CANDU Safety
#23 - Regulatory Requirements for Accident Analysis

Dr. V.G. Snell
Director
Safety & Licensing

Review of Safety Philosophy

- goal-oriented, not prescriptive
  - up to designer to define complete set of accidents
- risk-based origins
  - accident classes and dose limits based on frequency
- deterministic requirements for design basis accidents
  - accident analysis uses conservative input data & assumptions
- physically-based system models
- reference document: AECB Consultative Document C-6 Rev. 0
  - used in Darlington and beyond (Wolsong, Qinshan)

Purpose of Safety Analysis

- from designer point of view:
  - to assist in the design
  - to identify any safety design deficiencies
  - to ensure that the safety systems meet performance requirements
- from the regulatory point of view:
  - safety analysis is a way of testing the adequacy of the safety aspects of the design
  - provides evidence of acceptable risk to the public

Definition

- ***serious process failure*** **- failure of any process equipment which in the absence of special safety system action could result in significant fuel failures in the reactor or a significant release of radioactive material from the station**
- **these are serious process failures:**
  - **large loss of coolant**
  - **loss of reactivity control stopped by the shutdown systems**
  - **single channel flow blockage**
- **these are *not* serious process failures:**
  - **loss of reactivity control stopped by stepback**
  - **loss of primary side pressure control - high**

Process

- identify design basis accidents (systematic plant review)
- perform accident analysis
- compare results to acceptance criteria:
  - public dose: set by AECB
  - other criteria:
    - some set by AECB - e.g., no fuel failures for small LOCA
    - some set by designer: e.g., no calandria tube dryout for LOCA with loss of Emergency Core Cooling

Systematic Plant Review

- designers must identify all design basis accidents through systematic review:
  - all serious process failures resulting from failure of a single component or system, or combinations thereof
  - all serious process failures combined with failure or unavailability of mitigating systems
  - the frequency of all such events
- minimum list of events given as a starting point

Event Classes

- events and event combinations divided into 5 classes
- based approximately on frequency
- permissible dose increases with decreasing frequency
- AECB does not specify frequency but it can be inferred from their minimum list of events
- events identified by designer are put in the same class as events of similar frequency

Dose Limits

Class	*Whole Body Dose Limit (Sv)*	*Thyroid Dose Limit (Sv)*
1	0.0005	0.005
2	0.005	0.05
3	0.03	0.3
4	0.1	1
5	0.25	2.5

Class 1 - Examples

- loss of reactivity control
- loss of Class IV electrical power
- loss of main feedwater flow
- loss of service water flow
- loss of instrument air
- loss of moderator flow
- fuelling machine backing off reactor without replacing closure plug
- failure of instrument line
- fail open of heat transport system pressure relief valve

+ ***i.e., expected to occur once or so during plant operation***

Class 2 - Examples

- **feeder pipe break**
- **end-fitting failure**
- **pressure-tube failure + *assumed* calandria tube failure**
- **flow blockage of a fuel channel**
- **single heat transport system pump seizure**
- **pressure and inventory control system failures**
- **service water pipe failures**
- **design basis fires**

+ ***i.e., expected to occur less than once during plant operation***

Class 3 - Examples

- **large LOCA**
- **steam main pipe break**
- **feedwater pipe break**
- **design basis earthquake**
- **moderator pipe break**

+ ***i.e., events expected to occur less than once per thousand years***

Class 4 - Examples

- fuelling machine backing off reactor without replacing closure plug *and*, in turn:
  - loss of Emergency Core Coolant injection
  - heat transport system loop isolation failure
  - failure of crash cooldown of steam generators
  - one airlock door open and seals on other door deflated
  - containment isolation failure
  - failure of dousing
- main coolant pump shaft failure

+ *i.e., Class 1 failure + safety system impairment (1 in 10,000 years)*

Class 5 - Examples

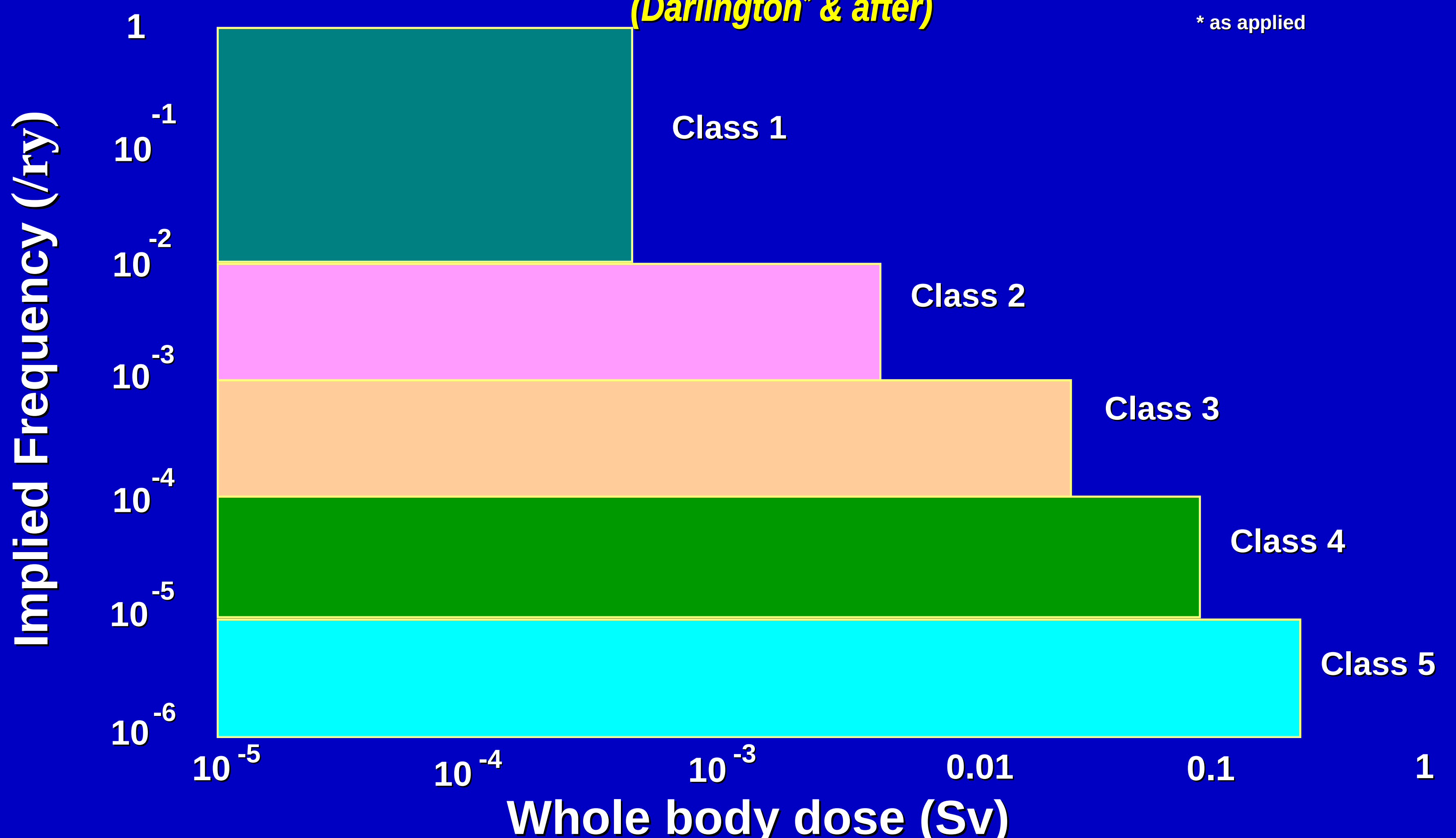
- small and large LOCA ***and***, in turn:
  - loss of Emergency Core Coolant injection
  - heat transport system loop isolation failure
  - failure of crash cooldown of steam generators
  - one airlock door open and seals on other door deflated
  - containment isolation failure
  - failure of dousing
- turbine breakup, design basis tornado
- structural failures unless designed to appropriate standards
- ***i.e., rare events + safety system impairment (less than 1 in 100,000 years)***

Specified Events Submitted for Information

- **small and large LOCA *and*, in turn:**
  - **failure of all containment coolers**
  - **open airlock doors**
- **no acceptance criteria**
- **used by regulatory to see if there is a “cliff-edge” - i.e., sudden increase in consequences**

AECB Consultative Document C-6 Criteria

(Darlington & after)*



Events Combined with Loss of Class IV Power

Initiating Event Class	*Event Class for "Initiating Event + Loss of Class IV Power"*
1	3
2	4
3	5
4	5
5	5 or beyond design basis

Techniques to Identify Other Accidents - 1

- pathways for movement of radioactivity
  - identify locations of radioactivity
  - identify events which would cause radioactivity to be relocated
  - identify system failures which would lead to these events
  - e.g., spent fuel bay: relocation due to overheating of fuel; overheating due to failure of bay cooling system
- system-by-system review
  - examine failure of each process system in turn to see its effects
  - e.g., heat transport system: loss of coolant, loss of flow

Techniques to Identify Accidents - 2

→ Probabilistic Safety Assessment
  - use of fault-trees to define frequency of top events
  - use of event trees to define required mitigating systems
- PSA now the method of choice
- no cutoff stated explicitly in C-6 but in practice do not consider events or event combinations below ~10^{-6} per year
- some exceptions: large LOCA + loss of Emergency Core Cooling is Design Basis but estimated frequency is 10^{-8} per year

Why is CANDU Accident Analysis So Complex?

- CANDU has more process systems (moderator)
- requirement to look at event combinations which are beyond design basis in most other countries
  - most of the accident analysis consists of multiple failures
  - in other countries, they would be in the PSA only, not in the design basis
- even for single events, onus is on designer to show the set of accidents is complete
  - he does not just take the list given by the regulator

Summary

- CANDU accident analysis does not stop at single initiating events, but considers double and triple event combinations
- in many ways it is like a Level 2 PSA done according to deterministic rules
- the disadvantage is complexity; the advantage is that the design examination is very thorough