Western safety standards make nuclear the safest energy around

This report was adapted from an article by nuclear engineer Jon Gilbertson that appeared in Fusion *magazine in September 1980.*

Critics have tried to claim that Three Mile Island was a "near disaster." The evidence proves just the opposite. Post-TMI studies show that nuclear power is even safer than had previously been thought.

In the words of Edwin Zebroski, head of the Nuclear Safety Analysis Center in Palo Alto, California: "Assertions of a narrowly averted catastrophe at TMI have no foundation. Even if the operators at TMI had continued to misread the condition of the core for several more hours and melting had begun, the addition of water at any subsequent point would have stopped the accident."

The utility-sponsored safety center is part of the Electric Power Research Institute (EPRI) and has done the most comprehensive technical investigation of the TMI incident to date [September 1980]. Zebroski based his statement on the results of EPRI's newly released study, "Nuclear Safety After TMI," June 1980.

Furthermore, the EPRI investigation concluded that no damage would have occurred to the containment building—even if the accident had gone on unchecked for many hours beyond the point of melting.

Although this conclusion has long been accepted, it is only through an actual incident as at TMI that reactor safety analysts have the opportunity to prove it by comparing their smaller-scale experiments and calculations to full-scale operating results. This, in fact, is what the group at EPRI has done in its analysis of the TMI incident. The actual event and EPRI's analysis simulating it have proved that in the real world of reactors, the result of an accident is actually much less severe than predicted from various postulated abnormal operating conditions. The design and construction of reactors are based on very conservative assumptions and calculations about such hypothetical, abnormal operating conditions.

We can confidently state that nuclear power is the safest energy around.

All U.S. reactors are designed around a concept called "defense in depth." The design engineers calculate the worst accident that could possibly occur in the plant, design the plant so it cannot happen, assume that it happens nonetheless, and then design the rector safety systems to withstand the effects of the worst-case accident while completely protecting the public from any danger. The reactor design provides many levels of protection in case of the worst event (or "design basis accident" as it is called) using backup systems, backups to backups, and so forth; hence the term defense in depth.

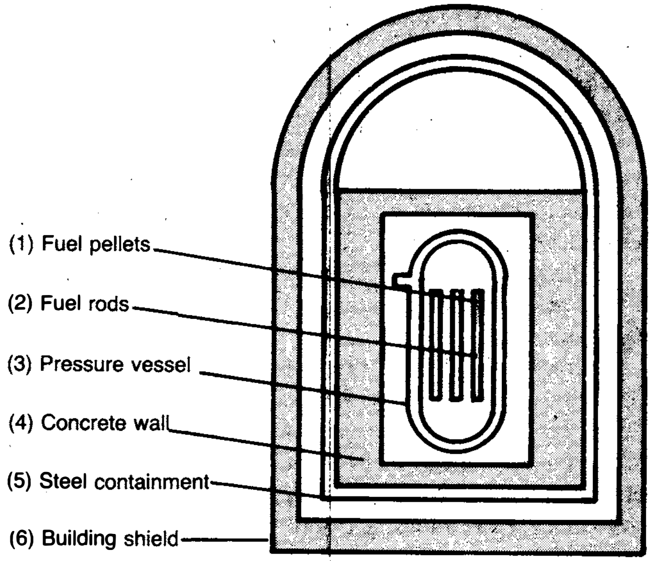
Specifically, the lines of defense include:

1) *quality assurance* to guarantee that all components and equipment in the plant have been manufactured and assembled to required design specifications;

2) highly redundant and diverse *protective systems* designed to prevent abnormal operating conditions; and

3) *engineered safety systems* designed to protect against the consequences of highly unlikely but potentially dangerous accidents, such as loss of coolant, equipment failure, human error, sabotage, and severe natural disasters such as earthquakes, tornadoes, and floods.

Multilevel physical barriers to contain radioactivity



The schematic of a nuclear reactor containment building shows the six levels of containment barriers to prevent any fission products from escaping: 1) the fuel pellet; 2) the fuel rods or tubes; 3) the pressure vessel with 10-inch thick walls; 4) 7-foot to 10-foot concrete shielding; 5) 4-inch thick steel shell; and 6) 3-foot concrete shielding.

Chernobyl: an archaic reactor design

The Chernobyl reactor is a light-water-cooled, graphite-moderated, 1,000-megawatt plant, one of 17 such units operating in the Soviet Union. The design is vintage 1950s, and was considered inappropriate by Western nuclear constructors for development as a civilian power plant. Instead, the West went with the now standard light-water or pressurized water reactor.

According to U.S. nuclear analysts, in the early 1970s, the Soviets were finding it too difficult to keep up with their goal for advancing nuclear power using the conventional light-water reactor used by other nuclear nations. The usual pressurized water reactors were technologically "too difficult" for the Soviets to achieve in a hurry, according to several sources. Their Atommash factory, which was planned to "mass produce" standard pressurized water reactors, ran into trouble. So the Soviets decided, at the time of the oil crisis, to go nuclear using a simpler reactor—a light-water-cooled graphite reactor.

The graphite reactor was originally designed for military use to make plutonium fuel. It is a simple design of blocks of graphite with channels running through it for the fuel rods. The fuel elements are encased in zirconium and are water cooled both inside and out. The Soviets upgraded this military design to commercial-reactor size and began building many, designating them RBMK-1000. Of the 17 such reactors in the Soviet Union of varying size, 12 are 1,000-megawatt-electric plants. Chernobyl has four RBMK-1000s, and there is a similar 4,000-megawatt complex ringing Leningrad, another four-reactor complex at Kurchatov, and a two-reactor complex at Smolensk. A new generation of even larger 1,500-megawatt units is also believed in operation in Lithuanian Russia Baltic.

Why graphite?

The special characteristic of graphite, which was used in the Manhattan Project bomb research in the 1940s at Argonne National Laboratory, is that it is a good moderator of the rate of nuclear reaction and relatively cheap. The special problem with graphite is that it has a high chemical affinity for water vapor, carbon dioxide, and metals. Physicists refer to the "Wigner effect" to describe the reaction of graphite under radiation exposure in a reactor. Energy is stored in the graphite crystal lattice in unstable or metastable concentrations. If this stored energy is released suddenly, it causes an enormous release of thermal energy—a temperature increase. Graphite-moderated reactors, therefore, must follow procedures to allow for controlled and gradual periodic heating of the material so that "annealing" of radiation damage can take place in order to prevent a catastrophic temperature rise.

There cannot be a meltdown in a graphite reactor because the graphite will not get hot enough, even if it is burning. However, if the graphite catches fire, the fire is dangerous and very difficult to put out. If you pour water on it, the water attacks the zirconium, opens the casings of the fuel elements, and lets the fission products out.

The biggest difference between the graphite reactor and conventional nuclear plants in other nuclear nations is that the Soviet design has no containment dome. In addition, the U.S. Department of Energy notes, there are other weak points in comparison to U.S. reactors: The Soviets use long lengths of small piping with numerous valves, for example. The refueling entry ports and bi-metallic joints are subject to potential failure from corrosion. The pressure-tube system is also subject to failure, and the stability of the graphite is aggravated by power changes.

Atomics International

In the early years of nuclear power, graphite reactors were used for research and producing plutonium. In the 1950s, the Western nuclear nations decided not to develop the graphite design for civilian power reactors. Here, a technician works on the graphite moderated reactor core of the Sodium Reactor Experiment at Atomics International in 1956.

What dangers are involved?

Contrary to the claims of antinuclear groups, reactors are not atomic bombs; they cannot undergo critical-mass detonation under any conditions. The enrichment of reactor fuel (that is, concentration of fissionable material) is far lower than in bombs, and hence cannot produce a nuclear explosion.

Explosions of hydrogen gas or other chemical explosions are also not possible within the reactor vessel. This was known before the TMI incident, yet the fraudulent story of an impending hydrogen explosion in the TMI reactor vessel was made into scare headlines for days in early April 1979. As the Nuclear Regulatory Commission later admitted, it was known at the time of the TMI incident that no free oxygen was present and, indeed, that no free oxygen could be present; thus a hydrogen explosion was impossible.

The main concern in reactor safety, in fact, is the large inventory of radioactive material (mostly fission products) that builds up in the reactor's fuel rods during operation. The goal of the reactor safety engineer is to make sure that this radioactive material is contained and controlled under all conceivable operating conditions, normal or accidental, and that only very small
environment at any given time.

Under normal conditions, the radioactive fission products remain contained within the fuel material itself and are part of every fuel pellet. Over the three-year lifetime of the fuel, the fission products build up to a little over 3% by weight of the pellets.

Radioactive material releases heat along with the radiation; therefore it must be cooled at the same time that it is contained. While the reactor is operating, most of the heat in the fuel is produced from the fissioning of the fuel that results from the neutron chain-reaction. After the reactor is shut down (that is, after neutron bombardment has stopped), heat is still produced from the decay of the radioactive fission products. To remove this heat, the fuel must continue to be cooled while the reactor is shut down.

Prevention of accidents

The protective system is a specialized electronic/mechanical system centralized by a computer that monitors every important operating parameter in the reactor—temperature, flow, pressure, reactivity, and so forth—and is prepared to take control of the plant in a preprogrammed manner if the system detects an abnormality. Actions taken by the protective system cannot be overridden manually by the operator. Once the protective system makes a decision to shut the plant down or to reduce the power output, it will carry out the decision no matter what the plant operators might think. The control-rod drives above the reactor vessel drop the rods to shut down the reactor or drive them in part way to reduce power. Control rods absorb neutrons, thereby slowing or stopping the fission chain reaction that is sustained by neutron bombardment.

There is also an inherent safety mechanism in the reactor arising from the nuclear physics of the core. Anything that causes the fuel and coolant to heat up at a given power level causes the chain reaction to shut down. In a water-cooled reactor, such as pressurized water reactors and boiling water reactors, this is called the *negative temperature coefficient of reactivity*. In fast breeder reactors, another physical principle leads to the same result.

The final feature of defense in depth is the engineered safety systems. Here the designer assumes that accident prevention has failed in spite of everything. He selects the worst conceivable accident that is just on the borderline of being not possible and designs the plant to withstand the effects of such an accident and to prevent harm to the plant personnel and the surrounding area.

This just-short-of-impossible accident is termed the design basis accident. After tens of thousands of manhours of analysis and investigation by hundreds of safety engineers, the conclusion is that the design basis accident for a light water reactor (pressurized water or boiling water) is the loss of coolant accident (LOCA).

In a LOCA, a massive rupture of the primary coolant system causes the water to depressurize, followed by rapid flashing to steam and a blowdown of this steam-water mixture out of the ruptured pipe. Such a massive rupture is not considered possible, even if there were an earthquake, since reactors are also designed to withstand earthquakes. The blowdown of this steam-water mixture would soon cause the reactor core to heat up, the fuel to melt, and radioactive fission products to escape the core—if the reactor safety designer had stopped here.

Multilevel containment barriers

The safety engineer provides as many physical containment barriers as necessary to prevent the release of dangerous levels of radioactivity outside the reactor building. The accompanying figure (page 36) illustrates these carriers, showing six levels of containment.

The first is the fuel pellet itself, made of very hard, close-grained ceramic uranium oxide that traps most of the radioactive fission products within its grain boundaries during normal operations. To back this up, the fuel pellets, less than a half inch in diameter and 1 inch long, are stacked in sealed 12-foot tubes of zirconium alloy. This assembly is called the fuel rod. Under normal operation, the pellets and tubes will contain nearly all of the radioactive fission products during the entire three- to four-year lifetime of the fuel.

A few of the zirconium alloy tubes will leak during normal operation, so that a very small amount of gaseous fission products will escape into the primary coolant water. The primary coolant system is therefore contained in a pressure vessel with walls 10 inches thick and a piping system that acts as the third containment barrier. This barrier will contain any radioactive material that escapes the fuel tubes during normal operation and also will act as the major containment barrier if an accident damages the fuel rods. This primary system has several filter systems to filter out any radioactive fission products that are released to the coolant and collect them for later disposal.

Under the assumed condition that the primary coolant system containment barrier has been breached in the design basis accident, three more barriers are provided to contain any fission products that escape from the ruptured pipes. First is the 7-foot to 10-foot thick layer of concrete shielding that surrounds the reactor vessel and the primary coolant system. Next is the containment building, which has two barriers: one is a sealed steel shell nearly 4 inches thick designed to a pressure of 60 pounds per square inch. Outside this shell is more than 3 feet of concrete shielding to absorb radiation.

These barriers are designed to protect the public in the case of the design basis accident. The incident at Three Mile Island was similar to what is called a small pipe break in reactor safety terminology, far less severe than the design basis accident. There was never any danger to the public.

Radioactive fission products give off heat long after the reactor is shut off and must always be cooled. To assure that cooling is always available, engineered safety provides redundant core cooling systems to guarantee that water is always available to the reactor core, even under the conditions of the design basis accident. The back-up core cooling systems are designed to keep the fuel from failing and melting under even these severe circumstances, and if there *is* failure or melting, to prevent so-called core meltdown.

The first line of defense is, of course, the primary cooling system itself. In most loss-of-coolant accidents, as long as the primary pumps (or even one out of the four) keeps running and make-up water is continuously supplied, the fuel will continue to be cooled. The make-up water is automatically supplied to the primary coolant-system by a set of large tanks held at pressures somewhat below normal reactor operating pressure. Thus if a coolant system rupture occurs and the pressure drops, these tanks will automatically inject water into the reactor vessel.

The water make-up system is entirely passive. It requires no pumps or valves to turn it on. The water in these tanks is borated—a boron salt is dissolved in it that absorbs neutrons and shuts down the reactor completely, if for some reason the control rods have not shut it down.

Under certain hypothetical LOCAs, it is necessary to get water into the reactor core faster and at larger volumes than the tanks can supply it. For this purpose there are sets of high-pressure and low-pressure emergency core cooling pumps that automatically turn on when preset pressures in the vessel are detected. The high-pressure pumps are for small ruptures, while the low-pressure ones come on during large ruptures, which require large volume and flows.

The 1979 antinuclear film *The China Syndrome* built an anti-science myth in the tradition of Mary Shelley's novel *Frankenstein*. According to this scare story, in the course of a core meltdown, the molten core forms into a round glob that melts through the reactor vessel, drops onto the concrete floor below, burns its way through more steel and many feet of concrete into the ground below, and defies gravity to emerge in China. Along the way, of course, the fiery glob gives off fission products, contaminating all ground water and everything else it touches.

Such a process is scientifically and physically impossible, as should be clear from the preceding discussion. A core meltdown could happen only if *no* cooling water got into the reactor core for many hours. The fuel would drip onto the massive steel support structure and perhaps eventually the vessel bottom. The splattered fuel would be cooled by contact and conduction of the thick steel walls.

What the experts say

Dr. Joseph M. Hendrie: It can't happen here

Joseph M. Hendrie, former chairman of the U.S. Nuclear Regulatory Commission, is now a consulting engineer. He served on the NRC from 1977 through mid-1981. In this interview he describes one essential difference between the Soviet graphite reactor and light water reactors.

EIR: How would you assess the state of U.S. nuclear safety, compared to Soviet safety systems?

Hendrie: The U.S. water reactors are simply incapable of producing the sort of gross release that has occurred in Russia. We don't have the flammables in core that would provide the kind of driving force they had there in the fire. Our systems are engineered with more extensive safety provisions and we then encapsulate the whole reactor system in a very strong and tight containment structure.

After Three Mile Island we made a very extensive reassessment of the safety of U.S. plants from all kinds of standpoints and all kinds of accidents and found it appropriate to upgrade a number of areas. We have concentrated attention on operator training and expertise and on a drive to achieve real excellence in operation at all U.S. plants. This is reflected in the industry efforts as well as in the regulatory incentives.

Furthermore, we undertook after Three Mile Island, a very extensive upgrading of the ability both on-site and off-site to take emergency measures in the event of accidents. I think those provisions are particularly notable against the background of the Russian accident.

EIR: Most of the material written in the 1970s on the Soviet safety question indicates that they are scornful of the Amer-