Chapter 9b - Whither Safety? - Passive Designs

Evolutionary and Passive Designs

In the final part of this chapter, we shall be discussing some of the advanced (paper) designs which are proposed to make nuclear power safer, or at least appear to be safer. These designs fall into two categories: **evolutionary**, and **advanced**.

Evolutionary designs, as their name suggests, build on the operating experience of the current plants, and add those improvements warranted by experience. They are based on the principle that an operating utility strongly dislikes two things:

1. To buy a new design
2. To be the *only* utility to buy a new design.

Other than the Advanced CANDU Reactor (ACR™), we shall not cover evolutionary designs further - not because they are not important, but because they are not novel, and the science has been covered already in previous chapters.

Advanced designs use passive concepts in their operation and particularly with respect to safety. The original idea behind use of passive safety was to:

- simplify the design and make it cheaper to build, operate and maintain
- increase the *real* safety of the plant through systems which were less complex and more reliable, since they used 'natural' forces
- increase the *perceived* safety of the plant for the same reasons.

In its broadest sense, passive safety emphasizes the use of natural forces (gravity, self-correcting neutronic feedback) and de-emphasizes systems which require large amounts of electricity (pumps), rapid automatic response, complex logic, or high energy. However like Alice in Wonderland, passive safety in many cases means what the speaker wants it to mean, so that a clear definition of terms is a must. The best job was done by an IAEA working group in 1991, and we shall abstract and discuss some of their definitions[1] (two of which we introduced in the previous half of this chapter):

Definitions

Inherent safety refers to the achievement of safety through the elimination or exclusion of inherent hazards through the fundamental conceptual design choices made for the nuclear plant. This is in fact impossible for practical reactor sizes, since it requires elimination of systems (because they would not be needed) to remove or compensate decay heat, excess reactivity, and high energy releases. It is possible to have inherent safety for low-energy pool reactors such as the 20 kW (th) SLOWPOKE-2 - the total potential reactivity addition can all be compensated without fuel damage by the inherent negative feedback from fuel and coolant temperature, and the power at which this compensation is achieved can be absorbed indefinitely by the pool and the surroundings. Elimination of one or more of these hazards does, however, give a reactor an *inherently safe characteristic*. Note that the hazard must be eliminated deterministically, not probabilistically - for example a plant is inherently safe against fires if it has no combustible material.

A **passive component** does not need an external input to operate; a passive system is composed of passive components and structures. Ideally a passive system has no reliance on external mechanical or electrical power, signals or forces. It does rely on natural laws[a], properties of materials, and internally stored energy. Thus heat removal from a reactor by thermosyphoning to an elevated tank of water is passive, at least until the water runs out. In practice most 'passive' designs do allow active signals since there is usually a need to switch from active heat removal systems for full power operation, to passive decay heat removal systems after an accident. CANDU shutdown systems are passive in this respect: once they receive a signal, they actuate by gravity or stored energy.

An **active component** or system is one which is not passive.

Fail-safe means that a given failure leads to a safe conditions - the component or system is then fail-safe *with respect to that condition*. The fail-safe characteristic is specific to the failure mode: for example Shutdown System 2 in CANDU is fail-safe with respect to a loss of electrical power to the valves, but not to a loss of gas pressure.

Grace period is the period of time during which a safety function is ensured after an accident without the necessity for human intervention. Colloquially it is also termed "walk-away safe" for whatever grace period is involved - this has unfortunate connotations (operators are not expected to walk away from an accident) and is best not used. A grace period can be achieved through active or passive means - usually the first line of defence is assumed to function in determining grace period. Thus the grace period for a loss of feedwater in first generation CANDUs is about 30 minutes, since after that period the operator must manually valve in an alternate heat sink; for CANDU 9, it was extended to three days through use of automatic depressurization of the steam generators, followed by automatic connexion of the elevated reserve water tank to the steam generators. User (customer) requirements for modern reactors, evolutionary or passive, require a grace period of 3 days for most single failures.

[a] The author observes that even active systems still have to obey natural laws and respect the properties of materials

Categories of Passive Safety

Very few systems are totally passively safe. To recognize the range of possibilities, the IAEA defined four categories of passivity, summarized in the following table:

Table 9b-1 - Categories of Passivity

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**

For many passive designs, even those for which the "execution" is passive, the actuation may be by an electrical signal. Part of the justification is that such signals themselves are highly reliable and can use backup power from batteries if the main power fails. Note that even some valves can be actuated on battery power.

Passive Safety Desiderata

A passive design strives to ensure that the three major safety functions can be carried out in a passive or pseudo-passive manner. Recall these functions are: shut down the reactor, remove the decay heat, and contain any fission products. We describe in general terms how each of these might be accomplished, then examine a few passive designs for further detail.

Shut-Down the Reactor

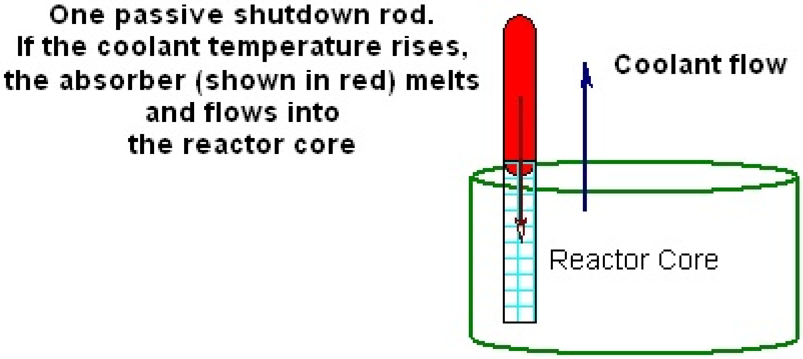
One passive shutdown rod.
If the coolant temperature rises,
the absorber (shown in red) melts
and flows into
the reactor core
Coolant flow
Reactor Core

Figure 9b-1 - SES-10 Second Shutdown System

As noted on several occasions, CANDU shutdown systems are passive in the sense that once they are actuated by a signal, the devices themselves are inserted into the core via gravity (shutoff rods) or stored energy (spring assist to the shutoff rods, and gas-driven poison injection). This places them into IAEA Category D above. More passive approaches could be developed based on change in material properties with temperature; recall that the SES-10 heating reactor had a second shutdown system consisting of tubes inserted into the reactor, with a low-melting-point neutron absorber within them, above the core (Figure 9b-1). This needs no external 'intelligence' but does have a moving fluid, placing it in Category B. Even more basic, fuel with a strong negative temperature feedback coefficient is certainly a passive form of reactivity compensation. If it truly shut down the reactor, it would be in Category A. However negative feedback does not necessarily shut down the reactor after, say, an inadvertent insertion of positive reactivity (control rod withdrawal) - it simply allows the power to rise and then equilibrate at a level where the negative reactivity due to the higher fuel temperature offsets the reactivity addition of the control rod. One still needs to be sure that the power can be removed somehow (by passive means) and that the fuel is not damaged. A strong negative coolant temperature feedback works the same way, but has the added concern that a fast insertion of cold water could cause a rapid power increase before the negative fuel or coolant temperature has time to compensate it. The SLOWPOKE 2 reactor dealt with this by physically limiting the *amount* of reactivity it was possible to add; SES-10 physically limited the *rate* at which it could be added, so the negative feedback had time to take effect. Note that shutdown in LWRs after a Loss of Coolant Accident is a "true" passive shutdown, as the loss of coolant also removes the moderator. As stated before, for every 'good' inherent safety characteristic, one can usually find a 'bad' one, especially in the power reactor range - so when the LWR core is refilled by ECC, the ECC has to be borated or the passive shutdown is reversed.

Remove Decay Heat

In passive designs, removal of decay heat from the fuel is normally done by thermosyphoning to an elevated heat sink, usually a heat exchanger in a large supply of water high up in the building. Alternatively the entire core and its surroundings can be flooded by pouring water by gravity from an elevated supply; the core heat is then turned to steam, which flows to and is removed passively from containment. In some but not all passive designs decay heat is removed at low pressure; thus some means of depressurizing the heat transport system is required first. This is done via a Category 'D' device, usually - intelligence is needed since depressurization in PWRs means opening valves on the primary side - i.e., creating a controlled small LOCA. CANDU offers some inherent advantages in this regard, as already stated - there are two large volumes of water around the core (the moderator and the shield tank), onto which one could engineer passive, low-pressure heat removal. Heat removal from the shield tank is only of interest for severe accidents, since by then the core geometry will have collapsed. The disadvantage of the moderator is that with current pressure-tube designs, the fuel will be severely damaged if the heat has to be taken out via the moderator.

Contain Radioactivity

The containment structure is already passive, category A. However there are a number of other containment functions for which a passive approach can be taken:

Ventilation Isolation

The building can simply be sealed during operation, or the isolation system can be Category D (e.g. a spring-loaded valve which fails closed on loss of signal).

Decay Heat Removal

This is an extension of core thermosyphoning. The idea is to get the heat into an elevated tank of water. So heat exchangers can be placed in the building, with the tube side connected to the tank and the shell side exposed to containment atmosphere. This requires two natural convection loops: one in the containment atmosphere, transporting heat from the core (e.g. steaming from a LOCA) to the heat exchangers; and one transporting heated water from the heat exchangers to the elevated tank. One interesting twist on this idea: the metal shell of the building becomes the heat exchanger, and the elevated tank trickles water down the *outside*.

Hydrogen Removal

Here passive autocatalytic recombiners can be used. These simply offer a catalyst-coated surface to the containment atmosphere and as the air/steam/hydrogen mixture flows through[b], the hydrogen and oxygen are catalytically recombined (Figure 9b-2).

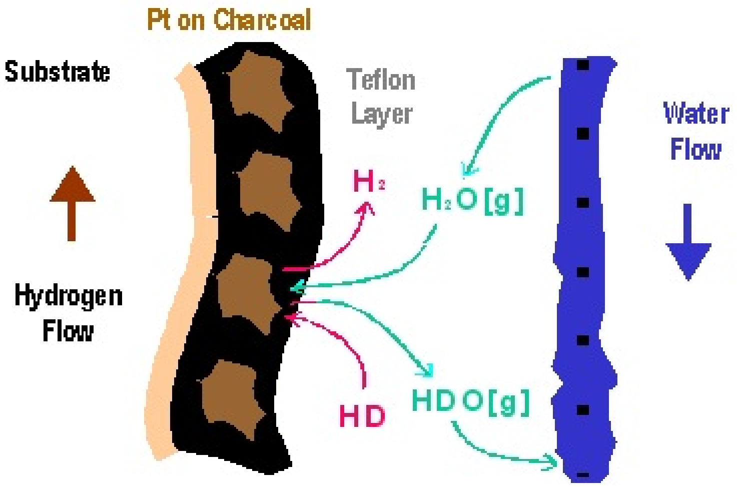

Figure 9b-2 - Hydrogen Recombination via Catalyst

We shall now consider three examples of designs with passive features - the Westinghouse AP-600/1000, passive CANDU, and the Eskom Pebble Bed Modular gas-cooled Reactor (PBMR). AP-1000s are under construction in China; the latter two are paper designs at this point. We shall concentrate just on their passive features to show how the ideas above are implemented.

AP-600/1000

The Westinghouse AP-600/1000 design is a PWR originally sized at 600MWe[c].

The combined control/shutdown system is relatively conventional.

Consider decay heat removal. PWRs have a large tank of cold water - the Refuelling Water Storage Tank (RWST), used to flood the core when it is shut down for refuelling. AP-600/1000 locates this tank inside containment and uses it for emergency decay heat removal[2]. Inside the RWST is a passive heat exchanger which is part of a full-pressure, closed, natural circulation loop connected to the reactor coolant system. The heat exchanger is activated by air-driven valves that open on loss of power. Thus decay heat can be removed passively.

The approach for small LOCA is interesting. As discussed previously, the conventional approach (in CANDU) is to provide a high-pressure Emergency Coolant Injection to prevent early fuel failures, then to depressurize the primary system through opening Main Steam Safety Valves *on*

[b] Implying that the recombiners must be placed within the containment atmosphere flow paths - hence they are a good fit to natural circulation containment concepts

[c] Unfavourable economy of scale has forced abandonment of this size; the current concept is 1000 MWe. The AP-1000 passive characteristics are similar.

the secondary side, to allow lower pressure injection in the longer term. Because the AP-600/1000 designers wanted to use a (passive) gravity-driven makeup from the RWST, and cooldown of the secondary side inserts positive reactivity as well as opening lines out of containment, there is an Automatic Depressurization System which depressurizes the *primary* cooling system into the RWST to get the pressure low enough - i.e., a deliberate small LOCA. ECC is then added by gravity.

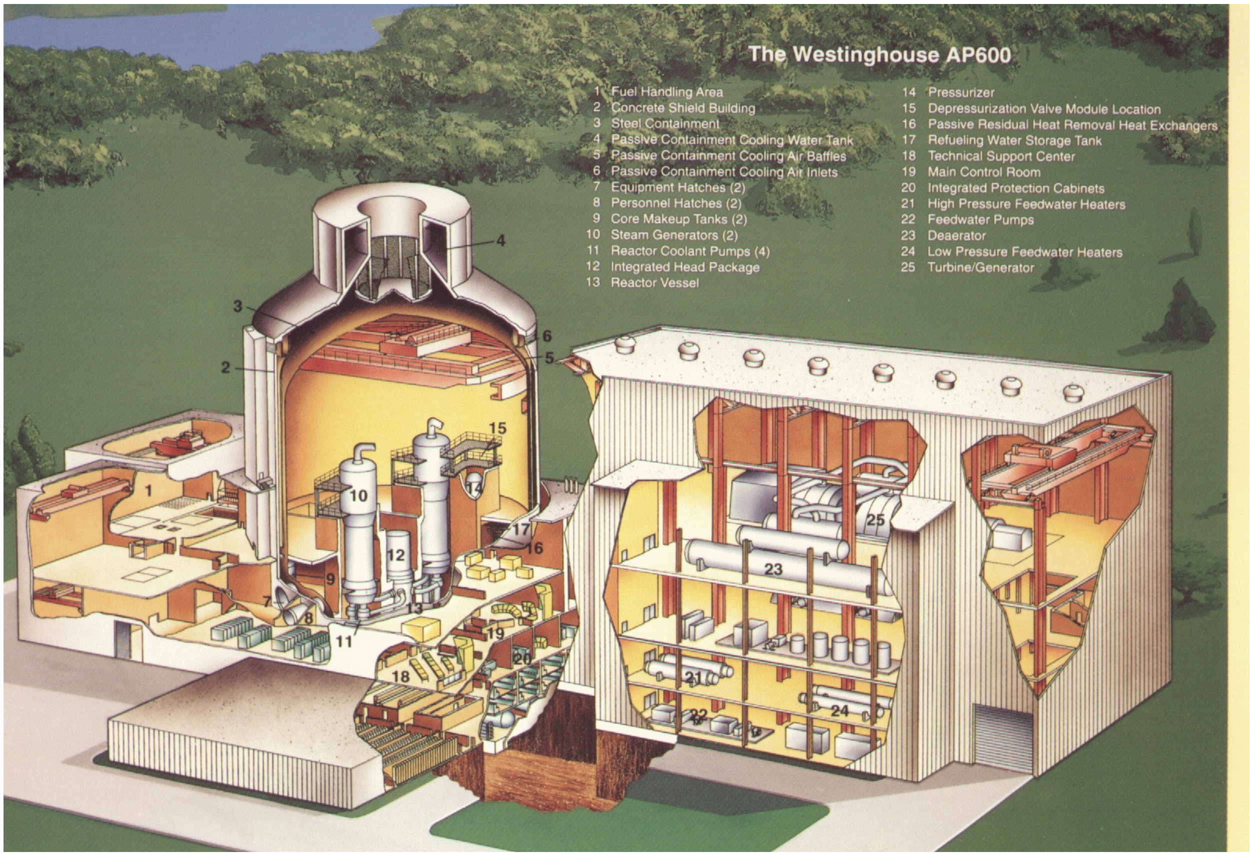
The Westinghouse AP600
1 Fuel Handling Area
2 Concrete Shield Building
3 Steel Containment
4 Passive Containment Cooling Water Tank
5 Passive Containment Cooling Air Baffles
6 Passive Containment Cooling Air Inlets
7 Equipment Hatches (2)
8 Personnel Hatches (2)
9 Core Makeup Tanks (2)
10 Steam Generators (2)
11 Reactor Coolant Pumps (4)
12 Integrated Head Package
13 Reactor Vessel
14 Pressurizer
15 Depressurization Valve Module Location
16 Passive Residual Heat Removal Heat Exchangers
17 Refueling Water Storage Tank
18 Technical Support Center
19 Main Control Room
20 Integrated Protection Cabinets
21 High Pressure Feedwater Heaters
22 Feedwater Pumps
23 Deaerator
24 Low Pressure Feedwater Heaters
25 Turbine/Generator
4
3
6
5
2
15
1
10
14
17
16
12
9
7
8
11
13
19
20
18
25
23
21
22
24

Figure 9b-3 - Overall Layout of AP-600

Containment is double, with an inner steel shell and an outer concrete shield building. Natural air circulation in the interspace provides heat removal, supplemented in accidents by draining water from an external elevated tank onto the steel shell.

Figure 9b-3 shows the overall layout[3] and Figure 9b-4 shows the containment heat removal system concept.[4]

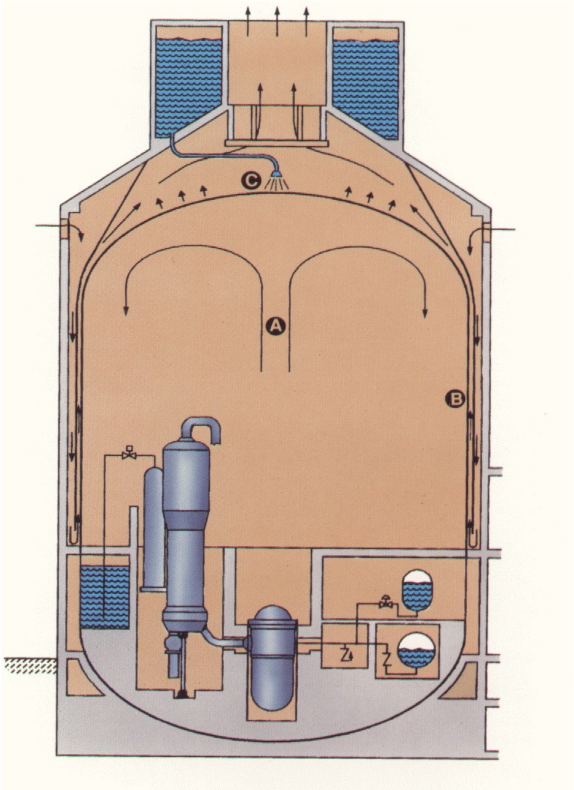

Figure 9b-4 - AP-600 Containment Heat Removal

PBMR

The Pebble Bed Modular Reactor is based on gas-cooled reactors developed in Germany. The following description is taken from the PBMR web sites[5]:

The PBMR consists of a vertical steel pressure vessel, 6.2 m. in diameter and about 27 m. high (Figure 9b-5), which is lined with 100 cm. thick graphite bricks. It uses coated particles of enriched uranium oxide (Figure 9b-7) encased in graphite to form a fuel sphere or pebble about the size of a tennis ball (Figure 9b-6). The fuel particles are coated with successive layers of porous carbon, pyrolytic carbon and silicon carbide. The porous carbon accommodates any mechanical deformation that the uranium oxide particle may undergo during the lifetime of the fuel. The pyrolytic carbon and silicon carbide layers are designed to contain the fuel and the radioactive decay products resulting from the nuclear reactions.

The uranium dioxide particles are less than half a millimetre in size. One fuel ball contains 15000 of them, totalling 9 grams of uranium.

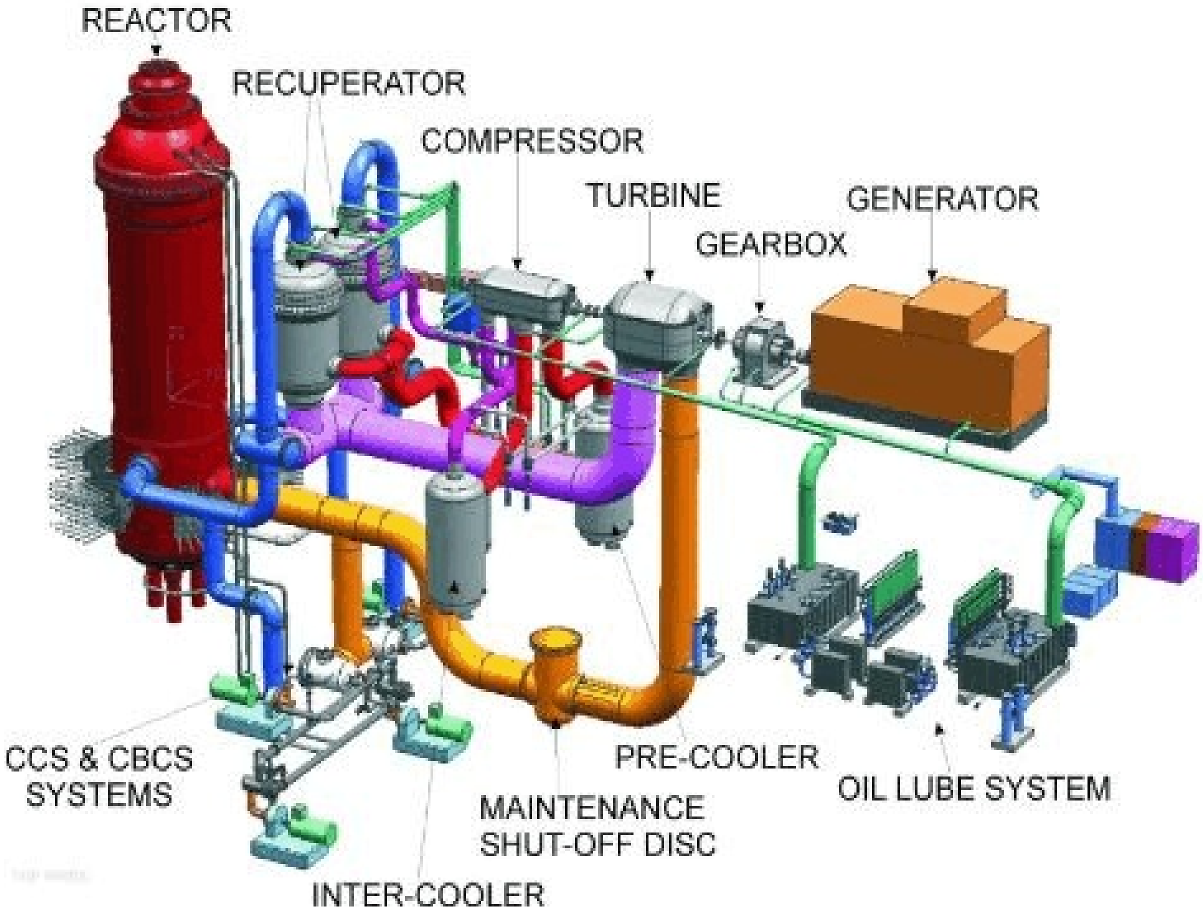

Figure 9b-5 - MPS Layout

During normal operation, the pressure vessel contains a load of 450000 fuel spheres. The rest are pure graphite balls which serve the function of an additional nuclear moderator.

Figure 9b-6 - Graphite Balls Containing Fuel Particles

Helium is used as the coolant and energy transfer medium to a closed cycle gas turbine and generator system.

To remove the heat generated by the nuclear reaction, helium gas at 500ºC enters the pressure vessel at the top. It then moves down between the hot fuel balls, after which it leaves the bottom of the vessel having been heated to a temperature of 900ºC. The hot gas then passes through a closed cycle gas turbine system to drive an electrical generator before being returned to the reactor.

In terms of shutdown, it is claimed[d] that because of the large negative temperature feedback of the TRISO fuel particles, and the ability of the fuel to withstand very high temperatures (1650C) without failure, the equilibrium power reached in an accident can be dissipated to the environment without fuel damage. This is aided by the relatively small unit size (110 MWe). Like CANDU, the excess reactivity available during operation is small, due to the continuous refuelling.

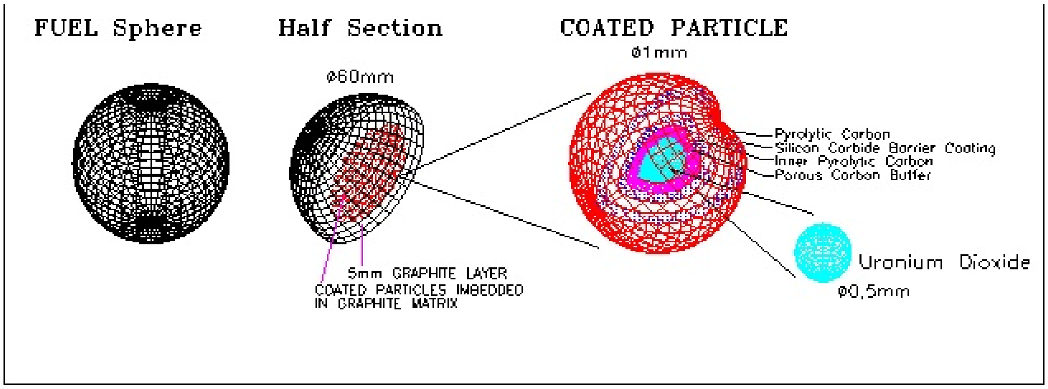

Figure 9b-7 - PBMR Fuel Particle

[d] As with any paper design, unless it has had rigorous review as part of a 'live' licensing application, claims should be regarded skeptically until independently verified.

Similarly in terms of decay power removal, it is stated that this can likewise be rejected to the environment.[6]

Containment is not described; previous gas-cooled reactor designs have been argued not to need a containment because of the ability to cool the fuel via natural circulation of gas, even after a loss of gas pressure. Note however that containment performs the function of a physical barrier against external events, both man-made and natural.

Passive CANDU

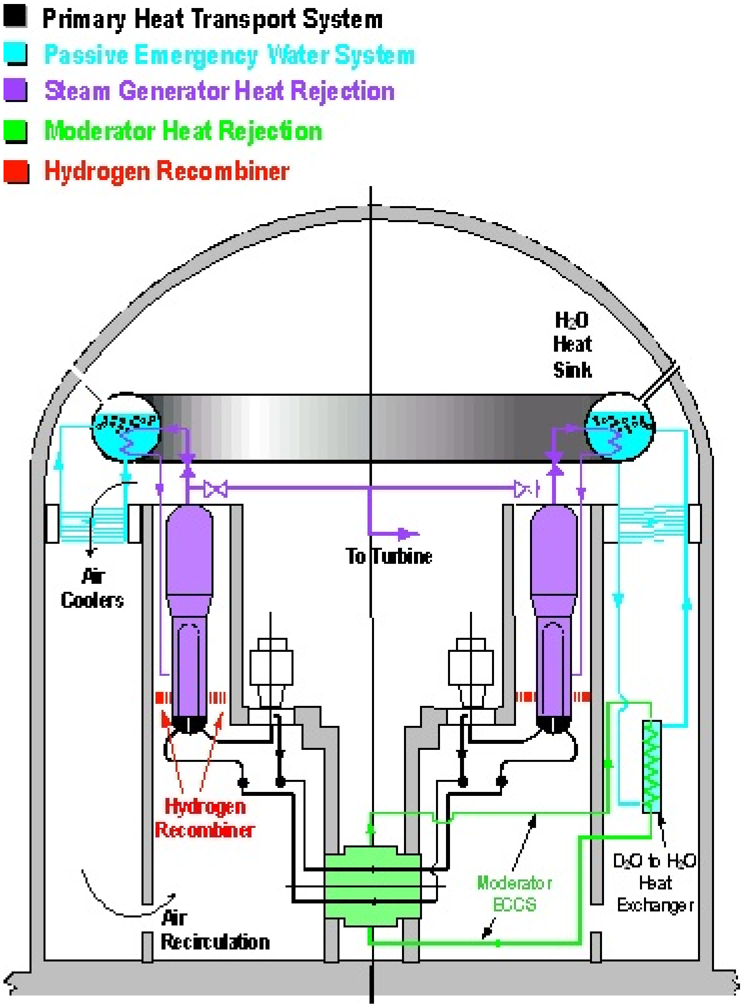
■ Primary Heat Transport System
■ Passive Emergency Water System
■ Steam Generator Heat Rejection
■ Moderator Heat Rejection
■ Hydrogen Recombiner
H_2O Heat Sink
Air Coolers
To Turbine
Hydrogen Recombiner
Air Recirculation
Moderator ECCS
D_2O to H_2O Heat Exchanger

Figure 2

Figure 9b-8 - Passive CANDU

The Passive CANDU is a vehicle for developing passive safety concepts rather than an actual project design. As these concepts mature, they are incorporated into the mainstream CANDU products.

In the passive CANDU[7,8], control and shutdown are conventional. Single channel events (flow blockage, feeder stagnation break) are a challenge to prevention of fuel damage for design basis events, since in current CANDUs the damage occurs before shutdown; very quick detection and shutdown is one possibility.

However decay heat removal from the reactor and from the containment are both passive. The elevated Reserve Water Tank in CANDU 9 and ACR has become a general purpose passive emergency water system (PEWS), for containment cooling, decay heat removal and/or emergency depressurization of the steam generators, and for the moderator in its role as a backup to the emergency core cooling system. The moderator role is augmented by a controlled heat transfer fuel channel, which allows passive heat removal from the fuel to the moderator at lower fuel temperatures than current CANDUs. Figure 9b-7 shows the concept.

The PEWS heat sink consists of a vented water pool in the containment dome. Its 2000m^3 volume can accept decay heat for three days via boil-off to atmosphere.

Steam generator depressurization (for a LOCA or steam line break) is effected via blow-down to heat exchangers in PEWS. The condensate returns by gravity with no secondary side makeup needed. There is no direct steam discharge to atmosphere. For cases where there is no break, steam generated by reactor decay heat can be rejected to these heat exchangers for up to three days.

Containment heat rejection is through tube banks high in the containment. They are cooled by natural circulation to the PEWS tank, and are inclined to give a preferential flow direction for the water or steam. As shown on the figure, an annular region in containment, and the large elevation difference between the heat source and the heat sink, enhances the natural circulation produced by these tube banks and naturally separates the upward and the downward atmospheric flows. The same flow patterns give good mixing of hydrogen, steam and air within the fuelling machine vault and effective hydrogen removal from the mixed stream as it exits the vault via the steam generator enclosure where catalytic hydrogen recombiners are positioned. Single-pass hydrogen recombination efficiencies of ~80% reduce hydrogen concentrations to less than flammability levels at containment locations outside the vault.

Moderator heat rejection is through a boiling-by-flashing natural-circulation D_2O loop to a natural circulation H_2O loop connected directly to the PEWS tank. The moderator is allowed to run near saturation (so that its heat can be used to improve station thermal efficiency through feedwater preheating).

To avoid fuel damage for all design basis accidents, however, the heat transfer path from the fuel to the moderator in the absence of coolant within the fuel channel has to be enhanced. Current CANDUs can

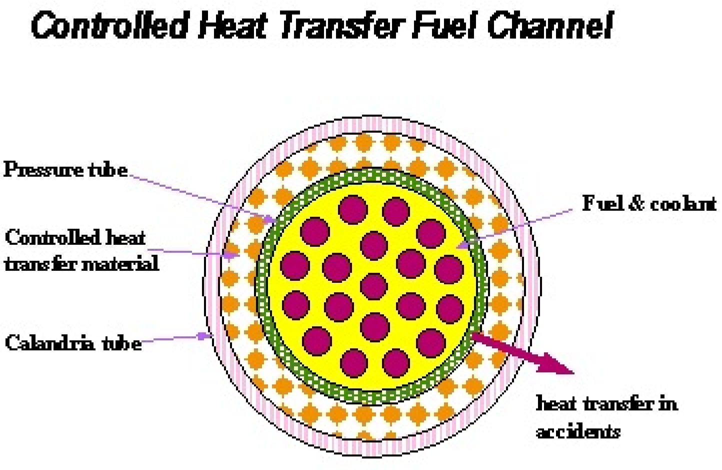
Controlled Heat Transfer Fuel Channel
Pressure tube
Controlled heat transfer material
Calandria tube
Fuel & coolant
heat transfer in accidents

Figure 3

Figure 9b-9 - Controlled Heat Transfer Fuel Channel

reject decay heat in this fashion without UO_2 melting, but the fuel would be severely damaged. Work has therefore focussed on replacing the annulus gas (between the pressure tube and the calandria tube) with a material which is resistant to heat transfer under normal operation (so as to minimize heat losses to the moderator) but is conductive at high temperatures typical of accidents (Figure 9b-9).

An Evolutionary Design - The Advanced CANDU Reactor[9]

Since this course does emphasize CANDU safety, it is appropriate to summarize AECL's newest design - the Advanced CANDU Reactor (ACR). It is primarily an evolutionary design with some passive systems taken from the Passive CANDU described above.

ACR's main break with CANDU tradition is the use of slightly enriched uranium fuel (SEU - about 2% U^{235}), instead of natural uranium fuel. This removes a number of design constraints which were previously set by the need for neutron economy, and frees them up for optimization based on economics. For example, the heavy-water coolant can now be replaced by light-water (impractical in a natural uranium design), giving significant cost savings. Not as much (heavy-water) moderator is required, so the core lattice pitch can be reduced, again saving heavy-water (Figure 9b-10). The pressure-tube thickness can be increased without as much concern about the increased parasitic neutron absorption, so the coolant pressure and temperature can likewise be increased, for increased thermal efficiency.

Figure 9b-10 - Comparison of ACR & CANDU Design

Reactor	**CANDU 6**	**Darlington**	**ACR-1000**
Output [MWth]	2064	2657	3187
Coolant	Pressurized D_2O	Pressurized D_2O	Pressurized Light Water
Moderator	D_2O	D_2O	D_2O
Calandria diameter [m]	7.6	8.5	7.5
Fuel channel	Horizontal Zr-2.5wt%Nb alloy pressure tubes with modified 403 SS end-fittings	Horizontal Zr-2.5wt%Nb alloy pressure tubes with modified 403 SS end-fittings	Horizontal Zr-2.5wt%Nb alloy pressure tubes with modified 403 SS end-fittings
Fuel channels	380	480	520
Lattice pitch (mm)	286	286	240

.

The economic optimization has some safety benefits. The reduced amount of heavy water moderator allows reduction in the void reactivity coefficient. As far as safety is concerned, the ‘best’ coefficients are small - whether positive or negative - since as we have pointed out, for every accident which benefits from a positive sign, there is one which is worsened. A small coefficient reduces the demands on the protective and mitigating systems for the case where its sign worsens the accident, at the price of reducing the benefit for accidents where its sign is compensatory. Hence the absolute value of the full core void reactivity in ACR has been selected to be <5 mk. For business reasons (foreign licensability - there is no restriction on the sign of the void reactivity in Canada), the sign has been chosen to be negative.

The ability to tolerate an increase in parasitic absorption has allowed the designers to increase the thickness of the calandria tube, to the extent that it will in all probability be able to withstand a pressure-tube failure. Besides providing the operating utility with increased protection against economic loss, containment of a pressure-tube rupture in the channel is an important safety benefit, since it challenges far fewer components and systems. Note that should both pressure-tube and calandria tube fail, however, the injection of light water into the moderator will shut ACR down - compared to CANDU Classic where injection of ‘clean’ D_2O coolant into a poisoned moderator sets the reactivity depth requirements for the shutdown systems.

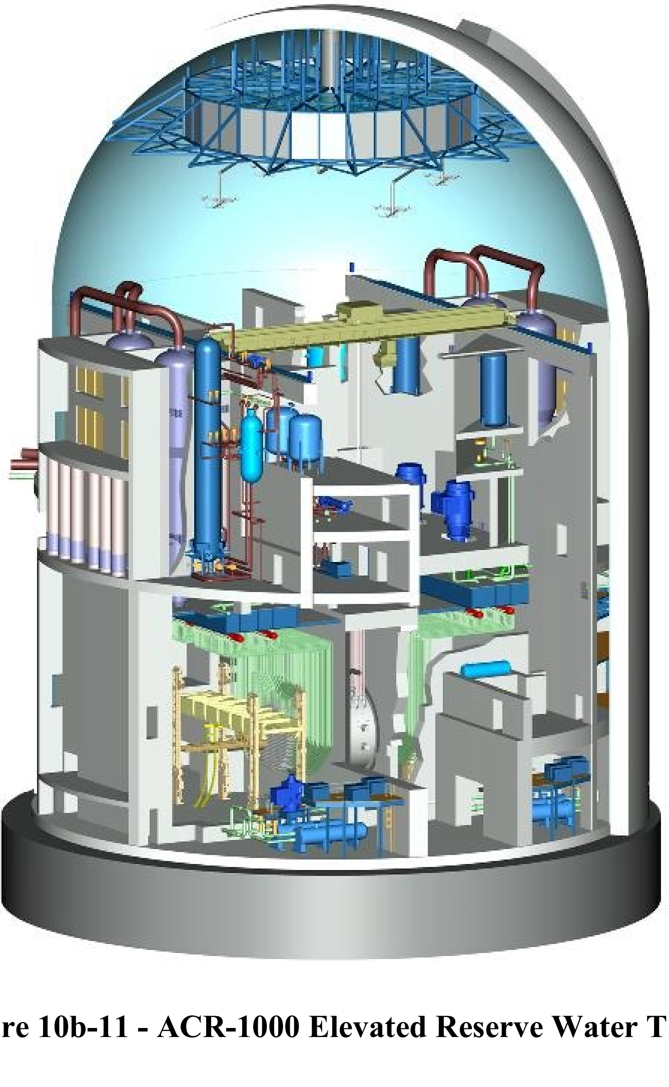

Figure 10b-11 - ACR-1000 Elevated Reserve Water Tank

In terms of passive safety, the ACR has adopted the elevated Reserve Water Tank (RWT) design from CANDU 9 and the Passive CANDU (Figure 9b-11). The tank can provide water by gravity, for at least a day's worth of decay heat removal, to the steam generators, the primary coolant system, the moderator and the shield tank. In an emergency with no other heat sinks, the operator's first choice would be to route it to the steam generators (as long as the heat transport system (HTS) was intact); with a pipe break in the HTS and no ECC, the choices would be to supply RWT water to the HTS, the moderator, and the shield tank, in that order, and depending on the core state when the RWT was brought in. As with the passive CANDU, this takes advantage of replenishing the existing sources of water surrounding the core.

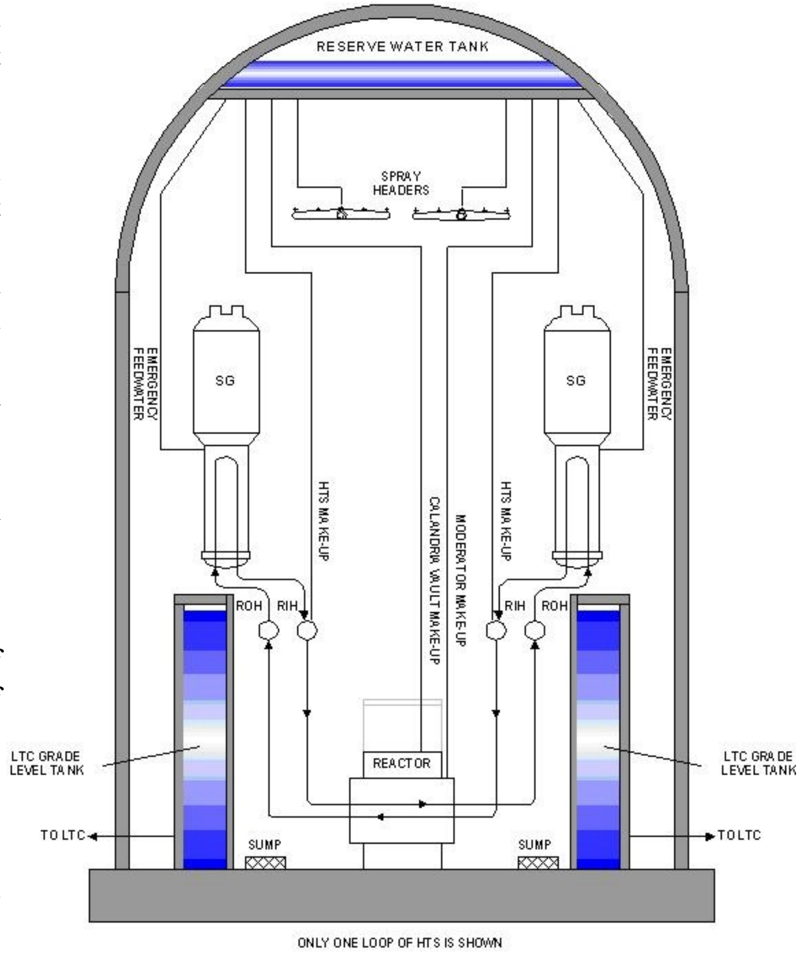

Figure 9b-10 - ACR Emergency Makeup

The containment is a dry steel-lined single unit containment. Although there is a spray system for long-term pressure control, there is no huge pressure-suppression system such as dousing - hence the need for a steel liner and higher design pressure to ensure low leakage after a pipe break. This approach is new for CANDU but has been used previously for some LWRs. Containment heat removal after an accident is conventional, with redundant active air coolers. Hydrogen removal from containment is however passive, using the Passive Autocatalytic Recombiners described previously. Shutdown systems are also conventional, although the need for *fast* shutdown for safety is clearly reduced.

Conclusion

This last Chapter has indicated the direction safety *may* take in the future.

Passive safety is attractive because of its simplicity, public appeal, and aura of high reliability.

Evolutionary designs have also incorporated safety enhancements while both remaining economic and posing less of an ‘innovation’ risk to customers.

Once adequate (or even more than adequate) safety is achieved, factors such as economics and provenness may become the determinants of the choice of technology, particularly as electricity markets become more deregulated. Or perhaps passive safety with its promise of reliance only on natural forces will prevail.

What do you think?

Exercise

1. Compare AP-1000, passive CANDU and Eskom Pebble-bed designs as follows: For each of the systems performing the fundamental safety functions (shut-down, cool, contain radioactivity), categorize them as passive A, B, C, or D as per Table 9b-1 (give reasons).

References

1. “Safety Related Terms for Advanced Nuclear Plants” IAEA-TECDOC-626, September 1991.

2. T. Anderson, “An Overview of the AP-600 Design”, American Nuclear Society Summer Conference, 1993.

3. “The Westinghouse AP600", Westinghouse Corporation, undated brochure.

4. H.J. Bruschi, “Westinghouse AP600 - Executive Summary”, Westinghouse Corporation, undated brochure

5. PBMR Web Sites, http://pbmr.co.za, February 2001.; and http://www.pbmr.com/, February 2008.

6. Kelvin Kemm, “Development of the South African Pebble Bed Modular Reactor System”, The Uranium Institute, 24th. Annual International Symposium, 1999.

7. N.J. Spinks and V.G. Snell, “CANDU Safety: Evolution and Recent Advances”, Fifth International Topical Meeting on Nuclear Thermal Hydraulics, Operations & Safety (NUTHOS-5), Beijing, China, April 13-16 1997.

8. V.G. Snell, M. Bonechi, W. Kupferschmidt, “Advances in CANDU Nuclear Safety”, Presented at PBNC 2000, Seoul, October 29 - November 2, 2000.

9. “An Evolution of CANDU - ACR-1000 Technical Summary”, AECL report 115-01372-230-001, Rev. 0, February 2006.