Design Features

Edited by D. B. Trauger

Pressurized Heavy-Water Reactor and Public Safety

By A. Kakodkar[a] and A. K. Babar[a]

Abstract: *The basic safety aspects of an Indian pressure-tube-type pressurized heavy-water reactor (PHWR) are described. Risk from an operating nuclear power plant depends on both the probability of occurrence of an accident (core damage) and the consequences in the public domain. This article compares the core damage frequency of a PHWR with that of pressurized-water reactors and explains the basis of its advantages from the viewpoint of public safety. Because of design safety characteristics of a PHWR (e.g., presence of cool moderator as a heat sink, calandria vault cooling system and double containment), the impact of worst-case accidents does not reach beyond the exclusion radius.*

Safety has been one of the most discussed and researched topics in any program related to nuclear energy. Perhaps there is no other branch of science and technology with such strong emphasis on safety. Although this effort has led to an objective assessment of all aspects related to nuclear safety, there still appears to be some need to bridge the gap between perception of acceptable risk as seen by scientific workers and as seen by members of the public. Regardless of their lack of validity on objective scientific grounds, arguments made by members of the public with regard to what they consider an acceptable or unacceptable risk must be understood.

Development of a technology brings with it great benefits to mankind. Often these benefits are accompanied by an element of risk. Usually, because of a quantum jump in the benefits that the new technology brings, the associated element of risk (when viewed in the context of risk–benefit analysis) is low. This certainly has been the case with nuclear energy. There are, however, some low-probability/high-consequence scenarios that pose problems of acceptability, particularly during the initial stages of introduction. This may be because of inadequate familiarity with the new technology, which leads to fear of the unknown, and also because of the possibility of a higher level of consequence (although of a much lower probability) that may have to be faced. Examples of such situations can be seen with every major technology that has had an impact on society. The initial responses of society when steam locomotives or major hydro power stations arrived on the scene are examples of this phenomenon. The scientifically accepted definition of risk (i.e., the probability of occurrence multiplied by consequences of the particular occurrence) would clearly demonstrate the relative risks associated with different technologies. Reduction of risk through reduction of probability of occurrence of the accident, however, is somewhat difficult for the general public to appreciate. A confidence in such comparisons can be more easily generated after the society has seen the technology deliver its goods over significantly long periods.

[a]Bhabha Atomic Research Centre.

The development of commercial nuclear power reactors was strongly influenced by early development of a nuclear power pack for submarine propulsion. Requirements of compactness and also of economy led to evolution of this reactor system in its present-day form. This exercise led to viable systems in commercial power reactors that have engineering features added to fulfill the requirements of safety. Provision of multiple echelons of defense against accidents has been the route to minimize the probability of accidents, particularly those associated with high consequences. Certain passive features, including lowering of power density, higher coolant inventory, and ability to establish natural circulation, have also been added whenever needed to satisfy emerging safety concerns. These systems offer a well-demonstrated engineering solution to exploitation of nuclear energy in a safe manner. Although the track record of the nuclear power industry has been very good, the concern about very low-probability events (severe accidents), which in theory could occur tomorrow, has been expressed often. Very low probabilities are yet to be accepted by the public. Similarly, there appears to be some linkage in the minds of lay public between a severe nuclear power-reactor accident and the explosion of a nuclear bomb. Although there is no comparison between the two (a nuclear power reactor can never explode like a bomb[1]), the general public probably does not fully understand this.

The accidents at Three Mile Island and Chernobyl have added to public concern. One could hope that these would turn out to be blessings in disguise in the long run in terms of creating a more realistic viewpoint toward nuclear energy. After all, even a severe accident like the one at Chernobyl has turned out to be much less damaging than some man-made and natural disasters. The accidents at Bhopal and Morvi are just two glaring examples of man-made events that have taken place in our country in recent times and have caused much more damage than the accident at Chernobyl; the accident at Chernobyl, however, has had a greater psychological impact.

The development of inherently safe reactor systems has attracted much attention in recent years. These systems achieve safety because of their physical characteristics and do not depend on the working of an active component, which, however reliable, has some probability of failure. These inherently safe systems are expected to provide assurance that consequences greater than an acceptable maximum are not likely to occur. Obviously, this idea would lead to a greater degree of public acceptance if it could be convincingly demonstrated to be valid.

A number of new systems that could belong to this category have been visualized.[2,3] Also, some of the existing reactor systems have been assessed for the degree of inherent safety that is built into them; of the existing commercial power-reactor types, the pressurized heavy-water reactor (PHWR) has been identified as one reactor system with a considerable degree of inherent safety. PHWR thus offers a practical, viable, engineering system, well demonstrated under Indian conditions, that should be acceptable to the public. Because PHWR is the mainstay of the current state of our nuclear power program, its safety characteristics are of interest, particularly in light of the preceding discussion. This article describes these characteristics and demonstrates that the limiting worst-case accident in the case of a PHWR would have a low consequence to the public.

PRESSURIZED HEAVY-WATER REACTOR

The PHWR (Fig. 1) consists of a calandria (reactor vessel) that houses a number of coolant channels. These channels contain fuel bundles that generate nuclear heat through a fission chain reaction. The pressurized (approximately 100 bars, 300°C) heavy-water coolant flowing over the fuel bundles removes the heat from the fuel bundles and transfers it to light water in the steam generators to generate steam. The primary heat transport pumps recirculate the heavy-water coolant through this coolant circuit.

The calandria contains moderator heavy water that is maintained at a low temperature (approximately 75°C). The calandria also houses various reactivity control devices used for regulating the reactor power and for shutdown of the reactor. These systems operate in a low-pressure (near atmospheric) environment. Two independent shutdown systems (both fast acting), distinct from the regulating system, are provided in a standardized PHWR.

The reactor has an on-power refueling system. As a result, it is not necessary to keep reactivity in excess of immediate requirements in the reactor core. Thus the system has very low excessive reactivity. This is an important characteristic providing an inherent limitation on the maximum power excursion that can take place.

The calandria is submerged in water contained in the calandria vault. The entire reactor system is enclosed by a double containment (Fig. 1). A passive vapor

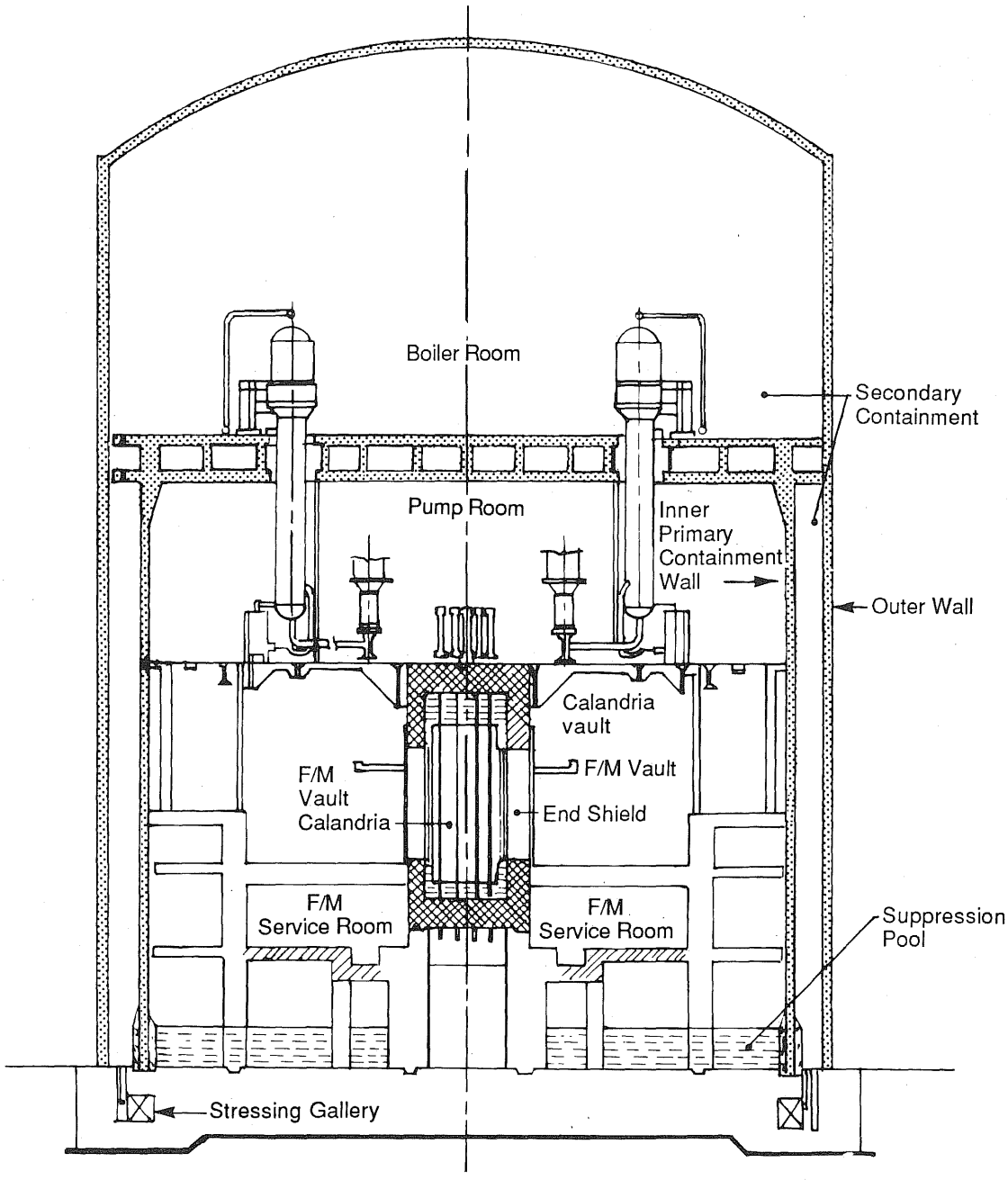

Fig. 1 Schematic diagram of Indian pressurized heavy-water 235-MW(e) reactor. F/M stands for "fueling machine."

suppression system is provided within the inner containment to absorb energy released in case of a loss-of-coolant accident (LOCA). An emergency core cooling system (ECCS) is provided to cool the core in case of a LOCA.

All reactor systems are designed for high levels of reliability and integrity to ensure good economy and safe performance. Reliability analyses of various important systems,[4] which are based on the best available data, are given in Table 1. Such estimates are obtained as a part of probabilistic safety assessment (PSA) studies performed during design and development of various reactor systems. Through frequent testing as a part of mandatory operating practice, validity of these reliability data is ensured.

Table 1 Summary of Reliability Analysis

System	Frequency/ probability of failure
Emergency core cooling	3.2×10^{-3}
Reactor building isolation	2×10^{-4}
Reactor shutdown system, mechanical shutoff rods	2×10^{-5}
Reactor shutdown system, liquid poison injection	5×10^{-4}
Moderator circulation	3×10^{-3}
Calandria vault circulation	5×10^{-2}
Large-break LOCA	1×10^{-4}/yr
Medium-break LOCA	1×10^{-2}/yr
Small-break LOCA	1×10^{-2}/yr

The reactor control system and surveillance on operating parameters normally ensures that the reactor would remain within the operating domain and would be safely shut down in case of any abnormality. It is worth while, however, to explore some abnormal event sequences regardless of their low probability of occurrence and examine how the system would behave in such situations. Such studies are useful for obtaining assurance about overall safety as a complementary exercise in addition to various safety evaluations concerning design and operation of the reactor.

SAFETY CHARACTERISTICS OF THE PHWR

For safety, a reactor system should have the following capabilities at all times:

- Ability to shut down the reactor.
- Ability to cool the reactor core.
- Ability to contain radioactivity.

In a practical reactor system, these capabilities are built in through a combination of inherent system characteristics and engineered features. Usually a number of alternative features are available to provide multiple echelons of defense to ensure availability of the three requirements.

The PHWR will now be examined in terms of the preceding requirements. As mentioned earlier, the reactor shutdown can be achieved by two diverse fast-acting shutdown systems independent of each other and also independent of the normal power regulation system. This is a feature specific to PHWR and makes the probability of failure to shut down the reactor orders of magnitude lower than other reactor systems and thus may be considered virtually impossible. Furthermore, since these shutdown systems are located in a low-pressure environment in contrast to pressure-vessel-type reactors located in a high-pressure environment, their design is simpler and possibilities of accidental control element ejection are virtually eliminated. Thus failure to shut down is much less probable in a PHWR than in light-water-cooled reactors (LWRs). Further, low worth of the individual reactivity devices and their simpler construction and operation in a low-pressure environment virtually eliminate any reactivity transient of any consequence related to reactivity devices. The prompt neutron lifetime (about 1 ms) in a PHWR is relatively longer than that in an LWR, and also the delayed neutron fraction is enhanced as the result of the presence of delayed photoneutrons. These factors slow down a potential power excursion considerably. Even the most unlikely power excursion would be limited because of inherent system characteristics.

The requirement of core cooling will now be examined. Table 2 compares power density and specific power of some of the typical reactor systems. As shown, PHWR has both these parameters on the low end of the spectrum. Thus PHWR would have a greater safety margin than other reactors. The cooling crisis in case of a loss of coolant in a PHWR is therefore more easily managed. A reliable ECCS is provided for the PHWR as in other reactors. The ECCS for a PHWR, however, should be capable of ensuring that no gross fuel failure would take place in case of a LOCA (Ref. 5).

What if emergency core cooling fails? Strictly speaking, this probability is rather low. Although in

Table 2 Average Power Density and Specific Power for Various Reactor Systems

Reactor[a]	Average power density, kW/L	Specific power, kW/kg
PHWR	9.2[b]	16
BWR	50[c]	18
PWR	85[c]	28
RBMK	4[d]	18

[a]Abbreviations used: PHWR, pressurized heavy-water reactor; BWR, boiling-water reactor; PWR, pressurized-water reactor; RBMK, heterogeneous, thermal–neutron pressure-tube-type reactor (U.S.S.R.).

[b]Moderator: cool heavy water.

[c]Moderator: water at same temperature as coolant.

[d]Moderator: graphite hotter than coolant.

most other water reactor systems it would mean a core melt, in a PHWR we have further defense: the presence of a cool moderator in the calandria. It has been shown that, as long as moderator cooling is available, the fuel will remain at a temperature below its melting point.[6]

Although we have already reached a sequence with probability so low that it can be considered impossible, we can argue further and ask: What if moderator cooling also fails? It has been estimated that, although the core may be severely damaged in such a case, the presence of cooling by vault water would maintain the calandria wall intact and permit cooling of core debris on the inside of the calandria wall. Although some local fuel melting may occur, the debris would eventually be cooled. Because this phenomenon is somewhat delayed, the loading on the containment through this accident sequence is well within its capability, and the impact of this sequence in the public domain is not likely to be any bigger than the design-basis accident (double-ended rupture in reactor inlet header).[7]

The PHWR thus has much greater diversity in cooling functions, which limit the extent of core damage. The alternative cooling modes are not specifically provided but are available as secondary functions of other primary functions, which would keep the system operating normally and ensure the availability of the cooling function on demand. The PHWR system is unique in this respect.

The third requirement, that of containing radioactivity, will now be examined. A number of barriers exist to prevent escape of radioactivity. Because containment is the ultimate barrier to the release of radioactivity in case of an accident in the core, particular care is exercised in containment design. The principle of double containment is used:

- Inner or primary containment designed for an internal pressure that would not be exceeded in an accident with a leak rate of approximately 0.1% of the contained volume per hour at the design pressure.
- Outer or secondary containment for which the design pressure is nominal with a leak rate again of 0.1% of the contained volume per hour.

Care has been taken to ensure that the provision of double containment extends over all penetrations and leak paths.

The layout considerations require a rather large containment for the PHWR, which adds certain useful safety features in terms of buildup of maximum hydrogen concentration, greater capacity, etc.

In addition to the large containment volume in a PHWR, various other engineered safety features are provided to further limit the consequences in the public domain. Automatic isolation of the containment is initiated in the event of a pressure rise or activity buildup in the containment. A pressure suppression system incorporating a suppression pool is used for limiting the peak pressure. This is an entirely passive system, and thus its availability is ensured to condense part of the steam and dissolve radioactive products in case of a postulated LOCA. The huge amount of suppression pool water is also used during long-term recirculation modes of ECCS. Because it is desirable to cool down and thereby depressurize the containment following an accident, a system of distributed building air coolers is provided for a fast depressurization. The coolers are supplied from an ensured process water supply, and the fan motors are fed on class III power supply from diesel generators to improve the system reliability.

Two systems have been provided for postaccident cleanup of atmosphere in the containment. In the primary-containment filtration and pump-back system, airflow is recirculated within the primary containment through the charcoal filter to perform containment atmosphere cleanup operation on a long-term basis. The secondary containment filtration, recirculation, and purge system provides multipass filtration and mixing by recirculation within the secondary containment space and also maintains a negative pressure. The negative pressure maintained in the secondary containment space brings the net ground-level release down to very small values.

The containment system has received the attention of our designers from the very beginning. In its present form, the containment of PHWRs is perhaps the best. We have a double containment with fully passive energy management features, a configuration far improved over the earlier concepts.

A large number of accident sequences have been analyzed, and it has been found that, as long as containment is available, there is virtually no additional impact in the public domain regardless of the accident scenario considered. There is no possibility of a threat to containment integrity.[8] Similar conclusions have been reached for similar reactors abroad.[9] It must be mentioned here that some of the sequences considered in the preceding study include failure to effect a prompt shutdown following a LOCA. Such a sequence is highly improbable. Further, on the basis of a study of the consequences of this accident sequence

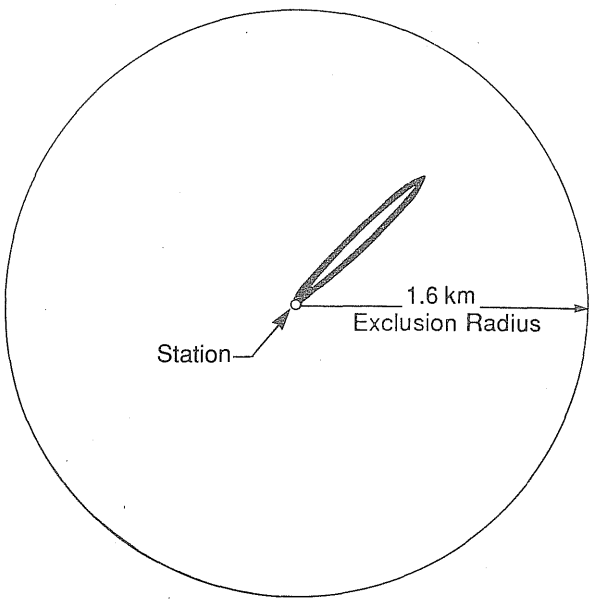

Fig. 2 Isodose curve for 50-rem thyroid inhalation dose.

and considering the resulting metal–water reaction, hydrogen generation, and energy liberated, the impact in the public domain is not greater than that already considered for the design-basis accident.[8] This is so because, even though the release from the core would be more, assuming the availability of the containment, the impact would be well within the exclusion radius. This is illustrated in Fig. 2, which depicts the zone in which the acceptable dose levels would be exceeded in an accident involving the failure of ECCS and shutdown following a LOCA. This zone is well within the exclusion radius. It is important to realize that the failure to shut down implies failure of the reactor protection system to bring about prompt subcriticality only and that reactor shutdown is subsequently achieved.

In any case, this brings out the important role played by the containment and validates the importance attached by our designers to evolution of a sound indigenous containment concept for PHWRs such that it effectively limits the consequences even when the entire core inventory of I-131 and noble gases is assumed to be released from the core.

PROBABILISTIC SAFETY ASSESSMENT

There is no unique set of rules by which different reactor designs may be judged safe or unsafe. The PSA methodology, however, offers means of risk comparison. The results of a number of PSAs performed through 1983 are presented in Ref. 10, wherein the range of core-melt frequencies (CMFs) for a pressurized-water reactor (PWR) varies from 1×10^{-6}/yr to approximately 1×10^{-3}/yr with a median of approximately 6×10^{-5}/yr. An examination of variability in the results indicates that quantitatively pinpointing reasons for the differences is extremely difficult. It is possible, however, to uncover general reasons attributable to plant design, operation, site characteristics, scope of the studies, methods employed, and assumptions postulated. In any case, extreme caution is essential when comparing the quantitative results of various PSAs. Table 3 compares the CMFs along with relative contributions of different initiating events in case of a typical PWR and PHWR. For comparison, numbers from the Sizewell-B study[11] are also shown.

The core damage frequency[a] (CDF) of a PHWR (Ref. 4) is estimated at 4×10^{-6}/yr, which is toward the lower range quoted in Ref. 10. Because CDF is obtained from aggregating the frequencies of various dominating accident sequences as identified in the PSA, a general comparison between PHWRs and PWRs may be attempted in terms of relative contributions from the respective dominating accident sequences of the two types of reactor units. LOCAs (particularly small-break LOCAs), coupled with the failure of emergency injection and the long-term decay heat-removal system, contribute about 60 to 70% to CMF in case of some PWRs. This contribution, in case of a PHWR, is not so because of the presence of the moderator as a heat sink in the calandria. Various studies[6] indicate that, in case of LOCA and failure of ECCS in a PHWR, no fuel melting is likely to occur. Thus the probability of failure of the moderator as a heat sink must be coupled with the failure of ECCS in the accident sequences initiated by LOCAs to reach core-melt probability. This factor is estimated as 3×10^{-3} and significantly reduces CDF as the result of such accident sequences.

Further, in view of the provision of two diverse, independent and fast shutdown systems in a PHWR, the contribution of accident sequences arising from anticipated transient without scram (ATWS) situations is significantly reduced. As a result of the pressure tube concept in PHWR involving several hundred coolant

[a]In case of a PHWR, on account of greater redundancy in residual heat removal, a large-scale core melt is less probable. Hence we prefer to use the term "core damage frequency" in the context of PHWRs.

Table 3 Comparison of Initiating Event Contributions to Core-Melt Frequency of Various Reactor Systems[a]

					PHWR	
Initiating event	CMF	Percent of total	General CMF	PWR (percent of total CMF)	CDF	Percent of total
Large LOCA	1.83×10^{-7}	15.8	9.6×10^{-6}	16	1.0×10^{-9}	0.03
Medium LOCA	2.5×10^{-7}	22.22			1.0×10^{-7}	2.8
Small LOCA	3.83×10^{-7}	33.0	1.9×10^{-5}	32	3.3×10^{-7}	9.0
Loss of offsite power	6.0×10^{-9}	0.5	1.4×10^{-5}	19	2.3×10^{-6}	62.2
Loss of feedwater	1.58×10^{-8}	1.4	8.4×10^{-6}	14	1.66×10^{-7}	4.5
Turbine trip	1.0×10^{-9}	0.1			1.0×10^{-8}	0.3
Main steam-line break	5.8×10^{-8}	5.0			3.2×10^{-8}	0.9
Active process water					8.0×10^{-8}	2.2
Nonactive high-pressure process water					6.6×10^{-7}	17.8
ATWS	1.37×10^{-7}	11.8	5.4×10^{-6}	9	1.0×10^{-8}	0.3
Others	1.0×10^{-7}	10.0	6.0×10^{-6}	10		
	1.0×10^{-6}	100	6.0×10^{-5}	100	4.0×10^{-6}	100

[a]Abbreviations used: ATWS, anticipated transient without scram; CDF, core damage frequency; CMF, core-melt frequency; LOCA, loss-of-coolant accident; PHWR, pressurized heavy-water reactor; PWR, pressurized-water reactor.

channels and the associated inlet and outlet feeder tube connections, the probability of a medium LOCA is somewhat higher (1×10^{-2}/yr, which in the case of LWRs is 1×10^{-3} to 1×10^{-4}/yr). This was accounted for in the analysis and does not show up as a significant contribution to CDF. Failures of pressure tubes in Pickering and Bruce did raise concerns about pressure tube safety. It is important, however, to realize that, in both instances of pressure failures, it was possible to mitigate the consequences without invoking the engineered safety systems, and also the affected channels could be replaced. The possibility of replacing the pressure tube would be a significant contributor in extending the life of a PHWR beyond the stipulated period. In the long run, one would expect the failure probability of the pressure tube to be consistent with the normal pipe failure rates. LOCA caused by failures in refueling operations, as well as other fuel-handling failures, has been considered in the PSA of the PHWR.

The dominant accident sequence in our context is station blackout caused by the high frequency of normal power (Class IV) failures. Because this is due to grid fluctuations more than to the characteristics of nuclear power plants, the effect would be more or less the same for different types of designs. An independent emergency cooling system for steam generators is provided wherein the pumps are driven by dedicated diesel generators independent of the emergency power supply. Thus the thermosyphoning mode of cooling on the primary side would be effective as long as the secondary-side flow is maintained. Even in case of a station blackout, when the moderator circulation is not available, the low-temperature pool of the moderator is available, which would delay the onset of fuel failure. In any case the vulnerability of the plant to this situation is realized, and in the current designs, $3 \times 100\%$ diesel generators are being provided to reduce the frequency of station blackout.

CONCLUSIONS

The CDF for the PHWR is at the lower end of the spectrum of CMFs for various PWRs. Further, because of the characteristics of PHWR systems, the impact in the public domain of even a worst-case accident in the PHWR is not likely to be any greater than that of the design-basis accident, which is considered while licensing the plant. Similar conclusions have also been reached for this type of reactor abroad.[9] PHWR reactors therefore have the distinct advantage of providing a viable engineering system with proven economics and ensuring a definite limitation on the worst consequences to the public.

REFERENCES

1. United Kingdom Atomic Energy Authority, *The Chernobyl Accident and Its Consequences,* Report NOR-42005, 1988.
2. Karl O. Ott, Inherent Shutdown Capabilities of Metal-Fueled Liquid-Metal-Cooled Reactors During Unscrammed Loss-Of-Flow and Loss-Of-Heat-Sink Incidents, *Nucl. Sci. Eng.,* 99: 13-27 (1988).
3. *Nucl. Saf.,* 28(1) (1987).
4. A. K. Babar et al., *Probabilistic Safety Assessment of Narora Atomic Power Project,* Bhabha Atomic Research Centre, Bombay, India.
5. G. Kugler, *Distinctive Safety Aspects of the CANDU–PHW Reactor Design,* Report AECL-6789, Atomic Energy of Canada Limited, 1980.
6. W. T. Hancox, *Safety Research for CANDU Reactors,* Report AECL-68034 (CONF-8112101-1), Atomic Energy of Canada Limited, October 1982.
7. J. T. Rogers, *Thermal and Hydraulic Behavior of CANDU Cores Under Severe Accident Conditions,* Report INFO-0136-2, 1984.
8. Bhabha Atomic Research Centre, Bombay, India, *Chernobyl Task Force Report,* 1988.
9. Hare Commission Report, *The Safety of Ontario's Nuclear Power Reactors,* February 1988.
10. *Risk Anal.,* Vols. 3 and 4 (1983–1984).
11. *Sizewell-B, Sizewell-B PSA Study,* Report WCAP-9991, Westinghouse Electric Corporation, 1982.

Technical Note: The OECD Report *The Role of Nuclear Reactor Containment in Severe Accidents*

[Editor's Note: The Nuclear Energy Agency of the Organization for Economic Co-Operation and Development has recently issued a monograph titled *The Role of Nuclear Reactor Containment in Severe Accidents,*[1] which was assembled by a group of experts.[2] Since we believe this report to be of significance for the nuclear reactor safety community, we here reprint the Foreword and Executive Summary of this document.]

FOREWORD

In November 1986, the Senior Group of Experts on Severe Accidents of the NEA's Committee on the Safety of Nuclear Installations (CSNI) was invited to examine the role of containment in severe accidents and to report to the Committee on the outcome of its discussions.

The Senior Group's discussions have strengthened and supplemented with more detail the conclusions reached in its previous report, *Severe Accidents in Nuclear Power Plants* (published in May 1986). It is now widely recognised that containments should play a major role in the management of the severe accidents. No fundamental shortcomings calling for radical change have been identified in existing designs.

Current relevant R&D activities are reasonably extensive and show an awareness of major issues; the Senior Group wishes to emphasize that it has not identified major shortfalls in existing research. Nevertheless it regards continuing research by OECD Member countries as vital, not least because of the need to base decisions on a realistic approach rather than on limiting (so-called "conservative") cases which might lead to inappropriate procedures.

The experts who prepared the report are listed at the end of this volume.[2]

EXECUTIVE SUMMARY

1. One of the principal conclusions in the report of the Senior Group of Experts on Severe Accidents (published May 1986) was that containments[a] in general have great potential to mitigate the consequences of a severe accident. They are not designed specifically for that purpose, but in practice the specifications of the basis to which they are

[a]In its 1986 Report the Senior Group defined "containment" as a structural envelope which completely surrounds the reactor system and is designed to hold the releases from design basis accidents with little or no release to the environment. The term is used in its broader sense to include associated leakage paths and buildings which contain the releases of severe accidents.