CANDU Safety #10: Design and Analysis Process

F.J. Doria

Atomic Energy of Canada Limited

Overview

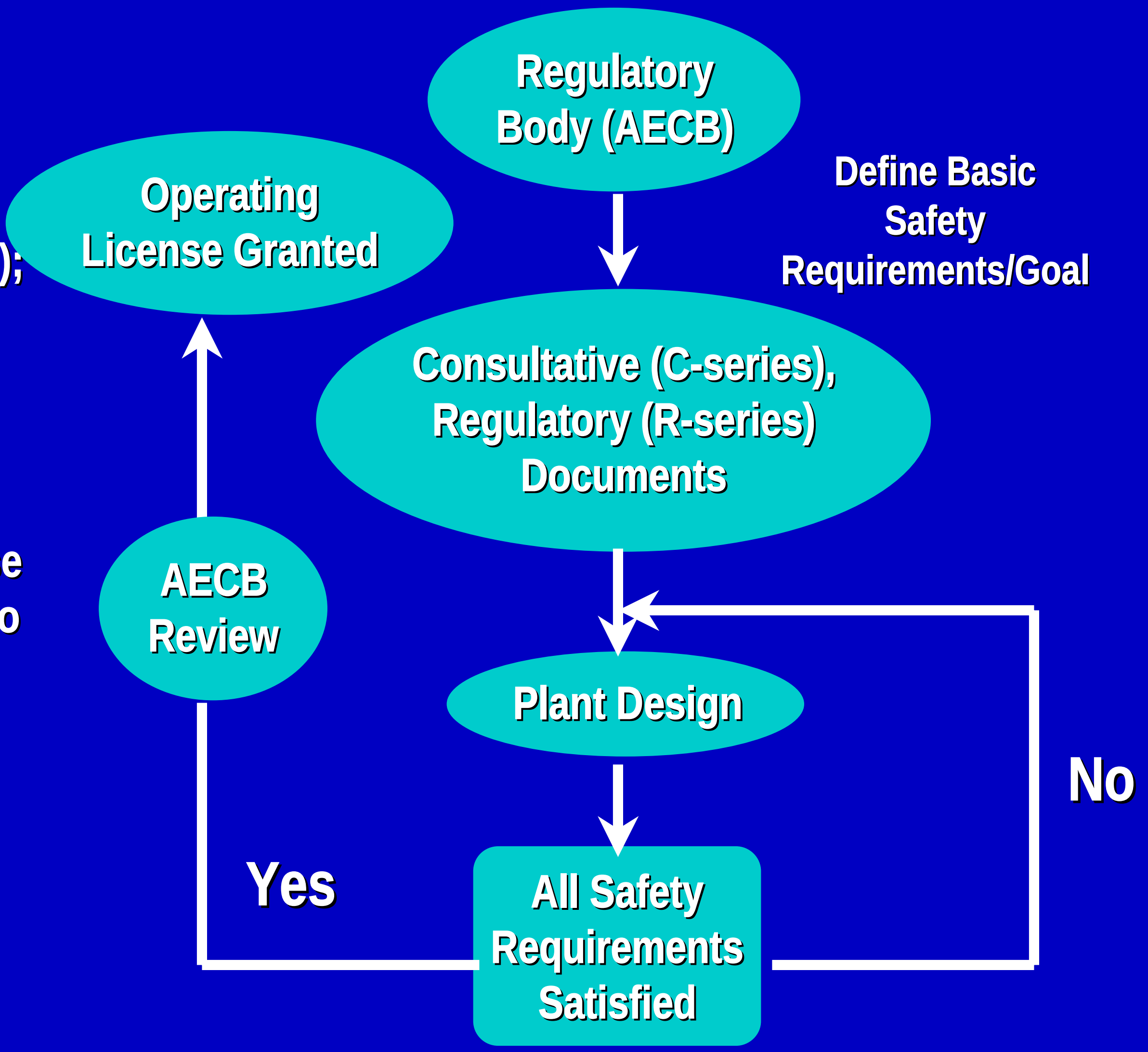
- Establishment of basic safety requirements by the Canadian regulatory body
- Design and safety process
- Regulatory documentation
- Safety design objective and defense in depth principle
- Safety analysis process

Safety Criteria

- The Canadian Atomic Energy Control Board (AECB) is the regulatory body for nuclear power plants in Canada
- The AECB defines the
  - basic safety criteria for normal operation and accident conditions
  - imposes requirements on major mitigating systems for accident conditions (i.e., shutdown safety systems SDS1 and SDS2, emergency core coolant injection and containment).
- AECB documents the criteria/requirements in a Consultative Document called C-6, and Regulatory documents R-7, R-8, R-9, R-10
- The plant designer is responsible for designing the power plant to satisfy the basic safety criteria

Simplified Design and Safety Process

- C-Series (Consultative documents); draft regulatory documents
- R-Series (Regulatory Documents); sets overall requirements
- Overall process is NON-PRESCRIPTIVE
  - AECB sets the goals to be achieved; however, how these goals are satisfied is left up to the designers (i.e., AECL)



AECB Consultative Document C-6

- **Provides a minimum list of abnormal events to be analyzed**
- **C-6 also requires that the plant designer also perform a systematic review of the plant design to identify all *additional* safety significant failures**
- **Accidents are categorized into 5 classes which reflect the frequency of the accident**
- **For example, some class categories include:**
  - **Class 1 category: highest frequency; high number of occurrences per reactor year (1 per 100 years < 1/ f < 1 per year)**
  - **Class 5 category: lowest frequency; low number of occurrences per reactor year (1 per 100,000 years > 1/f)**
- **Stricter dose limits apply to those accidents that occur more**

Summary of Some AECB Documents

- C-6: Requirements for Safety Analysis
- R-7: Requirements for Containment System
- R-8: Requirements for Shutdown Systems
- R-9: Requirements for Emergency Core Cooling
- R-10: The Use of Two Shutdown Systems

Safety Design Objectives

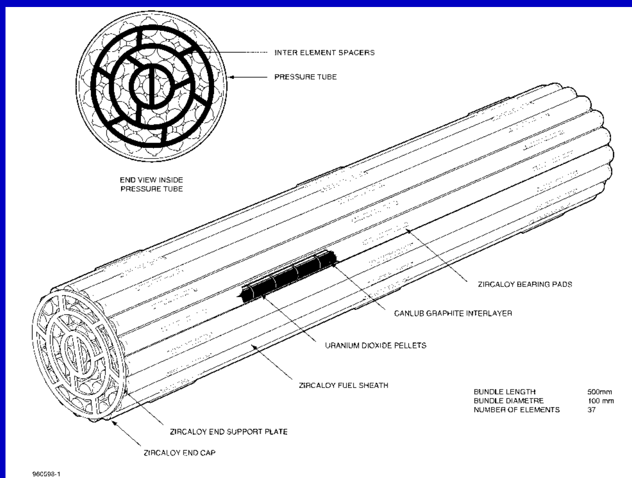
- The basic safety objectives for the design of the nuclear power plant are:
  - NORMAL OPERATION: limit the continuous emissions of radioactive material to a small fraction of the reference dose limit
  - ACCIDENT CONDITIONS: safety analysis must demonstrate that the accident dose limits are not exceeded
- General Safety Requirements
  - Shut down the reactor and maintain it in a safe shut down condition
  - remove decay heat from the core after shutdown
  - reduce the potential of radioactive material being released and to ensure the safety objective is satisfied (i.e., do not exceed

Safety Philosophy - Defense in Depth Principle

- **The defense in depth principle is applied in the CANDU design**
- **The defense in depth principle provides**
  - **an increase in the level of safety**
    - ***prevention*** **by including design features to reduce frequency of accident;**
    - ***protection and mitigation*** **by design features such as SDS1, SDS2;**
    - ***accomodation*** **by design features of the containment system, and**
  - **introduces several barriers to the release of fission products**

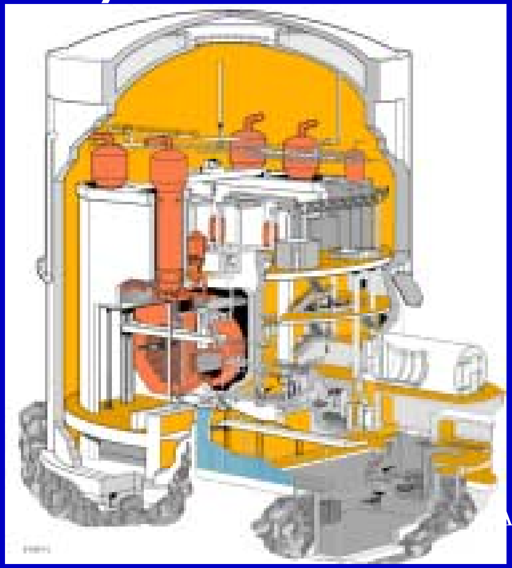
Defense in Depth Barriers

1) Uranium-Dioxide Fuel Matrix & 2) Sheath



3) Primary Heat Transport System

4) Containment



5) Exclusion Boundary

Safety Analysis

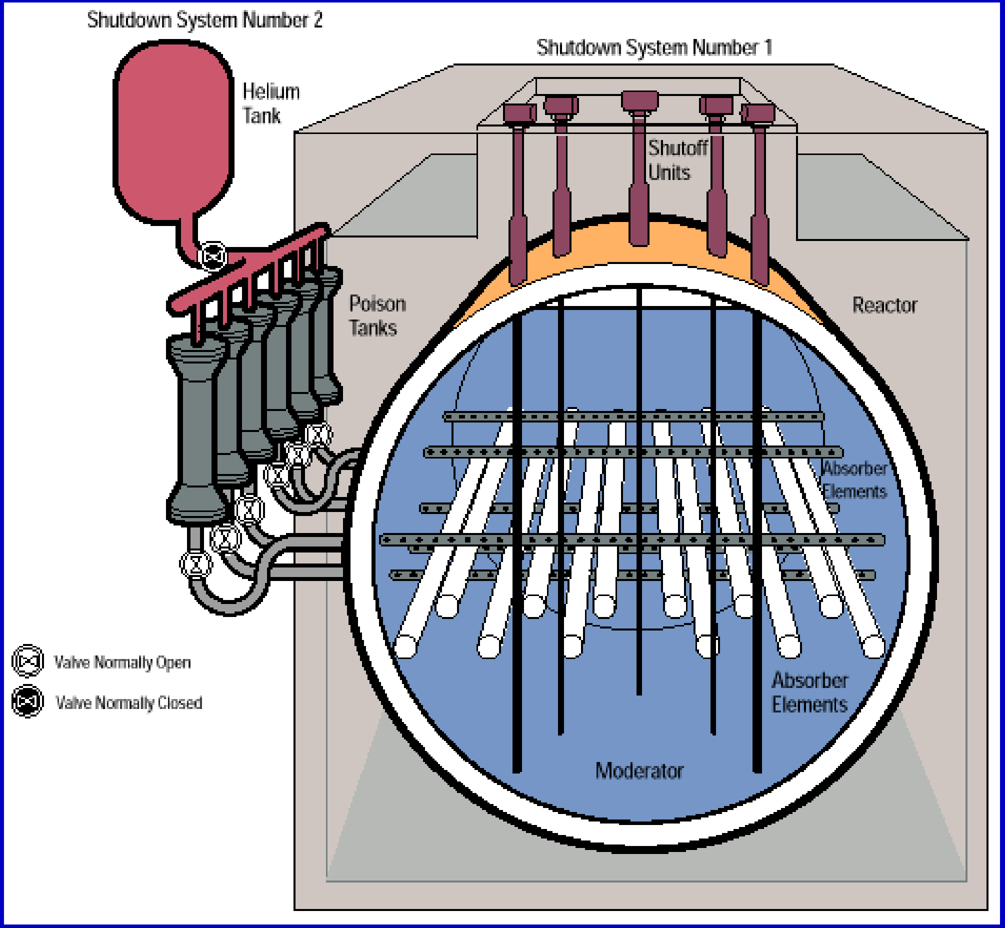
- Analysis Objective: To demonstrate that safety criteria are satisfied
- Types of failure:
  - Single failures
    - Failure of any process system. Process systems are those required for normal operation
  - Dual failures
    - Failure of any process system with the coincident failure of any one safety system. Safety systems are only required to reduce the consequences of a process system failure

Process and Safety Systems

- **Process System**
  - **Primary heat transport system**
  - **Reactor control**
  - **Electrical**
  - **Fuel and fuel handling**
- **Safety systems**
  - **Shutdown safety system No 1 (SDS1)**
  - **Shutdown safety system No 2 (SDS2)**
  - **Emergency core coolant (ECC)**
  - **Containment**

Shutdown System Failures

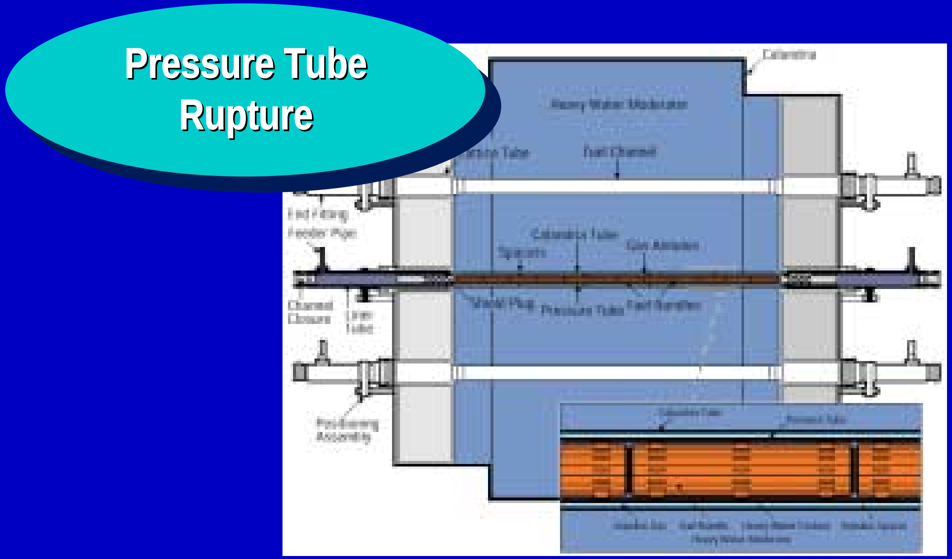
- Loss of shutdown following a process failure is not a credible event for licensing, since
  - Two independent shutdown systems
  - Each fully capable to shut down the reactor
  - The systems are spatially separate and
  - The systems have separate logic systems

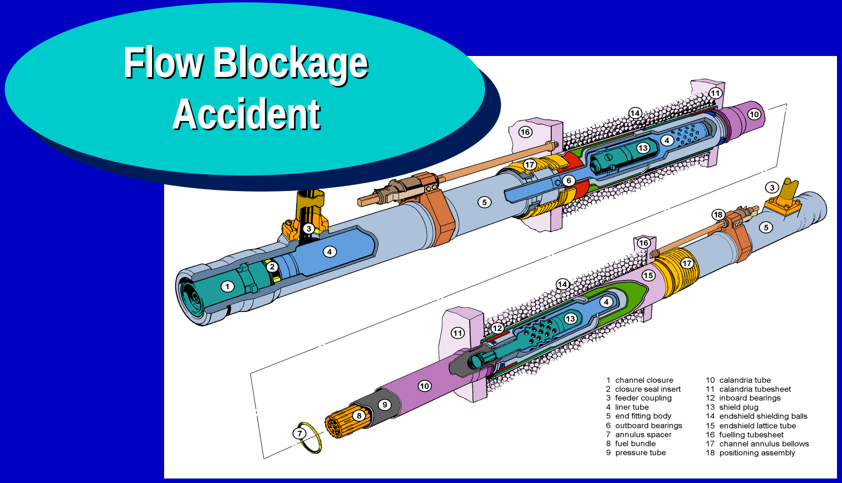


Some Accident Scenarios

- Loss-of-coolant accident (single-type failure)
- Single channel events (single-type failure)
  - In-core breaks
    - spontaneous pressure tube rupture that leads to the consequential rupture of its calandria tube
    - flow blockage events
    - feeder stagnation
  - feeder off-stagnation breaks
  - end fitting failure
- Loss-of-coolant accident with coincident loss of emergency core coolant injection (LOCA/LOECC)

Some Accident Scenarios





Accident Classes

EVENT CLASS (AECB C-6 Document)	FREQUENCY RANGE (f) (per Reactor Year)	ACCIDENT
1	$10^{-2} \leq f < 1$	Off-Reactor Fuelling machine accident
2	$10^{-3} \leq f < 10^{-2}$	Single-channel events (FSB, EFF, PTR, FB)
3	$10^{-4} \leq f < 10^{-3}$	Large LOCA
4	$10^{-5} \leq f < 10^{-4}$	Off-Reactor Fuelling machine accident *plus* failure to isolate containment
5	$f < 10^{-5}$	LOCA/LOECC

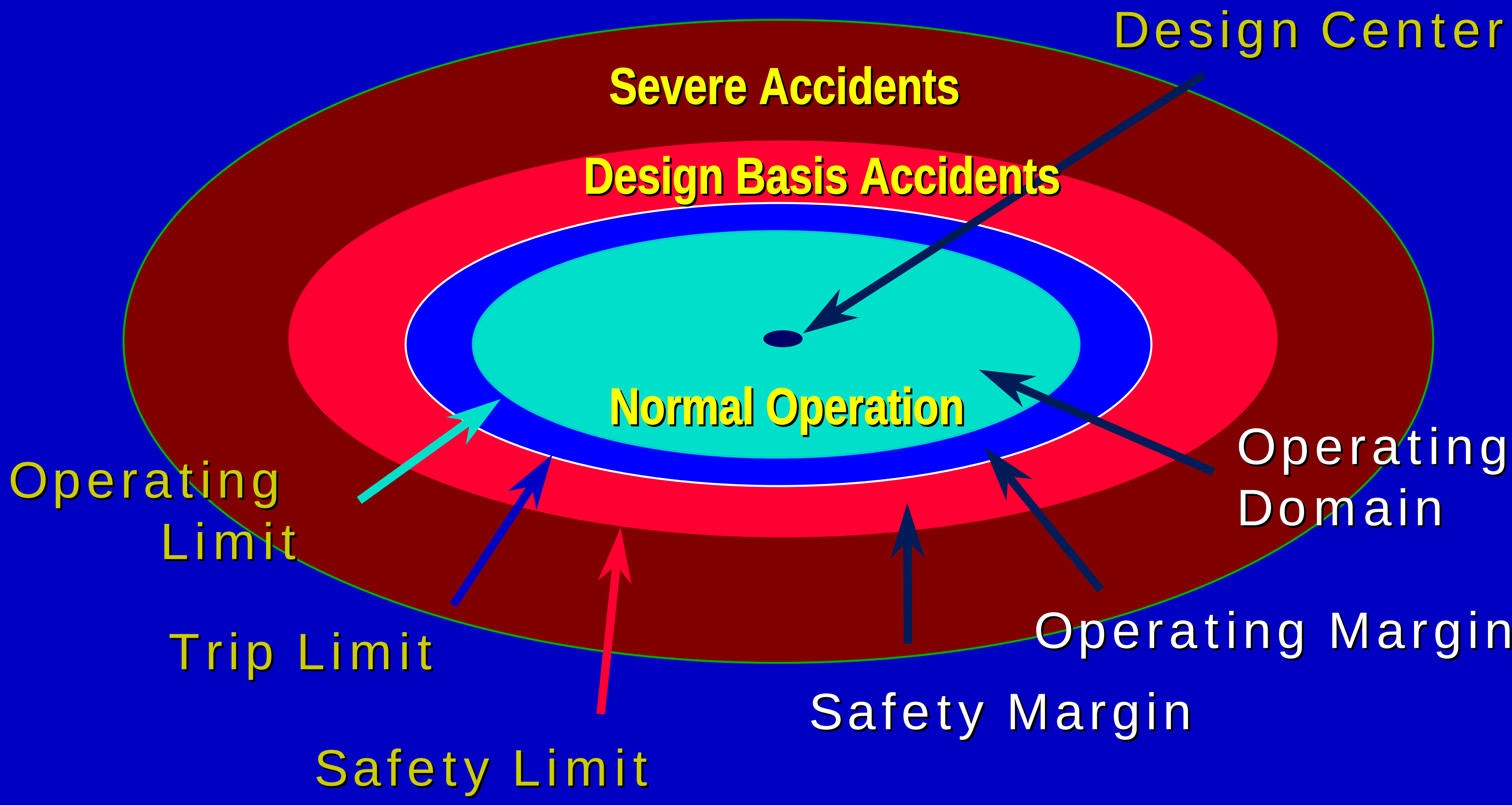
Some Analysis Acceptance Criteria (LOCA)

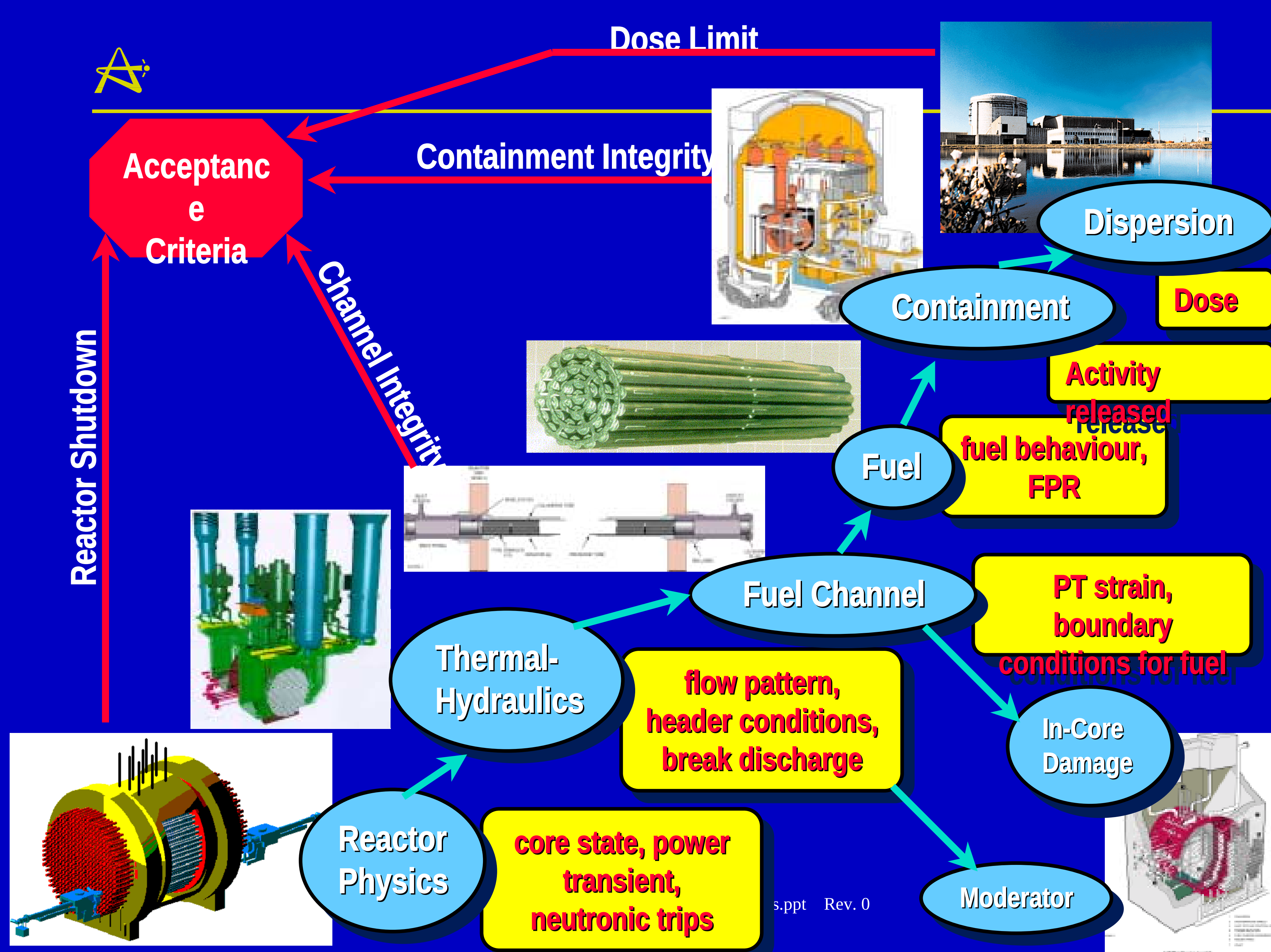
- Dose limits do not exceed the limits specified in AECB regulatory document R-10; dose limits also given in AECB regulatory document C-6
- Each of the 2 independent shutdown safety systems will arrest the reactivity and power excursions and will keep the reactor in a shutdown state (AECB regulatory document R-8)
- Fuel channel integrity must be maintained (AECB regulatory document R-8 and R-9)
- Structural integrity of containment must be maintained (AECB regulatory document R-7)

Analysis Philosophy

- In past safety analysis performed for CANDU reactors, a conservative approach is used
- That is, the assumptions and methodology applied in a particular analysis is selected in conjunction with the analysis objective
  - for example, LOCA/LOECC one objective is to maximize fission-product release and hydrogen==> methods and assumptions geared at maximizing these results
- Change in philosophy
  - recent analysis is moving towards a best-estimate approach
  - this is coupled with an uncertainty analysis to give a result (i.e., maximum sheath temperature during LOCA) with a

CANDU Margins and Limits




Dose Limit
Containment Integrity
Acceptanc
e
Criteria
Channel Integrity
Reactor Shutdown
Dispersion
Dose
Containment
Activity
released
Fuel
fuel behaviour,
FPR
Fuel Channel
PT strain,
boundary
conditions for fuel
Thermal-
Hydraulics
flow pattern,
header conditions,
break discharge
In-Core
Damage
Reactor
Physics
core state, power
transient,
neutronic trips
Moderator
s.ppt Rev. 0