Nuclear Plant Risk Studies

Failing the Grade

DAVID LOCHBAUM

August 2000
Union of Concerned Scientists

Acknowledgments

The author wishes to acknowledge Anita Spiess, UCS editor, for her invaluable suggestions on reorganizing this report.

David Lochbaum is nuclear safety engineer at the Union of Concerned Scientists.

The Union of Concerned Scientists is a partnership of citizens and scientists working to preserve our health, protect our safety, and enhance our quality of life. Since 1969, we've used rigorous scientific analysis, innovative policy development, and tenacious citizen advocacy to advance practical solutions for the environment.

In our work on nuclear power safety we expose unsafe nuclear plant conditions and practices and seek to enhance nuclear safety performance industrywide. We monitor and assess plant performance, ensure regulatory compliance, and champion safety concerns of nuclear professionals in order to maintain nuclear safety.

More information about UCS and its work on nuclear power safety is available at the UCS site on the World Wide Web, at *www.ucsusa.org/energy.*

The full text of this report is available on the UCS website *(www.ucsusa.org)* or may be obtained from

UCS Publications
Two Brattle Square
Cambridge, MA 02238-9105

Or email *pubs@ucsusa.org* or call 617-547-5552.

Printed on recycled paper

Contents

Figures and Tables

Nuclear Plant Risk Studies

Failing the Grade

Executive Summary

An accident at a US nuclear power plant could kill more people than were killed by the atomic bomb dropped on Nagasaki.[1] The financial repercussions could also be catastrophic. The 1986 accident at the Chernobyl nuclear plant cost the former Soviet Union more than three times the economical benefits accrued from the operation of every other Soviet nuclear power plant operated between 1954 and 1990.[2]

But consequences alone do not define risk. The probability of an accident is equally important. When consequences are very high, as they are from nuclear plant accidents, prudent risk management dictates that probabilities be kept very low. The Nuclear Regulatory Commission (NRC) attempts to limit the risk to the public from nuclear plant operation to less than 1 percent of the risk the public faces from other accidents.

The Union of Concerned Scientists (UCS) examined how nuclear plant risk assessments are performed and how their results are used. We concluded that the risk assessments are seriously flawed and their results are being used inappropriately to increase—not reduce—the threat to the American public.

Nuclear plant risk assessments are really not risk assessments because potential accident consequences are not evaluated. They merely examine accident probabilities—only half of the risk equation. Moreover, the accident probability calculations are seriously flawed. They rely on assumptions that contradict actual operating experience:

- The risk assessments assume nuclear plants always conform with safety requirements, yet each year more than a thousand violations are reported.
- Plants are assumed to have no design problems even though hundreds are reported every year.
- Aging is assumed to result in no damage, despite evidence that aging materials killed four workers.
- Reactor pressure vessels are assumed to be fail-proof, even though embrittlement forced the Yankee Rowe nuclear plant to shut down.
- The risk assessments assume that plant workers are far less likely to make mistakes than actual operating experience demonstrates.

1. US House of Representatives, Committee on Interior and Insular Affairs Subcommittee on Oversight & Investigations, "Calculation of Reactor Accident Consequences (CRAC2) for US Nuclear Power Plants (Health Effects and Costs) Conditional on an 'SST1' Release," November 1, 1982; and Nuclear Regulatory Commission, "A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants," NUREG/CR-6451, Washington, D.C., August 1997.

2. Richard L. Hudson, "Cost of Chernobyl Nuclear Disaster Soars in New Study," *Wall Street Journal*, March 29, 1990.

- The risk assessments consider only the threat from damage to the reactor core despite the fact that irradiated fuel in the spent fuel pools represents a serious health hazard.

The results from these unrealistic calculations are therefore overly optimistic.

Furthermore, the NRC requires plant owners to perform the calculations, but fails to establish minimum standards for the accident probability calculations. Thus, the reported probabilities vary widely for virtually identical plant designs. Four case studies clearly illustrate the problem:

- The Wolf Creek plant in Kansas and the Callaway plant in Missouri were built as identical twins, sharing the same standardized Westinghouse design. But some events at Callaway are reported to be 10 to 20 times more likely to lead to reactor core damage than the same events at Wolf Creek.

- The Indian Point 2 and 3 plants share the same Westinghouse design and sit side by side in New York, but are operated by different owners. On paper, Indian Point 3 is more than 25 percent more likely to experience an accident than her sister plant.

- The Sequoyah and Watts Bar nuclear plants in Tennessee share the same Westinghouse design. Both are operated by the same owner. The newer plant, Watts Bar, was originally calculated to be about 13 times more likely to have an accident than her sister plant. After some recalculations, Watts Bar is now only twice as likely to have an accident.

- Nuclear plants designed by General Electric are equipped with a backup system to shut down the reactor in case the normal system of control rods fails. On paper, that backup system is highly reliable. Actual experience, however, shows that it has not been nearly as reliable as the risk assessments claim.

To make matters worse, the NRC is allowing plant owners to further increase risks by cutting back on tests and inspections of safety equipment. The NRC approves these reductions based on the results from incomplete and inaccurate accident probability assessments.

UCS recommends that the NRC immediately stop cutting safety margins and postpone any further cuts until the faults in the probability assessments are corrected. The US Congress must provide the NRC with the budget it needs to restore the safety margins at America's nuclear power plants.

Nuclear Plant Risk Studies

Failing the Grade

Section 1: Introduction

There is a risk in the use of safety goals in nuclear regulation—and in one sense it cost us the Three Mile Island accident to learn that the risk is real. The nuclear community got hung up on the safety-goal application of probabilistic risk analysis (PRA) at the expense of valid risk management applications, which had anticipated a TMI-type event.

—Robert M. Bernero, Nuclear Regulatory Commission, 1983

The Nuclear Regulatory Commission (NRC) uses rules and regulations to manage nuclear plant risks. The objectives of the rules and regulations are to reduce the chance that a nuclear accident will occur, minimize the severity of an accident, and protect the public from radiation released during an accident. Recognizing that its rules and regulations do not guarantee zero risk, the NRC has defined acceptable risk:

> (1) The risk of an immediate fatality to an average individual in the vicinity of a nuclear power plant that might result from reactor accidents should not exceed 0.1% of the sum of the immediate fatality risks that result from other accidents to which the US population is generally exposed and (2) the risk of cancer fatalities to the population near a nuclear power plant should not exceed 0.1% of the sum of cancer fatality risks from all other causes.[1]

Data on immediate fatality risks from non-nuclear causes are readily available. For example, the federal government releases annual reports detailing the number of Americans dying due to diseases, suicides, homicides, and accidents.[2] No Americans other than workers have yet experienced immediate fatalities from nuclear plant accidents.[3]

The lack of previous immediate fatalities does not correspond to zero risk because a nuclear plant accident can cause hundreds, perhaps thousands, of immediate fatalities. As Bernero observes in the epigraph, "the risk is real." Governmental studies estimate that more people could be killed by a nuclear plant accident than were killed by the atomic bomb dropped on Nagasaki.[4]

When the NRC learns that a nuclear plant does not meet federal safety regulations, it relies on

1. Nuclear Regulatory Commission, "TIP: 12—Nuclear Reactor Risk," Washington, D.C., September 1999.

2. Donna L. Hoyert, Kenneth D. Kochanek, and Sherry L. Murphy, "Deaths: Final Data for 1997," Atlanta, Ga.: Centers for Disease Control and Prevention, June 30, 1999.

3. *Immediate fatalities* is used because it has been alleged that the Three Mile Island accident in 1979 caused cancer-related deaths years later. The courts are still processing this allegation.

4. US House of Representatives, Committee on Interior and Insular Affairs Subcommittee on Oversight & Investigations, "Calculation of Reactor Accident Consequences (CRAC2) for US Nuclear Power Plants (Health Effects and Costs) Conditional on an 'SST1' Release," November 1, 1982; and Nuclear Regulatory Commission, "A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants," NUREG/CR-6451, Washington, D.C., August 1997.

the calculated accident probabilities to assess the risk. The NRC's risk assessment could conclude that the plant must be immediately shut down for repairs. Most often, the NRC decides that the risk is not great enough to require immediate shutdown, so the plant owner is allowed to wait until the next scheduled opportunity to make the necessary repairs. In addition, the NRC—under constant pressure from the nuclear industry—has recently accepted a concept of "risk-informed regulation," in which many safety regulations are eliminated and the scope of other regulations is significantly reduced based on the results of risk assessments. A critical question, then, is whether risk assessments are accurate enough to rely on for these purposes.

This report examines nuclear power plant risk assessments and how their results are being used. Section 2 provides background on risk and describes the relationship of the key factors—probability and consequences—used in risk assessments. Section 3 discusses the safety studies the NRC required each plant owner to prepare and explains why these studies are probability, and not risk, assessments. Section 4 highlights flawed assumptions used in the probability assessments that make their results inaccurate. Case studies, presented in section 5, illustrate how the defective assessment process can lead to grossly inaccurate results. Section 6 outlines the material that has been neglected in the so-called risk assessments; namely, the consequences of nuclear plant accidents. This section also details how, because consequences are neglected, the accident probabilities are not low enough to meet the level of acceptable risk set by the NRC. Section 7 synthesizes this information and explains when the NRC's assessments can, and more importantly cannot, be used to make decisions about public health. The final section recommends actions the NRC should take to improve the quality of plant safety assessments and measures the US Congress should adopt to permit the NRC to efficiently do what is needed.

Section 2: Risk Assessment Basics

The values to society of risks and benefits, as perceived by the people in that society, are not the sums of the values to the individuals affected. The catastrophe that kills 1000 people at a whack is perceived as far more threatening—that is, it has far larger negative value—than 1000 single-fatality auto wrecks.

—Stephen H. Hanauer, Nuclear Regulatory Commission, 1975

Risk is defined as "the potential for realization of unwanted, adverse consequences to human life, health, property, or the environment; estimation of risk is usually based on the expected value of the conditional probability of the event occurring times the consequences of the event given that it has occurred."[5] To put some flesh on the bones of this definition, consider an event that occurs, on average, once a decade and injures 40 people when it happens. Consider another event that happens every other year, but injures only 8 people each time.

Let's say that you could spend a million dollars and totally eliminate the chance of one of these events occurring again. Faced with this decision, you want to spend the money where it will do the most good. Would you eliminate the first event because it injures 40 people as opposed to just 8 people? Or would you eliminate the second event because it happens more often?

In this case, you can't lose. The elimination of either event prevents it from injuring an average of 4 people each year:

- 1 event every 10 years injuring 40 people per event averages 4 injuries per year

- 1 event every 2 years injuring 8 people per event averages 4 injuries per year

These two events have exactly the same risk even though they have different probabilities and different consequences. But what if the second event injured 10 people each time it happened instead of only 8?

- 1 event every 2 years injuring 10 people per event averages 5 injuries per year

It might be tempting to spend the money on the first event because it causes 40 injuries, but it would now be wiser to eliminate the second event because it ultimately injures more people and thus poses greater risk. This exercise shows how critical it is, when evaluating risk, to consider both the probability of an event and the consequences from that event.

But as the epigraph points out, society demands extra protection when it comes to events with high consequences. The airline industry must constantly seek to minimize the probabilities of crashes even though air travel is—on paper—safer than automobile travel. And few technological disasters have higher consequences than a nuclear power plant accident. The next section describes how the nuclear industry determines the probabilities for these accidents.

5. Society for Risk Analysis, "Glossary of Risk Analysis Terms," McLean, Va. Available online at *www.sra.org/gloss3.htm*.

Section 3: Nuclear Plant Risk Assessment

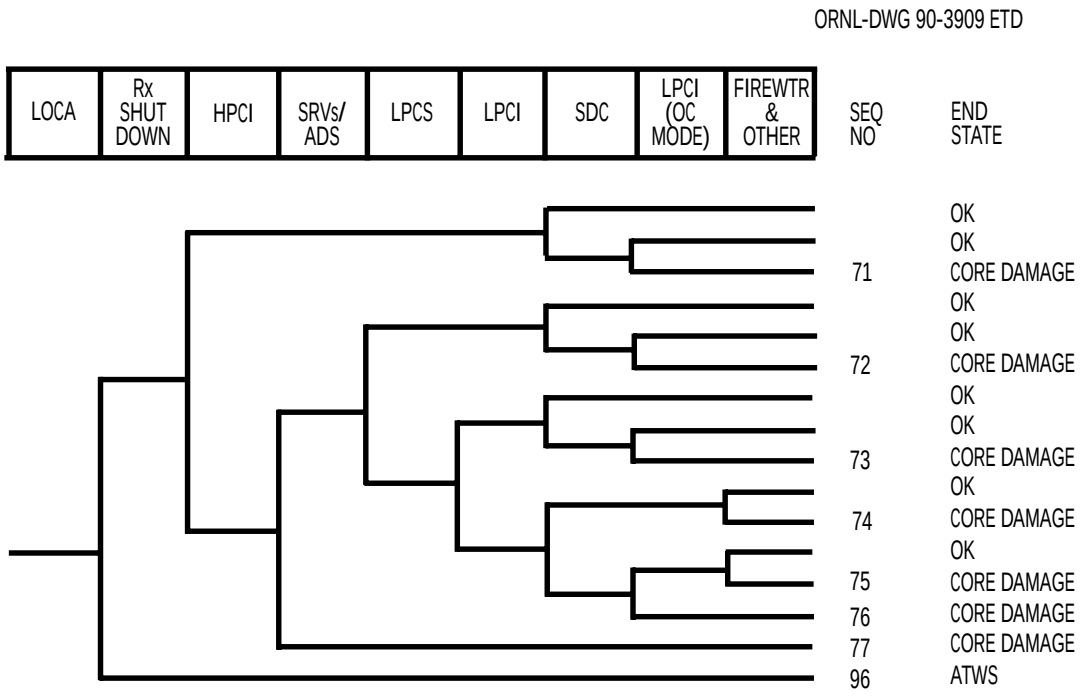
The only people I know who are enthusiastic about quantitative risk assessment are people who want to gain permission to expose other humans to dangerous chemicals so someone can make money. Risk assessment has proven to be an effective way to gain the necessary permissions.

—Peter Montague, Environmental Research Foundation, 1991

In 1988, the Nuclear Regulatory Commission required all nuclear plant owners to develop Individual Plant Examinations (IPEs). An IPE was to be an evaluation of each plant for accident vulnerabilities. All plant owners opted to perform probabilistic risk assessments (PRAs) to satisfy the NRC's request.[6] The NRC compiled the risk assessment information for all the plants and summarized it in a 1996 report.[7]

Probabilistic risk assessment is an analytical technique for evaluating potential accidents. The first level of assessment, Level I, examines events that can cause reactor core damage, such as a pipe break or power failure. Each event is then assessed using a fault-tree, which examines the possible responses to an event. The final product resembles a family tree chart, as the sample in figure 1 illustrates.

Figure 1. BWR Class B Small-Break Loss-of-Coolant Accident



6. Tim Leahy and Alan Kolaczkowski, "PRA for Technical Managers P-107," Washington, D.C.: Nuclear Regulatory Commission, December 1–3, 1998.

7. Nuclear Regulatory Commission, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," NUREG-1560, Vols. 1 and 2, Washington, D.C., November 1996.

The sample chart shows the fault-tree for a break of a small pipe connected to the reactor pressure vessel of a nuclear plant with a boiling water reactor. That event is termed a small-break loss-of-coolant accident (LOCA). The fault-tree moves from left to right asking a series of questions. When the answer is yes, the pathway moves upward. Otherwise, the pathway moves downward. For example, the first question is whether the reactor (Rx) can be shut down following the pipe break. If the answer is no, the fault-tree moves to the extreme right for ATWS (Anticipated Transient Without Scram). The ATWS event, which involves the failure of the normal control rod system to shut down the nuclear chain reaction, has its own fault-tree analysis. When the reactor can be shut down, the fault-tree progresses to the second question—can the high-pressure coolant injection (HPCI) system add enough water to compensate for the water being lost through the broken pipe? The right column shows the condition of the reactor core for each of the fault-tree paths. Some pathways result in core damage, while others do not.

The P in PRA enters into the picture by assigning probabilities for the answers in a fault-tree. The probability that a specific pathway in a fault-tree will occur is determined by multiplying each of the individual probabilities along the way.

A variety of events besides the pipe break illustrated above can lead to core damage. Other examples include the break of a large pipe connected to the reactor pressure vessel, the interruption of cooling water flow to the reactor core, the loss of normal electricity supply to plant equipment, and flooding of plant areas. The PRA includes fault-trees for each event.

The final step in Level I is to calculate the core damage frequency (CDF), i.e., the probability, per reactor year, of an accident leading to core damage.[8] This is done by adding up all the pathways resulting in core damage from all of the fault trees. The CDF is frequently expressed in mathematical form like $5x10^{-5}$ or 5E-05. In plain English, such a CDF value means 5 accidents in 100,000 reactor years (or 1 accident in 20,000 reactor years).

The second level of the probabilistic risk assessment, Level II, explores the ability of the plant's containment systems to cope with a core damage accident. This part of the assessment assumes that the reactor core is damaged and examines the pathways that lead to radioactive material being released to the environment. The fault-tree approach is the same as for Level I, except that the initiating event on the left side of the fault-tree is reactor core damage and the questions probe the plant's ability to deal with it.

Level III examines the impact on public health and the environment from a core damage accident with containment failure. This assessment assumes that reactor core damage has occurred and that radioactive material has been released to the environment. It then examines the pathways that lead to human health consequences. Two major factors in a Level III assessment are weather conditions and how close people live to the plant.

Plant owners submitted the Individual Plant Examinations (IPEs) to the NRC in the early 1990s. These documents are readily available from the NRC's Public Document Room. But they have not been updated to reflect new information and physical changes to the plants.

8. NRC, "Individual Plant Examination Program," Vol. 1, Part 1, p. G-3.

When plants are modified, the owners prepare a second type of document, the Plant Safety Assessment (PSA) to reflect the plant's new configuration. Like the IPEs, the PSAs include probabilistic risk assessments. However, few plant owners have submitted PSAs for their plants to the NRC, so the public has access only to the outdated IPEs.

Furthermore, most plant owners have submitted only Level I and II probabilistic risk assessments (PRAs). Level III assessments have been prepared and submitted for only a small handful of plants. Thus the IPEs for most plants do not contain true risk assessments. Because risk depends on both the probability of an event and its consequences, failure to include Level III evaluations provides an incomplete picture of the risk. At best, the Level I and II PRAs are only probability assessments because their results indicate how often an event is likely to occur without providing any clue about the consequences of that event.

In addition to presenting incomplete risk profiles, fundamental flaws in the Level I and II PRAs provide an inaccurate picture of the probabilities of nuclear plant accidents. The next section describes some of the major flaws in the PRAs. Section 5 explains how the flawed PRAs happened and vividly demonstrates the gross inaccuracy of their results.

Section 4: Unrealistic Assumptions

You can make probabilistic numbers prove anything, by which I mean that probabilistic numbers "prove" nothing.

—Stephen H. Hanauer, Nuclear Regulatory Commission, 1975

All probability analyses make assumptions. For example, when you calculate that the probability of getting heads upon a single flip of a quarter is 50 percent, you are assuming that the coin will not land on its edge. Nuclear plant probabilistic risk assessments (PRAs) rely on numerous assumptions, such as the following: [9]

- The plants are operating within technical specifications and other regulatory requirements.
- Plant design and construction are completely adequate.
- Plant aging does not occur; that is, equipment fails at a constant rate.
- The reactor pressure vessels never fail.
- Plant workers make few serious mistakes.
- Risk is limited to reactor core damage.

History shows there is a greater probability of a flipped coin landing on its edge than of these assumptions being realistic. Unrealistic assumptions in the PRAs make their results equally unrealistic. In computer programming parlance, "garbage in, garbage out." The unrealistic assumptions of nuclear plant PRAs are examined below.

Unrealistic Assumption #1—Plants Always Conform with All Regulatory Requirements

The technical specifications and regulatory requirements are essentially the rules of the road that plant owners are supposed to follow. When they do not, they must report violations to the NRC. As table 1 illustrates, more than a thousand violations are reported every year.

While some comfort might be taken from seeing that fewer reports were submitted at the end of the decade than at its beginning, that comfort dissipates when one remembers that the risk assessments assume that there are *zero* violations.

Table 1
Number of Violations Reported to NRC[a]

1987	2,895
1988	2,479
1989	2,356
1990	2,128
1991	1,858
1992	1,774
1993	1,400
1994	1,279
1995	1,178
1996	1,274
1997	1,473

a. Nuclear Regulatory Commission, "Office for Analysis and Evaluation of Operational Data 1997 Annual Report Reactors," NUREG-1272, Vol. 2, No. 1, Table 5.1, Washington, D.C., November 1998.

Nine nuclear reactors were shut down throughout the entire year of 1997 while their owners repaired safety equipment. Those reactors were Millstone Units 1, 2, and 3 in Connecticut; Salem Unit 1 in New Jersey; Crystal River 3 in

9. NRC, "Individual Plant Examination," Vol. 2, Parts 2–5, p. 14-3.

Florida; and Clinton, LaSalle Units 1 and 2, and Zion Unit 2 in Illinois.[10] The PRAs for each of these reactors, which had been submitted to the NRC before January 1, 1997, assumed that the reactors met *all* technical specifications and other regulatory requirements. Their year-plus outages demonstrate the fallacy of those assumptions.

As a result of this unrealistic assumption, the core damage frequencies (CDFs) calculated in the PRAs are too low. As section 3 explains, CDFs are determined from fault-trees for events that can lead to core damage. The fault-trees examine the plant's ability to respond to those events. By assuming that emergency equipment meets safety requirements when in fact it does not, the PRAs calculate better response capabilities than are supported by reality. In other words, the core damage frequencies are really higher than reported by the PRAs.

Unrealistic Assumption #2—Plant Design Is Completely Satisfactory

The assumption about plants' design and construction being adequate also defies reality, as table 2 illustrates.

The risk assessments assume that there are *zero* design and construction problems when hundreds of problems are discovered every year. The NRC's Office for Analysis and Evaluation of Operational Data documented 3,540 design errors reported between 1985 and 1994.[11] That means a design error was discovered at a nuclear power plant in the United States almost every single day for an entire decade.

Table 2
Number of Safety Problems Caused by Design, Construction, Installation, and Fabrication Errors Reported to NRC[a]

4th quarter 1995	86
1st quarter 1996	107
2nd quarter 1996	116
3rd quarter 1996	101
4th quarter 1996	143
1st quarter 1997	177
2nd quarter 1997	137
3rd quarter 1997	38

a. Nuclear Regulatory Commission, "Office for Analysis and Evaluation of Operational Data 1997 Annual Report Reactors," NUREG-1272, Vol. II, No. 1, Table A-1.14, Washington, D.C., November 1998.

Last year, Public Citizen's Critical Mass Energy Project documented more than 500 design problems found in US nuclear power plants between October 1996 and May 1999.[12] Topping the list was the Vermont Yankee nuclear plant with 42 design problems found during the 31-month period. Many of the design problems had existed since the nuclear plants began operating decades ago.

Moreover, according to the NRC, "Almost every plant-specific PRA has identified design or operational deficiencies."[13] Thus, even though preparation of the risk assessments revealed design problems, the assessments continued to assume that no design problems exist.

10. Nuclear Regulatory Commission, "Plant Status Report for January 2, 1998," Washington, D.C. Available online at *www.nrc.gov/NRR/DAILY/980102pr.htm.*

11. Sadanandan V. Pullani, "Design Errors in Nuclear Power Plants," AEOD/T97-01, Washington, D.C.: NRC Office for Analysis and Evaluation of Operational Data, January 1997.

12. James P. Riccio, "Amnesty Irrational: How the Nuclear Regulatory Commission Fails to Hold Nuclear Reactors Accountable for Violations of Its Own Safety Regulations," Washington, D.C.: Public Citizen, August 1999.

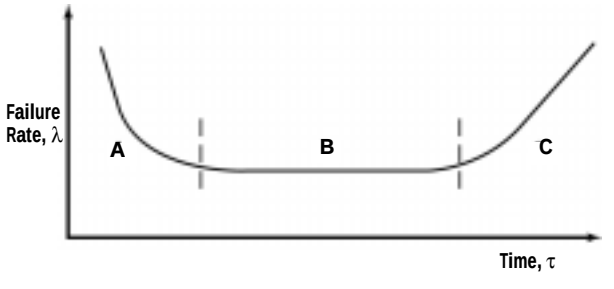
13. Nuclear Regulatory Commission, "Probabilistic Risk Assessment (PRA) Reference Document," NUREG-1050, p. 47, Washington, D.C., September 1984.

The NRC knows that nuclear plants had design problems that were not reflected in their risk assessments. In January 1999, UCS presented its views on risk-informed regulation to the NRC. During that presentation, NRC Chairman Shirley Ann Jackson interrupted UCS's David Lochbaum to ask a question of Ashok Thadani, Director of the NRC's Office of Research:

> *Mr. Lochbaum:* There is no feedback [to change the risk assessments to account] for design failures, just active component failures.
>
> *Chairman Jackson:* There is no feedback for design failures, just for active components?
>
> *Mr. Thadani:* For design failures that is correct. That is an area that is not dealt with in the risk assessments. That's a recognized weakness.
>
> *Chairman Jackson:* So how do you handle that? What do you do about that?
>
> *Mr. Thadani:* Design failure is like—pardon me for using this language—a blunder in my view. It's not really a random issue. At a plant there is or is not a design problem. It is not the sort of thing you can deal with in a probabilistic manner.[14]

So design blunders at nuclear plants are intentionally being ignored in the weakened PRAs even though design failure data are readily available. A nuclear widget needed to prevent or mitigate an accident may fail to perform this vital function if it is broken, if it is mistakenly disabled by plant workers, or if is improperly designed. The PRAs account for the breaks and mistakes, but not for the abundant design blunders.

Figure 2. "Bathtub" Curve of Failure Rate



Unrealistic Assumption #3—Like Dorian Gray, Nuclear Plants Do Not Age

Another incredible assumption is that nuclear plants and their equipment are getting older but not showing any signs of aging. Again the assumption is made in the face of clear evidence to the contrary. The NRC has issued more than one hundred technical reports about the degradation of valves, pipes, motors, cables, concrete, switches, and tanks at nuclear plants caused by aging.[15] These reports demonstrate that parts in nuclear plants follow the "bathtub curve" aging process illustrated in figure 2 above. Region A is the break-in phase, Region C is the wear-out phase, and Region B is the peak-health phase. The PRAs assume equipment failure rates from the flat portion (Region B) of the "bathtub curve," where the chance of failure is the lowest. And the NRC knows it. During a three-day training course in December 1998, NRC supervisors and managers were informed: "Most PRAs assume constant failure rates—in the

14. Nuclear Regulatory Commission, "Briefing on Risk-Informed Initiatives," transcript, Washington, D.C., January 11, 1999.

15. Nuclear Regulatory Commission, "NRC Research Program on Plant Aging: Listing and Summaries of Reports Issued Through September 1993," NUREG-1377, Rev. 4, Washington, D.C., December 1993.

'flat' portion of bathtub curve. This implies aging of components is not modeled in most PRAs."[16]

A telling demonstration of the effects of age occurred in 1986. Four workers were killed at a nuclear power plant in Virginia because a section of pipe eroded away with time until it broke and scalded them with steam.[17] Yet most PRAs assume *no* aging effects.

Unrealistic Assumption #4—Reactor Pressure Vessels Can Never Fail

The assumption about the reactor pressure vessel never failing is based on necessity, not science. The reactor pressure vessel is a large, metal "pot" containing the reactor core. The majority of a plant's emergency systems are intended to prevent water from leaking out of this pot or to quickly refill the pot if it leaks. The pot must remain filled with water to keep the reactor core from overheating. If the metal pot were to break open, water would pour out faster than *all* of the emergency pumps together could replenish. This would result in a reactor core meltdown and the release of huge amounts of radiation. Because there is no backup to the reactor pressure vessel and because the plant's emergency systems cannot prevent meltdown if it breaks, the risk assessments conveniently assume that it cannot fail—ever—under any circumstances.

Experience has shown that this assumption has as many cracks and flaws as the reactor pressure vessels themselves. In 1995, UCS issued a report on the fragile condition of reactor pressure vessels at nuclear power plants.[18] For example, the Yankee Rowe plant in Massachusetts closed in 1992 because its reactor pressure vessel had become brittle over time. Brittle metal can shatter, much like hot glass, when placed in cold water. Despite the closure of the Yankee Rowe plant and documented embrittlement at many other nuclear plants, the risk studies continue to assume a *zero* chance of reactor pressure vessel failure.

Unrealistic Assumption #5—Plant Workers Will Not Make Serious Mistakes

PRAs make bold assumptions about human performance during the periods of high stress and information overload associated with accidents and near-misses. Sometimes, the assumptions are totally unjustified. For example, the NRC commissioned a risk analysis of the spent fuel pool when engineers working on the Susquehanna nuclear plant raised concerns about its safety. That PRA assumed that workers immediately begin taking actions to restore cooling when the spent fuel pool temperature reaches 125 degrees Fahrenheit (°F).[19] When the engineers challenged that assumption, the NRC reported that plant's operating license required the spent fuel pool temperature to remain below 125°F and that workers were trained to conform to the rules of the operating license. Even after the engineers pointed out that the plant did not even have temperature instruments for the workers to use, the NRC retained this blatantly false

16. Leahy and Kolaczkowski, "PRA for Technical Managers P-107."

17. Brian Jordan, "NRC Finds Surry Accident Has 'High Degree' of Safety Significance," *Inside NRC*, Washington, D.C.: McGraw-Hill, January 5, 1987.

18. Robert Pollard, "US Nuclear Power Plants—Showing Their Age—Case Study: Reactor Pressure Vessel Embrittlement," Cambridge, Mass.: Union of Concerned Scientists, December 1995.

19. Joseph W. Shea, Project Manager, Nuclear Regulatory Commission, to David A. Lochbaum and Donald C. Prevatte, "Susquehanna Steam Electric Station, Units 1 and 2, Draft Safety Evaluation Regarding Spent Fuel Pool Cooling Issues," October 25, 1994. Available from the NRC Public Document Room, Washington, D.C.

assumption.[20] This had the effect of lowering the calculated probability by a factor of at least 10 and maybe 100.

A report issued in February 2000 by the Idaho National Engineering and Environmental Laboratory (INEEL) demonstrates that unjustified assumptions about worker behavior continue to be a problem. Researchers at INEEL examined 20 recent operating events at nuclear power plants and concluded:

> Most of the significant contributing human performance factors found in this analysis of operating events are missing from the current generation of probabilistic risk assessments (PRAs), including the individual plant examinations (IPEs). The current generation of PRAs does not address well the kinds of latent errors, multiple failures, or the type of errors determined by analysis to be important in these operating events.
>
> In the PRAs, human performance accounts for 5–8% of risk (i.e., contributes to less than 10% of core damage frequency estimates). … In the 20 operating events analyzed to date using qualitative and quantitative SPAR [standardized plant analysis risk] methods, the average contribution of human performance to the event importance was over 90%. … In nearly all cases, plant risk more than doubled as a result of the operating event—and in some cases increased by several orders of magnitude over the baseline risk presented in the PRA. This increase was due, in large part, to human performance.[21]

PRAs assume that workers will make fewer mistakes when responding to accidents than is justified by actual experience.

Unrealistic Assumption #6—Nuclear Plant Risk Is Limited Exclusively to Reactor Core Damage

Even if nuclear plant PRAs properly accounted for violations of regulatory requirements, design and construction errors, equipment aging, potential failure of the reactor pressure vessel, and actual human performance capabilities, they would still be flawed. The PRAs only determine the probabilities of events leading to reactor core damage. They do not calculate the probabilities of other events that could lead to releases of radiation, such as fuel going critical in the spent fuel pool or rupture of a large tank filled with radioactive gases. Some of these overlooked events can have serious consequences. For example, researchers at the Brookhaven National Laboratory estimated that a spent fuel pool accident could release enough radioactive material to kill tens of thousands of Americans.[22]

Thus, even the best nuclear plant PRA is incomplete because it neglects events that can release significant amounts of radiation. The effect of this incompleteness is to introduce

20. David A. Lochbaum and Donald C. Prevatte to Chairman Ivan Selin, Nuclear Regulatory Commission, "Susquehanna Steam Electric Station Units 1 and 2 / Comment on Draft Safety Evaluation Regarding Spent Fuel Pool Cooling Issues," November 29, 1994. Available from the NRC Public Document Room, Washington, D.C.

21. Jack E. Rosenthal to John T. Larkins, "Meeting with the Advisory Committee on Reactor Safeguards Human Factors Subcommittee, March 15, 2000, on SECY-00-0053, NRC Program on Human Performance in Nuclear Power Plant Safety," Washington, D.C.: Nuclear Regulatory Commission, March 6, 2000.

22. Nuclear Regulatory Commission, "A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants," NUREG/CR-6451, Washington, D.C., August 1997.

additional uncertainty into the results of the PRAs:

> Completeness is not in itself an uncertainty, but a reflection of scope limitations. The result is, however, an uncertainty about where the true risk lies. The problem with completeness uncertainty is that, because it reflects an unanalyzed contribution, it is difficult (if not impossible) to estimate its magnitude.[23]

Summary

Each of the unrealistic assumptions covered in this section causes the probabilistic risk assessments to underestimate the chances of a nuclear plant accident. In some cases, the accident probabilities are falsely lowered by a factor of 100. But the full extent of the underestimation is unknown.

The next section uses case studies to illustrate how unrealistic assumptions, along with lack of quality standards for the risk assessments, cause grossly inaccurate results.

23. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, p. 1.174-13, Washington, D.C., July 1998.

Section 5: Missing Quality Standards

The results of the Oak Ridge-SAI work and the INPO [Institute for Nuclear Power Operations] review of the Oak Ridge effort show clearly the reason why PRAs are not good measures of safety adequacy. So much subjective judgement is involved in the probability evaluation that the results cannot be trusted for absolute risk measurement.

—Myer Bender, Nuclear Regulatory Commission, 1983

Probabilistic risk assessments (PRAs) determine the probability of nuclear plant accidents resulting in reactor core damage as described in section 3. The nuclear industry uses this calculated core damage frequency (CDF) to rank safety threats—the larger the CDF, the greater the threat.

The whole purpose of the PRA is to calculate the CDF. The CDF is used extensively as a plant safety gauge. In reviewing the PRAs submitted by plant owners in their Individual Plant Examinations (IPEs), the NRC learned that

> One factor that can influence both the success criteria and the accident progression is the definition of core damage, which varied substantially in the IPEs from definitions involving vessel level to definitions involving fuel cladding temperature or oxidation.[24]

In other words, one plant owner could define core damage one way while another plant owner could define core damage in a completely different manner. How could something so vitally important to a PRA as the definition of core damage be left to such subjective interpretation? In the NRC's own words: "The NRC has not developed its own formal standard nor endorsed an industry standard for a PRA."[25]

The lack of a PRA standard gives plant owners free rein. That freedom manifests itself in PRA results for virtually identical nuclear plants being completely different. It also allows PRA results to be significantly more optimistic than reality. UCS prepared the following case studies to demonstrate these points:

- Wolf Creek and Callaway
- Indian Point Units 2 and 3
- Sequoyah and Watts Bar
- Standby Liquid Control Systems

These case studies are presented below.

Case Study #1—Wolf Creek and Callaway

Decades ago, the Westinghouse Electric Corporation designed what it called the Standardized Nuclear Unit Power Plant System (SNUPPS). Westinghouse sought to reduce costs, and thus make its reactors more saleable, by developing a plant design that could be replicated again and again. The Wolf Creek plant in Kansas and the Callaway plant in Missouri are the only two SNUPPS orders that were completed.[26] The plants were built using the exact same blueprints and materials. Callaway was licensed to operate by the NRC in October 1984, while Wolf Creek was licensed in June 1985.[27]

24. NRC, "Individual Plant Examination Program," Vol. 2, Parts 2–5, p. 15-3.

25. NRC, "An Approach for Using Probabilistic Risk Assessment," p. 1.174-10.

26. One of the two reactors ordered at Callaway was canceled during its construction.

27. Nuclear Regulatory Commission, "Information Digest," NUREG-1350, Vol. 10, Washington, D.C., November 1998. Available online at *www.nrc.gov/NRC/NUREGS/SR1350/V10/index.html.*

Both plant owners provided the NRC with risk assessments of postulated internal events, such as pipe breaks and valve failures, that could lead to reactor core damage. The risk assessments for core damage caused by external events, such as tornadoes and floods, are expected to vary because the plants are located in different states. But the internal event risk should be similar because Callaway and Wolf Creek were intentionally built to be identical twins.

In this case, however, the identical twins seem as different as Dr. Jekyll and Mr. Hyde. The most probable event leading to reactor core damage at Callaway is identified as a pipe break that causes Room 3101 to be flooded. Room 3101 contains electrical equipment that doesn't work well when submerged. Wolf Creek also has a Room 3101 housing plenty of electrical equipment. But when Wolf Creek's Room 3101 is flooded, it is reportedly 10 times less likely to result in reactor core damage.[28]

The fifth most likely event leading to reactor core damage at Callaway is a small-break loss-of-coolant accident, in which a small diameter pipe connected to the reactor pressure vessel breaks, leading to inadequate core cooling. Wolf Creek also has small diameter piping that can break and lead to reactor core damage. But the small-break loss-of-coolant accident at Wolf Creek is supposedly 20 times less likely to result in core damage and is estimated to be the eighteenth most likely event.[29]

The numbers make it look like Wolf Creek is the good twin and Callaway the bad twin. In reality, these risk assessments cannot be used to decide this sibling rivalry. They were developed using different methods and different assumptions. It is therefore no surprise that their results differ so radically. The data do not allow the safety levels of these identical plants to be evaluated, even on a relative basis.

This case study demonstrates a deeper problem: plant-specific risk assessments provide no meaningful insight into relative risks within a plant. Callaway and Wolf Creek have identical designs. Yet the Achilles' heel on Callaway seems no more than the funny bone on Wolf Creek. The input assumptions for the risk assessment at either plant could be tweaked and cause the numbers to flip-flop. The *actual* risks at the plants would be unchanged, but the *perceived* risks would change significantly.

Case Study #2—Indian Point

Indian Point Unit 2 (IP2) and Indian Point Unit 3 (IP3) are pressurized water reactors designed by the Westinghouse Electric Corporation. These plants are located side by side along the Hudson River in Buchanan, New York, about 35 miles north of New York City. The NRC issued operating licenses on September 28, 1973, for IP2 and on April 5, 1976, for IP3.[30] The individual plant examinations (IPEs) were completed in August 1992 for IP2[31] and in June 1994 for IP3.[32]

28. Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station Individual Plant Examination Summary Report," September 1992; and Union Electric Company, "Individual Plant Examination," October 9, 1992. Both documents are available from the NRC Public Document Room, Washington, D.C.

29. Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station"; and Union Electric Company, "Individual Plant Examination."

30. NRC, "Information Digest."

31. Consolidated Edison Company of New York, Inc., "Individual Plant Examination for Indian Point Unit No. 2 Nuclear Generating Station," August 1992. Available from the NRC Public Document Room, Washington, D.C.

32. New York Power Authority, "Indian Point 3 Nuclear Power Plant Individual Plant Examination," June 1994. Available from the NRC Public Document Room, Washington, D.C.

These two nuclear plants were designed by the same company and built in the same geographic location in the same era. One would expect these nuclear "sisters" would have comparable risks. That expectation appears incorrect, if one believes the risk numbers, which were both published at about the same time.

The overall chance of events leading to reactor core damage was calculated to be 27.3 percent higher for IP3 than for IP2. The disparity was even wider for individual events. One such event—the interfacing system loss-of-coolant accident—was calculated to be 89 percent more likely to occur at IP3 than at IP2.[33]

According to IP3's owner:

> A detailed comparison of the IPEs performed on IP2 and IP3 is made difficult by the difference in the methodologies used. The IPE prepared for IP3 employed the small event-tree/large fault-tree methodology used in the NUREG-1150 studies, considerable effort being devoted to the delineation of accident sequences. In contrast, the IPE prepared for IP2 used a large event-tree/small fault-tree methodology.[34]

IP3's owner concluded—paradoxically—that despite the different methodologies employed, "the core damage frequencies predicted for IP3 and IP2 are basically similar though significant differences do exist."[35]

Case Study #3—Sequoyah and Watts Bar

The two case studies above compare risk assessment results for nuclear plants that are very similar to each other. In each case, the nuclear plants were operated by different owners. The disparities in the results might be attributed to different approaches taken by the owners. However, analysis of two other plants suggests another explanation.

This case study looks at the risk assessments for the Sequoyah and Watts Bar nuclear power plants. Sequoyah and Watts Bar are sister plants. Each is a four-loop pressurized water reactor designed by Westinghouse with an ice-condenser containment. The two reactors at Sequoyah were licensed to operate by the NRC in 1980 and 1981.[36] The NRC issued TVA an operating license for Watts Bar in 1996.[37]

The Tennessee Valley Authority (TVA) operates both of these plants and prepared their risk assessments. Sequoyah has a core damage frequency of 1 in 26,525 years.[38] The original core damage frequency that TVA calculated for Watts Bar was 1 in 3,030 per year.[39] These numbers suggest that the newer plant, which TVA built using the lessons learned from Sequoyah, was nearly 10 times more likely to have a nuclear accident. One would hope that the passage of

33. NY Power Authority, "Indian Point 3," Table 1.5.1.1, p. 1-10.

34. NY Power Authority, "Indian Point 3," p. 1-23.

35. NY Power Authority, "Indian Point 3," p. 1-23.

36. NRC, "Information Digest."

37. NRC, "Information Digest."

38. Tennessee Valley Authority, "Sequoyah Nuclear Plant Units 1,2 Probabilistic Safety Assessment Individual Plant Examination," Vol. 1, February 20, 1998. Available from the NRC Public Document Room, Washington, D.C.

39. Tennessee Valley Authority, "Watts Bar Nuclear Plant Unit 1 Probabilistic Risk Assessment Individual Plant Examination Update, " Vol. 5, May 2, 1994. Available from the NRC Public Document Room, Washington, D.C.

15 years would have enabled TVA to make safety improvements or at least maintain the same safety levels as had been found at Sequoyah.

TVA later recalculated the core damage frequency for Watts Bar. By tweaking here and adjusting there, TVA reduced the core damage frequency for Watts Bar to 1 in 12,500 years.[40] Watts Bar is now only twice as unsafe as Sequoyah.

The saga of Sequoyah and Watts Bar clearly exposes the problem with probabilistic risk assessments (PRAs) performed by the nuclear industry. TVA, unsatisfied with Watts Bar's risk being 300 percent higher than the NRC's safety goal, waved its magic wand (in this case, it closely resembled a pencil eraser) until Watts Bar's risk dropped *lower* than the safety goal.

Case Study #4: Standby Liquid Control Systems

Our final case study explains just how the PRA wizards are able to dial in any risk number they want. The fault-trees have many branches. The branches represent the performance of emergency equipment and plant workers in response to the potential events.

The standby liquid control (SLC) system is a backup system in boiling water reactors designed by the General Electric (GE) Company, which is designed to stop the nuclear reaction if the control rods fail to do so. The SLC system is kept in standby mode when the nuclear plant is running. It consists of a large storage tank, two pumps, piping, and valves. Only one pump is required for the SLC system to fulfill its intended function—the second pump serves as a fully redundant backup. The system can be manually initiated by the operator to shut down the reactor when the normal reactivity-control system, the control rod drive system, fails. The SLC system injects a solution into the reactor vessel to absorb neutrons and end the fission chain reaction. The NRC ranked the SLC system as the eighth most important out of 30 safety systems it evaluated.[41]

Pennsylvania Power & Light, a nuclear plant owner with two boiling water reactors, calculated the chances that the SLC system would be unable to perform its vital safety function to be 1 in 16,666.[42] That means the system is expected to function properly 16,665 times out of 16,666 tries. Such high reliability for an important safety system would be comforting, if it were true. It is neither true nor comforting.

There are 35 boiling water reactors operating in the United States. If the SLC systems at these nuclear plants were tested every day and the reported system reliability were accurate, there would be one SLC system failure every 1.3 years. But the SLC systems are not tested every day. According to the NRC, the SLC system is routinely tested on a quarterly basis and nonroutinely tested following system maintenance.[43] The average frequency of SLC system testing at US nuclear plants falls between once per month and

40. TVA, "Watts Bar."

41. Nuclear Regulatory Commission, "Aging Assessment of BWR Standby Liquid Control Systems," NUREG/CR-6001, Washington, D.C., August 1992.

42. Harold W. Keiser, Senior Vice President—Nuclear, Pennsylvania Power & Light Company, to C. L. Miller, Project Manager, Nuclear Regulatory Commission, "Susquehanna Steam Electric Station—Submittal of the IPE Report," December 13, 1991. Available from the NRC Public Document Room, Washington, D.C.

43. Nuclear Regulatory Commission, "Standard Technical Specifications for General Electric Boiling Water Reactor 4, Section 3.1.7 and Bases Section 3.1.7, Standby Liquid Control System," NUREG-1433 Rev. 1, Washington, D.C., April 1995.

once per quarter. Thus, for the entire fleet of US boiling water reactors, there will be one SLC system failure reported every 39.7 to 119.0 years, *if* the SLC system reliability is as high as reported.

A cursory check of the NRC's Public Document Room revealed these reports:

- In August 1998, the owner of the Big Rock Point nuclear plant informed the NRC that its SLC system had been totally incapacitated for the past 13 to 18 years.[44]

- In January 1998, the owner of Susquehanna Unit 1 (i.e., the same entity that reported the extremely reliable SLC system) informed the NRC that both pumps of the SLC system were inoperable.[45]

- In December 1996, the owner of the FitzPatrick boiling water reactor informed the NRC that both pumps of the SLC system were inoperable.[46]

Thus, the SLC system is *not* as reliable as claimed in the plant risk assessments. Consequently, the actual risks from nuclear power plant operation are higher than reported in the risk assessments. Many branches of the fault-trees are similarly afflicted, rendering the results of the risk assessments virtually useless.

Summary

These case studies showed how the lack of quality standards for the risk assessments—particularly regarding the unrealistic assumptions described in section 4—enables the nuclear industry to subjectively "calculate" lower core damage frequencies. Decisions on public health must not be based on falsely optimistic accident probabilities. The consequences from a nuclear plant accident, as described in the next section, are potentially catastrophic.

44. Kenneth P. Powers, Site General Manager, Consumers Energy, to Nuclear Regulatory Commission, "Docket 50-155—License DPR-6—Big Rock Point Plant—Licensee Event Report 98-0001: Liquid Poison Tank Discharge Pipe Found Severed During Facility Decommissioning," August 6, 1998. Available from the NRC Public Document Room, Washington, D.C.

45. Pennsylvania Power & Light Company to Nuclear Regulatory Commission, "Licensee Event Report No. 50-387/97-025-00, Loss of Both Trains of Standby Liquid Control," January 2, 1998. Available from the NRC Public Document Room, Washington, D.C.

46. Michael J. Colomb, Plant Manager, New York Power Authority, to Nuclear Regulatory Commission, "Licensee Event Report: LER-96-011—Both Standby Liquid Control Subsystems Inoperable Due to Inoperable Pump Discharge Pressure Relief Valves," December 2, 1996. Available from the NRC Public Document Room, Washington, D.C.

Section 6: Consequences of a Nuclear Accident

Nuclear power is a business that can lose $2 billion in half an hour.

—Wall Street Journal, 1983

As the preceding sections indicate, the risk of a major accident at any nuclear power plant is unknown, because although the probability of an accident has been assessed (albeit with flawed assumptions, and inconsistent definitions and procedures), the consequences have not been assessed. This section draws on other sources to provide the missing piece of the risk puzzle.

A nuclear plant accident can harm the public by releasing radioactive materials. Radioactive materials emit alpha particles, beta particles, gamma rays, and/or neutrons. These emissions are called "ionizing radiation" because the particles produce ions when they interact with substances. Other materials can emit nonionizing radiation such as radio waves, microwaves, and ultraviolet light.[47]

Cells can be damaged or even killed by ionizing radiation. At high radiation exposures, tissues and organs can be damaged due to the large number of cells affected. Workers were killed by the radiation they received following the 1986 accident at Chernobyl in the Ukraine and the 1999 accident at Tokaimura in Japan. At lower exposures, it may take 5 to 20 years for radiation-induced effects, like cancer, to develop. Ionizing radiation can also produce genetic effects that appear in the individual's children or even several generations later.[48]

Following the Three Mile Island (TMI) accident in 1979, the Sandia National Laboratory estimated the potential consequences from reactor accidents that release large amounts of radiation into the atmosphere. Essentially, Sandia performed the equivalent of the Level III PRAs described in section 3 of this report: they assumed that reactor core damage occurred and that the containment buildings failed to prevent the release of radiation.

For each nuclear plant then in operation and nearing completion, Sandia determined the amount of radiation that could be released following a major accident, the area's weather conditions, and the population downwind of the plant. Then Sandia estimated how many Americans would die and be injured within the first year due to their radiation exposure. Sandia also estimated how many Americans would later die from radiation-induced illnesses like cancer. Table 3 provides a summary of Sandia's results.

The consequences vary because larger plants can release more radiation than smaller plants and because some plants are located near large population centers.[49] But in all cases, a nuclear accident was estimated to cause hundreds to thousands of immediate fatalities and thousands of subsequent cancer deaths.

47. Code of Federal Regulations, Title 10, Energy, Section 20.1003, Definitions.

48. Nuclear Regulatory Commission, "Biological Effect of Radiation," Technical Issue Paper 36, Washington, D.C., September 1999.

49. Decades ago, the forerunner of the NRC advocated higher safety standards for nuclear plants near high-population centers than for plants in remote areas. UCS contends now, as we did then, that all Americans deserve to be protected by the highest safety standards.

Table 3
Operating Nuclear Plant Accident Consequences[a]

Plant / Location	Early Fatalities	Injuries	Cancer Deaths
Beaver Valley / Shippingport, Penn.	19,000	156,000*	24,000
Browns Ferry / Decatur, Ala.	18,000	42,000	3,800
Byron / Rockford, Ill.	9,050	79,300	15,300
Callaway / Callaway, Mo.	11,500	32,000	9,600
Calvert Cliffs / Lusby, Md.	5,600	15,000	23,000
D C Cook / Bridgman, Mich.	1,950	84,000	13,000
Fermi / Laguna Beach, Mich.	8,000	340,000*	13,000
Harris / Apex, N.C.	11,000	31,000	6,000
Hatch / Baxley, Ga.	700	4,000	3,000
Indian Point 3 / Buchanan, N.Y.	50,000	167,000*	14,000
Limerick / Montgomery, Penn.	74,000*	610,000*	34,000
Millstone 3 / Waterford, Conn.	23,000	30,000	38,000
Nine Mile Point 2 / Oswego, N.Y.	1,400	26,000	20,000
Perry / Painesville, Ohio	5,500	180,000*	14,000
Pilgrim / Plymouth, Mass.	3,000	30,000	23,000
Salem / Salem, N.J.	100,000*	70,000	40,000
Susquehanna / Berwick, Penn.	67,000	47,000	28,000
Vermont Yankee / Vernon, Vt.	7,000	3,000	17,000

*For comparison, the atomic bomb dropped on Hiroshima killed 140,000 people, and the one dropped on Nagasaki killed 70,000 people.[b]

a. US House of Representatives, Committee on Interior and Insular Affairs Subcommittee on Oversight & Investigations, "Calculation of Reactor Accident Consequences (CRAC2) for US Nuclear Power Plants (Health Effects and Costs) Conditional on an 'SST1' Release," November 1, 1982.

b. Richard Rhodes, *The Making of the Atomic Bomb,* New York: Simon & Schuster, pp. 734 and 740, 1986.

How do these estimates relate to the NRC's policy of limiting the risk from a nuclear plant accident to less than 0.1 percent of the risk from other accidents?[50] During 1997, accidents claimed the lives of 95,644 Americans.[51] An accident at the Salem nuclear plant in New Jersey could—by itself—kill more than that many Americans. Yet the NRC's policy is to limit the number of deaths from nuclear plant accidents to less than 95 each year on average.

50. NRC, "TIP: 12."

51. Center for Disease Control and Prevention, "Fastats: Accidents/Unintentional Injuries," Atlanta, Ga., August 31, 1999. Available online at *www.cdc.gov/nchs/fastats/acc-inj.htm.*

As discussed in section 2, risk depends on both the probability and the consequences of an event. The NRC's risk goal can only be met if the probability of an accident is very, very low. How low? An accident causing 100,000 deaths must have a probability of less than 1 in 1,045 years to meet the NRC's risk goal of no more than 95 deaths from nuclear plant accidents.

In other words, nuclear power plants are acceptably safe under the NRC's goal so long as they kill no more than about 100 people per year, or 1,000 people every decade. A 50 percent chance of a nuclear accident killing 10,000 people every century would be acceptable. And the NRC's goal would accept a nuclear accident killing 100,000 people, provided that, on average, there would be no more than one accident per millennium.

This nuclear safety goal, of course, has never been explicitly approved by the American people or their representatives, the US Congress. As observed in section 2, society regards potential accidents with high consequences more seriously than the same consequences spread out over a long period of time. And few, if any, other technological disasters, whether dam breaks, airline crashes, bridge collapses, or train derailments, can result in such high consequences as a nuclear plant accident.

As the previous sections have shown, the PRAs cannot be relied upon to estimate the true probability of a nuclear accident. There are simply too many factors they do not consider and too many discrepancies that are not explained. As discussed in the next section, proper risk management strategies are neglected when accident probabilities are not well understood.

Section 7: Conclusions

There is no scientific or mathematical formula that can adequately measure risk.

—John H. Gibbons, Office of Technology Assessment, 1980

The risk from any event depends upon the probability of it occurring and the consequences if it were to occur. As explained in section 2 of this report, looking at only probability or only consequences results in an incorrect understanding of risk.

However, it is possible to properly manage risk without knowing much about the probability and/or consequences of an event. When every possible measure is implemented to prevent an event from occurring and every possible step taken to minimize the consequences should it occur, then the risk is as low as possible. But it is not possible to properly manage risk when only *reasonable*—instead of *all possible*—measures are taken to prevent and mitigate events unless the probabilities and consequences are accurately known.

The NRC required nuclear plant owners to prepare risk assessments in the early 1990s. But as section 3 reveals, these assessments merely evaluate the *probability* of reactor accidents. The plant-specific accident *consequences* have not been updated since a study done in 1982 using 1980 population information. Thus, the NRC has limited insight into nuclear plant risks.

The value of the NRC's partial insight is further diminished by the poor quality of the probability assessments. The probability assessment calculations rely on several assumptions that simply do not reflect reality, as documented in section 4. Thus, accident probabilities are higher than reported by the plant owners, and yet the NRC relies on them.

In large part, the probability assessments yield bogus results because the NRC never established minimum standards that plant owners had to meet. As the case studies in section 5 indicate, the lack of standard definitions and procedures for preparing probability assessments resulted in widely varying accident probabilities for virtually identical plants.

That a nuclear plant accident can have disastrous consequences may be known intuitively, but section 6 details the potential body counts. More people could be killed by a nuclear plant accident than were killed by the atomic bomb dropped on Nagasaki. The NRC attempts to manage this awesome risk by limiting the probability of an accident. But accident probabilities are not known with sufficient certainty to permit only *reasonable* instead of *all possible* safety precautions to be taken.

If this were just a historical observation, it would be bad enough. Unfortunately, the sad story gets worse.

The nuclear industry and the NRC are slashing safety regulations at a frenetic pace in an effort to make nuclear power plants more economical to operate. Nuclear plants must generate electricity at competitive prices if they are to survive in a deregulated electricity marketplace. In the past decade, plant owners made numerous changes to increase productivity (i.e., profitability). Refueling outages are an example. Nuclear power plants shut down every 18 to 24 months to load fresh fuel into the reactor core. Refueling outages that averaged 101 days in 1990 were

performed in only 51.1 days in 1998.[52] Consequently, the average output from nuclear plants rose from about 67 percent of capacity in 1990 to 79.5 percent in 1998.[53]

The remaining option for additional cost-savings is simply to do less. Plant owners are downsizing staff sizes by eliminating work. Fewer tests and inspections are performed at nuclear plants today than five years ago. For example, the NRC recently approved a request by the owner of the Duane Arnold nuclear plant in Iowa to test valves that limit the release of radioactive liquid every ten years instead every two years.[54] The NRC also allowed the owner of the San Onofre nuclear plant in California to relax the maintenance check on the valves that protect the main steam lines from bursting from too much pressure.[55] As a direct result, fewer problems are found and fewer repairs are needed. Plant owners save lots of money by reducing staffing levels and repair bills.

The NRC is approving these cost-cutting measures based on evaluations purporting to show that the reduced number of inspections does not increase the probability of accidents. But the incomplete and inaccurate probability assessments cannot identify the true risk of nuclear plant operation, nor can they provide a clue as to how far the results are from reality. How can that be possible? Imagine balancing a checkbook without having all of the deposit slips or all of the check amounts written against the account. You can calculate a balance, but it tells you nothing about how much money is in the account. And you can only guess if the number is higher or lower than the actual balance. Likewise, the NRC is guessing when it makes safety decisions using the results from incomplete and inaccurate probabilistic assessments.

The NRC is now proposing to move to so-called *risk-informed regulation*. This is the NRC's term for allowing plant owners to cut back on inspections and tests of safety equipment when risk assessment "shows" that such cutbacks would not increase risk. For example, the NRC has approved changing a test interval for a piece of equipment from once per month to once per quarter when risk information gathered and submitted by the plant's owner suggested that the equipment's failure will not significantly increase the probability of reactor core damage.

The NRC conceded that it cannot demonstrate the move to risk-informed regulation is necessary or will improve safety, the two criteria necessary to justify its use:

> More fundamentally, it may be very difficult to show that the risk informed changes, in any form, either: (i) will result in a substantial increase in overall protection of the

52. Nuclear Energy Institute, "Refueling Outages at US Nuclear Plants (Average Duration)," Washington, D.C., 1999. Available online at *www.nei.org.*

53. Nuclear Energy Institute, "US Nuclear Power Plant Average Capacity Factors 1980–1998," Washington, D.C., 1999. Available online at *www.nei.org.*

54. Brenda L. Mozafari, Project Manager, Nuclear Regulatory Commission, to Eliot Protsch, President, IES Utilities, Inc., "Duane Arnold Energy Center—Issuance of Amendment Re: Revised Excess Flow Check Valve Surveillance Requirements," Washington, D.C., December 29, 1999.

55. L. Raghavan, Senior Project Manager, Nuclear Regulatory Commission, to Harold B. Ray, Executive Vice President, Southern California Edison Company, "San Onofre Nuclear Generating Station, Units 2 and 3—Issuance of Amendments on Small Break Loss-of-Coolant Accident Charging Flow and Main Steam Safety Valve Setpoints," Washington, D.C., February 22, 2000.

> public health and safety or common defense and security, the initial backfit threshold finding; or (ii) are *necessary* for adequate protection.[56] [emphasis in original]

Yet the NRC continues to apply considerable resources to the move simply because it may save plant owners a few dollars. The public would be better served if these resources were applied to restoring safety margins at nuclear power plants. For example, the NRC could use these funds for additional inspections at nuclear power plants to seek out and correct more of the design blunders described in section 4 of this report.

56. William D. Travers, Executive Director for Operations, Nuclear Regulatory Commission, to Commissioners, Nuclear Regulatory Commission, "Options for Risk-Informed Revisions to 10 CFR Part 50—Domestic Licensing of Production and Utilization Facilities," SECY-98-300, Washington, D.C., December 23, 1998.

Section 8: Recommendations

The TMI accident revealed that perhaps reactors were not "safe enough," that the regulatory system has some significant problems (as cited in both the Kemeny and Rogovin investigations), that the probability of serious accident was not vanishingly small, and that new approaches were needed.

—Nuclear Regulatory Commission, 1984

The incomplete and inaccurate state of nuclear plant risk assessments does not provide a solid foundation for the NRC to move towards risk-informed regulation. Before the NRC takes another step towards risk-informed regulation, the NRC must complete the following tasks:

1. Establish a minimum standard for plant risk assessments that includes proper methods for

a) handling the fact that nuclear plants may not conform with all technical specification and regulatory requirements

b) handling the fact that nuclear plants may have design, fabrication, and construction errors

c) handling equipment aging

d) treating the probability of reactor pressure vessel failure

e) handling human performance

f) handling events other than reactor core damage in which plant workers and members of the public may be exposed to radioactive materials (e.g., spent fuel pool accidents and radwaste system tank ruptures)

g) handling nuclear plant accident consequences to plant workers and members of the public

h) justifying the assumptions used in the risk assessments

i) updating the risk assessments when assumptions change

2. Require all plant owners to develop risk—not probability—assessments that meet or exceed the minimum standard.

3. Require all plant owners to periodically update the risk assessments to reflect changes to the plant and/or plant procedures.

4. Require all plant owners to make the risk assessments publicly available.

5. Conduct inspections at all nuclear plants to validate that the risk assessments meet or exceed the minimum standards.

6. Disallow any use of risk assessment results to define a line between acceptable and unacceptable performance until all of the steps listed above are completed.

It will take considerable effort on the part of the NRC to implement these recommendations. Unfortunately, the NRC may be unable to take these safety steps because it is under attack from the US Congress to reduce its budget. Why? The NRC is a fee-based agency. Most of the NRC's budget is paid not by taxpayers but by the plants' owners. These plant owners lobbied Congress to slash the NRC's budget. Congress listened

and slashed. In 1987, the NRC had 850 regional and 790 headquarters staff members. Ten years later, chronic budget cuts had reduced the NRC to 679 regional and 651 headquarters staff members.[57] During a decade that began with 101 licensed nuclear power plants and ended with 109 plants, the NRC lost 20 percent of its safety inspectors.[58]

The US Congress must provide the Nuclear Regulatory Commission with the budget and resources necessary to implement the recommended safety steps.

This course of action was first advocated by Henry Kendall 25 years ago:

> Safety in the nuclear program must stem from a full understanding of potential mishaps and from the greatest diligence in applying that knowledge to design, construction, operation, maintenance and safeguarding of nuclear materials and facilities. With such care it might prove possible to protect against damaging accidents, arising from error and irresponsibility, equipment malfunctions, acts of God, and acts of intentional ill-will. Public acceptance of nuclear power depends not only on meeting the above requirements but also, in an important addition, on insuring that public concerns are abated by forthright disclosure of all safety issues together with convincing evidence of their full resolution.[59]

The old adage of "better late than never" certainly applies in this case.

57. NRC Office of Nuclear Reactor Regulation, "Regulatory Trends," Washington, D.C., April 1997.

58. Sadanandan V. Pullani, "Design Errors in Nuclear Power Plants."

59. Henry W. Kendall, "Public Safety and Nuclear Power," testimony before the US House Committee on Interior and Insular Affairs Subcommittee on Energy and the Environment, April 29, 1975. Available from the Union of Concerned Scientists, Cambridge, Mass.