



Lecture 13 – Whither Safety?

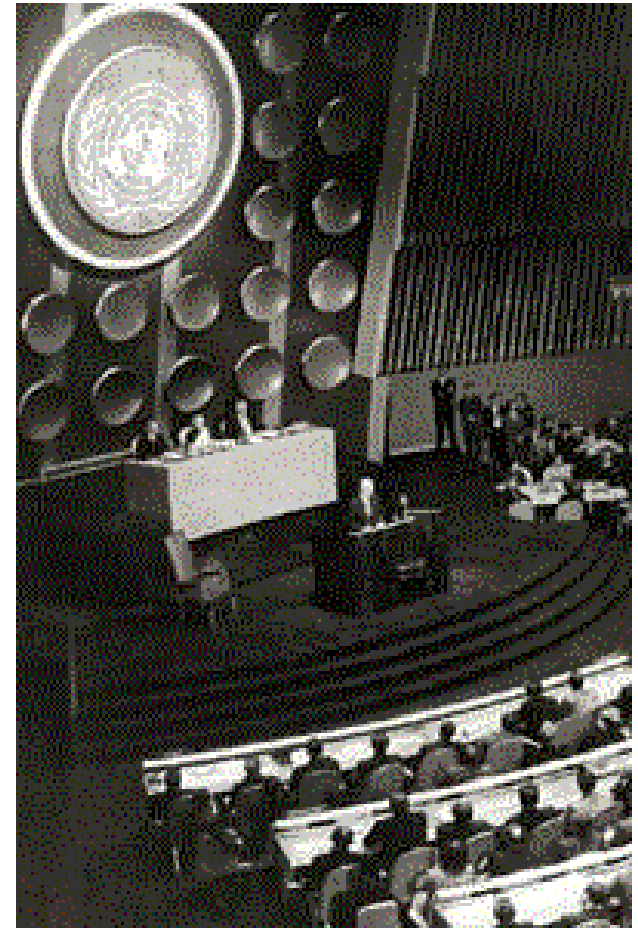
Dr. V.G. Snell

Nuclear Reactor Safety Course

McMaster University

International Atomic Energy Agency (IAEA)

- “Atoms for Peace” deal:
 - Weapons nations limit membership
 - Non-weapons states forgo weapons
 - Weapons states assist non-weapons states in civilian nuclear power
- Promotion in exchange for safeguards
- Safety Guides



The logo graphic consists of a vertical black line on the left, a horizontal black line below the text, and a cluster of overlapping colored squares (yellow, red, blue) to the left of the text.

INSAG

- International Safety Advisory Group
 - Independent group of experts formed after Chernobyl to advise the Director-General of the IAEA
- Key concepts:
 - Basic Safety Principles
 - Safety Culture



Basic Safety Principles

- Written after Chernobyl
- In present tense
 - If a reactor did not meet them, it should
- 5 levels
 - Objectives
 - Fundamental Management Principles
 - Defence-in-Depth Principles
 - General Technical Principles
 - Specific Principles



General Nuclear Safety Objective

- “To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard”



Commentary - Safety

- Does protecting people protect the environment?
- What concept of protection for the environment should be used?
 - Emission Limits
 - Optimized Emissions
 - Best Available Technology
 - Zero Emissions



Radiation Protection Objective

- “To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is kept as low as reasonably achievable and below prescribed limits, and to ensure mitigation of the extent of radiation exposure due to accidents.”



Commentary - ALARA

- “As Low As Reasonably Achievable”, economic and social factors being taken into account
- Requires identification and optimization of dose reduction
- Often equated to cost-benefit: \$100,000 per Sievert averted



Technical Safety Objective

- “To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.”



Commentary – Severe Accidents

- Restatement of Defence-in-depth +
- Large offsite release from severe accidents must be very low probability
- Severe core damage frequency for existing plants $< 10^{-4}$ / yr.
 - New plants: $< 10^{-5}$ /yr.
- Severe accident management and mitigation procedures should reduce risk of large prompt offsite release by $>$ factor of 10
 - = conditional containment failure probability



Safety Culture - INSAG

- “An established safety culture governs the actions and interactions of all individuals and organizations engaged in activities related to nuclear power”
- Defined as “the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants”

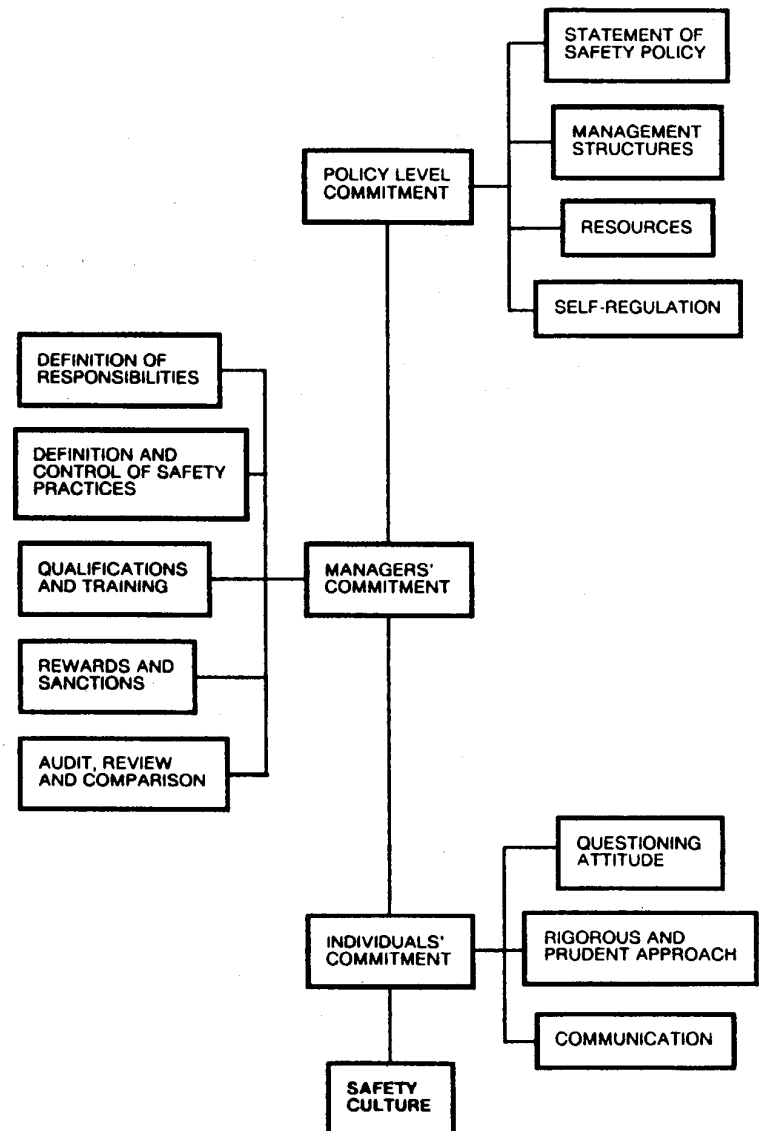


Safety Culture - Redefined

- “Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance”
- Easy to recognize & hard to quantify

Safety Culture Elements

- Attitudinal as well as structural
- Relates to both organizations and individuals
- Matches all safety requirements with appropriate perceptions and action



The logo graphic consists of a vertical black line on the left, a horizontal black line below the text, and a cluster of overlapping colored squares (yellow, red, blue) to the left of the text.

USNRC

- “A good safety culture in a nuclear installation is a reflection of the values, which are shared throughout all levels of the organization and which are based on the belief that safety is important and that it is everyone’s responsibility.”



More Definitions

- “Safety culture is what you do when the boss isn’t looking”
- “Safety culture is the way we do things around here”

Note that these definitions can also apply to a poor safety culture



INPO Warning Flags - 1

Overconfidence

- The "numbers" are good and the nuclear staff is living off past successes.

Isolationism

- There are few interactions with other utilities, INPO, and other industry groups.
- Benchmarking is seldom done or is limited to "tourism" without implementation.
- As a result, the plant is "behind the industry and doesn't know it."

Managing Relationships

- Mindset toward NRC/INPO is defensiveness or "do the minimum" - no bank account.
- Employees are not involved, not listened to, and raising problems is not valued.



INPO Warning Flags - 2

Operations and Engineering

- Operations standards, formality, and discipline are lacking.
- Plant operational focus is overshadowed by other issues, initiatives, or special projects.
- Engineering is weak (loss of talent) or lacks alignment with operational priorities.
- Design basis is not a priority and design margins erode over time.

Production Priorities

- Important equipment problems linger, and repairs are postponed while the plant stays on line.
- Nuclear safety is “assumed” but not emphasized in staff interactions and site communications.

Managing Change

- Organizational changes, staff reductions, retirement programs, or relocations are initiated before fully considering impact - recruiting or training is not used to compensate.
- Processes and procedures don't support strong performance after management changes.



INPO Warning Flags - 3

Plant Events

- Event significance is unrecognized or underplayed and reaction to events is not aggressive.
- Organizational causes of events are not explored.

Nuclear Leaders

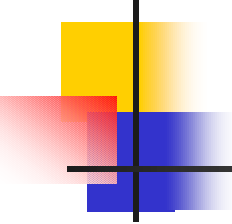
- Managers are defensive, lack team skills, or are weak communicators.
- Managers lack integrated plant knowledge or operational experience.
- Senior managers are not involved in operations and do not exercise accountability or follow-up.

Self-Critical

- Oversight organizations lack an unbiased outside view or deliver only good news.
- Self-assessment processes do not find problems or do not address them.

Stages of Organizational Decline (IAEA)

<i>Stage</i>	<i>Name of stage</i>	<i>Characteristic of stage</i>
1	Over-confidence	Good past performance leading to self-satisfaction
2	Complacency	Occurrence of minor events that are subjected to minimum self-assessment, and delay in improvement programmes
3	Denial	Number of minor events increases, with possibly a more significant event. These are treated as isolated events. Findings from audits are considered invalid. Root cause analysis not used.
4	Danger	Several potentially serious events occur but management and employees reject criticism from audits or regulator, by considering their views biased. The oversight function is afraid to confront management.
5	Collapse	Regulator intervenes to implement special evaluations. Management is overwhelmed and may need to be replaced. Major and very costly improvement needs to be implemented.



International Nuclear Event Scale (INES)

Level	Description	Criteria	Example
7	Major Accident	Large release, health effects, countermeasures	Chernobyl USSR, 1986
6	Serious Accident	Significant release, use emergency plans	Kyshtym, Russia, 1957 — waste tank explosion
5	Accident With Wider Consequences	External release, partial emergency plans, core damage	Windscale U.K. 1957; TMI, U.S. 1979



INES - 2

Level	Description	Criteria	Example
4	Accident with Local Consequences	Some core damage, large release within installation	Tokai Mura, Japan, 1999
3	Serious Incident	Contamination on site, high local exposure rate	Vandellos, Spain, 1989 – loss of safety systems due to fire
2	Incident	No damage, moderate exposure above limits, re-evaluation of safety	Forsmark, Sweden, 2008 – common cause electrical failure
1	Anomaly	Indicative of lack of safety provisions	Breach of operating limits




Passive Safety

- Evolutionary
 - CANDU 9 / ACR
 - CE System 80+
 - ABWR
 - EPR
- Advanced (passive)
 - AP-1000
 - ESBWR
 - Eskom PBMR



Utilities like
proven
designs



Utilities like
cheap designs
which seem to
be safer



Why Passive?

- Simplify the design and make it cheaper to build, operate and maintain
- Increase the real safety of the plant through systems which are less complex and more reliable, since they use 'natural' forces
- Increase the perceived safety of the plant



Characteristics of Passive Designs

- Use of natural forces (e.g., gravity, self-correcting neutronic feedback)
- De-emphasize systems which require large amounts of electricity (pumps), rapid automatic response, complex logic, or high energy



Definitions

- *Inherent safety* – eliminate hazard through fundamental design choice
 - Applies to characteristics, not reactor
- *Passive component* – no external input
 - Natural laws, properties of materials, stored energy
- *Fail safe* – specific failure leads to safe conditions
- *Grace period* – time during which safety function is assured without human intervention

Categories of Passive Safety

Characteristic	Category A	Category B	Category C	Category D
Signal Inputs of Intelligence	No	No	No	Yes
External power sources or forces	No	No	No	No
Moving mechanical parts	No	No	Yes	Either
Moving working fluid	No	Yes	Yes	Either
Example	Barriers such as fuel clad, containment; core cooling relying only on radiation or conduction to outer structural parts	Heat removal by natural circulation to heat exchangers in water pools, from the core or containment	Rupture disk or spring-loaded valve for overpressure protection; accumulator isolated by check valve	Shutdown System #1 and #2 in CANDU



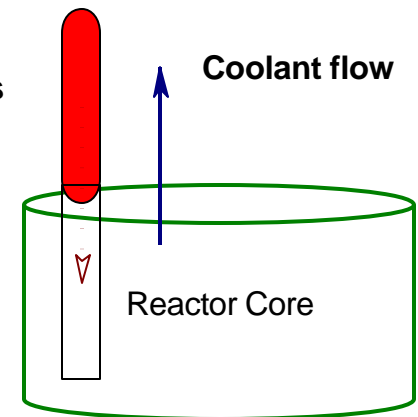
Passive Safety Functions

- Passive design – carry out the three safety functions in passive or pseudo-passive manner

Shutdown

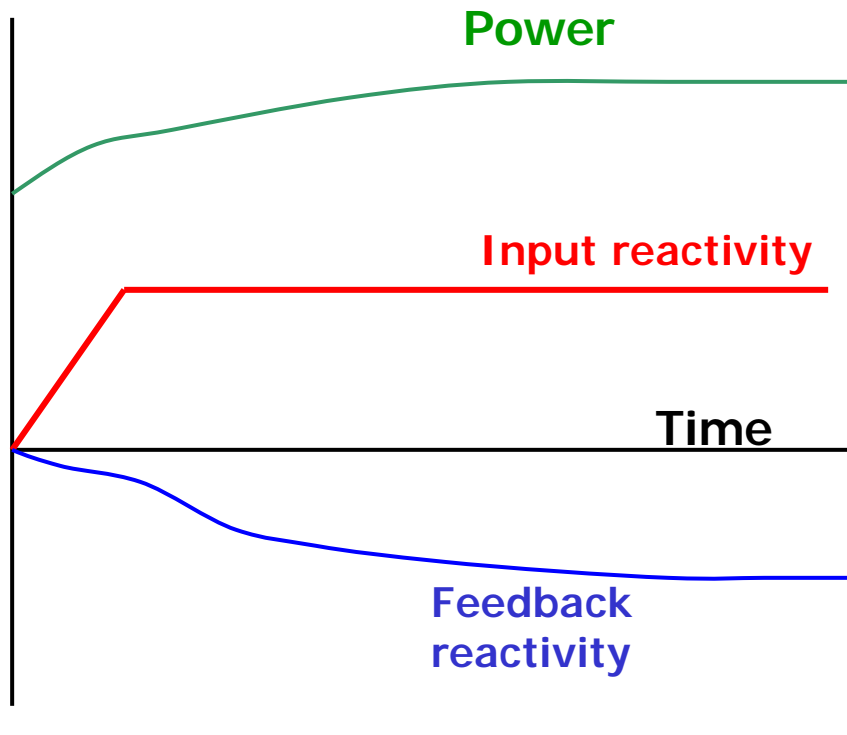
- E.g. 1: active actuation, passive execution (CANDU SDS)
- E.g. 2: Moving working fluid (SES-10)
- E.g. 3: Neutronic feedback (SLOWPOKE, LWR in LOCA)

One passive shutdown rod.
If the coolant temperature rises,
the absorber (shown in red) melts
and flows into
the reactor core



Neutronic feedback

Reactivity



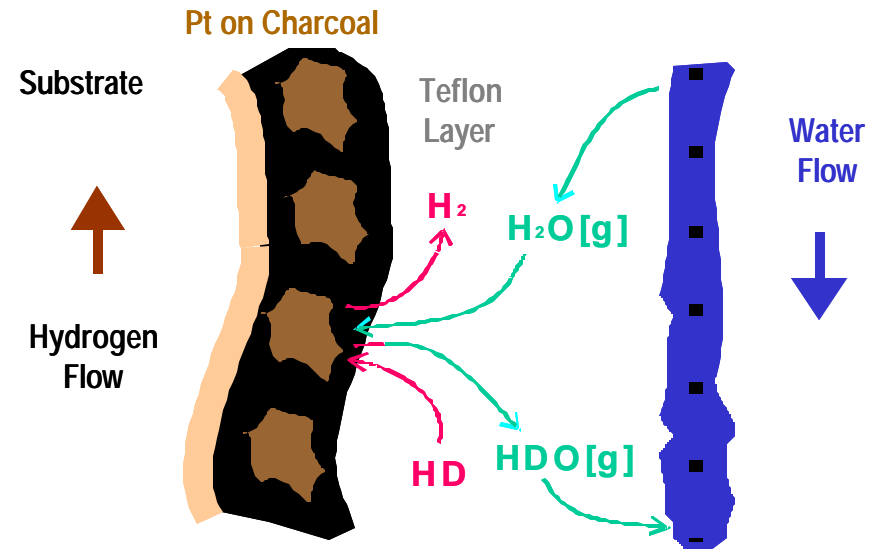


Remove Decay Heat

- Thermosyphoning to elevated heat sink
 - Need to depressurize core?
- Flood core & remove heat from containment
- Air cool core

Contain Fission Products

- Ventilation isolation
 - Passive *or* failsafe *or* normally isolated
- Decay heat removal
 - Elevated tank with HXs in containment
 - Use building structures
- Hydrogen removal
 - Passive auto-catalytic recombiners

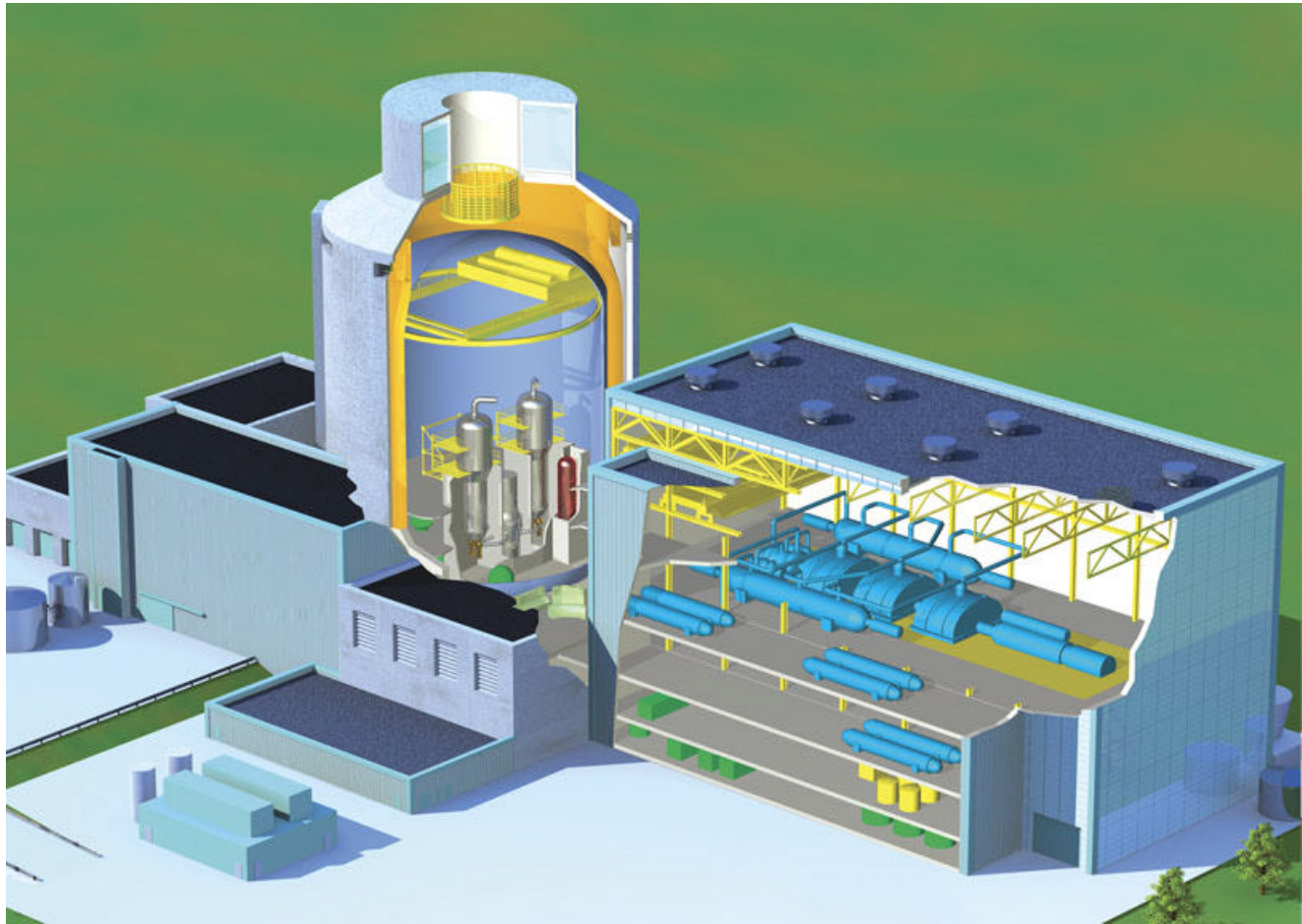




AP-1000

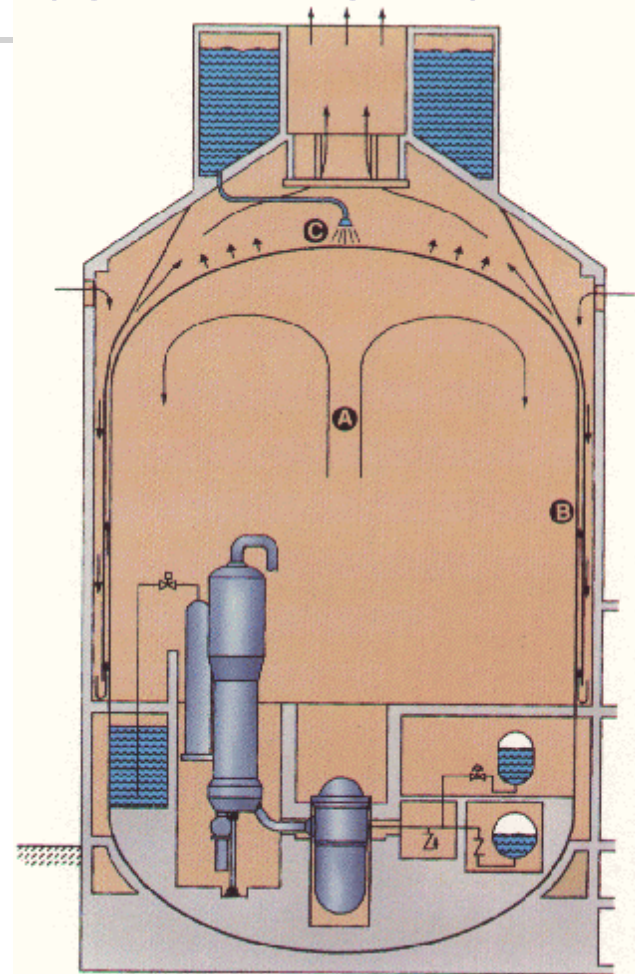
- Shutdown – conventional
- Decay heat removal – thermosyphoning to HX inside RWST, full pressure
 - Activated by fail-safe air-driven valves
- Small LOCA – primary side depressurization + gravity flood

AP-1000 Layout



AP-600/1000 Containment

- Double – inner steel, outer concrete
- Heat removal:
Natural air circulation + water spray from elevated tank onto steel shell



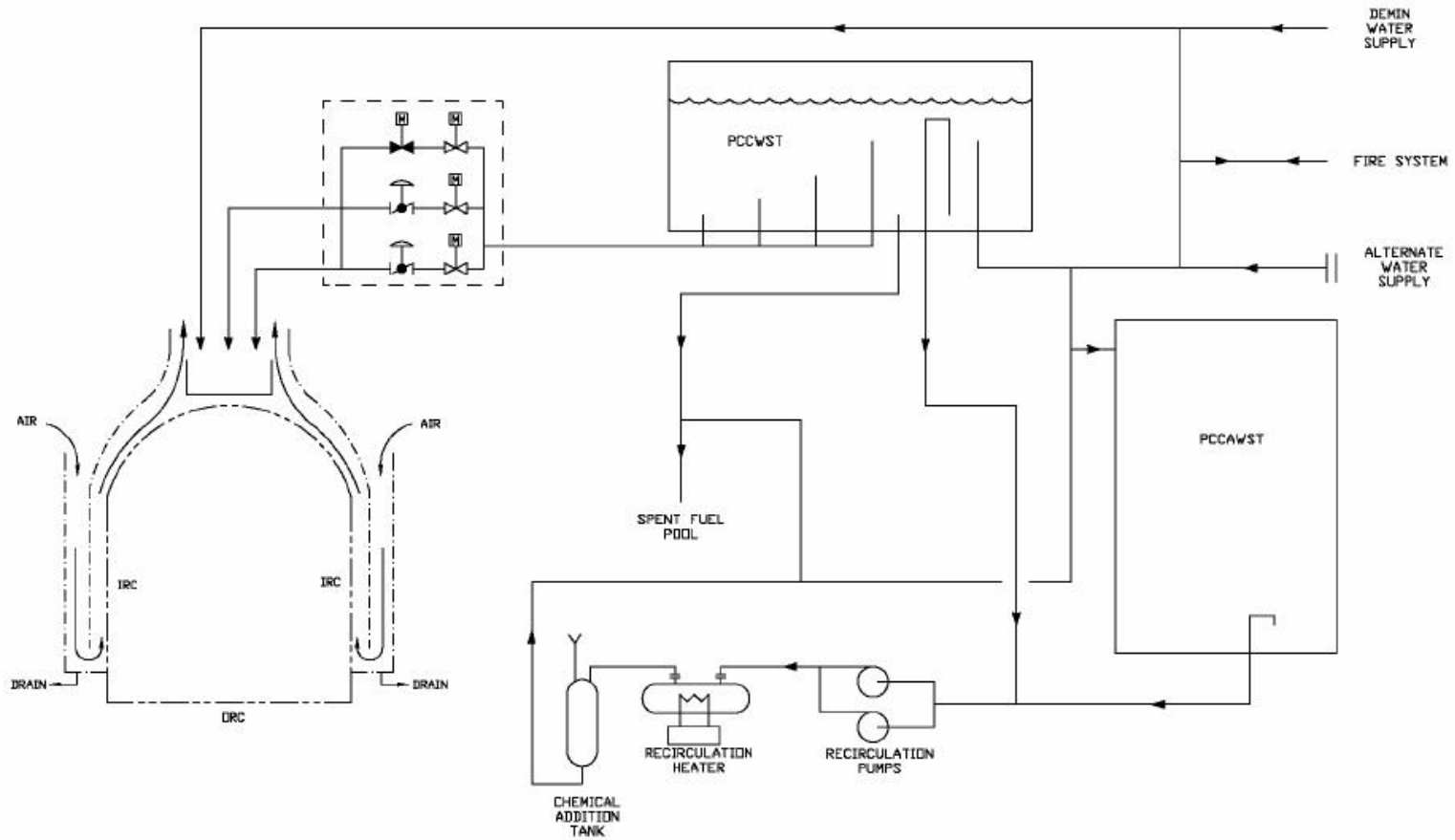


Figure 6.2.2-2

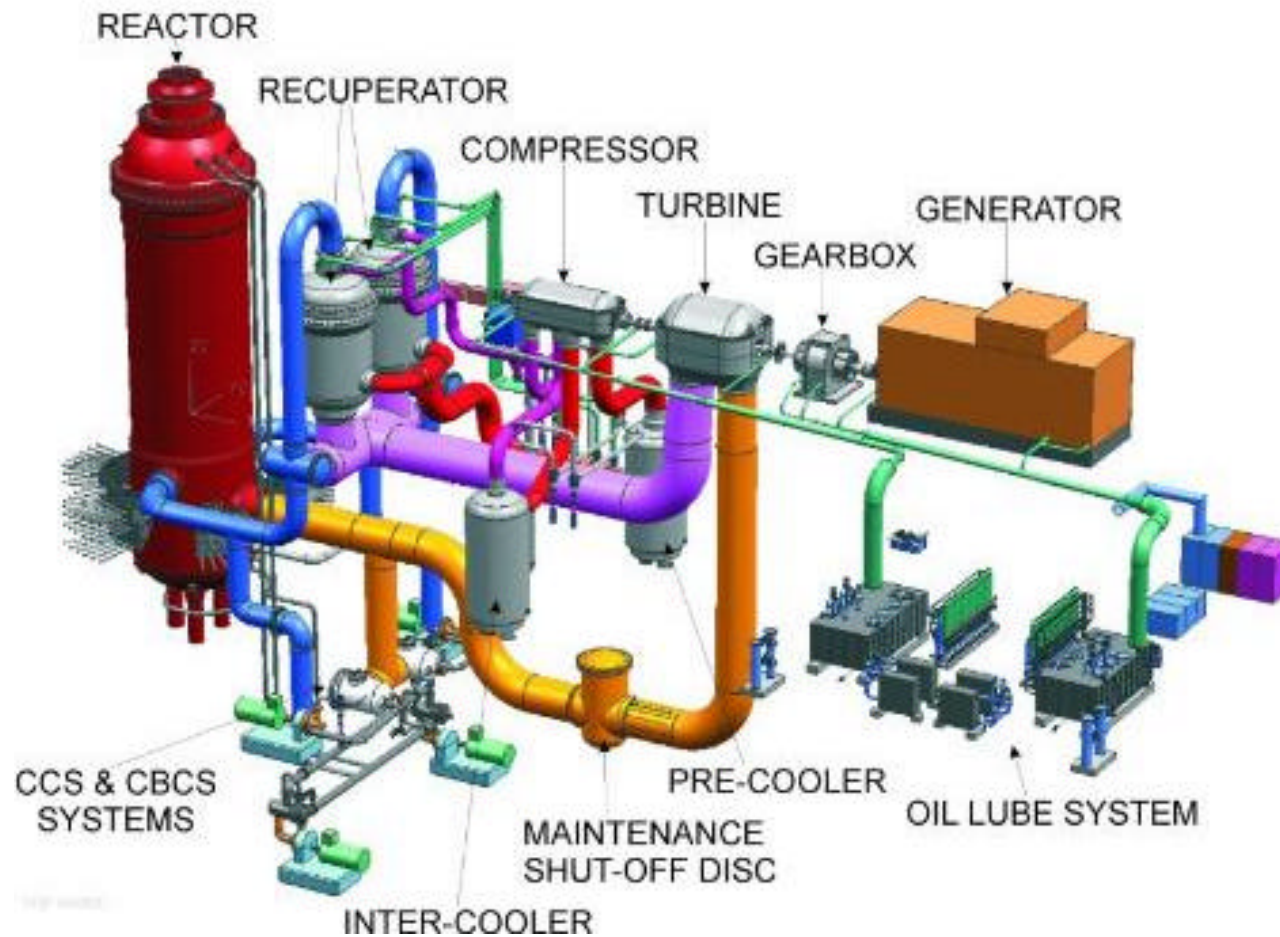
**Simplified Sketch of Passive
Containment Cooling System**

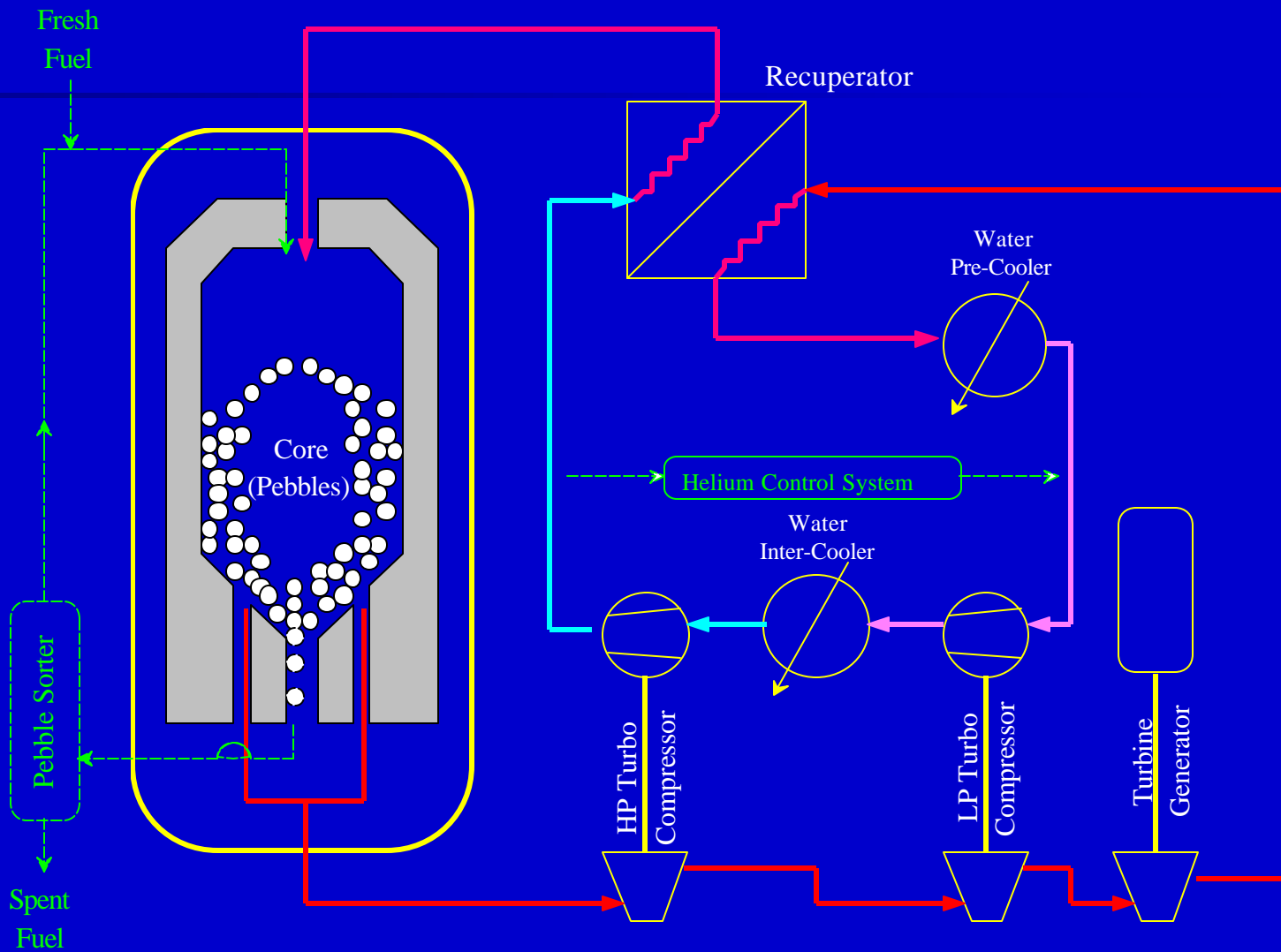
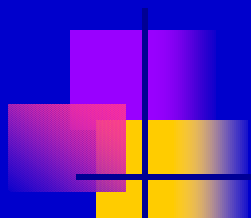


PBMR

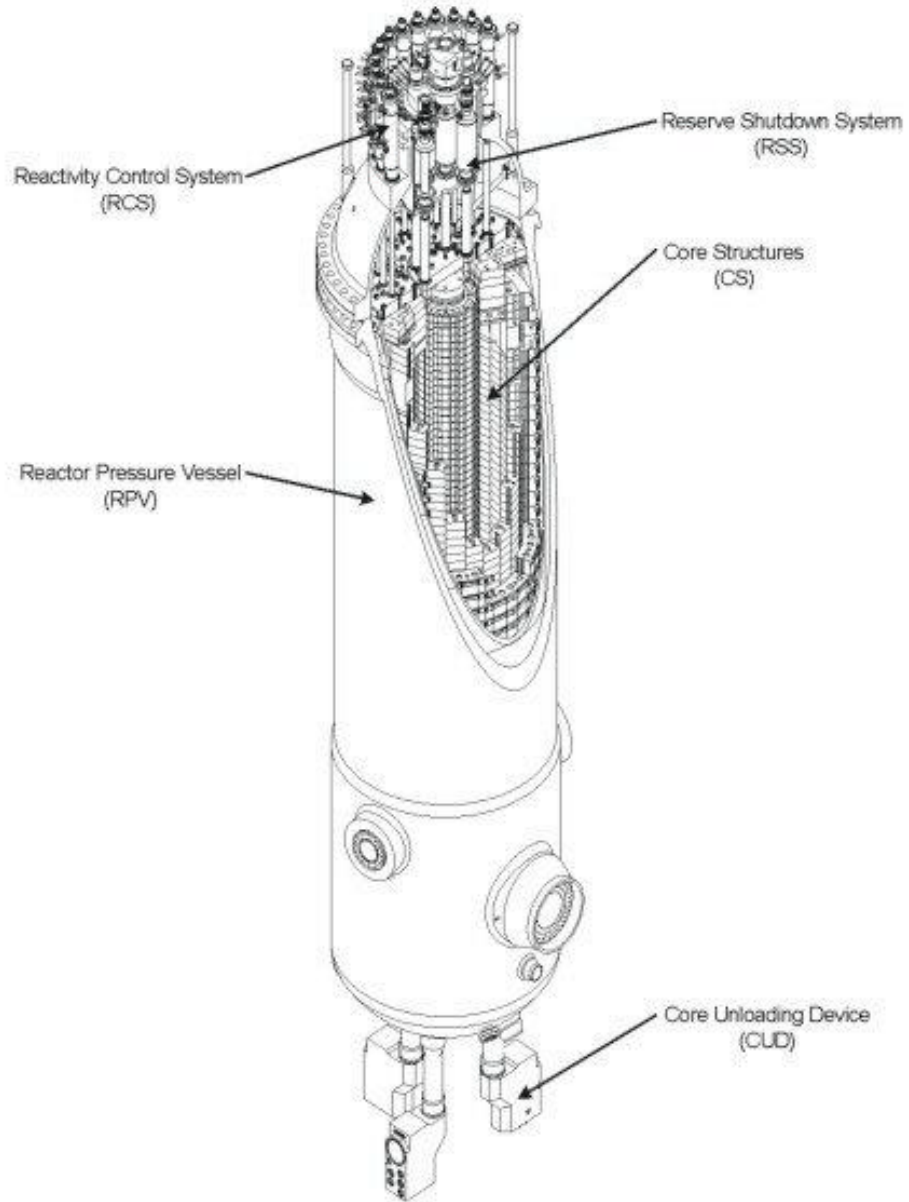
- Steel pressure vessel connected to gas turbine generator
- Helium coolant
- Particle fuel in graphite balls
- Graphite balls as moderator

PBMR layout





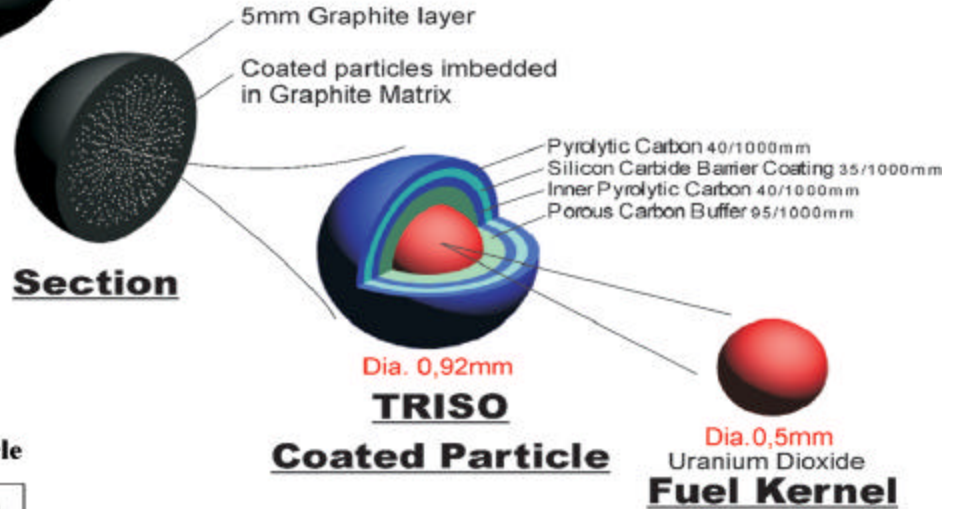
Pressure vessel



FUEL ELEMENT DESIGN FOR PBMR



Dia. 60mm
Fuel Sphere



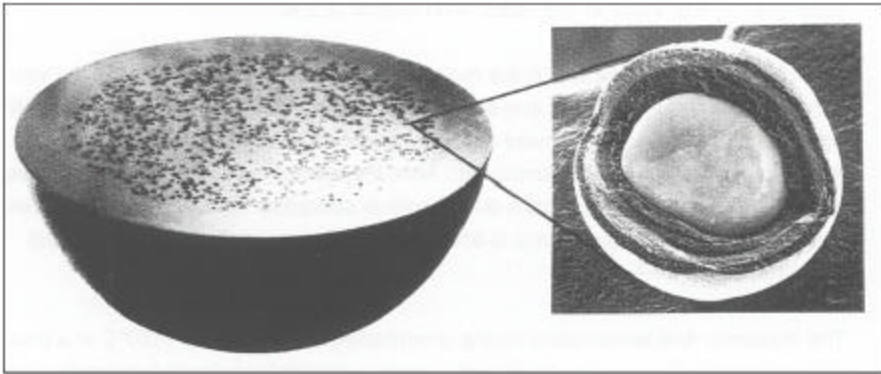
Section

Dia. 0,92mm
TRISO
Coated Particle

Dia. 0,5mm
Uranium Dioxide
Fuel Kernel

HTR Pebble Cross-section

Cut-away Coated Particle



Shutdown

- High temperature capability of fuel (1650C before failure of particles)
- Large negative feedback
- Power equilibrates





Decay Heat Removal

- Small excess reactivity due to on-line refueling
- Claim: equilibrium power can be removed to environment without fuel damage
- Aided by small reactor size (110 MWe per module)



Containment

- Gas-Cooled Reactors claimed not to need containment because of ability to remove heat via air circulation after a break
 - What about external events?
 - How do you prove the integrity of the particles?
 - What happens if air / water gets in?



Passive CANDU

- Vehicle for development of passive concepts, not a product
- Goal: prevent core damage using passive means
- Shutdown: conventional
 - Flow blockage, feeder stagnation: rapid detection & shutdown?

Decay Heat Removal

- Elevated tank: heat removal by natural circulation from:
 - Moderator (boiling)
 - Steam generators
 - Containment
- 2000 m³ gives 3 day capability
- Steams to atmosphere

- Primary Heat Transport System
- Passive Emergency Water System
- Steam Generator Heat Rejection
- Moderator Heat Rejection
- Hydrogen Recombiner

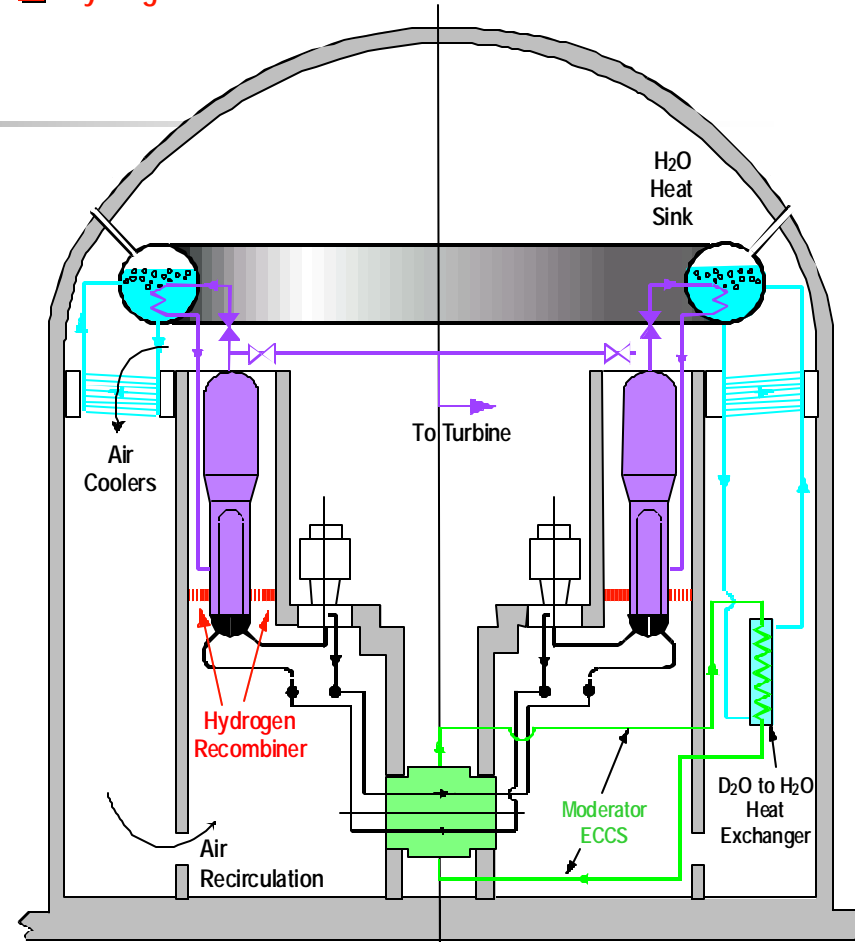


Figure 2



Containment

- Containment heat rejection through high inclined tube banks
- Compartmentalization enhances natural circulation
- Mixing of hydrogen, steam and air within the fuelling machine vault
- Hydrogen removal from the mixed stream as it exits the vault via catalytic hydrogen recombiners

Controlled Heat Transfer Fuel Channel

- Reduce heat losses to moderator in normal operation
- Increase heat losses in accident to prevent fuel damage

Controlled Heat Transfer Fuel Channel

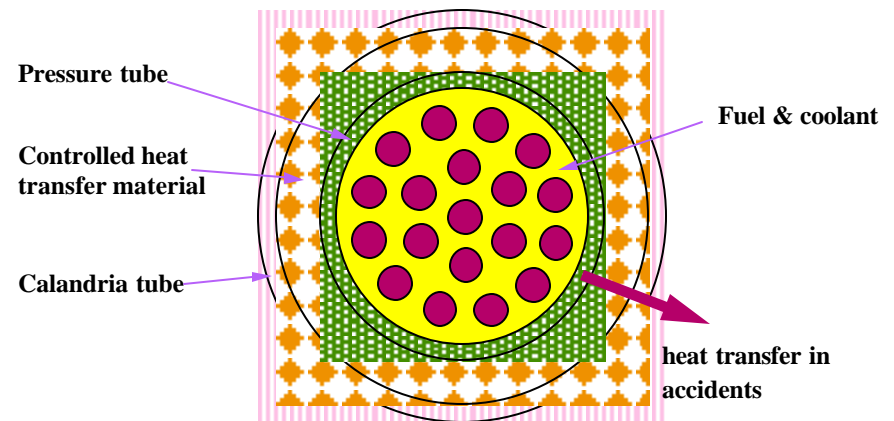
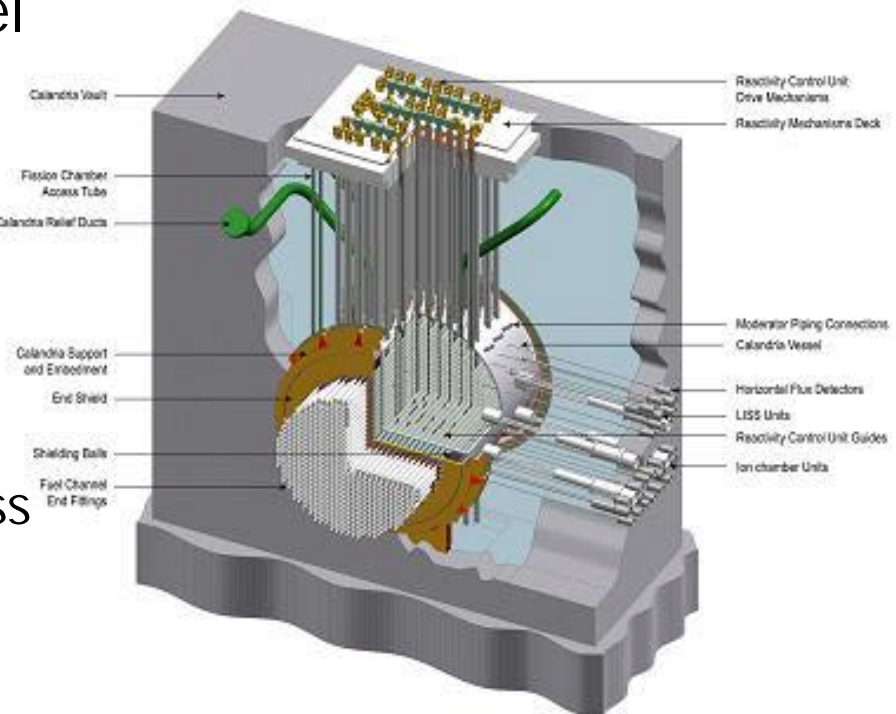


Figure 3

ACR – An Evolutionary CANDU

- Break with CANDU tradition – use LEU fuel ($\sim 2\%$ U^{235})
- Removes design constraints and allows economic optimization
 - Replace D_2O with H_2O coolant
 - Reduce lattice pitch (less moderator)
 - Increase PT thickness (higher operating pressure)





ACR-CANDU Comparison

Reactor	CANDU 6	Darlington	ACR-1000
Output [MWth]	2064	2657	3187
Coolant	Pressurized D ₂ O	Pressurized D ₂ O	Pressurized Light Water
Moderator	D ₂ O	D ₂ O	D ₂ O
Calandria diameter [m]	7.6	8.5	7.5
Fuel channel	Horizontal Zr-2.5wt%Nb alloy pressure tubes	Horizontal Zr-2.5wt%Nb alloy pressure tubes	Horizontal Zr-2.5wt%Nb alloy pressure tubes
Fuel channels	380	480	520
Lattice pitch (mm)	286	286	240

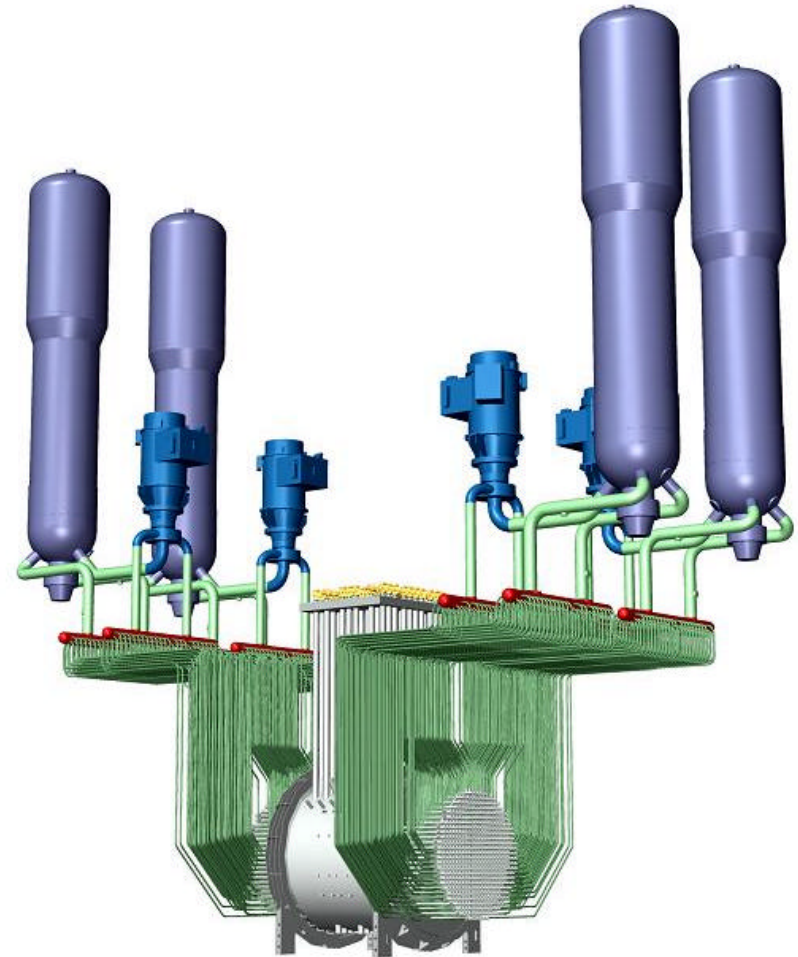


Fuel

	CANDU 6	Darlington	ACR-1000
Fuel	Natural UO₂	Natural UO₂	Low enriched UO₂
Enrichment level	0.71 wt% ²³⁵U	0.71 wt% ²³⁵U	Average ~2.0 wt% ²³⁵U
Fuel burn-up [MWd/Te U]	7,500	7,791	>10,000, target 20,000
Fuel bundle assembly	37 element	37 element	43-element CANFLEX®-ACR
Bundles per fuel channel	12	13	12
Fuelling Scheme	8-bundle-shift	4 & 8-bundle shift	2-bundle-shift

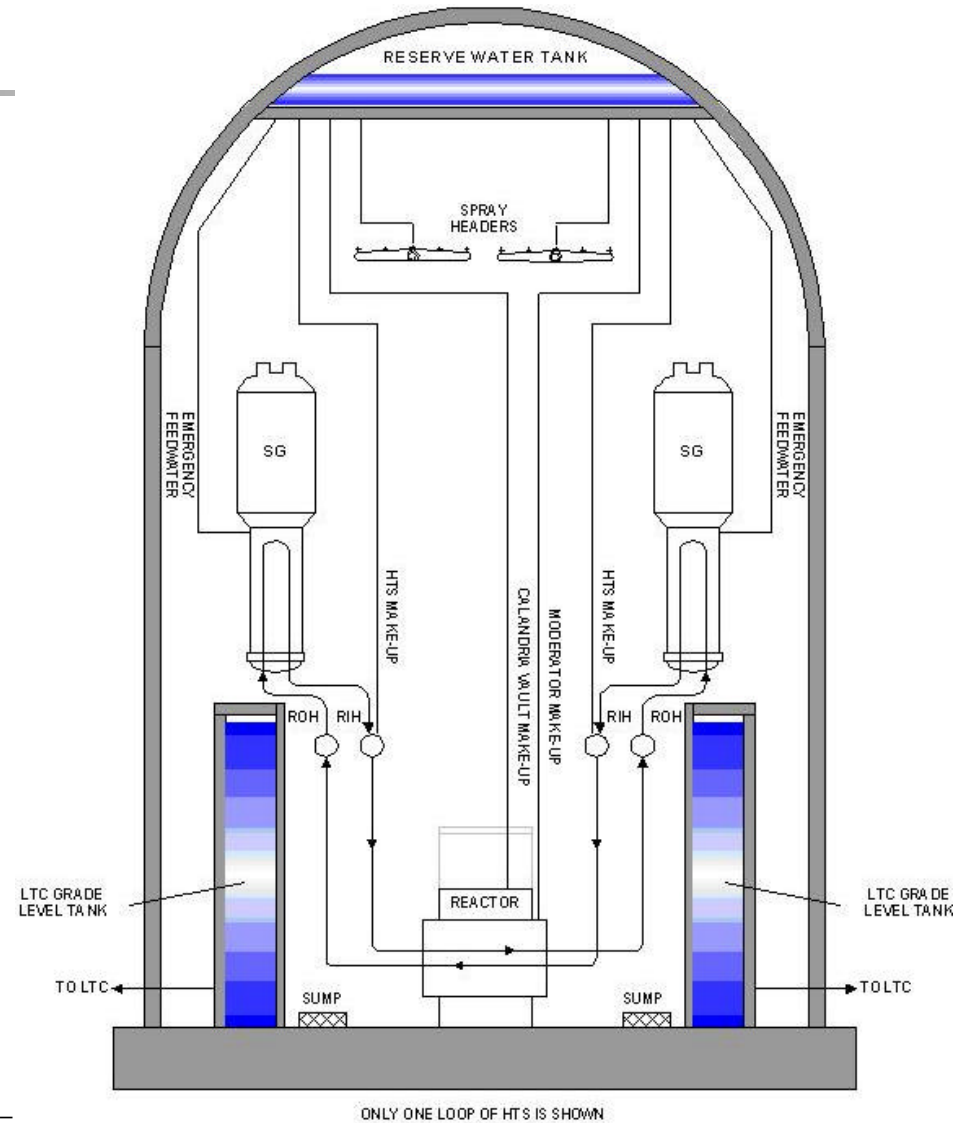
Safety Benefits

- Small (negative) void coefficient at design centre
- CT can withstand PT failure
- Channel failure shuts down reactor
- Core surrounded by 2 volumes of water



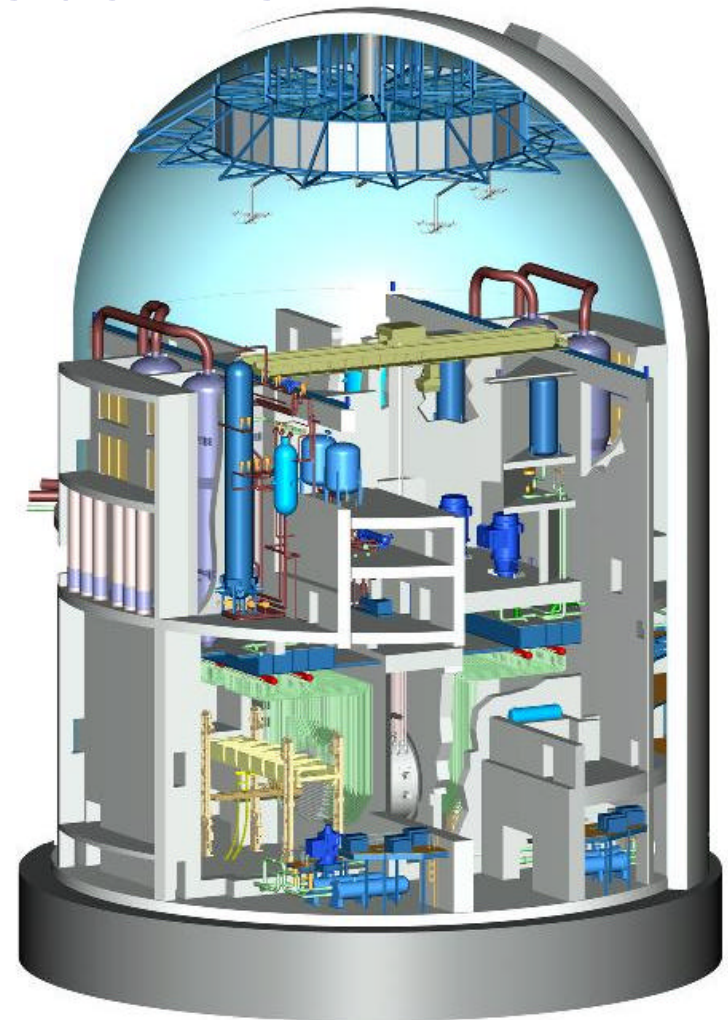
Reserve Water Tank

- Passive makeup to steam generators, heat transport system, moderator, shield tank



Other Safety Systems

- Dry steel-lined containment
 - Conventional active heat removal
 - Low flow spray
 - Passive auto-catalytic recombiners for hydrogen
- Conventional shutdown systems
 - Much reduced speed requirements





Conclusion

- Passive safety – simplicity, public appeal, aura of high reliability
- Evolutionary plants – enhanced safety, economic, less innovation risk
- Which direction do you think will be followed? And by whom?