NUREG/CR-4271

Recommended Safety, Reliability, Quality Assurance and Management Aerospace Techniques With Possible Application by the DOE to the High-Level Radioactive Waste Repository Program

Prepared by W. M. Bland, Jr.

Management and Technical Consulting

Prepared for
U.S. Nuclear Regulatory
Commission

8507080205 850630
PDR NUREG
CR-4271 R PDR

NOTICE

This report was prepared as an 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 of 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.

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082, Washington, DC 20013-7982
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR-4271

Recommended Safety, Reliability, Quality Assurance and Management Aerospace Techniques With Possible Application by the DOE to the High-Level Radioactive Waste Repository Program

Manuscript Completed: March 1985
Date Published: May 1985

Prepared by
W. M. Bland, Jr.

Management and Technical Consulting
Division of GeeB's Inc.
18575 Martinique Drive
Houston, TX 77058

Prepared for
Division of Waste Management
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN D1014

This report imposes no requirements.

ABSTRACT

Aerospace SRQA and management techniques, principally those developed and used by the NASA Lyndon B. Johnson Space Center on the manned space flight programs, have been assessed for possible application by the DOE and the DOE-contractors to the high level radioactive waste repository program that results from the implementation of the NWPA of 1982. Those techniques believed to have the greatest potential for usefulness to the DOE and the DOE-contractors have been discussed in detail and are recommended to the DOE for adoption; discussion is provided for the manner in which this transfer of technology can be implemented.

Six SRQA techniques and two management techniques are recommended for adoption by the DOE; included with the management techniques is a recommendation for the DOE to include a licensing interface with the NRC in the application of the milestone reviews technique. Three other techniques are recommended for study by the DOE for possible adaptation to the DOE program.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Valuable contacts were made with a number of people in the search for information to support the work on this Task 2 document. Some of these contacts furnished information a number of times. These contacts are identifed in the following list.

Mr. T. Jefferson Adams, NASA Lyndon B. Johnson Space Center
Dr. Stuart C. Black, U.S. EPA, Las Vegas, Nevada
Dr. Douglas P. Blanchard, NASA Lyndon B. Johnson Space Center
Mr. F. Robert Cook, U.S. NRC Division of Waste Management
Ms. O. Constance Crtizos, NASA Lyndon B. Johnson Space Center
Mr. Mark S. Delligatti, U.S. NRC Division of Waste Management
Mr. D. Gene Easterly, U.S. EPA, Las Vegas, Nevada
Dr. John W. Harris, NASA Lyndon B. Johnson Space Center
Mr. Arthur N. Jarvis, U.S. EPA, Las Vegas, Nevada
Mr. Jack E. Kohanke, NASA Lyndon B. Johnson Space Center
Mr. Joseph H. Levine, NASA Lyndon B. Johnson Space Center
Mr. Paul T. Prestholt, U.S. NRC Division of Waste Management
Mr. Tilak R. Verma, U.S. NRC Division of Waste Management

RECOMMENDED SAFETY, RELIABILITY, QUALITY ASSURANCE AND MANAGEMENT AEROSPACE TECHNIQUES WITH POSSIBLE APPLICATION BY THE DOE TO THE HIGH LEVEL RADIOACTIVE WASTE REPOSITORY PROGRAM

EXECUTIVE SUMMARY

Aerospace SRQA and management techniques, principally those developed and used by the NASA Lyndon B. Johnson Space Center on the manned space flight programs, have been assessed for possible application by the DOE and the DOE-contractors to the high level radioactive waste repository program that results from the implementation of the NWPA of 1982. Those techniques believed to have the greatest potential for usefulness to the DOE and the DOE-contractors have been discussed in detail in Section III of this document. In general the discussion for each technique provides information related to the background use experience of the technique; the interfaces that it has with other techniques and important activities; related direct experience and/or recommendations related to the technique from other sources; applicable operating philosophy; the benefits that can be obtained by adopting the technique; specific recommendations; time of application of the technique; a description of the estimated ease and mode of transfer of the necessary technology; and reference documents.

In the discussions, the importance of certain management attributes to the success of the programs from which most of the experience base used for this study was obtained included the following: attitude, commitment, attention-to-detail, technical understanding/program knowledge and participation.

It was noted that the application of the recommended aerospace techniques will require some tailoring to fit the specific needs of the DOE program.

The specific recommendations developed in the Section III of this document are as follows:

1. It is recommended that the DOE adopt the system safety technique and the specialized safety analysis techniques, as described, for use in the implementation of the activities associated with the NWPA of 1982; and that consideration be given to tailoring the requirements of these techniques to fit the specific needs of the high level radioactive waste repository program sites and of the waste transportation system.

2. It is recommended that the DOE adopt the utilization of

the FMEA (Failure Mode and Effects Analysis)/CIL (Critical Items List) technique, as described, for use in the implementation of the activities associated with the NWPA of 1982; and that the degree of development of this technique as applied to the Space Shuttle program would be a reasonable level to apply to the high-level waste repository engineering program, with some tailoring of the technique to accommodate differences between the two programs. Application of this technique should also be considered for the waste transportation system.

3. It is recommended that the DOE adopt the methodology and the operating philosophy of the NASA PRACAS (Problem and Corrective Action System) technique, as described, for use throughout the DOE and the DOE-contractor efforts related to the implementation of the NWPA of 1982; and that consideration be given to applying this technique as one system, from the top, in a tailored fashion to form the bases for satisfying the reporting and assessment, management, licensing and administrative requirements.

4. It is recommended that the DOE adopt the EEE parts control technique, as described. It should be tailored to fit the specific needs of the DOE efforts associated with the implementation of the NWPA of 1982.

5. It is recommended that the DOE adopt an equipment certification technique test approach for the high level waste repository program that includes the minimum guidelines, as described; that the additional guidelines that describe the approach to the certification test activity used on the Apollo program be considered, on a one-for-one basis, for possible addition to the minimum list; and that appropriate tailoring be applied to fit this technique to the specific needs of this DOE program.

6. It is recommended that the DOE adopt a data verification technique, as described, that is based upon a multiple number and level of peer reviews that reflects the NASA/NACA experience; and that the DOE strongly consider generation of an old data verification/review process similar to that developed by the U.S. EPA for the Love Canal investigation, but modified to meet the specific needs of the DOE for verification/validation of the older data that is to be used to support significant decision points in the high level radioactive waste repository program.

7. It is recommended that the DOE adopt the management technique of milestone reviews for application to the high level waste repository program; that this technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of the milestone reviews technique is dependent upon suitable implementation of a configuration

management program and the adoption of a number of the SRQA techniques recommended to the DOE in this document.

8. It is recommended that the DOE establish an operating interface with the NRC through each of the milestone reviews established as a result of implementation of the milestone reviews technique; that the DOE and the NRC agree on what the DOE is to provide to that interface and what the NRC is to bring to that interface; and that the DOE and the NRC agree to develop this interface to enhance the licensing process and to also do what has to be done with the licensing requirements to enable this interface to be effective.

9. It is recommended that the DOE adopt the management technique of configuration management for application to the high level waste repository program; that this configuration management technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of configuration management on their program will be dependent upon suitable implementation of the milestone reviews technique as part of configuration management, the adoption of a number of the SRQA techniques recommended in this document and other supporting techniques, or their equivalent, and the full backing and involvement of top DOE management associated with this program.

10. It is further recommended that the DOE study, for possible adaptation to the high level radioactive waste program, three other aerospace techniques briefly identified in the discussion material; these other techniques are material qualification and traceability, failure modes and effects analysis as applied to processes, and reliability centered maintenance.

11. It is recommended that the DOE pay particular attention to the interfaces of the techniques that are adopted, how these interact with each other and how they will interact with the existing and planned techniques employed by the DOE and DOE-contractors; these interfaces and their interactions are key to the success of the recommended techniques.

12. It is recommended that in implementing these recommendations that the DOE consider multiple modes of communications for accomplishing the transfer of technology that include the use of presentations, lectures, workshops, pilot programs and on-the-job guidance. The modes selected for a specific technique will depend upon the complexity of the technique and the experience level of the staff that is to implement the technique.

It is noted that the intent of the above recommendations is to provide the DOE with techniques to supplement current and planned activities; there is no intent that these recommended techniques summarily replace any of the DOE current and

planned activities. It is possible that some of the recommended techniques can be adapted to current DOE activities and implemented to supplement specific DOE activity already underway or planned for future application. In other cases, the DOE may have activities similar to some of the recommended techniques; in those instances the DOE need not adopt the recommended techniques. It is urged that the DOE explore beyond any name similarities before deciding on the degree of implementation to apply to the recommended techniques. The DOE is also urged to carefully consider the total impact of not implementing a specific recommended technique. The strong interaction between the techniques, as noted in the interface discussions, may make the impact of not implementing a specific technique greater than just the loss of benefits associated with that specific technique.

RECOMMENDED SAFETY, RELIABILITY, QUALITY ASSURANCE AND MANAGEMENT AEROSPACE TECHNIQUES WITH POSSIBLE APPLICATION BY THE DOE TO THE HIGH LEVEL RADIOACTIVE WASTE REPOSITORY PROGRAM

I. INTRODUCTION

The NRC has been engaged in defining the requirements, scope and function of an internal QA (quality assurance) Plan, with emphasis also on safety and reliability, for use in the Division of Waste Management and in defining recommendations to be given to the DOE for applying additional safety, reliability, quality assurance and related management technique requirements to the DOE effort in implementing the NWPA of 1982. These recommended requirements are in addition to those quality assurance requirements imposed from Appendix B of 10 CFR 50 and Subpart G of 10 CFR 60.

It is the intent of the NRC that there be an integrated and consistent approach used in defining the Plan, which is for internal guidance, and the recommendations, which are for application by the DOE and the DOE-contractors as doers and the NRC as the regulator. The recommendations, as presented in this document, are intended to represent the most applicable experience that has resulted from the United States aerospace effort and from the applicable efforts of other federal agencies where program success has been attributed to significant contributions made by their respective safety, reliability and quality assurance programs. There will be a deliberate attempt to avoid the invention of new techniques or the introduction of new terminology.

It is anticipated that these recommendations will benefit from the interchange of ideas between the NRC and the DOE following their introduction to the DOE for review and comment. Such an interchange will result in deeper technical understanding of the benefits to be achieved by adopting the recommendations by both the NRC and the DOE; the resulting refinements in wording can be expected to lead to a mature and fully useful document. It is possible that this understanding can be further enhanced through the use of presentations, lectures, workshops, on-the-job guidance and/or pilot programs.

Some of the recommended techniques, particularly those for the system safety, failure modes and effects/critical items list, and the problem reporting and corrective action system have potential application to the transportation system to be

used to relocate the high level radioactive wastes from temporary storage sites to the repository site.

This document has been prepared for the Policy and Program Control Branch of the Division of Waste Management, U.S. NRC by Management and Technical Consulting, a Division of GeeB's, Inc., under contract NRC-02-84-007.

II. GENERAL DISCUSSION

A. Purpose and Scope

For several years there have been a number of sources that have been recommending that those involved in the commercial nuclear power generating effort consider the utilization of the favorable experiences of the aerospace and other national efforts. The thought has been that the experiences and the learning efforts of other participants in activities where safety and reliability are major concerns, as they are in the nuclear power generating effort, could be utilized to the benefit of those engaged in the nuclear effort. Some of these sources are included in references 1 through 11; no attempt has been made to make this a complete list of sources. Generally the recommendations of the referenced documents have been that some of these experiences can be used to the benefit of the nuclear power effort, though care should be taken to make sure that the application is made to fit the case of nuclear power; that is, a simple transfer of technology is not sufficient. The transfer has to be tailored to fit the application. In some cases the recommendations and/or applications of aerospace technology have been made, after a detailed survey, of a large number of techniques, as in reference 3; in other cases there have been examples cited where considerable work has been expended in assessing/applying some of the aerospace techniques, such as, configuration management in reference 4, reliability and safety assessment techniques in reference 7 and readiness reviews in reference 11.

While the transfers of technology discussed in the references have concerned themselves primarily with applications to the nuclear power generation sector, it is believed that similar considerations can be made for the transfer of this technology to the national effort that is concerned with the implementation of the Nuclear Waste Policy Act of 1982, reference 12. Again, the transferred technology has to be tailored to fit the specific needs of the new application.

Not all persons skilled in the aerospace techniques have recommended transfer of their technology into "the nuclear power business". One of these, Dr. George M. Low, famed for his efforts in directing the Apollo Spacecraft Project to its successful achievement, deferred to "...those who understand nuclear systems and their operations better than I do.", reference 13. However, it is worth noting that Dr. Low identified and described some of the differences between the Apollo effort and "the nuclear power business". It is this consultant's opinion that many of the differences identified by Dr. Low become similarities when one substitutes the high-level nuclear waste effort for "the nuclear power business". This then further reinforces the belief that there is a place for a "tailored" transfer of aerospace technology to the

DOE's effort in accomplishing the Nuclear Waste Policy Act of 1982 and that this transfer can enhance the DOE's performance in directing this effort to a successful completion and can enhance its performance across the interface with the U.S. Nuclear Regulatory Commission and its licensing responsibilities.

There have been other studies made of the potential application of aerospace methods and techniques to the nuclear power industry that have concluded that such application would not be useful. These conclusions were apparently reached after comparing the missions of nuclear power and of aerospace; not by examining the methods and techniques. Such an examination may have led to different conclusions; conclusions more consistent with the recommendations contained in this document.

Techniques recommended in this document include a number that are generally included as specialty techniques in the specific work areas of safety, reliability and quality assurance. Other techniques include some that are generally included in the body of information identified as management techniques. However, it is noted that not everyone categorizes these techniques alike; and thus the reader should not let that cause a possible block in regards to their applicability and usefulness. It is further noted that the techniques identified as management techniques are critical to the application of the other techniques and also to the success of some of the techniques that are currently being applied or that are planned to be applied by the DOE.

Techniques presented, described and recommended for application by the DOE in the SRQA area include system safety, failure modes and effect analysis/critical items list, problem reporting and corrective action system, electrical, electronic and electromechanical parts control, equipment certification, and data verification. Management techniques include milestone reviews and configuration management. Three other techniques, material qualification and traceability, failure modes and effects analysis as applied to processes, and reliability centered maintenance, are recommended for study for possible adaptation to the DOE program.

The presented techniques are recommended for application for the achievement of the technical and management objectives of the high level radioactive waste repository program; some of these techniques could also be used to provide analysis suppport to other functions, such as those in support of the "OSHA" requirements.

B. Sources of Past Experience Utilized

Information on which this document is based comes primarily from the specific experiences of this consultant in the part

of the nation's aerospace effort that was directly related to NASA manned space flight activities from the Mercury Project and into the early part of the Space Shuttle Program. This information is supplemented with the experiences of the continuing manned flight effort and the experiences of other efforts, when that experience has been successful and is pertinent to this effort. In the many possible areas of this effort, currently available documentation that can serve as a source of detailed information is referenced in the text; in many cases important specific wording is cited to help establish the discussion in the text.

C. Features of Past Experience, Knowledge and Interfaces

Features of aerospace experience and the experiences of others that can provide a significant gain in project performance and licensing gain to the DOE include detailed project involvement, detailed technical knowledge and improved flow of licensing information, as follows:

1. The government staff's deep project involvement and knowledge of the details gave it the best opportunity for early detection and correction of contractor faults and the best opportunity to provide "midcourse correction"; these skills were helpful in achieving schedule objectives and in attaining project objectives at minimum costs. Helpful assistance in attaining this involvement comes from the following activities:
    a. Intimate project involvement of government management, line design and test engineers, and SRQA engineers and inspectors from initial design through construction and into operation;
    b. Involvement of government SRQA engineers with the contractor staff as well as with the government line engineers and managers;
    c. Ability of the government and contractor SRQA staffs to provide independent assurance evaluations without diluting or interfering with the responsibilities of the government and contractor line personnel; and
    d. Continued involvement in the details of the project from the beginning by the government managers through participation in the milestone review process, in the configuration management process and in the other management systems.

2. The government staff's detailed knowledge, accumulated and maintained through intimate involvement in the project(s), also enabled the government to react accurately and quickly to technical and management problems, thus avoiding the need to "come up to speed" each time a decision was needed by a contractor or by the government.

3. The milestone review system and the configuration management system, particularly the part involving configuration control panel and/or board actions, was used

to provide the government staff with important visibility of the project(s)/program activities. This visibilty greatly enhanced the government staff's knowledge and decision making ability.

Taking advantage of these features will also enable the DOE to provide a lot of program visibility relative to the licensing requirements available to the NRC by making NRC representatives a party to the milestone reviews and the configuration management activities. Such visibility will enable the NRC to reach early technical understandings and positions relative to the program activities that are vital to licensing approval. It will also enable the NRC to raise questions for clarification in nearly real time and thus eliminate the "bring me a rock game" that can result from the currently utilized licensing process that is based so much upon a review of documents that are not maintained in a "current" condition. Additional discussion of a potential arrangement for the licensing interface is provided in Attachment A to the section on milestone reviews technique.

D. Importance of Management Effort in Past Experience

The available literature contains a lot about management techniques and the effect of management on the successful achievement of program/project objectives. While the purpose of this document is to identify certain techniques that have been successfully used to attain difficult objectives and to describe how important features of these techniques can be utilized to an advantage, some emphasis needs to be placed on an obvious, but not necessarily widely accepted, lesson learned from experience about the role of management in introducing new techniques. Experience has shown that no matter how well the benefits of these techniques are "sold", no matter that the important parts of these techniques are "bought" with the intention of prompt application, and no matter how often the management tells their staff and their contractors to apply these techniques, the benefits from these techniques are not likely to be realized unless management, from the top down, adopts the attitude that leads to the understanding, application, and participation with these techniques as though they were their own.

E. The Use of Outsiders

The use of outsiders, that is, people from outside the close network formed by an agency and its contractors in accomplishing work in a program, is often looked upon as something to be avoided. Experience in the NASA manned space flight programs and in other NASA programs has shown that the use of outsiders can be of benefit. The benefit comes from the related, parallel, and supporting experiences that these outsiders can bring to the program; experiences that can be

expressed without the pressures of prior commitments in that program and without the pressures of cost and schedule.

These outsiders may be used as consultants, as members of interagency panels, as members of ad hoc committees and as members of standing committees. They may come from industry, educational institutions, other agencies, or be individual experts. It is also possible to use them to participate as members of boards of milestone reviews where their experiences can be readily applied to current program activities.

NASA experience also included the use of outsiders as members of advisory panels, committees and boards, some of which are identified and described in reference 14. One of these, the Aerospace Safety Advisory Panel, served a particularly useful oversight role with regards to the NASA manned space flight program activities. The way that this panel operated, its level of competence and its outputs could serve as a model for similar oversight review panels that are adapted to serve the specific needs of other agencies.

F. Application

It is intended for the material contained in this document to present enough descriptive information and supporting references about selected aerospace safety, reliability, quality assurance and management techniques to convince the Department of Energy to consider applying these techniques, in a tailored way, to their work on the high level radioactive waste repository program. The level of detail of information necessary for the actual transfer of technology for the implementation of these techniques is beyond the scope of this document. It is suggested that the necessary level of detail for an efficient transfer of technology is probably beyond the scope of any document or combination of documents. It is suggested that the detailed information needed could best be transferred by making use of presentations, lectures, workshops, pilot programs and on-the-job guidance furnished by those who have had first-hand experience in setting up and in using these recommended techniques.

G. Summary

Throughout these short descriptive paragraphs and in the longer discussions of the recommended techniques that follow in Section III, there is an intent to emphasize, through words and the use of references, features of the management mode of operation developed and applied during the NASA manned space flight programs that are believed to have been strong contributors to the success of those programs and that are believed to be applicable to other activities where

safety and reliability are important concerns. Included in this management mode of operation are management attributes and a management support service.

The management attributes include attitude, commitment, attention-to-detail, technical understanding/program knowledge, and participation.

The management support service singled out for emphasis is that of documentation. Provisions were made for documentation to be prompt, accurate, complete, and understandable and for it to be distributed to all of the needed places and, where needed, to be followed up to complete open actions and commitments.

The importance of these management attributes and this management support service to program success should not be overlooked; they are worthy of separate analysis efforts to determine the roles they should play in new endeavors.

H. General Discussion References

1. JSC 08981, "Application of NASA Safety, Reliability and Quality Assurance Techniques to the Nuclear Power Industry (A Literature Survey)", NASA Lyndon B. Johnson Space Center, July 1974. (3021)

2. William M. Bland, Jr. and Dwight H. Reilly, "Quality Assurance", Reports of the Technical Assessment Task Force, Vol. IV, pages 1- 118, Staff Reports to the President's Commission on the Accident at Three Mile Island, October 1979. (7010)

3. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", U.S. Department of Energy, April 1980. (2004)

4. Thomas N. Ewing and William R. Pogue, "Configuration Management for Black Fox Station Nuclear Project, A PSO Response to TMI", Presented to the Frontiers of Power Conference, Oklahoma State University, October 13, 1980. (7013)

5. William M. Bland, Jr., "Nuclear Power Can Be Safe: Attitude is the Key", Hazard Prevention Journal, pages 17-21, November/December 1981. (9016)

6. William M. Bland, Jr., "TMI Rare Event? Lessons to be Learned", Proceedings, 1982 Annual Reliability and Maintainability Symposium. (9018)

7. Donald W. Page and William H. Rasin, "Application of NASA Kennedy Space Center System Assurance Analysis Techniques

to a Nuclear Power Plant System Design", pages 18-2.1 - 18-2.22 of New Frontiers in System Safety, Sixth International System Safety Conference, September 26-30, 1983. (7015)

8. NP-3364, "Commercial Aviation Experience of Value to the Nuclear Industry", Electric Power Research Institute, 1984. (7001)

9. William M. Bland, Jr., "Nuclear Power can be Safe, II! Attitude is the Key! Will the Key be Used?", Hazard Prevention Journal, pages 28-32, January/February 1984. (9017)

10. W. Altman, T. Ankrum, W. Brach, "Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants", NUREG-1055, U.S. Nuclear Regulatory Commission, May 1984. (1002A)

11. R.E. Conway, "Readiness Review Program", Letter from Georgia Power to U.S. NRC, October 3, 1984. (7012)

12. "Nuclear Waste Policy Act of 1982", Public Law 97-425, January 7, 1983. (4004)

13. "Statement" of George M. Low, President, Rensselaer Polytechnic Institute, before the Subcommittee on Energy Research and Production of the Committee of Science and Technology for Hearings on Nuclear Reactor Safety, May 24, 1979. (7009)

14. NHB 1700.1 (V1-A), "Basic Safety Manual", NASA, January 17, 1983. (3051)

III. SPECIFIC DISCUSSIONS

A. Background

The roots of many of the SRQA and management techniques discussed in this section originated in the early days of this nation's NASA manned space flight programs. It is possible to say that these techniques had their beginnings as a result of a combination of the attitude and experiences of the pioneering NASA management, the experiences of the aircraft and missile industries, and those of the participating armed services. Gradually the experiences from the NASA manned space flight programs began to be documented. At first, the documentation reflected a series of lectures that recounted the experiences that had been attained in the many facets of these interesting operations; from design, through manufacturing, test, flight preparation, flight and post flight analyses. One such document is reference 1; there, many of the lessons learned from the early experiences are discussed. The topics covered are very similar to those in today's safety, reliability and quality assurance requirements manuals; of course the details do differ. Similar topics from that base of experience are discussed in reference 2; however, other topics that describe some management techniques that have become identified as milestone reviews and configuration management are introduced.

Later, as time permitted, more formal documents were prepared to more rigorously describe the safety, reliability and quality assurance experiences in a form that represented requirements (provisions) that were then utilized in subsequent manned space flight programs. Examples of such documents are listed in references 3 through 6. Examples of further documented reliability and quality assurance requirements for specific manned space flight programs, such as Apollo and Apollo Applications Programs, are contained in references 7 and 8. Early application of management techniques were based on a combination of the early experiences noted above and in documentation such as reference 9, which describes the requirements and features important to successful configuration management systems.

Still later, as the manned flight programs became more sophisticated, these requirements were expanded to include safety requirements and honed to their present state, reference 10. The safety, reliability and quality assurance techniques recommended in this document stem largely from personal experiences that led to the earlier documents and the application of the contents of reference 10 and supporting documents. These supporting documents provide implementation detail and reflect the great deal of aerospace experience that has been generated by NASA and the aerospace industry.

These referenced basic and current SRQA and management technique documents reflect the experience of the government space agency and the experiences of the aircraft and missile industries and their extensive network of speciality contractors, many support service contractors, special laboratories, institutions of learning and other parts of the Federal government. It has been the results of combined teamwork; the experience is still being accumulated. It can be anticipated that with the passage of time that the more newly acquired experiences will be utilized to modify or replace the most recent documents referenced herein with those that will provide better and more effective advice and requirements.

This document utilizes the available current documents to serve as a bases for the SRQA and management techniques that can be tailored to enhance the DOE and DOE-contractor work and the NRC licensing responsibilities in the activity related to the NWPA of 1982.

Following the listing of the references for the above Background discussion are discussions of the selected safety, reliability and quality assurance techniques, each with their applicable reference listing. Following these discussions are those of the selected management techniques and their applicable reference listings.

Background References

1. William M. Bland, Jr. and Lewis R. Fisher, "Reliability Through Attention to Detail", Chapter 38, Manned Spacecraft Engineering Design and Operation, edited by Paul E. Purser, Maxime A. Faget, and Norman F. Smith, Fairchild Publications, Inc., N.Y., 1965. (7011)

2. William M. Bland, Jr. and Lt. Col. Charles A. Berry, USAF, MC, "Project Mercury Experiences", pages 29-34, Astronautics and Aerospace Engineering, February 1963. (9019)

3. NPC 200-1, "Quality Assurance Provisions for Inspection Agencies", NASA Quality Publication, April 1962.

4. NPC 200-2, "Quality Program Provisions for Space System Contractors", NASA Quality Publication, April 1962. (3033)

5. NPC 200-3, "Inspection System Provisions for Suppliers of Space Materials, Parts, Components and Services", NASA Quality Publication, April 1962.

6. NPC 250-1, "Reliability Program Provisions for Space System Contractors", NASA Reliability Publication, July 1963. (3035)

7. NHB 5300.1, "Apollo Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, October 1965.

8. NHB 5300.5, "Apollo Applications Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, May 1967. (3037)

9. NPC 500-1, "Apollo Configuration Manual", NASA Headquarters Publication, May 18, 1964.

10. NHB 5300.4(1D-2), "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program", NASA, October 1979. (3009)

B. Safety, Reliability and Quality Assurance Techniques

1. SYSTEM SAFETY

Background

Scope-This section of the Recommendations Document presents a limited description of the system safety effort developed to support the NASA manned space flight programs and some details about three of the specialized safety analysis techniques that provided much of the support to the system safety effort. These three safety analysis techniques are the hazard analysis, the fault tree analysis and the sneak analysis; they are often identified by the acronyms HA, FTA and SA or SCA, respectively. These techniques have been developed from the time of the earliest of the NASA manned space flight programs and have made use of the appropriate experiences from other efforts where safety has also been of primary concern. Detailed descriptions of system safety and these three supporting safety techniques, as implemented by the NASA manned space flight programs and other NASA activities, are included in the safety discussions in references 1-6.

Because of the significant contributions of system safety and these three safety analysis techniques to the success of the NASA programs and their believed potential application to the DOE effort in the implementation of the NWPA of 1982 in the development of high level radioactive waste repositories, they have been identified for this specific discussion. Other areas of safety work, such as other parts of system safety, occupational safety and health, industrial safety, motor vehicle, and transportation safety are not included in these discussions. However, system safety and these three safety analysis techniques should be considered for application to the transportation system(s) that are to be used for moving the high level wastes to processing sites and to repository sites.

Management Thoughts-To help set the stage for discussions of

system safety and the safety analysis techniques for possible application to areas where such emphasis of safety has not been as visible as in the NASA manned space flight programs, several parts of references 1-3 are paraphrased or quoted, as follows:

a. The Basic Safety Manual is the central agency document containing guidelines, instructions, and requirements which define the NASA Safety Program. It is intended to serve as a general framework to structure the more specific and detailed requirements for Headquarters, Program and Field Installations Directors. (Reference 3.)

b. "The success of a safety program is dependent on the same criteria as the success of any other program -- the desire of management to see it succeed and the dedication of all employees in performing their assigned responsibilities." (Reference 3.)

c. "There is direct relationship between the degree of safety achieved in a NASA aerospace system and the management emphasis placed on the safety of the system being designed, manufactured, tested, and operated." (Reference 1.)

d. "Emphasis is to be placed on knowledge of hazards, the elimination or control of hazards, and risk management. Risk evaluations will be applied in the decision making process bearing on the safety of personnel and equipment." (Reference 3.)

e. "The program manager of an aerospace system must assume certain risks that are attendant to the design, manufacture, test, and operation of the hardware system to effectively accomplish the mission for which the hardware was developed. The acceptance of these risks should be based on thorough visibility as to the nature of hazards and risks that are in existence and the options and alternatives to the acceptance of the risks.

The decision on whether to assume a risk is clearly a program management responsibility. This decision is no better than the quality of the risk data that serves as a basis for the decision. Accordingly, the development of hazard and risk data should be assigned as a responsibility to professionals whose training and orientation cause them to search out and find the hazards in the system before these hazards manifest themselves in terms of damaged or destroyed hardware." (Reference 1.)

While the thoughts expressed by the above statements could probably be said in other ways, it is believed that they illustrate basic thoughts about aerospace system safety that can also apply to other activities where there is a genuine concern for safety.

Definitions-Selected definitions of system safety and the three safety analysis techniques emphasized in this discussion are provided in the following paragraphs.

1. System Safety-

a. From the System Safety Society.

"The System Safety concept is basically the application of appropriate technical and managerial skills that a systematic forward-looking hazard identification and control function is made an integral part of a project, program or activity at the conceptual planning phase, continuing through design, production, testing, use and disposal phases."

b. NASA, in reference 3, notes that system safety prescribes the overall approach to risk evaluation by:

"a. Systematically identifying the hazards of a defined set of hardware and software. This includes all phases of development and operations such as design, manufacture, test, transportation, storage, usage, maintenance, modifications disposal, etc.

b. Eliminating these hazards insofar as is possible. If the hazards cannot be eliminated, taking all practical steps to control them in a timely, cost-effective manner.

c. Assessing the risks remaining as inherent in the system or operation during its intended life.

d. Providing the safety risk assessments to the appropriate management level for a decision to either resolve the hazard or assume the risk.

e. Documenting the management decision and rationale regarding the acceptance of risk."

2. Hazard Analysis-

a. This is a systematic examination of the system, starting with the early design efforts and progressing with the design development and including all design changes, to identify all hazards associated with the design and its intended application. The examination includes consideration of all energy sources, interfaces with personnel, interfaces with other equipment, interactions with other items and with the environment, all types of radiation, control systems, fire potential, safety data, experience with similar systems, and operating, emergency and maintenance procedures. (References 1-3.)

b. NASA, in reference 5 describes the application of the hazard analysis technique to ground operations in a manner that is believed to be appropriate for this potential application.

> "Hazard analyses should be performed at the beginning of the critical phases of the system life cycle. The phases are concept, design, testing, development, production, operation, maintenance, modification, mishap investigation, and termination or disposal. Whenever possible, the hazard analysis process should begin during the conceptual phase. No matter when it begins, however, it should continue during the life of the system.
>
> All potential hazards should be analyzed, such as:
>
> a. Those that result from failures irrespective of subsystem or component redundancy.
> b. Those emanating from normal or emergency equipment operations, environment, operator error and design characteristics.
> c. Failures or malfunctions that could independently or collectively present a potential hazard to nearby systems or facilities.
>
> Equipment that will be utilized in more than one operational area or phase should be analyzed for each area or phase."

3. Fault Tree Analysis-This is also a systematic analysis of a system that consists of a graphical and logical representation of all combinations of events, both normal and faulty, which can contribute to or cause a postulated undesired event within a system. When developed this analysis presents a top down look; from the defined undesired event down through the interrelationships of components and parts within the system and the contributing events, whether machine or person initiated.

The U.S. NRC has provided a handbook, reference 6, that has also been useful to safety analysis effort in support of the current NASA manned space flight programs. The following quote from reference 6 provides additional insight to the fault tree analysis technique.

> "A fault tree analysis can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are

associated with component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event - which is the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive - they cover only the most credible faults as assessed by the analyst."

4. Sneak Analysis-This is a space-age analysis technique that often, but not always, relies on the performance of a sophisticated computer program to quickly analyze large amounts of input data to identify hazards. Many of the analyses conducted have searched for latent paths or conditions in electrical designs which exhibit unapparent cause-effect relations that may cause unintended functions to occur, that may inhibit desired functions, or that may cause glitches and other spurious activities. The sneak analysis technique has been applied in the NASA manned flight programs, in the nuclear power program and in other activities in the commercial sector. It has been applied to hardware systems other than electrical systems and has been applied to software. When applied to electrical systems this technique has been identified as a SCA (Sneak Circuit Analysis).

The sneak analysis technique may be one of the most misunderstood and most underrated of modern analysis techniques. Often this analysis is perceived as being a huge bundle of computer programs that turn out masses of expensive data; actually, the size, complexity and cost of the analysis are related to the size and complexity of the system or systems being analyzed. Experienced and skilled people are essential to achieving an accurate analysis.

Additional understanding about why sneak analyses are performed and what they provide is supplied by the following excerpts from reference 4.

"SA (Sneak Analysis) is a unique design assurance technique tnat was initially developed for NASA during the Apollo program. In early 1967, NASA contracted with the Boeing Company to develop a technique for the identification of sneak circuits. This development was undertaken because several "sneak" anomalies had occurred in unmanned space vehicles and in the commercial sector without a hardware failure and had escaped the normal design assurance analyses." (Emphasis added.)

"Although originally developed for electrical/electronic circuits (sneak circuit analysis), it has subsequently been extended to include software (software sneak analysis). In addition to the primary goal of detecting sneak conditions, the analysis technique provides a unique perspective of the design and, therefore, design problems and drawing errors are frequently detected and reported."

"The SA is also an effective tool to supplement system test programs for both hardware and software. The system test program is used to demonstrate proper system operation with the complete range of input parameters specified. The hardware SCA (sneak circuit analysis) is an analytical tool for identifying situations and combinations of inputs which may cause the system to work incorrectly. The software SA is good means to investigate coding problems, definition of inaccessible coding, interface problems with hardware, and undesired operating modes. An integrated hardware and software SA will provide a high degree of confidence that the system will perform as designed with no unusual responses."

"The assurance function performed by SA is to identify conditions such as sneak paths, sneak timing, sneak labels, and sneak indications in hardware and software. The effort is cost effective when applied as soon as manufacturing drawings become available to implement the released engineering drawings."

Results of sneak analyses have often disclosed dormant, unsafe events existing in systems that have shown no symptoms of problems after months and years of operation. The dormant, unsafe events were just waiting for the proper set of conditions, or even a single condition, to trigger them into action. Appreciation of what a sneak event can do to "your day" is often only realized after one has "eaten your lunch".

Discussion-Hazards identified by these safety analysis techniques are then processed through the system, as noted in reference 2. The first emphasis is to eliminate each hazard by changes in the design. Other effort on the remaining hazards is made to reduce their effects to the minimum, that is, to a satisfactory controlled level, through design, the use of safety and warning devices, and/or the use of special procedures. Those hazards that remain, the residual hazards, are then reviewed with management. The project does not proceed until all identified hazards have either been eliminated, controlled to acceptable levels, or have been accepted by management as acceptable risks. Those accepted as acceptable risks are specially identified and tracked so that effort to eliminate them or to reduce their significance can be continued and so they can be reconsidered when changes and/or modifications to the facility or to the procedures are considered.

The potential usefulness of the system safety technique, as described herein, to the related nuclear power industry has been emphasized in investigations and studies such as the investigation after the TMI accident, as reported in reference 7; in a DOE sponsored study of space and aviation technology, as reported in reference 8; and in the NRC sponsored study of programs of other agencies and industries for potential application to the NRC programs for the assurance of quality, as reported in reference 9. Since it is believed that there is a fairly close relation between the technical needs of the high level waste repository program and those of the nuclear power industry, pertinent quotes from these three references relative to the system safety technique are supplied for additional emphasis, as follows:

From reference 7, a major Finding.

> "There was a lack of detailed safety and failure modes analysis on all plant systems necessary to ensure the reliability and safety of the facility."

From reference 8, a recommendation.

> "The nuclear industry and the NRC should consider the NASA Hazard Analysis Technologies as part of their evaluation of new Safety, Reliability, and Quality Assurance (SR & QA) programs."

From reference 9, a recommendation from a special study.

> "9.2.1 Design and Quality Engineering
>
> The NRC should consider requiring that plant design be well advanced before initiating construction activities. Design requirements should include the completion of safety, reliability, and availability analyses including failure mode and effect analyses, fault tree and hazards analyses, and safety analyses. The analyses should be integrated with QA and should be completed before construction begins. This recommendation is based upon findings from the DOE, NASA, FAA, foreign nuclear, and shipbuilding programs."

Interfaces

While the identification of hazards is accomplished to a large extent by the safety professional staff using the described system safety analysis techniques in conjunction with the designers, the safety professionals also use the results of complementary analyses, such as failure modes and effects analysis, software/hardware interaction analyses and special analyses to provide clues that could identify additional hazards. Outputs of the PRACAS (problem reporting and corrective action system) and of the postflight

evaluations also provide opportunities for the identification of additional hazards.

During the activity to reduce hazards to acceptable levels, the safety engineer may work with the quality assurance people to provide special inspection points to confirm the absence of a condition that could aggravate a hazard or work with the reliability engineers to establish special tests to confirm the functionality of a component.

Whenever changes are proposed for equipment or procedures, they are assessed for hazards; and the safety staff presents their evaluations at the appropriate configuration control panel or milestone review.

Periodically the safety effort presents updated summaries of the identified hazards, including the rationale used by management to accept the risks presented by those hazards that could not be eliminated or reduced to an acceptable level, to keep management informed as to the cumulative risk of these hazards.

The safety effort maintains many interfaces to ensure that the information needed to identify hazards is complete.

Direct Experience

One of the most important features of the system safety analysis techniques as applied at the NASA Lyndon B. Johnson Space Center has been the ability, as with all of the aspects of the safety activity, to continue to work the analyses to accommodate changes to equipment and to operating modes and information through the various interfaces so that the outputs, the identified hazards, remained up to date and assessed and reduced to the maximum extent. With this effort safety was able to present coordinated, complete and factual integrated safety analysis assessments to support the major milestone reviews. Accomplishing the frequent, complete and factual assessments were important achievements; realizing that these assessments were documented and backed up with specific technical details to withstand major inquiry and were generally fully coordinated with design engineering and operational staffs before being presented to the milestone review board supports the description of this achievement.

Details of the experience obtained with the use of the system safety techniques in the NASA manned space flight programs and in many other areas of technical achievement can be obtained from the large amount of literature that exists, including that presented in references 10 - 12 for work done for the NASA Lyndon B. Johnson Space Center and that presented in references 13 - 15 for work done on nuclear facilities. Some details from some of these references are quoted in the following paragraphs to illustrate what types of weaknesses these special safety analysis techniques can

identify in designs that had been performed under close scrutiny.

Results of the hazard analysis performed on the Shuttle Training Aircraft for the NASA Lyndon B. Johnson Space Center are reported in reference 10. The RESULTS SUMMARY section of this reference indicated in part, the following:

> "A total of 67 hazardous conditions were identified and assessed during the performance of this hazard analysis. ..... The majority of the identified hazardous conditions can occur anytime during pilot training operations and, therefore, no attempt was made to classify the hazards by mission phase. Some of the identified hazardous conditions in the STA operations are independent of hardware failures. ....."

Results of a fault tree analysis performed for the NASA Lyndon B. Johnson Space Center on the Shuttle Training Aircraft are reported in reference 11. The Results section of the Fault Tree Analysis section of this reference noted, in part, the following:

> "The Fault Tree Analysis identified seven classes of failures which can result in loss of the aircraft during flight operation."

Results of a sneak circuit analysis performed in 1975 for the NASA Lyndon B. Johnson Space Center on the Shuttle Training Aircraft are reported in reference 12. The RESULTS section of this reference noted, in part, the following:

> "The STA (Shuttle Training Aircraft) systems analyzed were found to contain 86 basic sneak conditions which were documented in 40 sneak circuit reports. In addition, 46 design concern reports and 181 drawing error reports were written. ....."

Results of a sneak circuit analysis in 1976 for the Energy Research and Development Administration, Richland Operations Office, on the plant protection system elements of the Fast Flux Test Facility are reported in reference 13. The RESULTS section of this reference noted, in part, the following:

> "Five sneak circuits were found during the analysis. ..... Thirteen Analyst Concern Reports were written to address design or procedural deficiencies noted during the analysis. ..... Ten Drawing Error Reports were submitted to document incorrect or confusing information discovered in the detailed schematics, wiring diagrams, circuit schedules, and connection diagrams. ....."

Probably not all of the weaknesses identified by these techniques turned out to be real concerns; however, it is very likely that the aircraft or facility to which these

special safety analysis techniques were applied were safer because of this effort.

Operating Philosophy

The operating philosophy developed by the safety engineers on the NASA manned space flight programs, including the ground support activities, has been one of an aggressive, knowledgeable and independent approach that worked the many technical interfaces in a cooperative way. There was a close working relationship between the contractor and government design engineers and safety engineers similar to the relationships that existed between groups of contractor and government engineers participating in the other SRQA techniques discussed. This mode of operation did much to enable the productivity achieved.

Benefits

Adoption of the system safety technique and the specialized safety analysis techniques described in this section, tailored to fit the specific needs of the high level radioactive waste repositories being developed by the DOE, will enable the site management to identify hazards early in the program life and give them the opportunity to bring about corrective action when the cost and schedule impacts are the least. Other benefits include the ability to periodically obtain an assessment of the cumulative risk incurred as a result of individual management decisions to accept hazards that could not be eliminated or controlled to an acceptable level; the ability to provide accurate and current safety assessments related to the NRC licensing requirements; and to provide assistance to the other safety efforts at the site in the mutual quest for site safety.

Properly implemented, the system safety technique encourages better engineering and more informed management.

Recommendations

It is recommended that the DOE adopt the system safety technique and the specialized safety analysis techniques, as described in this section, for use in the implementation of the activities associated with the NWPA of 1982; and that consideration be given to tailoring the requirements of these techniques to fit the specific needs of the high level radioactive waste repository program sites and of the waste transportation system.

Time of Application

The application of the part of the system safety technique, as described herein, should be considered for the time period when engineering is initiated for such things as the disposal package, the engineered barriers and the facility equipment that will be used during the repository construction, operating and decommissioning phases, to construct the facility, to handle waste packages, to backfill, to retrieve and to accomplish all of the functions that will serve to

protect the workers, the public and the environment. It is possible that the safety analysis technique, sneak analysis, may also be useful for examination of the software used in the analysis and modeling of the data from the site characterization phase.

Anticipated Ease of Technology Transfer

It is anticipated that the transfer of the capability to accomplish the system safety technique from aerospace to the DOE will be straightforward for the parts associated with the hazard analysis and the fault tree analysis specialized safety analysis techniques since they are widely used and are an established part of good engineering practice; some parts of these techniques developed specifically by the NASA manned space flight programs may require additional time to transfer. The sneak analysis technique will not be as easy to transfer because it is a fairly recent development; not many people have experience with it; and it does require special training and experience to accomplish. The method of transfer most likely to succeed would probably involve the use of lectures and work shops for most of the system safety technique; the use of an aerospace contractor with specific experience would probably be required for extensive sneak analysis work.

System Safety Techniques References

1. NHB 1700.1(V3), "NASA Safety Manual, Volume 3, System Safety", NASA, March 6, 1970. (3050)

2. NHB 5300.4 (1D-2), "Safety, Reliability, Maintainability and Quality Assurance Provisions for the Space Shuttle Program", NASA Reliability and Quality Assurance Publication, October 1979. (3009)

3. NHB 1700.1(V1-A), "Basic Safety Manual", NASA, January 17, 1983. (3051)

4. JSC 18377, "Sneak Analysis Applications Guideline for New Procurements", NASA-JSC Safety Division, July 12, 1984. (3059)

5. JSC 17773, "Instructions for Preparation of Hazard Analysis for JSC Ground Operations", NASA Lyndon B. Johnson Space Center, December 1984. (3107)

6. W.E. Vesely, F.F. Goldberg, N.H. Roberts, D.F. Haasl, "Fault Tree Handbook", NUREG 0492, U.S. NRC, January 1981. (1069)

7. William M. Bland, Jr. and Dwight Reilly, "Quality Assurance", pp 1-118, Reports of the Technical Assessment Task Force, Vol. IV, Staff Reports of the President's Commission on the Accident at Three Mile Island, Oct. 1979. (7010)

8. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", prepared for the U.S. DOE, April 1980. (2004)

9. W. Altman, T. Ankrum, W. Brach, "Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants", NUREG 1055, U.S. NRC, May 1984. (1002A)

10. JSC XXXXX, Draft, "Shuttle Training Aircraft Hazard Analysis Report", NASA Lyndon B. Johnson Space Center. (3056)

11. D2-118652-1, "Engineering Analysis of the Shuttle Training Aircraft", prepared for the NASA Lyndon B. Johnson Space Center by The Boeing Company, January 25, 1979. (3089)

12. JSC 10626, "Sneak Circuit Analysis of the Shuttle Training Aircraft", for the NASA Lyndon B. Johnson Space Center by the Boeing Aerospace Company, January 23, 1976. (3054)

13. D2-118597-1, "Sneak Circuit Analysis of LMFBR Plant Protection System", prepared for the Energy Research and Development Administration by The Boeing Company, September 30, 1976. (7042)

14. D2-118623-1A, "Sneak Circuit Analysis of P,K, & C Reactor Safety Circuits - Savannah River Plant", Boeing Aerospace Company, July 29, 1977. (7044)

15. D2-118542-1, "Sneak Circuit Analysis: N Reactor", Boeing Aerospace Company, July 31, 1974. (7041)

2. FAILURE MODES AND EFFECTS ANALYSIS/CRITICAL ITEMS LIST

Background

Another very effective technique for assuring success of the NASA manned space flight programs has been that of the failure modes and effects analysis/critical items list, generally better known by the acronym of FMEA/CIL. The FMEA part of this technique is the action part in which the analysis of items is accomplished and problems identified; the CIL is used to focus attention on the identified critical concerns and problems in an effort to eliminate them or to cause effort to be generated that will either minimize the likelihood of their occurrence, minimize the effect of occurrence, or both.

The failure modes and effects analysis technique, herein after called the FMEA technique, has had a number of slightly differing definitions over the years as this technique has matured and as the characteristics of the different areas that it has been applied in are reflected in the terminology.

One generally acceptable definition, from reference 1, is as follows:

> "FAILURE MODE AND EFFECTS ANALYSIS (FMEA): A procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity."

A recently informally used definition of FMEA by the NASA Lyndon B. Johnson Space Center's Reliability Division is as follows:

> "FAILURE MODES AND EFFECTS ANALYSIS -- Study of a system and working interrelationships of its elements to determine ways in which failures can occur (failure modes), effects of potential failure on the system element in which it occurs and on other system elements, and the probable overall consequences of each failure mode on the success of the system's mission."

The consequences of each failure mode are the principal determining factors in the assignment of the criticality label to a failure mode.

These definitions can be amplified by noting that the FMEA is a systematic approach that is best conducted at the time the design process begins and is maintained through final design, including changes to the design. The analysis is generally conducted by the design engineers to a written procedure generally developed by the design engineers and the reliabilty engineers that also prescribes the methods for documentation; both the design and the reliability engineers sign off and support the results of the analysis. The early NASA manned flight programs performed the intent of the defined analysis, but without the benefit of definitive documentation. The maturing development of the FMEA technique and the companion technique of the CIL (Critical Items List) can be observed through the NASA manned space flight programs as contained with the documents of references 2 through 7.

The CIL, the companion activity to the FMEA, was developed from the beginning of the NASA manned space flight programs to satisfy a need, as was the FMEA; however, it only became identified by name of CIL for the Space Shuttle Program. The CIL is the record of the critical concerns and problems identified by the FMEA process; it is used to focus attention on items with postulated significant undesirable effects. It includes, for the current NASA manned space flight program, single failure modes with effects that could cause loss of crew, vehicle or mission and redundant elements, whose failure could cause loss of crew or mission if not detected. The CIL also includes single generic failure cause(s) that could lead to loss of crew or mission in spite of built-in

redundancy. In the application of the CIL during the technical reviews, rationale is added for each item that documents the actions that have been taken to minimize the potential occurrence of that item and the resulting undesirable effects. These include the design features that minimize the failure mode causes and effects, the required tests to detect the existence of these critical modes, inspections that minimize the possibility of the failure effects being built into the hardware and the failure history to demonstrate the effectiveness of the rationale.

Equipment appearing on the CIL is given special attention in a number of ways, including the following: in establishing hardware certification (qualification) requirements; in manufacturing, inspection and test planning; in the formulation of operating and maintenance procedures and mission rules; and in the visibility given them during technical and management reviews and decision making sessions, including configuration control panel meetings and milestone reviews.

The potential usefulness of these techniques, the FMEA and the CIL, to the related nuclear power industry has also been emphasized in investigations and studies such as the investigation after the TMI accident, as reported in reference 8; in the DOE sponsored study of space and aviation technology, as reported in reference 9; and in the NRC sponsored study of assurance of quality in other agencies and industries, as reported in reference 10. Since it is believed that there is a fairly close relation between the technical needs of the high level waste repository program and the nuclear power programs, pertinent quotes from these three references relative to this technique are supplied for additional emphasis, as follows:

From reference 8, a major Finding.

> "There was a lack of detailed safety and failure modes analysis on all plant systems necessary to ensure the reliability and safety of the facility."

From reference 9, a recommendation.

> "The nuclear industry and the NRC should examine the NASA Failure Mode and Effects Analysis/Critical Item List (FMEA) techniques and associated software documentation programs for application to LWRs. NRC should also consider this from a reactor safety and licensing perspective."

From reference 10, a recommendation from a special study.

> "9.2.1 Design and Quality Engineering
>
> The NRC should consider requiring that plant design be

well advanced before initiating construction activities. Design requirements should include the completion of safety, reliability, and availability analyses including failure mode and effect analyses, fault tree and hazards analyses, and safety analyses. The analyses should be integrated with QA and should be completed before construction begins. This recommendation is based upon findings from the DOE, NASA, FAA, foreign nuclear, and shipbuilding programs."

Interfaces

While the FMEA and the CIL are documents generated by and for the engineering and reliability efforts for achieving the safest and most reliable designs, they are also most useful to a number of the other significant technical disciplines. They are used as a convenient way to describe the state of the design to upper management, as at the time of design reviews, other milestone reviews and configuration control panel meetings; as a means to alert the test people of potential failure modes to be on the alert for during the test program and in the generation of test requirements; as identification of weaknesses to be worked with preventive steps in the generation of operating and emergency procedures and to be emphasized in the formulation of training procedures; as inputs to those performing special safety analyses to ensure that identified hazards are either eliminated or properly controlled; as information to those concerned with planning for maintenance, test and/or inspection during operation; as an identification of places where quality assurance should consider the establishment of special or mandatory inspection points; and as a reference for those who are considering, proposing or acting on design changes. Thus it can be seen that these techniques have useful outputs to satisfy not only the original intent of providing indepth analyses for engineering design use, but that the outputs are also of significant use to many other technical and management activities that are working to assure safe and reliable operations.

Direct Experience

Details of the experience obtained with the use of the FMEA and the CIL techniques in the NASA manned space flight programs and in other areas of technical activity can be obtained from the large body of literature that exists, including references 6 and 7. The application of these techniques has been increased in depth and in scope with the benefit of experiences gained during the NASA Apollo and Space Shuttle programs and is planned to have very significant roles in the Space Station program of the future, reference 7. It is believed that these should provide sufficiently convincing arguments to have these techniques applied to the DOE-directed activities in accomplishing the NWPA of 1982, despite the seeming large differences in the engineering activity. Features of particular interest from

Apollo and Space Shuttle efforts are listed, from references 6 and 7, in order to illustrate the value of the FMEA/CIL.

The FMEA/CIL techniques provided the following information:

1. identified possible failure modes;

2. enumerated and described the failure effects from the possible failure modes;

3. described the primary and most likely causes of the possible failure modes;

4. described the methods of detecting the conditions that would give rise to possible failure modes or to failures;

5. described the actions to be taken to prevent the possible failure modes from occurring; and

6. provided documentation of the retention rationale, such as special provisions of design, test, and inspection and the failure history of the pertinent equipment, for those identified possible critical failure modes that were not eliminated; those not eliminated, but retained, also required a waiver signed by project management or higher.

An important feature of the FMEA/CIL techniques is that they force the designers to systematically think about what may go wrong with the hardware and what the effect will be. The designers are then prompted to identify the cause or causes and to determine what needs to be done to prevent the occurrence of the postulated "what may go wrong" event.

Operating Philosophy

The operating philosophy developed through the years of experience of the FMEA/CIL techniques on the NASA manned space flight programs is very close kin to that developed in a number of the other SRQA techniques described. This happens to be true because many of the same people, or their very close associates (supervisors, subordinates or peers) were involved in the application of these and the other SRQA techniques. Thus, the same commitments, goals and attention-to-detail, governed the way the involved people, the contractor and government design engineers and reliability engineers (in this case) went about their tasks related to FMEAs and CILs. Other factors about the people role, the data base and the knowledge distribution discussed under **Operating Philosophy** in the discussion of the Equipment Certification technique applies to this discussion for FMEA and CIL techniques.

Benefits

Adoption of the FMEA/CIL technique, particularly as the technique has been developed and implemented by the NASA manned space flight programs, and then tailored to fit the

specific needs of the high level radioactive waste program can provide a number of benefits to the DOE effort. This technique will force the designers to systematically identify weaknesses in the design effort and note their importance to safety, to isolation and to the graded "Q" effort. Those significant weaknesses not corrected by the designers will then be brought to management attention where additional effort will be made to eliminate these weaknesses; those remaining will, with management's acceptance of the potential risk of their presence, receive possible attention from design, testing, inspection and procedures to provide maximum possible assurance that the weaknesses will have a minimum possibility of causing problems.

Properly implemented, the FMEA/CIL technique encourages stronger engineering and more knowledgeable management.

Recommendations

It is recommended that the DOE adopt the utilization of the FMEA (Failure Mode and Effects Analysis)/CIL (Critical Items List) technique, as described herein, for use in the implementation of the activities associated with the NWPA of 1982; and that the degree of development of this technique as applied to the Space Shuttle program would be a reasonable level to apply to the high-level waste repository engineering program, with some tailoring of the technique to accommodate differences between the two programs. Application of this technique should also be considered for the waste transportation system.

Time of Application

The application of the FMEA and CIL techniques should be considered for the time period when engineering is initiated for such things as the disposal package, the engineered barriers and the facility equipment that will be used during the repository construction, operating and decommissioning phases to construct the facility, to handle waste packages, to backfill, to retrieve and to accomplish all of the functions that will serve to protect the workers, the public and the environment. The most efficient time to initiate the application of these techniques is at the time of the initial engineering, although catch-up can be effectively done when the decision to do so is made with conviction. Whenever the application of these techniques is made, it will be most important to implement them so that the information generated by the FMEA/CIL techniques is made available across the interfaces, such as between the waste package and the facility handling equipment, and that the interfaces are also analyzed by the FMEA technique.

Anticipated Ease of Technology Transfer

It is anticipated that the transfer of the capability to accomplish the FMEA/CIL technique from the aerospace to the DOE high level radioactive waste repository program will be straightforward. The methodology, basically the questions to

be asked and answered by the engineers in accomplishing the analysis, is fundamental to good engineering practice and is not expected to present a problem. There is nothing unique about the documentation involved; thus it should not present a problem. It is expected that relatively brief training sessions and some longer on-the-job guidance can make the methodology and documentation transfer occur very simply. The application of these techniques, as in the operating philosophy and in the utilization of these techniques by management, both of which are considered to have unique roots, may require additional effort to transfer, such as with the use of lectures, workshops and on-the-job guidance.

Failure Modes and Effects Analysis/Critical Items List References

1. MIL-STD-721C, "Definitions of Terms for Reliability and Maintainability", U.S. DOE Military Standard, 12 June 1970. (5006)

2. NPC 250-1, "Reliability Program Provisions for Space System Contractors", Reliability Publication, NASA, July 1963. (3035)

3. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, 1970. (3023)

4. NHB 5300.1A, "Apollo Reliability and Quality Assurance Program Plan", NASA, July 1966. (3036)

5. NHB 5300.4(1D-2), "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program", NASA, October 1979. (3009)

6. Joseph H. Levine, "NASA Approach to Space Shuttle Reliability", JSC-18187, NASA Lyndon B. Johnson Space Center, July 1982. (3038)

7. JSC 19689, "NASA Preliminary FMEA (Failure Modes and Effects Analysis) and CIL (Critical Items List) Approach for Space Station", NASA Lyndon B. Johnson Space Center, May 1984. (3044)

8. William M. Bland, Jr. and Dwight Reilly, "Quality Assurance", pp 1-118, Reports of the Technical Assessment Task Force, Vol IV, Staff Reports to the President's Commission on the Accident at Three Mile Island, Oct. 1979. (7010)

9. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", U.S. DOE, April 1980. (2004)

10. W. Altman, T. Ankrum, W. Brach, "Improving Quality and the Assurance of Quality in the Design and Construction of

Nuclear Power Plants", NUREG-1055, U.S. NRC, May 1984. (1002A)

3. PROBLEM REPORTING AND CORRECTIVE ACTION SYSTEM

Background

A very strong contributor to the success of the NASA manned space flight programs has been the PRACAS (Problem Reporting and Corrective Action System). From the very first of these programs the prompt reporting of flight hardware failures, their analysis, the achievement of a complete understanding of the cause and the application of corrective action has been a significant part of the actions which contributed to the reliability of the spacecraft. The following quotations from reference 1 are presented to indicate the seriousness with which concerns about hardware anomalies, which included failure to operate, were considered in the earliest of these programs.

> "It has been adequately demonstrated in the manned space flight program that no launchings should proceed in the face of anomalies that could adversely affect flight safety of mission success. Further, launchings should proceed only after the anomalies have been resolved and all necessary changes in equipment or procedures have been thoroughly qualified and examined."
>
> "Random failure is not an acceptable explanation for anomalous behavior."

Even with the wording of activities that occurred more than twenty years ago, the intent of the quoted material above is quite clear about the seriousness with which equipment failures were treated; this treatment was consistent from the bottom to the top of the organization.

As experience was accumulated through the accomplishment of various manned space flight programs, emphasis remained on the requirements to have failures promptly reported, analyzed, understood and corrected. The requirements became better defined and documented, the scope of reportable types of problems increased, the manual manipulation of the extensive paper work gave way to computerized systems, and the name of the system in use at the NASA Lyndon B. Johnson Space Center (also identified as JSC in this document) became PRACAS part of the way into the Apollo Spacecraft Program.

The evolution of the requirements of the failure, or the problem reporting system that it evolved into, can be traced in the NASA Headquarters documents in references 2 through 6 to the requirements for the NASA Space Shuttle Program. Examination of these requirements show that the basic requirements have remained about the same, though there has been some modification to fit the specific needs of the

programs. An example of the detailed action required by these NASA documents during the time of the Apollo Program is given by a quotation from reference 4, as follows:

> "c. Every failure encountered in testing, checkout, or operation of flight equipment (including GSE and GOSS interface equipment) will be verified, recorded, analyzed, compared with previous occurrences, and corrected on the item and subsequent items, so that no unexplained failures will be present in the Apollo Hardware. Human errors during testing and training will be recorded."

A similar statement from reference 6 that was intended to be directed to NASA Space Shuttle contractors is as follows:

> "The contractor shall provide a closed-loop system for the reporting of all problems (failures and unsatisfactory condition reports) and the establishment of corrective action for all problems concerning flight, test, simulator, and training hardware where that hardware is representative of flight hardware, GSE, applicable GFE, and spare hardware. The contractor shall be responsible for ensuring that problem reporting and corrective action systems of suppliers will meet the requirements of this section."

More detailed requirements have been developed for use by the involved government element offices and their contractors in NASA Center documents, such as those contained in reference 7 that apply to the Space Shuttle Program. These requirements treat such subjects as applicability to specific program phases, activity, and hardware types; responsibilities of government and contractor elements; system requirements such as time constraints, problem analysis criteria; definition and treatment of constraining and nonconstraining problems, problem trending; treatment of in-flight anomalies; problem report data elements; and data system requirements. These requirements were tailored specifically for the needs of the Space Shuttle Program from the basic problem reporting and corrective action system for JSC programs that is described in reference 8. The information in reference 8 includes the assignment of responsibilities related to the PRACAS at the Center, a listing of the basic PRACA system requirements and definitions of applicable terms.

The implementation procedures used by the JSC SR&QA personnel in operating the PRACAS are presented in reference 9. This reference includes detailed process flow diagrams, which also include the interfaces with personnel outside of the NASA JSC SR&QA office; definitions of terms, detailed instructions on the use of forms. It also describes how important PRACAS functions like rapid notification to responsible technical personnel, notification to project management at JSC and other Centers of system-level problems; periodic publication and distribution of listings of open

problems; presentation of status of hardware problems to JSC program and project management; timely and adequate remedial action and recurrence control of problems; and storage and retrieval of problem data are accomplished.

It is emphasized here that the PRACAS is a "Problem" reporting system. That is, it has been established to handle and process a variety of problems that include the following: hardware and equipment failures, problems caused by procedures and software, conditions that are unsatisfactory, safety-related problems, and others that may be defined. Further emphasis is given by the following quotes selected from reference 9.

> "Problem - Any nonconformance which fits or which is suspected of fitting one of the following categories:
>
> > Failure or unsatisfactory condition occurring during or subsequent to....." and
>
> "Failure - The inability of a system, subsystem, component, or part to perform its specified function within specified limits, under specified conditions, or for a specified duration." and
>
> "Unsatisfactory Condition - Any defect for which engineering resolution is required and which requires recurrence control beyond the specific article under consideration. Included in the definition are conditions which cannot be corrected to specified configuration using the standard planned operation; or an event which could lead to a failed condition....." and
>
> "Safety-Related Problem - A CFE or GFE problem which could result in loss of life of vehicle. A GSE problem which could result in loss of personnel capability or loss of ....." and
>
> "Significant Problem - Any problem determined to warrant project management attention on the basis of any of the following:
>
> > Problem analysis and resolution indicate retrofit to hardware on the vehicle is required.
> >
> > Problem affects an extensively used electrical, electronic, or electromechanical part and analysis indicates a generic defect.
> >
> > Problem has significant impact on program schedules, design, or resources.
> >
> > Problem is a catastrophic failure of qualified hardware which will affect the next flight vehicle.

Problem where hardware has failed in a criticality 1 mode or can affect the safety of the next flight vehicle." and

"System-Level Problem - Any problem that has one of the following characteristics:

Common hardware - Problem occurring .....

Interface hardware - Problem affecting ....."

These examples of definitions from reference 9 are presented to illustrate the wide variety of events that are included in the PRACAS experience. The above definitions used as examples were not always quoted in their entirety because the aerospace language used does not always have an apparent analogy with the language used in the high level waste effort. The definitions applied to a PRACAS-type activity by the DOE could have definitions tailored to fit the needs of the high level waste program.

Additional implementation procedures and responsibility assignments within the SRQA organizations relative to the PRACAS are included in reference 10, which is a compilation of the current issues of SRQA Policy Statements and implementing procedures.

There are other documents available that describe the implementation of the PRACAS from the point of view of the major NASA contractors, as on the Space Shuttle Program and Element Projects and on the earlier NASA manned space flight programs; however, it is believed that the essential ingredients of the operation of the PRACAS can be obtained from documents like references 8 to 10. From these ingredients it will be necessary to generate new requirements and implementing procedures to fit the needs of other activities, including activities like those of the DOE and the DOE-contractors in implementing the NWPA of 1982.

That the application of a PRACAS, suitably tailored from the aerospace experience to fit the needs, can be potentially very useful to the DOE and the DOE-contractors in their implementation of the NWPA of 1982 is also suggested by the likely imposition of NRC major problem reporting arrangements on the DOE during the licensing steps that are similar to those imposed by the NRC on the nuclear power industry. A DOE sponsored study of the application of space and aviation technology, reference 11, included the recommendation that NASA's PRACAS be examined for possible use by the NRC (for nuclear power reactors) to supplement or replace the Licensee Event Reports. In earlier assessments of the NRC Licensee Event Report System and related activities, reference 12 noted significant requirements missing for complete problem reporting and corrective action on hardware failures and unsatisfactory conditions that led to a lack of utilization

of these data; reference 13 noted a number of significant weaknesses of the Licensee Event Reports, which resulted in an ineffective system, and included recommendations for the application of the NASA PRACAS to the nuclear power industry.

Interfaces

Of all of the SRQA techniques discussed in this document for application by transfer of technology to the DOE implementation of the NWPA of 1982, the technique named PRACAS probably has the most numerous and the most active set of interfaces. This arrangement of interfaces is due to the emphasis that the NASA has placed on this technique through the years of experience with the manned space flight programs. The emphasis on timeliness of reporting of events, on the thoroughness of analysis and understanding, on the certainty of application of corrective action, on the detailed documentation, on the reviews at special meetings, management reviews and during the milestone reviews, and on the possible hold of tests and flights in event problems of certain criticalities had not been closed out has made these interfaces particularly sensitive to performance.

At the heart of the interfaces, in the NASA-JSC application of the PRACAS, are the contractor and government quality assurance personnel to make sure that problems are identified, reported, statused and documented; for certain types of problems they are also responsible for the analysis and resolution. For most of the problems involving design problems or weaknesses, the contractor/government combination of design and reliability engineers are responsible for the analysis and corrective action. This is a continuation of the very close working arrangements between these engineers that has been noted in some of the other SRQA techniques; such as the equipment certification technique and the failure modes and effects analysis/critical items list technique. This working arrangement can be given a lot of the credit for enabling the development of extremely knowledgeable contractor and government engineering, reliability and quality assurance staffs.

In the routine utilization of the information provided through the PRACAS, a number of different actions take place. Examples of these actions include the safety staff considering modifications to hazard analyses and to operating procedures; the design and reliability engineering staffs considering design changes, redo of certification tests, or substitution of parts; the mission planners considering modifications to mission rules; the checkout people considering modifications to checkout and test procedures; and others considering modifications to training, to sparing, to maintenance and to procurement.

Direct Experience

Details of the PRACAS requirements development during the NASA manned space flight programs can be obtained from

references 1 through 6. Current application of the PRACAS at the NASA Lyndon B. Johnson Space Center with the contractor(s) and government staffs is described in references 7 through 10. Summaries of the experiences with the PRACAS on the Apollo Program are contained in reference 14 and on the Space Shuttle Program, up to mid 1982, are included in reference 15. The following quote from reference 15 very well summarizes the PRACAS guidelines for these two programs and gives an idea of the "traffic" handled by the system.

> "The Space Shuttle problem reporting and corrective action system was initially designed for the Apollo Spacecraft Program. Problem reporting and disposition was of great significance in assuring the maturity of the Apollo spacecraft hardware. The recognition of the importance of a rigorous problem reporting and corrective action system necessitated three basic ground rules.
>
> 1. No flight shall be authorized with unresolved or unexplained problems.
> 2. All problems shall be analyzed to establish the cause to enable corrective action or to define the risk of not taking action.
> 3. The disposition shall be a documented corrective action (i.e., drawing change, specification change, process change, or procedure change).
>
> The design of the Space Shuttle problem reporting and corrective action system is very similar to that used in the Apollo Spacecraft Program, which accumulated upward of 60,000 failures requiring disposition."

It was further noted in reference 15 that the Space Shuttle Orbiter problem reporting and corrective action system was designed using the above ground rules; these were augmented by some additional guidelines. Some of these additional guidelines which are most pertinent to this discussion follow:

> "2. All problems require analysis by knowledgeable design-responsible individuals to ascertain the cause of the problem and to devise an acceptable corrective and preventive action.
>
> 3. The analysis and corrective action taken for each problem are reviewed independently by [contractor] Reliability and Quality Assurance personnel.
>
> 4. An [another] independent review is made by Safety, Reliability, and Quality Assurance personnel and technical personnel of the NASA Lyndon B. Johnson Space Center (JSC) to assure that adequate corrective action has been taken."

(The [ ] enclose additions to the quoted material.)

The material in references 14 and 15 contain useful experience in the application of the PRACAS. The material, from reference 15 illustrates the seriousness with which the PRACAS was applied, the depth of the technical reviews and the quantity of the problems handled. Additional reviews of the information provided by the PRACAS at the various milestone reviews included trends, repeat problems of significance, current status of problems not yet with established resolutions and selected resolved problems.

Operating Philosophy

The operating philosophy of the PRACAS technique is well represented by the documented system requirements of the system and the guidelines discussed above. Beyond these attributes are two great drivers that made the system perform outstandingly; these are continuous management use of the system and the information that it provided and the consistent attention to detail by the people who worked the PRACAS.

Benefits

Adoption of the NASA problem reporting and corrective action system, tailored to fit the requirements and needs of the DOE effort with high level waste repositories, will result in one operating system that can provide rigorous and responsive outputs for the several reporting systems that now exist in the DOE plans and in the NRC licensing requirements and others that may be identified later. It will provide from the one source, consistently prepared documentation that is backed up with the accumulated technical experience of the staff that interfaces with the system. Management will have to look to only one source to obtain a complete "picture" on such information, and its current status, as pending reporting notices, incomplete or open followup actions, open (unsolved) problems, current problem relations to past problems, historical performance, and recommendations to minimize recurrence of problems.

Recommendations

It is recommended that the DOE adopt the methodology and the operating philosophy of the NASA PRACAS (problem reporting and corrective action system) technique, as described herein, for use throughout the DOE and DOE-contractor efforts related to the implementation of the NWPA of 1982; and that consideration be given to applying this technique as one system, from the top, in a tailored fashion to form the basis for satisfying the reporting and assessment, management, licensing, and administrative requirements.

Time of Application

The decision to adopt the methodology and the philosophy of the NASA PRACAS technique should be done well in advance of

the time that hardware is produced for any of the activity at the repository sites. This will allow time for the PRACAS requirements to be tailored from the basic NASA experience to fit the needs of the sites and for the detailed operating procedures to be written and for the people to receive training in their application. Further, it is recommended that the DOE establish the PRACAS to cause the exchange of common interest information between sites to enhance experience transfer. It is also recommended that the DOE consider the application of the PRACAS during site characterization since the PRACAS is also suited to handle procedural problems and data generation and manipulation problems.

Anticipated Ease of Technology Transfer

It is estimated that the technology transfer for the PRACAS technique from the NASA to the DOE activity that is implementing the NWPA of 1982 will be fairly difficult to accomplish. The application of the basic philosophy and the development of specific guidelines can be straightforward as long as it is recognized that two types of people are involved; those who set up and make the system perform and those who use and depend on the system to perform. The development of operating guidelines and procedures will probably be considerably more difficult to accomplish because of the potentially many working interfaces involved in the PRACAS. It is envisioned that the most effective means of accomplishing this technology transfer will include lectures, workshops and fairly long periods of on-the-job guidance at both the working level and at the various management levels.

Acronyms

GSE - ground support equipment
GOSS - ground operational support system
GFE - government furnished equipment

Problem Reporting and Corrective Action System References

1. William M. Bland, Jr. and Lewis R. Fisher, "Reliability Through Attention to Detail", Chapter 38, Manned Spacecraft: Engineering Design and Operation, edited by Paul E. Purser, Maxime A. Faget, and Norman F. Smith, Fairchild Publications, Inc., N.Y., 1965. (7011)

2. NPC 250-1, "Reliability Program Provisions for Space System Contractors", NASA Reliability Publication, NASA, July 1963. (3035)

3. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical And Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1970. (3023)

4. NHB 5300.1A, "Apollo Reliability and Quality Assurance

Program Plan", Office of Manned Space Flight, NASA, July 1966. (3036)

5. NHB 5300.5, "Apollo Applications Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, May 1967. (3037)

6. NHB 5300.4 (1D-2), "Safety, Reliability, Maintainability and Quality Assurance for the Space Shuttle Program", Reliability and Quality Assurance Publication, NASA, October 1979. (3009)

7. JSC 08126, "PRACA (Problem Reporting and Corrective Action) System Requirements for the Space Shuttle Program", NASA Lyndon B. Johnson Space Center, December 14, 1982. (3014)

8. JSCM 5324A, "Problem Reporting and Corrective Action System for JSC Programs", NASA Lyndon B. Johnson Space Center, March 1977. (3012)

9. JSC 09296C, "JSC Procedures for Problem Reporting and Corrective Action", NASA Lyndon B. Johnson Space Center, February 1983. (3013)

10. JSCM 5312, "Safety, Reliability and Quality Assurance Manual", NASA Lyndon B. Johnson Space Center. (3005)

11. DOE/TIC 11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", prepared for the U.S. DOE, April 1980. (2004)

12. JSC 08981, "Application of NASA Safety, Reliability and Quality Assurance Techniques to the Nuclear Power Industry (A Literature Search)", NASA Lyndon B. Johnson Space Center, July 1974. (3021)

13. William M. Bland, Jr. and Dwight Reilly, "Quality Assurance", pp 1-118, Reports of the Technical Assessment Task Force, Vol. IV, Staff Reports to the President's Commission on the Accident at Three Mile Island", October 1979. (7010)

14. T.J. Adams, "Apollo Experience Report-Problem Reporting and Corrective Action System", NASA TN D-7586, February 1974. (3020)

15. Joseph H. Levine, "NASA Approach to Space Shuttle Reliability", JSC-18187, NASA Lyndon B. Johnson Space Center, July 1982. (3038)

4. ELECTRICAL, ELECTRONIC AND ELECTROMECHANICAL PARTS CONTROL

Background

When the intent is to design very reliable equipment, one place to put emphasis is on the selection of the parts that are designed into the devices and components that are then assembled into equipment and subsystems. In its experience with the manned space flight programs, NASA has learned the importance of establishing parts requirements and application control early in the design phase of a program. Because EEE (Electrical, Electronic and Electromechanical) parts can be state-of-the-art, complex, very inaccessible when installed, and often require long procurement lead times, NASA has formalized its EEE parts control technique; it is believed that the benefits obtained with this technique have played a significant role in the success of the NASA manned flight programs.

As defined in reference 1, "part" is one piece or two or more pieces joined together in such a way that they can not be disassembled without destruction. Examples of EEE parts include transistors, diodes, microcircuits, resistors, capacitors, relays, connectors, switches, transformers and inductors.

The evolution of the EEE parts control technique can be traced in the NASA Headquarters documents, references 1 through 5, which contain the reliability requirements for the NASA manned flight programs subsequent to the Mercury Project. The Space Shuttle EEE parts requirements (provisions) applied to the contractors and implemented by the main NASA Field Centers have been well-developed and are documented in reference 5. Some of the highlights of these requirements, as excerpted from reference 5, have been listed in the following paragraphs.

a. The contractor shall implement a system for controlling the selection, reduction in number of types, specification, application review, analyzing failures, stocking and handling methods, installation procedures, and establishing reliability requirements for EEE parts to be used in contract and off-the-shelf hardware.

b. The contractor and suppliers shall select EEE parts for the contract hardware on the basis of suitability for their application(s) and proven qualifications of each to the requirements of its specification. The contractor is fully responsible for the satisfactory performance of each part regardless of the source from which the part was selected or who wrote or approved the controlling documentation.

c. Each EEE part shall be controlled by a specification (or combination of specifications) which delineates specified detailed information about the part.

d. Qualification of EEE parts shall be at the part level to the requirements of the applicable specifications. Requalification of parts shall be conducted as necessary to ensure continued control over design, materials, manufacturing processes and quality controls after initial qualification.

e. The contractor and suppliers shall prepare and maintain a project EEE parts list and composite where-used parts list.

f. The contractor (or supplier, if appropriate) shall conduct thorough parts application reviews on the design of each component at appropriate milestones during its design and development. The results of these reviews will be an input to the Space Shuttle Program milestone design reviews. These applications reviews were conducted to a rigorous set of guidelines that treated derating, life requirements, functional and environmental stresses and historic and current failure experience.

g. The contractor shall assure that backward traceability data can be provided for all EEE parts. Provisions shall be made to record and retrieve information relating to the specific tests performed, test results, and processes on each lot of parts. Identification of the part manufacturer's production, assembly, or test lot shall be available for each part installed in deliverable end items.

h. The contractor shall investigate the cause of each part failure and determine remedial and preventive action. The significance of the failure as related to like parts used elsewhere in the system and the possibility of the occurrence of additional failures shall be determined and documented as part of the problem disposition.

i. The contractor shall establish and maintain an adequate system to monitor and control the use of deviated and substituted parts.

A full accounting of these EEE parts requirements can be found in reference 5.

In addition to the above highlights of the EEE parts requirements from the Space Shuttle Program, it is noted that reference 5 also contains another very important and very closely related requirement on the reporting and resolution of NASA EEE parts problem reports, the ALERTS. Problems with parts which are of mutual concern to NASA and associated contractors are reported by utilizing the ALERT system. The contractor is required to establish a systematic approach to evaluate and respond to all NASA ALERTS and to investigate, resolve, and document EEE parts problems. Previously published ALERTS are to be reviewed to assure that lots, batches, or other groupings of hardware noted as suspect in ALERTs are not used in the supplied equipment.

Instructions for implementing the ALERT system in NASA are contained in reference 6 for the headquarters level and in reference 7 for a major NASA field center. These references note that the ALERT system handles problems with a variety of part types, including EEE parts, and problems with materials and safety problems. The ALERT system in NASA interfaces with and participates with the larger Government-Industry Data Exchange Program (GIDEP), which is managed by the U.S. Navy.

NASA, at the Lyndon B. Johnson Space Center, considered the EEE parts control to be such an important contributor to the reliability of the manned spacecraft that it established a EEE parts control capability that has been functioning since early in the Apollo Program. This parts function, though having close working arrangements with the contractors parts function, performs independent EEE parts assessments and reports its findings to the major milestone review boards as part of the major SRQA assessment reports. It is noted that this close interface with the contractor and the independent assessment of the function is comparable to the working arrangements noted for some of the other techniques, such as the system safety technique, the FMEA/CIL technique, the PRACAS technique and the equipment certification technique.

The potential usefulness of part of the EEE parts control technique to the related nuclear power industry has been noted by the DOE sponsored study of space and aviation technology, reference 8. In this study it was noted that there were several NASA reliability techniques that were considered "transferable" and "applicable" to the LWR nuclear power industry. Among these techniques was the ALERT System that is discussed above and in more detail in reference 8. To make use of the ALERT system, the features described for the EEE parts control technique need to be in place and functioning.

Interfaces

Even though the EEE parts control technique appears to utilize specialists that would appear to work best without outside interference or active external interfaces, it is found that this activity has a number of active interfaces. The EEE parts information is supplied to the designers early in the design effort and at times when design changes that involve EEE parts are considered; this also involves interfaces with the configuration control panels and the board of the configuration management system. Another close interface is with the PRACAS; failures of equipment that involve EEE parts or are suspected of involving EEE parts are reasons for this technique to be involved in the failure investigation. Evaluations of EEE parts activity and the status of parts problems under investigation are included as part of the reliability assessments provided to the boards of the major milestone reviews. Throughout all of these

activities the contractor and government EEE parts specialists work closely together; even though they work together the government parts specialists do provide independent assessments and do assure that the contractor EEE parts control activity meets the contract requirements.

Direct Experience

Details of the operational experience of the EEE parts control technique during the early part of the Space Shuttle Program are contained in reference 9. This experience has been examined in two studies that have been conducted; the most recent study of the EEE parts control technique applied to the Shuttle Orbiter Program was conducted in 1980. The results of this study, which reviewed the parts activities covered by the highlights discussed in the Background section, include a statement, from reference 9, "...(the results) indicate that no major changes to parts controls have been required for the Space Shuttle Orbiter; corrective actions have been related primarily to a given part, manufacturer, or lot."

From the experiences with studies of the EEE parts experience with the Space Shuttle Program and the experiences from past programs have come some recommended EEE parts procurement approaches for application to the proposed Space Station Program, reference 10, with its significantly longer planned useful life that is approaching a possible life of use in the same order as that of the operating life of the repositories that are expected to result from the DOE implementation of the NWPA of 1982. The major features of these approaches include the use of the highest levels of parts available for essential subsystems and the use of a EEE parts control technique similar to those used in the previous manned space programs and much like that used for the Space Shuttle Program. These approaches, therefore, appear to be strong candidates for application to portions of the high level waste repository program that require high reliability and long life from EEE parts.

In addition, an extensive set of preliminary guidelines have been generated for long-life advanced space vehicles, reference 11, that apply to a whole range of parts, including EEE parts, subsystems, structures and assemblies. These guidelines may also have application to the design of the equipment that will be used during the operating phase of the repositories for high level waste.

Operating Philosophy

The operating philosophy developed by the specialists in the EEE parts control technique has become similar to that in some of the other techniques discussed in this document, such as FMEA/CIL, PRACAS and equipment certification techniques. They had strong commitments to getting the jobs done; they applied themselves to "attention-to-detail"; they knew their parts; they provided detailed documentation of their

findings; and they kept management informed. The similarities in operating philosophy with some of the other techniques suggests that this came about because of the strong sense of team work and the very close and active interfaces between the parts specialists and those in the design and reliability engineering and in the quality assurance areas on both the contractor and the government sides of the contract "fence". Their philosophy was further strengthened by the frequent interfaces with interested and knowledgeable management, at the milestone reviews and in the frequent configuration control panel sessions. Management made full use of the NASA EEE parts control resource.

Benefits

A properly functioning EEE parts control technique is one of the important technical efforts in achieving reliable electrical, electronic and electromechanical equipment; reliable equipment contributes significantly to safety. This means that with a EEE parts control activity there will be a decrease in equipment "down time" due to failed parts, to generic parts problems, and to obsolete parts.

In addition, with an active EEE parts control capability it is very possible to avoid equipment failures and attendant systems "down times" at the wrong times. This is accomplished by using the EEE parts traceability capability to identify which equipment contains suspect parts, that is, parts for which notices have been received that indicate possible imminent failure. With information about which equipment contains the suspect part, replacement can be made at a safe time and place rather than after equipment failure, which often comes at the wrong time and at the wrong place for maintaining a proper safety posture. This capability also can make it possible to differentiate among operating equipment and, where the option exists, to not use or to remove from service before a failure occurs equipment that contains suspect EEE parts.

Recommendations

It is recommended that the DOE adopt the EEE parts control technique as described herein and in the identified references; it should be tailored to fit the specific needs of the DOE efforts associated with the implementation of the NWPA of 1982.

Time of Application

The application of the EEE parts control technique should be initiated at the time that design work is first begun on facility construction equipment and disposal package handling equipment, whose failure to operate or to operate in the wrong manner could cause a real or potential hazardous condition. While the most active periods of the technique will be during the design phase, its activity continues fairly strongly during the certification testing phase. The activity drops to a maintenance level during the operational

phase. During this phase, it may be necessary to investigate causes of failures and to decide on the necessary action to prevent recurrence in the particular equipment and to prevent occurrence in similar equipment; or to decide on the necessary action to prevent occurrence when informed of, as by an ALERT, of a failure experienced on similar equipment at another location.

Anticipated Ease of Technology Transfer

It is anticipated that the transfer of the capability to accomplish the EEE parts control technique from the NASA aerospace experience to the DOE high level waste effort will be straightforward and relatively easy. The methodology involved is fundamental to good engineering practice and should not present a problem. It is estimated that detailed training sessions at the designer and parts specialists level can be relatively brief and that workshop sessions will be useful in describing the philosophy of operation and the ways that management can best utilize the EEE parts control capabilities.

EEE Parts Control Technique References

1. NPC 250-1, "Reliability Program Provisions for Space System Contractors", NASA Reliabilty Publication, NASA, July 1963. (3035)

2. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1970. (3023)

3. NHB 5300.1A, "Apollo Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, July 1966. (3036)

4. NHB 5300.5, "Apollo Applications Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, May 1967. (3037)

5. NHB 5300.4(1D-2), "Safety, Reliability, Maintainabilty and Quality Assurance Provisions for the Space Shuttle Program", Reliability and Quality Assurance Publication, NASA, October 1979. (3009)

6. NMI 5310.1C, "Alert-Reporting of NASA Parts, Materials, and Safety Problems", NASA, June 10, 1975. (3102)

7. JSCMI 5310.2F, "Alerts Parts, Materials, and Safety Problems", NASA Lyndon B. Johnson Space Center, 3/29/79. (3103)

8. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", prepared for the U.S. DOE by International Energy Associates Limited, U.S. DOE, April 1980. (2004)

9. Joseph H. Levine, "NASA Approach to Space Shuttle Reliability", Presentation to the NATO Advanced Study Institute, JSC 18187, NASA-Lyndon B. Johnson Space Center, July 1982. (3038)

10. JSC 19297, "Space Station Electrical, Electronic, and Electromechanical Parts Approach", NASA-Lyndon B. Johnson Space Center, September 1983. (3041)

11. JSC 19434, "NASA Long-Life Assurance Study for Advanced Space Vehicles", Contract Study by Lockheed Missile and Space Co., Inc., December 30, 1983. (3031)

5. EQUIPMENT CERTIFICATION

Background

Another of the very effective techniques for assuring success of the NASA manned space flight programs has been that of equipment certification. Equipment certification is the process by which specific pieces of hardware, generally at the subsytem level or higher, are demonstrated to be capable of meeting the established requirements. Equipment certification has been accomplished by test, by analysis, by similarity and by combinations of test, analysis and/or similarity. The preferred manner of certification when rigor is an objective is by test. The remainder of the discussion in this section is about certification by test.

Certification by test is likely the most expensive way of certifying equipment in terms of up-front money. However, when operation of the equipment being certified is essential for safe and reliable operations in risky and remote environments, it is quite likely that certification by test will result, in the end, being the least expensive method of equipment certification.

The mainstream technical heart of this technique has been composed of rigorous test requirements, integrated test planning, verifiable test procedures, the use of test equipment identical to the flight equipment, very close monitoring of parameters during test, careful inspection after the test, prompt and detailed analysis of the test results, very close team work between contractor and government technical staffs, and frequent and full reviews by management, as in special requests, and as normal business during milestone reviews and during related configuration change control board considerations.

The rigorous testing was provided by the application of test environments selected to represent the normal expected conditions that the equipment would be expected to function in and the worst of the abnormal and emergency conditions that could be anticipated. The selected environments also

included the application of margins (safety factors) when conditions that could possibly get worse were exaggerated for the tests. Included in the tests were operations of the equipment in all of its normal and emergency modes and conditions of operation.

The certification tests were conducted strictly to approved, written test procedures that stemmed from approved integrated test plans; the test procedure accomplishments were fully verified by quality control in real time to ensure achievement of the test requirements, identification and reporting of any problems suspected or encountered during the tests, preservation of the equipment configuration and verification of its pre-test, test and post-test conditions and configuration. It was not unusual for two to three levels of inspectors to participate in the verification of the conduct and completion of the test. These levels would include the prime contractor and the government inspectors. This continued the parallel contractor and government activity where the test plans and test procedures, though generated by the contractor engineering staff were also reviewed and approved by the contractor reliability and quality assurance staffs and given final approval by the government engineering, reliability and quality assurance staffs. These reviews and approvals were carefully documented and became part of the permanent record that received additional attention at each succeeding milestone review, as design change requests were considered for that subsystem by the configuration control board, and whenever failure reports related to that subsystem were being analyzed for corrective action. This very close working arrangement between contractor and government design engineers, reliability engineers and quality assurance staffs, while perhaps unusual in many contractor/government contracts, is typical of the mode of operation in the NASA manned space flight program activities. This arrangement required government staffs that had skills and energy levels well above what had been considered the "norm" in the past in other areas of endeavor.

Much care was taken to assure that equipment to undergo certification testing was identical, in all respects, to the equipment that was to fly. When tests had been completed and then there were changes made to the flight equipment, or in its modes of operation, the certification test was redone with the changed equipment and/or tested in the new mode of operation.

The inspection of the certification test equipment emphasized the usual steps of ensuring that the equipment was of the proper configuration, that the equipment was free of manufacturing defects (special testing was often required for this determination), that the equipment was properly prepared for the test, that the equipment required to support the test was as specified, that the test properly followed the

approved test procedure, and that every problem occurring during the preparations and the testing was properly and promptly documented and reported. In addition, it was usual for the inspection effort to continue after the completion of even the successfully completed tests to determine if any parts of the subsystem, for example, were on the verge of failure; such findings were also documented and reported. Such incipient failures could lead to corrective action, such as redesign, and to retest, depending on the engineering and reliability assessments.

Interfaces

Important interfaces that were exercised during the certification testing periods included: assessment and feedback into the master certification plan of the specific experiences that might affect the certification test requirements of other equipment; information that confirmed or disputed results of special analyses, such as hazard and fault tree analyses and failure mode and effects analyses; information into the failure reporting and corrective action system; accomplishment reports into the configuration management system; experience feedback into the safety assessment activity that might result in modifications to operating procedures or the generation of new ones, and the noting of the accomplishment or lack of accomplishment of the certification test requirements into the program status keeping system and into the information processed for the milestone reviews.

Direct Experience

Additional details about the equipment certification experiences during the manned space flight programs can be found in the available literature, including references 1 through 6. It is believed that the certification test effort applied to the Apollo spacecraft hardware was the most extensive and most thorough of the certification test efforts for any of the manned space flight programs, perhaps of any programs. The experiences of the Mercury and Gemini programs were still very fresh and were applied and extended to reduce the risks of equipment failures on the exacting lunar missions. The specific requirements and techniques are described in detail in the available literature; however, specifics such as vibration levels, temperature and pressure ranges, cycles of operation and duration do not necessarily apply to other activities, such as high level waste repositories. There are certain certification test information items or requirements, perhaps better identified as guidelines that are considered to be well worth considering for application on other activities and endeavors where safety and reliability are important concerns. The significant guidelines that represent a good look at the Apollo spacecraft activities, from reference 6, are as follows:

"a. Test and analysis to demonstrate hardware design capability.
b. Use production hardware.
c. Test at highest practical level of assembly.
d. Use two test articles (one for design-limit testing and one for mission-life testing).
e. Use dynamic, induced and climatic environments.
f. Use combined environments when practical.
g. Test all redundant paths.
h. Perform acceptance test before certification test.
i. Use certification by similarity to eliminate test duplication.
j. Use analysis to supplement tests.
k. Test higher levels of assembly to demonstrate interfaces.
l. Thoroughly understand all anomalies.
m. Implement positive corrective action for anomalies and retest as appropriate.
n. Recertify after design change, process change, manufacturing change, and a change in vendors.
o. Successfully complete all certification tests before flight."

While some relaxation in the amount of hardware dedicated to the certification testing program has occurred as experience has been gained with progression through the NASA manned space flight programs, other certain very important basic guidelines have remained in the certification testing activity into the Space Shuttle Program and are presently recommended, reference 6, by the reliability organization for application to the most recent effort on the Space Station program. The most important of these guidelines are as follows:

a. Use production hardware to accomplish certification testing.
b. Test at the highest level of assembly that is practical.
c. Test all redundant paths.
d. Test or analyze for natural and/or induced environments; test preferred.
e. Impose acceptance tests on the hardware before commencing certification testing.
f. Supplement analysis with testing.
g. Understand and resolve all test anomalies.
h. Certify by similarity where feasible; be positive of the actual similarity.

These guidelines should be considered as minimum certification guidelines to be applied to high level radioactive waste management equipment that is to be used to handle the waste, to provide engineered safety containment barriers and to be used to provide a safe environment for the worker during the times of repository construction and operation. Consideration should also be given to the

adoption of the more pertinent items from the previous list that summarized the guidelines that portrayed the certification test experience of the Apollo spacecraft program.

Operating Philosophy

While much has been written about the requirements and guidelines applied to equipment certification and to certification testing, very little has been emphasized about the operating philosophy, or the people role, that had so much to do with the success of the certification test effort. It is possible that without this operating philosophy/people role that certification test may not have been successful, despite the requirements and the guidelines. This people role, as described earlier in this section on certification test, involved detailed knowledge and close working arrangements between the contractor and government design engineers, reliability engineers and quality assurance people. This resulted in the establishment and maintenance of a substantial data base of engineering information that grew with the overall program and that spread throughout the organizations to the very top as a result of status reports, documentation reviews, correspondence concurrence channels, milestone reviews, configuration control panels and board activities, problem resolutions and everyday conversations. As a result, technical knowledge, supported at the lower levels of the organization with the details and fresh achievements, was so substantial and widespread that at the highest levels of management technical, resource and funding decisions were made accurately and in minimum time periods with appropriate considerations for the program status and predictions for the future.

This knowledge distribution, which is considered to have been a significant contributor to the successes of the manned space flight programs, was so good that the responsible top supervisors, managers and directors, who also had schedule and budget responsibilities, were able to consistently handle large amounts of technical detail and consistently decide the very important issues, such as, "when was all in readiness for launch?" They were also able to penetrate the "fog factors" that generally surrounded remote operational failures with appropriate questions, to sort the recommendations and to consistently make correct decisions. These capabilities need to be understood and reproduced in other activities where safety and reliability are important concerns.

The NASA manned space flight programs experience has avoided a potential equipment certification requirements weakness that has been noted in an earlier assessment of the application of ANSI/ASME NQA-1, which is also identified in reference 7 for application to the DOE effort on the high level radioactive waste repository program. The supplements

in NQA-1 to basic requirement 11, Test Control, references 8 and 9, note in part the following;

> "..... . Required tests, including, as appropriate, prototype qualification test, production test,...."

This wording in the supplement has given rise to an interpretation that prototype equipment can be used to satisfy the equipment qualification (certification in NASA terms) requirements. This is an interpretation that must be corrected! More often than not, prototype equipment is the same as production equipment in concept only; parts, materials, controls, accessories and method and place of fabrication and assembly can differ significantly from the production equipment. Prototype equipment should only be permitted to be used to satisfy the equipment certification test requirement when it can be certified that the prototype equipment is identical to the production equipment and was made with the same processes and on the same production line by people trained in the same way. The wording in Criteria XI of Appendix B, reference 10, while in need of improvement, didn't encourage the erroneous thought that prototype equipment could normally be used to satisfy the equipment certification test requirement.

Benefits

Adoption of the NASA manned space flight programs concept of equipment certification by selecting and tailoring the appropriate certification test guidelines to the needs of the high level waste repository program can provide the DOE with a number of benefits. These benefits include a systematic approach to ensuring that the equipment designed is capable of performing in all of the different modes of operation in all of the possible environments that it may have to operate in or to survive and then later operate. The end result will be to minimize equipment down time for repairs, minimize exposure of work crews to potentially unsafe environments while providing for equipment retrieval and/or repair, and minimize danger to personal injury due to equipment failure during operation. These benefits can be summed, as follows: appropriate application of the equipment certification technique can maximize the possibilities of program schedule completion and minimize the possibilities of program cost and schedule overruns due to equipment deficiencies.

Recommendations

It is recommended that the DOE adopt an equipment certification test approach for the high level waste repository program that includes the minimum guidelines presented herein; that the additional guidelines that describe the approach to the certification test activity used on the Apollo program be considered, on a one-for-one basis, for addition to the minimum list; and that appropriate tailoring be applied to fit this technique to the specific needs of this DOE program.

Time of Application

The equipment certification testing technique becomes active at the time the production articles of equipment become available for test. However, well before that time, it is necessary for the engineering, test and reliability engineers to produce a master test specification, that is derived from the site specification, and an overall test plan. Individual test requirements and test procedures that are complete with pass-fail criteria are then generated and approved before the time of the tests. The approval of the master test specification and of the test plan will be achieved during the design reviews conducted as part of the milestone review technique, also recommended for application by the DOE. Changes to the test documentation, remedies of problems encountered during tests and approval of test completions will be handled by coordination between design engineering, test and reliability engineering and thence as part of the appropriate milestone review activity or the configuration change control activity, which is part of the configuration management technique that is also recommended for application by the DOE.

Anticipated Ease of Technology Transfer

It is anticipated that the transfer of the technical capability to utilize the equipment certification technique from aerospace experience to the DOE high level waste effort will be straightforward since the technique is based upon fundamental engineering. The application of this technique, as through the described operating philosophy and in its utilization by management through the management techniques of milestone reviews and configuration management, is expected to require additional effort to bring about an effective transfer; this additional effort could include the use of lectures and workshops.

Equipment Certification References

1. William M. Bland, Jr. and Lewis R. Fisher, "Reliability Through Attention to Detail", Chapter 38, Manned Spacecraft Engineering Design and Operations, edited by Paul E. Purser, Maxime A. Faget, and Norman F. Smith, Fairchild Publications, Inc., N.Y., 1965. (7011)

2. William M. Bland, Jr. and Lt. Col. Charles A. Berry, USAF, MC, "Project Mercury Experiences", pages 29-34, Astronautics and Aerospace Engineering, February 1963. (9019)

3. NPC 250-1, "Reliability Program Provisions for Space System Contractors", Reliability Publication, NASA, July 1963. (3035)

4. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, 1970. (3023)

5. NHB 5300.4(1D-2), "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program", NASA, October 1979. (3009)

6. JSC-19298, "Certification Approach for Space Station", NASA Lyndon B. Johnson Space Center, September 1983. (3042)

7. DOE Order 5700.6A, "Quality Assurance", U.S. DOE, 8-13-81. (2008b)

8. "A Comparison of 10CFR50, Appendix B and ANSI/ASME NQA-1-1979", Southwest Research Institute, San Antonio, TX. (5002)

9. "Quality Assurance Program Requirements for Nuclear Power Plants". ANSI/ASME NQA-1-1983, American Society of Mechanical Engineers, United Engineering Center, New York. (5003)

10. "Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants". Title 10 Code of Federal Regulations Part 50, 1984. (4001)

6. DATA VERIFICATION

Background

The importance of the verification of data, as obtained from tests, experimentation and exploration, and of the application of data, as in analyses, calculation and prediction, has been stressed by the NASA and by its predecessor agency, the NACA (National Advisory Committee for Aeronautics). The NASA set up a comprehensive review system that served to establish credibility for the scientific results that have emanated from the studies of the rocks and material that have been brought to earth from the lunar surface by the Apollo astronauts. The NACA, much earlier, had also set up a review system that was used to confirm the credibility of its research data and its application in the area of aerodynamics and related sciences.

These review systems, though dealing with different data bases and different application techniques, had several common features that are believed to be of interest and possible application to others who are currently concerned with establishing and confirming the credibility of data and its application in today's environment. These features are described as they were applied to the work of individuals and teams of individuals as they completed work in their areas of scientific endeavor and reported it to the related scientific community with presentations and papers/books; they are presented in the normally applied sequence, as follows:

a. Peer reviews by members of the normal supervisory chain.
b. Formal peer reviews by appointed groups of peers led

by a chairman that was not associated with the immediate organization of the producer of the material under review. Often these appointed groups included members from other, but related, technical activities and from other agencies and/or institutions. Records of comments, resulting adjustments, and decisions were maintained and forwarded to the official files.

c. Open conferences where the new, unusual, innovative and potentially controversial data and their applications were presented and discussed. Audience participation, in real-time and sometimes later, with the individuals reporting their results could influence the final form of the published results. It is suggested that such conferences can be considered as "super peer reviews"; the third in the series of peer reviews.
d. Publication and distribution of the final form of the results.

Examples of the content and the form that a final publication can take are given in references 1-3. These particular examples were the end points of much painstaking work by many people who performed the initial study of the lunar rocks and other material brought to earth by the Apollo 11 astronauts. Along the way to this end point, the authors went through the review system described and passed through a "super peer review", which was the first of a series of annual lunar science conferences sponsored by the NASA Lyndon B. Johnson Space Center. The subsequent lunar science conferences were documented in a similar fashion.

Interfaces

The experiences in successfully dealing with new, unusual, innovative and/or potentially controversial data and the application of such data with the described review systems indicates the benefits of exposing such data and their application to the rigors and trials of peer reviews; peer reviews systematically arranged through comprehensive interfaces with the related scientific community. It is believed that the key ingredient of this success has been the detailed interchanges between the generator/applier/author and the many members of the related scientific community contacted as a result of the series of peer reviews. Such active interfaces possibly led to the establishment of acceptable consensus positions before controversy could become firmly established.

Direct Experience

The experience by the NASA and the NACA described in the **Background** section has been with data that had been gathered under recognized and controlled, but sometimes remote, conditions. In some ongoing activities, as with those of the U.S. EPA (Environmental Protection Agency), there has been need to consider the utilization of a base of data that had not been collected under such favorable and controlled conditions. In a specific investigation being handled at

Love Canal, N.Y., the EPA has had to decide on a course of action that will make the best possible use of data collected by a number of sources, for a number of different reasons, and over a period of years; this effort is reported in reference 4. A description of this EPA effort as it relates to the present discussion is provided by quotes from this reference, as follows:

> "..... Before these data are used in such a highly sensitive and important decision, the TRC has requested that information describing the "quality" of the data be available. ...."
>
> "One of the concerns in using previously collected environmental data has to do with the "quality" of the data. In this case, "quality" refers to several issues:
>
> - Were the samples properly collected, handled, and analyzed, and were the analytical results correctly interpreted and reported?
>
> - Was a numerical value assigned (or can it be) to indicate how close the reported value is to the true value (bias)?
>
> - ....."
>
> "Bias, precision, and detection limits are important QA measurements and are needed by those making the habitability decision. This same information may also be helpful for remedial action decisions and for litigation purposes." Emphasis added.
>
> "This chapter describes the methodology recommended for the QA Review and Assessment Task and includes a general description of the methodology and the criteria to be used to evaluate the "quality of the data. The methodology is a hybrid of several of the alternatives presented in Appendix C, together with the Automated Data Processing (ADP) Methodology. Briefly, the alternatives considered were:
>
> - Existence/Verification of QA Information -- a "bare essentials" approach to determine if certain QA information exists
> - Delphi Technique -- a consensus opinion of experts on the "quality" of various Love Canal environmental monitoring studies
> - ADP Methodology -- use of environmental data without reviewing collection or analytical records
> - Field and Lab Audits -- in-depth audits of protocols used in sample collection and laboratory analysis
> - Phased Approach -- use of several phases of increasing level of detail, with each phase screening data sets for the next
> - Sequential Approach -- review of studies from the

activities in chronological order that produce environmental data"

The above material from reference 4, which describes the EPA's effort to establish the credibility of some previously obtained data, appears to have application, in the broadest sense, to the concerns that the DOE faces in the application of some of the existing older data that is planned to be used in the site characterization phase of the selected high level waste repository site(s). The data and data application concerns of the DOE are likely to be both similar and different from the concerns facing the EPA effort relative to Love Canal. The similarities are believed to be sufficient enough to encourage the DOE to examine the EPA thought process described in reference 4 for application to their high level radioactive waste repository program. The differences may make it necessary for the DOE to enlarge on the EPA process and to also place emphasis on the extensive peer review system utilized by NASA/NACA activities.

Experience suggests the importance of early and substantial effort, as with super peer reviews that culminate in public conferences, to strive for acceptable consensus for technical positions that depend on the application of data with less than substantial pedigrees. Achievement of less than an acceptable consensus relatively early in the program can provide more opportunity to seek alternatives.

Operating Philosophy

Since data and the application of data will form the basis for many significant decisions in the DOE's high level radioactive waste repository program, it is apparent that the operating philosophy most important to apply is a combination of attention-to-detail and early and complete exposure to establish a favorable consensus. Such attention has to be paid to ensure that data used to support significant decisions, including those related to the licensing process, are what they are portrayed to be, that they are applicable to the task to which they are to be applied, and that they are interpreted and applied correctly; application of the proper thought and review processes and a thorough peer review process can be of positive assistance in the achievement of success.

Benefits

The benefits attainable from appropriate application of the data verification technique include the following: maximizing the possibility of withstanding criticism of DOE siting decisions and recommendations; and minimizing the possibility of adverse technical and legal decisions during the NRC license hearing process.

Recommendations

It is recommended that the DOE adopt a data verification technique, as described herein, that is based upon a multiple

number and level of peer reviews that reflect the NASA/NACA experience; and that the DOE strongly consider generation of an old data verification/review process similar to that developed by the U.S. EPA for the Love Canal investigation, but modified to meet the specific needs of the DOE for verification/validation of the older data that is to be used to support significant decision points in the high level radioactive waste repository program.

Time of Application
In consideration of the state of the high level radioactive waste repository program and the need to have the data verification technique ready to apply at the onset of the site characterization work, development of the technique should be started now.

Anticipated Ease of Technology Transfer
It is anticipated that the transfer of the technology for the part about the establishment of the recommended multiple number and level of peer reviews, based on the NASA/NACA experience, can be readily accomplished in a minimum of time. However, it is anticipated that adaptation of the thought process developed by the U.S. EPA on the Love Canal study to the data problems of the DOE will require the direct assistance of U.S. EPA personnel with applicable experience in data concerns in a series of workshop-type meetings.

Data Verification Technique References
1. "Proceedings of the Apollo 11 Lunar Science Conference, Volume 1, Mineralogy and Petrology", Pergaman Press, 1970. (7051)

2. "Proceedings of the Apollo 11 Lunar Science Conference, Volume 2, Chemical and Isotope Analyses", Pergaman Press, 1970. (7052)

3. "Proceedings of the Apollo 11 Lunar Science Conference, Volume 3, Physical Properties", Pergaman Press, 1970. (7053)

4. EPA 86.2L05 (Task 7), "Love Canal Environmental Data Quality Assurance Review and Assessment Methodology", U.S. EPA Hazard Site Control Division, September 20, 1984. (7029)

C. Management Techniques

1. MILESTONE REVIEWS

Overview
Like many other techniques that have been developed for a particular activity, the management technique known as milestone reviews grew from very humble beginnings, without extensive planning and without developed procedures, to fill a specific perceived need in the NASA manned space flight programs. The need was to provide the assurance that everything was in the proper state of readiness for the next

major step in a program; initially the program for NASA was the Mercury Manned Spacecraft Project and initially the "next step" being considered was the launch of an unmanned version of the intended Mercury manned spacecraft. Guidance in setting up these first milestone reviews, often called Launch and Flight Readiness Reviews, came from the personal experiences of the principal managers involved and from supporting industry and armed services advisors.

As experience was gained in the manned space flight programs and in the use of milestone reviews, this review concept was applied at other important phasing points in the programs; and the application of the individual review procedures and supporting services was tuned to fit the specific management and technical needs.

At the current stage of development, as described in the following paragraphs, the milestone reviews technique is very much in tune with the specific needs of the NASA manned space flight programs and can also be seen as filling a very vital spot in the larger management concept of configuration management, which is discussed as a management technique suitable for technology transfer in another section of this document. The very close association of the development of the milestone reviews technique with the NASA manned space flight program does not lessen its potential effectiveness for use in the DOE's effort in implementing the high level radioactive waste repository program defined in the Nuclear Waste Policy Act of 1982. To the contrary, the DOE can benefit from the developmental process that has already occurred with the milestone reviews technique and with assistance from people experienced with the application of the milestone reviews technique, readily tailor guidelines and procedures to fit their own specific needs.

Application of the milestone reviews process to the DOE's high level radioactive waste program can also provide other benefits that could significantly ease the burden of the required licensing interface with the Nuclear Regulatory Commission. The milestone reviews technique can provide a mechanism on timely basis for providing the NRC, through appointed representatives to the milestone reviews, with current technical information and for giving the NRC representatives the opportunity of expressing concerns related to licensing in real time during the milestone reviews. This type of interface with the NRC will, obviously, require some adjustments to the usual way of doing business between the regulator (NRC) and the licensee (DOE); it could also result in changes in the way that the licensee has been preparing and submitting licensing information to the regulator and in the way that the regulator has been accustomed to responding to licensing requests of the licensee.

Attachment A of this section of this document includes

guidelines for possible DOE milestone reviews applied to high level radioactive waste repositories; provisions are included in these guidelines for a NRC licensing interface.

Background

In its experience with the manned space flight programs, NASA has developed the management technique of milestone reviews to the point that it is recognized as a major management tool for assuring the success of their programs. A description of the early application of such reviews just prior to the launch of a Mercury Project spacecraft is given in reference 1. A quotation from this reference illustrates the perceived value of these early reviews, which became known as FRRs (Flight Readiness Reviews), is as follows:

> "Technical reviews, attended by top management, probably constituted the most significant management tool used in Project Mercury to insure that the proper attention had been given to necessary details. These reviews were held in the days just before launch, and preparations for them proceeded simultaneously with the launch preparations. ..... Mercury launchings will not take place in the face of known troubles or in the face of unresolved doubts of any magnitude that affect mission success or flight safety."

Today, with appropriate adjustments of wording to relocate the activity to the high level waste repository arena of action, the above philosophy could be reflected in the DOE instructions for milestone reviews.

The development of the milestone reviews technique continued with the experiences of the NASA manned space flight programs and with the responsibilites assigned to the reliability and quality assurance functions, and later also to the safety function, to the support of these programs. This development is documented by requirements that were levied by NASA headquarters offices on contractors and supporting government agencies and on the implementing NASA major field offices through the reliability and quality assurance functions as noted, for example, in references 2 through 9.

To fit the needs of NASA management and the technical requirements of newer programs and to reflect the growing experience with this review process as detailed requirements and as individual milestone reviews were added, altered, named and renamed, the milestone reviews technique was developed as can be seen, at least to a limited extent, in these references. For instance, reference 2 contains a requirement for "End-Item Tests and Final Inspection". This requirement was only a beginning; it led a little later to a major milestone review that was often called a CARR (Customer Acceptance Readiness Review), which for the NASA manned space flight programs was significant enough to involve major

managers and large numbers of engineers of the NASA and the contractors.

Reference 3, as another example, contains the requirement for the contractor to provide design reviews, as follows:

> "It is mandatory that the contractor establish and conduct a formal program of planned, scheduled and documented design reviews at the system, subsystem, and major component level. These reviews shall be comprehensive critical audits of all pertinent aspects of the design, particularly its reliability, and be conducted at all major milestones in the program beginning in the feasibility stage and additionally at various stages in the evolution of the design..... Participation shall be interdepartmental, including personnel from design, fabrication, reliability, quality, parts application and other areas of the contractor's organization, as well as NASA representatives..... The contractor's reliability group, as well as other participating elements of the contractor's organization, shall sign all design review reports to indicate concurrence with the completeness of the review and actions to be taken.....
> .....
> c. Design review reports, including a listing of the representation at the review, a statement of the actions to be taken, and responsibility therefor shall be provided....."

By the time of the Apollo and the Apollo Applications Programs, the definition of the participation of the reliability and quality assurance functions into the various milestone reviews had become more specific and covered more topics, references 7 and 8. As these reliability and quality assurance contributions developed, so did those of the various engineering and test organizations and of the system safety organization; this elaboration applied to the contractor's effort and to the participation of the government management and technical staffs.

As in the normal course of events of human nature, the NASA headquarters requirements for the Space Shuttle Program's application to reliability and quality assurance became more detailed and more specific and, then, also included requirements (provisions) for safety and maintainability in the same basic document, reference 9. Some requirements for safety, reliability and quality assurance participation in the milestone reviews process were also included in this reference. At about this point in the evolution of the milestone reviews process, several management developments that had occurred through experience in the NASA manned space flight programs now became specifically implemented systems in the Space Shuttle documentation. These management developments included the following:

a. integration of the milestone reviews technique into the larger management technique of configuration management, reference 10; and
b. more specific definition of the participants and their responsibilities in the planning, accomplishment, follow up, and documentation of the milestone reviews, reference 10.

As noted in the Preface to reference 9,

> "This publication establishes common safety, reliability, maintainability and quality provisions for the Space Shuttle Program.
>
> NASA Centers shall use this publication both as a basis for negotiating safety, reliability, maintainability and quality requirements with Shuttle Program contractors and as the guideline for conduct of program safety, reliability, maintainability and quality activities at the Centers. ....."

The combination of the guideline action of reference 9 and the instructions of reference 10 resulted in the generation of a number of contemporary documents by the NASA major field centers and their contractors for the implementation of the milestone reviews technique for the Space Shuttle Program. These implementing documents contained a great deal of detail that was maintained in a current condition to reflect the actual operation of the milestone reviews. Some idea of the amount of detail provided in the instructions can be obtained by examining the contents of typical review planning documents, such as references 11 and 12. Reference 11 describes for an Orbiter Configuration and Acceptance Review such things as purpose and scope of the review; systems and documentation identification; procedures to be followed; data requirements; description of review procedure; identification of team members, special teams, and members-at-large; review task responsibility assignments; team minutes and review item dispositions; the sequence of activities through the various review boards; designation of review board membership; review board agenda and minutes; post review activities including board minutes distribution, action status report, closeout resolution, permanent history; review coordination; identification of data to be reviewed; formats for various summary statements and forms; and instructions for the participation of the contractor in the review and for the logistic support expected from the contractor. Similar instructions are provided in the Space Shuttle Orbiter Review Flight Readiness Review Plan, reference 12.

Additional ideas about the scope and detail associated with these reviews can be obtained by examining other implementing documents such as "General Operating Procedure 14" and its Appendix, references 13 and 14, which define the government (NASA Lyndon B. Johnson Space Center) SR&QA staff's

participation in design and hardware milestone reviews for the early part of the Space Shuttle Program effort. Current documentation describing the SR&QA participation in the Space Shuttle Orbiter design and hardware milestone reviews is contained in reference 15. Included in this reference are general responsibilities of SR&QA team members and major organizational elements, instructions to be followed for the different types of milestone reviews, and a wide range of check lists to be used by SR&QA team leaders and by individual SR&QA team members for the various areas to be reviewed in the various types of milestone reviews. More than 70 pages of instructions are contained in this reference.

This discussion of the background of the milestone reviews technique is intended to show that this management technique evolved to satisfy a need; that it matured through application and use; that it is an involved process requiring the attention of management and the application of experienced technical staffs by both the contractor and the customer (the government in the case of the NASA manned space flight programs); and that a great deal of documentation is involved in the milestone review process. It was also intended to imply, through this discussion, that since this milestone reviews technique has been developed and that it played a significant role in the safe achievement of the NASA manned space flight programs objectives, it can be similarly developed and tailored to apply to and assist in the successful achievement of the objectives of the DOE's effort in implementing the NWPA of 1982.

Perspective and Interfaces

It has been noticed that "readiness reviews" have been the topic of a number of conversations and is a term that appears in a number of NRC and DOE documents where, perhaps, it would be more appropriate for the term "milestone reviews" to be discussed and to be used. Because of this, it seems appropriate to present a few words to put "readiness reviews" in perspective with the topic of "milestone reviews" being discussed in this section as a management technique that is considered to be a candidate for technology transfer.

"Readiness review", as used in aerospace and, more specifically, as used in the NASA manned space flight programs, refers to an <u>end</u> point in a series of milestone reviews. This series of milestone reviews generally starts with a sub-series of reviews that have to do with the design process. The reviews of the design process are major events and occur in the early definition phase of the design effort and at selected phases of percent of design completion, such as at 30%, 50% and 90%, in order to ensure that the design work will lead to the product that is desired.

Additional milestone reviews are held after the design phase of work has been completed and the design has taken on form

and substance to the extent that the first article, assembly, or faciltity is essentially complete. These reviews are conducted to ensure that the interpretation of the design is producing the desired product that doesn't contain design flaws that have not been detected during the design review phases, to ensure that the production effort is not also introducing other flaws, and to ensure that the qualification/certification test phase is being properly accomplished and that the results of these tests are being properly incorporated into the design. Names applied to these particular milestone reviews often include Design Engineering Inspections, Design Certificaton Reviews, or First Article Reviews.

Later, in the series of milestone reviews comes the Customer Acceptance Readiness Review; this is the occasion when the customer pays particular attention to the way or the manner in which a produced article, item or facility has been manufactured, constructed and/or assembled. This is the time that particular attention is paid to the way that the basic requirements have been implemented through the drawings and the manufacturing and process specifications to come into existence as the product. Physical inspections with "flashights and mirrors", acceptance and operating tests of the systems and subsystems, and examinations of the dispositions of manufacturing defects and equipment and structural failures and problem reports are carefully done during this milestone review.

Later on, after much exhaustive testing and exercising to affirm that the end item or faciltity is constructed, connected and wired up exactly to the drawings and specifications; after all types of problem and failure reports written on the specific end item and on all related equipments have been examined for accurate disposition; after all supporting equipments have also been similarly tested, verified and been found to be free of defects; after normal and emergency operating procedures have been verified for accuracy and appropriate application; after all training requirements have been verified as satisfactory and complete; and after all other worries have been investigated, the final end point, the readiness review, is convened to carefully examine all of the analyses, records, documents, test results, and the actions described above to confirm that the item is really ready to operate.

Through this long series of milestone reviews several threads provided continuity and experience. These threads consist of the following:

a. Continuity of people who chair and staff main management boards of the various steps of the milestone reviews.

b. Continuity of people who support the review process and

those who perform the detailed examinations of hardware, software and documentation.

c. Documentation that is provided to support the review and documentation that records all of the decisions and their implementation through the milestone review process and that interacts accurately with the documentation of the configuration management system and becomes part of that system.

There are also the interfacing functions that enable the system of milestone reviews to operate effectively; these interfaces include the following activities:

a. The Configuration Management System, which is the umbrella under which the NASA form of the milestone reviews technique operates; it provides the concise set of documentation that is needed for the reviews. It also provides the configuration control panels for the "day-to-day" decisions and the record of them between the major events in the milestone reviews process.

b. The specialty activities, such as the special engineering analysis techniques which are used to perform double checks (confirmation) on the design process and also identify, for management corrective action, those weaknesses or hazards that the engineering process has not been able to eliminate in its normal course of work.

c. The qualification/certification test activity that "rings out" each piece of hardware and software to prearranged depth and detail to prove, beyond doubt, that it can and will perform as designed in all of the intended environments and in all possible modes of operation.

d. The PRACAS, the Problem Reporting and Corrective Action System, that provides prompt and accurate reporting of all unplanned performances, failures and problems of hardware, software, people, procedures and supporting elements; that ensures thorough analysis and the determination of the cause of the unplanned performances, failures and problems; and that requires the attainment of careful and necessary corrective action and its verification through item c., above.

There are still other interfaces that provide the support to make the milestone reviews technique effective; these other interfaces include all of those described in the discussions of the recommended SRQA techniques and provides for a potentially very effective location for the establishment of a new interface, one not found on the aerospace experience, that of a licensing interface with the appropriate NRC representation.

There are also many organizational interfaces to be

considered. These include those organizations which provide review team participants and participants on the review board.

Of all these interfaces, the one that is most often overlooked or ignored also happens to be the one that has the most significant impact on success; the most important one is the documentation support interface. This interface must provide for each of the milestone reviews current and accurate documentation to the proper level of detail; it must represent the approved configuration at the point in time that corresponds to each of the reviews; it must maintain the record of the review process, including the problems identified, the decisions made, the actions assigned, and it must provide followup to all of the open items and record their eventual closure actions; and it must integrate each of the decisions back into the configuration baseline documentation and provide current and accurate documentation to support the next milestone review event and any configuration control panel/board considerations, assessments, and/or actions that occur in the meantime.

Direct Experience

Assessments of some of the SRQA and management techniques applied through the NASA manned space flight program experiences, as noted in references 16 and 17, note the positive benefits of "special reviews", "factory rollout inspection", "flight safety review", "design reviews", "Customer Milestone Reviews", and "Milestone Reviews" as important contributors to the achieved reliability. These assessments have been made with a bias toward reliability; however, this may prove to be a neutral bias when the statements concern milestone reviews since reliability has been shown during the review of the early requirements documents in the **Background** section to have had early and detailed interest in the accomplishment of milestone reviews that were related to the development of the design.

While there have been differences in the way that milestone reviews have been conducted, when they have been conducted and how they have been identified as NASA has proceeded through the manned space flight programs, several things stand out in a consistent pattern; these are as follows:

a. milestone reviews have been held at the points where the next step in a planned series of steps could be expensive, dangerous, or irreversible if something wrong had occurred in an earlier step and had not been corrected or if something planned to be done had not been done; as in going into manufacturing with an important flaw or omission in the design, as in accepting delivery of an item that was incomplete or had not been built to the approved drawings, and as in committing an item to test or to use when

it had not been completed or had not been completely prepared.

b. Certain milestone reviews were chaired and staffed by the government with persons from the main field office staff with participation from their headquarters staff; contractors, mostly, and main field office staffs provided presentation and documentation material.

c. Other milestone reviews were chaired and staffed by the government with persons from the headquarters staff with participation from government main field office staff; contractors and main field office staffs provided presentation and documentation material.

d. Continuity of participants and of documentation was a priority concern.

e. Participants, presenters and documentation consistently reflected "attention-to-detail".

In preparing for the new NASA manned space flight program that is to involve a space station, there has been reflection by the NASA Lyndon B. Johnson Space Center reliability organization on the experiences of the past programs to identify lessons learned that will be beneficial to apply to this new program. In doing this they have collected, in reference 18, these lessons learned from doing milestone reviews and the major features of effective milestone reviews. The most relevant lessons learned and features with potential for application to the DOE's effort in implementing the NWPA of 1982 from this reference are repeated below and then interpreted as appropriate.

"Efficient management of the Space Station Program dictates that effective controls of the program activities be established. These activities are documented, baselined, and subsequently controlled by a configuration management process which is strongly interwoven with the milestone review process."

This reference identifies the basic tasks of the configuration management process as the following:

a. Configuration identification.
b. Configuration change control.
c. Configuration accounting.
d. Configuration verification.
e. Configuration status reporting.

Definitions of these tasks is included in a following section of this document entitled, "Configuration Management Technique".

Reference 18 further ties the milestone reviews technique into the configuration management process with the following description.

> "The above tasks of the configuration management process must be implemented effectively for the milestone review process to be successful. As such, milestone reviews are considered to be an integral part of the configuration management activity. Participation in the reviews by responsible configuration management personnel is necessary. The milestone reviews .... can be viewed as the primary mechanism by which each task of configuration management is officially implemented."

In addition to the above description, from reference 18, of the role that the milestone reviews play in the larger management technique of configuration management, the reader must also understand that this role may not be the primary mechanism and certainly isn't the only mechanism by which the tasks of configuration management are implemented. The milestone reviews do accomplish most of the configuration verification task just by the very nature of how these reviews are conducted. Examples are given by the efforts of the reviewers during the design milestone reviews when emphasis is placed upon ensuring that the design requirements and the designated design standards have been incorporated; and by the efforts of the reviewers during configuration milestone reviews when emphasis is placed upon ensuring that the drawings and specifications are accurately and completely reflected by the hardware/software.

The major milestone reviews envisioned in reference 18 for application on the NASA Space Station Program are listed and described below. With the use of these descriptions it may be possible to match up appropriate milestone reviews with the DOE program phases at each major repository site selected for implementation of the NWPA of 1982. The following has been quoted from reference 18.

> "2.1 INTERFACE REQUIREMENTS REVIEW. This review will include all major Space Station Program participants and will be chaired by the Space Station Program Manager or his designated representative. The purpose of the IRR is to review the contractor's conceptual approach of the program and to establish the interface requirements for the program elements. The result of the IRR is to establish the conceptual definition of the program.
>
> 2.2 SYSTEM REQUIREMENTS REVIEW. This review will include all major Space Station Program participants and will be chaired by the Space Station Program Manager or his designated representative. The purpose of the SRR is to establish the requirements of and the conceptual approaches to meeting the requirements of the program,

project, system, or task. The configuration plans and requirements, mission objectives, and conceptual approach are established during the SRR. The ultimate goal of the SRR is the approval of the requirements baseline for the program, project, system, or task.

2.3 SYSTEM DESIGN REVIEW. This review will include all major Space Station program participants and will be chaired by the Space Station Program Manager or his designated representative. The purpose of the SDR is to assure that all of the final system design approach definitions are compatible with the program objectives and the mission requirements. In addition, the overall system integration and test program are reviewed. The SDR completes the system definition and preliminary design phases of the program.

2.4 PRELIMINARY DESIGN REVIEW. This review will be conducted by each of the responsible NASA project offices and will be chaired by the project manager. The purpose of the PDR is to review the basic design approach to assure compatibility with the program and project requirements and the producibility of the design approach. The PDR process includes approval of the basic design conceptual approaches, confirmation of the design requirements, and evaluation of the progress and technical adequacy of the design approach. It determines whether the selected design conceptual approach is compatible with the planned end item. The result of the PDR is the authorization to the contractor to proceed with the detailed design planning and development in accordance with the reviewed design approach and interface requirements. The end-item specification is baselined during the PDR and placed under configuration change control.

2.5 CRITICAL DESIGN REVIEW. This review will be conducted by each of the responsible NASA project offices and will be chaired by the project manager. The purpose of the CDR is to verify that the detailed design meets the specified requirements and to determine whether the end-item is ready for manufacture. The CDR should be conducted when the detailed design is approximately 90 percent complete. The CDR verifies that the design still conforms to the requirements established at the SRR, confirmed at the PDR, and updated to the time of the CDR. During the CDR, the integrity of the design is verified through review of the analytical and prototype data, and the system capability is defined through reference to all system engineering documentation. As a result of the CDR, the detailed design baseline is established and placed under configuration change control. In additon, the end-item specifications are updated (pending approval of the change board); test procedures are approved; and specific end-item designs are accepted for release and production.

2.6 CUSTOMER ACCEPTANCE REVIEW. The purpose of the CAR is to assure the customer that the specified product is being provided. A detailed configuration inspection will be conducted and the results presented to the program manager prior to formal acceptance of each major end-item of deliverable hardware/software. This inspection is basically to compare the "as-built" configuration to the "as-designed" requirements and to identify and resolve any differences. The combination of the configuration inspection and acceptance review will formally establish and document the "as-built" configuration of each item of hardware/software at the time of acceptance by the customer. The most significant data output of the CAR is the "Material Inspection and Receiving Report" (DD Form 250), which defines the terms of acceptance, including successfuly completed requirements and waiver items.

2.7 DESIGN CERTIFICATION REVIEW. The purpose of the DCR is to certify the design of the end-item and to evaluate the results and status of the verification planning, testing, and analysis. This review includes the results of operation and performance analysis for the total end-item and interfacing ground support systems. Planning for the DCR is a program/project management function, with the DCR Board being chaired by NASA Headquarters.

2.8 FLIGHT READINESS REVIEW. Immediately prior to the launch of any vehicle or payload, a final review is held to assure the Space Station Program Manager that there have been no technical or documentary discipline oversights resulting in system degradation and that test experience, handling, and transportation subsequent to acceptance reviews have led to no significant concerns with the capability of the flight hardware to perform the mission successfully."

Elsewhere in reference 18, it is noted that the NASA Program Manager generally is the chairman of the Customer Acceptance Review; however, it appears that this appointment may be contingent upon the level of the end-item that is subject to a particular CAR. In some cases the chairman of the CAR may be the NASA Project Manager.

Also, it is noted that the description in the forgoing material of the activity that is expected to take place during the FRR is abbreviated. It is expected that when consideration is given by the DOE in establishing such a review that this description can be made more detailed and more complete so that there would be no misunderstanding of the purpose of an FRR-type review at a DOE repository. It is also noted that the FRR-types of reviews are generally so significant that it is possible that they may be done at two levels. The NASA experience has been that FRRs have been held by the major field centers with headquarters

participation and then later held again, on a wider scope, by headquarters with the field center's participation.

It is anticipated that tailoring the milestone reviews technique to the needs of the DOE effort in the implementation of the NWPA of 1982 will result in modifications to the above milestone review objectives. During the time that the tailoring is done, it should be the objective to also review, for applicability to the DOE programs, the lessons learned from prior experience with the milestone reviews technique that are discussed in reference 18. The subject titles of the lessons learned contained in reference 18 are as follows:

Establishment of program requirements.

Control of electrical, electronic, and electromechanical parts.

Redundancy verification.

Clarity of design criteria and standards.

Accuracy of failure modes and effects analysis/critical items list.

Flexible design review schedules.

Inadequate design verification.

Adequate data accessibility.

Continuity and followup.

In addition to the views and experience that have originated from those who have had experience with the NASA manned space flight programs milestone reviews technique, others have surveyed and analyzed significant activities around the country for methods in use that might also be used to bring improvements to nuclear power plant activity. It is believed that there is enough "closeness" of purpose that the results of these analyses can contribute to this current work. Reference 19, which was a study of space and aviation technology techniques done for the DOE, includes in its recommendations one that notes that

"The utilities involved in procuring and constructing reactors should study NASA's Configuration Management (CM) and select appropriate NASA management tools and techniques".

A detailed discussion of NASA's configuration management system supporting this recommendation included material on milestone reviews that was very similar to that discussed

earlier in this section that was based on material from reference 18.

In another extensive study done by the NRC and some of its contractors, as reported in reference 20, the advantages of design reviews and readiness reviews were discussed; and it was suggested that the NRC should analyze the feasibility of requiring licensees of nuclear power plants to perform such formal reviews. It is believed that the similarity of the endeavors and of the licensing activities make this suggestion applicable for consideration by the DOE in its activity directed toward the high level radioactive waste repositories.

To illustrate the possible features of DOE-conducted milestone reviews at a repository site, a set of guidelines has been generated and a set of milestone events has been identified; these are presented in Attachment A. This work is intended only as an illustration; generation of guidelines for actual events will mostly require close collaboration between repository project experts and those familiar with the planning, implementation, and application of milestone reviews.

It should also be noted that the identified set of milestone events presented in Attachment A contain some suggested milestone reviews that have not yet shown up in the aerospace experience. These milestone reviews have been tentatively identified as Operating Performance Reviews and are applied to the long period of time that the repositories are in an operational mode. Footnote 4 on page 7 of Attachment A provides additional explanation.

Operating Philosophy

From the forgoing discussion it is obvious that the management technique of milestone reviews is a very elaborate system that the NASA manned space flight programs management has believed to be worth the extra effort for assurance toward the success that was attained. In some respects, the milestone reviews technique represents an operating philosophy in its own right. In other respects the milestone reviews technique concentrates into one special activity a number of attributes that come to mind when the NASA manned space flight programs are discussed; these attributes include the following: "attention-to-detail", systematic approaches to accomplishing work, team work, and "making the most of prior experience".

Benefits

The benefits of the application of the milestone reviews technique have been discussed throughout this section as part of the development of the technique. Summarized, these benefits include the following: a systematic way of assuring that the intended program objectives are achieved while minimizing the chances that something will go wrong through

technical or management oversight and/or error; a positive way of providing management with the knowledge needed to be able to most often make correct and timely programmatic decisions; and the generation of a documentation trail that will enable management to locate and fix late appearing problems with the minimum of perturbation and expense to the program.

Recommendations

It is recommended that the DOE adopt the management technique of milestone reviews for application to the high level waste repository program; that this technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of the milestone reviews technique is dependent upon suitable implementation of a configuration management program and the adoption of a number of the SRQA techniques recommended to the DOE in this document. [Note: Additional recommendations on this subject are presented in Attachment A.]

Time of Application

To accrue the maximum benefits from the application of the milestone reviews technique it should be applied at the beginning of the site characterization phase. To be effective at that time, the planning, documentation and training should be completed well ahead of time so that management, staff, support systems, and procedures for both the government and the contractor are ready. It is likely, based on past experience, that emphasis will have to be applied early and often to have the very important documentation system functioning in time to support the beginning of the operation of the milestone reviews technique.

Anticipated Ease of Technology Transfer

While the basic concept of the milestone reviews technique is quite straightforward, it is anticipated that technology transfer for this technique from the NASA to the DOE activity that is implementing the NWPA of 1982 will be difficult to accomplish. This difficulty is anticipated because of the many functional and organizational interfaces that have to function properly to assure success of the process. It is envisioned that the most effective means of accomplishing this technology transfer will involve lectures, workshops, and on-the-job guidance at all working and management levels for the intended participants; additional training will be needed for those who will have the task of planning the reviews and providing the documentation, data, and tracking system and making the support system work.

Milestone Review Technique References

1. William M. Bland, Jr. and Lt. Col. Charles A. Berry, USAF, MC, "Project Mercury Experiences", pages 29-34, Astronautics and Aerospace Engineering, February 1963. (9019)

2. NPC 200-2, "Quality Program Provisions for Space System Contractors", Quality Publication, NASA, April 1962. (3033)

3. NPC 250-1, "Reliability Program Provisions for Space System Contractors", Reliability Publication, NASA, July 1963. (3035)

4. NHB 5300.4(1B), "Quality Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1969. (3024)

5. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1970. (3023)

6. NHB 5300.4(2B), "Quality Assurance Provisions for Government Agencies", Reliability and Quality Assurance Publication, NASA, November 1971. (3007)

7. NHB 5300.1A, "Apollo Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, July 1966. (3036)

8. NHB 5300.5, "Apollo Applications Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, May 1967. (3037)

9. NHB 5300.4 (1D-2), "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program", Reliability and Quality Assurance Publication, NASA, October 1979. (3009)

10. JSC 07700, Volume IV, Book 1, "Space Shuttle Program, Configuration Management Requirements", NASA Lyndon B. Johnson Space Center. (3101)

11. JSC 09705, "Configuration and Acceptance Review Plan for Orbiter", NASA Lyndon B. Johnson Space Center, June 1976. (3109)

12. JSC 16898, "Space Shuttle Orbiter Flight Readiness Review Plan", NASA Lyndon B. Johnson Space Center, June 1981. (3108)

13. JSCM 5312, "JSC Safety, Reliability, and Quality Assurance Manual", General Operating Procedure 14, SR&QA Participation in Design and Hardware Milestone Reviews, NASA Lyndon B. Johnson Space Center. (3005)

14. JSCM 5312, "JSC Safety, Reliability, and Quality Assurance Manual", Appendix A of General Operating Procedure 14, SR&QA Participation in Design and Hardware Milestone Reviews, NASA Lyndon B. Johnson Space Center. (3005)

15. JSC-16081A, "JSC Procedure for SR&QA Participation in

Orbiter & GFE Design and Hardware Milestone Reviews", NASA Lyndon B. Johnson Space Center, March 1982. (3010)

16. Kenneth S. Kleinknecht and Joseph H. Levine, "United States Manned Spacecraft Reliability Experience", NASA Lyndon B. Johnson Space Center, Presented at the International Astronautical Federation XXVth Congress, 30 September - 5 October 1974. (9027)

17. Joseph H. Levine, "NASA Approach to Space Shuttle Reliability", Presentation to the NATO Advanced Study Institute, JSC-18187, NASA Lyndon B. Johnson Space Center, July 1982. (3038)

18. JSC 20181, "Milestone Review Considerations for Space Station Program", NASA Lyndon B. Johnson Space Center, November 1984. (3040)

19. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", prepared for the U.S. DOE by International Energy Associates Limited, U.S. DOE, April 1980. (2004)

20. NUREG-1055, "Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants", U.S. NRC, May 1984. (1002A)

2. Attachment A, GUIDELINES FOR POSSIBLE DOE MILESTONE REVIEW

Overview

The purpose of this Attachment is to describe in broad terms the general arrangements for an example, but nonspecific, milestone review that could fit into the general scheme of the DOE effort in bringing a high-level radioactive waste repository on-line, operating it and taking it through the decommissioning phase. These general arrangements include an interface activity that is designed to enhance the licensing activity with the NRC. Also included is a list of possible milestone review events that could be applied at a repository site.

The material in this Attachment is based upon the material in the previous discussion entitled "Milestone Reviews Technique"; and no references are provided to support the discussion in this Attachment. For actual application to a specific milestone review these guidelines would have to receive specific tailoring to fit the milestone event selected for review, be amplified considerably, and then be used as the basis for specific management instructions and operating procedures.

A **Recommendations** section is included.

Objectives and Benefits

The objective of a milestone review can be generally thought of as an indepth management and technical review of designated program material, documents and hardware/software, to provide assurance that everything is in a state of readiness for advancement to the next major step of the program.

Such a review is expected to be able to confirm that most of the planned work has been effectively accomplished; to identify incomplete, unsatisfactory and undefined work; tp provide action plan assignments of corrective and completing work that has to be accomplished and confirmed before the program moves into the next step. Alternative decisions can result in forgiving all or part of the incomplete, unsatisfactory or undefined work with corresponding modifications to the basic specification and configuration management baseline document or permitting advancement into the next step of the program with certain restrictions being in effect until the correcting and completing work has been completed and confirmed.

The benefits of performing milestone reviews can be summarized as follows:

a. a systematic way of assuring that the intended program objectives are achieved while minimizing the chances that something will go wrong through technical or management oversight and/or error;

b. a positive way of providing management with the knowledge needed to be able to most often make correct and timely programmatic decisions; and

c. the generation of a documentation trail that will enable management to locate and fix late appearing problems with the minimum of perturbation and expense to the program.

Conduct of a Milestone Review

Basically a milestone review is a review of the contractor's work in accomplishing the contract Statement of Work over a designated contract period. Activity on such a review begins with the identification, generation and collection of the appropriate contractor documentation and produced hardware/software. Identified teams of contractor technical and inspection personnel review the documentation and hardware/software and compare it with the baselined specification and design. ("Baselined", as used here, means documents that have been reviewed and approved by the customer and then used as references for subsequent project work and from which project decisions are made.) At the final stages of this contractor review, or as a separate step, identified and prepared customer technical and

inspection teams accomplish an independent review of the same documentation and hardware/software and compare their findings with the contractor teams.

The results of this comparison are documented in a formal system; achievements, open, incomplete and incorrect work, areas of concern or question, and areas needing additional emphasis and appropriate recommended corrective actions are noted. When the customer teams' reviews are complete, the results are formally presented to an appointed customer review board by contractor team members for customer inquiries, discussions and decisions. Where differences of opinion exist between the contractor and customer technical and inspection teams, the customer team members will present the differences and accompanying recommendations in the same formal manner used by the contractor team members.

The appointed members of the customer review board participate in the review by questioning the results presented to the board by the technical and inspection review teams on the basis of their direct knowledge of the program and on the basis of their specific experiences. It is not unusual for board members to identify problems requiring corrective action that are in addition to the problems identified by the technical and inspection review teams. It is the responsibility of the review board to provide the assurance that the review conducted was thorough and that the results represented the real status of the program at that time.

The results of the board review are documented; including the program status, the decisions, the open work and the action items assigned by the board. This documentation is updated as open work is completed and the action items are accomplished; the completed documentation is incorporated into the specification/design baseline to form the new baseline documentation from which subsequent decisions, changes and milestone review will depart.

Important Ingredient

Other than the people involved and their skills and experience, the most important ingredient to the success of a milestone review is the documentation that exists before the review, the documentation provided for the review and the documentation that records the results of the review. The importance of this ingredient is often overlooked; thus the emphasis that is placed here.

Documentation must be provided, generally through the work of the configuration management system, to the review effort that accurately reflects the specification/design as basedlined. This documentation must include the current drawings, specifications, test requirements, problem reports, manufacturing travelers, and so on that reflect the complete and current status of the contractor's work and must be made

available at the assigned time and location to support the reviews of the technical and inspection teams. One may assume that the availability of this documentation is an automatic accomplishment; experience has shown that such an assumption does not reflect real world experience. Special effort is needed by customers and by contractors to achieve consistent success in this effort.

Board Membership and Attributes

Typically, milestone review boards are chaired by the customer's manager of a project. For a DOE high level radioactive waste repository site, the chairman could be the manager of the DOE site project office; possible exceptions to this are noted in the section of this Attachment entitled **List of Possible Milestone Review Events.** Some milestone reviews are suggested as candidates for chairing by a higher authority. Also, typically, the chairman of the milestone review board would be supported by a core board membership and by other board membership. For a DOE site, the core membership is envisioned as being that set of milestone review board members that consistently serve for each of the reviews and would typically consist of the top technical subordinate(s) of the project manager, the quality assurance, reliability, and safety representative(s) on the same organizational level as the project manager, the top technical subordinates of project managers from other DOE HLW sites, and representatives of the DOE Office of Civilian Radioactive Waste Management.

The other board membership is envisioned to consist of other top technical subordinates of the project manager and other special invited participants. These other board members would be invited to participate because of their special skills and experience relative to the agenda of the specific milestone review in which they were invited to participate. These other board members could come from other parts of the DOE, other government agencies, the academic arena and from industry.

The most important attributes of the board membership are specific and related knowledge and experience, ability to ask probing questions relative to the program in review and to assimilate the responses, desire and capability to prepare for the milestone review sessions and the ability to pursue board directed action items to completion. In addition to these attributes, the chairman and the core board membership also need continuity of experience with the milestone reviews at a site.

Technical and Inspection Teams Membership and Attributes

The heart of the milestone reviews action is the membership of the technical and inspection teams. These teams have to be staffed with members specifically knowledgeable in the areas to which they are assigned, whether they be from the customer's or from the contractor's organization. Generally,

it can be expected that the contractor's team members will be more numerous than those of the customer's since they are doing all of the review and most of the presentation to the board. The customer's team members must be skilled in the areas they are assigned to review, since their review must be independent of the contractor's team review; and they must be able to argue their technical positions at least on par with the corresponding contractor's team members.

NRC Licensing Interface

The utilization of the milestone reviews technique by the DOE at the sites that are selected for site characterization and beyond presents an opportunity for the DOE and the NRC to set up an interface activity that can lead to more timely and efficient licensing. To make this opportunity become reality in the way envisioned by this contractor it will be necessary for the DOE to invite certain NRC participation in the milestone reviews, provide the NRC participants with the same notification, documentation and the opportunity of participation as the other milestone review members. This NRC participation would include a position on the milestone review board, similar to that of a core board member, and positions on the technical and inspection review teams.

The NRC, on the other hand, would have to carefully select the appropriate representative to participate consistently as a milestone review board member and would have to support this appointed representative with consistent advisors to prepare this representative for each review with current and "real" licensing concerns and must support the representative with properly constituted NRC technical and inspection team efforts that would participate in the reviews by the DOE and contractor technical and inspection teams.

Special arrangements would include having the NRC board representative serving as a review board member without a vote and being expected to ask questions and receive responses as any other board member. The emphasis of the NRC board member would be in the area of licensing requirements.

To further enhance the performance of this licensing interface, the documentation reflecting milestone review results and the specific decisions and action assignments by the board would identify those parts that were related to the licensing activity.

Because this manner of implementing the licensing interface is different than that described in 10 CFR 60 and in the NWPA of 1982, it will probably be necessary for some adjustments to be made in the regulations to enable the DOE and the NRC to realize the benefits to be gained in reducing the time and effort required to accomplish the licensing effort through the use of this milestone reviews interface.

The actual licensing benefits to be gained will be dependent

upon the quality and the completeness of the milestone reviews as performed for the DOE; the quality of the documentation, as provided for the reviews and as used to record the results of the reviews and of any followup activity; and the performance of the NRC-provided board member and of the NRC technical and inspection review teams participants, their consistency of participation, and the timeliness and quality of the support received by the board member and the team members from the technical elements of the NRC.

Operating Philosophy
The are certain operating guidelines that need to be applied to make the milestone reviews technique effective; these are as follows:

a. provide continuity of people who chair and staff the core board membership and, to the extent possible, for the other board members;

b. provide continuity of people who staff the technical and inspection review teams;

c. work from configuration management baselined documentation;

d. provide a complete trail of documentation of milestone review activity and tie it into the configuration management documentation system at the end of each milestone review; and

e. provide for identification of review documents and results documents that are relevant to the licensing process.

Listing of Possible Milestone Review Events
A list of possible events that could fit into the milestone review technique for a DOE site to be considered for and developed into a HLW repository follows:

Preliminary Siting Plan Review

Siting Plan Review

Siting Data Review (A)

Siting Data Review (B)

Siting Data Review (Etc.)

Final Siting Data Review/Site Recommendation Decision

Preliminary Site Characterization Plan Review

Site Characterization Plan Review

Site Characterization Data Review (A)

Site Characterization Data Review (B)

Site Characterization Data Review (Etc.)

Summary Site Characterization Data Review

Site Preliminary Design Review

Site Design Review/Construction Authorization Request*

Construction Performance Versus Design (10%)

Construction Performance Versus Design (25%)

Construction Performance Versus Design (50%)

Construction Performance Versus Design (90%)

Construction Performance Versus Design (100%)
and Operating License Application*

Delta Construction Performance Versus Design
and Delta Operating License Application as necessary

Operating Performance Review (at 6 months)

Operating Performance Review (at 1 year)

Operating Performance Reviews (at appropriate intervals)*

Preliminary Decommissioning Plan Review

Decommissioning Plan Review

Decommission Review/License Withdrawal Application*

Delta Decommission Review * (as Necessary to Receive License Change)

Notes related to the listed milestone review events:

(1) "*" indicates those milestone review events that are suggested to be chaired by DOE OCRWM.

(2) Operating Performance Reviews have been added to the list of milestone review events to accommodate such occurrences as replacement equipment; changes in design and/or procedures brought on by experience and/or new knowledge; changes in personnel; and to offset the

possibility of project complacency over long stretches of time.

(3) It is suggested that every other one of the Operating Performance Reviews be chaired by DOE OCRWM.

(4) These guidelines have been generated to fit a generalized milestone review for a DOE HLW repository site. When it is decided to apply the milestone review technique to this DOE activity it will be necessary to tailor-make guidelines of this type and specific operating procedures and operating rules for each type of milestone review event.

Recommendations
It is recommended that the DOE establish an operating interface with the NRC through each of the milestone reviews; that the DOE and the NRC agree on what the DOE is to provide to that interface and what the NRC is to bring to that interface; and that the DOE and the NRC agree to develop this interface to enhance the licensing process and to also do what has to be done with the licensing requirements to enable this interface to be effective.

3. CONFIGURATION MANAGEMENT

Overview
The configuration management technique, like the management technique of milestone reviews discussed in an earlier section of this document, developed from small beginnings to fill the needs that were perceived in the early stages of the initial NASA manned space flight programs. The need at first was to provide assurance that equipment used in the test program to prove/verify/certify/qualify that the design was adequate for manned flight was truly the same as the equipment that would be used for the manned flight. It also became apparent, when a design change was being considered to correct some equipment deficiency, that it was important to know accurately the current state of the equipment design that was being considered for change. Soon other needs became apparent; and these too were satisfied by techniques that have become identified with the technique of configuration management.

These early needs can be associated with the need, in the first case, for accurate identification of the test equipment and the flight equipment; and, in the second case, of accurate identification of the design of the equipment at the time that the change to it was being considered. Today's application of the term "configuration management" includes the task of identification and three other tasks; configuration accounting, configuration change control and

configuration verification. Configuration management also is applied to software, specifications, procedures and other documentation, as well as to hardware items. These tasks will be described in more detail in subsequent paragraphs; however, it seems appropriate to note, at this point, that configuration management has been developed into a powerful management tool for the NASA manned space flight programs and for many other complex and expensive projects with emphasis on safety. It seems logical to extend the application of configuration management to other areas of human endeavor that are also associated with complex and expensive projects where safety is an ultimate concern, such as the DOE's effort in implementing the high level radioactive waste repository program defined in the Nuclear Waste Policy Act of 1982.

It should also be noted that at the current stage of development, configuration management as described herein is compatible with the SRQA techniques and with the milestone reviews technique described earlier in this document. Further, it is noted that the milestone reviews technique is one of the primary methods for accomplishing the configuration verification task and that the SRQA techniques provide close support to the milestone reviews and to the deliberation phases of the part of the configuration management technique identified as the task of configuration change control. The application of the management technique of configuration management, in combination with other techniques recommended in this document and other techniques that are needed to satisfy the overall DOE and NRC requirements, can provide a proven, systematic method of approach for the DOE's implementation of the NWPA of 1982.

Background

In its experience with the manned space flight programs, NASA has developed the configuration management technique to the point where it has been recognized as a major contributor to the success of these programs. That the importance of configuration management was recognized early in these programs can be confirmed by the following quotation from reference 1.

> "Engineering, technical configuration, and mission reviews have been held within Manned Spacecraft Center on about a weekly basis to present up-to-date information on proposed technical changes, problem areas, potential problem areas, and test results. At these meetings, the necessary day-to-day decisions were made to keep the program moving along the chosen path.
>
> At other times, development engineering inspections were held at the spacecraft contractor's plant as significant spacecraft approached delivery status. ....."

The larger reviews and inspections performed the configuration verification task and, in combination with the

smaller and more frequent meetings held within the Manned Spacecraft Center, performed the configuration change control task. Key to the success of these meetings and reviews was the documentation provided; complete records of the meetings and reviews were provided quickly and used as the basis for the decisions made with new information at a subsequent meeting or review.

The development of the configuration management technique as applied to the NASA manned space flight programs can be traced through a number of sets of older documentation; one set that is available is the set containing the reliability and quality assurance requirements, as in references 2 and 3 and references 5 through 10. This set of references has been selected for this discussion to demonstrate the long-time involvement of the reliability and quality assurance techniques with configuration management. This involvement continues into the current NASA manned space flight programs with application of the SRQA techniques described earlier in this document.

The development of requirements for contractor and customer (government) quality assurance participation in end item inspections and in the control of changes to important documents, such as, engineering drawings, specifications, and engineering orders related directly to the tasks of configuration verification and configuration identification and accounting, can be seen in references 2, 5, 6, and 8. These references also contain many other requirements for the contractor quality assurance activities to accomplish.

It should also be noted that the customer quality assurance generally made independent assessment reports at the milestone reviews and at other special reviews about the results of their inspections of hardware and documentation. This requirement for independent assessments made it necessary for the customer (government) to have sufficient numbers of people, skills and competency to do these described assessments in addition to accomplishing other independent performance checks of the remaining contractor quality assurance contract tasks.

At about the same time as the requirements were being developed for contractor quality assurance participation in activities associated with early efforts in configuration management, requirements were developed for contractor reliability participation in activities that became aligned with the configuration management technique, as can be read into the descriptions in references 3 and 7. These activities included reliability performing independent checks of design review reports for "completeness and accuracy", ensuring documentation of the results of design review minutes and participation in configuration control panels and board activities to evaluate the effects of the proposed

changes on reliability as these panels and the board were established and began operating.

As in the case of the customer quality assurance independent participation and assessment of contractor activities, it was generally required that the customer (government) reliability organization make independent assessment reports at the milestone reviews and at other special reviews about the results of their reviews of contractor engineering and reliability accomplishments. This requirement for independent assessments made it necessary for the customer (government) reliability effort to have sufficient numbers of people, skills and competency to do these described reviews and to also accomplish reviews of the other contractor reliability tasks to ensure fulfillment of the contract.

The NASA experience with parts of the configuration management task in the early manned space flight program was put to work in the planning and implementation of the Apollo Spacecraft Program. Early in 1964 the Apollo Program Office in NASA Headquarters issued the "Apollo Configuration Manual", reference 4, which had been developed utilizing the experiences of the industry and the services. This manual laid out the fundamental configuration management concept and plan that contributed so much to the success of the Apollo Program. Participation of the reliability and quality assurance staffs in this configuration management work was emphasized in "The Apollo Reliability and Quality Assurance Program Plan", reference 9, by specific assignments of responsibilities. Examples are as follows:

> "Participation in the establishment and exercise of configuration management procedures."
>
> "Verification that the space vehicle hardware end items are described by officially released engineering and that all required engineering changes after hardware delivery from the factory have been installed in the hardware."

Further, paragraph 2.3.7. of reference 9 noted the following:

> "The provisions of NPC 500-1, Apollo Program Configuration Management Manual, constitute the basic requirements to establish uniform configuration management methods and procedures which accurately define all Apollo Program equipment at any point in time. Apollo R&QA program hardware activities at all levels will be based on configuration management techniques required by NPC 500-1."

With the accumulation of the experience gained with the accomplishment of manned space flight programs, NASA, through its headquarters office, prepared for the Space Shuttle Program by issuing new directives and guidelines documents that were tailored to fit the needs of the Space Shuttle

Program. Among these was the document, "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, reference 10. While this document describes in quite a lot of depth the safety, reliability, maintainability and quality assurance requirements for contractors and guidelines for the customer (government), which could be of interest to the DOE, it contains very little reference to the configuration management technique and the participation of the safety, reliability, maintainability and quality assurance with it. The details of the configuration management technique and the interfacing of participants for the Space Shuttle Program are described in a Level II document issued by the NASA Lyndon B. Johnson Space Center, "Space Shuttle Level II Program Definition & Requirements, JSC 07700". Additional details of the related responsibilities of the safety, reliability and quality assurance functions are included in other NASA Lyndon B. Johnson Space Center documents, such as, "Space Shuttle Program Safety, Reliability, and Quality Assurance Plan-Level II". While the 07700 document can be looked upon as a NASA Field Center document because of its point of issue, it is actually a headquarters type of document since it applied to all of the Space Shuttle Program regardless of the NASA Field Center that had specific responsibility for a function. This document could be used as a model to provide assistance to the management of other large and complex programs with significant national impact. Of course, the counterpart of such a document generated for a different program would be tailored to fit the needs of that program. Those considering this NASA document as a model should be aware that it is not and was not intended to be a one-time issue; by plan, it has been updated with change sheets and reissuances because the information contained in it needed to be current in order to be useful.

This Level II document is made up of a number of volumes that present the Space Shuttle Program management requirements, technical requirements and resource requirements. The basic requirement for configuration management is contained in Volume I, reference 11; the detailed requirements are included in Book 1 of Volume IV, reference 12. Some selected parts of these references are quoted and/or discussed below to present the fundamental concepts and some of the operating details of the configuration management system as applied, and as being applied, to the Space Shuttle Program. These selected parts are as follows:

> "... configuration management includes identification, documentation, accounting, change control, and verification functions performed to insure that the "as-built" configuration of particular item of hardware/software is in conformance with an established baseline and authorized changes." (reference 11)

The main four parts of configuration management are established in reference 12 as configuration identification, configuration accounting, configuration change control and configuration verification. Configuration documentation is the service function which ties these four parts together; its well-being and performance are vital to the success of the configuration management technique. Other descriptive quotes from reference 12 are as follows:

> "Configuration identification is the task of determining the manner in which the requirements for and configuration of all program hardware/software is to be described and the documentation of these descriptions."

The configuration identification task includes defining a baseline document(s) from which to work, interface control documents to bridge the gap between participating contractors and other government agencies, acceptance baseline configuration description, requirements traceability, and baseline documentation maintenance. Subjects contained in the Shuttle Program baseline documents include the following: top level requirements, system responsibilities allocations, system schedules, system budget and cost allocations, management system requirements, information requirements, system design and performance requirements, system interface requirements, system verification requirements, training requirements, and acceptance configuration descriptions and indentured parts listings for flight hardware/software.

> "Configuration accounting is the element of configuration management that provides the essential records and reporting of precise configuration data for all Space Shuttle hardware/software. The primary objectives of configuration accounting are as follows:
>
> a. To maintain and disseminate the current configuration data of each program/project element.
>
> b. To maintain correlation among the configuration data of the various equipments, software, and support elements.
>
> c. To maintain current and accurate records of the status of changes completed and in the process."

> "Configuration Change Control. After a baseline is established, it is essential that effective, positive control be established which will preclude any unauthorized changes to that baseline."

Configuration change control includes the establishment of the necessary levels of change control management, often called Configuration Control Boards (CCBs) and Configuration Control Panels (CCPs); the definition of the scope of authorities and responsibilities of each level; the

membership of each level; and the manner in which configuration changes are identified, processed, documented/packaged, coordinated, reviewed, and recorded. The importance of the way proposed changes are documented/packaged is emphasized by detailed instructions concerning the information that must be presented with the proposed changes; the information required varies relative to the source point, level, reason for and type of the proposed change. Experience has shown the definite need for the information defined for use in processing proposed changes.

The importance of technical support to these levels of change control management is illustrated by the detailed procedures set up by the supporting organizations. Examples of such procedures are presented in references 14-16, which contain, respectively, safety, reliability, and quality Operating Procedures through which support is provided to some of these panels.

> "Configuration Verification. Configuration management includes activities associated with assuring that requirements are properly implemented and that the hardware/software is certified as having been designed and built to the correct configuration."

As noted in references 11 and 12, the process of verification is vested largely in the activity that goes into the various milestone reviews. Possibly unlike other experience, the NASA experience in the manned space flight programs has shown the necessity to include requirements under the control of configuration management. Most of the effort in assuring that the requirements are properly implemented occurs in the first several scheduled milestone reviews; the Program Requirements Review (PRR), Shuttle System Requirements Review (SRR), and in the various stages of the design review. Requirements can be processed as proposed changes at other than milestone reviews when necessary. Most of the effort during milestone reviews after the time of the design reviews is spent in certifying that the hardware/software has been built to the correct configuration; the configuration that has been baselined for acceptance by configuration management as illustrated by the configuration summary, reference 13, which contains for each hardware/software part, information such as part number, part nomenclature, serial number and drawing revision. This configuration summary is an important output of configuration management because it represents an accurate accounting of the management decisions during the life of the project.

This discussion of the background of the configuration management technique is intended to show that this management technique, with the help of industry and the services, had evolved to satisfy a need; that it had matured through application and use; that it had played a significant role in the success of the NASA manned space flight programs; and to

imply that it can be developed and tailored to apply to and assist in the successful achievement of the DOE's effort in implementing the NWPA of 1982.

Interfaces

Since configuration management, as described in this document, is at the center of a project's activity, its interfaces include all project and project support organizations and functions. As noted in the description of the milestone reviews technique, configuration management was described as the "umbrella" under which milestone reviews operated. Thus, all of the interfaces to the milestone reviews technique interface with the configuration management activity. There are also the many organizational interfaces that support the configuration change control activity on both the contractor side of the project and the customer (government) side at the meetings of the configuration control boards and panels. In addition there are the functional interfaces which include the SRQA techniques described in this document and others such as training, medical, motivation contracts, legal and still others that are identified as having a specific role in the program.

Direct Experience

Assessments of the experiences of the NASA manned space flight programs have highlighted the effectivenss of the configuration management technique in a number of positive ways, as noted in references 17 through 19. Processes, tasks and actions that were the direct responsibility of the NASA Manned Spacecraft Center (now named the Lyndon B. Johnson Space Center) that contributed to the success of the Apollo Program have been identified in reference 17. Among the important contributors to the success identified was "the control of changes"; this function was part of configuration management at that time, as it is in the present description. A quote from this reference illustrates the way that the changes to the configuration were controlled.

> "... In Apollo we handled all changes through a series of Configuration Control Panels and a Configuration Control Board. The panels considered minor hardware changes early in the development cycle, as well as crew procedures and all computer programs. The Board considered more significant hardware changes, all hardware changes after spacecraft delivery, and procedures or software changes that could affect schedules or missions."

In an act of self assessment in the aftermath of the accident at Three Mile Island nuclear power plant number 2, another power company that had fulfilled the Nuclear Regulatory Commission requirements for a construction permit, investigated management techniques used in high technology projects for potential adaptation to their project. As noted in reference 18, their investigation identified NASA configuration management as a management method that was

"particularly adaptable to nuclear power plants". A particularly interesting description of configuration management from their perspective is quoted, as follows:

> "Configuration Management is a crucial element in the management structure for any complex project. It can provide all elements of management a high level of visibility into conditions within the project, as they exist and as they undergo change. It can provide an efficient framework for ascertaining status and in performing performance surveillance functions. It can greatly enhance safety, reliability and quality assurance activities. It is a major supporting activity that can bring order out of chaos for the manager and the operator."

In another assessment of the possible application of space and aviation technology to improve the operations of nuclear power plant subsequent to the accident at Three Mile Island, a contractor for the DOE, in reference 19, included the following in its conclusions.

> "NASA's style of management, characterized by the terms 'Configuration Management' and 'Configuration Control' is thorough, rigorous, and disciplined. The technique predominately applies to the design of new, complex hardware developed by multiple contractors on a large scale. This management concept is probably the single most important factor which has contributed to NASA's overall safety and reliability."

This same contractor also provided a series of recommendations that resulted from this assessment. One recommendation touched upon configuration management, as follows:

> "The utilities involved in procuring and constructing reactors should study NASA's Configuration Management (CM) and select appropriate NASA management tools and techniques."

It is believed that the results of these assessments, even though some were made specifically for the nuclear power industry, also apply very directly to the DOE effort in the high level radioactive waste repository program because of the need for strong management controls and accurate engineering in the quest for long-term safety.

Operating Philosophy

While the NASA-style of configuration management may appear, in some respects, to be a technique that automatically "does it all", it isn't a system that will automatically provide good results. Without <u>full</u> management support and personal <u>participation</u> in the details of configuration management, it probably won't produce the results that have been obtained by

its application in the NASA manned space flight programs. Configuration management enables all levels of management and the technical staffs, on both the contractor and the customer (government) teams to pay rigorous "attention-to-detail" in a systematic way that is so well-documented that the visibility created minimizes chances for error and oversight.

Benefits

The benefits attainable from the application of configuration management have been noted throughout this section of the document and in the section of this document on the application of the milestone reviews technique. The benefits from both of these techniques are realized here because in the concept presented, configuration management also includes the milestone reviews technique. Summarized, these benefits include the following: a systematic way of assuring that the intended program objectives are achieved while minimizing the chances that something will be missed through technical or management oversight and/or error; a positive way of providing management with the knowledge needed to be able to most often make correct and timely programmatic decisions; and the generation of a documentation trail that will enable management to do a number of things including having the ability to locate and fix late appearing problems with a minimum of perturbation and expense to the program.

The above benefits sound like extensions of the benefits described for the application of the milestone reviews technique; and indeed they should. The main difference is that the application of the configuration management technique includes the application of the milestone reviews technique and completes the management scope of control with the operation of the configuration control panels and the configuration control board, which operate in the intervals between the major events of the milestone reviews.

In addition, there is another benefit to be gained by the application of the configuration management technique; that is the configuration summary. The configuration summary, which is a normal output of the configuration management technique, accurately represents the results of management decisions over the life of the project; it is suggested that the DOE could make use of configuration summaries to form the bases for such other important functions as Q-Lists and lists of items that are important to safety and important to isolation.

Recommendations

It is recommended that the DOE adopt the management technique of configuration management for application to the high level waste repository program; that this configuration management technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of configuration management on their program will be dependent upon suitable

implementation of the milestone reviews technique as part of configuration management, the adoption of a number of the SRQA techniques recommended in this document and other supporting techniques, or their equivalent, and the full backing and involvement of top DOE management associated with this program.

Time of Application
To accrue the maximum benefits from the application of the configuration management technique, it should be applied at the beginning of the site characterization phase. To be effective at that time, the planning, documentation and training should be completed well ahead of time so that management, staff, support systems, and procedures for both the government and the contractor are ready.

Anticipated Ease of Technology Transfer
It is anticipated that technology transfer for this management technique from the NASA to the DOE activity that is implementing the NWPA of 1982 will be difficult to accomplish. This difficulty is anticipated because of many of the same reasons anticipated for the technology transfer for the milestone review technique, namely because of the many functional and organizational interfaces that have to be established and set up with procedures and training. It is envisioned that the most effective means of accomplishing this technology transfer will involve lectures, workshops, on-the-job guidance at all working and management levels; that this transfer be provided by teams of people with actual experience in the planning for, implementation of, and participation in NASA manned space flight configuration management; and that this transfer effort also include those experienced in providing configuration management supporting services.

With a decision to adopt and to apply the configuration management technique, allowance should be made to provide for the comments noted in the section **Anticipated Ease of Technology Transfer** for the milestone reviews technique. Implementation of the configuration management technique should also include implementation of the milestone reviews technique.

Configuration Management Technique References
1. William M. Bland, Jr. and Lt. Col. Charles A. Berry, USAF, MC, "Project Mercury Experiences", pages 29-34, Astronautics and Aerospace Engineering, February 1963. (9019)

2. NPC 200-2, "Quality Program Provisions for Space System Contractors", Quality Publication, NASA, April 1962. (3033)

3. NPC 250-1, "Reliability Program Provisions for Space System Contractors", Reliability Publication, NASA, July 1963. (3035)

4. NPC 500-1, "Apollo Configuration Manual" NASA Headquarters Publication, May 18, 1964.

5. NPC 200-1A, "Quality Assurance Provisions for Government Agencies", NASA Quality Publication, June 1964. (3032)

6. NHB 5300.4(1B), "Quality Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1969. (3024)

7. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication,, NASA, April 1970. (3023)

8. NHB 5300.4(2B), "Quality Assurance Provisions for Government Agencies", Reliability and Quality Assurance Publication, NASA, November 1971. (3007)

9. NHB 5300.1A, "Apollo Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, July 1966. (3036)

10. NHB 5300.4 (1D-2), "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program", Reliability and Quality Assurance Publication, NASA, October 1979. (3009)

11. JSC 07700, Volume I, "Space Shuttle Program, Program Definition and Requirements Baseline", NASA Lyndon B. Johnson Space Center. (3049)

12. JSC 07700, Volume IV, Book 1, "Space Shuttle Program Configuration Management Requirements, Level II Program Definition and Requirements", NASA Lyndon B. Johnson Space Center. (3101)

13. JSC 07700, Volume IV, Book 2, "Space Shuttle Program Configuration Management Requirements, Level II Program Definition and Requirements, Space Shuttle Configuration Summary", NASA Lyndon B. Johnson Space Center. (3100)

14. JSCM 5312, "JSC Safety, Reliability, and Quality Assurance Manual", General Operating Procedure #2, SR&QA Participation in Hardware Change Evaluation and Configuration Control Boards and Panels, NASA Lyndon B. Johnson Space Center. (3005)

15. JSCM 5312, "JSC Safety, Reliability, and Quality Assurance Manual", Safety Operating Procedure #6, Safety Program Management - System Software Hazard Analysis, Change Evaluation, and Change Control Board Participation, NASA Lyndon B. Johnson Space Center. (3005)

16. JSCM 5312, "JSC Safety, Reliability, and Quality Assurance Manual", Quality Operating Procedure # 4.18,

Evaluation and Processing of Change Requests, NASA Lyndon B. Johnson Space Center. (3005)

17. NASA SP-287, "What Made Apollo A Success?", NASA, 1971. (3099)

18. Thomas N. Ewing and William R. Poque, "Configuration Management for Black Fox Station Nuclear Project, A PSO response to TMI", Presented to Frontiers of Power Conference, Oklahoma State University, October 13, 1980. (7013)

19. DOE/TIC-11143, "Application of Space and Aviation Technology to Improve the Safety and Reliability of Nuclear Power Plant Operations", prepared for the U.S. DOE by International Energy Associates Limited, U.S. DOE, April 1980. (2004)

D. Other Techniques

Overview

Three other techniques are introduced in the paragraphs below. The necessary references to provide full discussions of these techniques are not available for this study. However, the potential usefulness of these techniques to the DOE for application to the high level radioactive waste repository program is believed to be so great that the information that is available is presented.

1. MATERIALS QUALIFICATION AND TRACEABILITY

Background

The NASA manned space flight program developed a system for identifying materials used in certain critical functions and requiring that these materials be qualified to certain specifications, those specifications that were necessary to be met in order for the material to do its intended task. Further, it was required that systems be established to certify that the material was, indeed, as identified, to record the history of the material from its source and to provide records of where the material was applied and its history after application. Some idea of these requirements, relative to the reliability and quality assurance activities on the Apollo program, can be obtained from the information in references 1 - 3. Examples of some of these requirements are as follows:

From Reference 1.

> "Each article and material shall be identified by a unique part or type number. Where control of individual articles or lots of materials is required, one or more of the following detailed identification methods shall also be used, as applicable:

1. DATE CODES .....

2. LOT NUMBERS .....

3. SERIAL NUMBER .....

4. OTHER IDENTIFICATION .."

"..... Records for articles and materials shall indicate applicable part or type numbers and associated detailed identification. This shall provide the capability of tracing backward to the material from which fabrication originated and forward to determine the location of like articles or materials within a level of process or assembly. ....."

An experience in the Apollo program is described to emphasize the importance of control of materials and of the information concerning the source, history and application of the material. At one point in the program, during the acceptance testing phase, a failure occurred in a propellant tank. The cause of the failure was traced to some minute impurity that the tank material had been subjected to in its prior normal cleansing and testing routine. Months later, flaws in the material caused by this impurity reacted with another normal testing fluid and caused the failure. This experience resulted in the identification of a new failure mechanism and caused the rejection of a number of tanks that had been exposed to what had previously been thought of as a benign environment.

Without the benefits of the information furnished by this technique, the problem may never have been solved. In addition the impact may not have been limited to just the tanks that had been through the specific environment that had been determined to be bad; and there may not have been a way to identify those particular tanks from all of the other tanks that had already passed through the process and did not have the bad exposure.

Benefits

The application of this technique to certain materials, such as those used in the engineered barriers, the high-level waste form and the high-level radioactive waste cannisters, can provide the DOE with information needed to limit the impact of unexpected reactions of selected materials with the environment or with a combination of process and environment effects. The application of this technique to transportation devices to be used in moving the high level radioactive wastes from temporary storage sites to the repository site can provide similar benefits.

2. FAILURE MODES AND EFFECTS ANALYSIS AS APPLIED TO PROCESSES

Background
The recent development of an analysis technique with apparently a great potential for identifying potential weaknesses in processes has been announced, as noted in reference 4. This analysis technique applies the thought process of the standard FMEA (failure modes and effects analysis) to processes; processes being defined for this discussion as any step-by-step activity used to fabricate, construct, assemble, produce, etc. something. This application of the FMEA provides a logical and systematic approach to each step in such processes and can identify undesired effects of mistakes or oversights. Once identified these mistakes and oversights can be eliminated or controlled so that the product is not degraded and its performance is assured.

This application of the FMEA is new, but the thought process is similar to the application of the FMEA to hardware. It is believed that the potential for savings is large with the application of the FMEA to processes.

Benefits
The application of this technique by the DOE to the transportation, construction, installation and operational phases of the high level radioactive waste repository program will provide a systematic way of identifying potential weaknesses in the process early in the program when corrective action can be applied with minimum impact.

3. RELIABILITY CENTERED MAINTENANCE

Background
The reliability centered maintenance technique was originated to improve the maintenance and the economics of the commercial airline operating industry. It has been so successful that it has also been adopted by the U.S. Department of Defense for military equipment and put into practice with the help of the textbook described in reference 5. From these applications, it can be correctly surmised that reliability centered maintenance has been originated to be applied to complex, expensive equipment.

A description of this textbook, "Reliability Centered Maintenance", in reference 5 also fits the technique and can serve to describe reliability centered maintenance in broad terms; it is as follows:

> "..... The net result of this analytic tool is a structured, systematic blend of experience, judgement, and specific information to determine which maintenance tasks, if any, are both applicable and effective for those items whose failure has significant consequences for the

equipment in which they are installed. ....."

Also, the potential application of reliability centered maintenance to other equipment is described in reference 5, as follows:

> "The widespread and successful application of RCM (reliability centered maintenance) principles in the air-transport industry has important implications for many types of complex equipment other than aircraft. Many of the current problems with rapid-transit equipment, fleets of ships and ground vehicles, and even machinery used in complex manufacturing processes indicate that the relationship between design and maintenance is not clearly understood. .....RCM analysis does provide a means of identifying the specific maintenance tasks and product improvements that will alleviate such problems."

The contribution of the technique of reliability centered maintenance to the high level radiaoactive waste repository program will likely be centered around the transportation system that is to move these wastes from the locations of temporary storage to implacement in a repository. The significance of a trouble-free transportation system that is not also cost prohibitive is self-evident, particularly where it interfaces with the public.

Benefits

The application of this technique to the transportation system that is to move the high level radioactive wastes from temporary storage locations to implacement in a repository can be expected to increase the reliability of the system; this will provide for greater safety to the public and to the workers.

Recommendations for Other Techniques

It is recommended that the DOE study, for possible adaptation to the high level radioactive waste repository program, three other aerospace techniques; materials qualification and traceability, failure modes and effects analysis as applied to processes, and reliability centered maintenance.

Other Techniques References

1. NHB 5300.4(1B), "Quality Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1969. (3024)

2. NHB 5300.4(1A), "Reliability Program Provisions for Aeronautical and Space System Contractors", Reliability and Quality Assurance Publication, NASA, April 1970. (3023)

3. NHB 5300.1A, "Apollo Reliability and Quality Assurance Program Plan", Office of Manned Space Flight, NASA, July 1966. (3036)

4. J.H. Levine, Draft Presentation Charts, "Failure Mode and Effects Analysis - An Approach to the Evaluation of Processes", NASA Lyndon B. Johnson Space Center, Reliability Division, February 1985. (3124)

5. F.S. Nowlan et al, "Reliability Centered Maintenance", AD/A066 579, United Airlines, San Francisco, December 1978. (7034)

SECTION IV. RECOMMENDATIONS

Recommendations from the technique discussions in the previous section of this document are identified in the following listing. In addition, there are some other recommnedations included that stem from an integration of some portions of the technique discussions that warrant additional emphasis.

1. It is recommended that the DOE adopt the system safety technique and the specialized safety analysis techniques, as described, for use in the implementation of the activities associated with the NWPA of 1982; and that consideration be given to tailoring the requirements of these techniques to fit the specific needs of the high level radioactive waste repository program sites and of the waste transportation system.

2. It is recommended that the DOE adopt the utilization of the FMEA (Failure Mode and Effects Analysis)/CIL (Critical Items List) technique, as described, for use in the implementation of the activities associated with the NWPA of 1982; and that the degree of development of this technique as applied to the Space Shuttle program would be a reasonable level to apply to the high-level waste repository engineering program, with some tailoring of the technique to accommodate differences between the two programs. Application of this technique should also be considered for the waste transportation system.

3. It is recommended that the DOE adopt the methodology and the operating philosophy of the NASA PRACAS (Problem and Corrective Action System) technique, as described, for use throughout the DOE and the DOE-contractor efforts related to the implementation of the NWPA of 1982; and that consideration be given to applying this technique as one system, from the top, in a tailored fashion to form the bases for satisfying the reporting and assessment, management, licensing and administrative requirements.

4. It is recommended that the DOE adopt the EEE parts control technique, as described. It should be tailored to fit the specific needs of the DOE efforts associated with the implementation of the NWPA of 1982.

5. It is recommended that the DOE adopt an equipment certification technique test approach for the high level waste repository program that includes the minimum guidelines, as described; that the additional guidelines that describe the approach to the certification test activity used on the Apollo program be considered, on a one-for-one basis, for possible addition to the minimum list; and that appropriate tailoring be applied to fit this technique to the specific needs of this DOE program.

6. It is recommended that the DOE adopt a data verification technique, as described, that is based upon a multiple number and level of peer reviews that reflects the NASA/NACA experience; and that the DOE strongly consider generation of an old data verification/review process similar to that developed by the U.S. EPA for the Love Canal investigation, but modified to meet the specific needs of the DOE for verification/validation of the older data that is to be used to support significant decision points in the high level radioactive waste repository program.

7. It is recommended that the DOE adopt the management technique of milestone reviews for application to the high level waste repository program; that this technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of the milestone reviews technique is dependent upon suitable implementation of a configuration management program and the adoption of a number of the SRQA techniques recommended to the DOE in this document.

8. It is recommended that the DOE establish an operating interface with the NRC through each of the milestone reviews established as a result of implementation of the milestone reviews technique; that the DOE and the NRC agree on what the DOE is to provide to that interface and what the NRC is to bring to that interface; and that the DOE and the NRC agree to develop this interface to enhance the licensing process and to also do what has to be done with the licensing requirements to enable this interface to be effective.

9. It is recommended that the DOE adopt the management technique of configuration management for application to the high level waste repository program; that this configuration management technique be based on the NASA experience and tailored to fit the specific needs of the DOE program; and that it be recognized by the DOE that the effectiveness of configuration management on their program will be dependent upon suitable implementation of the milestone reviews technique as part of configuration management, the adoption of a number of the SRQA techniques recommended in this document and other supporting techniques, or their equivalent, and the full backing and involvement of top DOE management associated with this program.

10. It is further recommended that the DOE study, for possible adaptation to the high level radioactive waste program, three other aerospace techniques briefly identified in the discussion material; these other techniques are material qualification and traceability, failure modes and effects analysis as applied to processes, and reliability centered maintenance.

11. It is recommended that the DOE pay particular attention to the interfaces of the techniques that are adopted, how

these interact with each other and how they will interact with the existing and planned techniques employed by the DOE and DOE-contractors; these interfaces and their interactions are key to the success of the recommended techniques.

12. It is recommended that in implementing these recommendations that the DOE consider multiple modes of communications for accomplishing the transfer of technology that include the use of presentations, lectures, workshops, pilot programs and on-the-job guidance. The modes selected for a specific technique will depend upon the complexity of the technique and the experience level of the staff that is to implement the technique.

SECTION V. CONCLUDING REMARKS

Aerospace SRQA and management techniques, principally those developed and used by the NASA Lyndon B. Johnson Space Center on the manned space flight programs, have been assessed for possible application by the DOE and the DOE-contractors to the high level radioactive waste repository program that results from the implementation of the NWPA of 1982. Those techniques believed to have the greatest potential for usefulness to the DOE and the DOE-contractors have been discussed in detail and are recommended to the DOE for adoption; adoption by the DOE will include the need for some tailoring of the detailed application of these techniques to fit the specific needs of the DOE program.

The recommended SRQA techniques are system safety; failure modes and effects analysis/critical items list; problem reporting and corrective action system; electrical, electronic and electromechanical parts control; equipment certification; and data verification.

The recommended management techniques are milestone reviews and configuration management; included is a companion recommendation that the milestone reviews technique include provisions for a licensing interface with the NRC.

In addition, three other techniques were identified as important for the DOE to study for possible adaptation to their program; these are materials qualification and traceability, failure modes and effects analysis as applied to processes, and reliability centered maintenance.

Other recommendations identified the importance of interfaces related to the recommended techniques and identified the various means for transferring the technology from the NASA and other places to enable the effective use of the recommended techniques.

It is noted that the intent of the above recommendations is to provide the DOE with techniques to supplement current and planned activities; there is no intent that these recommended techniques summarily replace any of the DOE current and planned activities. It is possible that some of the recommended techniques can be adapted to current DOE activities and implemented to supplement specific DOE activity already underway or planned for future application. In other cases, the DOE may have activities similar to some of the recommended techniques; in those instances the DOE need not adopt the recommended techniques. It is urged that the DOE explore beyond any name similarities before deciding on the degree of implementation to apply to the recommended techniques. The DOE is also urged to carefully consider the

total impact of not implementing a specific recommended technique. The strong interaction between the techniques, as noted in the interface discussions, may make the impact of not implementing a specific technique greater than just the loss of benefits associated with that specific technique.

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)

NUREG/CR-4271

2. TITLE AND SUBTITLE

Recommended Safety, Reliability, Quality Assurance and Management Aerospace Techniques with Possible Application By the DOE to the High Level Radioactive Waste Repository Program

3. LEAVE BLANK

4. DATE REPORT COMPLETED

MONTH	YEAR
March	1985

5. AUTHOR(S)

William M. Bland, Jr.

6. DATE REPORT ISSUED

MONTH	YEAR
June	1985

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Management and Technical Consulting
Division of GeeB's Inc.
18575 Martinique Drive
Houston, TX 77058

8. PROJECT/TASK/WORK UNIT NUMBER

Task 2

9. FIN OR GRANT NUMBER

FIN D1014

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Waste Management
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555

11a. TYPE OF REPORT

Final Technical Report

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

Aerospace SRQA and management techniques, principally those developed and used by the NASA Lyndon B. Johnson Space Center on the manned space flight programs, have been assessed for possible application by the DOE and the DOE-contractors to the high level radioactive waste repository program that results from the implementation of the NWPA of 1982. Those techniques believed to have the greatest potential for usefulness to the DOE and the DOE-contractors have been discussed in detail and are recommended to the DOE for adoption; discussion is provided for the manner in which this transfer of technology can be implemented.

Six SRQA techniques and two management techniques are recommended for adoption by the DOE; included with the management techniques is a recommendation for the DOE to include a licensing interface with the NRC in the application of the milestone reviews technique. Three other techniques are recommended for study by the DOE for possible adaption to the DOE program.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS

Quality Assurance
Reliability
Safety
Radioactive Waste Management
Program Management
Aerospace Industry

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT

Unlimited

16. SECURITY CLASSIFICATION

(This page) Unclassified

(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FOURTH CLASS MAIL
POSTAGE & FEES PAID
USNRC
WASH. D.C.
PERMIT No. G-67