CANDU Safety
#21 - Regulation of CANDU

Dr. V.G. Snell

Director

Safety & Licensing

1. Why Regulate At All?

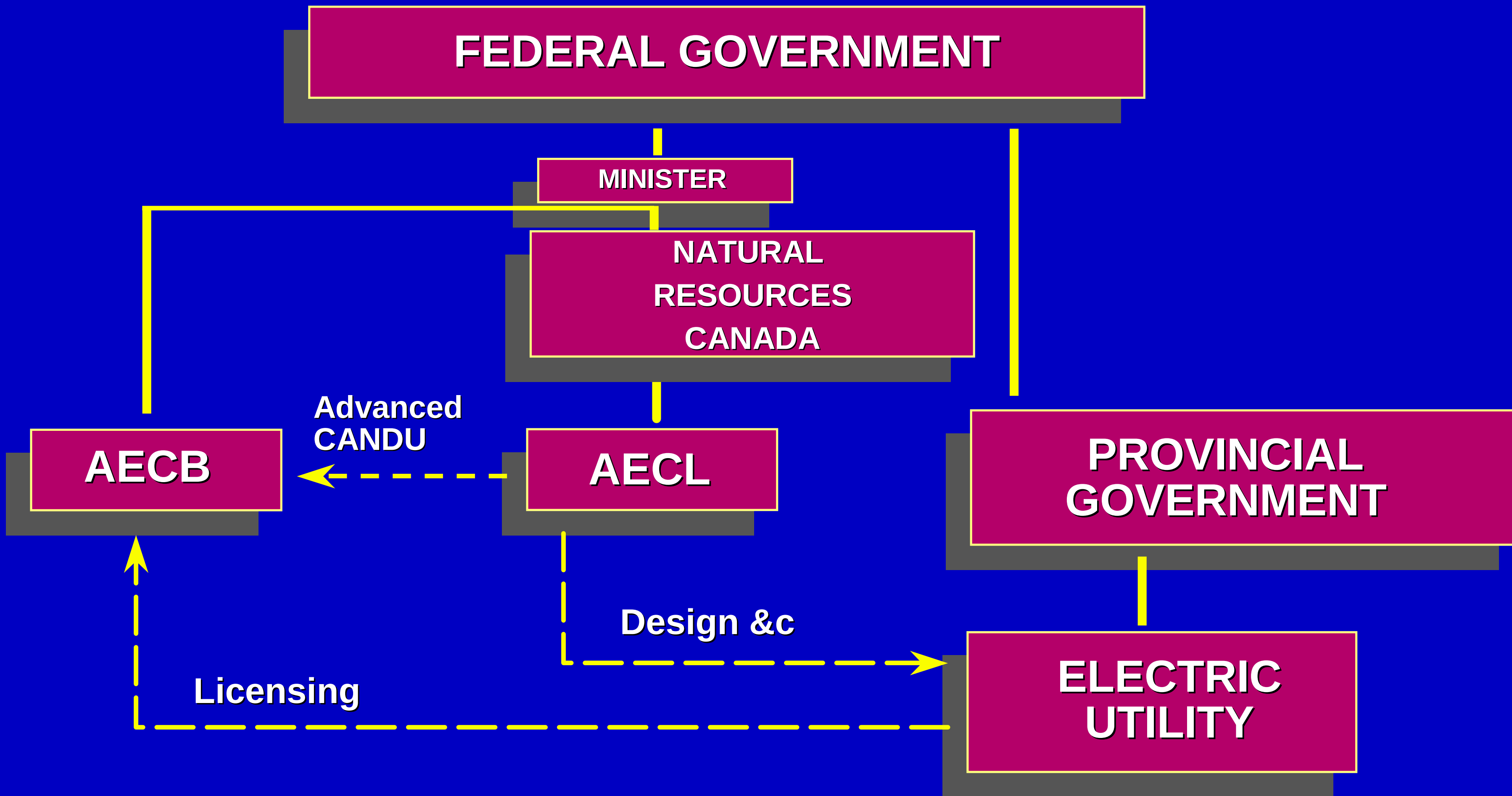
- nuclear power is complex and potentially dangerous
- minimum public safety requirements should be the same everywhere in the host country (Canada), so there is a need for regulation at the national government level
- countries which purchase CANDU should ensure the product meets national requirements (as appropriate to the design)
- independent review is a powerful means of avoiding complacency and group-think

2. Legal Basis for the Canadian System

- after the war, Canada's heavy-water reactor programme was reoriented to civilian nuclear power
- Atomic Energy Control Act (1946)
  - declared atomic energy as matter of national interest
  - established Atomic Energy Control Board (AECB) to administer it
- 1960 - extended to health & safety
- emphasis has moved from control of information to public safety
- regulation process & results in Canada are open to the public

ZEEP - The First Reactor to Go Critical Outside The USA, in September 1945

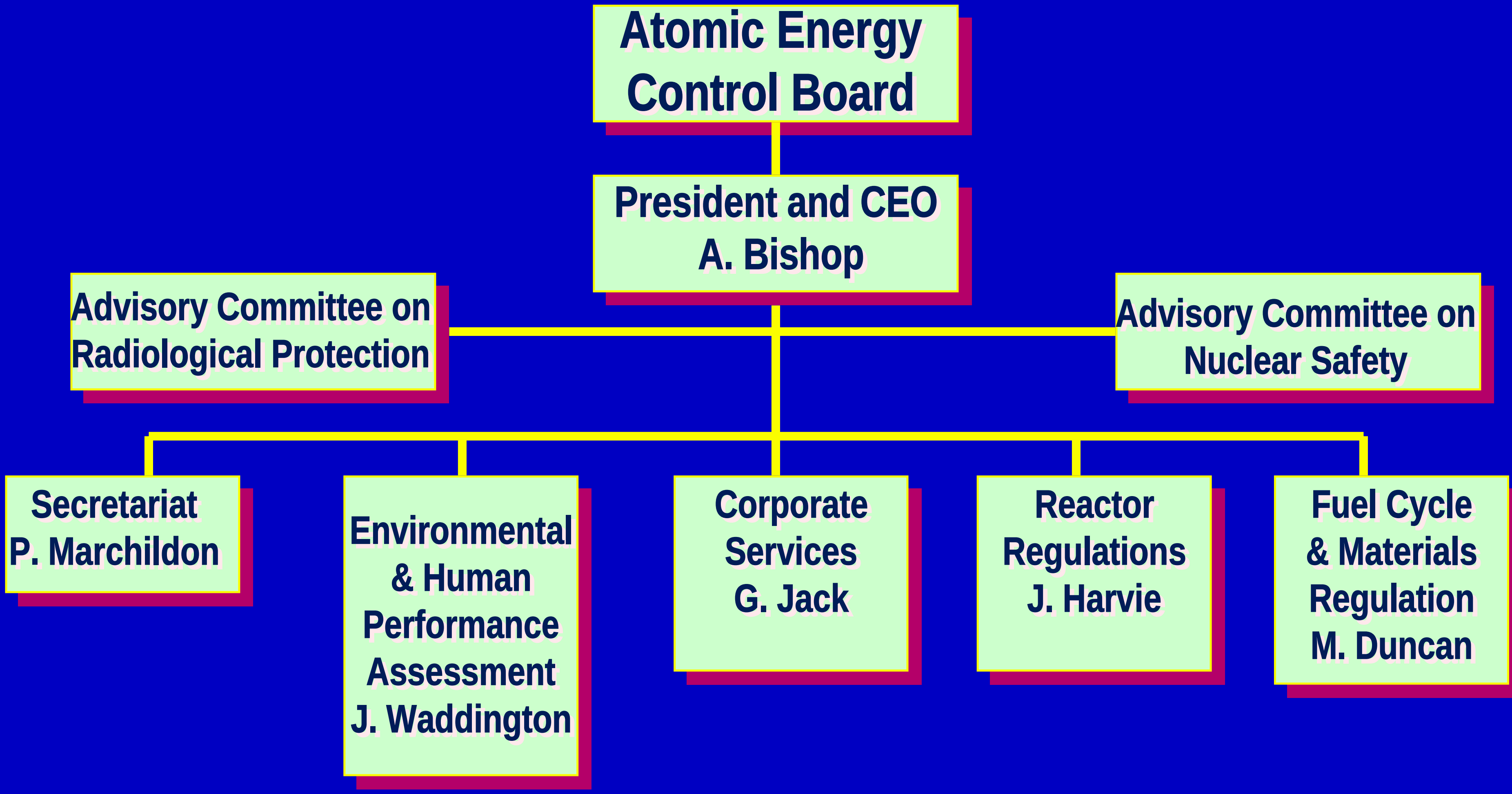
Structure of the Canadian Nuclear Industry



Atomic Energy Control Board
Five Member Board, about 400 staff

- President of the AECB (Board) is also head of the AECB (Staff)
- regulation of all civilian nuclear radiation activities
- operating licences for all nuclear facilities in Canada
- resident staff at all Canadian nuclear stations
- administers international nuclear & proliferation policy
- regulatory training to nations interested in CANDU
- reviews Environmental Assessment on behalf of gov't

AECB Organization



Regulations Structure (Today)

Atomic Energy Control Act

↓

Regulations

↓

Regulatory Documents (R-series)

↑

Consultative Documents (C-series)

↑

Precedent, Practice & Innovation

Regulations Structure (Today)

- ***Regulations*** **- enforceable by law**
- ***R-series*** **- regulatory documents - hard requirements, not law**
- ***C-series*** **- consultative, developing or draft regulatory documents**
- **R- & C- documents cover safety analysis, requirements for safety-related systems, quality assurance, operations, decommissioning, etc.**
- ***non-prescriptive and results-oriented*****: encourages innovation & avoids inherent conflict of interest**

Four Simple Steps to Licensing a Nuclear Power Plant

- ← Letter of Intent
- ↑ Site Acceptance
  - site evaluation and proposed design
  - environmental assessment
  - public consultation
- → Construction Licence
  - Preliminary Design and Preliminary Safety Report
- ↓ Operating Licence
  - Final Design and Final Safety Analysis Report

Regulations Structure (Coming Soon)

Nuclear Safety & Control Act

↓

Regulations

↓

Regulatory Policy

↓

Regulatory Standard

↓

Regulatory Guide

↓

Regulatory Notice

↓

Regulatory Procedure

Regulatory Guidance Documents: Compliance optional unless incorporated in licence

New Regulatory Documents

Regulatory Policy	Philosophy, guides AECB Staff and applicants
Regulatory Standard	Measurable evaluation criteria, can be put in licence
Regulatory Guide	AECB accepts and recommends but not put in licence
Regulatory Notice	Advice & information
Regulatory Procedure	AECB Work Processes

3. Regulatory Philosophy in Canada

- origins
  - small country, single unique reactor type, single designer
  - government sponsored & developed
  - “on our own”
- safety responsibility on owner, regulator audits

Prescriptive

Regulator tells you what to do and how to do it

Non-Prescriptive

Regulator tells you what safety requirements you have to meet and you find the best way of doing it

4. *Major Regulatory Requirements in Canada*

- initial safety goal (1960s): risk of prompt death in nuclear accident < 1/5 risk of death in coal, or 0.2 deaths/year
- led to probabilistic treatment on Douglas Point

  Total risk =

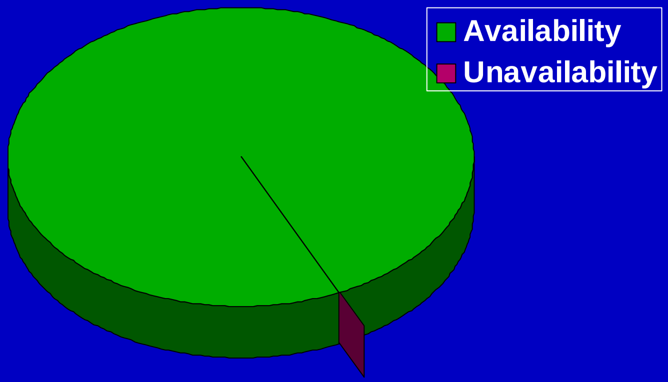
  Σ (probability of accident) x (consequence of accident)

  < safety goal
- requires:
  - design to ensure low *frequency* of accidents
  - design, test & maintain to *demonstrate availability*
  - *separate* normal and safety systems

Evolved to More Deterministic Requirements: The Single/Dual Failure Approach

- Single Failure - failure of a system used in the operation of the plant (e.g., LOR, LOCA)
- Dual Failure - single failure combined with the assumed unavailability of a safety system
- dose and frequency/unavailability limits assigned
- one shutdown system must be assumed unavailable in all accident analysis
- reactors before Darlington all licensed using this approach

Safety System Requirements



- SDS1, SDS2, containment, ECC
- must be:
  - independent
  - testable to unavailability of 10^{-3} years/year
  - diverse & redundant (shutdown systems)
  - fail safe to extent practical
  - separate from process systems and each other - minimum shared components

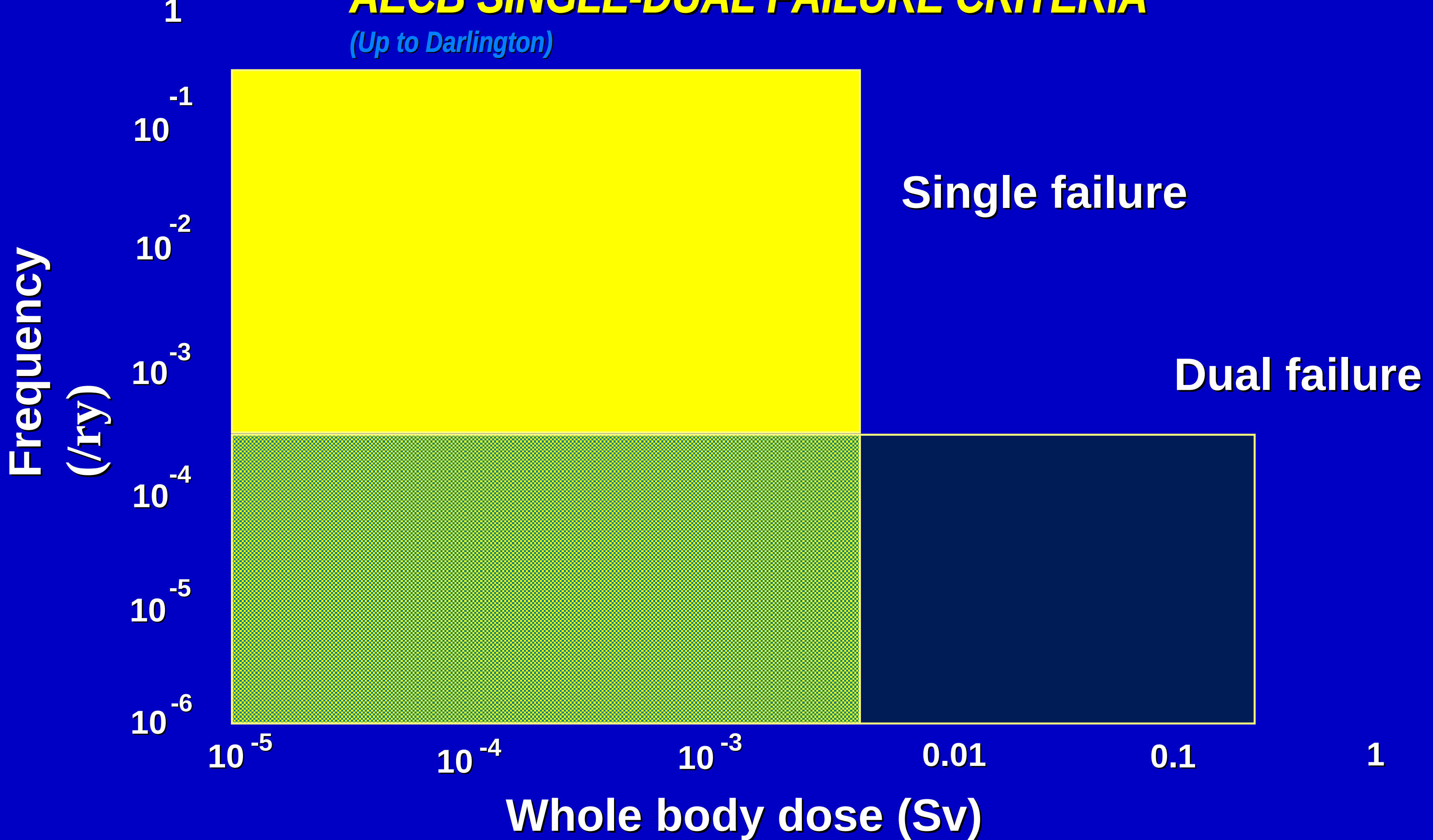
AECB Single-Dual Failure Criteria

(from R-10)

	SINGLE FAILURES		DUAL FAILURES	
	WHOLE BODY	THYROID	WHOLE BODY	THYROID
INDIVIDUAL	0.005 Sv	0.03 Sv	0.25 Sv	2.5 Sv
POPULATION	100 per-Sv	100 per-Sv	10^4 per-Sv	10^4 per-Sv

AECB SINGLE-DUAL FAILURE CRITERIA

(Up to Darlington)



Single/Dual Failure - Why So Special?

- **maximum process failure frequency large enough (1 in 3 years) that it can be *shown* to be met**
- **requires *demonstration* of claimed reliability for special safety systems**
- **requires consideration of severe accidents (LOCA+LOECC) *within* design basis**
  - **hydrogen in the Three Mile Island accident was a surprise to the LWR community but had been analyzed in Canada for years**

Single/Dual Failure - What's Missing

- treats rare accidents (large LOCA - 10^{-5} per year) and less rare accidents (loss of reactivity control - 10^{-1} per year) on same basis
- does not have a good framework for safety related systems other than special safety systems
  - instrument air, electrical power, process water
- can miss multiple failures which have frequency comparable the single or dual failures
- led to Probabilistic Safety Analysis and AECB Document C-6

Probabilistic Analysis

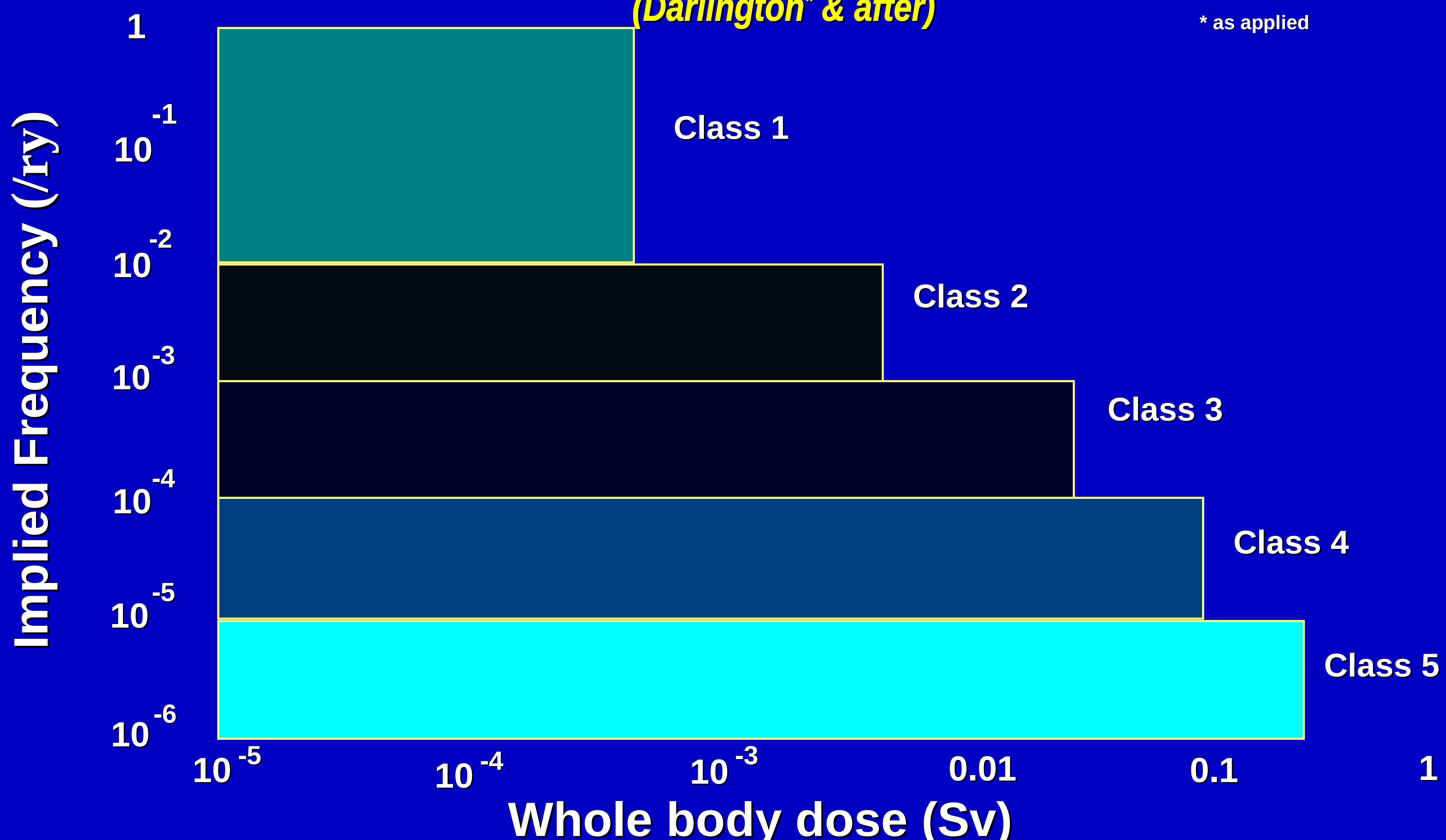
- explicitly account for probability of an accident in calculation of risk
- incorporate probability of plant state
- model mitigating system reliability and performance realistically
- compare to acceptance criteria set by designer

AECB Introduces C-6

- first used on Darlington
- 5 event classes but not explicitly assigned to frequency
- requires *systematic plant evaluation* to capture all events
- a poor man’s Probabilistic Safety Analysis with deterministic rules

AECB Consultative Document C-6 Criteria

(Darlington & after)*



Other Major Regulatory Documents

R-7	Containment
R-8	Shutdown Systems
R-9	Emergency Core Cooling System
R-10	Use of Two Shutdown Systems
C-22	Quality Assurance
R-77	Overpressure Protection Requirements
R-90	Decommissioning
C-98	Reliability
R-99	Reporting
C-129	ALARA

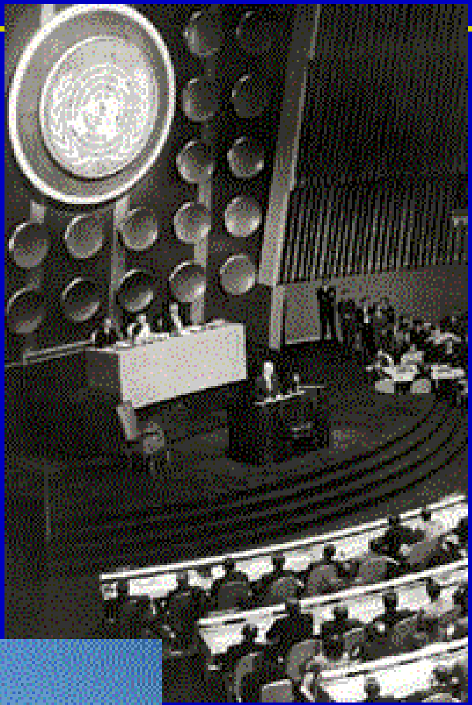
5. Prescriptive Regulation - The U.S. Approach

U.S.	Canada
Many vendors, many designs	One vendor, one design
Legal-oriented	Consensus oriented
About 6 binders of detailed laws (Code of Federal Regulations)	About 100 pages of laws
Prescribes overall requirements plus specific acceptance criteria and how to do design	Prescribes high-level acceptance criteria; onus on designer to justify the design
Easy to “check-off” that the rules have been met by a foreign regulator	Hard for others to understand process and needs deep understanding of CANDU to apply

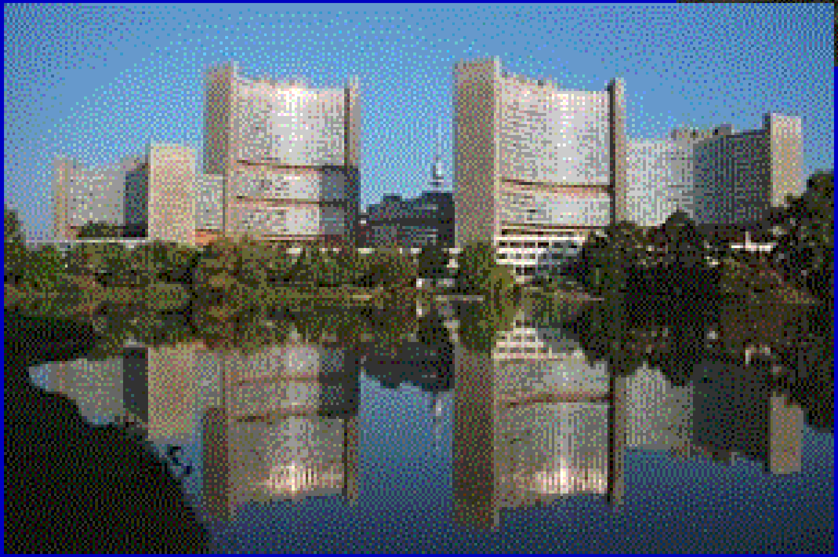
Example: Sheath Embrittlement in Large LOCA

- U.S. 10CFR50 Section 46(b(1)
  - "The calculated maximum fuel element cladding temperature shall not exceed 2200°F"
- Canada - R-9, Section 3.2(c)
  - "All fuel in the reactor and all fuel channels shall be kept in a configuration such that continued removal by ECCS of the decay heat produced by the fuel can be maintained..."
- U.S. - prescribes not only limit but models used to calculate it
- Canada - describes objective and up to designer to do tests and develop models to prove it is met

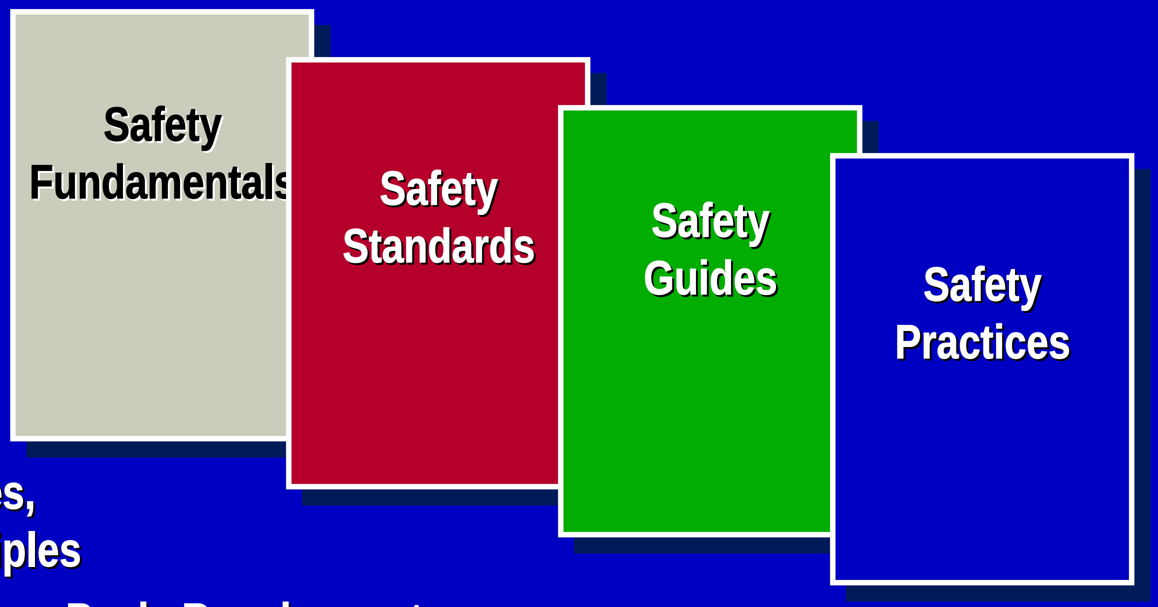
6. *IAEA - Toward World Regulations*



- **IAEA - International Atomic Energy Agency**
- **UN body, HQ in Vienna**
- **"to accelerate and enlarge the contribution of atomic energy to peace, health, and prosperity throughout the world"**
- **Hence:**
  - **safeguards**
  - **safety**
  - **promotion**



IAEA Safety Documents



Basic Objectives,
Concepts & Principles

Basic Requirements
for specific applications

Recommendations

Examples and Methods

CANDU complies directly or “meets intent”

Specific Changes to Wolsong 2,3&4 & Qinshan 1&2

- reorganized Safety Report per USNRC format
- meet Canadian *and* Korean or Chinese requirements for siting
- Level 2 PSA with external events, performed by Korea
- first application of AECB Consultative Document C-6 on a CANDU 6
- comprehensive dual parameter trip coverage
- Technical Support Centre
- Critical Safety Parameter Monitoring System

Wolsong 1, 2, 3, & 4

Specific Changes to Wolsong 2,3&4 & Qinshan 1&2 - cont'd

- tornado protection of key safety related systems on Qinshan due to site characteristics
- seismically qualified fire protection system in addition to existing two-group design approach

Qinshan Phase 3 - Units 1& 2

(Projected appearance - site being prepared)

8. Conclusions

- Canadian goal-oriented licensing regime facilitates licensing in diverse jurisdictions although it may be harder to understand
- CANDU owners develop their own licensing system incorporating the best of Canadian and national requirements
- IAEA is slowly becoming an international regulator and its requirements are met