

EDO

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Oct 13, 2000 12:18

PAPER NUMBER: LTR-00-0630 **LOGGING DATE:** 10/13/2000
ACTION OFFICE: EDO ✓

AUTHOR: CHRM Dana Powers
AFFILIATION: ACRS
ADDRESSEE: CHRM Richard Meserve
SUBJECT: Concerns Union of Concerned Scientists Report, "Nuclear Plant Risk Studies: Failing the Grade"

ACTION: Appropriate
DISTRIBUTION: RF

LETTER DATE: 10/11/2000
ACKNOWLEDGED: No
SPECIAL HANDLING:

NOTES:
FILE LOCATION: ADAMS

DATE DUE: **DATE SIGNED:**



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

October 11, 2000

The Honorable Richard A. Meserve
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Dear Chairman Meserve:

SUBJECT: UNION OF CONCERNED SCIENTISTS REPORT, "NUCLEAR PLANT RISK STUDIES: FAILING THE GRADE"

During the 475th and 476th meetings of the Advisory Committee on Reactor Safeguards, August 30 - September 1 and October 5-7, 2000, we met with a representative of the Union of Concerned Scientists (UCS) concerning the report entitled, "Nuclear Plant Risk Studies: Failing the Grade," issued in August 2000 [Ref. 1]. We reviewed this report for two reasons. First, the UCS report asserts that NRC decision making is increasing risk for the American people. Second, the report criticizes a major current initiative of the agency, namely, risk-informing the regulations. In support of the Commission's objective of building and maintaining public trust and confidence in regulatory decisions [Ref. 2], we offer the following comments regarding the UCS report.

Conclusions

1. The UCS report's assertion that "the risk assessments are seriously flawed and their results are being used inappropriately to increase – not reduce – the threat to the American public" is not valid.
2. The UCS report's claim that consequences of potential reactor accidents are not evaluated is not valid. Many probabilistic risk assessments (PRAs) calculate consequences, and the NRC has sponsored PRAs that have resulted in extremely detailed assessments of consequences and their associated uncertainties.
3. The UCS description of PRA is misleading.
4. The UCS report's list of "unrealistic assumptions" is not accurate. The report exaggerates their significance and ignores the agency's ongoing efforts to assess the validity of the data used in PRAs.
5. The report correctly identifies the need for PRA quality standards, but fails to mention the significant efforts under way to develop such standards.

6. Disparate results from “sister” plants are interpreted in the report as reflecting inadequacies in PRAs, but often, in fact, reflect differences in the design of the plant and in operating practices. The sources of these differences are investigated by the NRC staff when these PRAs are used in decision making.
7. The statement that “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” is unrealistic. No risk issue is ever managed by taking “all possible measures” to prevent and mitigate risk.
8. We disagree with the recommendation that the use of risk information should be disallowed until the methodology includes the improvements recommended by the UCS report. It would be a disservice to the nation if the agency ignored the benefits provided by the continued use of this technology.
9. The author of the UCS report was forced to rely on summary results derived from Individual Plant Examination (IPE) submittals without having access to the supporting PRAs. The NRC needs to facilitate public access to PRAs and risk information used in regulatory decisions.

Background

We briefly reviewed the history of the evolution of reactor safety philosophy to allow a better understanding of the impact that PRA has had on reactor safety assessments.

In the early days of nuclear power development (in the 1950s and 1960s), both the industry and the regulators recognized that large uncertainties existed in the assessment of the consequences of potential reactor accidents. A nuclear safety philosophy to both prevent and mitigate the consequences of these potential accidents evolved, but the resulting degree of safety could only be determined by subjective judgment. The cornerstones of this safety philosophy were defense in depth and safety margins.

Defense in depth is an element of the NRC’s safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility [Ref. 3]. Safety margins, i.e., the differences between the failure and the operating points, were purposely made large in order to accommodate a range of uncertainties.

The first major reactor PRA, the Reactor Safety Study, was published in 1975 [Ref. 4]. Subsequently, a number of important developments occurred. Major research programs were established to advance PRA methodology. Additional PRAs were completed both in the United States and internationally, which added greatly to the understanding of the potential risks of nuclear power systems and the maturity of the methodology. These PRA developments have changed the views on how to manage reactor safety in several fundamental ways:

1. Plants can be analyzed as integrated systems through the systematic development of accident sequences. The fundamental questions: "What can go wrong?", "How likely is it?", and "What are the consequences?" [Ref. 3] can be addressed. Unlike conventional analyses that are based on a single failure, these sequences consider multiple failures, including hardware failures and human errors, as well as physical phenomena, and any other factors that are thought to affect the progression of the accident. This approach permits a more in-depth analysis of plant behavior.
2. The analysis of facilities as integrated systems has identified a number of important safety improvements. Examples are the requirement to automate the initiation of the auxiliary feedwater systems, and, in part, the rules to address accident sequences initiated by anticipated transients without scram and station blackout.
3. Thousands of accident sequences are considered in a PRA in contrast to the relatively small number of design-basis accidents considered in conventional analyses. Even so, completeness remains an issue: are there accident sequences that have not been considered? The broad application of PRA by diverse practitioners has made it unlikely that any major contributors to risk have not been identified. Experience shows that the systematic search for accident sequences produces a far more complete picture of the way failures can occur in complex systems.
4. The probabilities of accident sequences can be quantified. This allows the estimation of risk metrics such as the frequency of severe damage to the reactor core, the frequency of release of large amounts of radioactivity, and the probability of death of an individual living near the plant. Accident sequences can be ranked according to their contribution to risk.
5. Although thousands of accident sequences are considered in a PRA, it has been found that the risk is dominated by relatively few sequences. The identification of dominant sequences and risk-significant events provides valuable insight. By focusing resources on these, risk can be more effectively managed. An example is the significant decline in the rate of common-cause failures over the years [Ref. 5].

In over two decades of development following the Reactor Safety Study, PRA reached a level of maturity that allows it to be used to identify unnecessary regulatory burden, as well as additional safety improvements. It is unfortunate that the two uses of PRA (to impose burden, when necessary, and to remove it, when unnecessary) have been separated by time, because this may create the false impression that burden reduction is the primary use of risk information.

The Commission issued the PRA Policy Statement in 1995 [Ref. 6] directing the staff to use PRA insights in all regulatory matters to the extent supported by the state of the art. Following this, Regulatory Guide 1.174 [Ref. 7] was issued establishing a framework for using PRA in risk-informed decisions on plant-specific changes to the licensing basis. Regulatory Guide 1.174 and the associated Standard Review Plan Chapter 19 [Ref. 8] enabled licensees to include risk information in the justification of license changes.

Regulatory Guide 1.174 proposes a "risk-informed" approach in which PRA insights (including quantitative results) are one set of inputs to an "integrated decision-making process." This

process must also consider traditional engineering safety analyses, defense in depth, and maintenance of adequate safety margins. Performance after such changes in the licensing basis must be monitored to detect unanticipated consequences. Regulatory Guide 1.174 also recognizes that there are uncertainties in PRAs and provides guidance for licensees to assess how these might affect the decision-making process.

Discussion of the UCS Report

The UCS report overstates the reliance of the Regulatory Guide 1.174 decision-making process on quantitative PRA results (the verb “rely” appears in numerous places in the UCS report). It gives passing mention to “risk-informed regulation” (page 22), but does not elaborate on what it is. The inclusion of additional information in the decision-making process and of the requirement to monitor performance after changes are made are not discussed.

The UCS report claims that PRAs are not full risk assessments because potential accident consequences are not evaluated. This is not true. Many PRAs calculate these consequences, e.g., the population dose and the number of prompt and latent cancer fatalities. NUREG-1150 [Ref. 9] involved very detailed assessments of the consequences of nuclear accidents and the associated uncertainties. It showed that the consequences were very site-specific and subject to large uncertainty. For these reasons, it is appropriate to introduce the core damage frequency (CDF) and the large early release frequency (LERF) as surrogate metrics appropriate for decision making regarding most plant modifications. CDF and LERF reflect plant design and operation. Core damage itself is an undesirable event and is, in fact, necessary for serious consequences to occur. Thus, preventing core damage is both wise and an appropriate application of an effective defense-in-depth philosophy. The relationship of LERF to prompt fatalities has been studied and is well understood [Ref. 10]. The numerical goal for LERF used in Regulatory Guide 1.174 has been shown to be consistent with the NRC safety goal on prompt fatalities. While we believe that CDF and LERF are useful metrics for regulatory applications, we hope that in the future it will be possible to have complete Level 3 PRAs for every plant so that complete risk profiles will be available [Ref. 11].

The UCS report provides an unsatisfactory description of PRA. The “fault” trees referred to in the report are normally called “event” trees. The fact that it is the *conditional* probabilities of the branches that are multiplied together to give the probability of an accident sequence is not mentioned. The fact that these conditional probabilities are produced from detailed fault trees that search for potential system failure modes is also not mentioned. A critical assessment of a technology should have a better discussion of its basic elements. In addition, one would expect that a report concerned with the potential uncertainties in PRA results would reference studies like NUREG-1150, which contains very detailed and comprehensive discussion of potential uncertainties and how they affect PRA results. The report’s description fails to reflect the depth of analysis that goes into constructing a PRA.

It is very misleading to list the number of regulatory violations (Table 1, page 7) and the number of design problems (Table 2, page 8) in each year without providing any evaluation of their impact on safety. The NRC regularly evaluates the safety significance of violations and design deficiencies that have been identified. A recent study of design basis violations showed that in 1990 about 8% had some safety significance, i.e., could potentially result in a change in the CDF

on the order of several events per million reactor years. In 1998, only about 1% had safety significance [Ref. 12].

Although PRAs generally do not explicitly include aging, the critical issue is whether there is any evidence that the failure rates assumed in the PRAs are unrealistic. For passive components like piping, steam generator tubes, and valve bodies that are not subject to periodic testing, extensive work has been done to characterize the degradation that occurs due to fatigue, general corrosion, stress corrosion cracking, thermal aging, and erosion-corrosion. When necessary, additional inspections are performed as part of reactor aging management programs. Both analysis and experience demonstrate that these aging management programs are succeeding in maintaining values of failure rates and failure probabilities consistent with those assumed in the PRAs.

PRAs do not assume that reactor pressure vessels (RPVs) never fail as claimed in the UCS report. Conservative estimates show that as-fabricated pressure vessels have very low probabilities of failure. Because the probability is so low, sequences involving RPV failure (the "R sequences") make negligible contribution to the total CDF. Irradiation does embrittle the RPV. This embrittlement is well understood and is carefully monitored. Although the probability of vessel failure does increase with time, conservative regulations ensure that the frequency of RPV failure remains well below five failures per million reactor-years. Thus, vessel failure still makes a negligible contribution to the total CDF.

The claim that PRAs assume that "plant workers will not make serious mistakes" is false. In fact, many experts believe that PRAs do not give operators the credit they deserve. As contrasted to conventional analyses that do not consider human error, it was PRA technology that focused attention on the significance of human error. Some IPEs made very optimistic assumptions about human error probabilities, but NRC review identified those immediately. Human error analysis is still one of the larger sources of uncertainty in PRA results, and the PRA community is actively pursuing better models to describe human performance. The NRC has been a major supporter of such research efforts.

The UCS report fails to mention the agency's ongoing efforts to assess the validity of the data used in PRAs. Work sponsored by the former Office for Analysis and Evaluation of Operational Data and the Office of Nuclear Regulatory Research compared actual plant performance with IPE estimates. The conclusion has been that IPE estimates are sometimes higher and sometimes lower than the estimates based on experience. The NRC staff has investigated the reasons for these differences. It is important to note that the significance of such differences has to be evaluated in the context of the PRA accident sequences. The NRC is using the data-based estimates in its evaluations.

Current PRAs are frequently limited in scope, i.e., they only analyze the behavior of the plants for full-power operation; they do not treat the effects of some initiators, such as fire and those at shutdown operations, as completely as others. In addition, other potential accidents not involving the core, such as those involving spent-fuel pools, should also be assessed, using PRA techniques. We believe that the development and expansion of PRA technology is needed, but this should not inhibit the use of PRA for problems within the scope of the currently available PRAs. Most practitioners know that one does not always need a "perfect" PRA to gain important insights regarding plant safety.

We agree that standards establishing minimum requirements for PRA quality are necessary to reduce the staff effort required to assess the quality of PRAs used for risk-informed decision making. We are surprised that the UCS report does not mention the ongoing significant efforts by the American Society of Mechanical Engineers, the American Nuclear Society, the National Fire Protection Association, and the NRC to develop such standards. Industry is also undertaking programs to assess the quality of existing PRAs.

The report concludes that the differences in PRA results between “sister” plants raise questions about the quality of PRAs. Sister plants are not necessarily identical. For instance, St. Lucie Units 1 and 2 are sister plants that have significant differences in their cores. Unit 1 has 14 x 14 fuel rod assemblies whereas Unit 2 has 16 x 16 fuel rod assemblies. This resulted in many more control rods in Unit 2 and in associated changes in the configuration and drive systems. Sister plants also tend to have differences on the secondary side either because they were built by different architect engineering firms or because the owners chose different configurations for the supporting systems. These differences in sister plants should and do have an impact on the PRA results. These results can also be affected by differences in emergency and abnormal operating procedures, management processes and practices, and control room layout. Of course, the team of analysts performing the PRA and the approach they use also affect the results. Similar issues were raised and investigated when the NRC staff reviewed the IPEs [Ref. 14]. We anticipate that having a standard for PRA quality will reduce the current sensitivity of PRA results to the team doing the analysis.

Are there deficient PRAs out there? Yes. It is very doubtful, however, that they will be used in risk-informed regulatory decisions. The greater the reliance on risk information in regulatory decision making, the greater the scrutiny of the PRA. PRA quality is evaluated in the context of the decision the PRA supports, as it should be.

The UCS report argues that “it is not possible to 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.” No society, including our own, takes all “possible” measures to prevent and mitigate accidents. Societies do what they deem to be reasonable even when the relevant probabilities and consequences of accidents are not known quantitatively. To demand that these quantities be known “accurately” is meaningless as a general statement. Risk management, by its very nature, deals with uncertainty regardless of its magnitude.

The UCS report relies on summary results derived from IPE submittals by licensees. These IPE submittals are now substantially out of date. They did not have the qualification and scrutiny expected to be currently required for any risk assessment information that is submitted in support of a risk-informed request from a licensee. The author of the UCS report had to rely on the outdated IPE results because the updated PRAs are not publicly available. This raises the question of how to best provide the public with ready access to detailed risk assessments that will be used to support licensee requests. Without ready access to these risk analyses, the public may not have confidence in regulatory decisions that use risk information. This situation should be rectified.

We disagree with the UCS report’s recommendation that risk information should not be used until all of the requirements listed in the report are met. Current PRAs provide the best available understanding of the potential risks. There are definite benefits to society from the use of risk

information in the regulation of nuclear reactors, and it would be a disservice to the nation if the agency ignored the valuable insights that this technology provides.

Sincerely,



Dana A. Powers
Chairman

References:

1. Union of Concerned Scientists, "Nuclear Plant Risk Studies: Failing the Grade," David Lochbaum, August 2000.
2. U.S. Nuclear Regulatory Commission, NUREG-1614, Vol. 2, Parts 1 and 2, FY2000-2005 NRC Strategic Plan, September 2000.
3. Memorandum dated February 24, 1999, from Annette Vietti-Cook, Secretary, NRC, to William D. Travers, Executive Director for Operations, NRC, Subject: Staff Requirements Memorandum - SECY-99-144 - White Paper on Risk-Informed and Performance-Based Regulation.
4. U.S. Nuclear Regulatory Commission, NUREG-74/014, "Reactor Safety Study, An Assessment of Accident Risks in the U.S. Nuclear Power Plants, WASH-1400," October 1975.
5. Memorandum dated July 30, 1999, from C.E. Rossi, Office of Nuclear Regulatory Research, NRC, to John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards, Subject: Proposed Resolution of Generic Safety Issue 145, "Actions to Reduce Common Cause Failures."
6. U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," August 16, 1995.
7. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
8. U.S. Nuclear Regulatory Commission, NUREG-0800, Standard Review Plan Chapter 19.0, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," July 1998.
9. U. S. Nuclear Regulatory Commission, NUREG-1150, Volume 3, "Reactor Risk Reference Document," February 1987.
10. Report dated April 11, 1997, from R. L. Seale, Chairman, Advisory Committee on Reactor Safeguards, to Shirley Ann Jackson, Chairman, NRC, Subject: Risk-Based Regulatory Acceptance Criteria for Plant-Specific Application of Safety Goals.
11. ACRS Report dated November 18, 1996, from T. S. Kress, Chairman, ACRS, to Shirley Ann Jackson, Chairman, NRC, Subject: Plant-Specific Application of Safety Goals.
12. U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Draft Report, "Causes and Significance of Design Basis Issues at U. S. Nuclear Power Plants," May 2000.
13. U. S. Nuclear Regulatory Commission, NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995," February 1999.
14. U. S. Nuclear Regulatory Commission, NUREG/CR-1560, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," December 1997.