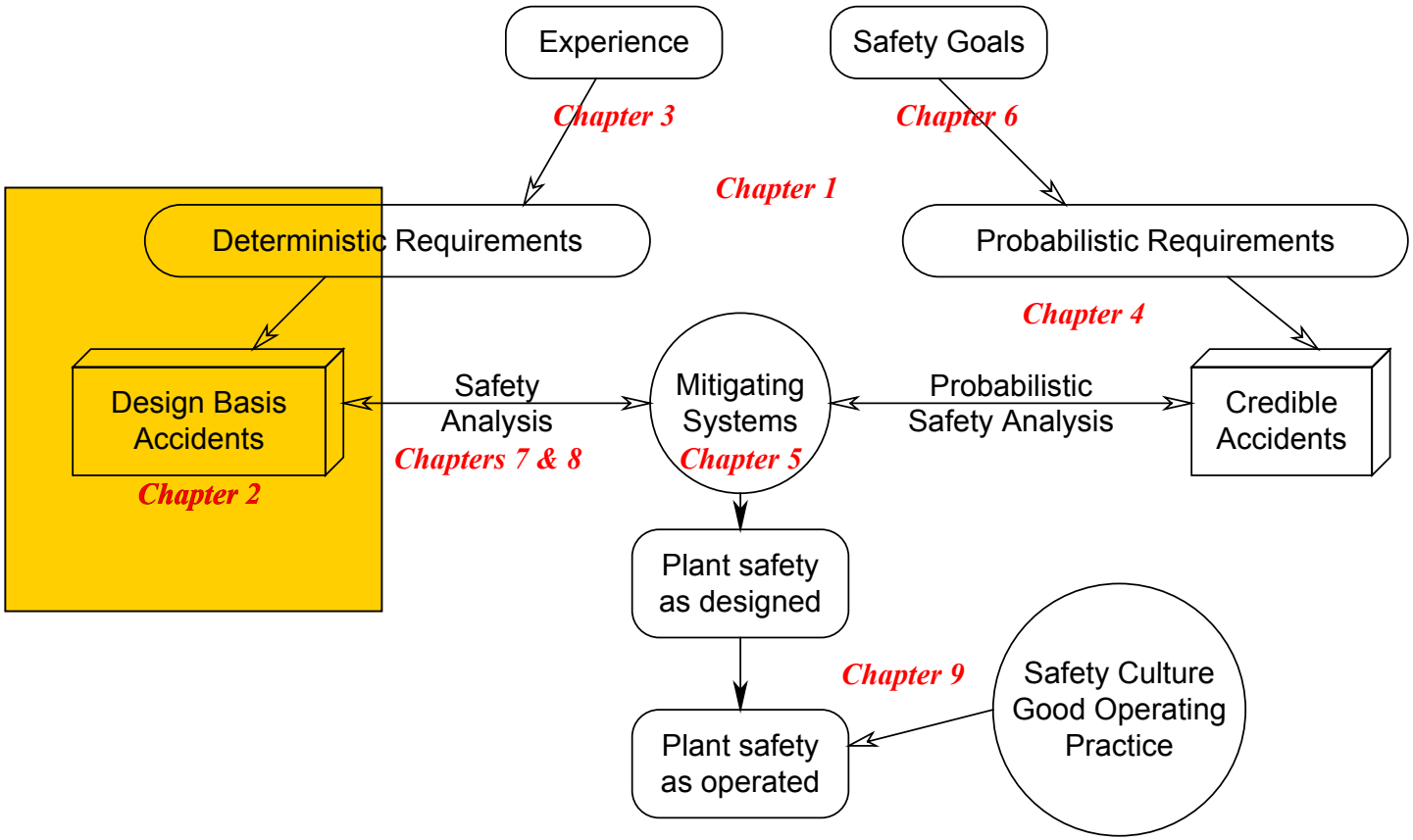
Lecture 2 - Design Basis Accidents

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

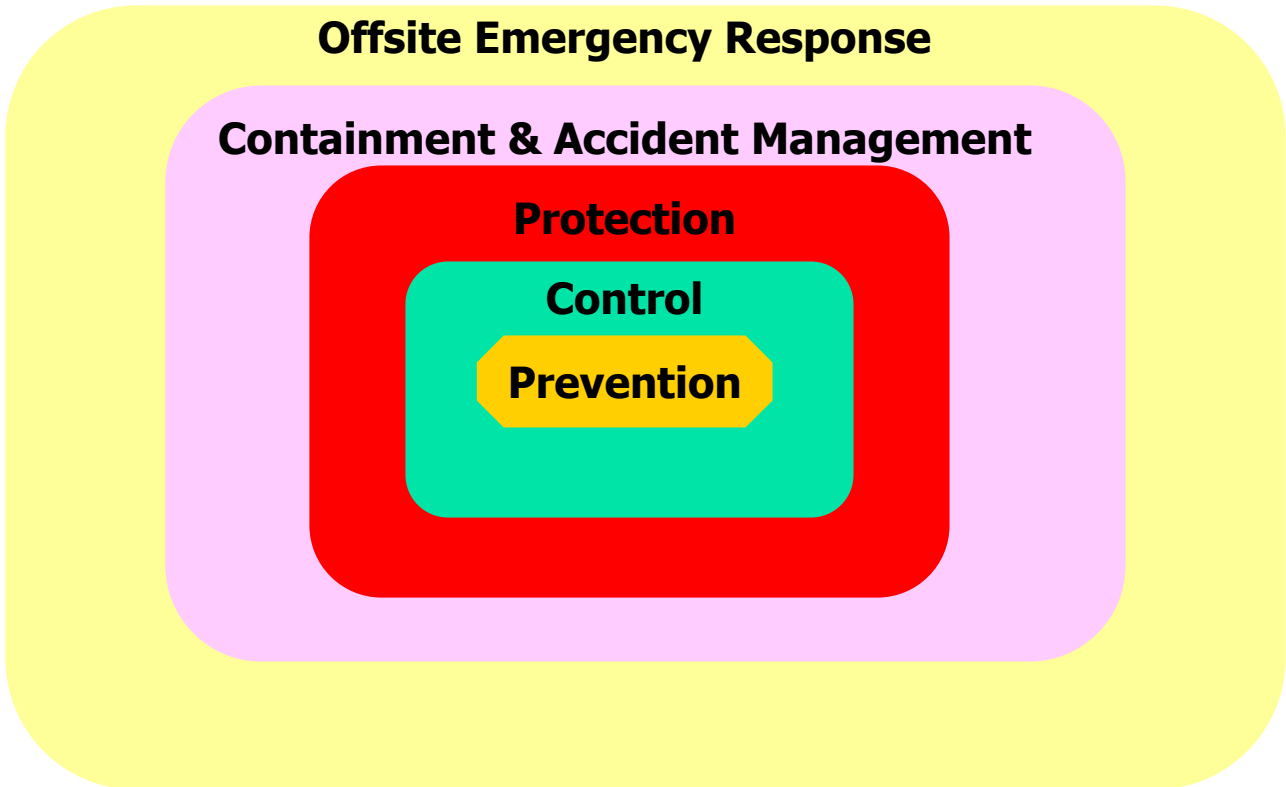
How do you get them all?

- Whose job is it to make the list?
- Deterministic Analysis
- Probabilistic Analysis
- Rule or standard
  - Pressure vessels?
- Use them all!

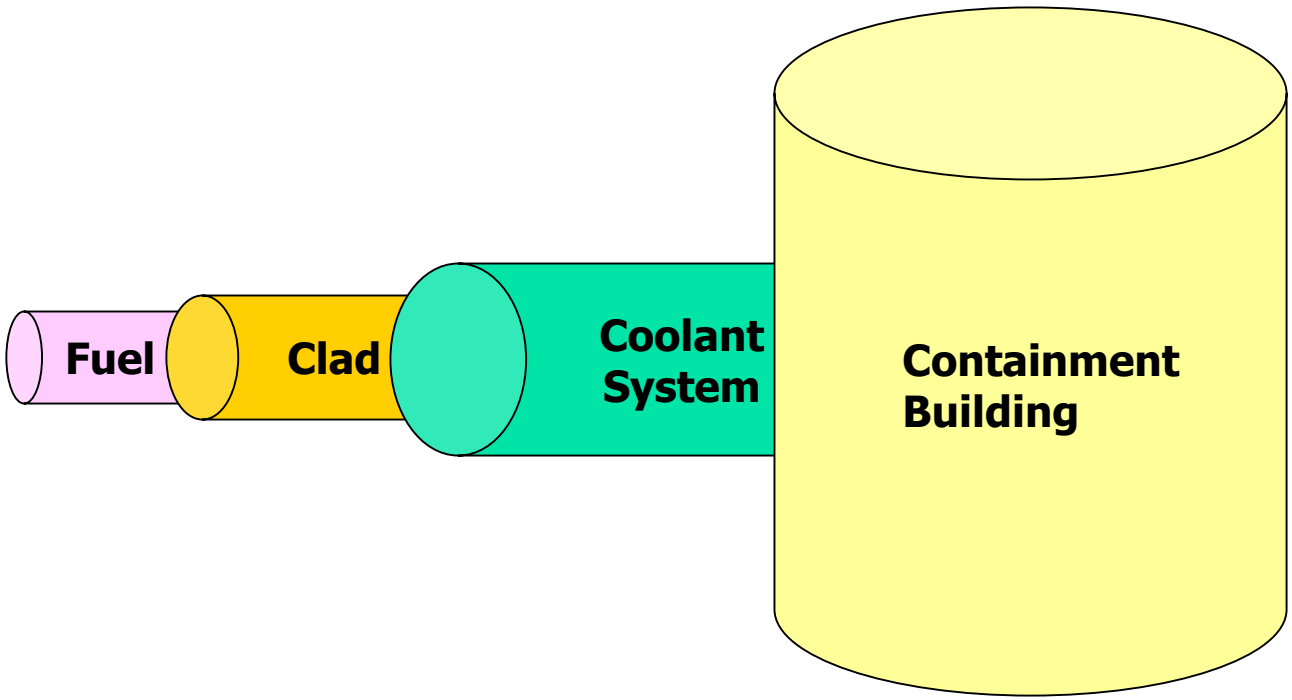
Defence-in-Depth – One View

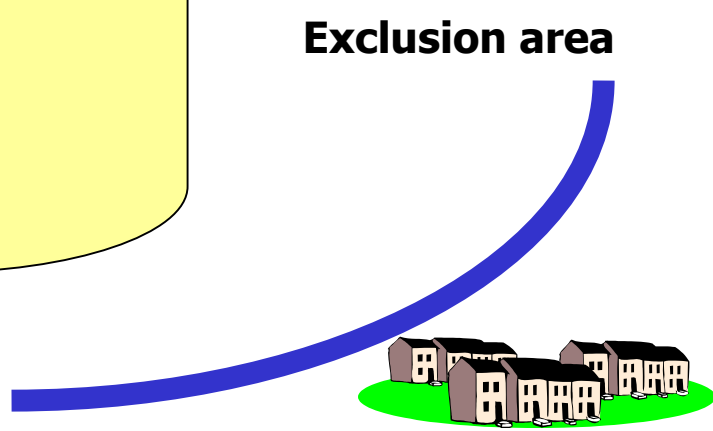
Level	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Defence in Depth – One View

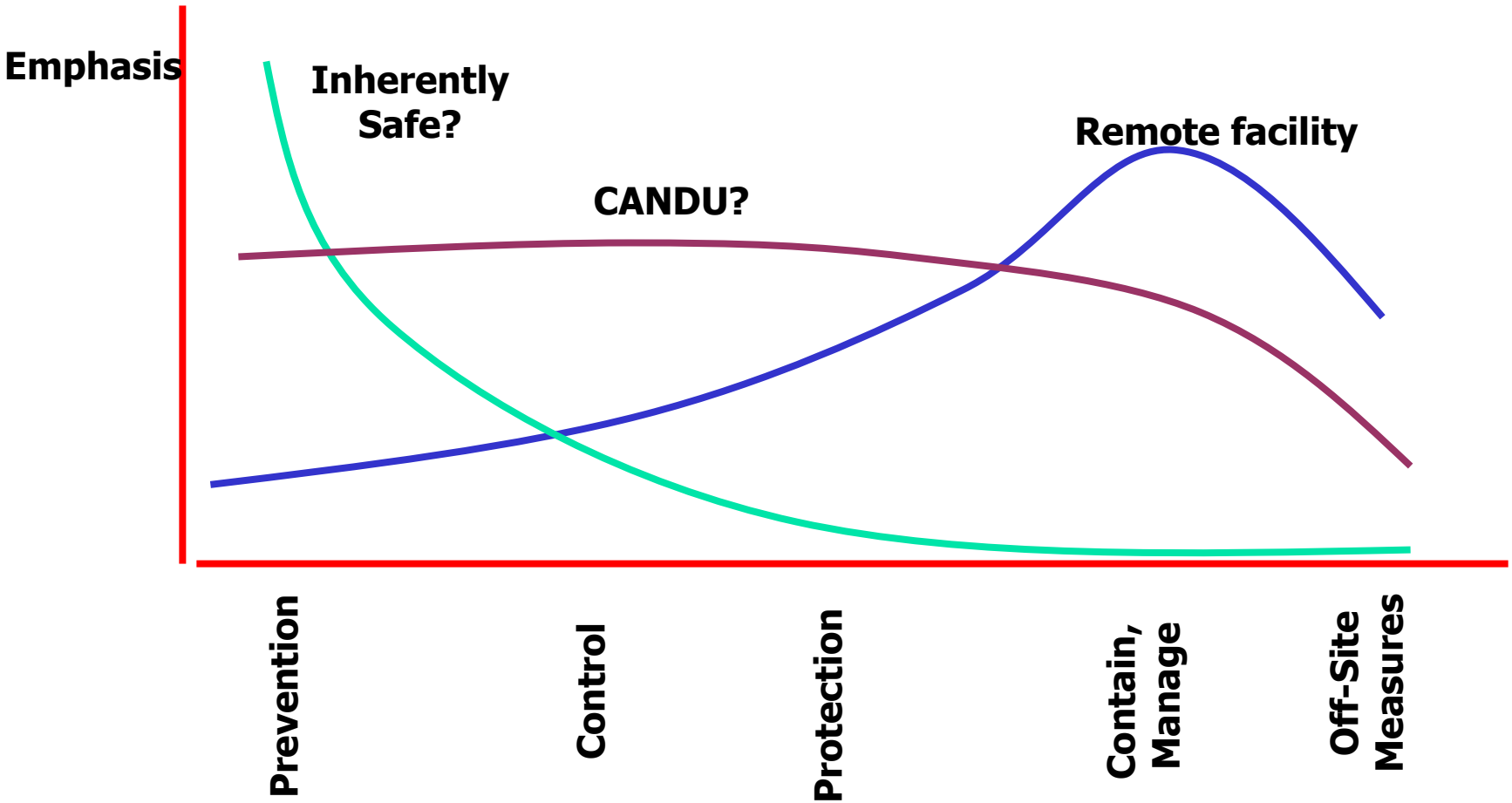


Physical Barriers – Another View





Design Approaches to D-in-D

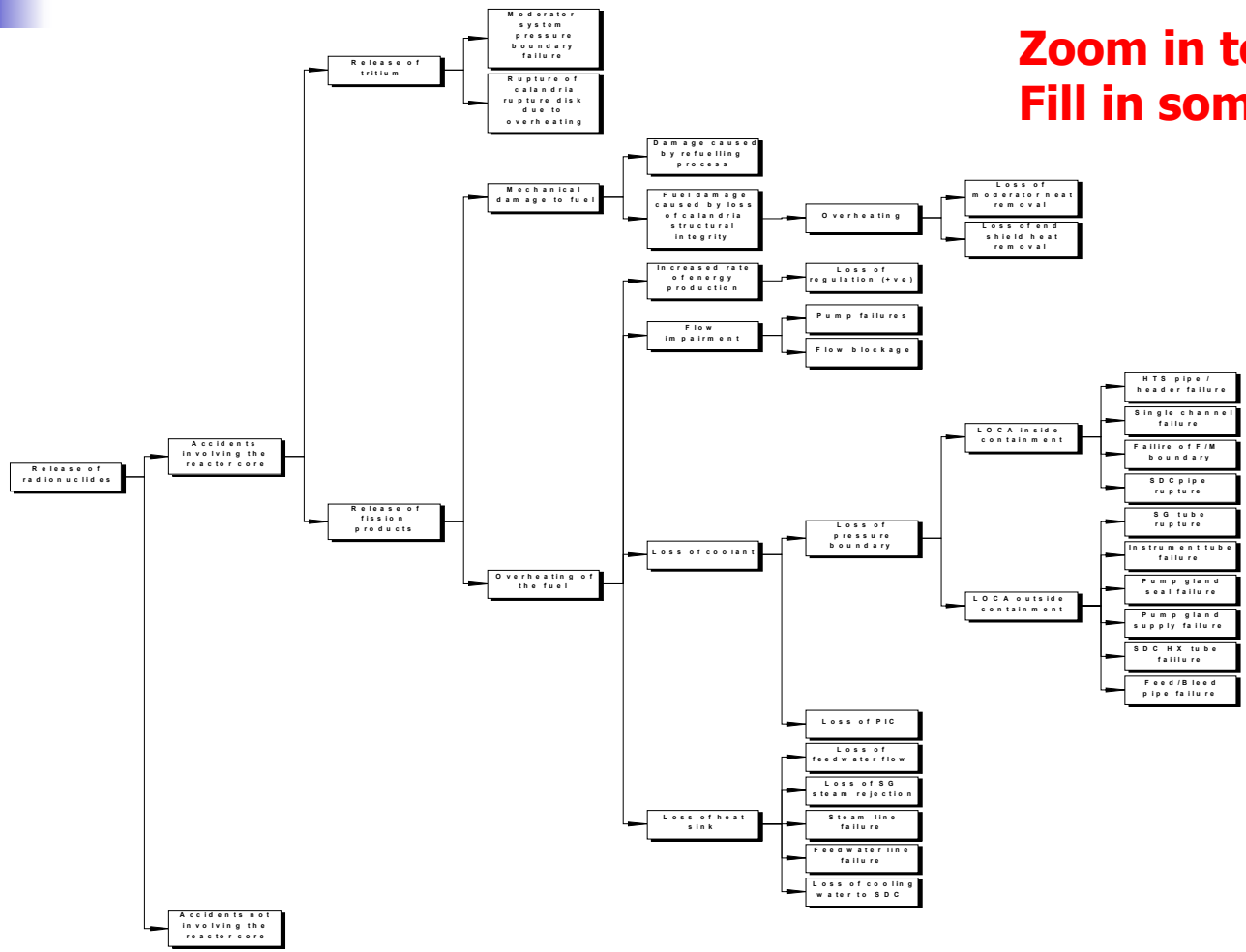


Accidents Lists - Top Down

- Use principle of immediate cause
- Start from what you want to avoid

Reactor - Top Down

Zoom in to view
Fill in some missing steps

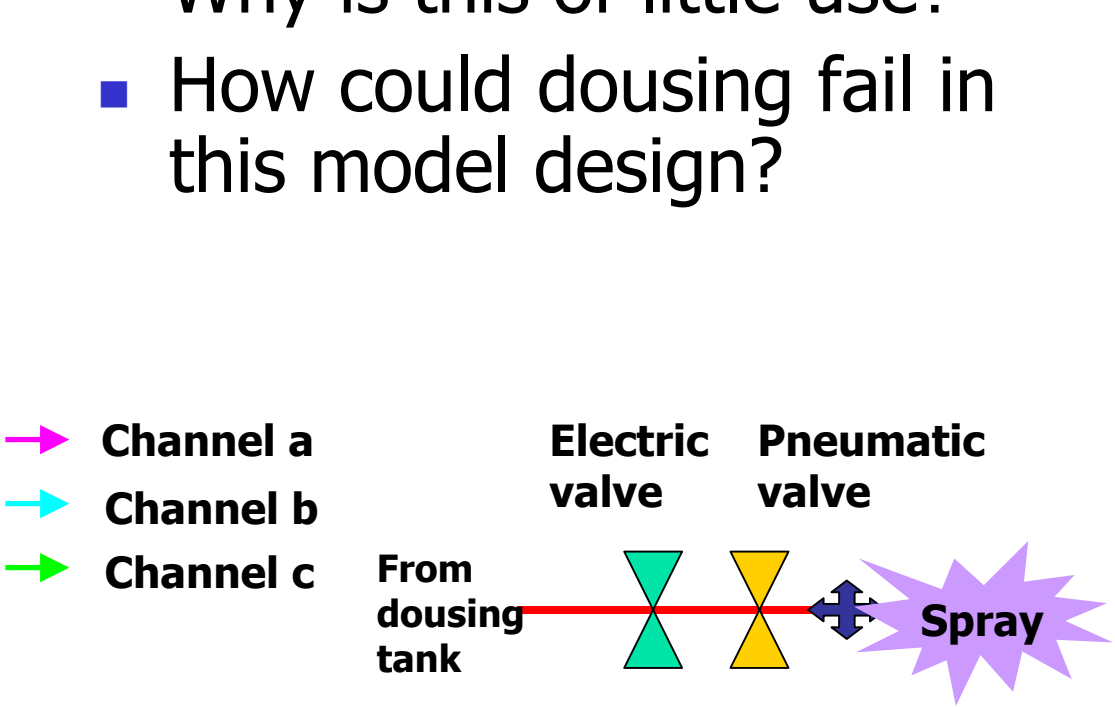


Accidents Lists - Bottom Up

- Look at failure of each component or system in turn

Reactor – Bottom Up Example

- FMEA – just one level. Why is this of little use?
- How could dousing fail in this model design?



External Hazards

- Fire, flood, earthquake, tsunami
- Explosions
- Can affect more than one system at a time
- Site dependent
- Sabotage, terrorism, war
  - To what extent can the plant be protected?

Canadian Safety Philosophy

- NRX – need robust & independent shutdown systems
- Siddall – 1959
  - Nuclear 5 x safer than coal
  - Catastrophic accident versus mining
  - Target: < 0.2 deaths/year on average

Siddall's Safety Goals

LOSS OF COOLANT	**One in 50 years**
LOSS OF POWER CONTROL	**One in 16 to one in 160 years, depending on severity**
SHUTDOWN SYSTEM UNAVAILABILITY	**One in 500 tries**

Laurence (1961)

- **Safety goal:** 10^{-2} deaths per year from nuclear power plant accidents
- Disastrous accident < 1000 early deaths
- Frequency of disasters < 10^{-5} / yr
- Failure of process system

  + Unavailability of shutdown

  + Failure of containment

What is the weakness in this approach?

Laurence's Design Targets

Process failures	**One in 10 years**
Protective System Unavailability	**One in 100 demands**
Containment System Unavailability	**One in 100 demands**

Must be observable!!

Douglas Point Safety Goal

- Risk of death to individual member of public < 10^{-6} per year
- Risk of injury to individual member of public < 10^{-5} per year
- Effects of an accident on workers

Single-dual Failure (1967)

- *Single failures* = failure of any one process system in the plant
- *Dual failures* = single failure coupled with the unavailability of either the shutdown system, or containment, or the emergency core cooling system
  - Special safety systems
- *Population dose limits* to deal with siting of Pickering A

Dose Limits (Siting Guide)

ACCIDENT	MAXIMUM FREQUENCY	INDIVIDUAL DOSE LIMIT	POPULATION DOSE LIMIT
Single Failure	1 per 3 years	0.005 Sv 0.03 Sv thyroid.	10^2 Sv 10^2 Sv thyroid
Dual Failure	1 per 3000 years	0.25 Sv 2.5 Sv thyroid	10^4 Sv 10^4 Sv thyroid

Consequence Plot of Various Canadian Safety Criteria

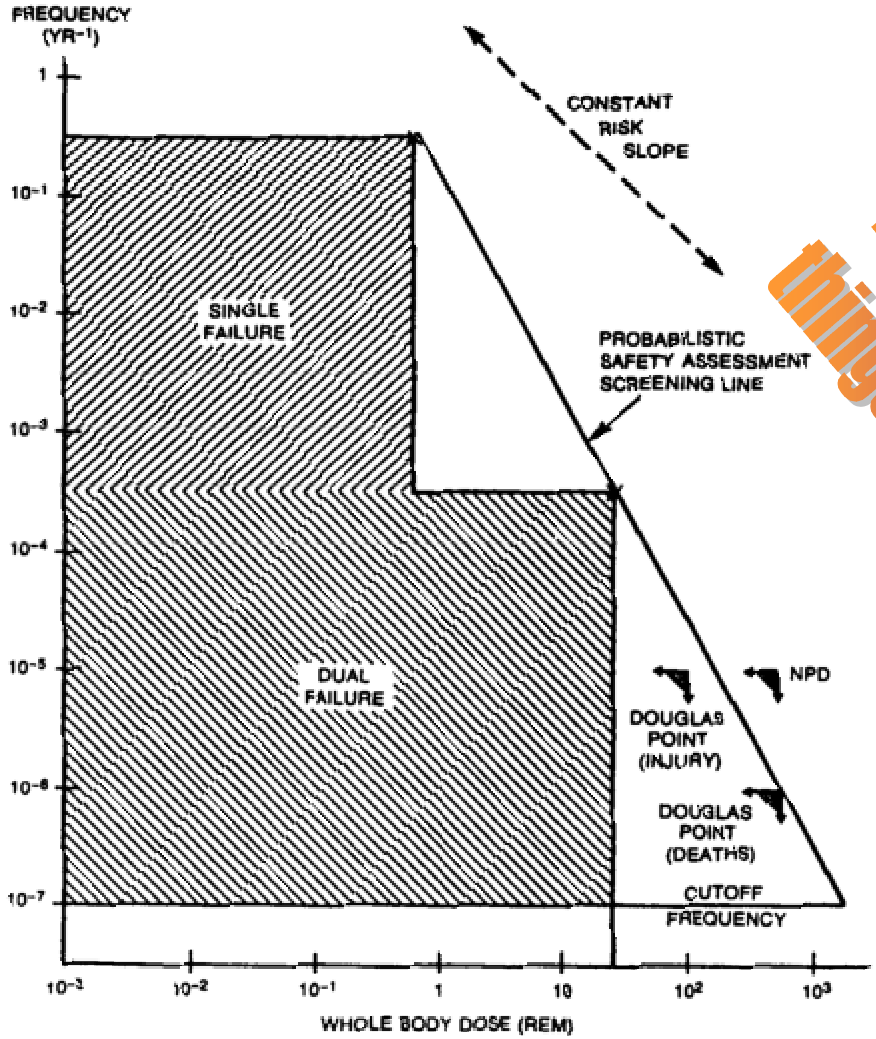


FIGURE 1 PROBABILISTIC SAFETY ASSESSMENT (SDM) SCREENING LINE

Plotting non-equivalent things on the same graph

Figure 2-3 Consequence Plot of Canadian Safety Criteria

Limitations of Siting Guide

- Multiple process failures
- Unrealistic frequencies
- Conservative assumptions
- Simplified treatment of safety system failures
- Long-term reliability

-> Safety Design Matrices (PSA)

Consultative Document C-6

DOSE/FREQUENCY LIMITS FROM C-6

	REFERENCE DOSE LIMIT, Sv	
EVENT CLASS	*WHOLE BODY*	*THYROID*
1	0.0005	0.005
2	0.005	0.05
3	0.03	0.3
4	0.1	1
5	0.25	2.5

C-6 on CANDU Pseudo-Risk Plot

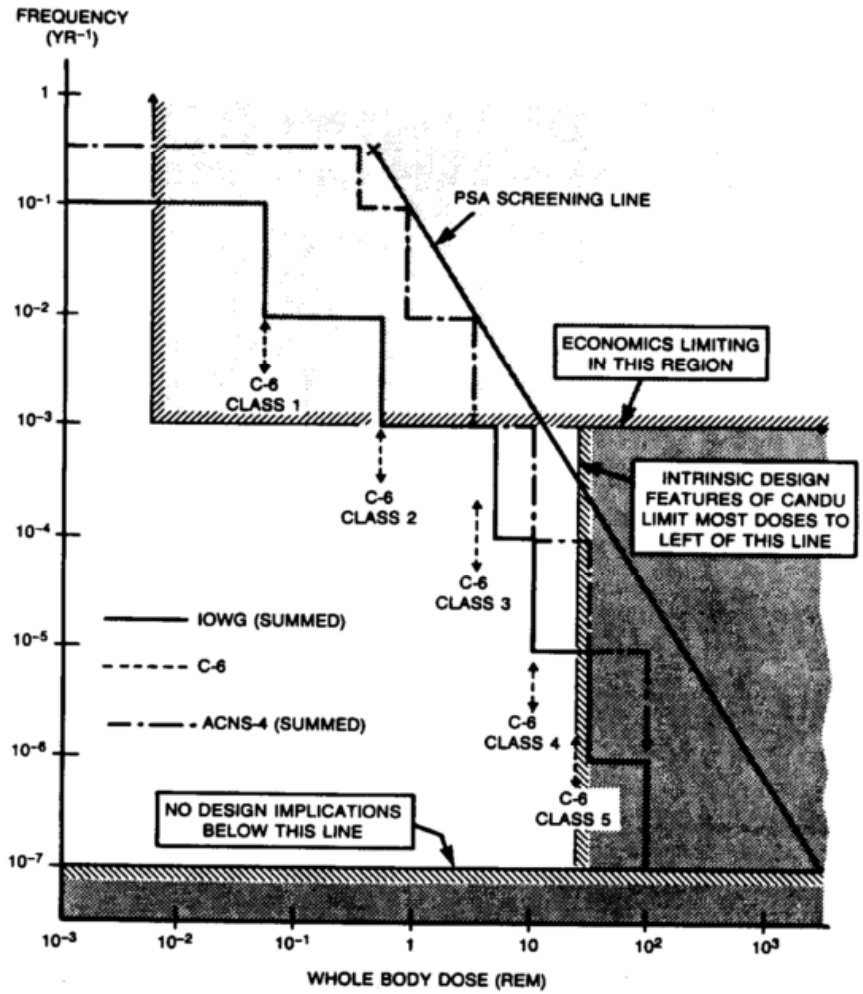


FIGURE 2 COMPARISON OF SAFETY GOALS AND "NATURAL" RESTRICTIONS

Figure 2-4 Consultative Document C-6 Limits

RD-337

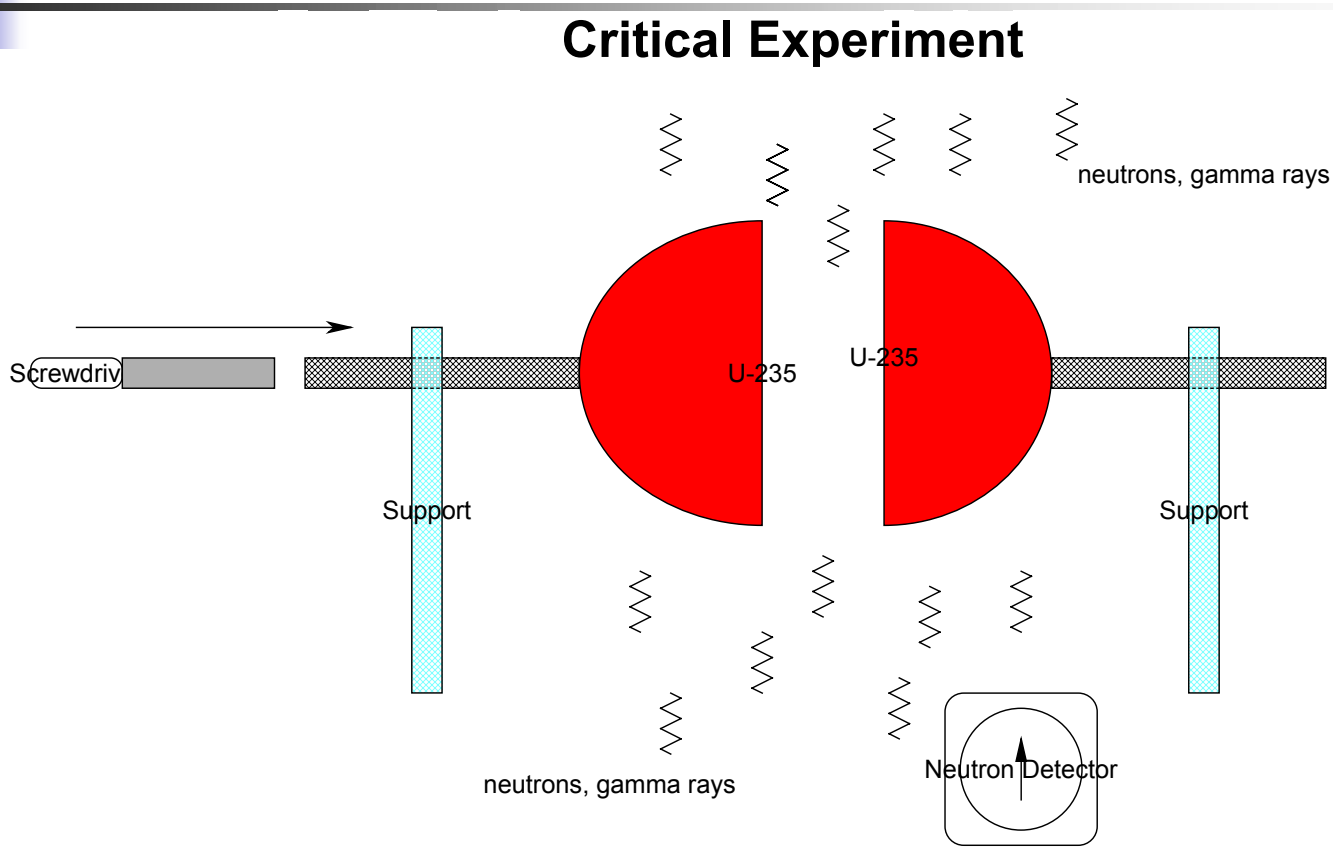
- AECL developing the Advanced CANDU Reactor (ACR-1000™; others have modern LWR designs
- Nuclear industry more international and more competitive
- Pressure to align Canadian rules with international practice – although latter not really neutral
- CNSC "Design of New Nuclear Power Plants", RD-337, sets new rules for new build and refurbishment
- Less emphasis on purity of separation between process and safety systems, more on severe accidents, more design rules etc.

RD-337 Dose Limits

AOOs	DBAs
0.0005 Sv	0.020 Sv

Class discussion – what does this change emphasize?

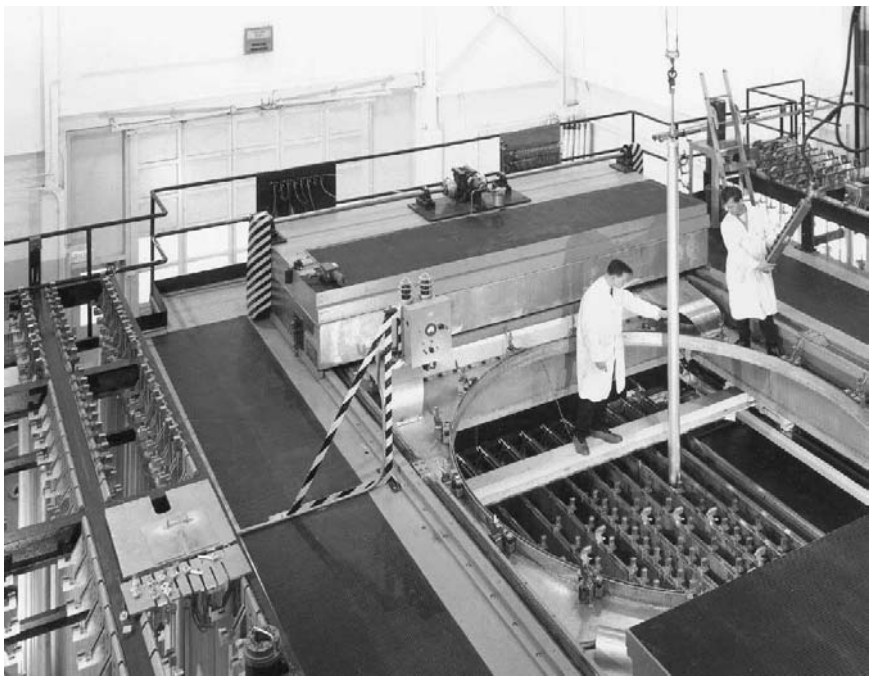
Exercise – Critical Experiment

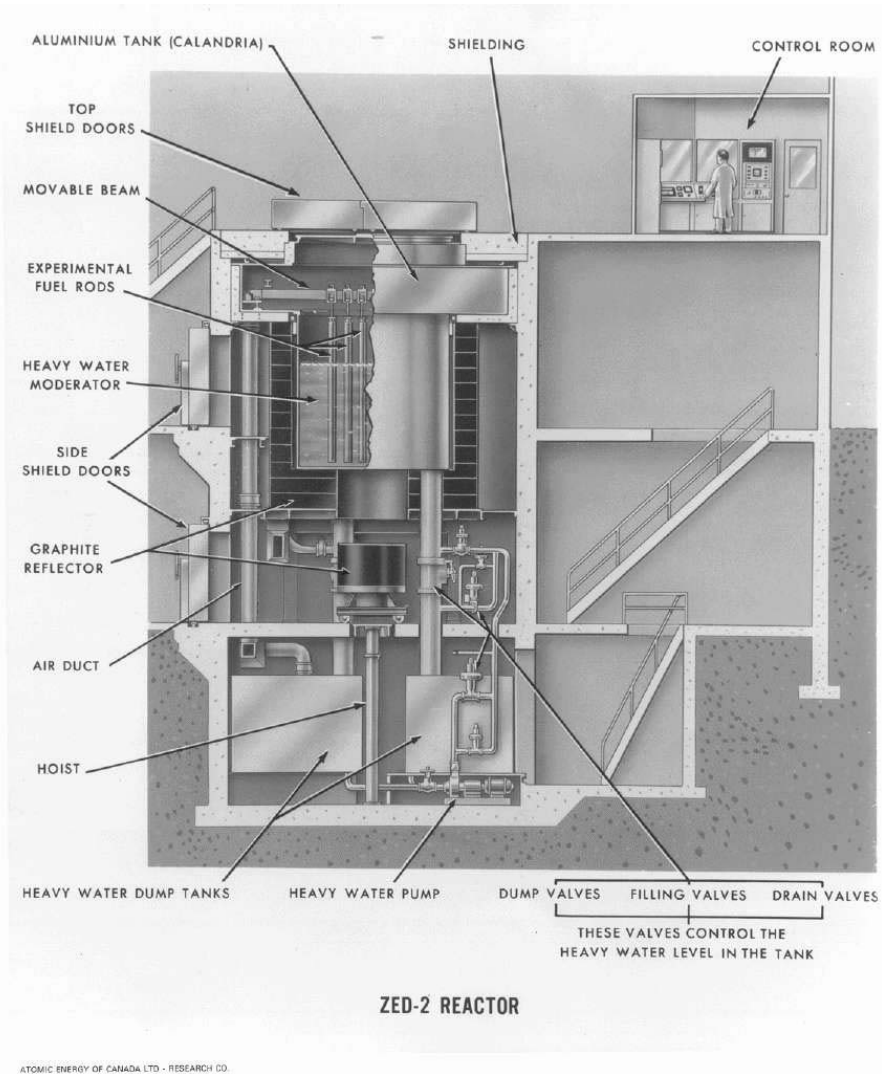


Questions

- Develop a safety approach using the concept of design basis accidents as follows:
  - Use both 'top down' and 'bottom up' approaches to define a set of accidents. Specifically: What is the "top event' that is to be avoided? What could cause the accidents?
  - How fast do they occur (i.e. what physical process determines the time-scale)? What inherently limits the consequences (i.e., you don't get a nuclear bomb - why)?
  - Compare the nature of the hazard to the scientists with that to the public?
  - How could the consequence of an accident be prevented or mitigated:
    - Without any further equipment - i.e., just after it has occurred?
    - With equipment installed beforehand?

Exercise – Zero Power Reactor





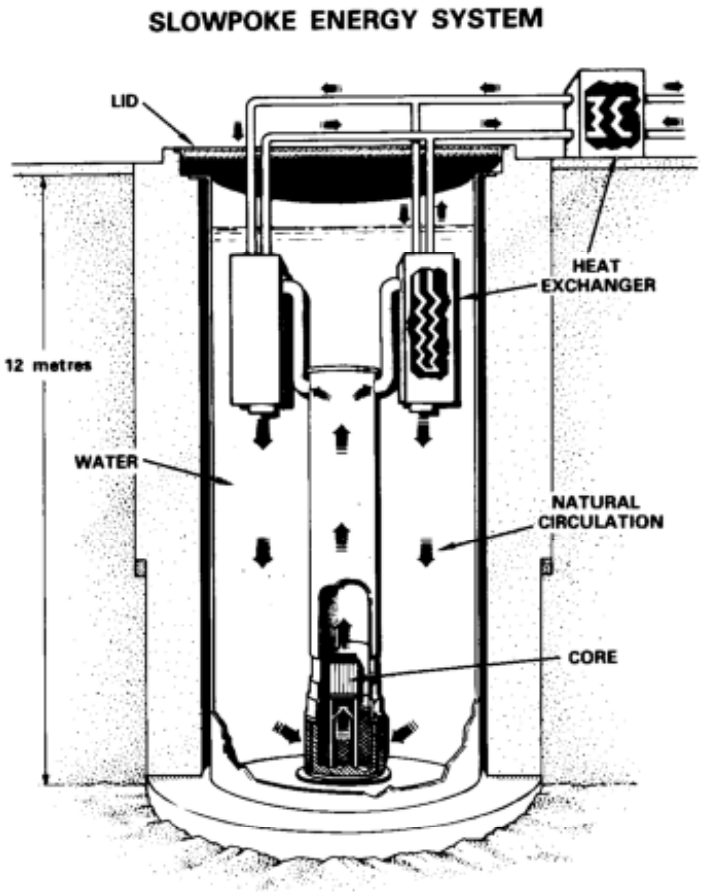
Characteristics

- **pool reactor, natural circulation, atmospheric pressure**
- **nominal zero energy (a few watts), no engineered heat removal systems**
- **low fuel temperatures, very little fission products in the fuel**
- **fuel rods suspended from hangars, can be arranged manually to different lattice pitches and geometries. Fuel rods are stored beside the pool.**
- **capability to use fuel with a large range of enrichment (but not highly irradiated fuel)**
- **provision for insertion of a few channels consisting of fuel inside a pressure tube containing electrically-heated coolant at high pressure and high temperature, inside a calandria tube (but still nominally ~zero nuclear power)**
- **control via moderator level (pump-up and drain), pump-up speed limited by pump capacity**
- **manual start-up and shutdown**
- **three redundant dump valves open to trigger a heavy-water dump on high neutron power or high log-rate**
- **no emergency core cooling system, no containment. A cover provides shielding of operators when the reactor is critical.**

Questions

- **Develop a set of design basis accidents for this reactor. It is important that you show *how* you did this, not whether you get the same answer as AECL did. Start from a large list developed using *at least two* of the techniques discussed in this Chapter and then suggest which accidents you would consider too rare to design against, and why. Provide details - e.g., it is not enough to say "increase in power" - list all the ways this could occur.**
- **If you wanted to reduce the risk from this reactor (based on your list of design basis accidents and a judgement about probability), what design changes would you do first?**
- **What elements of defence in depth are present in this design? What are missing?**

Exercise – District Heating



Schematic Diagram of the SLOWPOKE Energy System

Safety Characteristics

Small reactor for urban district heating

- **pool reactor, natural circulation, atmospheric pressure**
- **double-walled pool (350,000 litres) with a purification system (small pump and ion exchange resins, outside the pool)**
- **10 MW(th) output**
- **forced-flow secondary side, heat exchanger immersed in the pool**
- **tertiary heat exchanger connected to heating grid**
- **negative reactivity feedback from fuel temperature, coolant temperature, coolant void**
- **active reactor control devices (rods) with limits on rate (a few mk/hour) and depth (no rod in excess of a couple of mk)**

Safety Characteristics – cont'd

- **low fuel temperatures - no free fission products in the fuel**
- **two shutdown systems - one active (drops the control rods) and one passive (rods within the core which are thermally activated: the absorber material inside the rods, normally above the core, melts and fall into the core on high temperature)**
- **a confinement boundary (not shown in the figure) covering the pool top, but the building is conventional**
- **no Emergency Core Cooling System**
- **a licensed operator is *not* required to be in the control room. Any upset sounds an alarm which notifies a local attendant (who can shut the reactor down, but not restart it). Licensed operators can remotely monitor the reactor but not control it.**

Questions

- Develop a set of design basis accidents for this reactor. Are they consistent with an urban location? If not, what could be done?
- Discuss defence in depth. What does it have? Is it OK even if some aspects are missing?

Homework

- Chapter 2, questions 1,2,3,4

Project

- Select a project from the list given or (even better) propose an equivalent one. Form teams of 2 people (3 if you make the project more difficult).Develop a scope where you outline the problem you are going to solve, e.g.:
  - Objective
  - Methodology, level of detail & limitations
  - Development or research needed
  - Effort
  - Milestones
- We'll discuss informally next week. The following week you have to present the scope in detail, for credit.