CONF-840813--7



# An Evaluation of Reliability Assurance Approaches to Operational Nuclear Safety

by

C. J. Mueller and W. A. Bezella*

CONF-840813--7

DE84 009210

This report discusses the results of research to evaluate existing and/or recommended safety/reliability assurance activities among nuclear and other high technology industries for potential nuclear industry implementation. Since the Three Mile Island (TMI) accident, there has been increased interest in the use of reliability programs (RP) to assure the performance of nuclear safety systems throughout the plant's lifetime [1]. Recently, several Nuclear Regulatory Commission (NRC) task forces or safety issue review groups have recommended RPs for assuring the continuing safety of nuclear reactor plants. The NRC rulemaking action on anticipated transients without scram (ATWS) [2] and the NRC staff investigation of the control rod insertion failures at Salem [3] have both called for implementation of a voluntary RP by licensees to ensure the reliability of their scram systems. In connection with the Indian Point Hearings, the NRC staff recommended the integration of risk and reliability methods into the operation of Indian Point [4].



Shortly following TMI, the Department of Energy (DOE) and Electrical Power Research Institute (EPRI) sponsored studies [5-7] to determine the transfer potential of safety/reliability assurance approaches used in aerospace and commercial aircraft programs. More recently, NRC-sponsored studies [8,9] identified activities practiced in these and military programs that could be used in the nuclear industry. Studies to date have made only

*This work was performed under the auspices of the U. S. Nuclear Regulatory Commission.



ps

rather broad generalizations on the benefits or costs of such programs or their activities. No study has defined and then actually integrated a Reliability Program with existing utility operations programs for potential industry-wide implementation.

To derive a reasonable structure for an integrable Reliability Program and identify its key activities, the NRC's Division of Risk Analysis in the Office of Research contracted the Reactor Analysis and Safety Division of Argonne National Laboratory (ANL) in collaboration with the Charles Stark Draper Laboratories (CSDL). Early efforts in this research reviewed other industries and safety/reliability approaches; investigated current nuclear regulations and practices vis-a-vis a safety/reliability integration approach; and evaluated current risk-important issues [10-13] to determine safety/reliability needs. Recent work has coalesced this information into a recommended RP structure with preliminary definition of activities. A summary of investigations to date and associated results is as follows:

The first major task surveyed specific safety-critical programs under NASA and military direction, assessed related Federal Aviation Administration (FAA) practices, and reviewed the existing literature for transferability of useful practices. Fundamental differences in the way space and military programs are developed, funded, and regulated made transferability conclusions tenuous. However, it was concluded that commercial airline/FAA practices have attractive features from which the nuclear industry could benefit. These include the use of industry representatives who monitor and approve various production and manufacturing phases for the FAA; maintenance issues such as certification of personnel, FAA/industry interactions, failure experience feedback, and reliability-centered-maintenance; and the anonymous reporting of the "Aviation Safety Reporting System". Some of these relate directly to RP

integration within an individual plant; others imply a new approach to regulatory/industry interfacing across the industry.

The second major task involved the benchmarking and evaluating of the existing nuclear regulations and practices relevant to safety/reliability integration for comparison with other industry programs as cited above. It was concluded that the current body of NRC rules, requirements and guidance allows more freedom in accomplishing reliability and quality assurance than other high tech regulations. On the other hand, the Technical Specifications on operating reactors impose overly limiting requirements on licensees relative to say, the maintenance specifications imposed on commercial airlines (which may be relaxed if equipment performance justifies it). Nuclear regulations have the framework in which to integrate, not add, a reliability performance-based regulatory program that could both reduce risk and relieve licensees of overly restrictive operating practices.

The third major task involved reviewing current risk-dominant issues to identify safety/reliability integration practices to address these issues. Here an in-depth review was made of existing analyses generated for the Interim Reliability Evaluation Program (IREP) [14] and the Severe Accident Sequence Analysis (SASA) program [15,16] for the Browns Ferry systems important to risk. WASH-1400 [17] assumptions were reviewed for comparison. Plant specific information such as emergency operating instructions was reviewed. Licensee Event Reports (LERs) for these systems were analyzed to identify the dominant causes of failure indicated by operating experience. The core melt probability was used as a quantitative measure of safety. The work in this task confirmed, not surprisingly except for degree, the dominance of dependent (common cause) failures on risk-important sequences involving complex nuclear systems and highlighted the importance of the operator(s) being able to recover safety functions during an accident.

The fourth and ongoing major task of this research has been to distill the results of the above and aforementioned related work to develop a viable structure for an RP that could be integrated with existing operations and recommend specific RP activities. It was concluded that the elements that should constitute a Reliability Program would include a safety/reliability assessment program; a failure reporting, evaluation, and corrective action program; and dedicated tasks that integrate these programs with the day-to-day operating, surveillance, and maintenance of the plant with emphasis on those systems/activities/requirements having an impact on risk. Value/impact analysis using the guidelines of Ref. 18 is being used to screen the individual activities within each program element to define the scope of each of these elements. This analysis and the development of a plausible prototype for the interfaces of a Reliability Program with a licensee's design, operations, maintenance, and QA programs is currently under study at ANL.

References

1. U. S. Nuclear Regulatory Commission, "NRC Action Plan Developed as a Result of the TMI-2 Accident," NUREG-0660, August 1980.

2. "ATWS Rule: Statement of Considerations," SECY-83-293, July 19, 1983.

3. U. S. Nuclear Regulatory Commission, "Generic Implication of ATWS Events at the Salem Nuclear Power Plant," NUREG-1000
--Vol. 1, "Generic Implicatins," April 1983.
--Vol. 2, "Licensee and Staff Actions," August 1983.

4. "Atomic Safety and Licensing Board Recommendations to the Commission in the Matter of Indian Point Units 2 and 3," ASLBP 81-466-03-SP, pp. 141 and 432, October 24, 1983.

5. International Energy Associates Limited, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations," DOE/TIC-11143, April 1980.

6. Pickering Research Corporation, "Space and Missile Reliability and Safety Programs," NSAC-31, February 1981.

7. Pickering Research Corporation, "Application of Aerospace Failure-Reporting Systems to Power Plants," NSAC-4, June 1980.

8. H. A. Lauffenburger et al, "NRC Reliability Program Plan Task 2: Recommendations," RAC-TR-82-E01, December 1982.

9. "Phase I Final Report on Developing a Guide to Perform a System Assurance Analysis of Pressurized Water Reactor Facilities," NASA/KSC DL-NED, June 1, 1983.

10. S. A. Halverson et al, "Benchmark Description of Current Requirements and Practices in Nuclear Safety and Reliability Assurance," April 1983, ANL unpublished report.

11. C. Tzanos and W. Bezella, "Risk-Related Reliability Assurance Requirements for BWR Safety Important Systems with Emphasis on Residual Heat Removal Systems," April 1983, ANL unpublished report.

12. "NRC Reliability Assurance Study, Interim Summary," March 31, 1983, Charles Stark Draper Laboratory, unpublished report.

13. "Reliability Assurance Program (RAP) Research Support Program Report-Task 1: FAA Reliability Approaches, June 1983, Reliability Technology Associates, unpublished report.

14. S. E. Mays, et al., "Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant," NUREG/CR-2802, EGG-2199 (July 1982).

15. D. H. Cook, et al., "Station Blackout at Browns Ferry Unit One-Accident Sequence Analysis," NUREG/CR-2182 (November 1981).

16. D. H. Cook, et al., "Loss of DHR Sequences at Browns Ferry Unit One-Accident Sequence Analysis," NUREG/CR-2973, Preliminary Draft.

17. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/104) (October 1975).

18. U. S. Nuclear Regulatory Commission, "Regulatory Analysis Guidelines of the U. S. Nuclear Regulatory Commission, NUREG/BR-0058, January 1983.

## DISCLAIMER