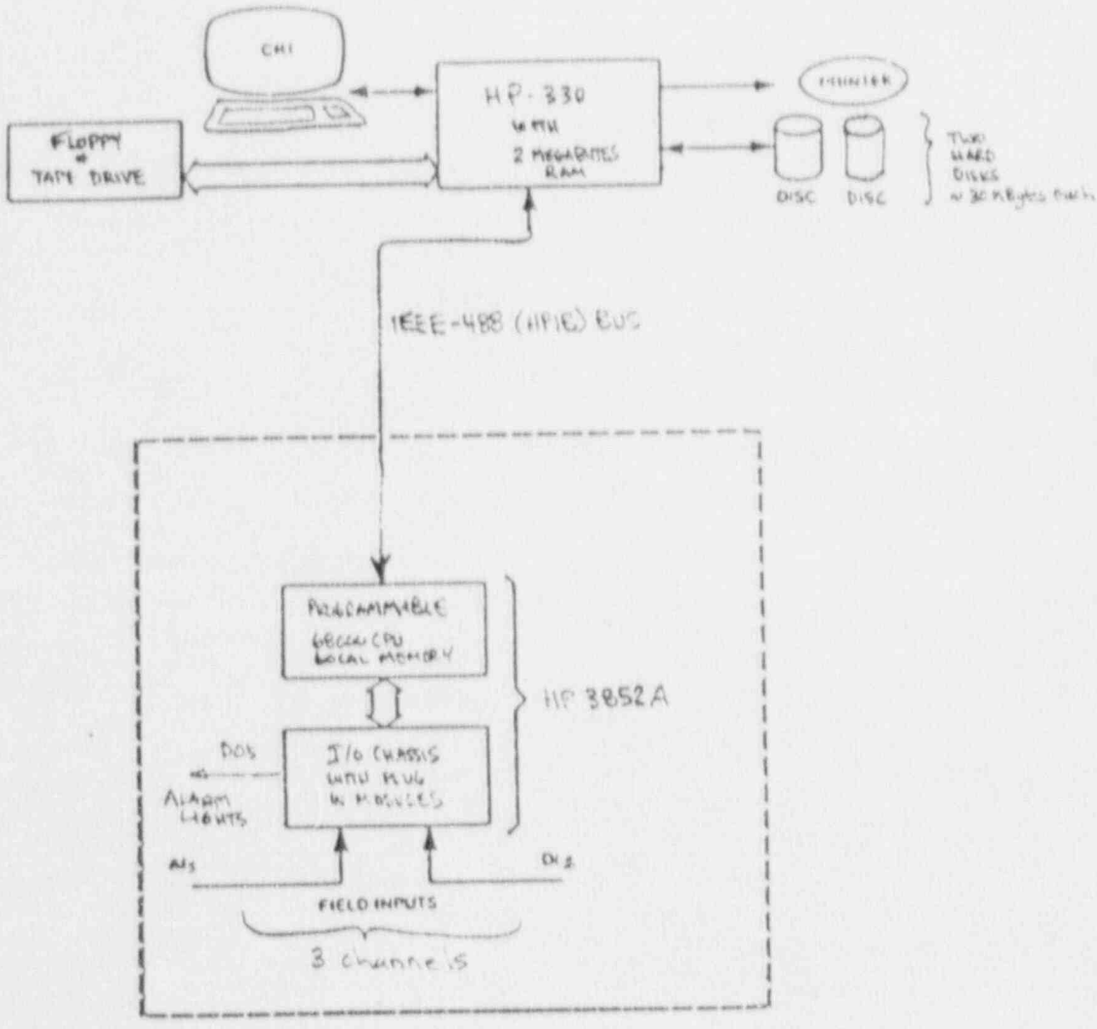


Figure 28 Monitor Computer System (G2)

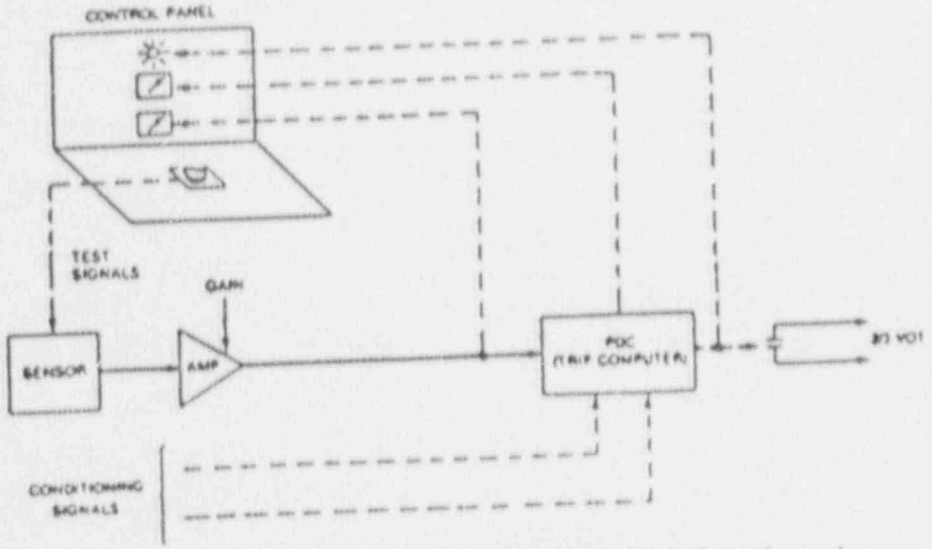


Figure 29 Trip Computer (600 MW Stations)

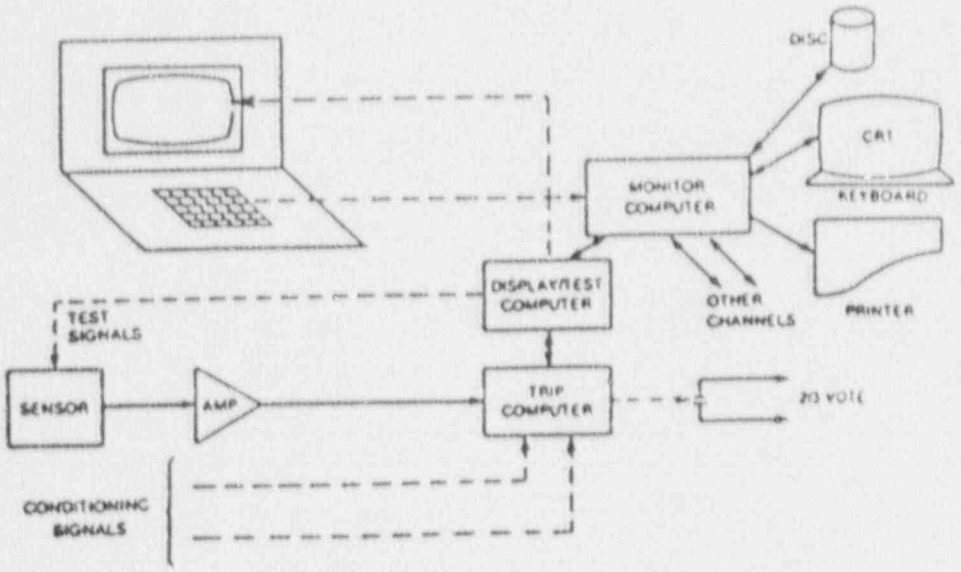


Figure 30 Fully Computerized Shutdown System

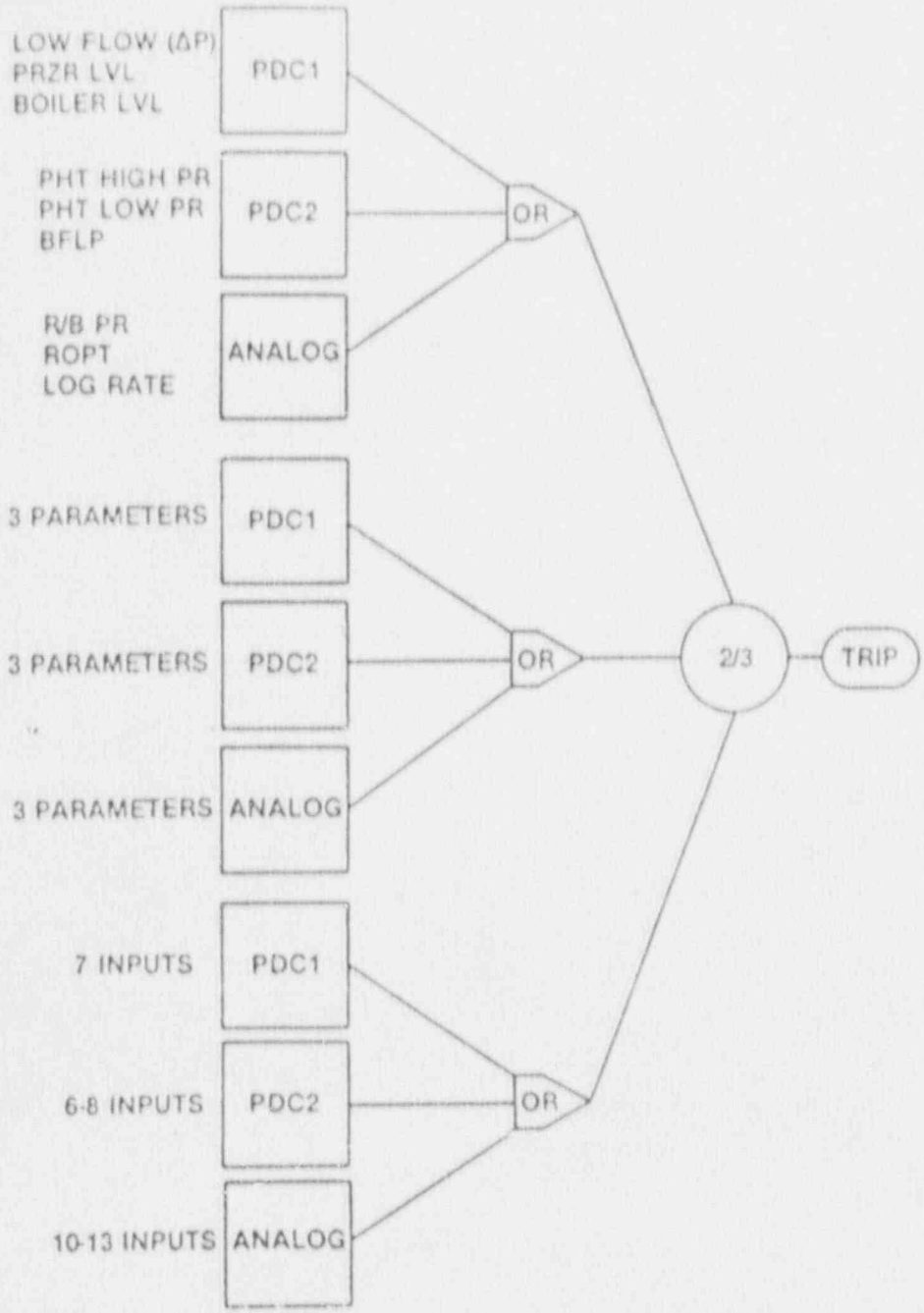


Figure 31 CANDU 6 Shutdown System Utilizing PDC's

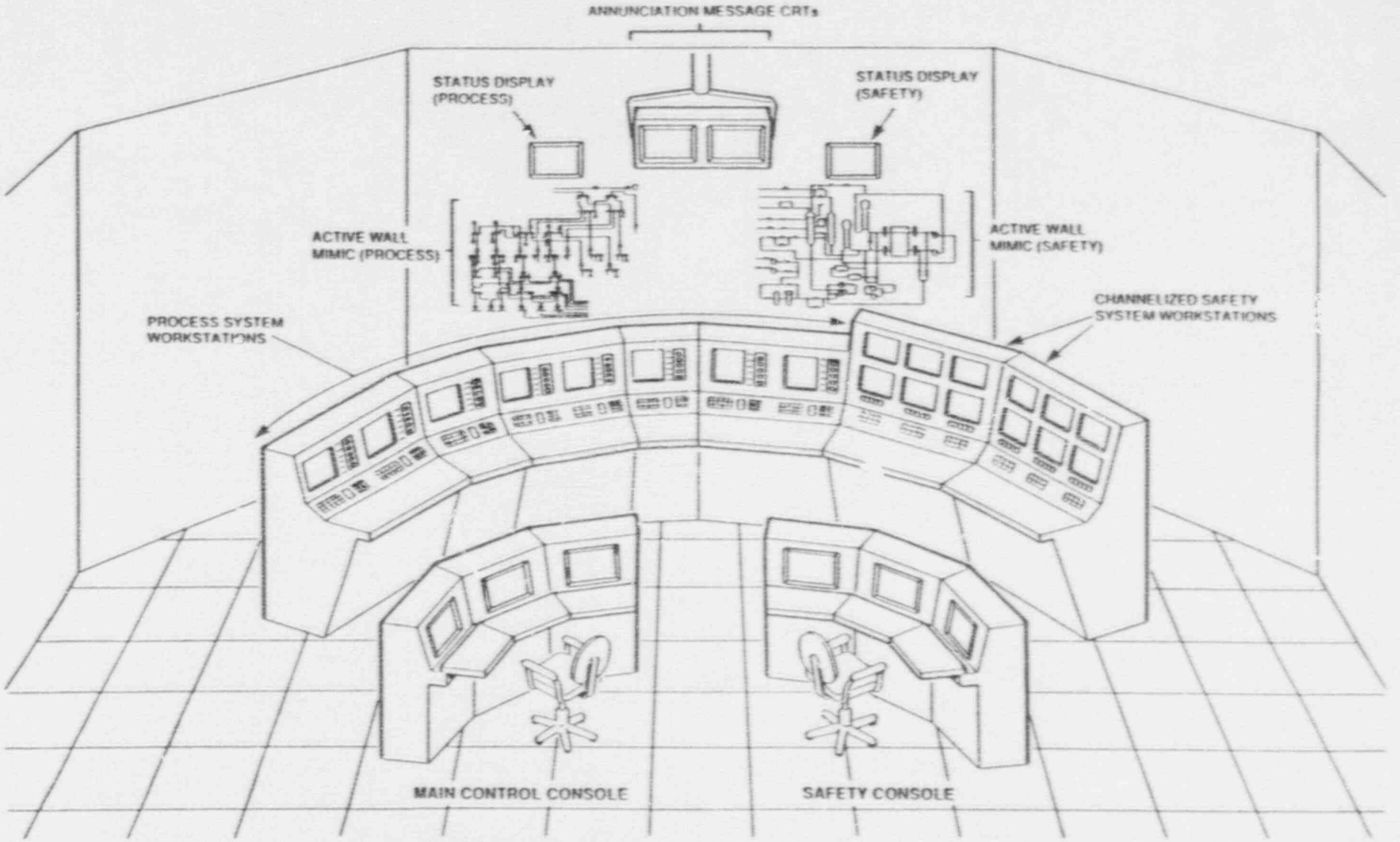
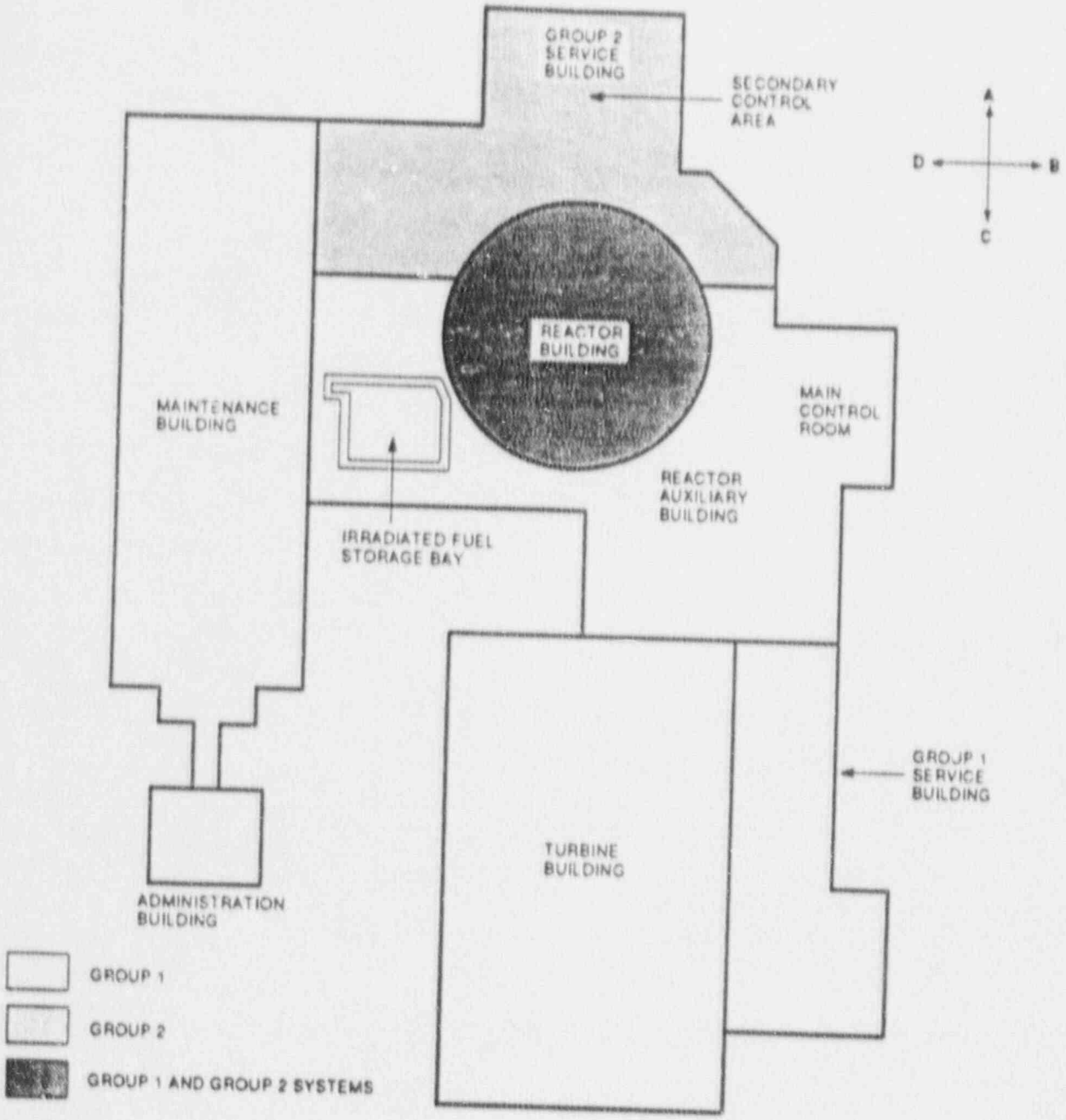


Figure 32 CANDU 3 Control Room



GROUP 1

SHUTDOWN
- REACTOR REGULATING SYSTEM

HEAT REMOVAL
- STEAM GENERATOR FEEDWATER SYSTEM
- LOCAL AIR COOLERS

MONITORING AND CONTROL
- MAIN CONTROL ROOM

SUPPORT SYSTEMS
- ELECTRICAL POWER SYSTEM
- INSTRUMENT AIR SYSTEM

GROUP 2

SHUTDOWN
- SHUTDOWN SYSTEM NO.2
- SHUTDOWN SYSTEM NO.1

HEAT REMOVAL
- GROUP 2 FEEDWATER SYSTEM
- SHUTDOWN COOLING SYSTEM
- EMERGENCY CORE COOLING SYSTEM

MONITORING AND CONTROL
- SECONDARY CONTROL AREA

CONTAINMENT
- CONTAINMENT SYSTEM

SUPPORT SYSTEMS
- GROUP 2 ELECTRICAL POWER SYSTEM
- GROUP 2 RAW SERVICE WATER SYSTEM

Figure 33 CANDU 3 Two Group Separation