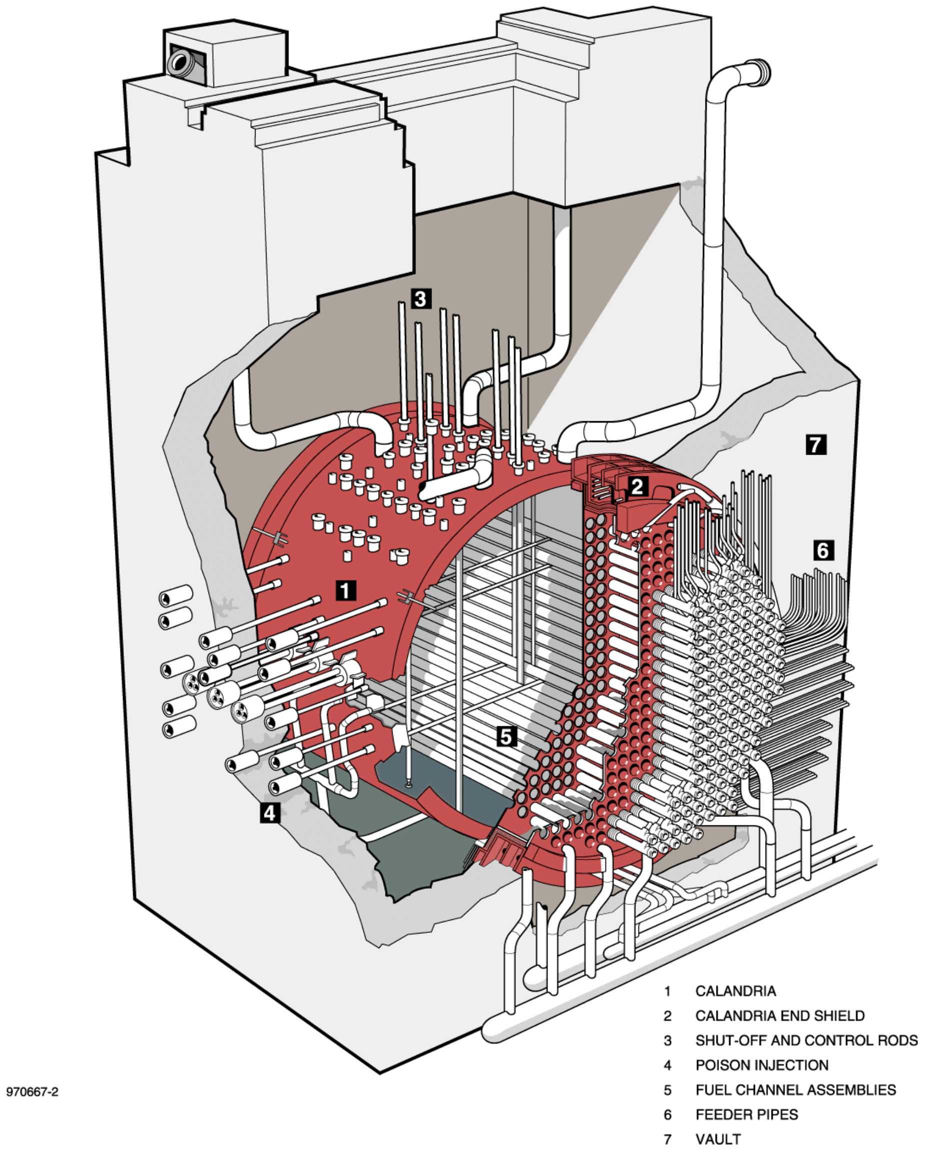
CANDU Safety
#5 - Safety Functions - Shutdown Systems

Dr. V.G. Snell
Director
Safety & Licensing

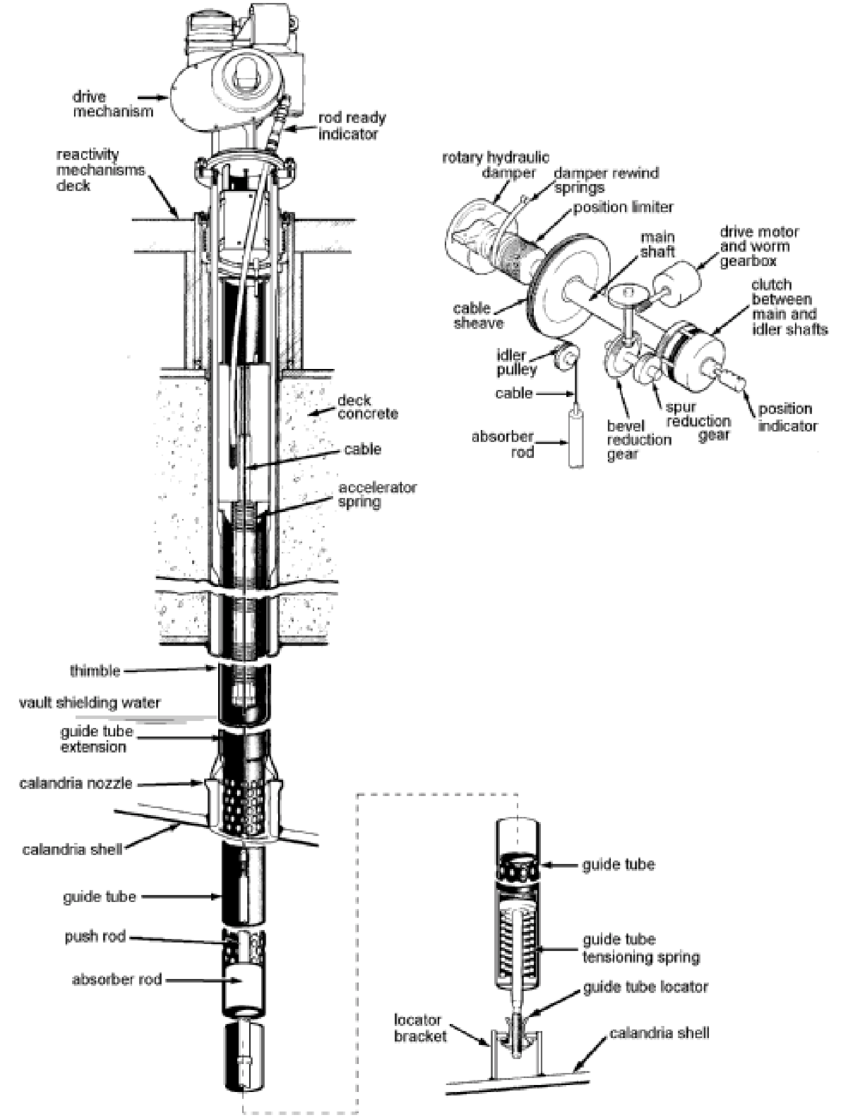
Location of Shutdown Systems Relative to the Reactor and Reactivity Mechanisms



CANDU 6 Reactor Assembly

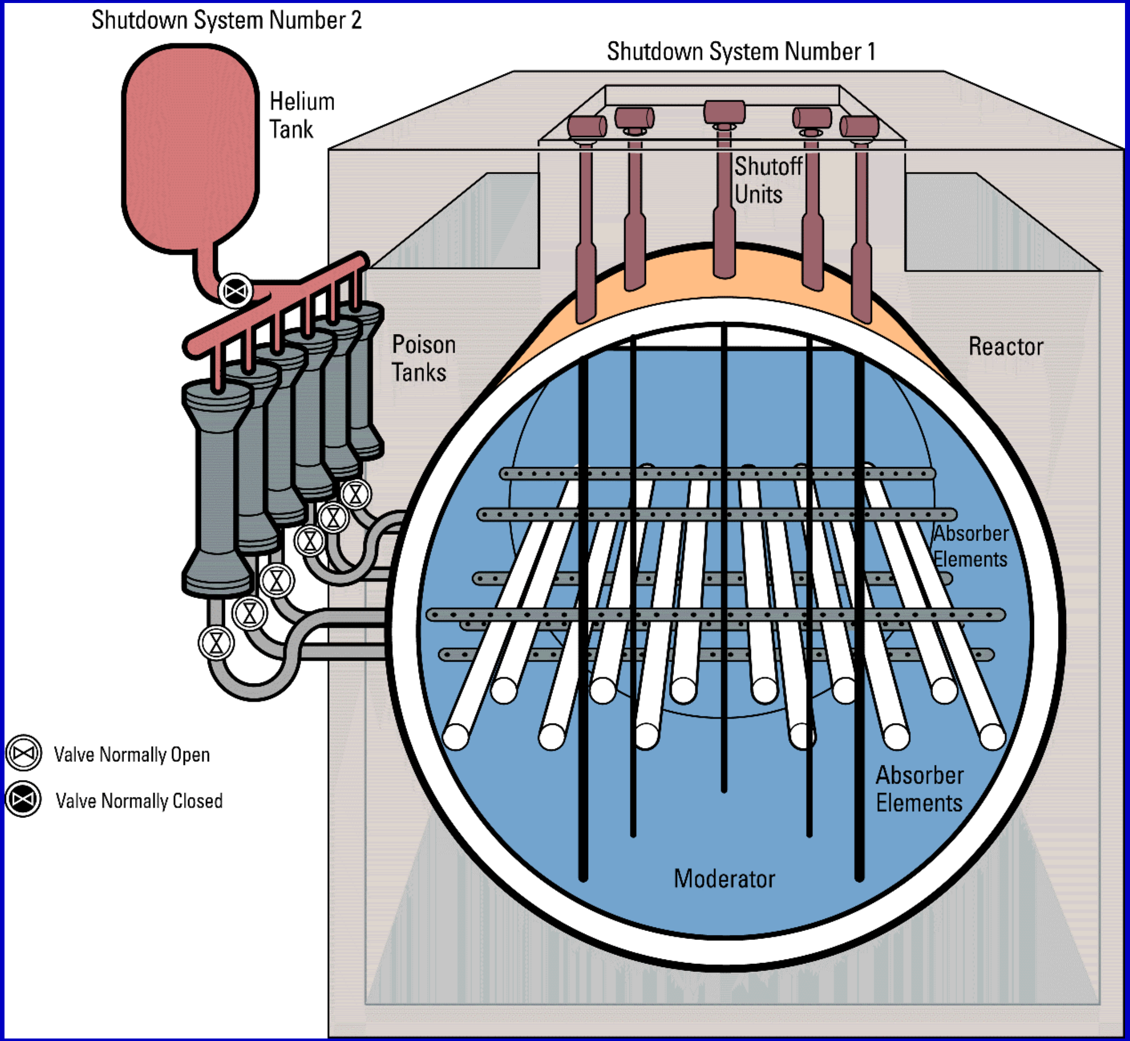
Shutdown System 1

- 28 spring-assisted gravity-drop absorber elements
- poised above core
- supported by cable
- held against spring by clutch; loss of power to clutch causes rods to fall into moderator
- guide tubes guide the absorbers as they fall in
- full insertion in < 2 seconds



Shutdown System #2

- 6 perforated nozzles run horizontally across the moderator
- each nozzle is connected to a liquid tank full of $GdNO_3$
- a high-pressure helium tank forces the "poison" into the moderator in < 2 sec.



Performance Requirements

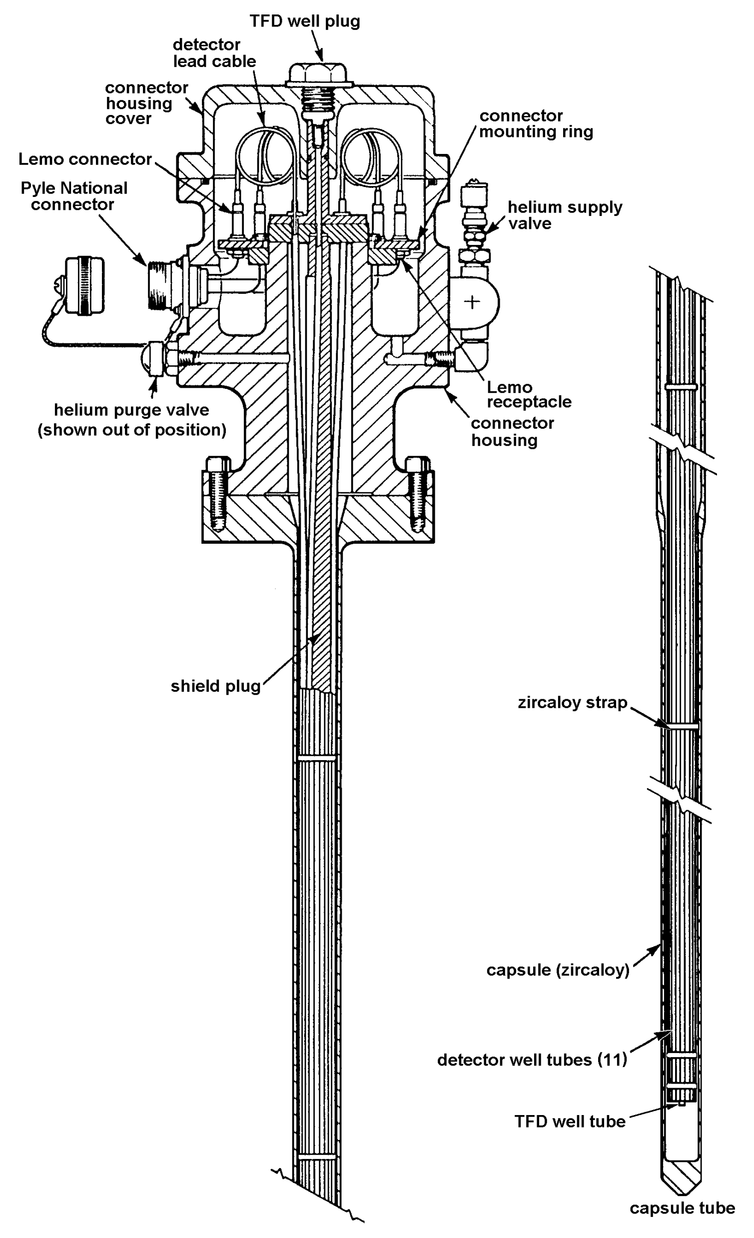
- insertion speed and initial negative reactivity
  - set by the large LOCA
  - turn over the power increase before the fuel or sheath melts
  - significant negative reactivity within 0.6 seconds of trip
- reactivity depth
  - set by a fuel channel rupture (in-core break) on startup after a long shutdown
  - moderator contains boron / gadolinium and after rupture is displaced by “unpoisoned” coolant
  - some shutoff rod guide tubes may be damaged

Reactivity Balance for In-Core Break

Reactivity Change Due to:	*Reactivity (mk) at 15 minutes*
Moderator poison displacement	10.5
Coolant void	13.3
Coolant Temperature	0.3
Fuel Temperature	4.1
Downgrading Moderator Purity	-4.8
Moderator Temperature	-0.1
Total to be compensated by shutdown	23.3

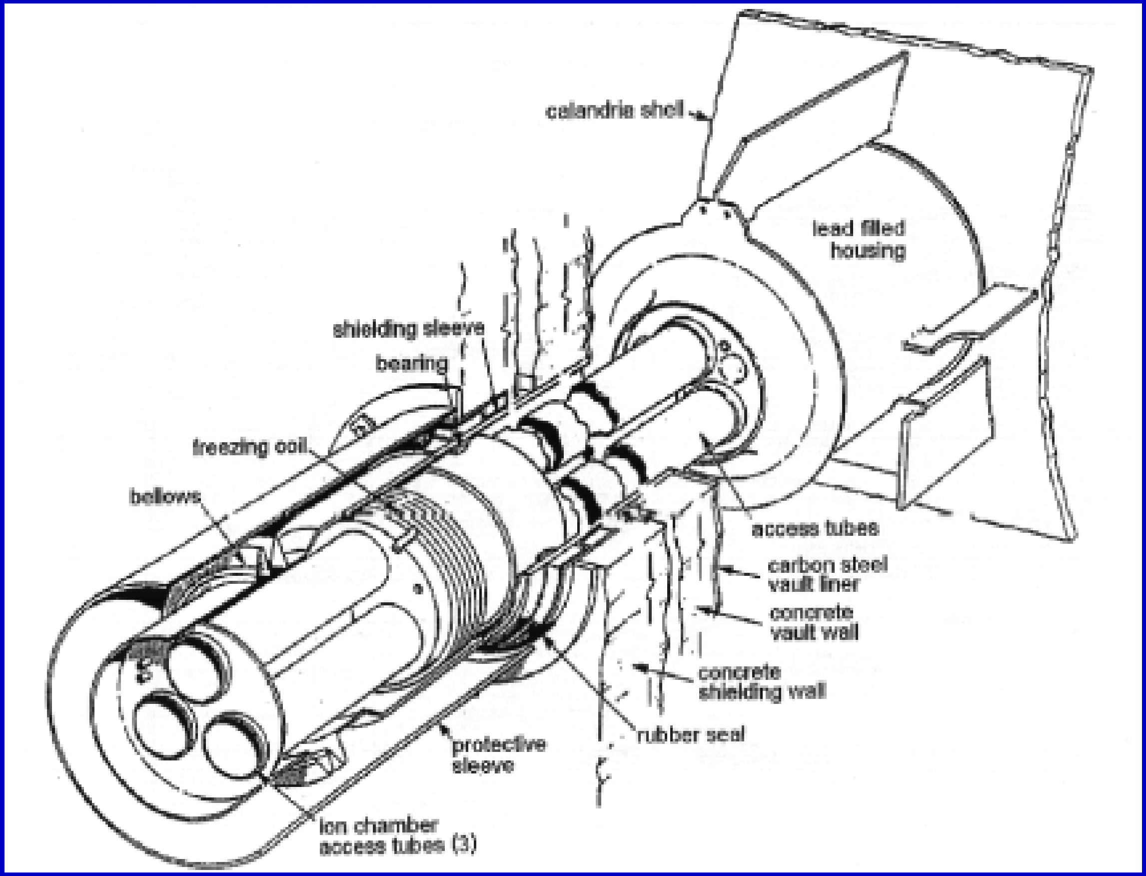
Flux Detectors

- SDS1 uses vertical self-powered fast-response platinum flux detectors in core
- they are not shared with the control system nor with SDS2
- they are used for local overpower protection and for bulk overpower
- SDS2 uses separate horizontal in-core detectors



Ion Chambers

- SDS1 and SDS2 use (separate) ion chambers on the side of the core
- the main purpose is to generate a low-level power signal and a high-rate signal



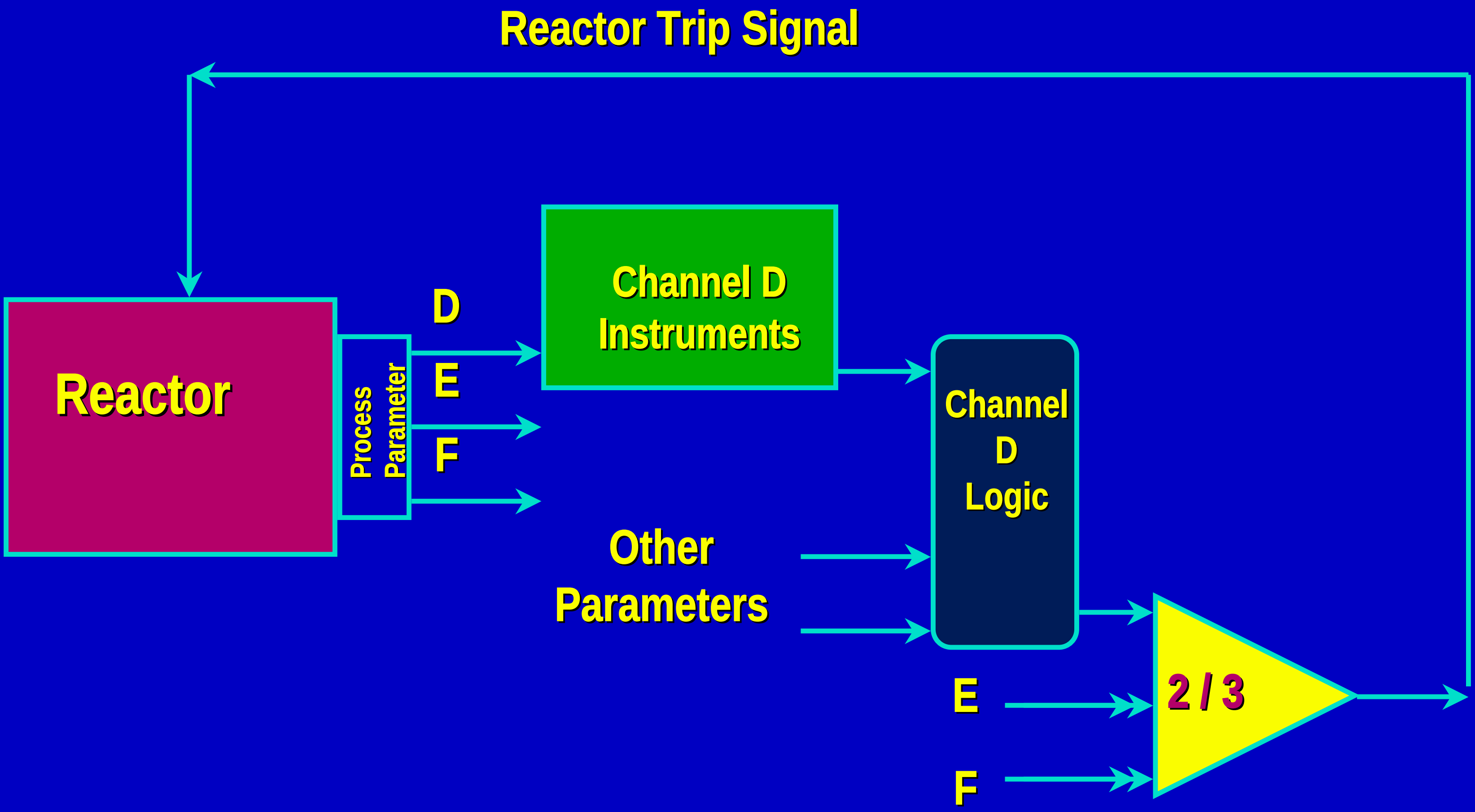
Typical SDS1 Trip Parameters

Parameter	*Purpose - examples*
High Neutron Power	**Loss of reactivity control, LOCA**
High Rate of Rise of Neutron Power	**LOCA, loss of reactivity control from low power**
High Coolant Pressure	**Loss of flow, loss of heat sink**
Low Coolant Pressure	**Small LOCA**
High Building Pressure	**LOCA, steam line break**
Low Steam Generator Level	**Steam and feedwater line breaks**
Low Pressurizer Level	**Small LOCA**
High Moderator Temperature	**Loss of service water**
Low Coolant Flow	**Loss of flow**
Low Steam Generator Pressure	**Steam line break**

Typical SDS2 Trip Parameters

Parameter	*Purpose - examples*
High Neutron Power	**Loss of reactivity control, LOCA**
High Rate of Rise of Neutron Power	**LOCA, loss of reactivity control from low power**
High Coolant Pressure	**Loss of flow, loss of heat sink**
Low Coolant Pressure	**Small LOCA**
High Building Pressure	**LOCA, steam line break**
Low Steam Generator Level	**Steam and feedwater line breaks**
Low Pressurizer Level	**Small LOCA**
Low Header Δp	**Loss of flow**
Low Steam Generator Pressure	**Steam line break**

SDS1 Two- Out-of-Three Logic



2 out of 3 Logic

- allows one channel to be tested without tripping the reactor
- allows one channel, if it is known to be faulty, to be put in a safe (tripped) state without tripping the reactor
- permits comparison of the three signals and alerts the operator if any seem inconsistent

Shutdown System Design Requirements

- each shutdown system is effective for all accidents
- they do not share sensing, logic or actuation devices with each other or with the reactor control system
- the design of the two shutdown systems is diverse
  - solid absorber rods and liquid poison injection
  - logic microprocessors programmed by different groups of people in different languages
- where practical, each shutdown system has two diverse trip parameters which are effective for each accident
- in a few cases SDS1 and SDS2 trips are diverse
  - e.g., low flow and low Δp

Shutdown System Design Requirements - More

- the two shutdown systems are oriented differently
  - vertical rods and horizontal nozzles, also for flux detectors
- the cables and instrumentation are physically separated
- each SDS is controlled from a different control room
- each SDS is designed to meet an unavailability of 1 in 1000
- each SDS is tested during operation to show that this unavailability is met:
  - each channel is testable up to the final 2 / 3 logic
  - any shutoff rod can be partially dropped
  - any poison valve can be opened without firing SDS2

Shutdown System Design Requirements - More

- most process parameters are directly testable: e.g., a shutter can be moved in an ion chamber to test the log rate trip for that channel
- the systems are fail safe as far as possible:
  - loss of power to clutches or poison valves trips the system
  - loss of power to a channel trips the channel
  - loss of power supply trips the channel
  - watchdog timers trip the channel if the logic is not routinely operating
- the operator cannot easily prevent tripping the systems nor change the logic

Lesson Learned from Chernobyl

- the shutdown systems in Chernobyl were adequate according to the safety analysis
- the designers assumed the operator would not operate the plant in an unusual configuration
- he did, and the shutdown systems made the accident worse
- in CANDU:
  - the reactor state does not change much once equilibrium fuelling is reached
  - the shutdown system effectiveness does not depend much on reactor state

Summary

- CANDU Shutdown Systems are:
  - effective, acting alone; therefore they are fully redundant
  - diverse in design
  - designed to numerical reliability target
  - testable during operation to show the reliability target is met
  - separated so that a hazard in a local area will not affect both systems