Committee I
The Nuclear Option in the Past,
Present and in the Future

DRAFT--6/15/92
For Conference Distribution Only

NUCLEAR SAFETY FOR NUCLEAR ACCEPTANCE

by

Kåre Hannerz
Chief Scientist, Retired
ABB Atom
Västerås, SWEDEN

The Nineteenth International Conference on the Unity of the Sciences
Seoul, Korea
August 19-26, 1992

NUCLEAR SAFETY FOR NUCLEAR ACCEPTANCE

Abstract

Well managed, nuclear power could make an important or even decisive contribution to an economic future energy supply for an expanding world population with much less negative impact on the environment than practically available alternatives.

However as is well known, public aversion threatens to greatly reduce or even eliminate this contribution. The prevalent public conviction seems to be that because of inherent human fallibility nuclear power will inevitably lead to unacceptable contamination of the environment with radiation from reactor accidents (or leaking waste repositories.)

Unfortunately the basic design of the Light Water Reactors dominating the nuclear power scene today is not conducive to the dispelling of such beliefs.

This is because their safety is contingent on the intervention of specially provided safety systems that may or may not function.

With excellence in their construction, maintenance and operation, the probability of malfunction leading to serious accidents is extremely small and safety is more than adequate.

The difficulty is in proving the actual presence of this excellence. The frequently encountered claims for extremely low probability of serious accidents (such as once per million operating years or so) can hardly be reconciled with the existing opportunity for erroneous or malicious human intervention.

Could the public aversion to nuclear power be overcome by the introduction of a more convincing technology in which this opportunity is seen to be largely eliminated?

This paper does not discuss this question per se but rather , in case of a positive answer, what the characteristics of such a technology should be to achieve the desired acceptance The discussion is limited to reactor safety.

Since all technological risks ultimately originate in human lack of understanding, error or malice the primary merit of a nuclear technology from the safety point of view should be the extent to which these elements could be present in a system without introducing risks of serious accidents with major radiation doses in the environment.

Initially without considering realistic possibilities of complying with them, some "ideal" design rules are formulated with this in mind. Could compliance with these rules be achieved, rational objections on safety grounds to the use of nuclear energy would no longer exist, for reasons understandable to the educated layman,

A qualitative review is then made of to which extent these rules are complied with by a number of proposals put forward by various reactor vendors with the stated purpose of achieving improved public acceptance.

Two groups of such proposals can be discerned.

In the first group, proposed mainly by two leading US reactor vendors and supported by the US Department of Energy , the main emphasis is on limiting the deviations from present commercial designs to such an extent that the investment in development work can be minimized and no prototype will be required for licensing. The main new feature is the elimination of the need for sustained post accident electric power generation for preserving core integrity. However the dependence of safety on the function of other potentially error prone equipment such as instrumentation and its calibration,valves and control rod drives etc. remains.

The other group of proposals achieves a much higher degree of independence of human fallibility in the protection against serious accidents, but at the cost of a larger amount of design innovation with the concomitant increase in costs and time requirements for introduction on the market.

These are mainly the PIUS pressurized water reactor proposal and the Modular High Temperature Gas Cooled Reactor.

In so far as it is accepted that the existence of a safety-wise more convincing solutions will significantly contribute to the future rational use of the nuclear option, there are strong arguments for international support for taking these concepts through the precommercial phase.

For the longer run breeder reactors are expected to be needed although the time scale for this is very difficult to forsee at the present. Among concepts in this field under development, the American Integrated Fast Reactor (IFR) system appears to offer special merits because it seems to offer both a high degree of the desired "inherent" safety and the fissioning of the long lived higher actinides that otherwise complicate the high level waste issue.

CONTENTS

Introduction

Principal safety criterion

Design rules to ensure acceptance

The present technology

Classification of enhanced safety reactor concepts

The AP-600 reactor

The PIUS reactor

The Modular High Temperature Gas Cooled Reactor

Breeder reactors

Conclusions

Introduction

How to supply energy for a decent life for a world population that is unlikely to stabilize below ten billion people should be a dominant theme for a conference like this. Clearly, even if energy conservation measures bring down per capita consumption considerably below that in the industrialized world today we must expect a very large increase in global use unless we cynically assume that the "developing nations" will never get out of their present misery.

Let us recall what the available options are:

- Liquid hydrocarbons will be fully used up for transportation needs.
- Natural gas will be a major contributor during the next few decades but from the longer range point of view it must be considered a stop gap measure.
- Massive reliance on coal has few remaining proponents; using the atmosphere as waste dump appears untenable altough the jury may still be out in the greenhouse case.
- The renewables may make important contributions locally but are likely to fall far short of being able to take on the the whole burden,
- Fusion still remains a mirage and appears unlikely to be economic even if eventually technologically feasible.

In this situation energy from fission represents an highly desirable and probably absolutely essential contribution. And unlike the case with many of the highly touted renewables a mature, demonstrated basic technology is available.

And yet this contribution is in danger of being lost because of a combination of public "radiation phobia" and distrust of the technology (Korea may represent one of the few exceptions here). In most countries an antinuclear stance represents an irresistible temptation for a politician out to grab power at the polls. And even though where there may be no antinuclear majority in the the public opinion polls the NIMBY (Not In My Back Yard) syndrome stifles any practical attempt to revive of the nuclear option.

It is beyond the scope of this contribution to discuss the origin of and and any possible ways of alleviating "radiation phobia". It is anybodys guess whether the public will ever learn to judge risks with ionizing radiation in a "realistic" way. Waiting for this to happen anytime soon would appear as a vain hope.

In many technologies introduced during the industrial age, such as air transportation, accidents with large loss of life do sometimes occur, and are tolerated by the public in the sense that there is no outcry for the phasing out of the technology. Because of the "radiation phobia" this is not the case with nuclear power technology. Accidents with loss of

life and significant environmental consequences are simply intolerable. The high level waste disposal complex aggravates the situation.

Even though probably little can be done to get rid of the fear of radiation, is it possible to convince even a sceptic public that adequate means are at hand to prevent its release into the environement by introducing improved technology?

There is certainly no agreement about this. It is not meaningful to propose a technological answer to a nontechnological problem, so the argument goes among those who want , for competitive or other reasons, to preserve the present technology essentially unchanged. In the present depressed conditions this is an understandable attitude from the nuclear industry.

On the other hand there are strong reasons for the opposite stance, perhaps most persuasively expressed by the honorary chairman for this committee.. The lay public is not deaf to technical arguments if they can only be kept free of emotional bias. A case in point is that the public in Sweden has certainly learned to appreciate the difference between the Sovjet RBMK reactors with their nuclear instability and the Western LWR:s.

In the following are discussed the characteristics a technology should presumably have to enjoy general acceptance and some of the attempts to move in this direction are briefly reviewed.

Principal safety criterion

The health effects from ionizing radiation (at least their upper limit) are probably better known than those of any other environ-mental pollutant and a review here would be redundant. Equally well known is the public aversion to exposure to it , referred to above as "radiation phobia" and constituting the main impediment to public acceptance of nuclear power.

Nevertheless, if an accident (judged as such as very unlikely) results in an exposure not greater than that received from the natural environment in e.g. a year then it seems reasonable to assume that this would be acceptable for the large majority of people.

If this is true, then an important consequence is that accidents that do not damage the core can be considered relatively harmless and their possible occurrence should not be incompatible with public acceptance of nuclear power. This is because larger doses can only result from the dispersal of (mostly volatile) nuclides from the fuel subsequent to core damage involving cladding breach and overheating. Hence in the discussion below we need only be concerned with accidents that result in some form of core degradation.

This statement may not appear compatible with the uproar that has resulted in the past from rather trivial incidents resulting in negligible environmental radiation doses (such

as a steam generator tube rupture in a Japanese reactor). However, this may be explained by the fact that the safety systems provided did not work properly and the incident was seen as a prestage of a severe accident narrowly averted by the operators, rather than a concern with the radiation dose as such.

The basic criterion for an acceptable nuclear technology should then be an ability to ensure core integrity following any credible incident even under the most pessimistic assumptions one could reasonably make regarding the status of the plant and its operators. And this must be achieved in a way that is readily understandable to the interested layman and without significant penalty in costs and practical operability.

Hence a tenet underlying this paper is: In reality an unharmed core is tantamount to acceptable nuclear safety. It should however be observed that this definition of safety, used troughout in the following, is not necessarily in agreement with current safety regulation.

Of course, even assuming that the core is damaged , environ- mental radiation exposure can still be prevented by enclosing the reactor in a leaktight containment as was the case in the Three Mile Island accident. However, putting the main emphasis on containment rather than prevention of core damage does not appear to be a reasonable approach, partly because it does not contribute to the protection of the investment in the plant, partly because a situation with a degraded (perhaps molten) core is hardly amenable to a reliable safety evaluation. A good containment is a valuable supplement to safety and probably a necessity for public acceptance but can never be the basis for an acceptable design.

Design rules to ensure acceptance

As has been pointed out above serious nuclear accidents are widely seen as both unacceptable and sooner or later inevitable by a suspicious public.

Could design rules be formulated that, if adhered to, could virtually guarantee , in a way readily understandable to the concerned layman, that accidents involving core degradation will not occur, thus eliminating the impression of inevitability? What would such rules say?

To begin with it should be pointed out that the risks of failure of a technological system at any given time have their roots either in the status of the physical system itself or in the minds of the people operating it.

If either or both are associated with significant uncertainties, then an ensurance for the safe outcome of incidents that could conceivably occur cannot be provided, only a reasonably wellfounded hope that everything will be OK. This is something we accept when we board an airliner, but nuclear technology seems to occupy a unique position in the public

mind in that it is evidently not considered sufficient. Here we appear to have to accept a much more stringent requirement .

A possible concise formulation of it could be as follows:

A prerequisite for permissible plant operation is that the presence of all the conditions necessary for a safe termination of any credible incidents can be verified at all times/e.g. for an independent outside representation entitled to observe plant operation.

Let us discuss the two categories of uncertainties in relation to this requirement, starting with the mind of the operators.

This includes their knowledge and training, general intelligence and judgement, reaction to stressful challenges and general loyalty and dedication etc. It is clear that genuine, unquantifiable uncertainty will always prevail here. It may be sufficient to recall the fact that the two major accidents so far in civilian nuclear power had their roots in operator transgressions of rules or misunderstandings.

Training, education and operator competence examinations can help to improve the situation but the effect is temporary and local, whereas the impact of a serious accident anywhere will be global.

Clearly, the suggested ground rule requires that if safety related incidents occur the operators must be divorced from ensuring their safe termination, not only in the sense that no action from them is needed but also that they must have no opportunity for jeopardizing it by mistaken (possibly even malicious) operation of plant control systems.

The responsibility of the operators should be limited to normal running of the plant and checking that the necessary preconditions for safe termination of incidents do exist. If the latter is found not to be the case operation should be discontinued.

Going now to the physical status of the plant it is instructive to discuss how uncertainties are introduced.

In the design stage the opportunity to find errors is the best. The design describes the ideal system that is in every respect up to specification. Licensing authorities undertake their own in-depth analysis of the system including a wide range of abnormal situations. Assumptions not based on recognized facts or demonstrated performance are subjected to experimental tests. Design errors may however result from overlooking complex interactions between systems when their number is large and the consequences of unplanned but possible operator actions. A ground rule for avoidance of this is a small number of systems impacting on safety.

In the manufacture of equipment and components various forms of defects may appear. It is useful to divide items into two categories - structures and active equipment (apparatuses)
such as valves, instrumentation etc. which are of course both subject to quality control.

Structures are as a rule examined by means of nondestructive testing (ultrasonics, eddy current etc.). This testing may be incompetently performed (e.g. cracks overlooked) or simply skipped for reasons only the erring or dishonest technician knows. Documentation supplied will not reflex such errors and may be "doctored". Hence the long term integrity of a structural component based on the integrity of a single load carrying member (such as a pipe or steel pressure vessel) with vital safety function will be critically dependent on the performance of fallible humans and hence in principle open to doubt.

Active equipment will of course be tested both by the manufacturer and after installation. The case of undetected nonfunction after this should have negligible probability. The case of in service performance after exposure to fatigue,wear and corrosion etc. is quite another matter. Although in service inspection is made to reduce the probability of malfunction of safety related equipment it can never eliminate it. Furthermore testing may in itself degrade the equipment; the test just made may have been the last time it functioned.

Plant construction means erection of concrete structures, piping systems and electrical systems.

Because they are built up a large number of redundant load carrying components (rebars , tendons) concrete structures are unlikely to contain overlooked safety-wise important flaws.

The integrity of piping systems are subject to the same kind of reservations as that of factory produced structural components, only more so. Construction errors in electrical systems not detected in testing (such as poor soldering, loose cable connections) may also be present.

Maintenance activities have an extremely important impact on safety. Erroneous, careless or plainly malicious acts by maintenance technicians, e.g in instrument calibration, cable routing, valve positioning etc, could be one of the main contributors to uncertainties regarding the true state of the plant.

What conclusions can be drawn from the above regarding the design rules for a reactor that not only produces electrical power in an effective and economic way but also can win the confidence of an informed but sceptic lay public?

Clearly, avoidance of complexity must be one of the ground rules. Reliance on a great number of redundant, diverse safety systems alraedy in itself eliminates any practical possibility of public understanding.

Since, as pointed out, the status of safety related active equipment (meaning apparatuses as opposed to structures) can rarely be ascertained during operation the design rule must be to avoid any dependence of safety against serious accidents on the function of active equipment (such as valves, including check valves, instruments etc.)

Regarding load carrying structures it has been pointed out that the presence of hidden flaws critical to mechanical integrity, of load carrying members cannot be excluded. Hence safety against serious accidents should not be critically dependent on the integrity of any single load carrying structural member.

If a practically operable reactor could be designed to comply , in a way understandable to the educated layman, with the initially stated requirement by being designed with the above rules in mind, then no rational objections to safety could be invoked and resistance to nuclear power would be limited to to those who oppose it on purely ideological grounds,(provided a convincing solution to the high level waste issue is available, which we believe is the case in Sweden.)

The expressions "passive safety" and "inherent safety" have been used in a meritorious sense for some of the characteristics described above. Since their interpretation may be ambiguous and they have sometimes been used in a misleading way they are avoided here.

To what extent real reactor designs can approach this ideal will be discussed below. To place the discussion in proper perspective a reference to present technology and the reason it has encountered so much opposition on safety grounds is necessary.

The present technology

Today the nuclear power scene outside previous communist areas is dominated by the Light Water Reactors (LWR:s) of US origin. In a few countries (Canada, Argentina , Korea, India and Pakistan) there are Heavy Water Reactors of Canadian origin and in the UK there are Gas Cooled Reactors. An inclusion in the discussion of these other reactor types would not significantly influence the conclusions that can be drawn from this paper and is therefor omitted for brevity reasons.

The Light Water Reactors are of two types: Pressurized Water Reactors (PWR:s) and Boiling Water Reactors (BWR:s).

Both are characterized by the presence of a high power density core in a relatively small thickwalled steel pressure vessel
(particularly for the PWR).

The type of fuel is the same in both i.e. small diameter cylinders of enriched uranium oxide sealed in tubes of a zirconium alloy.

The water circulating through the core serves both as neutron moderator and coolant. In the BWR the heat produced in the nuclear fuel directly generates steam in the core whereas in the PWR the coolant is heated in the liquid state and produces steam in an external steam generator.

For control of the power generated in the core and ensurance that it does not exceed the cooling capability of the circulating coolant these reactors use a large number (over 100 in case of the BWR) control rods , each operated by a separate mechanism on the basis of signals from neutron detectors.

For supply of coolant for post accident removal of fission product deay heat in case of leakage, such as from pipe breaks, the reactors are supplied with emergency cooling systems. These take their water from storage ponds in the plants and must be started up quite rapidly since in some cases all normal coolant can be lost in a matter of seconds. In case the electrical grid is lost diesel generators have to be started up to operate the pumps transporting the water to the core, often against a high pressure head.

Since a safety system can fail to work when called into action several systems have to be supplied for a given function (redundancy). Furthermore the risk of so called common mode or common cause failures dictate the use of "diverse" systems for a given need. Finally, to prevent several redundant systems from being disabled by the same event (e. g. a fire) they have to be localized in sufficiently separated rooms.

This all leads to a highly complex and costly plant design, which has to be built with very large unit capacity to be economic.

There is however no doubt that if the LWR:s of modern design are built, maintained and operated with excellence through-out , then the risk of serious accidents is extremely low and safety is more than adequate. Hopefully this is the case with most or all reactors in the industrialized countries today, excepting some of Soviet origin.

But how to make a sceptical public realize for themselves that this is so and will remain so even with a vastly expanded nuclear power generation?

It is quite clear that the design of present type LWR:s is quite incompatible with the stringent requirement for acceptance of safety proposed above .

Active equipment is extensively used. Its status at a given moment can seldom be ascertained. Safety is also critically dependent on the absence of undetected flaws in critical load bearing structures,mainly the reactor vessel. Above all the operators can interfere with the safety systems in various ways as happened e.g. in the TMI accident.

By the use of redundancy etc. as described the probability of existence of an unsatisfactory defence against safety related incidents is reduced. Quantitatively this probabilty is estimated by means of so called Probabilistic Safety Analysis (PSA).

PSA is a very valuable technique for finding weak points in a complex design with many interacting systems but its use for making claims for a high degree of safety has proved if anything counterproductive. There is also a danger that the calculated probabilities tend to eventually assume the status of some sort of physical reality to those

working with the reactor design. Thus one can see statements in the literature such as " the core melt probability of the X reactor is 2.10^{-6} per annum".

This is obviously a preposterous statement since as mentioned the risk is a function of both the physical status of the plant and the mental processes in the people maintaining and operating it and the latter are definitely not amenable to quantitative asessment.

For instance one can point out the opportunities a knowledge-able infiltrated terrorist doing maintenance work would have for disabling safety systems. Of course it is rather unlikely to unwittingly have an employee in this category but it would obviously be ridiculous to claim that it would happen only once in say 100.000 years of reactor operation! This is an issue conveniently disregarded by the nuclear indutry because of its intractability.

To summarize , the basic design of the present type of reactors makes their safety hostage to the performance of fallible (and perhaps malevolent) humans to an extent that is likely to continue to block improvement in public confidence.

The LWR:s have now been in the market place for more than a quarter of a century and during this time a very extensive regulatory framework has been built up, to a large extent prescriptive and related to specific design features of the PWR and BWR. Because of its legal status, at least in the US, introduction of innovations conceived to improve safety against serious accidents but not consistent with this framework may encounter some difficulties and costly introduction of technical features of little value for protection of the public might be required. This will be a very important issue for market introduction of the new concepts.

Classification of enhanced safety reactor concepts

There are quite a number of new reactor proposals making claims for improved safety, mainly on the basis of of a reduction of the number of systems needed for safe termination of conceivable incidents. It would be out of question to include a description of them all in this paper.

Workers at the Oak Ridge National Laboratory have suggested a lucid classification scheme in which they can be grouped in categories as follows [1)]

1. Evolutionary plant reactors

These are reactors from most of the leading vendors of essentially current modern design in which the supporting plant, such as the safety systems, have been improved and rationalized on the basis of previous experience. They are large (1000 MWe or more) and

provided with conventional active safety systems. These reactors undoubtedly represent some improvement in safety over those currently in operation. However because the underlying design principle of relying on a multiplicity of active safety systems is unchanged their introduction is unlikely to influence public acceptance to a major extent and they will therefor not be discussed further.

2. Evolutionary technology reactors

They include significant innovations in the design of the reactor itself and its primary system but these are limited by an emphasis on retaining commercially demonstrated features as much as possible. Generally they are being developed for the medium (≈ 600 MWe) power range.

The safety-wise important advancement common to the reactors in this category is the elimination of the need for sustained electric power generation for keeping the core cooled under post accident conditions. This eliminates the dependence on the function of diesel generators and one of the dominating contributors to core melt probability, the so called station black out. It also contributes to a considerable simplification in plant design and layout.

For other functions these reactors are still critically dependent on the function of active equipment such as valves, control rod drives, instrumentation etc.

The most important Evolutionary Technology Reactors are the following:

- The Westinghouse AP-600 PWR, to be further decribed later.
- The General Electric SBWR, a 600 MWe BWR with natural circulation of coolant. It features a reactor vessel that is very large in relation to the core power, allowing a long response time in transients. Long term core cooling in case of leakages is ensured by pressure blow down and thereafter connection, in a natural circulation arrangement, to a large atmospheric water pool. Development is funded mainly by contributions from the US Department of Energy (DOE) and the Electric Power Research Institute (EPRI).
- The Mitsubishi SPWR. This is equipped with a new kind of steam generator with horizontal tubes which is claimed to make possible natural circulation cooling in a leakage situation with station black out. Reportedly this reactor is being developed also for a power of 1200 MWe and may turn out to be a major contender in the future marketplace.
- The Hitachi and the Toshiba small BWR designs with a number of safety motivated "passive " features.

- The SIR reactor developed by a US-UK consortium primarily for deployment in the UK. This is a very interesting and innovative concept but it suffers from the difficulty that the power is limited to the 3-400 MWe range. This is because it is a PWR in which the whole steam generating system including the steam generators and redirculation pumps are enclosed in a steel pressure vessel. The fabricability and transportation possibilities for this vessel limit the possible unit output. SIR includes many attractive advanced safety features.

Later the AP-600 will be singled out as a typical representative of evolutionary technology reactors and described in sufficient detail to make the difference in safety philosophy in comparison with the following category of reactors clear.

3. PRIME reactors

PRIME is an acronym proposed by the Oak Ridge workers for Passive safety, Inherent safety,Resilient safety, Malevolence resistence and Extended time for external aid after an accident. The reactors in this category have been designed from the outset to avoid the sources of safety concerns that hamper the acceptance of nuclear power today. Doing this has necessitated larger deviations from existing designs than is the case with those in the previous category but nevertheless the concepts are mainly based on established technology (in such basic fields as fuel, materials etc.)

There are two concepts in this category that have been the subject of extensive engineering effort, namely the PIUS PWR and the Modular High Temperature Cas cooled Reactor (MHTGR). These will be discussed below.

4. Breeder reactors

These are not part of the suggested Oak Ridge classification scheme but are included here because of their long range importance. They are briefly dicsussed at the end of this paper.

The AP-600 reactor

Out of the reactors pursuing the introduction of "passive" design features with the intention of achieving simplification and improved safety with reduced risk of mistaken human intervention the majority belong to the category termed evolutionary technology reactors above. In these, new design features have been introduced in the reactor proper and

its primary system but the extent of innovation has been limited enough to hopefully make prototype operation before commercial introduction unnecessary.

It is important to give a feeling for the outlook for improved acceptance of nuclear power by the introduction of this category of reactors but it would be out of question to include a description of each of them. For that reason the Westinghouse AP-600 (AP for Advanced Passive) PWR will instead be selected as a typical representative of the category. Although many differences exist, the basic safety philosophy used for the other members of the category is much the same,

The AP-600 reactor is in all essential aspects a typical PWR but is distinguished from todays commercial PWR:s, e.g. from the same vendor in the following respects:

- The reactor power is reduced to 600 MWe, i.e. about half of that of a modern present day PWR. This is partly because the "passive" features introduced are less suited for large unit outputs, partly because US utilities are expected to prefer smaller plants in the future.
- The core power density is reduced, providing improved thermal margins and allowing increased response times in emergencies.
- The coolant pumps are "closed" i.e. working without shaft seals, thus eliminating one of the most troublesome components in a conventional PWR. Furthermore, the pumps are working with hanging motors mechanically integrated with the bottom end of the steam generators. This eliminates certain situations in which coolant flow through the steam generators becomes blocked.
- The safetywise dominating new feature is the method of securing post accident cooling of the core e.g. in a leakage situation when power from the normal electric grid is unavailable.

The reactor system is then depressurized by successive opening of a set of valves in the primary system. The flow emerging from these valves is sent to an In Containment Refuelig Water Tank (IRWT), which is a large pool of high boron content water located at a high level. This water is used for normal refueling operations.

When the depressurization has progressed sufficiently another set of valves are opened which connect a lower part of the primary system to the IRWT. In this way a natural circulation coolant circuit is formed through the core and the IRWT and the latter takes over the cooling. Because of the location of the reactor in a cavity at low level its outside becomes flooded in this situation

In case electric power for active cooling systems continues to be unavailable steam pressure from heating of the IRWT builds up inside the containment building. Heat is then transferred to ambient air by condensation on the inside of the containment steel wall and heating of air flowing on its outside. The rate of air flow is enhanced by chimney action in

an annulus between the steel wall and an outside concrete building, which also acts as a protection against e.g. aircraft impact.

During an initial post accident period, when core decay heat generation is still high, heat transfer from the containment wall is augmented by gravity fed spraying with water from a storage tank on the roof of the concrete building. Later, as the rate of heat generation decreases, cooling with dry ambient air is sufficient.

Thus, provided the initial series of valve operations is correctly carried out, the reactor is left in a state in which at least in principle it can take care of itself indefinitely. In contrast a conventional PWR would have to continously rely on power provided by back up diesel generators. This in essence is the safety advantage claimed for AP-600 and for the other reacors in the considered category. The principle is illustrated in figure 1.

- For limitation of reactor power (both total and local) to a safe level the AP-600 uses control rods with drives actuated by a reactor protection system processing signals originating from neutron detectors just like a present day reactor.

The AP-600 reactor is now under design and development by Westinghouse Electric Corp. and seems to represent their main thrust for the future market. As with the SBWR this effort is funded on the basis of a cost sharing scheme where the US DOE provides about half and EPRI most of the rest. Active marketing is going on and design certification is forseen for about 1996, although some confusion currently seems to exist regarding the licensing process.

The PIUS reactor

The PIUS reactor has been conceived from the outset with the suggested "ideal" design rules in mind. In other words an attempt has been made to create a design where the presence of all the conditions necessary for safe termination of any credible incidents during operation can be verified at all times.

PIUS is an acronym for Process Inherent Ultimate Safety, meaning that the safety (against serious accidents) is an inherent consequence of the design of the heat extraction process and that this safety is always ultimately available if all normal active systems fail.

As far as the energy production is concerned PIUS is just a reconfigured, somewhat deintensified PWR. It uses standard PWR fuel and pumps and steam generators of designs demonstrated in other plants. Operating temperatures and pressures as well as power densities are lower than in conventional PWR:s. Therefor, from the strictly nuclear point of view there are no new major features that should require reactor operation for confirmation.

From this point of view one can argue that a prototype is not necessary; the new design features could be demonstrated in a non-nuclear mock-up. They are illustrated in figure 2.

The special feature that confers the unique safety properties on the system is the primary system configuration with always open connection of the energy producing circuit with its core, pumps and steam generators to a large pool of relatively cold water with a high concentration of the neutron poison boron (in the form of boric acid, used also in the primary circuit in conventional PWR:s).

The heat producing circuit (operating at about 280 °C) is in contact with this pool at two different levels, separated by about 20 meters in elevation. The difference in density between the cold pool water and the hot coolant causes a higher hydrostatic pressure differential between the two contact levels in the cold pool water than in the hot process water. If the difference is compensated for on the hot coolant side by the dynamic pressure drop due to the coolant flow through the core, then the pressure differential at both contact levels can be kept to zero and no flow occurs through the connections. In this way the hot coolant, with a low boron content can be kept separated from the cold high boron pool water in spite of the open connections between them.

At the connecting levels, named thermal barriers or "density locks", hot coolant is stably layered on top of cold pool water and the vertical position of the hot/cold interfaces monitored by temperature instrumentation. The position of the lower interface is kept at a specific level by controlling the speed of the recirculating pump (and hence the dynamic pressure drop).

The pump speed has an upper limit given by the AC frequency of the electric grid. If the circulating coolant becomes too hot or it contains steam bubbles then the difference in hydrostatic pressure differential becomes greater than the dynamic pressure drop the pump can achieve at its maximum speed. The primary system then takes the missing flow needed to equalize the pressure at both contact levels fom the cold high boron pool. As a consequence of the boron ingress the reactor power is reduced or the reactor shut down,

For instance if the feed water flow to the steam generators is lost (i.e. there is no longer a heat sink for the primary system) then the resulting temperature increase in the coolant causes ingress of pool water with a high concentration of boron and reactor shut down.

Similarly, if one tries to increase reactor power beyond permitted values by decreasing the boron concentration in the coolant the resulting temperature increase also leads to pool water ingress and power reduction. If boron dilution continues unabated in spite of the abnormal conditions a periodic oscillation of reactor power is obtained, always in a safe range.

This "process inherent" safety feature is in no way dependent on any outside signals or intervention or active equipment function and cannot be tampered with by the operators.

The large pool of high boron water (about 2000 cubic meters for a 600 MWe plant) with the core near its bottom is housed in a prestressed concrete pressure vessel. Hundreds of mutually independent high strength tendons are responsible for the mechanical integrity of this vessel and hence, as required by the proposed design rules, hidden flaws in some of them have no serious consequences. Besides, the very size of the vessel would exclude shop fabrication and transportation to the site of a steel vessel.

The inside of the concrete vessel is clad with a steel membrane called the liner. During operation the liner is under compression and so cracks should not occur in it. Nevertheless it is conservatively assumed that this can still happen and therefor the lower part of the vessel (which has no penetrations) is provided with an additional leakage barrier and the interspace between the latter and the liner monitored for leakage. There is thus no way the water in the lower part of the vessel can be lost by leakage since there is no common cause for penetration of both barriers.

In case of the worst possible leakage situation (a rupture of a large coolant pipe leading from the reactor to the steam generator) a large amount of hot water will be lost from the concrete vessel. Nevertheless the remaining water level is well above the core that thus remains submerged and is cooled by natural circulation via the pool.

The pool water in turn is cooled in natural circulation by a number of intermediate circuits that reject the heat to ambient air in dry cooling towers. These are arranged so that only a fraction of them can be damaged by e.g. an impacting aircraft.

Thus even worst case post accident cooling of the core is ensured indefinitely without reliance on any active measures at all and with no possibility of missing by maloperation of plant controls.

As pointed out previously this is also the case with the ensurance that the reactor power is kept at a safe level. No case has been found where this built-in safety, impregnable to outside intervention, fails to protect core integrity.

The PIUS reactor therefor appears to be able to comply with the suggested basic acceptance criterion of having all the conditions necessary for safe termination of credible incidents verifiable at all times, namely:

- The presence of the large pool of water, without which no operation is possible
- Its open connection to the primary system
- Its boron content
- The integrity of the two series connected leakage barriers in the concrete vessel.

The only one of these conditions that could be affected during operation is the boron content in the pool. The quantity of boric acid is in the tens of tonnes and it would take several shifts of concerted intentional misoperation to achieve a dangerously low boron content. This is not considered a credible assumption.

The safety performance of PIUS has been verified both by specially developed computer codes and by running a large test circuit where the dynamics of the electrically heated model core (one fuel assembly) i.e. its dependence on coolant composition, temperature and void fraction is simulated by means of an advanced control system.

While there have been few if any objections to the safety claims made for PIUS there have been frequent assertions by critics that operating performance and availability have been sacrificed to make them possible. Usually the alleged source of disturbance has been inadvertent boron ingress through the "density locks". While admittedly reactor operating experience is not available, nothing in the operation of test circuits and in the systematic investigation of the thermohydraulic conditions in the "density locks" supports such a contention.

Normal plant operation will in fact in many ways be simpler than for a conventional PWR since the large number of control rods that need to be repositioned during operation in the latter has no counterpart in PIUS. During normal operation the reactor power usually self-adjusts to the rate of feed water flow to the steam generators.

The reactor is housed in a pressure suppression type containment. This is not necessary for core integrity protection but makes the environmental dose in leakage cases negligable and is probably a necessity for public acceptance.

Preliminary economic analysis indicates that PIUS is competitive with other LWR:s in the medium (6-700 MWe) range. It can probably be built in unit sizes up to 1000 MWe although such designs have not yet been worked out.

The work with PIUS has now gone on for more than a decade with varying levels of effort. In the mid-80:s discussions were held about building a small demonstration reactor in Korea but this did not come through.

Up to mid-1992 all work on PIUS has been privately financed by ABB. From now on to the end of 1994 the work will to a large extent be financed by the Italian state utility ENEL and performed by a consortium between ABB Atom, Ansaldo and Fiat. The Italians have to look for a reactor with enhanced safety after conventional nuclear power was rejected in a referendum in the wake of the Chernobyl disaster. Furher decisions concerning the fate of PIUS in Italy will be taken after the conclusion of this study phase.

In the U.S. the Nuclear Regulatory Commission is undertaking a preliminary licensability evaluation of PIUS. The results of this will be guiding for a decision whether to proceed later with full scale design certification.

The Modular High Temperature Gas Cooled Reactor (MHTGR)

This is the other reactor concept in the PRIME category that has been the subject of extensive engineering effort. It uses a totally different technology than the Light Water Reactors that dominate the industry today which in itself may be a possibly insurmountable barrier to commercial introduction. On the other hand its safety properties should make it well suited for public acceptance and this merits its inclusion here.

The basis for the technology is essentially the unique all ceramic fuel concept. By chemical vapor deposition of alternate layers of pyrolytic carbon and silicon carbide on small spherical fuel particles (uranium oxide or carbide) it has been possible to create a fuel that can survive temperatures up to 1600 °C without giving off significant amounts of fission products.

Permitting such a high temperature , it is possible to allow fission product decay heat to be dissipated from the core to the environment simply by solid conduction without using any heat carrying flow through the core. This obviously means an enormous simplification since the otherwise allimportant question of the whereabouts of the primary coolant suddenly becomes immaterial.

However, using this principle obviously puts a maximum on the core size and heat output that is of the order of 450 thermal megawatts and a high height to diameter ratio of the cylindrical core has to be used.

Two different types of core designs, one German and one American have been proposed, depending on how the graphite moderator is arranged in relation to the coated particle fuel.

In the German design the fuel particles are placed in the center of graphite balls that are slowly circulating through the core vessel and removed after having reached desired burn up. The helium gas coolant flows between the graphite balls.

In the US design the fuel particles are placed in holes in prismatic graphite blocks which are cooled by helium gas flowing through other parallel holes. The graphite blocks are handled intermittently like normal fuel assemblies.

With the inert gas coolant and the all ceramic fuel much higher temperatures (over 700 °C outlet) can be used than in the LWR:s. This makes possible steam cycle conditions representative for modern fossil fired boilers and much better thermal efficiency in spite of the greater fraction of the output used for primary coolant circulation.

Figure 3 shows the main configuration for a 170 MWe steam cycle MHTGR in a below grade placement.

As far as safety performance is concerned the advantage of a highly temperature resistant fuel is combined with that of a negative moderator temperature reactivity

coefficient, i.e. the reactor shuts itself down if it is heated up to an abnormal temperature due to loss of primary coolant or feed water.

It is claimed that the reactivity absorbed in heating up the core to a local maximum of 1600 °C can take care of the case of inadvertent withdrawal of all control rods.

It is difficult to find anything to criticize in the safety of the MHTGR, at least for a non-specialist. The basis of safety lies entirely in the (known) properties of the core and its physical environment and could hardly be undermined by inadvertent or malicious intervention, The suggested stringent conditions for public acceptance seem to be fulfilled.

A possible question could concern the result of a sudden hypothetical rupture of the main steam or feed water headers. Since the secondary steam pressure is much higher than that in the primary coolant could this possibly lead to unacceptable destruction of the primary system?

This is not the case with the direct cycle gas turbine plant with an MHTGR as heat source proposed by prof. Lawrence Lidsky of M.I.T. which may perhaps be said to represent the ultimate in terms of reactor safety.

An economic advantage claimed for the MHTGR is that most of the plant can be factory produced and shipped ready-made to the site. It is not clear whether this can compensate for the disadvantage of having to use a comparatively large number of units for a central generating station; the cost figures quoted by the proponents are relatively high.

In the US a small prototype HTGR was built early in the 1950:s . Its larger follow on, the Fort S:t Vrain plant in Colorado unfortunately proved to be a failure for resons that could not be said to be generic, but it was enough to discredit the concept.

Interest in the technology was rekindled when its safety potential became obvious and in 1989 it was proposed to build a new tritium production reactor for the US DOE on its basis. Under the existing political conditions this is unlikely to come through. The outlook for any type of gas cooled reactor plant construction in the US appears dim.

In Germany the fate of the gas cooled reactor is downright tragic. For many years a small test reactor was successfully operated and a 300 MWe follow on reactor, the THTR was eventually placed in operation with massive federal funding. Due to various technical problems, and above all a clear lack of utility interest, it is now being decommissioned. Once bright hopes for a Soviet project have obviously evaporated. It is very difficult to see a return of interest in the MHTGR in the country that provided most of the funding for its development.

Breeder reactors

Although not everyone agrees with it, it is likely that an important contribution from fission to mankinds future energy supply will eventually require the introduction of breeder reactors. The exact timing for this cannot be predicted; it may be relevant to recall that it was felt to be much more imminent thirty years ago than it is today.

In any case prudence requires that an acceptable technology is available when the need arises. Although there are several roads to breeder technology (using either uranium 238 or thorium as fertile material) the past and present concentration to the sodium cooled fast reactor (named the LMFBR in the US) seems to make it the only likely candidate (with the Russian proposal using liquid lead cooling perhaps a dark horse).

Public acceptance of the LMFBR has been facing particularly severe difficulties which have their roots in the theoretical possibility of an explosive core disassembly accident. This is due to the fact that, unlike the case with e.g. LWR:s, the core can assume a more reactive configuration than in the normal state as a result of melting or expulsion of the coolant by vapor formation.

Even though the use of sodium as coolant will always put higher demands on the operating and maintenance crews than the LWR:s , at least the above problem should have a solution that is largely independent of their performance . This means that trying to cope with it by introducing more numerous and sophisticated surveillance and safety systems is unlikely to be successful in securing public acceptance.

This, and the present lack of urgency means that the extensive European, above all French, development programs, culminating in the Superphenix reactor, appear to have come to a dead end. This also has to do with the high cost of aqueous reprocessing of spent fuel and the general reluctance to accept a "plutonium economy" with this metal a commodity moving through society with the attendant risk of theft and nuclear terrorism.

Fortunately there seems to be a way out of these difficulties represented by the Integrated Fast Reactor (IFR) program conducted by the Argonne National Laboratory and some industrial contractors in the US.

This program is based on the use of a new kind of reactor fuel, a uranium-plutonium-zirconium alloy in relatively small modular reactors.

This fuel offers both good burn up behavior and an inherent safe response to the challenges of loss of coolant flow or heat sink that compromize the safety of the large oxide fueled reactors that are the basis of the European program. This response has already been demonstrated very successfully in operation of the EBR-II reactor in Idaho.

Furthermore, the IFR concept proposes pyrometallurgical (electrorefining) processing of spent fuel and refabrication of fuel by remote handling without ever having the plutonium in a purified state in which it could be exposed to theft or highjacking.

Finally, the long lived transplutonium actinides that, at least in the publics imagination, causes the high level waste disposal to be a million year issue, are returned to the fuel in the reprocessing and fissioned in the core instead of ending up in the waste repository.

Thus the IFR program may make possible an energy supply with good answers to all the four basic questions:

- Long term resource availability
- Reactor safety
- A convincing solution to the waste disposal problem
- No risk of nuclear terrorism from theft of plutonium

In the authors opinion, admittedly formed without detailed insight, the IFR program is likely to be of more value to mankinds future energy supply than all the billion dollar fusion programmes combined. As this becomes more widely appreciated it is hoped that international support will be forthcoming.

Conclusions

The possibility of substantially improving the public acceptance of the safety of nuclear power and of increasing its future contribution to a nonpolluting energy supply by technological means remains an unproved assumption. It seems, however, to be reasonable enough that, from a global community point of view, not trying would be indefensible.

Hopefully the review above has given some idea of the options available.

What conclusions can be drawn regarding the desirability to proceed with the various alternatives from this general point of view?

It is probably a safe assumption that the LWR:s will continue to dominate the scene for the next several decades until the breeders eventually take over, perhaps in the middle of the next century. The utilities will probably be loath to embark on a completely new technology such as helium gas cooling in the absence of very compelling reasons, particularly since a new fuel cycle infrastructure has to be built from scratch.

This unfortunately tends to leave the MHTGR behind as an orphan . How to resurrect it in spite of its impressive safety credentials is difficult to see. Possibly an eventual entry into the electric power market must be via high temperature process heat applications where it has no nuclear competitors.

An illustrative graphic comparison between the three categories of future LWR:s as defined by the Oak Ridge classification scheme used above is shown in figure 4.

The evolutionary plant reactors will be offered in the near future by those leading vendors who have decided to survive the present drawn out hiatus in ordering and no special encouragement is needed here.

The work on some of the evolutionary technology reactors such as the AP-600 appears to be well funded and at least one or two of them are likely to be operating in the early years of the next century.

Are they likely to have an important impact on public acceptance? This appears questionable. Even though the elimination of dependence for safety on diesel generators etc. represents an important progress, there are other worries that those with ingrained suspicion regarding safety can turn to. For instance erroneous or missing valve maneuvres can lead to a core melt. Certainly the criteria for public acceptance proposed in this paper are in no ways complied with.

In fact the vendors behind these concepts now seem to talk less than before about their safety merits, emphasizing instead simplicity and reduced number of components. The published core melt probabilities for AP-600 are roughly the same as for the large "evolutionary plant" Westinghouse PWR.

As illustrated in the figure proponents of PIUS emphasize the absence of such concerns in that there are no credible chains of events leading to significant core degradation.

The case of a rupture in the primary system leading to severe coolant leakage provides a good illustration of the difference in safety behavior between PIUS and the "evolutionary technology" reactors such as AP-600.

If this happens in PIUS nothing at all needs to be done for core integrity protection - the needed system configuration is there from the beginning and the core simply settles down into a state of passive heat rejection to the environment.

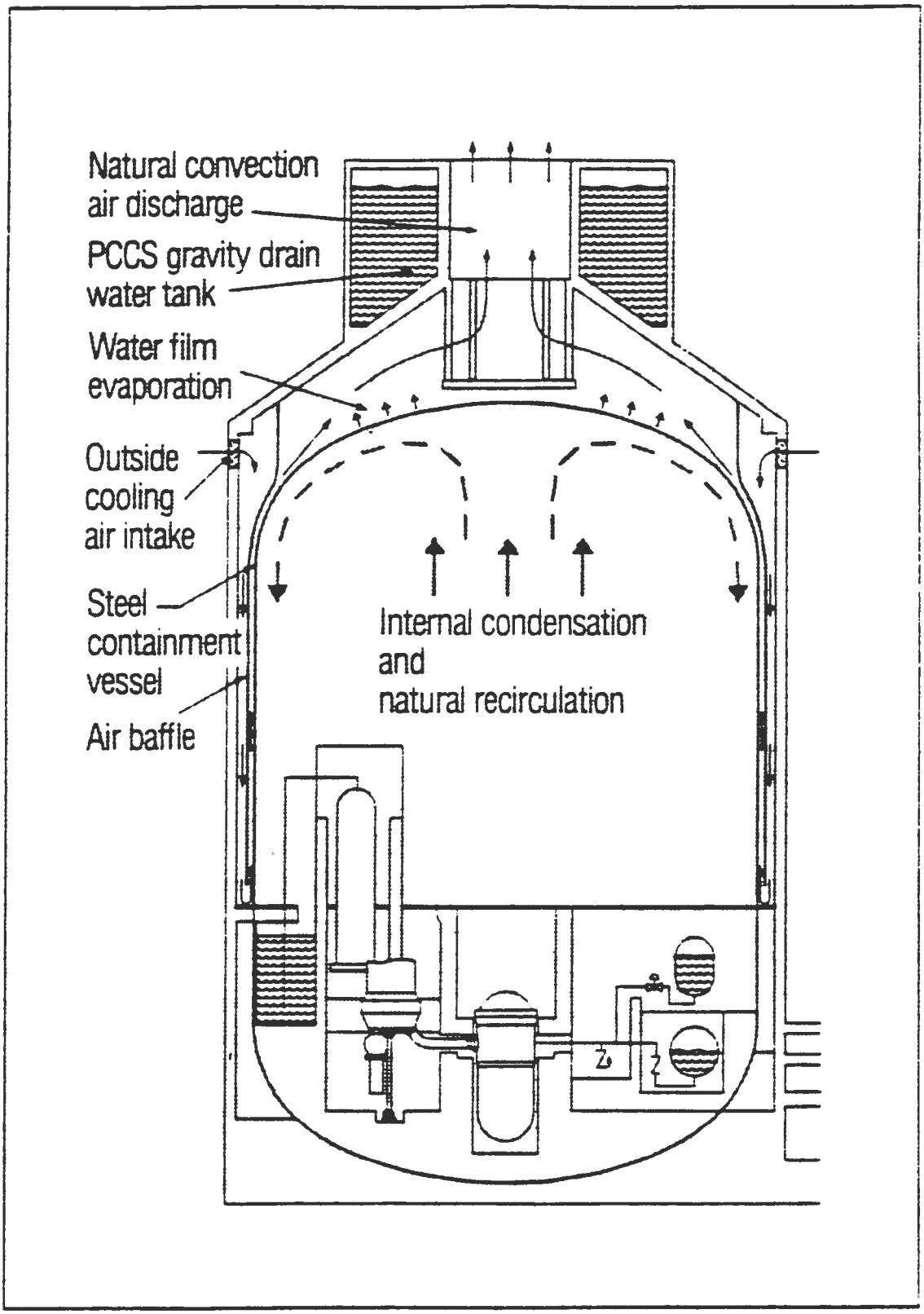
In AP-600, on the other hand, a safe configuration has to be created by the correct execution of a series of valve maneuvres. Unless this is accomplished a serious accident (core melt) will result.

If the extensive engineering effort now beginning in Italy confirms the present conclusions regarding economy and operability as well as the safety performance described above, would the difference in comparison with the "evolutionary technology" reactors exemplified above make it worthwhile to invest the ≈ $ 300 million in public funds needed to make it an available option for large scale deployment?

The members of the committee are invited to consider this question.

Reference: 1) Charles W. Forsberg and William J. Reich
Worldwide Advanced Nuclear Power Reactors with Passive and Inherent Safety: What, Why, How, and Who
ORNL/RM-11907 Oak Ridge National Laboratory September 1991

Note:
The author is a former employee of ABB Atom, now retired. The views expressed in this paper are his own and are in no way authorized by the company.



The AP600's passive containment cooling system.

FIGURE 1

PIUS

Main features of NSSS

1. Pressurizer steam volume
2. Steam generator (4)
3. Upper density lock
4. Main coolant pump (4)
5. Riser
6. Core instrumentation
7. Embedded steel membrane
8. Pool liner
9. Core
10. Lower density lock
11. Submerged pool cooler, cooled in natural circulation by ambient air.

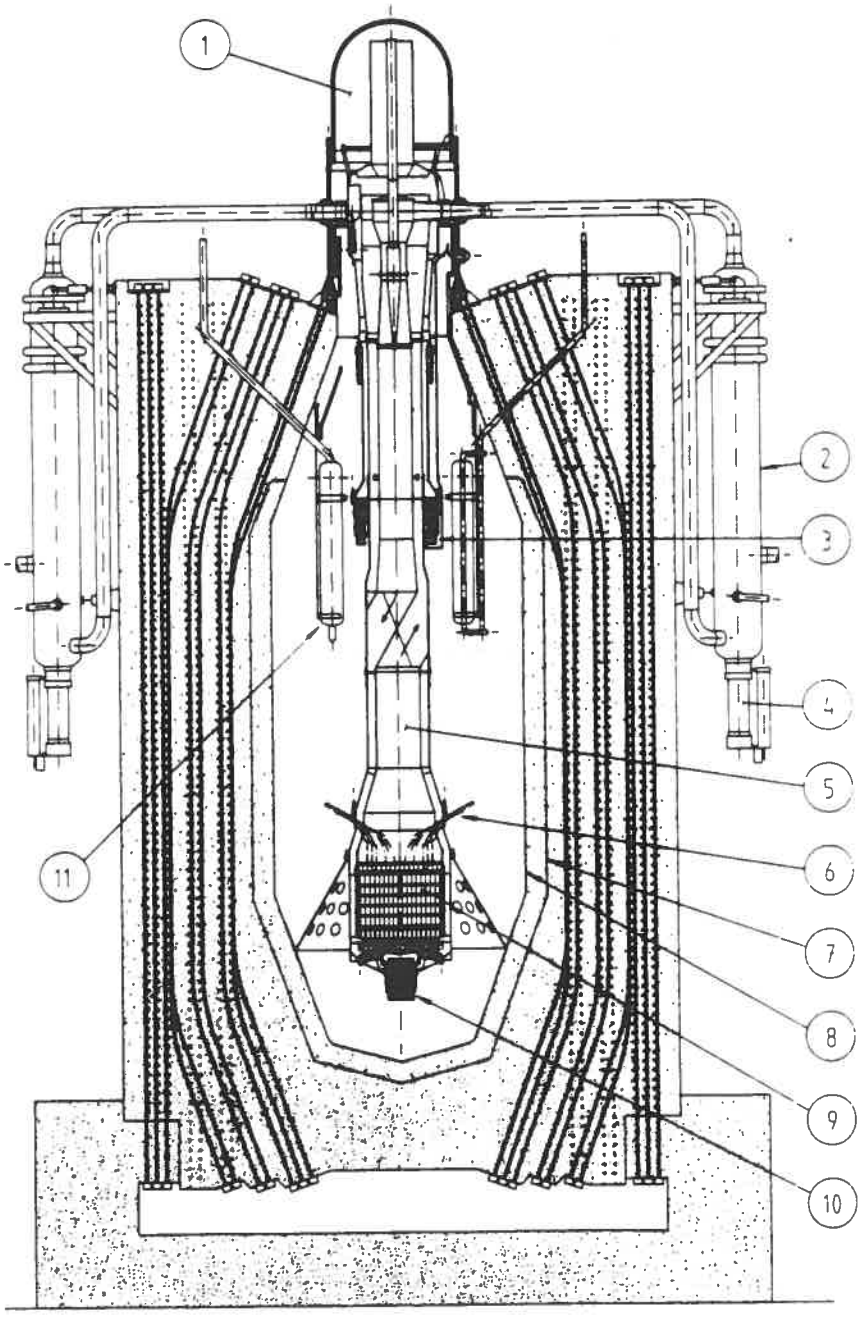


FIGURE 2

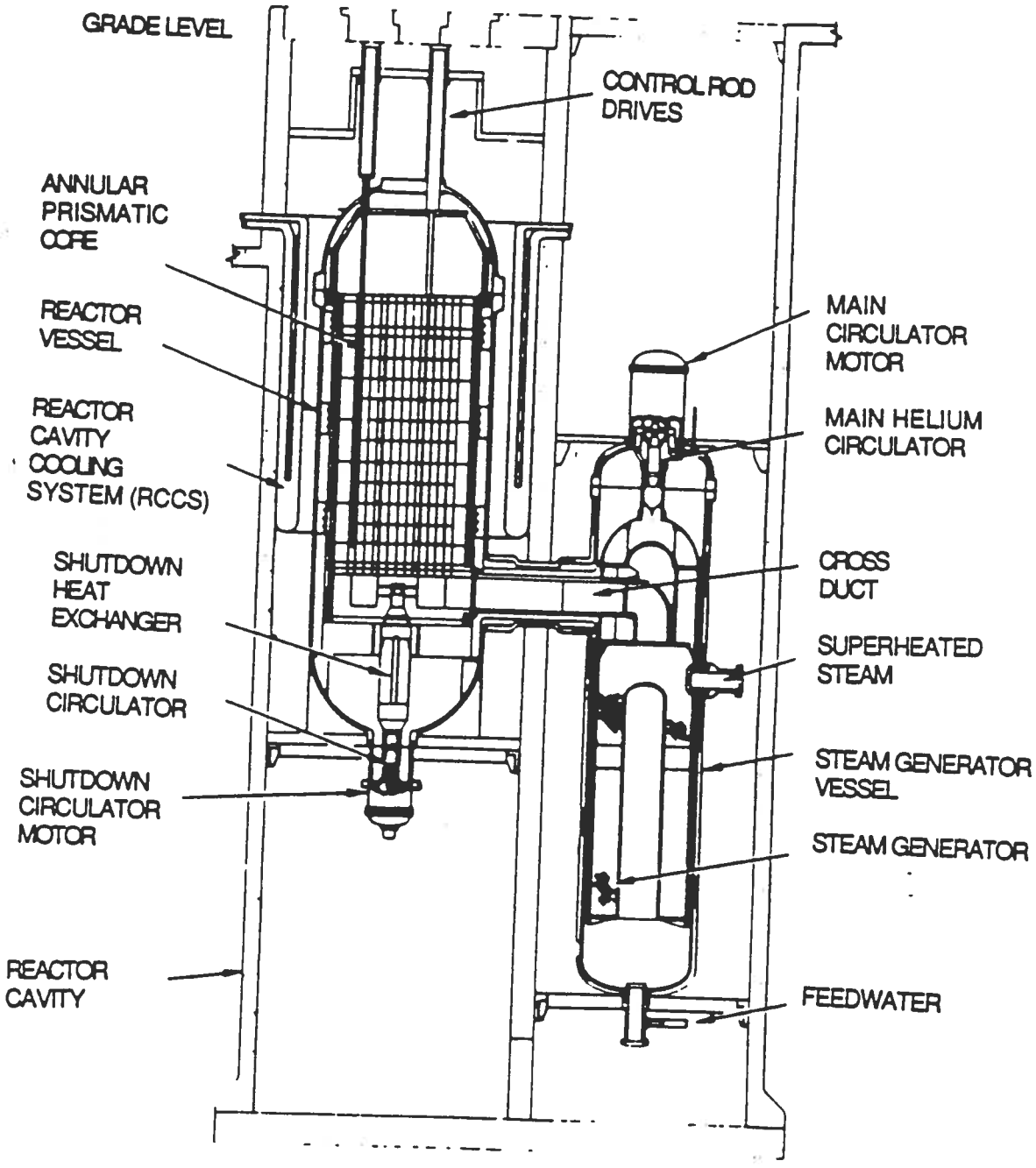
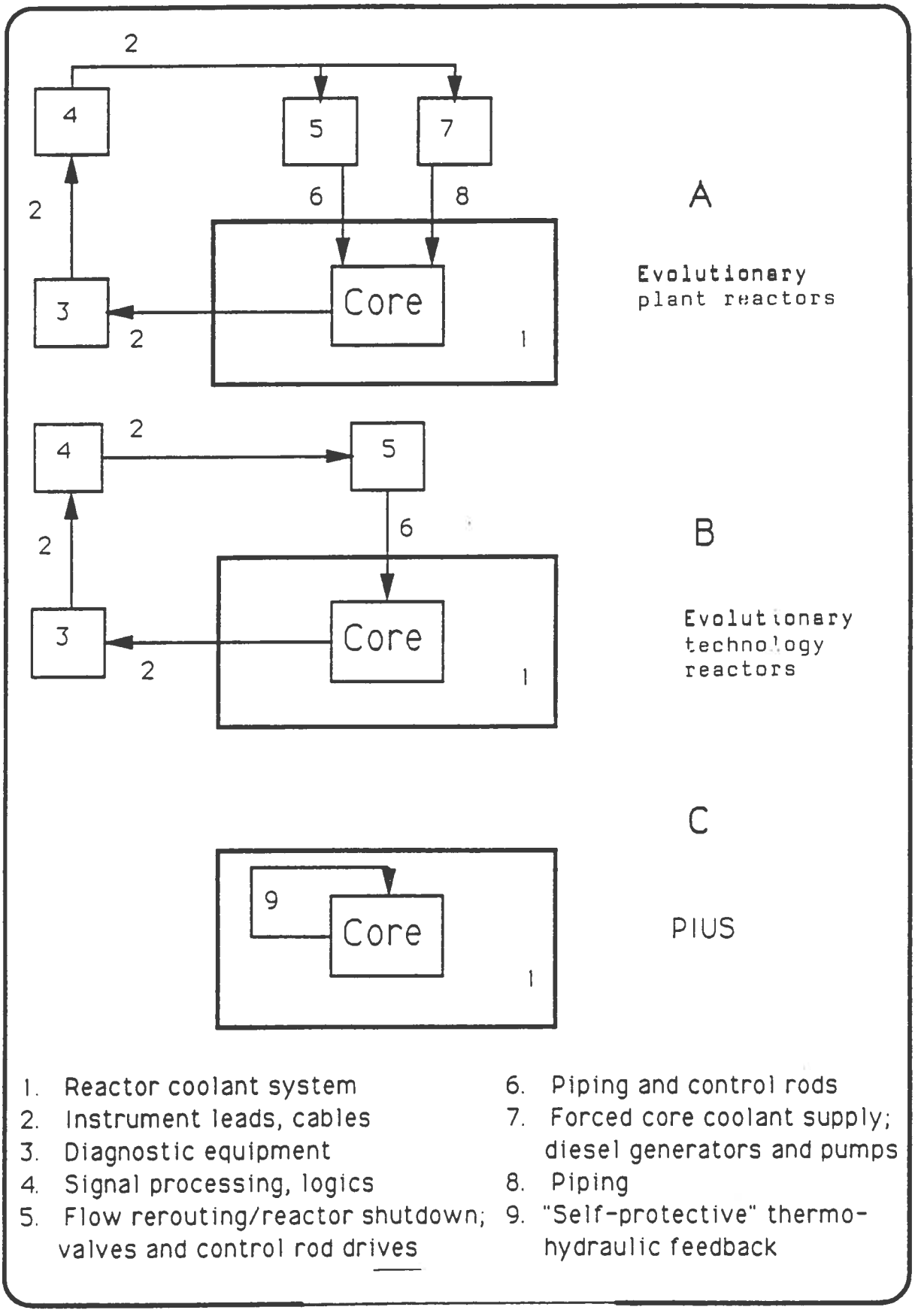


FIGURE 3. MODULAR 350 MW(t)
High-Temperature Gas-Cooled Reactor



1. Reactor coolant system
2. Instrument leads, cables
3. Diagnostic equipment
4. Signal processing, logics
5. Flow rerouting/reactor shutdown; valves and control rod drives
6. Piping and control rods
7. Forced core coolant supply; diesel generators and pumps
8. Piping
9. "Self-protective" thermo-hydraulic feedback

FIGURE 4