Ann. Rev. Energy. 1985. 10 : 431–62

INHERENTLY SAFE REACTORS[1,2]

Irving Spiewak and Alvin M. Weinberg

Institute for Energy Analysis, Oak Ridge Associated Universities, Post Office Box 117, Oak Ridge, Tennessee 37830

INTRODUCTION

No power reactor has been ordered in the United States, and 70 reactors have been cancelled, since 1978; one must therefore wonder whether nuclear energy will survive here. This same question is being asked in many European countries, for example in Sweden, where a 1980 referendum calls for shutting down all of Sweden's 12 reactors by 2010—even though they now produce more than half of Sweden's electricity. David Lilienthal, the first Chairman of the Atomic Energy Commission, in his most recent book, *Atomic Energy: A New Start*, published in 1980 (1), recognized the precariousness of the nuclear option. He called on nuclear engineers to come up with a technical fix: a reactor that both friends and foes of nuclear energy would agree could not under any circumstances suffer the fate of the Three Mile Island-2 reactor—in short, a reactor that was transparently and patently immune from a core melt. This he regarded as the key to a rebirth of nuclear energy.

Lilienthal's views had been anticipated by several technologists and energy analysts, particularly in Sweden and Germany, and in the United States. Soon after Lilienthal's book appeared, the Institute for Energy Analysis convened a dozen old-timers who had been responsible for setting nuclear energy on its main technical paths, to consider Lilienthal's

[2] Abbreviations used: LWR, light water reactor; PRA, probabilistic risk assessment; CMP, core melt probability; RY, reactor year; HTGR, high-temperature gas-cooled reactor; PWR, pressurized water reactor; BWR, boiling water reactor; APWR, advanced pressurized water reactor; PIUS, process inherent ultimately safe; LOCA, loss-of-coolant accident.

challenge: Could inherently safe reactors be designed? (2) If inherently safe reactors could be built at competitive costs, would their use restore the public's confidence in nuclear energy? The old-timers' workshop concluded that such a reexamination of the technical options was appropriate; and the Mellon Foundation supported the Institute for Energy Analysis in an examination of a "Second Nuclear Era" that would be based on inherently safe reactors. About the same time, studies by the Office of Technology Assessment (3) and by the Massachusetts Institute of Technology (4) addressed many of the same questions.

All three studies concluded that inherently safe reactors were feasible. The three studies, however, differed in emphasis; IEA focused strongly on inherently safe reactors as technical fixes, whereas OTA and MIT considered institutional improvements as well as improved light water reactor technology as the probable route to a revival of nuclear energy in the United States. Here we shall review mainly the technology of inherently safe reactors.

ACTIVELY SAFE AND PASSIVELY SAFE REACTORS

When nuclear reactor design began in 1942, safety was always a strong concern, but the idea of a reactor whose core could not melt never occurred to the early designers. Commercial power reactors in the United States grew out of pressurized water reactors, which were originally designed for ships. Compactness and simplicity, not inherent safety, were their primary design criteria. Thus the low thermal inertia of the light water reactors (LWRs), which meant that if uncooled, the temperature of the water in a 1000-MW(e) reactor would rise 30°C/min even after a scram, was a design constraint that had to be lived with. As commercial reactors grew in size, the possibility of a core melt became an increasingly dominant challenge for reactor designers. Since the LWR leaves so little time for remedial action if something goes awry, designers have festooned LWRs with many safety systems—e.g. the High Pressure Safety Injection System, Fast Acting Scram Rods, and Core Sprays. In consequence, modern LWRs are immensely complicated. They depend for their safety not on intrinsic properties of the reactor itself or on passively activated systems, but rather on the active intervention of electromechanical devices, such as valves, scram rods, emergency pumps, and backup diesels. What is true of LWRs is to some degree true of all other commercial reactors—their safety depends on active interventions, sometimes including action by the operators. We shall call such reactors "actively safe."

To estimate the likelihood of mishap in an actively safe reactor, one must resort to probabilistic risk assessment (PRA)—i.e. one tries to imagine all events that can lead to core damage; one then assigns a probability to each of these events. This procedure was used by Rasmussen in his famous WASH-1400 (5): he concluded that the median core melt probability (CMP) in light water reactors was 5×10^{-5} per reactor year. He assigned an uncertainty factor of around 5 to this estimate, but others (as well as Rasmussen, on further reflection) have put the uncertainty higher (6, 7).

Regardless of one's degree of confidence in PRA as a means of estimating the likelihood of a core damaging event, all must agree that one can reduce that likelihood by adding redundancy. For example, a PRA for the Calvert Cliffs reactor revealed the most important contributor to its rather high core melt probability (2×10^{-3}) was the failure of its single auxiliary feedwater train. A second train was added; this reduced the estimated core melt frequency some fivefold (8). Thus one approach to achieving Lilienthal's safe reactor would be to add more active safety systems. This "incremental" approach to safety builds entirely on existing technology; it suffers, however, from its dependence on active systems that may fail. Though enough redundancy can reduce the probability of failure to arbitrarily small values, skeptics can always claim that not all events leading to accidents can be imagined, that the probabilities used in PRAs are faulty, or that acts of war or sabotage or earthquake (so-called external events) can nullify the active safety systems.

The alternative way of meeting Lilienthal's call for a "safe" reactor is through passive systems that rely on inherent characteristics of the reactor. Such reactors we shall call passively or inherently safe. For example, if a reactor has large thermal inertia, it is obviously less likely to melt than if it has low thermal inertia. Or if it is encased in a totally inaccessible concrete structure, it is probably immune from sabotage or acts of conventional war. Thus, inherently safe reactors are safe not because of the intervention of active systems, which always have some probability of failure, but because of the workings of immutable laws of thermomechanics, of gravity, and of nuclear physics. The trick is to choose reactor configurations that embody such immutable principles.

In some sense there is no such thing as a totally safe reactor. Some events, with probabilities of, say, 10^{-9} per reactor year (RY), that could damage even the most inherently safe reactor can probably always be conceived. One can argue that, ultimately, one relies on a PRA, albeit a very far-fetched one, for ensuring safety. Thus one can hardly avoid answering the question, "How safe is safe enough?", even with inherently safe reactors. However, as we shall see, some of the advanced actively safe reactors yield PRA estimates of core melt in the range of 10^{-7}/RY, and passively safe reactors yield PRA estimates of 10^{-8}/RY—1000–10,000 times lower than the safety goals promulgated by the NRC. Reactors with such low CMPs ought to be regarded as meeting Lilienthal's call for a safe reactor.

A reactor that puts out little heat, and that by design is resistant to large overpower transients, can hardly cause much damage to itself or to its environs. This had been realized at the time of the Ergen task force on the China Syndrome (9). Ergen, in private discussion at the time, asked at what maximum power would a reactor, after shutdown, be able to dissipate its heat to the environment by natural convection and conduction. His answer, around 30 MW, was not considered of practical importance; but it does illustrate that smaller, by and large, is safer.

This perception of "smaller is safer" fits nicely with the current outlook of almost all American utilities. Having been stung by brutal cost overruns in 1000-MW nuclear plants, and faced with all but indeterminate projections of future load growth, utilities are interested in modular plants, whether nuclear or fossil-fueled. The modules might be as small as 100 MW, could be built quickly, and could be grouped to make large plants. Modular plants are being examined by several manufacturers.

Though modular plants fit better into most utilities' plans for expansion than do large plants, they would appear to sacrifice economy of scale for greater intrinsic safety. Does this imply that utilities choosing modular plants might be committing to higher cost electricity than they would were they to buy a small share of a larger plant? Perhaps, but large plants might also be made intrinsically safe, and modular plants might be made economical through factory construction and very rapid deployment at the utility's site. Of course, these considerations are rather speculative since we have no firm data on the economics of small modular plants, nor on the intrinsic safety of large, advanced ones.

THE TECHNOLOGY OF SAFER NUCLEAR PLANTS

The terms "intrinsically safe" and "forgiving" for reactors were introduced around 1980 by Fortescue, Hannerz, and O'Farelly (10–12). In the intervening years the idea has caught on remarkably; intrinsic or passive safety features have been incorporated in newly developed actively safe reactors; and several truly inherently or passively safe reactors are now under consideration (13). We now describe these proposals for both actively and passively safe reactors as of 1984.

Actively Safe Reactors

The world's power reactors are classed as actively safe reactors, though they incorporate passive features to varying degrees. Here we discuss only those that might be considered for future deployment in the United States, the light water reactor, the CANDU pressurized heavy water reactor, and the high temperature gas-cooled reactor (HTGR).

Light water reactors account for 85% of the world's commercial power reactor capacity. In addition, all naval reactors and most research reactors are moderated and cooled by light water. Because this type is so dominant, and perhaps also because TMI-2 was a light water reactor (of the pressurized water type), most of the actual development effort has gone toward improving the safety of LWRs, both by incorporating passive safety features and by strengthening active safety features.

After the TMI-2 incident, the Nuclear Regulatory Commission mandated a number of backfits on existing LWRs to correct deficiencies revealed by the incident. The Rasmussen PRA had estimated a median core melt probability of the Surry pressurized water reactor (PWR) and the Peach Bottom boiling water reactor (BWR) to be 6×10^{-5}/RY and 3×10^{-5}/RY respectively, for an average probability of 5×10^{-5}/RY. This number has been widely quoted both in the literature and in the nuclear debate. An analysis by Minarick & Kukielka (14) of actual precursors to potentially serious events in operating reactors between 1969 and 1979 suggests that the actual core melt probability of the LWRs operating during this period was closer to 10^{-3}/RY. This number agrees with Okrent's pessimistic estimate (7). An analysis by these authors of precursors during 1980 and 1981 suggests that the core melt probability in the post-TMI period had fallen to around 15×10^{-5}/RY—within a factor of 3 of the core melt probability estimated in WASH-1400 (15). Following TMI-2, every LWR in the United States has been required to strengthen its equipment and operations and many have conducted PRAs, both with and without the NRC-mandated backfits. D. Phung has concluded from thesc analyses that the median core melt probability of US reactors with the TMI-2 backfits is now comfortably within the range estimated by WASH-1400 (16). This means that reactors today are perhaps six times safer than they were before 1979, when Minarick & Kukielka's semiempirical analysis found them to be considerably less safe than indicated by the WASH-1400 median estimate. The backfits responsible for these improvements in PRA estimates include direct measurement of the water level in the reactor—(recall that ambiguity in measurement of this water level at TMI-2 prompted the operators to shut off the emergency core cooling system, with disastrous results)—and direct measurement of the state of the pilot-operated relief valve (whosc failure to close, and incorrect indication of this state, led directly to the accident). Altogether Phung estimates that the backfits mandated in response to the TMI-2 accident will cost about \$25/kW(e) (17). Probably more significant than the plant changes have been changes in operator training and procedures. One must therefore concede that, insofar as PRA is a believable estimator of core melt probability—or better, PRA backed up by the semiempirical evidence of Minarick & Kukielka—today's LWRs are about as safe as Rasmussen claimed (CMP = 0.5×10^{-4}/RY). This is well within NRC's promulgated safety goal of 10^{-4}/RY.

IMPROVED PWRs From PRA one finds that small break loss-of-coolant acidents (such as occurred at TMI) are the largest contributors to the estimated core melt probabilities for PWRs (Figure 1) (18). To reduce the CMP, designers of PWRs have therefore focused strongly, though not exclusively, on measures to avoid or mitigate loss-of-coolant accidents. Such design precepts are exemplified in the Sizewell B PWR (19), the Advanced PWR (APWR) (21), and the Combustion System-80 PWR (20).

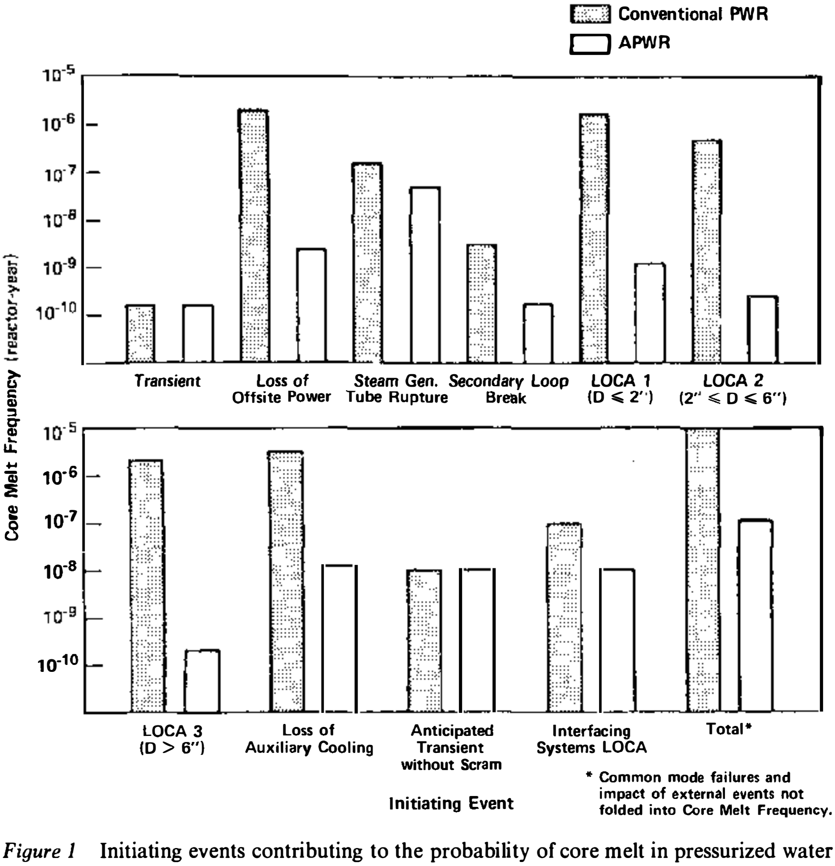


Figure 1 Initiating events contributing to the probability of core melt in pressurized water reactors. Source: (18).

The Sizewell-B PWR The United Kingdom, in collaboration with Westinghouse, has incorporated additional redundancy and diversity in the latter's Callaway Standardized Nuclear Unit Power Plant System (SNUPPS) design for its proposed 1300-MW(e) Sizewell-B PWR. Sizewell-B achieves a lower core melt probability through additional safety equipment, e.g.

1. Four high-pressure safety injection pumps, each with heads lower than 2000 pounds per square inch (psi) and higher flows than Callaway's.
2. Four accumulators, any two of which are sufficient for core cooling at the 600-psi range (instead of the required three at Callaway).
3. A steam-driven auxiliary feed pump, in addition to the two electric pumps already in SNUPPS.
4. Four diesel generators (instead of two) to provide emergency power.
5. An emergency boration system as a backup reactor trip system to cope with anticipated transients without scram.

These exemplify the dozen or so redundancies added to Sizewell-B. The United Kingdom Atomic Energy Authority and Westinghouse have estimated, by means of PRA, the median core melt probability of the Sizewell-B reactor to be only 1.1×10^{-6}/RY—almost 50 times lower than the WASH-1400 value—and the estimated probability of a large release of radioactivity to be only 3×10^{-8}/RY. The various contributors to this core melt probability are summarized in Table 1. The measures added to Sizewell-B to achieve its lower estimated core melt probability add about 20% to the cost of the reactor.

The APWR Westinghouse and Mitsubishi, together with five Japanese utilities and the Japanese government, are spending $\$150 \times 10^6$ to design a 1350-MW(e) Advanced Pressurized Water Reactor for deployment in Japan. The total CMP for APWR is estimated to be only 2×10^{-7} per RY—some 300 times lower than the CMP for the PWR analyzed by Rasmussen (Figure 1). The APWR contains a number of innovations compared to earlier Westinghouse four-loop designs. Here we dwell on those improvements that lead to the much lower estimated core melt probabilities for the APWR. These include:

1. The increased volume of primary coolant in the reactor vessel above the core increases the time available to deal with a loss of coolant.
2. A lower core power density increases safety margins.
3. There are four complete safeguard trains of mechanical equipment in the safety system.
4. A large emergency water storage tank is provided inside the containment as the water source for four safety injection pumps. This storage

Table 1 PRA for the Sizewell-B reactor core melt by initiating event (23)

Initiating event	Core melt frequency	Percentage of total core melt frequency
Large LOCA[a]	1.83×10^{-7}	15.8
Medium LOCA	2.58×10^{-7}	22.2
Small LOCA	3.83×10^{-7}	33.0
Steam generator tube rupture	1.91×10^{-8}	1.6
Secondary side break inside containment	2.32×10^{-8}	2.0
Secondary side break outside containment	3.54×10^{-8}	3.0
Loss of main feedwater	1.58×10^{-8}	1.4
Closure on one MSIV[b]	5.71×10^{-11}	<0.01
Loss of RCS[c] flow	8.11×10^{-11}	<0.01
Core power excursion	5.11×10^{-12}	<0.01
Turbine trip	8.36×10^{-10}	0.07
Spurious safety injection	1.44×10^{-10}	0.01
Reactor trip	8.54×10^{-10}	0.07
ATWS[d]	1.37×10^{-7}	11.8
Loss of off-site power/turbine trip	6.03×10^{-9}	0.5
Interfacing systems LOCA	2.37×10^{-9}	0.2
LOCA beyond capacity of ECCS[e]	1.00×10^{-7}	8.6
Total	1.16×10^{-6}	100.0

[a] LOCA = loss-of-coolant accident.
[b] MSIV = main steam isolation valve.
[c] RCS = reactor cooling system.
[d] ATWS = anticipated transients without scram.
[e] ECCS = emergency core cooling system.

tank automatically receives water flows from ruptures in steam generator tubes.

5. Containment sumps are kept filled with water to increase the available heat capacity.
6. Safety and control systems are separated to increase reliability and reduce common mode failures.
7. Four separate and hardened compartments are provided to house high- and low-pressure safety injection pumps. This feature reduces the likelihood of radioactivity release to the atmosphere and makes sabotage of the safety systems very difficult.
8. The control room is improved, with improved diagnostic capabilities.
9. The larger pressurizer and core provide for improved response to transients.
10. The large dry containment vessel is conservatively designed.
11. The steam generator secondary-side water inventory is controlled automatically.

12. There is injection of pressurized water to reactor coolant pump seals.
13. The reactor vessel neutron fluence is reduced.
14. The overall improvements in plant availability, reliability, and maintainability translate into improved safety.

Westinghouse has performed a comparative PRA of the APWR and a conventional PWR for internal events. The results are shown in Figure 1. The internal risk in the APWR appears to be dominated by the steam generator tube break accident, itself at the very low level of 10^{-7} core melts per reactor year. The reported total risk from internal events of less than 2×10^{-7}/RY is well below Westinghouse's target of 1×10^{-6}/RY overall risk from the APWR. External event analysis, which is site-specific, will be carried out later.

Combustion System-80 Combustion Engineering, Inc. (CE) currently offers a standard nuclear steam supply system, System-80, rated at 3800 MW(t) (1270 MW(e)). The first System-80 plant to be completed will be the Palo Verde plant of Arizona Public Service Company.

CE believes that the System-80 design has pioneered many features contributing to the safety of the plant. These features are now being offered by other vendors as well, either as backfits or incorporated into new designs. These features include:

1. Greater core thermal margin.
2. Large pressurizer volume to absorb loss of electrical load.
3. Improved secondary-side steam generator materials (stainless steels).
4. Use of two-of-four concurrent measurements of the same parameter to actuate safety systems, with one channel available for off-line testing.
5. Use of a core-monitoring computer to monitor core thermal-hydraulic parameters continually.
6. Advanced control room.

CE's efforts on future plants are concentrated on upgrading certain aspects of the System-80 design to increase reliability, decrease costs, and provide greater assurance of safety. To a certain extent, modifications may be required to satisfy new NRC regulations, but the primary driving force for these changes would be innovation based on construction and operating experience.

The further evolution of System-80 is expected to include the following features:

1. Simplification, to the extent possible.
2. Emphasis on reliability and maintainability.
3. High-quality steam generators and improved steam generator materials.

4. High-quality heat exchangers and condensers to avoid ingress of contaminants to the steam generator.
5. Upgraded control room and instrumentation.
6. Fewer pipe supports (seismic and pipe-whip criteria).
7. Optional full-pressure decay heat removal system.
8. Reactor pressure vessel design that greatly reduces the impact of neutron fluence.
9. Improved feedwater systems and control systems.
10. Design to avoid spurious trips.
11. Fully replaceable major equipment.

No PRA has been reported thus far for the System-80. It is anticipated that the design could achieve core melt frequencies of the magnitude reported earlier for the Sizewell-B plant.

BOILING WATER REACTORS The relative contribution to core melt probabilities of various initiating events in BWRs are shown in Figure 2 (22). In PWRs a pipe break followed by a loss-of-coolant accident poses the dominant threat of a core melt; in BWRs, transients—in particular loss of off-site power—are the dominant threat. Thus the main strategy for improving the safety of BWRs has to do with providing additional protection against loss of off-site power and other transients, and improving the on-site emergency power supplies.

The BWR/4, which represents the kind of reactor analyzed in WASH-1400, yields an estimated CMP of around 3×10^{-5}/RY. The standard General Electric (GE) offered, the BWR/6 GESSAR, has a reported core melt probability from internal sources of 4.7×10^{-6}—about 8 times lower than the CMP for the BWR/4. Most of this improvement results from better instrumentation and automatic depressurization of the reactor to make it easier to supply emergency feedwater. By contrast, the loss of off-site power remains the dominant contributor to CMP, at approximately 6×10^{-6}, compared to 8×10^{-6} for the BWR/4.

GE, Hitachi, and Toshiba are developing a 1350-MW(e) Advanced Boiling Water Reactor (ABWR) for which the CMP is claimed to be substantially below that of the BWR/6 GESSAR. The key changes in going from BWR/6 GESSAR to ABWR are summarized in Table 2.

GE has described a small BWR concept (23) with modest innovations to simplify safety functions (Figure 3). Gravity-driven shutdown rods and liquid poison injection provide assurance of shutdown. An isolation condenser increases assurance of decay heat removal. Water from the elevated pressure suppression pool will automatically flood the reactor vessel should it become depressurized. At the low end of the projected capacity range (200 MW(e)) the power is normally removed without

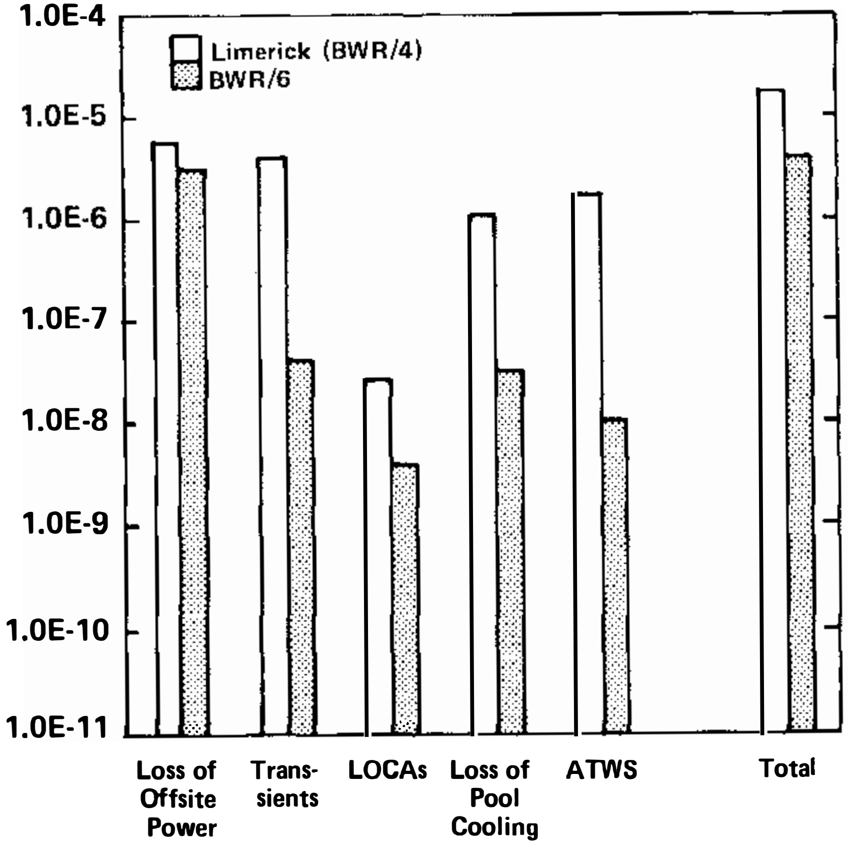


Figure 2 Initiating events contributing to the probability of core melt in boiling water reactors. Source: (22).

mechanical recirculation pumps; at the high end of the capacity range (600 MW(e)) internal circulation pumps are used, as in the Advanced Boiling Water Reactor.

THE CANDU-PRESSURIZED HEAVY WATER REACTOR The CANDU reactor has operated successfully since 1968, and a total of 16 CANDU reactors are in commercial operation in four countries.

The core consists of an array of horizontal pressure tubes surrounded by a low-pressure calandria containing the relatively cool moderator. Zircaloy-clad natural uranium fuel bundles are loaded and removed from the pressure tubes during operation by fueling machines operating at the two faces of the core. Heat is transferred from the heavy water primary

Table 2 Key differences between ABWR and GESSAR designs

Plant feature	GESSAR	ABWR
Recirculation system	External pumps Flow control valve	Internal pumps Solid state power supply
Control rod drives	Hydraulic	Electric/hydraulic fine motion
Emergency core cooling	Three divisions: 1 high-pressure spray 1 low-pressure spray 3 low-pressure flooders	Three completely separate divisions: 2 high-pressure sprays 1 steam-driven reactor core isolation cooling system 3 low-pressure flooders
Core spray sparger	Side	Overhead
Decay heat removal	2 steam-condensing heat exchangers	2 modulating valves 3 wetwell/drywell heat exchangers
Control of reactor flow, feedwater, and pressure	Analog	Digital
Transmission of control and safety signals	Wires	Multiplexed
Containment	Horizontal vents Steel Open pool Air	Vertical vents Concrete Covered pool Inerted
Steam bypass capacity	35%	100%
Fuel transfer	Inclined tube	Cask lift

Source: (20).

system to a light water secondary system in vertical U-tube steam generators.

Control of the CANDU reactor is maintained primarily through on-stream refueling. Computers control the routine plant operation.

The CANDU reactor is subject to many of the same potential accident initiators as a PWR. However, transients would generally occur more slowly because of the large thermal inertia of the moderator and pressure tubes. No PRA of a CANDU reactor has yet been reported, but preliminary estimates indicate a CMP of 10^{-5}/RY, in the same range as that of an LWR (24).

Studies of CANDU reactors for US construction (25, 26) have indicated that some design and licensing decisions could prove difficult. The pressure tubes, which contain the full primary system pressure, do not currently

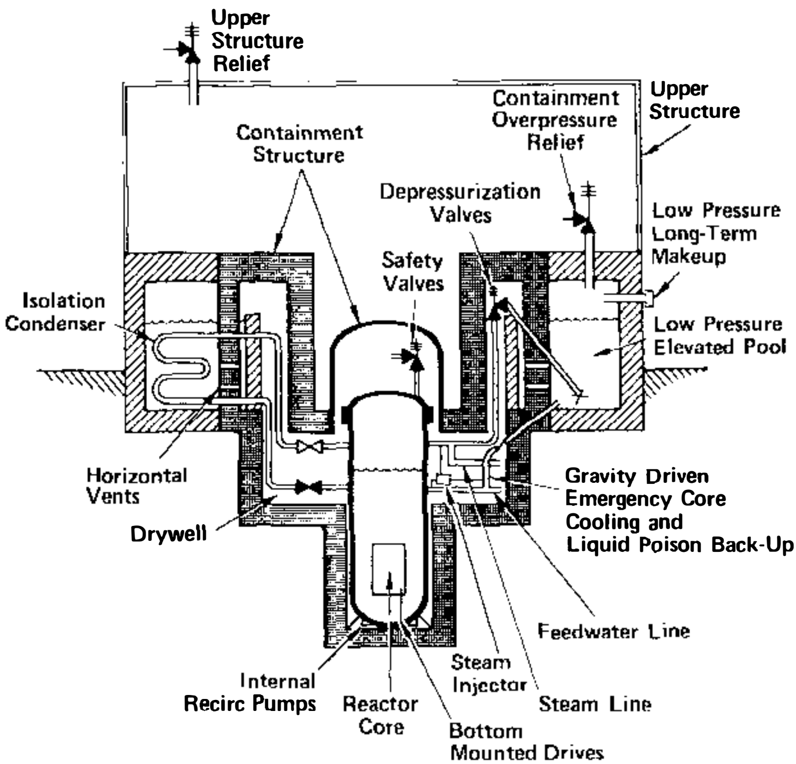


Figure 3 Small boiling water reactor concept with innovative safety features. Source: (23).

conform to the American Society of Mechanical Engineers Pressure Vessel Code. If the tubes were required to have thicker walls, then slightly enriched fuel would be preferred to natural uranium. Other features that would be novel to the Nuclear Regulatory Commission include the seismic analysis of the core, the use of on-stream refueling (and the security problems related to continuous fuel handling), and computer control of the reactor. It is our understanding that some Canadian studies of advanced CANDUs suited for Japanese or perhaps US application are under way but have not been publicly disclosed.

THE HIGH-TEMPERATURE GAS-COOLED REACTOR (HTGR) A prototype HTGR has been in operation at Fort St. Vrain in Colorado since 1979. A related high-temperature reactor, but with pebble bed instead of prismatic fuel, is in a startup process in West Germany. The HTGR is a helium-cooled, graphite-moderated reactor assembled in a prestressed concrete pressure vessel. The primary system pumps and steam generators are located in cavities in the vessel. Fuel is in the form of graphite-coated uranium oxide or uranium carbide particles in graphite blocks dispersed in a large stack of graphite moderator blocks. The superior high-temperature characteristics of the fuel and moderator allow the HTGR to generate steam at temperature and pressure conditions approximating those of modern fossil-fueled boilers.

The HTGR has some inherent safety advantages (27). Probably most important is the relatively low power density of HTGRs—between 5 and 10% of that of a conventional PWR. Further, because the fuel is dispersed throughout the moderator, the heat capacity closely associated with the fuel is over 100 times that of an LWR. Thus, in the event of an accident that interrupts the flow of coolant to the core, the elapsed time between the cessation of coolant flow and severe damage to the core (if no automatic or operator action is taken) is of the order of 10 hours in an HTGR, rather than tens of minutes for a PWR—a difference of more than an order of magnitude. One factor contributing to this feature is that lateral heat conduction through the graphite blocks in the HTGR core is sufficient to remove a substantial fraction of the afterheat from the core and carry it out through the reflector, from which the heat is radiated to the water-cooled steel liner of the reinforced concrete pressure vessel.

The HTGR's prestressed concrete pressure vessel has redundant load-carrying steel tendons, which are readily inspectable and replaceable. The tendons keep the concrete and the vessel liner in compression. The vessel is designed to withstand 2400 psi, over twice its operating pressure. Should a crack form during a pressure transient, the resulting small gas leak would tend to be sealed when the gas pressure was reduced. Thus, catastrophic failure of the vessel is not possible under loads possibly imposed by the HTGR.

The PRA of the reference HTGR indicates a fuel damage probability of 4×10^{-5}/RY, comparable to those of PWRs. It should be recognized that the character of the fuel damage in an HTGR would be less severe than that in an LWR. The fuel and graphite structure would remain basically as before, except that some of the more volatile fission products would escape from the coated fuel particles into the gas stream. Severe accident analysis of HTGRs indicates that there would be damage to the heat transport systems in the event that the dedicated core cooling systems fail and that there would be damage to the vessel should the linear cooling system be lost. However, most of the non–rare gas fission products are retained in the reactor vessel even in the worst accident scenario that has so far been envisioned.

Inherently or Passively Safe Reactors

Both the APWR and the ABWR, with CMPs below 10^{-6}/RY, must be regarded as extraordinarily safe, at least insofar as one is willing to trust probabilistic risk assessment. It is also plausible that advanced CANDUs and the HTGR could provide equal safety. Even if one is skeptical of PRA for absolute estimates of safety, one can hardly deny that PRA ought to be much more reliable for estimating the additional safety added by an incremental improvement on an existing reactor. One must therefore be impressed with the two and more orders of magnitude in reduction of CMP as one goes from existing PWRs and BWRs to APWRs and ABWRs, even if these estimates depend on PRA.

This additional safety incurs cost and complication. Anyone who has walked through a 1000-MW nuclear power plant must be impressed by its complexity; utility executives canvassed by the Electric Power Research Institute in 1982 (28), almost without exception, expressed dissatisfaction with the complexity of their nuclear plants.

Can this complexity be avoided, and safety possibly even improved, by designs that exploit inherent characteristics of the reactor? Can some external events, such as acts of nonnuclear war or sabotage, which are never considered in PRAs, be protected against? And can estimates of safety be made deterministic rather than probabilistic if the reactor incorporates clever enough passive safety features?

At least two well thought out proposals for reactors that meet such stringent criteria have been seriously proposed: The Secure-P or PIUS reactor, invented by K. Hannerz of ASEA/ATOM in Sweden (29); and the modular HTGR, originally proposed by G. H. Lohnert of Kraftwerk Union AG (KWU) (Interatom/GE) (30) and also by General Atomic (31). In addition, several other proposals for inherently safe reactors have appeared in the past few years.

THE SECURE-P OR PIUS (PROCESS INHERENT ULTIMATELY SAFE) REACTOR PIUS is a pressurized water reactor whose entire primary system, including the steam generator, is submerged in a large pressurized pool of cold water containing boric acid. The water containing boric acid, which is held in a huge prestressed concrete pressure vessel, is connected at top and bottom to the circulating primary system via a mechanically unblockable natural circulation circuit (see Figure 4). If the submerged pumps in the primary system are operating normally, the interfaces between pool and primary circuit are maintained. Should the primary circulation be disturbed in any way (pump failure or boiling in core, for

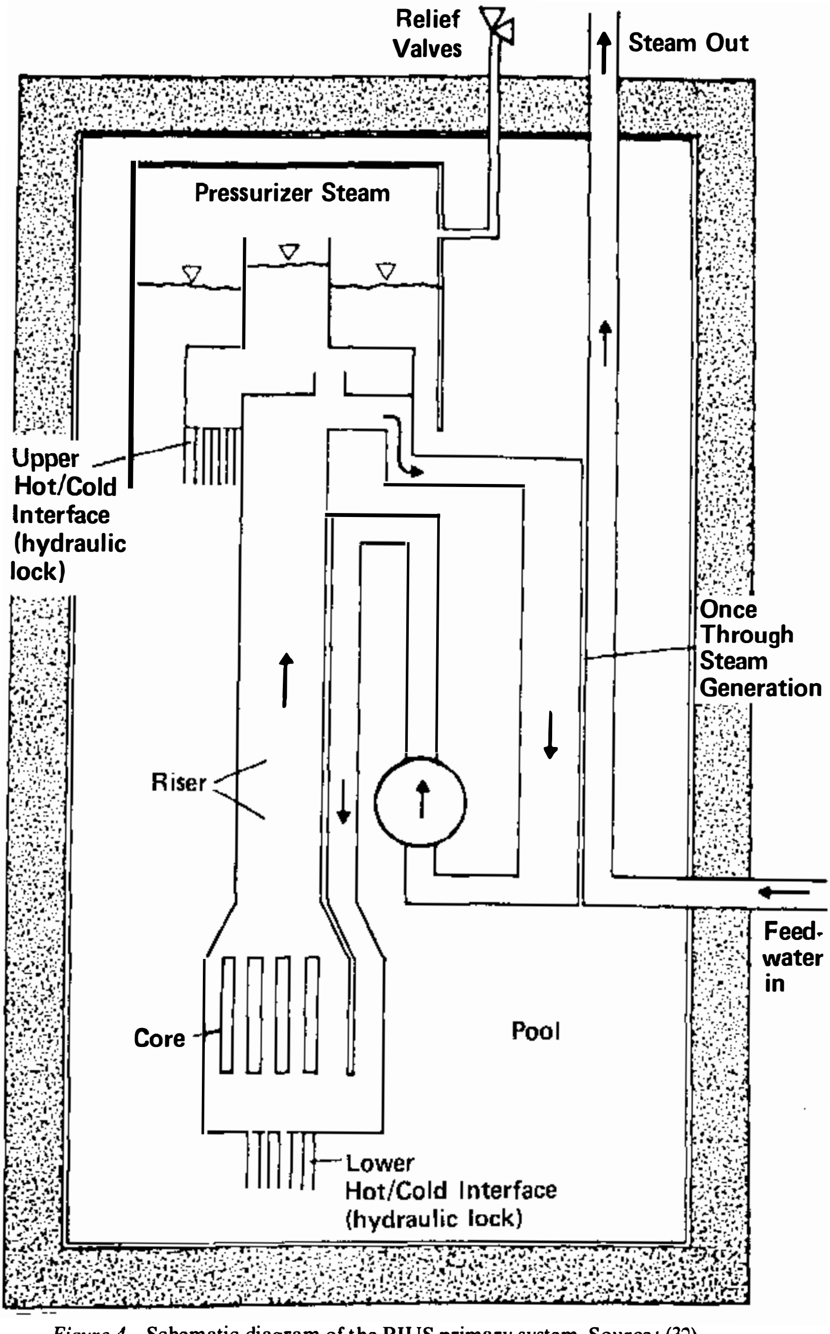


Figure 4 Schematic diagram of the PIUS primary system. Source: (32).

example) the cold boric acid is forced by gravity into the reactor, causing the reactor to shut down (because boron absorbs neutrons so strongly), and a natural convection circuit through the reactor and the pool is established. Enough water is in the pool to keep the reactor cool for at least a week, after which time a fire truck can provide additional water if necessary.

The PIUS reactor, through its very clever hydraulic locks, eliminates the low thermal inertia of the standard PWR. Because PIUS can thereby guarantee core integrity, it eliminates the risk of major releases of radioactivity by virtue of the laws of thermohydraulics and gravity alone. The redundant, diverse, spatially separated engineered safety systems now distributed throughout most of today's nuclear plants are no longer needed.

The response of PIUS to various transients has been studied by groups in Sweden and in Japan. As pointed out by Babala (32), all such transients can be divided into two groups according to the qualitative character of the final state: 1. transients that end with an autonomous reactor shutdown and 2. transients that end in a quasi-steady state at a new power level. For type 1 transients, caused, for example, by recirculation pump trips, total loss of secondary system heat sink, or depressurization of the system, the reactor automatically shuts down within 0.5–2 minutes because of the massive ingress of borated water. Figure 5 shows the results of Babala's simulation of the initial phase of a feedwater trip without scram (an event in an ordinary LWR that requires immediate intervention). The secondary side of the steam generator boils dry within 10 seconds, whereupon the primary system starts to heat up. The density of the fluid in the riser section of the loop decreases, and the event culminates in a brief void episode (between 23 and 28 seconds), which eventually overrides the pump controller that tries to keep the pool water out of the loop. The boron concentration in the core starts to rise at 28 seconds, and the reactor power is down to 10% after about 90 seconds.

Of type 2 transients, the one that often concerns critics of PIUS is inadvertent dilution of the boron in the pool. A simulation of continuous boron dilution caused by injecting 100 kg per second (twice the design maximum) of clean water into the loop leads to the following: the coolant density decreases as reactor power rises and borated water enters the loop at 340 seconds. A quasi-equilibrium is reached at 500 seconds, when the effect of the injected clean water is neutralized by a steady inflow of pool water. The 10% overpower that cannot be dissipated in the steam generators is deposited in the pool by natural circulation. Babala states that the external inventory of clean water will generally be exhausted before a dangerous increase in the temperature of pool water occurs.

The response of PIUS to transients has been studied, independently, in Japan (33), with results that generally confirm the claims made for PIUS—

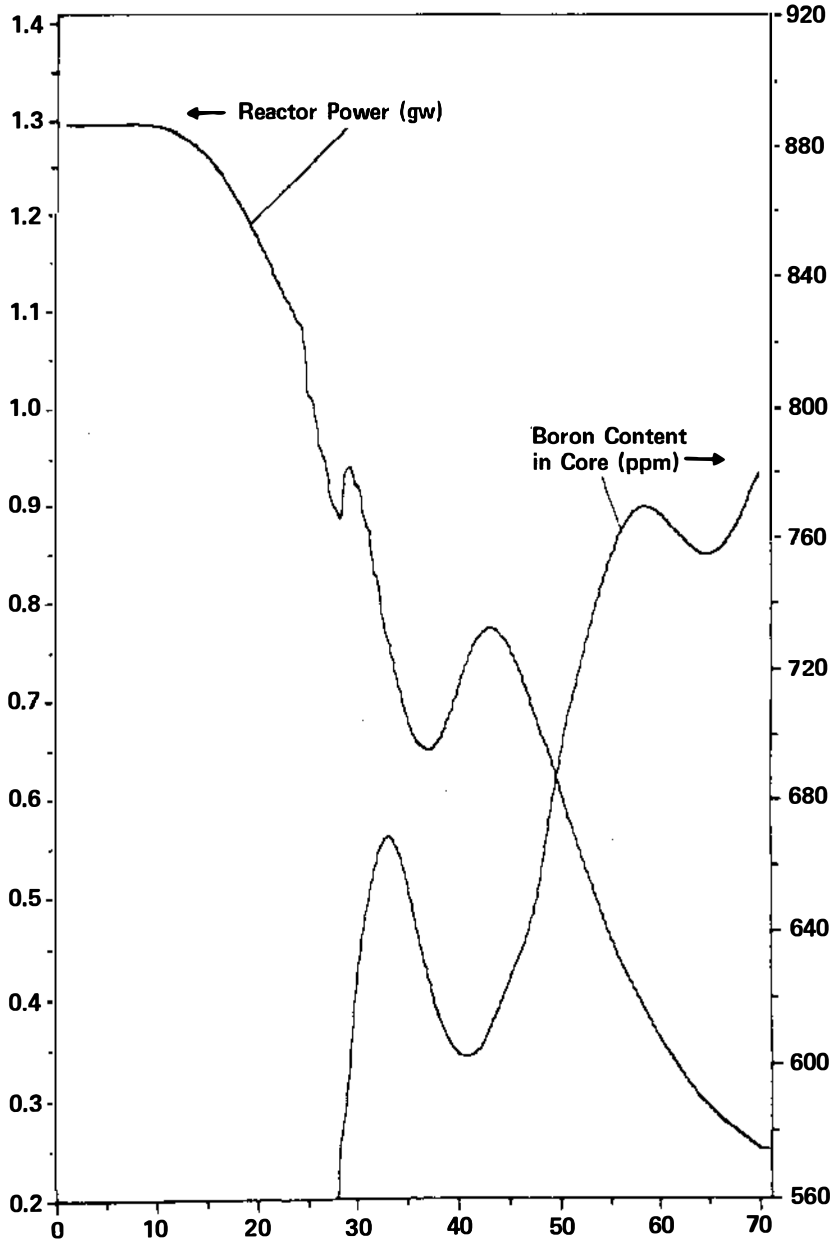


Figure 5 Simulation of a feedwater trip without scram, PIUS reactor. Source: (32).

that no transient has been identified that can lead to core damage. PIUS is also remarkably resistant to most loss-of-coolant accidents (LOCAs), since any break in the primary system immediately breaks the hydraulic lock, and borated pool water rushes in. A catastrophic failure of the steam generators, though it too would cause the reactor to be flooded with borated water, conceivably might offer a path for partial draining of the pool. For this reason, the steam generators are located above the reactor so that, at the very worst, the level of the pool would be lowered to the point of the break; enough of the pool would be left in place to provide cooling, by evaporation, for several days. Even farther fetched is a massive failure, induced by an earthquake, of the prestressed concrete vessel itself. This event is regarded as incredible by ASEA/ATOM. In any event, the vessel is built into the ground, much like an ICBM silo. Water leaking from a massive failure would accumulate in the hole around the vessel, which would in any case be lined.

PIUS is a derated PWR, and therefore requires no development of fuel elements or pumps; nevertheless skeptics have raised questions about its feasibility.

1. Will the hydraulic locks work as planned? Two experimental rigs, one a table-top model tested at the Tennessee Valley Authority in the United States (34), and the second a one-tenth scale model tested at ASEA/ATOM, have demonstrated that the locks work exactly as predicted. A 2500-kW, electrically heated mock-up is under construction at ASEA/ATOM; results from it should be forthcoming in 1985.
2. Is the steam generator feasible? The bayonet-type, once-through steam generator, located in the pool above the core, requires considerable development. Since the hot steam generator is immersed in the cold pool, it must be insulated from the pool. ASEA/ATOM proposes stainless steel sheeting to cover, and thus insulate, the entire primary system, but this approach needs testing.
3. What about thermal shock caused by ingress of the pool water? This presumably can be obviated by design, but this presumption needs to be demonstrated.
4. Will PIUS operate continuously, or will it always be shut down due to boron's inadvertent invasion of the primary cooling system? The remarkable stability of the hydraulic locks demonstrated in the ASEA/ATOM mock-up, as well as the computer simulations, should be reassuring on these scores. However, not enough is yet known about ingress of boron across the hydraulic lock.
5. Can PIUS be maintained? ASEA/ATOM claims that maintenance

through the large pool should be no more difficult than the maintenance now performed routinely during refueling of LWRs.

As presently conceived, a single large prestressed concrete vessel would house up to four PIUS modules, each rated at 200 MW(e). Whether these modules would be regarded as separate reactors by licensing authorities remains to be seen. A single module of 500 MW(e) is also being studied.

Economics Whether or not PIUS would be economic depends on how it fares with licensing authorities. Though the large concrete vessel is very expensive, its use eliminates essentially all the safety systems needed in conventional reactors. Moreover, there is no reason to build the balance-of-plant (BOP) to nuclear standards since the PIUS is resistant to transients caused by failures in the balance-of-plant. In particular, a full-fledged containment vessel is not needed. If these contentions can be sustained before licensing authorities, the PIUS might cost no more per kilowatt, and possibly less, than a conventional LWR of 1000 MW(e).

Present status As of this writing, PIUS is being developed only by ASEA/ATOM. A 400-MW reactor with many features of PIUS has been offered by ASEA/ATOM for district heating in Helsinki. Whether this tender will be accepted will be known within the coming year.

These writers conclude that PIUS, with its clever hydraulic locks, must be regarded as inherently safe. Moreover, in extremis, it protects not only the public, but also the owner of the reactor; and neither an act of nonnuclear war nor sabotage could cause an accident that threatens the public. K. Hannerz's PIUS reactor therefore represents a quantum leap in the quest for inherently safe reactors.

THE MODULAR HTGR We have already seen that the thermal inertia of the HTGR is some hundred times greater than that of the LWR. Moreover, the volumetric power density, around 6 MW/m^3, is 15 times lower than in an LWR. G. H. Lohnert (35) of KWU has proposed lowering the specific power of the HTGR even further as well as reducing the power output, so that even if all systems for removing after heat were to fail, the reactor could still cool itself by heat conduction, radiation, and natural convection. KWU, GE, and General Atomic (GA) (36) have proposed modular HTGRs whose maximum power is around 200 MW(e). A 1000-MW(e) plant would consist of five or more such modules.

The KWU design uses a pebble bed; the GA design uses either prismatic or spherical fuel elements. The fuel itself, as in large HTGRs, consists of tiny uranium oxide spheres triply coated with silicon carbide and graphite; these are embedded, like raisins in a cake, in fuel elements, either graphite prisms or spheres ("pebbles"). At a maximum power density of 3 kW(t) per liter (some 30 times lower than the power density of an LWR), and with an elongated core that maximizes surface area, the highest temperature reached by any fuel sphere is around 1550°C even if all active cooling fails. At this temperature the release of fission products to the atmosphere poses no hazard to the public, although the release may contaminate the reactor itself. Of course, loss of all cooling is a very unlikely event; and in almost any situation in which the system retains pressure, natural convection keeps the fuel well below 1550°C. Nevertheless, it is remarkable that a 200-MW(e) HTGR poses no danger to the public even if the reactor loses pressure and all cooling is lost.

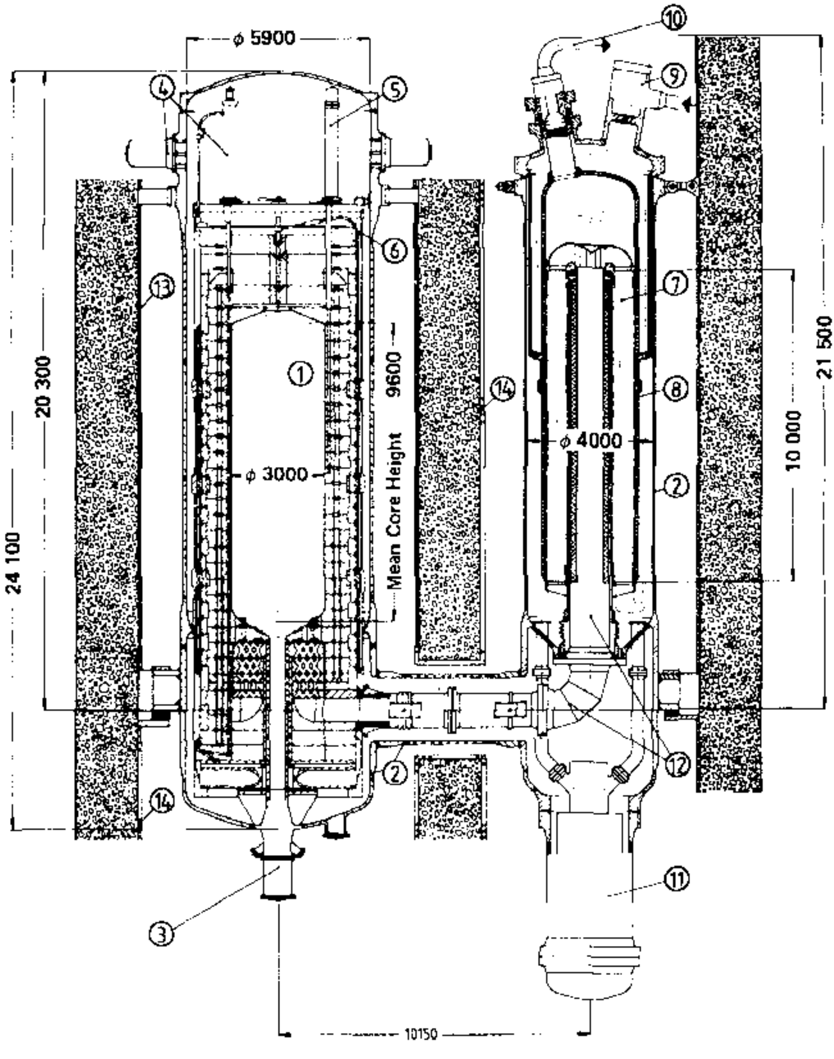
A schematic of the KWU/GE modular HTGR is shown in Figure 6. In Figure 7 we see how the hottest fuel element temperature rises, but remains below 1550°C in a core heat-up accident initiated by depressurization combined with a failed steam generator or blower. In Figure 8 we show how the release of ^{137}Cs in these extreme circumstances varies with the volumetric power density. Below 3 MW/m^3, the release is well below that allowed by the German safety authorities; the release rises quickly with power density, and reaches unacceptable levels at power densities above 3.5 MW/m^3.

The only event that might compromise the inherent safety of a modular HTGR would be a graphite fire. This would require a catastrophic failure in both the main inlet and outlet to the reactor, and this could be initiated, if at all, only by a saboteur, or possibly by an earthquake that exceeds design specifications. These possibilities must be regarded as extraordinarily remote. One must therefore regard the modular HTGR as inherently safe.

Can a modular HTGR be afforded? At 200 MW(e) one is sacrificing economy of scale for safety. On the other hand the reactor is now so small that much of it can be fabricated in a shop; and, as with PIUS, the BOP need not be built to nuclear standards.

One is naturally tempted to compare the modular HTGR and PIUS as to practicality and inherent safety. Though no serious comparison of the two has appeared in the literature, we would point out the following:

1. Favoring modular HTGR. (*a*) No new mechanical devices or physical principles are involved; several HTGRs have been built, and their forgiving nature has been demonstrated. (*b*) Following a loss-of-coolant accident, no intervention would be required to protect the public.
2. Against modular HTGR. (*a*) In the worst accident, even though the public is unharmed, the reactor and its building might be contaminated. (*b*) HTGR is not absolutely immune from earthquakes and graphite fires.



1. Pebble Bed
2. Pressure Vessel
3. Fuel Discharge
4. Boronated Spheres
5. Reflector Rod
6. Fuel Loading
7. Pipe Assembly
8. Outer Shroud
9. Feed Line
10. Live Steam Line
11. Blower
12. Hot Gas Duct
13. Surface Cooler
14. Insulation

Figure 6 Cross section of a modular HTGR. Source: (17).

3. Favoring PIUS. (*a*) Even in the worst accident, the reactor would remain intact. (*b*) No fuel element or pump development is needed. (*c*) The reactor is immune from sabotage and acts of war.
4. Against PIUS. (*a*) Intervention is required after a loss-of-coolant accident, though only after about a week. (*b*) PIUS probably is

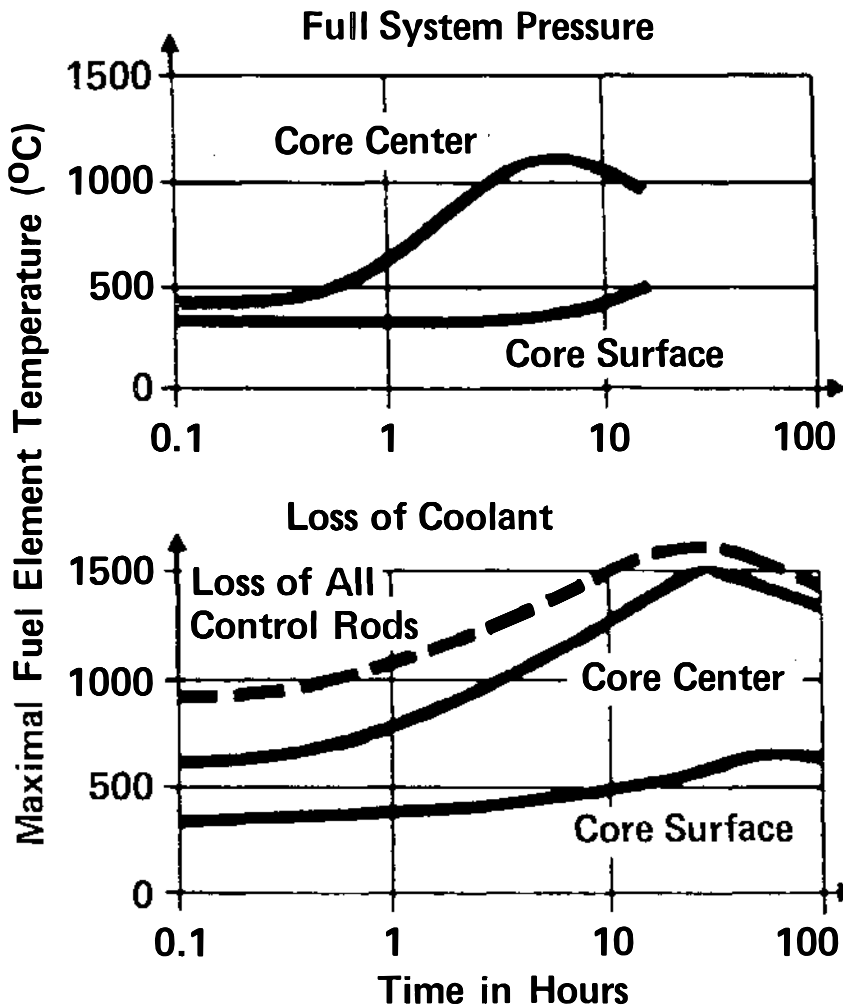


Figure 7 Time-dependent maximum fuel element temperature following loss of flow (upper figure), loss of coolant (lower figure), modular HTGR. Source: (35).

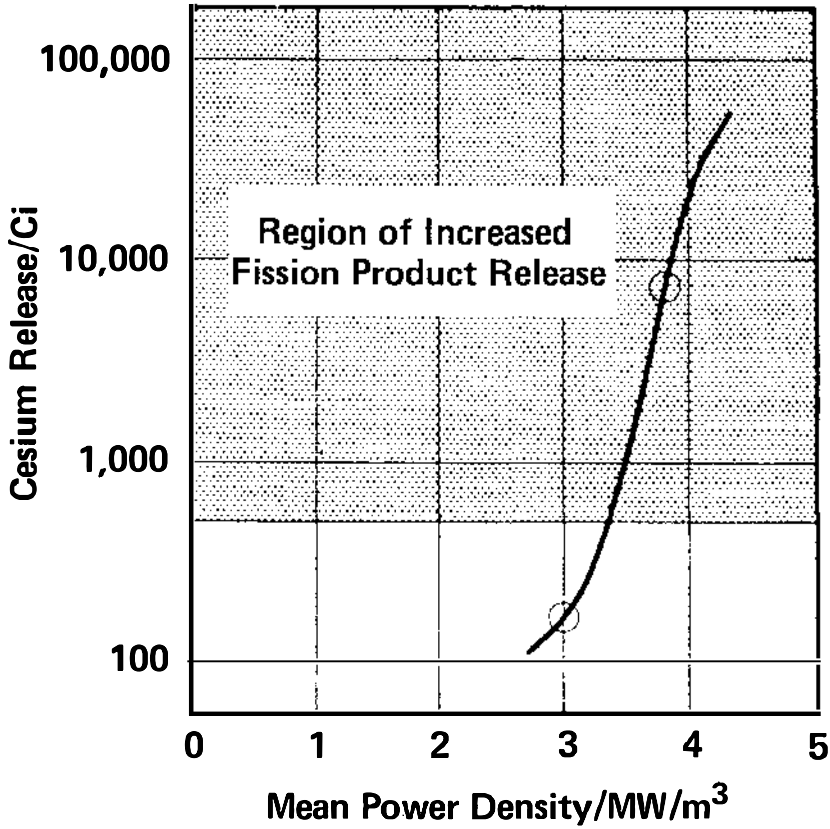


Figure 8 Cesium release during core heat-up accident vs power density, modular HTGR. Source: (35).

sufficiently different from a conventional LWR to require a demonstration; in particular, the steam generator is novel and must be developed.

At present, the US Department of Energy is supporting the development of the modular HTGR at about $30 million in fiscal year 1985. In contrast, the PIUS reactor development is being supported by ASEA/ATOM, a private company, at a much lower level.

Other Ideas for Inherently Safe Reactors

THE SCHULTZ-EDLUNG STEAM-COOLED FAST REACTOR (37) In 1982, M. Schultz and M. Edlund, while participating in IEA's Second Nuclear Era Study, proposed a steam-cooled fast breeder reactor that incorporated many of the safety features of PIUS. These designers noticed that a steam-cooled fast reactor could be stable against ingress of water if enough boron-10 were incorporated in the fuel. If the density of steam decreased (because the reactor power increased), neutron leakage would increase and thereby reduce power. On the other hand, if the steam condensed in the reactor, the neutron spectrum would soften. Since the capture cross section of boron increases as $1/v$, v being the neutron velocity, whereas fission cross sections do not rise as sharply as neutron energy falls, the reactivity of the reactor would tend to decrease as the result of the ingress of water. Thus the reactivity peaks at some intermediate steam quality. An example of the reactivity as a function of steam quality in a Schultz-Edlund fast reactor is shown in Figure 9. Depending on the detailed configuration of the reactor, the peak in reactivity corresponds to saturated steam pressures between 3.45 and 22.1 MPa (500–3200 psia).

With such a characteristic reactivity curve, one can configure an inherently safe reactor that embodies the hydraulic locks of PIUS, but—and this is a great advantage—the pool water need not be borated. Thus a Schultz-Edlund steam-cooled reactor would sit at the bottom of a large pool of ordinary water. As in PIUS, the steam circuit is separated from the pool water by hydraulic locks. At some steam quality, the chain reaction sets in; and this operating point should be stable. Any deviation from the

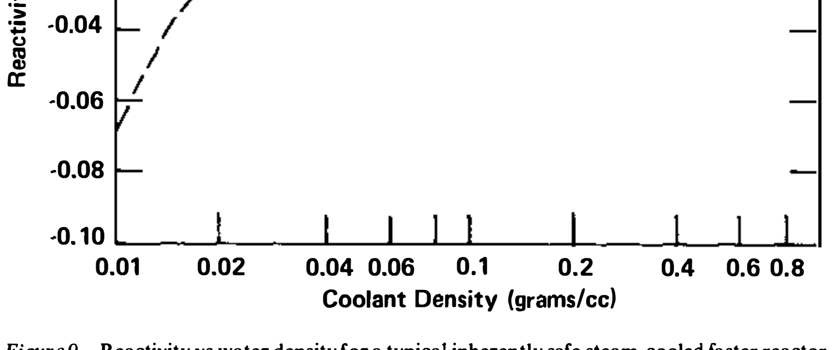


Figure 9 Reactivity vs water density for a typical inherently safe steam-cooled faster reactor. Source: (37).

operating point would shut the reactor down, with a resulting ingress of water. The reactor would continue cooling itself by natural convection.

The Schultz-Edlund reactor embodies a very ingenious idea that should be pursued further.

LIQUID METAL FAST REACTORS (LMFRs) With the recent interest in inherently safe reactors, designers of LMFRs have incorporated passive safety features into them. This trend in design coincides with the collapse of the Clinch River Breeder Reactor project; out of these studies a new, intrinsically safe design for an LMFR may emerge. One would hope that such a reactor would not evoke the bitter antagonism that ultimately led to cancellation of CRBR.

Sodium-cooled reactors with enhanced passive safety have not received as much attention as have PIUS or the modular HTGR. Nevertheless one can discern two main threads in the attempts to design an intrinsically safe LMFR.

1. *Inherently safe oxide-fueled LMFR* This approach is being followed by Westinghouse, Rockwell International, and GE. As described by Schmidt et al (38) of Westinghouse, conventional LMFRs are vulnerable to Loss of Flow with Failure to Scram (LOFS); to Transient Overpower; and to Loss of Normal Heat Sink. Any of these events, when coupled with failure of both primary and secondary shutdown systems, could lead to a core disruption.

To deal with all three events occurring simultaneously, Westinghouse has developed a design that limits the amount and rate of reactivity insertion to a level that does not heat the sodium to boiling. This is done in one of three ways: independently operated control rods, each of limited worth, gravity-operated shutdown rods actuated by magnetic couplings that lose their magnetic properties when sodium is heated beyond the Curie point of the magnet material, and/or injection of a liquid poison (indium) under transient conditions. There is a passive decay heat removal system that allows heat to move through the reactor vessel to the guard vessel. The latter is cooled by natural air convection, enhanced by fins on the guard vessel. Westinghouse proposes intentionally extending the primary pump coastdown by means of a flywheel or equivalent, which would keep the coolant below its boiling point even during an overpower transient.

In addition, the design of the core has been optimized to increase inherent negative reactivity feedbacks so as to limit the overpower excursion. This is accomplished through thermal expansion of the core supports, which increases neutron leakage as the core heats up. Advantage is also gained from the differential thermal expansion of the control rods and core. These negative reactivity inputs as the core heats up must offset positive reactivity inputs, such as the Doppler effect due to the fuel's cooling off from operating conditions to shutdown condition.

The Westinghouse approach is claimed to be feasible for both small and large cores, and for both pool and loop plant configurations. However, inherent safety can be gained more easily at smaller size (simpler decay heat removal) and with a pool design (more thermal inertia slowing temperature excursions).

General Electric (39) and Rockwell International (40) are proposing modular fast reactors. Such pool-type reactors would be shop fabricated. Several modules could be put together to form a large power plant. The principles for gaining inherent safety are similar to those described for the Westinghouse plant.

2. *Reemergence of the metal-fueled LMFR* (41) Argonne National Laboratory has reintroduced the metal-fueled LMFR on the grounds that such a reactor is intrinsically safer than an oxide reactor of the same size. Argonne's case rests on the better thermal conductivity of the metal fuel. Since the temperature rise in fuel on going to power is lower in metal than in oxide, the reactivity that must be compensated for because of the Doppler effect is less in a metal fuel than in an oxide fuel. Thus less reactivity must be dealt with during a failure to scram, and the Doppler coefficient can be counted on to terminate the LOFS transient without allowing the sodium to reach its boiling point. This may be seen in Figure 10; the metal-fueled system rides out the LOFS accident with a lower temperature excursion than in the oxide system.

Metal fuel elements have operated flawlessly in the EBR-II, with burnups of 100,000 MW-days per ton—i.e. about 10% of the fissile atoms are fissioned. On the other hand, this remarkable performance at EBR-II cannot be extrapolated directly to a full-scale LMFR since the fast neutron flux in EBR-II, for a given burnup, is about one third that in a commercial reactor (a consequence of the three times higher enrichment in EBR-II as compared to the full-scale reactor). The cladding in the commercial reactor, being bombarded by a three times higher fast fluence, might be expected to deteriorate faster than that in EBR-II.

Argonne proposes to reprocess its LMFR fuel on site; the pyrometallurgical process had been demonstrated on fuel elements at EBR-II. Keeping the fuel on-site would, according to proponents of the scheme, all but eliminate the likelihood of clandestine diversion of plutonium, since the fuel is never decontaminated enough to be handled directly.

Loop or pool The current reexamination of LMFRs has reopened a sensitive subject: which configuration, pool or loop, is safer? At the time

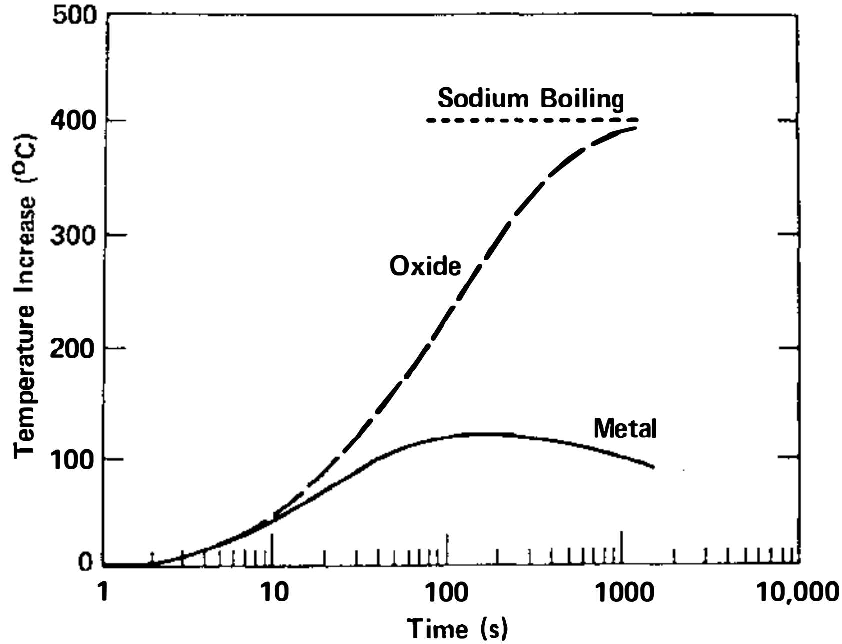


Figure 10 Increase in reactor outlet temperature during loss-of-flow transient without scram, liquid metal fast reactor. Source: (41).

when the Atomic Energy Commission (AEC) decided on the loop configuration for the fast flux test facility and for the Clinch River Breeder Reactor, the standard doctrine held that loop and pool were equally safe. This assertion says nothing about the relative inherent safety of the two configurations. The pool reactor, immersed in a large pot of sodium, would appear to be intrinsically the safer, because the pool of sodium provides a heat sink that is passive and reliable. The matter is hardly settled; during this period of reexamination the relative safety of these two systems will likely be debated in a more serious and revealing way than has previously been the case, at least in the United States.

THE MOLTEN SALT BREEDER (42) Reactors based on molten salt fuel can hardly suffer a core melt since the fuel is already molten. In the 1970s, when molten salt reactors were still actively pursued, the late Professor T. Thompson (who became an AEC Commissioner) argued on general grounds that molten salt reactors were inherently safer than sodium-cooled solid fueled reactors. No definitive comparison of the two types was possible since the design of molten salt reactors (MSRs) had not been fully worked out. Experience drawn from the operation of the Molten Salt Reactor Experiment (MSRE), an 8-MW molten salt reactor that operated from 1965 to 1969, suggests that MSRs, though they may be less vulnerable than LMFRs to accidents that might break containment, are perhaps more vulnerable to incidents in which small amounts of radioactivity are released. The issue remains an academic one unless a molten salt reactor is built.

INTRINSICALLY SAFE FUSION REACTORS The afterheat generated immediately after shutdown in a 1000-MW(e) fusion reactor is about 20 MW (if the first wall is made of steel cooled with Pb-Li), and about 12 MW (if the first wall is made of V-20 titanium alloy). Though these afterheats are much smaller than the 200 MW of after heat generated in a fission reactor of the same electrical output, they are sufficient to melt the first wall of the fusion reactor unless the wall is cooled vigorously. Thus, contrary to some popular belief, fusion reactors are, in principle, subject to "wall melt" accidents that could release tritium and other isotopes to the environment, as well as being awkward and expensive for the operator of the device. G. Logan (43) of Lawrence Livermore National Laboratory has therefore proposed that fusion reactors be designed with wall loadings of only 3–5 MW/m^2, rather than the 10–20 MW/m^2 assumed in many current design studies. At this lower wall loading, the first wall would cool itself by radiation, conduction, and natural convection. Logan points out that a 300-MW(e) fusion reactor with such low wall loading would therefore be inherently safe. Though the cost per kilowatt of the fusion reactor itself would thereby be increased, this increase would be compensated for by simplification of the balance-of-plant. Logan's ideas have just been presented to the fusion community; one cannot as yet estimate how much influence they will have on the design of fusion reactors.

CONCLUSIONS

The case for inherently safe reactors has been neatly summarized by K. Hannerz and P. Isberg (26):

> Nearly all the problems facing the nuclear industry can be traced back, directly or indirectly, to the nuclear safety issue. There is no doubt that the latter is causing the technology to be too complex and demanding to be attractive to the utilities, at least in the U.S.
>
> There is no agreement on how to remedy this situation. Should the technology be improved and made less demanding, or should the competence of the utilities be strengthened, licensing streamlined, etc.?
>
> The latter path seems to be the preference so far. However, the choice between "institutional" and "technological" approaches should not be based solely on a myopic

view of present problems but must also consider broader aspects of the expected world energy future. Institutional reforms, e.g. in the U.S., are obviously of little relevance for the situation in the third world when large scale application of nuclear energy there comes under way, as will inevitably happen.

This duality between technological fixes and institutional fixes is paramount. As J. Ahearne (44) has said, nuclear power is a complex, demanding technology. To deal with it safely requires sophisticated people and appropriate institutions. Obviously, the more inherent safety is built into a reactor, the fewer demands it makes on the people entrusted to run it. Inherently safe reactors might therefore find a niche where the institutions are not up to the demands conventional nuclear power has made of them—notably in the Third World, or even among less qualified utilities in the United States.

Though inherent safety has now become a watchword among US reactor designers, many in the industry seem to view inherently safe reactors as an unnecessary diversion, or even as a threat. For example, the Atomic Industrial Forum (45) recently stated:

> Increasing discussion in recent months, presumably as a result of the accident at Three Mile Island, has been directed at the rhetorical question of whether renewed utilization of the nuclear option should not be based on some system other than the light water reactor (LWR). The discussions, however, have failed to acknowledge the extensive research, development and demonstration effort that went into alternative systems in the late 50s and early 60s. They have failed to recall the deliberative reasoning that went into the selection of the LWR, not only in the U.S. but subsequently in Europe and the Far East. They have failed to recognize the improvements that have been incorporated into the LWR as a result of 25 years of design and operating experience, including the improvements made since the accident at Three Mile Island. And finally, they have failed to specify how they consider the LWR system to be flawed or why alternative systems could be expected to perform any better.
>
> None of this is by way of suggesting that research and development on the LWR as well as alternative reactor designs should not be vigorously pursued. Nuclear power is no different than the product of any other technology in that there should always be room for improvement. At this point in time, decisions as to which concepts are to be pursued should be made in the marketplace.

One must therefore ask, "Can passively safe and actively safe reactors coexist?" Or, more practically, "Would the demonstration of a reliable, passively safe reactor like PIUS or the modular HTGR bring on demands to shut down existing reactors because they are not as safe as PIUS or modular HTGR?" We cannot judge this question; but we can point out that DC-3s are not as safe as 767s, yet no one is demanding that the DC-3 be decertified. The public apparently does accept devices with which it has had long and acceptable experience. Should the next 15 years pass without a repetition of the TMI-2 accident, one might hope that the public would become less concerned about reactor safety. We can estimate the likelihood of a serious core melt over the next 15 years as follows: the 400-odd reactors now on line or under construction will amass 6000 reactor years by the year 2000. If the core melt probability for these reactors is 5×10^{-5}/RY, the probability of a core melt by then is 0.3; if improvements now being installed reduce the CMP to 10^{-5}/RY, this probability falls to 0.06. We would suggest there is a good chance that we shall reach 2000 without a repetition of TMI-2.

But in a way this misses the point. Though nuclear energy is at a low ebb in many countries, notably the United States, most analysts continue to see nuclear power as a long-term, even permanent energy source. We are just beginning the nuclear era. Many, many thousands of reactor years may well be amassed by future generations. Core melt probabilities that are adequate for nuclear power in the short run may not be adequate over the very long run. Thus there will develop, and indeed there has already developed, pressure to reduce CMPs—to 10^{-6}/RY, to 10^{-7}/RY, or even lower. And once the existence theorem has been proven, that passively safe reactors with CMPs in this range or lower are feasible, this knowledge can never disappear. It will continue to haunt the nuclear power enterprise until some inherently safe reactors are built. With the safety issue exorcised by inherently safe reactors, perhaps we can look forward to a second nuclear era no longer tormented by visions of Class IX accidents causing vast damage. Nuclear power could then be part of the solution to the problems of acid rain and the accumulation of carbon dioxide rather than a festering source of political conflict.

Literature Cited

1. Lilienthal, D. E. 1980. *Atomic Energy: A New Start*. New York: Harper & Row
2. Firebaugh, M. W., ed. 1980. *Acceptable Nuclear Futures: The Second Nuclear Era*, ORAU/IEA-80-11(P). Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis
3. US Office Tech. Assessment. 1984. *Nuclear Power in an Age of Uncertainty*, OTA-E-216. Washington, DC
4. Lester, R. K., Driscoll, M. W., Lanning, D. D., Lidsky, L. M., Rasmussen, N. C., Todreas, N. E. 1983. *Nuclear Power Plant Innovation for the 1990s: A Preliminary Assessment*. MIT-NE-258. Dept. Nuclear Engineering, MIT
5. US Nuclear Regul. Commission. 1975. *An Assessment of Accident Risk in U.S. Commercial Nuclear Plants*. WASH-1400 (NUREG 75/014). Washington, DC: US Dept. Energy
6. Lewis, H. W., Budnitz, R. J., Kouts, H. J. C., Loewenstein, W. B., Rowe, W. D., et al. 1978. *Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission*. NUREG-CR-0400. Washington, DC
7. Okrent, D. 1981. *Nuclear Reactor Safety, On the History of the Regulatory Process*, Madison, Wisc: Univ. Wisconsin Press
8. US Nuclear Regul. Commission. 1982. *Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant, Vol. 3*. NUREG/CR-1659 (SAND80-1897, 3 of 4). Sandia National Lab.
9. Ergen, W. K., chairman. 1967. *Report of Advisory Task Force on Power Reactor Emergency Cooling*. TID-24226. Washington, DC: US Atomic Energy Commission
10. Fortescue, P. 1980. See Ref. 2, p. 16
11. Hannerz, K. 1983. *Towards Intrinsically Safe Light Water Reactors*. ORAU/IEA-83-2(M) Rev. Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis. Also Hannerz, K. 1973. Applying PIUS to power generation: the SECURE-P LWR. *Nuclear Eng. Int.* 28(349):41

12. O'Farelly, C. 1980. Towards a more forgiving reactor. Presented at *Int. Conf. on Current Nuclear Power Plant Safety Issues*. Stockholm, Sweden. IAEA-CN-39/58
13. Forgiving or Inherently Safe Reactors, I and II, *Trans. Am. Nuclear Society* 47:286–304
14. Minarick, J. W., Kukielka, C. A. 1982. *Precursors to Potential Severe Core Damage Accidents: 1969–1979, A Status Report*. ORNL/NSIC-182 and NUREG/CR-2797. Oak Ridge, Tenn: Oak Ridge Natl. Lab.
15. Cottrell, W. B., Minarick, J. W., Austin, P. N., Hagen, E. W., Harris, J. D. 1984. *Precursors to Potential Severe Core Damage Accidents: 1980–1981, A Status Report*. ORNL/NSIC-217/V1 and NUREG/CR-3591. Oak Ridge, Tenn: Oak Ridge Natl. Lab.
16. Phung, D. L. 1984. *Assessment of Light Water Reactor Safety Since the Three Mile Island Accident*. ORAU/IEA-84-3(M). Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis
17. Weinberg, A. M., Spiewak, I., Barkenbus, J. N., Livingston, R. S., Phung, D. L. 1984. *The Second Nuclear Era*. ORAU/IEA-84-6(M). Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis. Also Weinberg, A. M., Spiewak, I. 1984. Inherently safe reactors and a second nuclear era. *Science* 244:1398–1402
18. Paulson, C. K., Iacovino, J. Jr. 1984. *Increasing Safety Margins at Nuclear Power Plants*. Westinghouse Electric Co.
19. Weinberg, A. M. 1984. See Ref. 17, pp. 18–22
20. Spiewak, I. 1985. *Survey of Light Water Designs to be Offered in the United States*, p. 24. Oak Ridge, Tenn: Oak Ridge Natl. Lab. In press
21. Spiewak, I. 1985. See Ref. 20, p. 7
22. Hucik, S. A., General Electric Co. 1984. Personal communication
23. Duncan, J. D., Sawyer, C. D. 1984. Capitalizing on BWR simplicity at lower power ratings. ANS/ENS meeting. Nov.
24. Siddall, E. 1984. *The CANDU-PHW Reactor in Relation to a Second Nuclear Era*. ORAU/IEA-83-11(M). Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis
25. Combustion Engineering, Inc. 1979. *Conceptual Design of a Large HWR for U.S. Siting*. CEND-379, Vols. 1–4. Washington, DC: US Dept. Energy
26. Electric Power Res. Inst. 1977. *Study of the Development Status and Operational Features of Heavy Water Reactors*. EPRI NP-365. Palo Alto, Calif.
27. Fischer, C., Fortescue, P., Goodjohn, A. J., Olsen, B. E., Silady, F. A. 1984. *The HTGR—An Assessment of Safety and Investment Risk*. ORAU/IEA-84-7(M). Oak Ridge, Tenn: Oak Ridge Associated Universities, Inst. Energy Analysis
28. Martel, L., Minnick, L., Levey, S. 1982. *Summary of Discussions with Utilities and Resulting Conclusions*. EPRI-RP 1585. Palo Alto, Calif: Electric Power Res. Inst.
29. Hannerz, K., Isberg, P. 1984. See Ref. 13, pp. 286–87
30. Lohnert, G. H., Pflasterer, G. R. 1984. See Ref. 13, pp. 287–89
31. Silady, F. A., McDonald, C. F., Weicht, U. H. 1984. See Ref. 13, pp. 290–91
32. Babala, D. 1984. See Ref. 13, pp. 296–97
33. Asahi, Y., Wakabayashi, H. 1984. See Ref. 13, pp. 297–98
34. Tenn. Valley Authority. 1984. *A Tabletop Flow Demonstrator for the PIUS Reactor Concept*. TVA/OP/EDT-84/17, WR28-1-900-118
35. Lohnert, G. H., Pflasterer, G. R. 1984. See Ref. 13, pp. 287–89
36. Silady, F. A., McDonald, C. F., Weicht, U. H. 1984. See Ref. 13, pp. 290–91
37. Schultz, M. A., Edlund, M. C. 1984. See Ref. 13, pp. 291–92
38. Schmidt, J. E., Doncals, R. A., Markley, R. A., Lake, J. A., Coffield, R. D., et al. 1984. See Ref. 13, pp. 298–99
39. GE, Rockwell win reactor race. October 15, 1984. *The Energy Daily* 12(199): 1
40. McDonald, J., Brunings, Lancet, R. 1984. See Ref. 13, pp. 299–301
41. Chang, Y. I., Marchaterre, J. F., Sevy, R. H. 1984. See Ref. 13, pp. 293–94
42. US Dept. Energy. 1980. *Nuclear Proliferation and Civilian Nuclear Power: Report of the Nonproliferation Alternative Systems Assessment Program, Vol. IX: Reactor and Fuel Cycle Description*, DOE/NE-0001/9, pp. 227–40. Washington, DC
43. Logan, B. G., *A Rationale for Fusion Economics Based on Inherent Safety*. 1984. UCRL-91761. Livermore, Calif.: Lawrence Livermore Natl. Lab.
44. Ahearne, J. 1983. Prospects for the U.S. Nuclear Reactor Industry. In *Ann. Rev. Energy*, ed. J. Hollander, H. Brooks, 8:355–84. Palo Alto, Calif: Ann. Rev. Inc.
45. AIF Study Group, *Nuclear Power in America's Future*. 1984. Bethesda, Md: Atomic Industrial Forum, Inc.