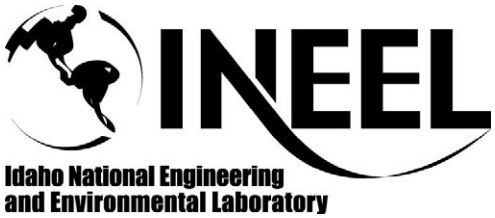

INEEL/CON-04-01551
PREPRINT

Advanced Test Reactor Safety Basis Upgrade Lessons Learned Relative to Design Basis Verification and Safety Basis Management

Gregg L. Sharp
Richard T. McCracken

May 1 – 4, 2004

EFCOG/SAWG 2004 Workshop

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author.
This document was prepared as a account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the U.S. Government or the sponsoring agency.

Advanced Test Reactor Safety Basis Upgrade Lessons Learned Relative to Design Basis Verification and Safety Basis Management

Gregg L. Sharp
Richard T. McCracken
Bechtel BWXT Idaho, LLC
Idaho National Engineering and Environmental Laboratory
P.O. Box 1625, Mail Stop 7136
Idaho Falls, ID 83415
(208) 533-4646
shargl@inel.gov

Introduction

The Advanced Test Reactor (ATR) is a pressurized light-water reactor with a design thermal power of 250 MW. The principal function of the ATR is to provide a high neutron flux for testing reactor fuels and other materials. The reactor also provides other irradiation services such as radioisotope production. The ATR and its support facilities are located at the Test Reactor Area of the Idaho National Engineering and Environmental Laboratory (INEEL).

An audit conducted by the Department of Energy's Office of Independent Oversight and Performance Assurance (DOE OA) raised concerns that design conditions at the ATR were not adequately analyzed in the safety analysis and that legacy design basis management practices had the potential to further impact safe operation of the facility.[1] The concerns identified by the audit team, and issues raised during additional reviews performed by ATR safety analysts, were evaluated through the unreviewed safety question process resulting in shutdown of the ATR for more than three months while these concerns were resolved.

Past management of the ATR safety basis, relative to facility design basis management and change control, led to concerns that discrepancies in the safety basis may have developed. Although not required by DOE orders or regulations, not performing design basis verification in conjunction with development of the 10 CFR 830 Subpart B upgraded safety basis allowed these potential weaknesses to be carried forward. Configuration management and a clear definition of the existing facility design basis have a direct relation to developing and maintaining a high quality safety basis which properly identifies and mitigates all hazards and postulated accident conditions. These relations and the impact of past safety basis management practices have been reviewed in order to identify lessons learned from the safety basis upgrade process and appropriate actions to resolve possible concerns with respect to the current ATR safety basis. The need for a design basis reconstitution program for the ATR has been identified along with the use of sound configuration management principles in order to support safe and efficient facility operation.

Department of Energy Audit Summary

The Department of Energy's Office of Independent Oversight and Performance Assurance (DOE OA) conducted an audit in August 2003 of the environmental, safety, and health management at the INEEL.[1] The audit included an in-depth review of the ATR Emergency Firewater Injection System and the Firewater Supply System. Concerns identified by the DOE OA audit team and issues raised during additional evaluations performed by ATR safety analysts resulted in multiple positive unreviewed safety question determinations and shutdown of the ATR while the specific concerns identified were resolved. The issues included:

- Potential emergency firewater injection system time delay increase,
- Firewater supply system modeling issues,
- Potential deficiencies identified during system interaction walkdowns, and
- Potentially inadequate component supports identified during seismic walkdowns.

The DOE OA team acknowledged the presence of a number of positive aspects with respect to current management of the facility. For example, the ATR staff was credited with being knowledgeable of key plant design specifications, with being highly motivated, and showing ownership of responsibilities. However, the audit team reported that the ATR had "several design deficiencies that were not adequately analyzed in the safety analysis" and that "weaknesses in configuration management, surveillance testing, and maintenance have the potential to further reduce the margin of safety." The audit team recognized that resource allocations in past years (e.g., not previously funding a design reconstitution) may have contributed to these conditions and that this possibility would be reexamined. The team concluded that the "identified design analysis weaknesses warrant a detailed evaluation of the specific concerns and a management review to determine why these concerns were not previously identified, including the underlying factors that may reduce the effectiveness of engineering evaluations and safety analyses."

The specific deficiencies identified by the audit team and ATR safety analysts were addressed, and the ATR resumed operation in late November 2003.

Advanced Test Reactor Safety Basis Evolution

The DOE OA team raised questions with respect to the ATR safety basis upgrade in that the requirements and scope may have allowed legacy weaknesses in the safety basis to be carried forward. The original ATR safety basis was documented in a safety analysis report (SAR) dated April 1965.[2] The 1965 SAR was not maintained beyond the first few years. The ATR Plant Protection System and Technical Specifications Design Basis Report[3] (DBR) was later prepared to support design of an upgraded plant protection system. The DBR contained accident analyses that supported the performance requirements (setpoints and response times) for the plant protection system, which includes the reactor shutdown system and engineered safety features. The DBR was maintained as a configuration controlled document, with periodic updates, and served as the facility accident analyses from 1976 until the Upgraded Final Safety Analysis Report (UFSAR) was completed and implemented.[4]

The upgraded safety basis for the ATR was prepared in response to DOE Orders, and now regulations, for upgrading and maintaining the safety basis of a DOE nuclear facility. The UFSAR was prepared following the format and content guidance of Nuclear Regulatory Commission (NRC) Regulatory Guide 1.70.[5] The upgraded safety basis was approved by DOE in 1996, and implemented in 1998.[4] The selection of Regulatory Guide 1.70 proved to be prudent since this document was subsequently identified as the safe harbor standard for a DOE reactor in Appendix A to 10 CFR 830 Subpart B. The ATR UFSAR was later approved by DOE under 10 CFR 830 Subpart B in November 2001. The UFSAR has been maintained via the annual update process as required by current DOE regulations.

DOE requirements and guidance did not require that facility design basis verification be performed as part of developing the upgraded safety basis. That is, there was no specific requirement to verify or reconstitute the design basis of a reactor facility within 10 CFR 830 Subpart B or through application of Regulatory Guide 1.70 as the safe harbor standard. There also was no such requirement imposed previously through DOE Order 5480.23.[6]

The initial ATR safety basis upgrade project scope included review of the facility design basis and performance of the structures, systems, and components. However, limited funding available for the upgrade and the apparent lack of a clear requirement resulted in the design basis reconstitution scope being cut from the project. Note DOE Standard 1073-93[7,] recently updated as DOE Standard 1073-2003[8], provided guidance for performing design basis reconstitution; however, it did not represent a requirement to perform such an activity. DOE Order 420.1A[9], which currently requires documents that define the design basis and supporting documents be compiled and kept current, was not issued until well after implementation of the UFSAR.

Safety Basis and Design Basis Management

DOE Order 420.1A requires that documents that define a system's design basis and supporting design information documents be complied and kept current using a formal change control/work control program. If the design basis is not clearly defined, the Order requires identification of system requirements and performance criteria essential to performance of the system's safety function, the basis for the requirements, and how the current system configuration satisfies the requirements and criteria. This is necessary to support various plant activities, including design control and configuration management. Design codes and standards have evolved significantly over the 40-year life of the ATR. Efforts to demonstrate facility safety by comparison to modern design codes and standards and the lack of a definitive back-fit policy applicable within the DOE complex, have resulted in a piecemeal application of new codes and standards. This piecemeal application of updated codes and standards, combined with the long operating history, has resulted in a patchwork of supporting design information documentation that is at best confusing. Hence, the ATR lacks a clearly defined and controlled design basis and supporting design information baseline and is not in department order compliance.[4]

As concluded by the DOE OA team, the lack of a clear baseline has led to potential weaknesses in the facility safety basis. Therefore, a design basis reconstitution program is necessary that will reestablish the facility design basis and supporting design information documentation. In addition to reestablishing the baseline design basis documentation important to the safety

function of structures and systems, the functionality of the safety structures and systems needs to be defined and validated.

Design Basis Reconstitution Program Summary

Reconstitution of the design basis will be accomplished through the following elements of the ATR design basis reconstitution program.[4]

Identification of Design Basis Requirements: This element involves identification of system requirements and performance criteria essential to the system's or structure's performance of its safety function based on the UFSAR, Technical Safety Requirements, and supporting technical documentation.

Configuration Validation: This element involves walkdowns of the structures and systems to compare the as-built facility to the design basis and supporting design documentation. Any discrepancy identified during this phase that indicates the system or structure configuration is not consistent with the safety basis will be evaluated using the unreviewed safety question process.

Functionality Validation: This element involves defining the system functional requirements that are essential to safety based on the UFSAR, Technical Safety Requirements, and related technical documentation. The design basis and supporting design information will be assessed to determine that the defined functionality is supported by surveillance tests, system operational tests, manufacturer specifications, etc.

Populate the Configuration Management System: Design basis documents and supporting design information identified by the requirement identification element will be entered into a configuration management database. Missing information will be identified and tracked for future action.

ATR UFSAR Validation: This element will review the UFSAR for compliance with regulatory requirements and requirements from departmental orders. The UFSAR analyses will be reviewed for verification that the UFSAR addresses all design basis accidents, the analyzed accident sequences are complete and appropriate, and certified computer codes have been used in the accident analysis.

Corrective Action Planning: This element of the program involves planning corrective actions to mitigate weaknesses identified during the design basis reconstitution program. A resolution plan will be developed for identified items.

The ATR design basis reconstitution plan is based on DOE guidance plus experience and guidance from similar programs conducted at commercial nuclear power plants. Note that most commercial nuclear power plants completed equivalent efforts without experiencing long-term facility shutdown while identified issues were resolved. The discovery of potential safety concerns through the ATR design basis reconstitution program will be addressed through the USQ process as noted above.

Elements of Successful Configuration Management

The importance of configuration management was not recognized during the early years of the nuclear industry. Designers were concerned with meeting design requirements and producing documents that could be used by construction organizations to build the facility. The knowledge of the design basis was not effectively transferred with the documents and commercial utilities had neither the experience nor information to establish long-term design maintenance processes. Indicators of a growing disconnect between the design basis and the physical plant became apparent in the late 1970's and received intermittent attention through subsequent years.[10] A more recent and heavily publicized configuration management event occurred in 1996 and culminated with shutdown of the three Millstone units. This occurrence led to the NRC issuing a 10 CFR 50.54(f) letter to all license holders of nuclear reactors.

The value of the ATR design basis reconstitution program must be realized through a continuing commitment to sound configuration management. Configuration management aims to establish and maintain consistency between the facility design requirements, the technical documentation supporting facility operation (e.g., safety basis), and the facility "as-built" configuration.[11] Achieving consistency among design requirements, physical configuration, and facility documentation provides a foundation for safe and efficient operation. Six basic elements of a successful configuration management program include[11]:

Program Management: Development and implementation of a configuration management program requires prioritizing, direction, and monitoring.

Design Requirements: The design requirements (and functional requirements) associated with the facility structures, systems and components need to be established, documented, communicated and maintained.

Information Control: Facility configuration information (including document and electronic information control) related to the physical configuration and the design requirements must be identified and managed.

Change Control: Consistency among the design requirements, the physical configuration, and the facility documentation as changes are made is maintained.

Assessments: The effectiveness of the configuration management, with emphasis on the product, is evaluated.

Training: Facility personnel are made aware of the configuration management vision, concepts, and procedures such that they are able to carry out their work in a manner that supports successful configuration management.

The most important element of configuration management is change control, which goes well beyond keeping records of facility modifications.[11] Change control is essential such that all facility changes are appropriately addressed and incorporated into the safety basis, thereby maintaining a sound basis for continued facility operation. With respect to the ATR safety basis,

not maintaining the 1965 SAR and subsequently building on that original documentation resulted in weaknesses within the upgraded safety basis. The cost of lost operating time in addition to future costs of reviewing and reestablishing the design and safety basis are extensive.

ATR Safety Basis Upgrade Lessons Learned

Existing weaknesses in the ATR safety basis were unknowingly carried forward into the upgraded safety basis. Change control practices and documentation show a strong ability to record and trace modifications to the ATR. Modifications have not been captured as well in facility drawings or in the safety basis documents. The condition of the ATR safety basis has been further impacted by the evolution of codes and standards over the 40-year life of the facility and the resulting patchwork of design information. The original ATR safety analysis report and the design basis report were assumed to be a reliable source of information forming the baseline for development the upgraded safety basis. No detailed validation or walk-down of the functionality of systems and structures, as described in these documents, was performed.[4]

The decision to not perform any type of design basis verification or reconstitution in conjunction with developing the upgraded safety basis led to a more than three-month unplanned reactor shutdown at an approximate cost of three million dollars per month in lost productivity. The costs due to lost productivity are separate from the costs of performing a design basis reconstitution, and may have been avoided through a more comprehensive safety basis upgrade scope. A design basis reconstitution must now be performed under much less favorable circumstances, with greater scrutiny, and at greater direct cost than may otherwise have been required. The cost of recovering the design basis may also exceed the cost of continuous maintenance through sound configuration management.

Some concerns raised by the DOE OA team resulted directly from similar conditions experienced by commercial nuclear plants. Although ATR is very different from the design of typical power reactors, closer attention to industry events and regulatory notifications could have led to these concerns being identified and addressed in a more timely manner. The ATR design basis reconstitution effort includes development of a system/process to access, screen and review nuclear reactor and power plant operating experience in order to aid timely assessment of lessons-learned that could be important for continued safe operation of the ATR.[4]

The benefits of good configuration management are not always clear and can become the victim of internal efforts to reduce cost. This tends to drive a cyclic condition. A benefit of the NRC 10 CFR 50.54(f) letter, at least in the present, has been to solidify the importance of configuration management in the commercial nuclear power industry.[10] A commitment to continuous configuration management that ensures consistency between design requirements, physical configuration, and facility documentation is essential to maintaining a firm basis for safe and efficient operation. The ATR design basis reconstitution effort emphasizes the importance of continuous design basis management by populating a design basis database that can be a tool for long-term configuration management.

Conclusions

The impact on the facility safety basis due to not maintaining the early SAR and the patchwork approach to applying updated codes and standards which resulted in potential weaknesses in the safety basis was not recognized when preparing the upgraded safety basis. The decision to exclude the design basis verification scope from the safety basis upgrade project led to these weaknesses being carried forward into the new safety basis. Discovery of this condition, through a DOE OA audit and reviews by ATR safety analysts resulted in shutdown of the ATR for more than three months at a cost of approximately three million dollars per month in lost productivity. A design basis reconstitution program must be performed under much less favorable circumstances and likely, at greater direct cost than would have been required if performed in conjunction with the safety basis upgrade project.

Although the design of the ATR is unique, issues and lessons-learned identified within the commercial nuclear power industry can be applicable to the ATR. The ATR design basis reconstitution effort includes development of a system/process to access, screen and review nuclear reactor power plant operating experience in order to aid timely assessment of lessons-learned and assist continued safe operation of the ATR.

Sound configuration management that achieves consistency among design requirements, physical configuration, and facility documentation provides a foundation for safe and efficient facility operation. Configuration management requires steady performance in order to avoid potentially greater recovery costs.

The design basis reconstitution program is underway at ATR.

References

1. DOE OA, *Inspection of Environment, Safety, and Health Management and Emergency Management at the Idaho Operations Office and Idaho National Engineering and Environmental Laboratory*, no report number, U.S. Department of Energy Office of Independent Oversight and Performance Assurance, September 2003, Summary Report pp. 6, 9 and Volume I pp. 7, 63.

2. D. R. deBoisblanc and S. Cohen, *Safety Analysis Report Advanced Test Reactor*, Philips Petroleum Company, IDO-17021, April 1965.

3. S. A. Atkinson and G. H. Hanson, *Advanced Test Reactor Plant Protective System and Technical Specifications Design Basis Report*, EG&G Idaho, Inc., RE-E-76-048, May 1977.

4. PLN-534, “Advanced Test Reactor Design Basis Reconstitution Program Plan,” Revision 1, Idaho National Engineering and Environmental Laboratory, February 2004, pp. 1, 2, 4, 7-10.

5. NRC Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, LWR Edition," Revision 3, U.S. Nuclear Regulatory Commission, November 1978.

6. DOE O 5480.23, "Nuclear Safety Analysis Report," U.S. Department of Energy, April 1992.

7. DOE-STD-1073-93, “Guide for Operational Configuration Management Program (including adjunct Programs of Design Reconstitution and Material Condition and Aging Management),” U.S. Department of Energy, November 1993.

8. DOE-STD-1073-2003, “Configuration Management,” U.S. Department of Energy, October 2003.

9. DOE O 420.1A, “Facility Safety,” U.S. Department of Energy, May 2002, Attachment 2 pp. 18.

10. L. R. Hancock, *A Nuclear Power CM Historical Perspective*, http://www.cmbg.org/papers/cmbg-historical-perspective.htm, published date unknown, Web page visited December 18, 2003.

11. IAEA-TECDOC-1335, “Configuration Management in Nuclear Power Plants,” International Atomic Energy Agency, January 2003, pp. 3-6.