1

When is a Reactor Safe?

The Design Basis Accident

For the first twenty-five years of the Atomic Age, engineers and technicians operated reactors uncertain of the probability of a major accident. Automobile and aircraft safety regulations grew from the grisly accumulation of accident data, but there had been no reactor accidents and, thus, no data. Nuclear experts constructed an alternative safety approach. From the start-up of the first wartime plutonium production reactors at the Hanford Engineering Works in Eastern Washington State, safety assurance relied on the "Three Ds," as I will call them—Determinism, Design Basis Accidents, and Defense in Depth. They relied not on determining and limiting the known probabilities of accidents, but by imagining far-fetched catastrophes and developing conservative designs.

The first D—deterministic design—differed from probabilistic safety in the way it addressed three safety questions that came to be known as the "risk triplet." 1) What can go wrong? 2) How likely is it to go wrong? 3) What are the consequences? In brief, what are the possibilities, probabilities, and consequences of reactor accidents? A probabilistic design had to address all three questions for a broad range of accidents.[1] With no history of reactor accidents, nuclear engineers could not answer question 2 except in a qualitative way by subjectively judging that some accidents were "incredible" and not worth considering, such as a meteor striking a reactor, though even that remote probability was estimated in the 1970s.[2] Worst-case thinking was a mainstay of reactor safety.

Deterministic design compensated for this ignorance of probabilities by addressing questions 1 and 3 in a very conservative way. For question 1, engineers developed "imaginatively postulated" or "stylized" accidents judged to be extreme but credible that would result in "the most hazardous release of fission products." They further calculated the consequences of question 3 by assuming pessimistic conditions during an accident, such as weather conditions that might concentrate an escaping radiation cloud over a nearby population center. Without careful definitions, terms for these accidents were used in defense and civilian reactor applications. Terms like Maximum Hypothetical Accident and Maximum Probable Incident were similar to Maximum Probable Flood, used previously by flood control engineers. The winner, Maximum Credible Accident (MCA), gained common usage in the late 1950s.[3] A decade later the AEC switched again, to Design Basis Accident (DBA), a name that captured the purpose of these accidents as safety design standards. DBA remains in use today and the term will be used throughout this book.[4] Reactor designers analyzed DBAs to "determine" the safety features necessary to prevent these extreme accidents or mitigate their consequences. Typically, designers used a combination of qualitative factors, such as remote reactor siting, careful system design to ensure there was enough component redundancy (for example, backup pumps and power supplies), and extra margins of material strength and quality. This deterministic design approach to a few DBAs, engineers reasoned, would cover many lesser accidents, too. It set a conservative outer boundary of safety that simplified a designer's task from having to explore the many paths to failure in complex reactor systems.

When the DuPont Corporation designed the plutonium production reactors at Hanford during World War II, the design basis accident was extreme and simple: an explosive reactor power surge that spread radioactivity about 1.5 miles away. Protecting the public was also simple: isolation. The first reactors were spaced several miles apart and well inside Hanford's expansive borders, out among the sagebrush and rattlesnakes of eastern Washington. The reactors and workers were protected with shielding and redundant shutdown and cooling systems. A deterministic approach aligned with DuPont's chemical engineering culture, stressing large safety design margins.[5]

THE REACTOR SAFEGUARD COMMITTEE

The concept of defense in depth—the second D of safety—was also articulated early in the postwar period by the Reactor Safeguard Committee, an AEC panel of eminent experts chaired by physicist Edward Teller. The committee's task was to analyze the design safety of existing and proposed reactors at AEC and contractor facilities. Teller held nuclear safety to a high standard. He and the committee worried about the impact of an accident on public opinion and sought to make reactors safer than conventional technologies. The committee enjoyed a reputation for excessive caution. "The committee was about as popular—and also as necessary—as a traffic cop," Teller recalled. Unpopular but influential, the Committee's judgments carried weight.[6] In 1949, it spelled out its understanding of reactor hazards and safety in a report with the AEC identifier WASH-3 (WASH stood for Washington, DC, the AEC's headquarters). Although the term "defense in depth" did not come into usage for another decade, WASH-3 contained its key elements. From the physical properties of their fuel, to shutdown systems, emergency pumps, auxiliary power, shielding, and location, AEC reactors were to be designed with multiple lines of defense to prevent an accident or mitigate its consequences.

While all the lines of defense were important, the Safeguard Committee believed some were more reliable and important than others. For example, the committee favored designs with "inherent" safety features that could make certain accidents nearly impossible. Inherent features were self-correcting mechanisms built into the plant's physical properties, such as a reactor fuel with a "negative coefficient of reactivity." If power rose in a reactor with a negative coefficient, the extra heat generated naturally slowed down the chain reaction by reducing the neutrons available to split atoms. As a reactor started up and rose to operating temperature, reactor operators worked to keep a chain reaction going by turning a "shim switch" that pulled neutron-absorbing control rods further out of the fuel. Keeping a reaction going was hard, but safe, work. By contrast, a positive coefficient meant a reactor had its own gas pedal. Once power and temperature started rising the reaction fed itself, creating more and more neutrons and fissions until there was a "runaway," or even an explosion similar in force to what might happen at a chemical plant, as later happened at the Soviet Union's Chernobyl power plant in 1986. Operators or automatic shutdown systems had to insert the control rods to keep the reactor under control. It was no coincidence that the Hanford reactors with their positive coefficients were sited in remote Eastern Washington.[7]

Defense in depth consisted of other less reliable lines of defense that offered compensating safety advantages. Physical or "static" barriers such as shielding and airtight containment buildings could be important for runaways or coolant leaks. Static barriers were highly reliable if not perfect. Least reliable were "active" safety systems, such as emergency cooling systems or the reactor "scram" system that shut down a reactor by inserting control rods into the fuel. Active systems could quickly bring a troubled reactor under control. But the committee warned that "such systems are liable to failure in operation." Pumps had to start, relays had to actuate, switches could not jam, valves had to close, and operators could not make mistakes. Yet, all those things were almost certain to happen in a plant's lifetime. The varied advantages of inherent, static, and active systems forced the AEC to rely on all layers together, some slow but certain, others fast but a bit fickle.[8] The committee established a general priority for the lines in defense in depth that would not be seriously questioned for the next fifteen years: (1) isolation and inherent features; (2) static barriers: and (3) active systems. Not all reactor designs had the ideal arrangement of defense in depth and each line was supposed to compensate for the weaknesses of the others. The Hanford reactors had a positive coefficient, but their isolated location provided acceptable safety given the Cold War need for their plutonium.

The days of safety certainty at Hanford were brief. After World War II, General Electric Company (GE) took over Hanford's management from DuPont. The reactors were worse for the wear of wartime production. DuPont's own internal history of Hanford observed: "the production facilities at Hanford that DuPont turned over to General Electric had major operational problems" so severe that it expected them to have short production lives.[9] GE concluded the probability and consequences of an accident were growing. It was understood that Hanford reactors had positive reactivity coefficients, but the aging graphite bricks that surrounded the uranium fuel created a new problem. By 1948, a Hanford supervisor wrote, the "appalling prospect" of a runaway from the bricks' stored energy "is immediately conceivable."[10] It was possible the heat could be inadvertently released to the fuel, and the positive reactivity coefficient could cause a runaway. While operational changes and further research by GE later reduced concern about this problem, the Safeguard Committee worried that a runaway was credible, and radiation could be “suddenly released in a single catastrophe.”[11] It prodded Hanford staff to study a range of conceivable runaway initiators, such as sabotage, earthquakes, and even the almost inconceivable failure of the Grand Coulee Dam upstream on the Columbia River.[12] The committee also believed the consequences of a runaway were “far more disastrous” than wartime estimates. Fission product contamination from isotopes of iodine and strontium were likely to spread well beyond the original 1.5-mile radius.[13]

At the Hanford reactors, the Safeguard Committee concluded the existing isolation standard was insufficient. It recommended expanding the exclusion radius around the reactors to about five miles, but that pushed it outside Hanford’s boundaries and encompassed small communities nearby. Worse, the exclusion area would have to grow larger as the AEC responded to Cold War tensions by building even larger reactors and raising power levels of existing ones. Lacking containment buildings, Hanford reactors also had a weak second line of defense. Public safety depended on active systems, the least reliable line in defense in depth. The Safeguard Committee thought a safer reactor design was possible, but “the present Hanford type pile is definitely not in this category.”[14] Even their designer, DuPont, agreed that Hanford’s reactors were less safe than the new heavy-water production reactors it was building at Savannah River, South Carolina. The latter reactors, DuPont bragged, enjoyed greater inherent safety. Even a decade later in the early 1960s, Hanford engineers admitted that it was “obvious that the Hanford reactor safety systems cannot measure up” to current standards of safety.[15] Shuttering Hanford, however, was unthinkable while the Korean War and tensions with Russia kept the nation on a wartime footing. The expense of plutonium production made impracticable costly redesign that had unproven value. The Safeguard Committee implored GE to find creative ways to make Hanford reactors safe enough to operate.[16]

But how safe was “safe enough”? Ideally, the answer required risk quantification—the product of accident probabilities and consequences. GE already had conceived of several worst-case scenarios. For Question 3—consequences—they had the benefit of data from weapons testing and Hanford’s secret “green run” where, for over six hours, the facility released and monitored the dispersion of fission products from very radioactive fuel, including about four thousand curies of the dangerous isotope Iodine-131. By comparison, the accident at Three Mile Island released less than twenty curies of Iodine-131, while the Fukushima