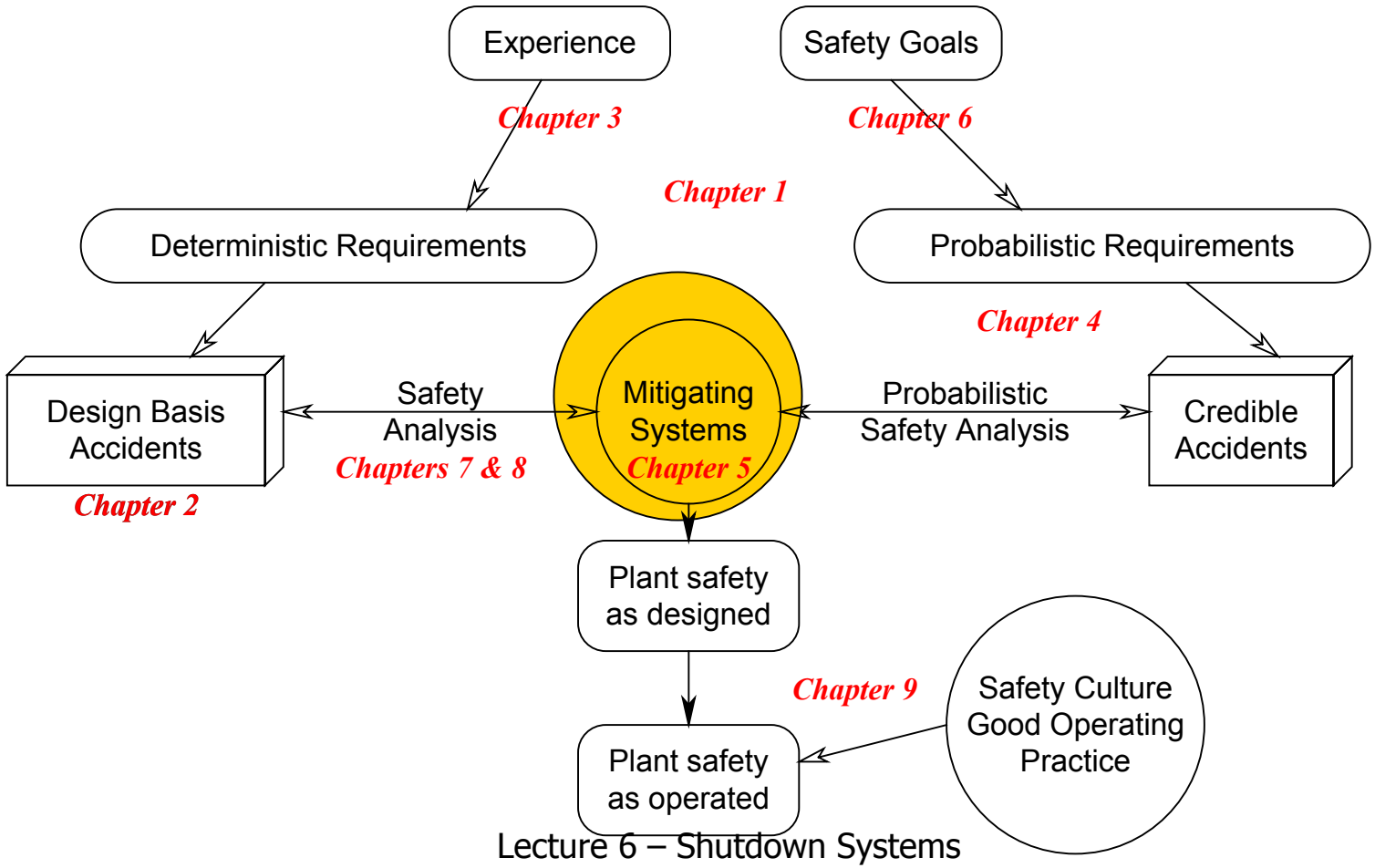
Lecture 6 – Shutdown Systems

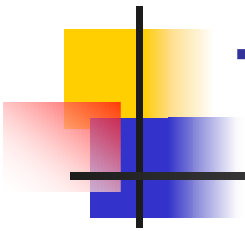
Dr. V.G. Snell
Nuclear Reactor Safety Course
McMaster University

Where We Are...


Experience
Safety Goals
Chapter 3
Chapter 6
Chapter 1
Deterministic Requirements
Probabilistic Requirements
Chapter 4
Design Basis Accidents
Chapter 2
Safety Analysis
Chapters 7 & 8
Mitigating Systems
Chapter 5
Probabilistic Safety Analysis
Credible Accidents
Plant safety as designed
Chapter 9
Safety Culture Good Operating Practice
Plant safety as operated

Why Shutdown?

- So that in an accident the remaining systems have to deal only with decay heat



Topics

- How do we insert negative reactivity?
- How fast?
- How much?
- How reliable?
- What is good enough performance?
- How is it started?
- What environment must it work in?
- Common mode susceptibilities?
- How do we know it will really work?
- How does the operator know it worked?

How is –ve Reactivity Put In??

- Multiple "rods"
- Trip of recirculation pump in BWRs
- Boron dust, balls for GCRs
- Moderator Dump
- Reflector Dump
- Poison Injection
- Inherent shutdown – how?

CANDU Shutdown Systems

'Fail-safe' is an ideal – how close do these systems come?

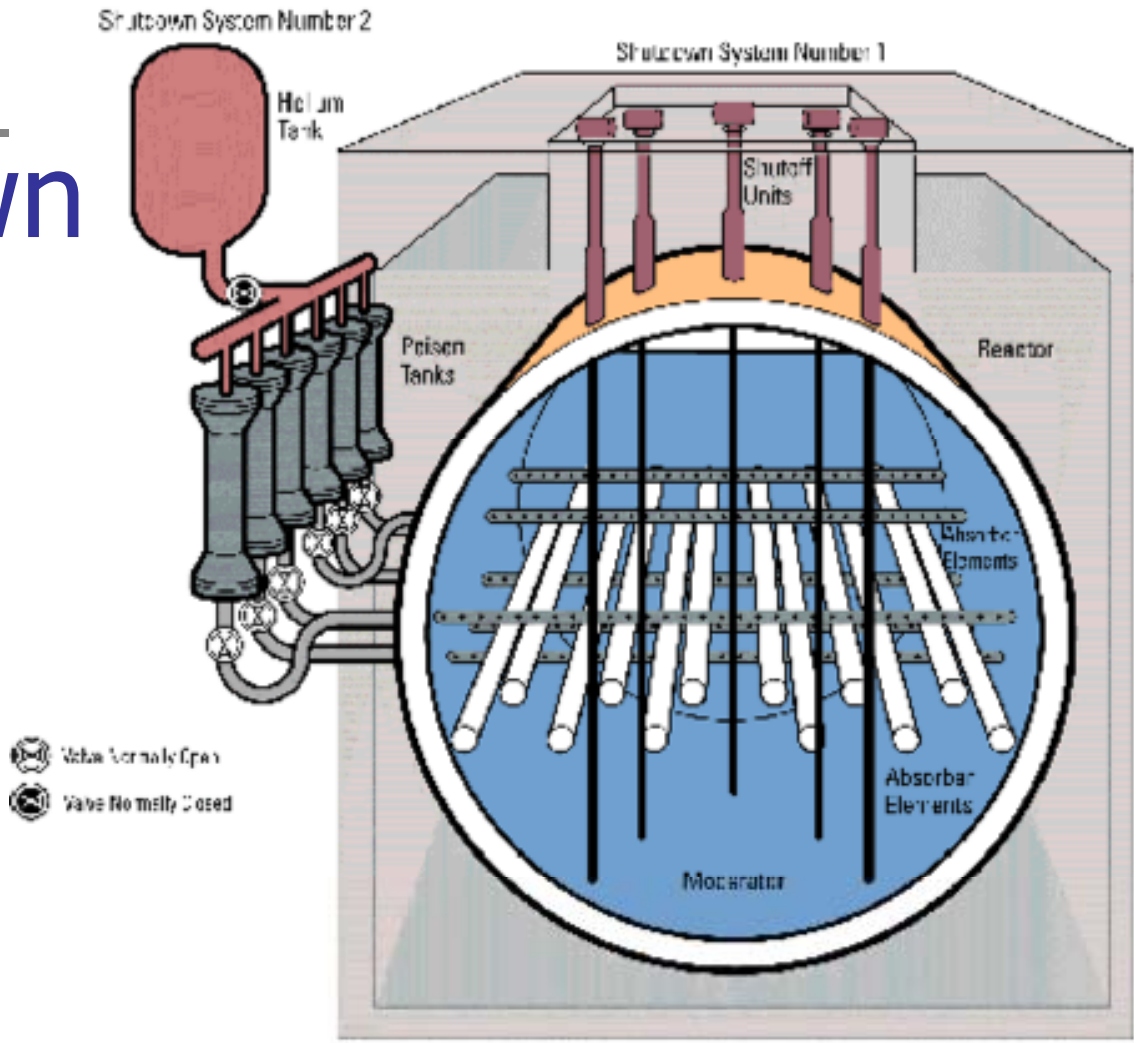
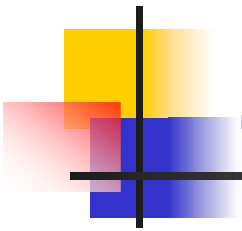


Figure 5-1 - Shutdown Systems #1 and #2



Speed

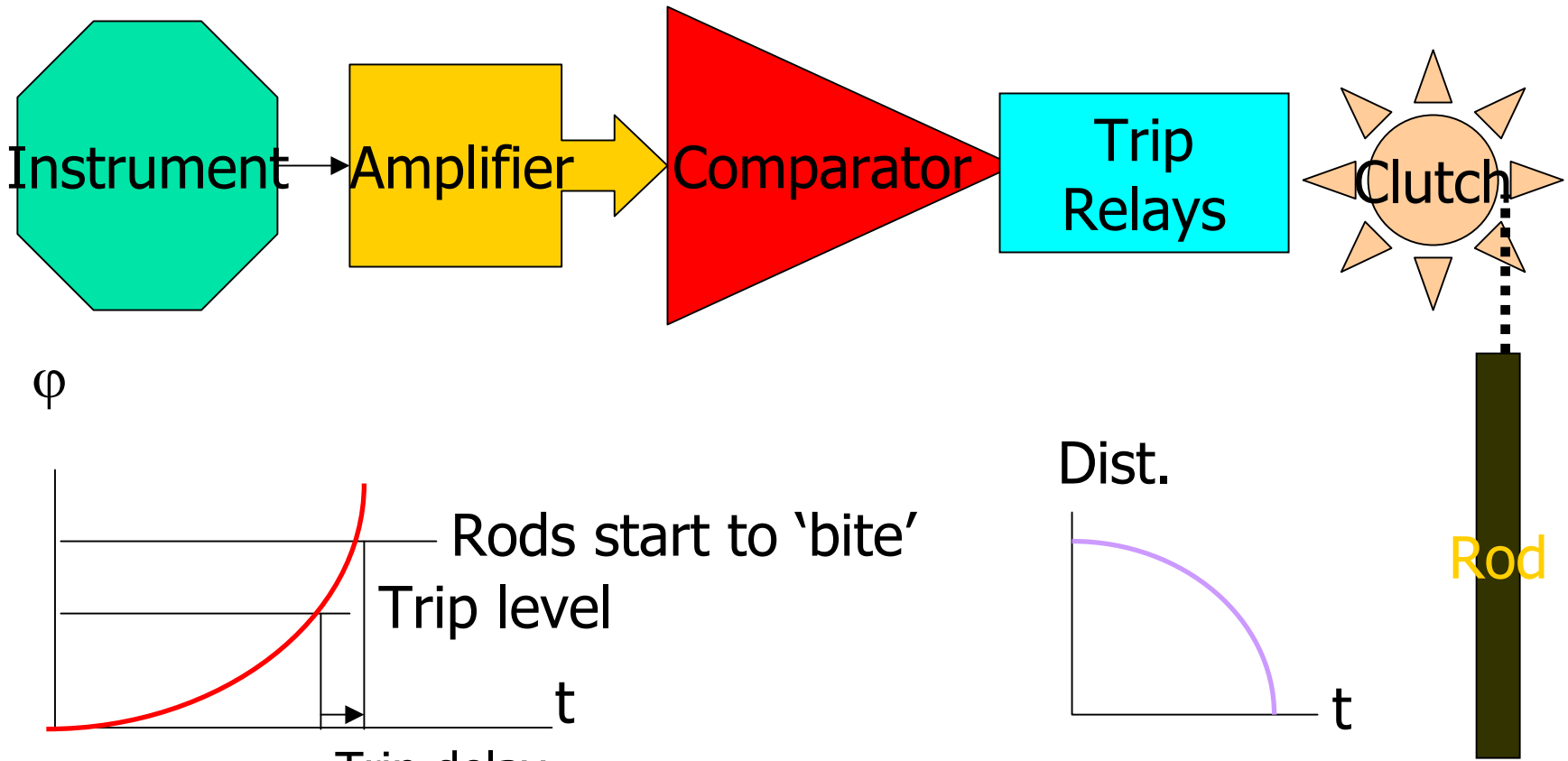
- How fast is the first 'bite'?
  - Large LOCA, +4 mk/s
  - Prevent fuel melting $\rightarrow$ bite in ~1sec. & turnover by ~1.5 sec.
  - i.e., 10s of mk/sec. negative
- What signal is fast enough?
  - Neutron flux, log rate
  - Others?

All sorts of delays

Time of "bite" =

+ time of large break
+ time for signal to rise to trip set-point
+ response time of detector and amplifiers
+ response time of instrumentation which decides if a signal has passed its set-point
+ response time of trip relay chain
+ time to release clutch holding shutoff rod in place
+ time to accelerate shutoff rod from parked position to about the first row of fuel channels

Typical Trip Chain



Reactivity Depth

Xenon Decay

$$^{135}\text{Te} \Rightarrow_{<1\text{min}} \Rightarrow {}^{135}\text{I} \Rightarrow_{6.7\text{h}} \Rightarrow {}^{135}\text{Xe} \Rightarrow_{9.2\text{h}} \Rightarrow {}^{135}\text{Cs} \Rightarrow {}^{135}\text{Ba (stable)}$$

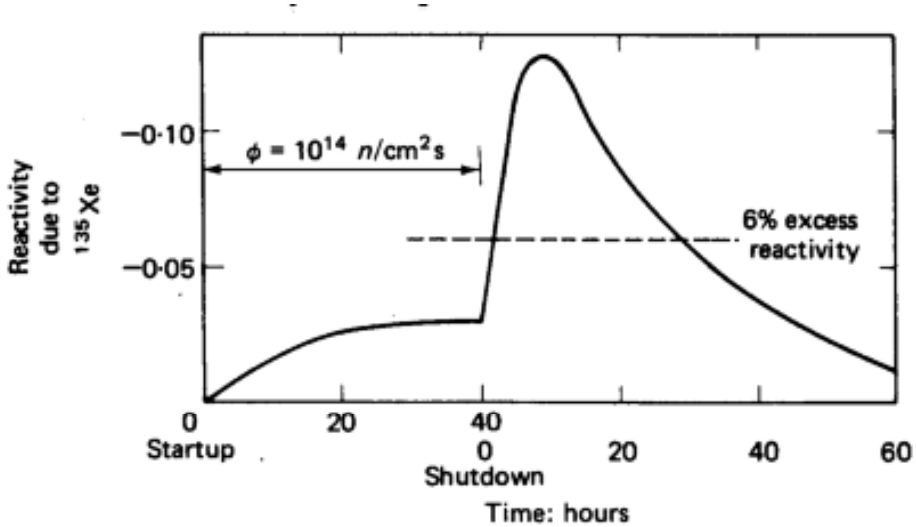


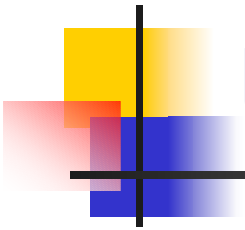
Figure 5-2 - Xenon Reactivity (negative) versus Reactor Power History

Reactivity Depth for CANDU Classic

- Small in-core break with poisoned moderator - positive reactivity from:
  - Coolant voiding
  - Fuel temperature
  - Displacement of poisoned moderator by clean coolant
  - Moderator temperature
  - Xenon decay
- Damage to shutoff rods in core
- Versus: shutdown system, ECC
- Shutdown depth vs. shutdown margin

Speed & Depth – Negative Void Coefficient

- What are the trip signals for large LOCA?
- What sets the reactivity depth?



Unavailability

- Requirement: demand unavailability of 10^{-3} years/year (8 hours/year)
- With two shutdown systems, can we claim 10^{-6} unavailability?
- What does the rest of the world do?

Accident Categorization

Name	Definition	Example	Typical Frequency
Anticipated Operational Occurrence (AOO)	Expected to occur once or more during plant lifetime	Loss of offsite power	$>10^{-2}$ /year
Design Basis Accident (DBA)	Basis of design of safety systems	Small LOCA, large LOCA	10^{-2} to 10^{-5} / year
Beyond Design Basis Accident (BDBA)	Rare accident more severe than DBA	LOCA + LOECC	$< 10^{-5}$ / year
Severe core damage accident	Loss of core structure	LOCA + LOECC + loss of moderator heat removal	$<10^{-6}$ / year

Acceptance Criteria

- AOOs: re-use of fuel
- More frequent DBAs: no fuel sheath failures
  - Exceptions?
- All DBAs:
  - No further risk to pressure boundary
  - Coolable fuel geometry
  - Adequate time for operator action
  - No damage to containment or other safety systems etc. etc.

Trip Signals - 1

Accident	Symptoms	Typical Trip Signals
Loss of reactor power control	Reactor power rises Reactor power rises rapidly Heat transport system pressure rises	High neutron flux High log rate of neutron flux High heat transport system pressure
Loss of forced circulation	Coolant flow drops Pressure rises Reactor power rises[1]	Low heat transport system flow / low core pressure drop High heat transport system pressure High neutron flux
Large loss of coolant	Reactor power rises Reactor power rises rapidly Containment pressure rises Coolant flow drops Coolant pressure drops	High neutron flux High log rate of neutron flux High containment pressure Low heat transport system flow Low coolant pressure

Trip Signals – 2

Small loss of coolant	Pressurizer level drops Coolant flow drops Containment pressure rises Moderator level rises[1] Coolant pressure drops	Low pressurizer level Low heat transport system flow High containment pressure High moderator level Low coolant pressure
Loss of feedwater	Boiler level drops Feedwater flow drops Heat transport system pressure rises	Low boiler level Low feedwater flow High heat transport system pressure

Trip Signal Requirements

- Historically and ideally, two diverse trip signals on each shutdown system for each accident
  - Little safety improvement from second trip
  - Dropped in RD-337 for direct trip
- To credit operator action:
  - 15 minutes from first clear signal (MCR)
  - More detailed models in PSA
  - Modern reactors: 8 hours or more for DBA

Operating Environment

- Design the system to withstand the conditions of the event it is supposed to mitigate
- Exceptions
  - e.g., fire in the MCR
- Separation / barriers

Protection of Shutdown Systems

- Devices themselves in moderator
  - In-core break
- No high-energy pipes in striking range of R/M deck
- Fire separation / barriers
- Steam, high-temperature, radiation fields, flood, seismic
- Limited mission time

Common-Cause Failures

- Two group philosophy
  - At least two ways of performing each safety function
  - Geometric separation
  - Barriers
  - Diversity if possible & practical
  - Environmental protection
  - Qualification

What to Separate?

- Each safety system has three logic channels + power supplies (2 or 4 channels)
- The control system has 2 logic channels and 2 power channels
- Many safety support systems have 2 logic and 2 power channels
- Not practical to separate them all

If separation is impractical…

- Ensure there is no credible hazard in area
- Another Group 2 system outside the area will mitigate the event
- System or component is protected by barrier
- System or component is fail safe
- Component is designed to withstand the hazard

CANDU 6 Grouping

Safety Function	Group 1	Group 2
Shutdown	Reactor Control System Shutdown System 1	Shutdown System 2
Heat Removal From Fuel	Heat Transport System Steam & Feedwater Systems Shutdown Cooling System ECC Moderator	Emergency Water System
Contain Radioactivity	Reactor building air coolers	Containment & containment subsystems
Monitoring & Control	Main Control Centre	Secondary Control Area

CANDU 6 Safety Support

Safety Support Function	Group 1 Safety Support	Group 2 Safety Support
Electrical Power	Class IV	Emergency Power System
	Class III diesels	Diesels
	Class II	Class II
	Class I	Class I
Service Water	Raw Service Water	Emergency Water System
	Recirculating Service Water	
Instrument Air	Instrument Air System	Local Air Tanks

Cable Routing

System Group	System Name	Channel		
1	Reactor Regulating System	A	B	C
1	Shutdown System 1	D	E	F
1	Emergency Core Cooling System	K	L	M
2	Shutdown System 2	G	H	J
2	Containment System	N	P	Q
1	Emergency Core Cooling System - Seismically Qualified	KK	LL	MM

Example – CANDU 6

- Single channels within a group can share routing
- Triplicated channels separated
- Power cables separated
- Only Group 2 seismically qualified

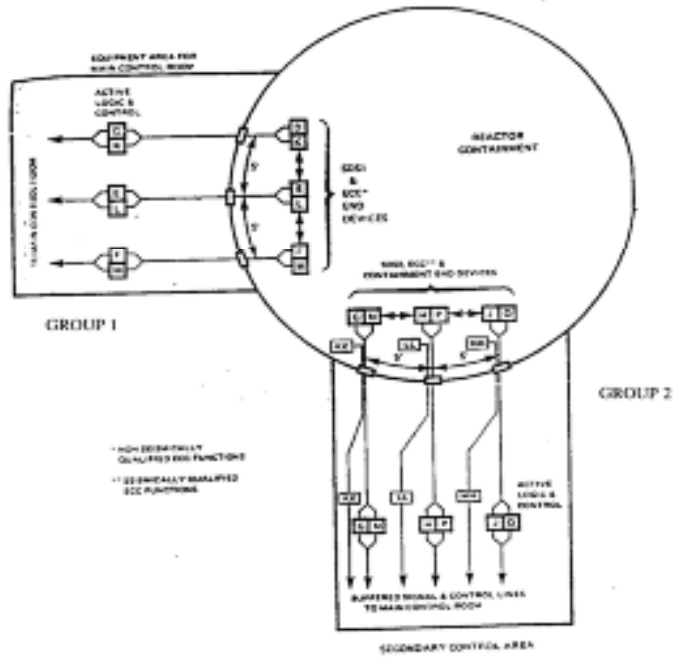
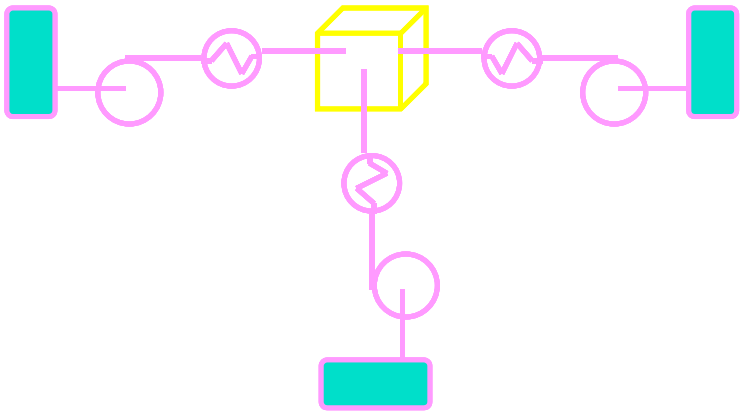


Figure 3 Location and Separation Requirements for Safety Related Systems

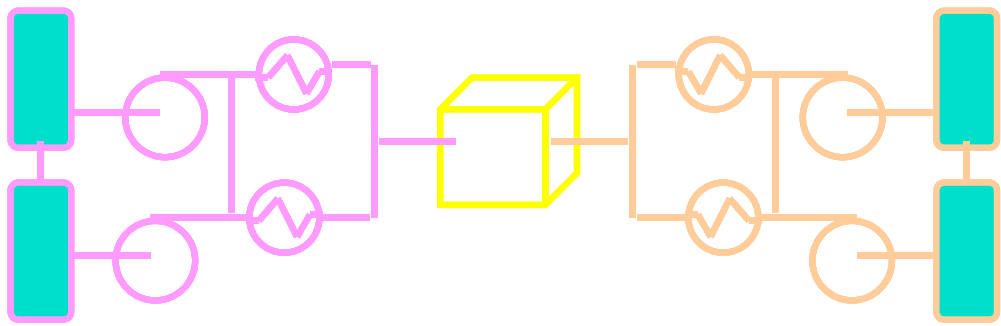
Figure 5-3 - Grouping and Separation for Safety-Related Systems

LWR vs. CANDU Classic



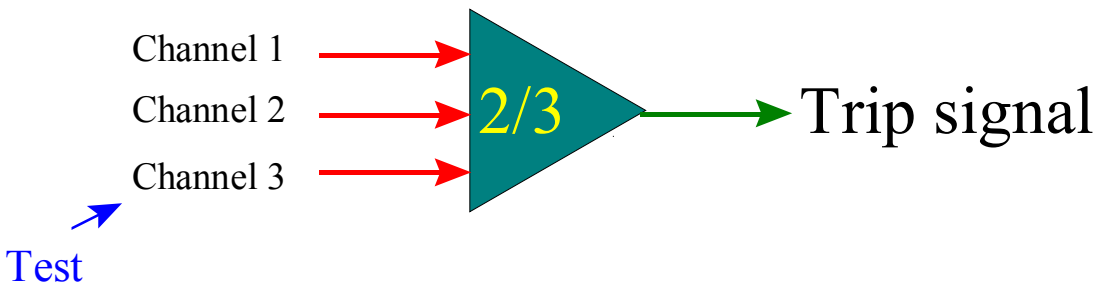
LWR – multiple trains,
Each single failure-proof

CANDU Classic –
cross-connected
components



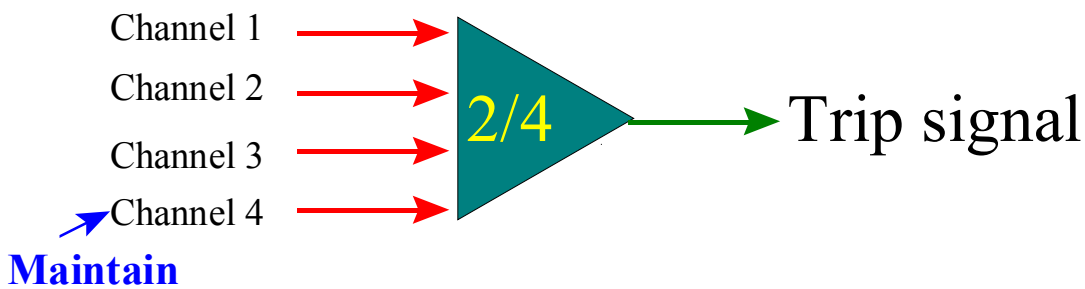
Testing

- 2/3 logic for test & reliability
- Test hardware devices separately
- Performance testing (valve opening times, rod drop through 'gates')

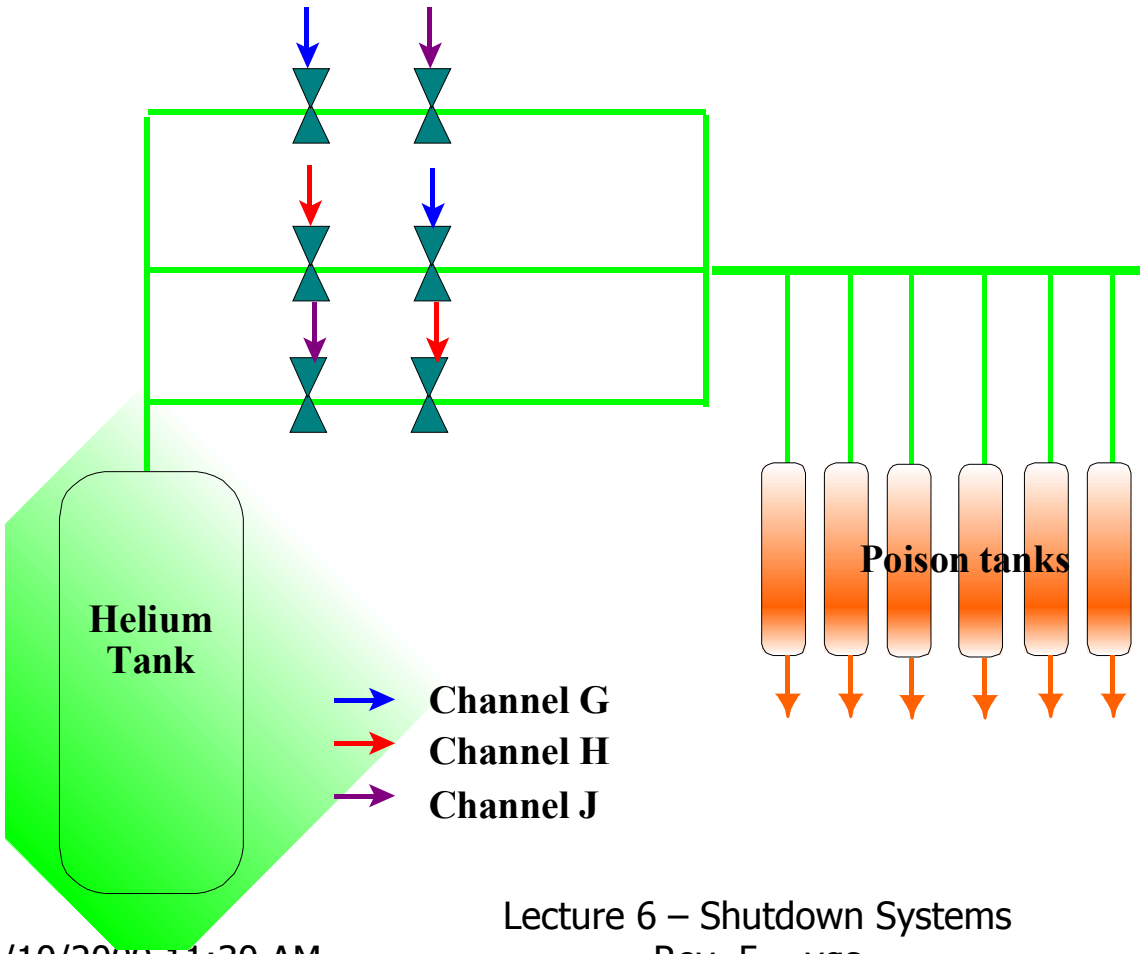


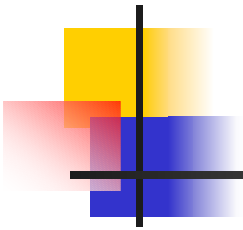
Four trains - ACR

- 2/4 logic
- One train can be taken out for maintenance without tripping it



Valve Testing





Human Interface

Operator must:

- Know that the shutdown system has tripped
  - Direct vs. indirect
- Confirm that it has actuated correctly
- Have procedures to follow in case it has not