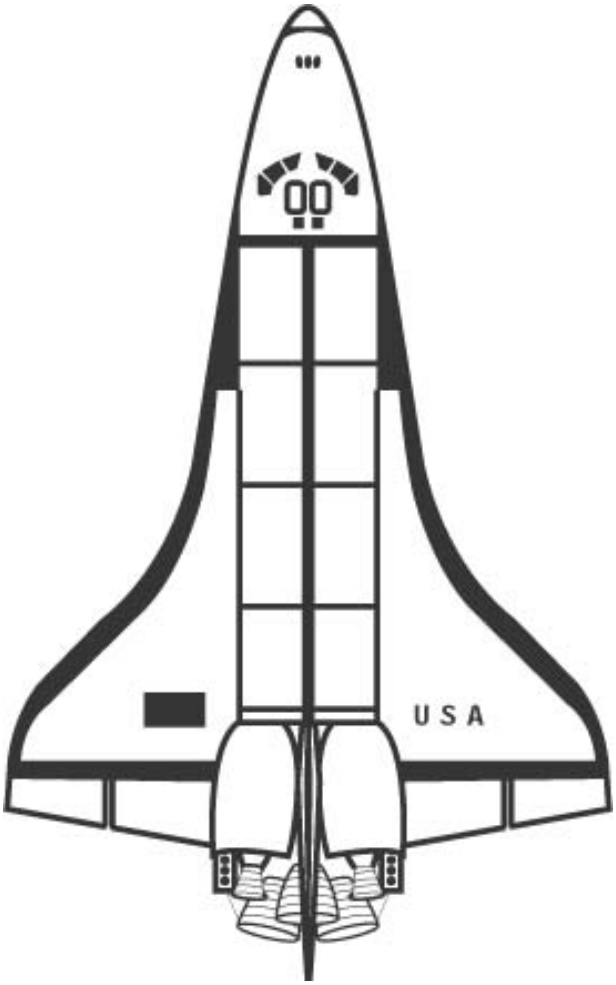
National Aeronautics and
Space Administration

# NASA/Navy Benchmarking Exchange (NNBE)

## Volume II

**Progress Report | July 15, 2003**

## Naval Reactors Safety Assurance




NNBE Benchmarking Team

**NASA Office of Safety & Mission Assurance**

**NAVSEA 08 Naval Reactors**

**NAVSEA 07Q Submarine Safety & Quality Assurance Division**

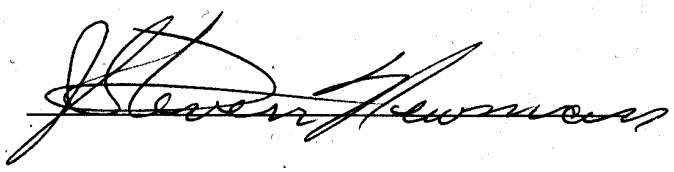
## Acknowledgement

The NASA/Navy Benchmarking Exchange (NNBE) Team gratefully acknowledges the cooperation and outstanding support of the Naval Nuclear Propulsion Program, as well as NASA and Space Shuttle program management. Particular thanks go to the people of Kennedy Space Center who supported the NNBE site visit, including the opportunity to observe a Flight Readiness Review, access to Shuttle processing facilities, and a close-up view of the Space Shuttle Columbia. The NNBE Team mourns the loss of Columbia and her crew, and as NASA focuses on Return to Flight, we are committed to seek out best practices between our organizations. Through this exchange we have discovered similarities in our experiences and in the challenges facing our organizations. We anticipate that this exchange will continue to serve as a basis for further knowledge sharing and continuing growth in the relationship between our communities.

# Signature Page

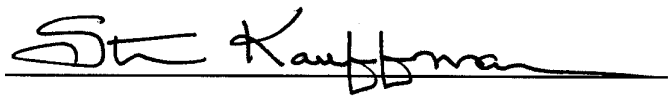
The undersigned participated in developing the content and verifying the accuracy of a) the information presented in section 3 of this Progress Report and b) the comparisons provided in section 4.1.

**NASA Team Lead**



Dr. J. Steven Newman
Independent Assessment Team Lead
Office of Safety & Mission Assurance

**Naval Reactors Representative**



Mr. Storm Kauffman
Director, Reactor Safety & Analysis
Naval Sea Systems Command (NAVSEA 08)

**NAVSEA Team Lead**

Mr. A. H. Ford, Jr., PE
Deputy Director, Submarine Safety & Quality Assurance
Naval Sea Systems Command (NAVSEA 07Q)

The opportunities discussed in section 4.2 of this document represent the consensus of the NASA core benchmarking team membership.

# Executive Summary

The NASA/Navy Benchmarking Exchange (NNBE) was undertaken to identify practices and procedures and to share lessons learned in the Navy's submarine and NASA's human space flight programs. The NNBE focus is on safety and mission assurance policies, processes, accountability, and control measures.

In August 2002, a team was formed, co-chaired by senior representatives from the NASA Office of Safety and Mission Assurance and the NAVSEA 07Q Submarine Safety and Quality Assurance Division. During the first phase of activity July -December 2002, the NASA team closely examined the Navy submarine safety (SUBSAFE) program. Information gathered during this first phase of the benchmarking was reported in the NNBE Interim Report of December 20, 2002. In January 2003 the benchmarking exchange continued with a visit by NAVSEA to Kennedy Space Center and with several NASA visits to NAVSEA 08 Naval Reactors (NR). This progress report summarizes further NASA observations concerning the Navy submarine program with focus on the Naval Nuclear Propulsion Program. (Note: The abbreviation "NR" is used throughout this document to represent both the Naval Reactors organization and the Naval Nuclear Propulsion Program)

NASA's examination resulted in identification of the following key leadership, organizational, and management attributes of NR safety implementation.

- NR has total programmatic and safety responsibility for the design, fabrication, test, installation, operation, and maintenance of all U. S. Navy nuclear propulsion plants.
- NR represents a very stable program based on long-term relationships with three prime contractors and a relatively small number of critical suppliers and vendors.
- NR employs well-documented, conservative and achievable technical requirements whose implementation is verified through robust audit and review processes.
- NR is a relatively flat organization with quick and assured access to the NR Director
- Critical NR program decisions require concurrence of all appropriate system, component, and support technical managers in addition to the program manager.
- NR has embedded the safety process within its organization such that safety and quality assurance are mainstreamed to an extent that a quality or safety office per se is unnecessary.
- NR relies upon recruiting, training, and retaining highly qualified people who are held personally accountable and responsible for safety.
- The theme of recurrent training is a major element of the NR safety culture and NR incorporates extensive outside experience to build a safety training regimen that has become a major component of the NR safety record.
- NR promotes the airing of diverse and differing opinions and recognizes that when no differing opinions are present it is the responsibility of management to ensure critical examination of an issue to actively encourage such opinions.
- NR has institutionally embedded a closed-loop lessons learned process that begins with a technical requirements base built on 5400 years of reactor operational experience, which in turn provides the foundation for the next generation propulsion plant design specifications.

The following opportunities are identified for NASA to consider based on the benchmarking:

- Increase the capability and functions of current NASA engineering organizations.
- Strengthen independent safety analysis and compliance assurance organizations.
- Consider alternative approaches for safety critical decision making, including enhanced roles for independent technical and safety organizations.
- Consider alternative organizational/management approaches for future human space flight programs
- Employ selected Navy submarine approaches to create stronger NASA system safety performance, including system safety training, alternative *fora* for discussion of safety critical engineering issues and the airing of differing opinions, as well as verification of safety behavior.
- Implement a Process Sponsor Program to enhance the retention of corporate knowledge and strengthen critical material and manufacturing processes.

## TABLE OF CONTENTS

## LIST OF FIGURES



## LIST OF TABLES

# NASA/NAVY Benchmarking Exchange (NNBE) Progress Report

## 1.0 Introduction and Scope

### 1.1 Introduction

The NASA/Navy Benchmarking Exchange (NNBE) was undertaken to identify practices and procedures and to share lessons learned from both the Navy's submarine and NASA's human space flight programs. Initiated in August 2002, the NNBE focus is on safety and mission assurance (SMA) policies, processes, accountability practices, and control measures. The benchmarking exchange has been divided into a multi-phase effort consisting of NASA's review of Navy practices and procedures and the Navy's review of NASA space flight SMA processes. An interim report summarizing the initial activities completed through October 2002 was prepared and presented to the NASA Administrator on December 20, 2002.

### 1.2 Scope

As a result of the Space Shuttle Columbia accident and subsequent investigation, NNBE activities to complete NASA reviews of the Navy and to initiate Navy benchmarking of NASA were put on hold from February 1 through mid-April 2003. This report details the re-initiation of these activities and documents the progress since the restart.

One of the key activities not completed prior to the December 20, 2002, Interim Report was an in-depth review of the NAVSEA 08 Naval Reactors (NR) organization focusing on naval nuclear reactor safety processes and training, quality assurance, compliance verification, software, and human factors. Consequently, the major part of this progress report describes the observations and opportunities derived from recently completed meetings with NR personnel. In addition to an introductory meeting with NR on October 1, 2002, these include a more detailed meeting on January 30, 2003, subsequent NASA participation in a NR training session (The Challenger Accident Re-Examined) held on May 15, 2003, and meetings on June 9 and 13, 2003 covering NR management and organization, requirements policy, implementing processes, and compliance verification and certification practices. By design, these topic areas correspond to the overall framework and structure established at the outset of the NNBE activity. Also by intent, the observations and opportunities identified in this Progress Report are closely coupled to, and build upon, the Potential Opportunities section of the December 20 Interim Report.

### 1.3 Follow-On Activities

Additional NASA review activities remain to be completed and are, therefore, not included in this Progress Report. These include potential NASA participation in a full-

scale non-nuclear shipyard functional audit and NASA observation of NAVSEA certification audits for both new construction and submarines completing a major availability depot maintenance period. Software has been reserved as a special topic for future NNBE discussions with NR (e.g., discuss design methods, quality assurance, quality control, and design philosophies relative to mechanical override and backups.) It is anticipated that these will be completed later this year as specific opportunities become available.

Other areas to be pursued during the next six months include: 1) the development and implementation of MOAs for "Reciprocal Participation in Reviews" (NASA NEQA and Navy SUBSAFE functional audits) and "Reciprocal Participation in Engineering Investigations," 2) the restart of the Subject Matter Expert Work Group activity, 3) the plans for a small Navy benchmarking group to observe NASA's (post-Columbia accident) return-to-flight activity, and 4) further investigation of the NAVSEA "Warrant" Program to establish and identify subject matter experts in key technical areas.

# 2.0 Background

## 2.1 Naval Sea Systems Command

Naval Sea Systems Command (NAVSEA) is the largest of the Navy's five systems commands, with Headquarters located at the Washington Navy Yard in Washington, DC. NAVSEA is the organization responsible for designing, acquiring, maintaining, and modernizing ships and systems for the Navy in accordance with Fleet and Office of the Chief of Naval Operations (OPNAV) sponsor needs and requirements.

Located in NAVSEA and reporting to the Assistant Secretary of the Navy (ASN) for Research Development and Acquisition (RD&A) the Program Executive Officer for Submarines (PEO SUB) is responsible for acquisition of new submarines and systems. The Deputy Commander for Undersea Warfare (NAVSEA 07) is responsible for support of in-service submarines and systems. Figure 2.1 shows the overall NAVSEA organizational chart and reflects the reorganization and restructuring that was completed subsequent to the December 20, 2002, NNBE Interim Report.

## 2.2 NAVSEA 08 Naval Reactors (NR)

The principal focus of this report is the Naval Nuclear Propulsion Program (NNPP). The NNPP is comprised of military personnel and civilians who design, build, test, operate, maintain, and manage the nuclear-powered ships and the many facilities that support the U.S. nuclear-powered fleet. Program elements include:

- Research, development, and support laboratories;
- Contractors responsible for the design, procurement, and construction of propulsion plant equipment;
- Shipyards that construct, overhaul, and service the propulsion plants of nuclear powered vessels;
- Navy support facilities and tenders;
- Nuclear power schools and NR training facilities; and
- The NNPP Headquarters (NR) organization and field offices.

**Note:** The abbreviation "NR" is used throughout this document to represent both the Naval Reactors organization (NAVSEA 08) and the Naval Nuclear Propulsion Program

NR is a joint Navy/Department of Energy organization (see figure 2.2) responsible for all aspects of Navy nuclear propulsion. Reactor safety is fundamentally addressed in each aspect of NR's responsibilities. For example, propulsion plant design features include inherent self-regulation for stability, equipment redundancy, and rugged design for battle shock. As another example, the nuclear propulsion plants are operated and maintained by highly trained crews, who receive over a year of academic and hands-on training before

qualification. Subsequently, operators receive continuing training to maintain their proficiency. A summary of NR's practices regarding reactor safety training can be found in Admiral Hyman G. Rickover's (the founder and director of NR for 34 years) testimony to Congress in 1979[1], following the reactor accident at Three Mile Island.

Since its inception in 1948, the NR program has developed 27 different plant designs, installed them in 210 nuclear powered ships, taken 500 reactor cores into operation, and accumulated over 5,400 reactor years of operation and 128,000,000 miles safely steamed. Additionally, 98 nuclear submarines and six nuclear cruisers have been recycled.

## 2.3 NNBE Context

It is important to note that NASA's benchmarking of the Navy submarine program has been focused on the SUBSAFE and Naval Nuclear Propulsion Programs with full understanding that these programs represent only two of the Navy submarine safety domains (see figure 2.3). This deliberate selectivity results from an early consensus of the NNBE management team that these two high reliability programs would provide the most meaningful comparison to NASA's human rated space flight programs.

[1] Comment by Admiral H. G. Rickover, USN, Director, Naval Nuclear Propulsion Program Subsequent to the Accident at Three Mile Island, August 1979 -- "Differences Between Naval Reactor and Commercial Nuclear Plants"

# Naval Sea Systems Command Leadership

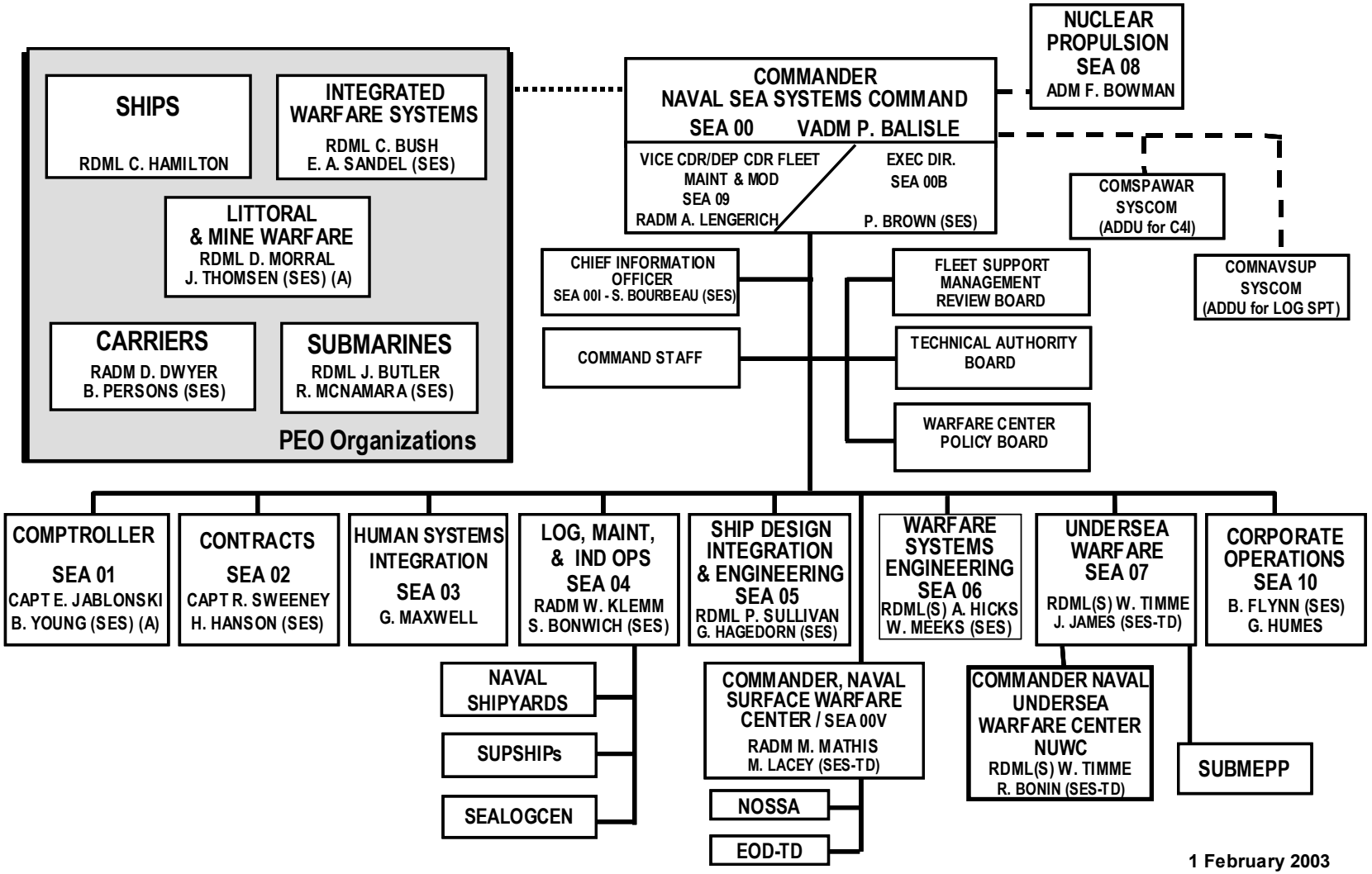



**Figure 2.1 Naval Sea Systems Command Leadership**

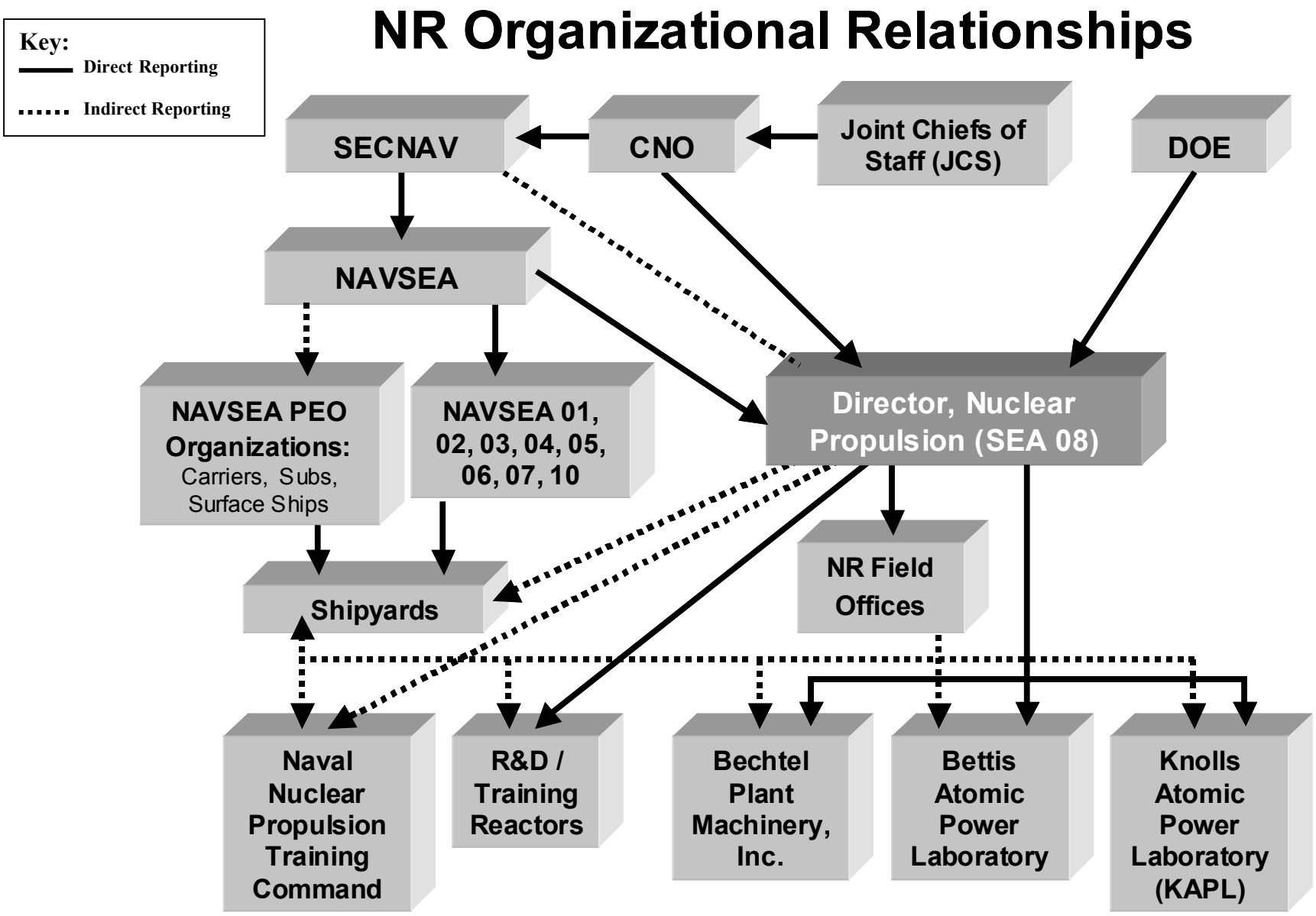



**Figure 2.2 NR Organizational Relationships**

# High-Level Submarine Hazards and Organizational Responsibilities for Mitigation & Management

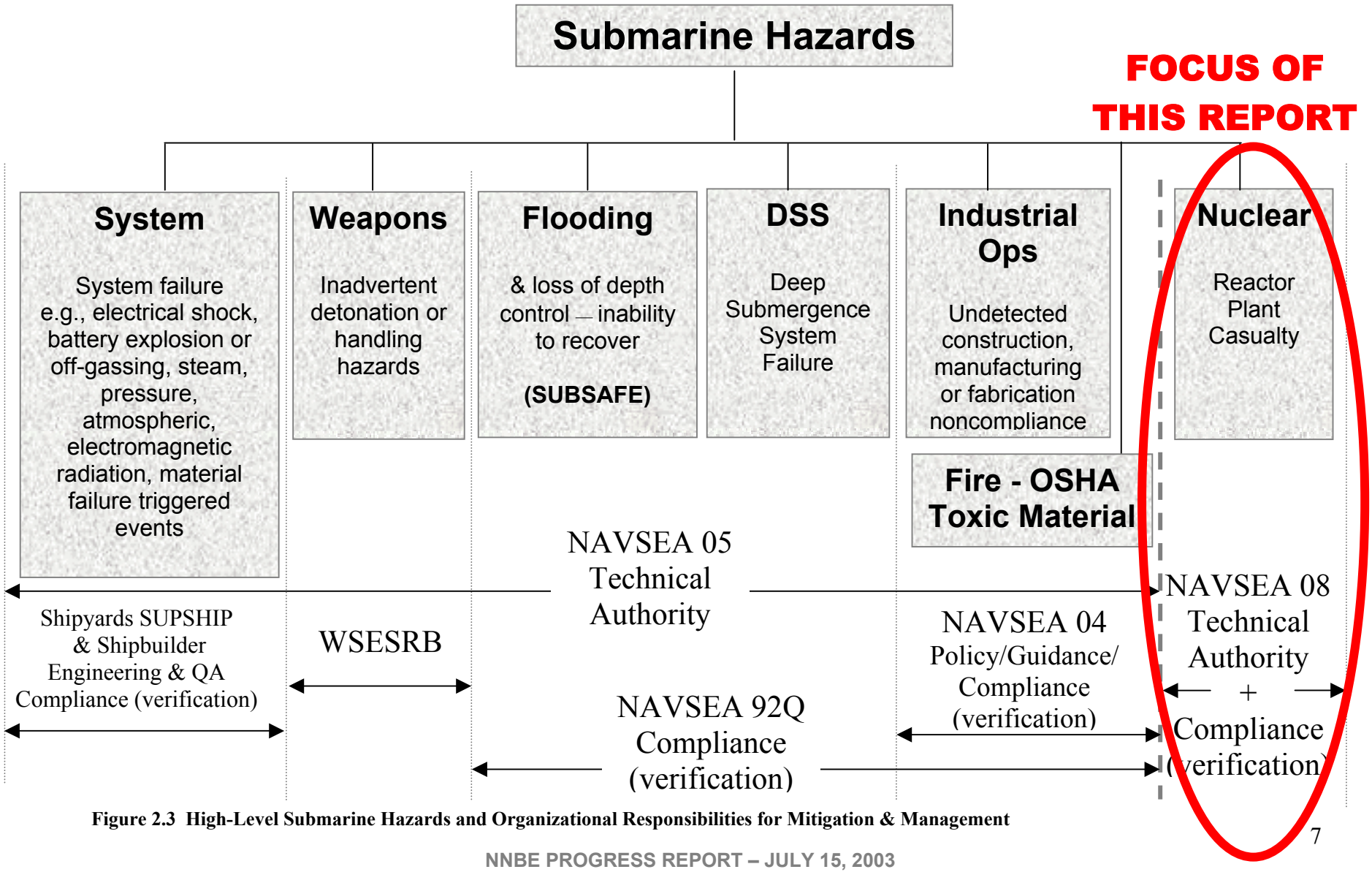



**Figure 2.3 High-Level Submarine Hazards and Organizational Responsibilities for Mitigation & Management**

# 3.0 Summaries and Key Observations

The basic elements of the NR safety and mission assurance function have been examined using the following framework:

3.1 Organization
3.2 Safety Requirements
3.3 Implementation Processes
3.4 Compliance Verification/Work Review Processes
3.5 Compliance Certification Processes

Each section includes a narrative summary and key observations.

## 3.1 Organization

### 3.1.1 Organizational Description

NR is the Navy code responsible for all naval ship reactors, their prototype and Moored Training Ship plants (today 103 reactors), and their associated radioactive materials. NR establishes requirements and verifies implementation of requirements for reactor design, construction, testing, installation, training, operation, maintenance, and shipment for disposal. NR field offices are responsible for oversight, surveillance, and assurance. NR is a joint (dual identity) organization in both the Navy and the U.S. Department of Energy (DOE). This has been the case since its inception, with Admiral Rickover's dual-hatted position in the Navy and the Atomic Energy Commission (AEC) at the beginning of the Navy's nuclear propulsion efforts.

Executive Order 12344 and its translation to Public Law 98-525 and 106-65 cast the structure of NR and NNPP. NR is directed by a four-star admiral with an 8-year tenure imposed, the longest chartered tenure in the military. As shown in figure 2.2, the NR organization is located within NAVSEA and also reports to the Chief of Naval Operations, with direct access to the Secretary of the Navy for nuclear propulsion matters. The NR Headquarters organization has approximately 380 personnel including 300 engineers. An additional 240 individuals are at NR field offices located at their laboratories, shipyards and contractor facilities.

All members of the NR management hierarchy (including support management, e.g., Director of Public Communications) are technically trained and qualified in nuclear engineering or related fields. They are experienced in nuclear reactor operating principles, requirements, and design.

NR Headquarters Internal Organization

The NR organization is flat, with 25 direct reports to the Admiral within Headquarters and generally no more than two technical levels below that (see figure 3.1). The direct reports, or section heads, consist of technical leads for various parts of design and operation and project officers. Overlapping responsibilities of the sections are intended to provide different perspectives. For example, an issue with a fluid component involves the component section, the fluids systems section, the project officer for the affected ship, and possibly other technical groups (e.g., materials, reactor safety).

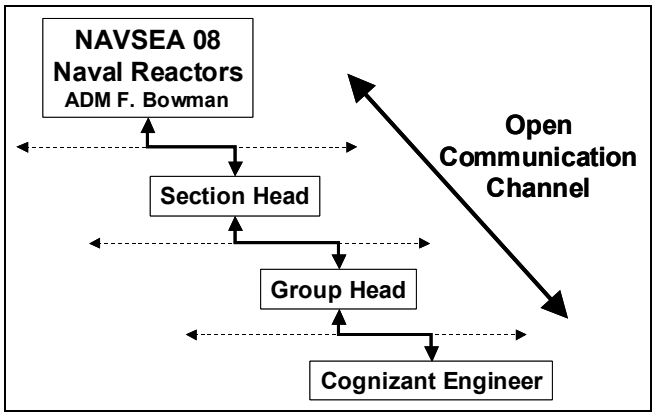



**Figure 3.1 Notional Organization Chart**

Field Offices

NR field offices at shipyards, laboratories, training locations, and other major program facilities are considered a part of the Headquarters organization. The field offices include approximately 70 personnel at each laboratory and from about 6 to 20 personnel at each shipyard. Currently, four public and two private shipyards work on naval nuclear propulsion. These field offices are headed by senior personnel from the Washington Navy Yard Headquarters who often return there after their field duty to fill the highest management and technical positions.

Laboratories

NR relies upon two prime contractors to manage the activity of two Department of Energy-owned laboratories:
1.) Bettis Atomic Power Laboratory (near Pittsburgh, PA), operated by Bechtel Bettis, a subsidiary of Bechtel; and
2.) Knolls Atomic Power Laboratory (KAPL) (near Schenectady, NY), operated by KAPL Inc., a subsidiary of Lockheed-Martin. A third prime, Bechtel Plant Machinery Inc. (BPMI) has both engineering and procurement responsibilities (see figure 3.2).

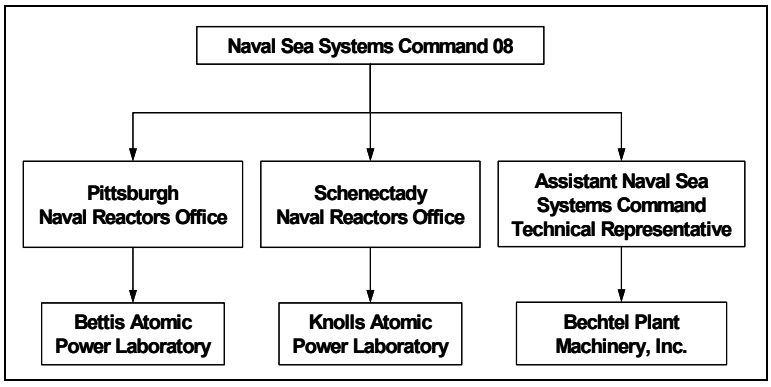



**Figure 3.2 NNPP Prime Contractor Management Structure**

The laboratory organization parallels NR Headquarters in there being many direct reports to the laboratory head (General Manager) and many of the same technical groups. These laboratories provide system design, lifecycle support, and some of the operator training for naval nuclear propulsion plants. The laboratories only serve the NNPP and do not perform unrelated work. The NR Director can call on the laboratory General Managers, who have available the full range of laboratory resources, for independent technical assessment of issues and policies. The two laboratories employ a total of approximately 5,500 people, a majority of whom are scientists and engineers.

There are relatively few critical suppliers (30-35). NR has a long tradition and relationship with suppliers, and the knowledge, understanding, and capabilities of those suppliers provide a significant and beneficial impact on overall hardware quality and reliability. Many of the key contractors are basically captive contractors in that a significant portion of their product line is dedicated to the nuclear-powered Navy.

Contract Types

The contracts with these prime contractors are cost-plus-fixed-fee, and have no incentive or bonus awards. The contracts with key component suppliers are typically fixed price type contracts.

### 3.1.2 Organizational Attributes

Communications

Processes are designed to keep Headquarters staff, in particular top management, informed of technical actions and to obtain agreement (concurrence) of the appropriate technical experts. There is a great emphasis on communicating information, even if an issue is not viewed as a current problem. The process embraces differing opinions, and decisions are made only after thoroughly evaluating various/competing perspectives.

Key personnel throughout the organization directly inform the Admiral of activities on a regular basis. The heads of field offices and the prime contractors privately and personally discuss issues with the Admiral at least biweekly. The heads and technical assistants at field offices write biweekly letters to the Admiral. The prime contractor General Managers write biweekly reports with many of the next level managers providing letters every four weeks. Additionally, the author of each letter is required to discuss the subject issue with the cognizant Headquarters personnel. Commanding Officers of nuclear-powered warships write monthly letters to the NR Director when in a maintenance availability and quarterly letters when operational.

Selectivity

NR stresses the selection of the most highly qualified people and the assignment and assumption of full responsibility by all members. The very best people are recruited, interviewed by the Director, trained, and retrained over their careers in NR. Most

Headquarters technical and financial personnel begin as naval officers. Engineering personnel must meet requirements for technical course work and grade point average. Engineers being considered for NR Headquarters are interviewed by three senior NR personnel, and the Admiral also interviews every candidate. Those technical personnel selected are committed to the program for 5 years. At the 5-year point, individual performance is assessed and the best are offered the choice of staying at NR as naval officers or converting to civil service while working for NR. NR candidates attend a basic reactor familiarization course, and then spend 6 months in residence at the Bettis Reactor Engineering School (BRES) to ensure all personnel have an equivalent understanding of nuclear engineering as applied in the NR Program. Another post-BRES training series is also conducted.

For the fleet, schools overseen by NR train approximately 3,000 students per year. Over 107,000 sailors have been trained and qualified as nuclear propulsion plant operators since the program began.

Officers entering the Naval Nuclear Propulsion Program (NNPP) typically have a college degree, usually in engineering, the physical sciences, or mathematics. These officers represent the highest tier of the Nation's college graduates, having been previously accepted into the United States Naval Academy, the Naval Reserve Officers Training Corps (NROTC) program, or the navy's Nuclear Propulsion Officer Candidate Program. Some officers receive their commissions through the Navy's Enlisted Commissioning Program, based on their outstanding performance in their enlisted jobs and academics.

All officers who apply for the NNPP to serve as operators in the fleet are interviewed by at least two senior NR engineers. The Director then personally interviews each individual and makes the final decision whether to accept that individual into the program.

Enlisted candidates for the Naval Nuclear Propulsion Training Program are high school graduates with a strong interest in the program. They are recruited directly into the NNPP. In addition, all enlisted personnel have performed well on special aptitude and entrance examinations.

Individual Responsibility

A basic tenet of the NR culture is to make every person acutely aware of the consequences of substandard quality and unsafe conditions. Each person is assigned responsibility for ensuring the highest levels of safety and quality. NR puts strong emphasis on mainstreaming safety and quality assurance into its culture rather than just segregating them into separate oversight groups. The discipline of adhering to written procedures and requirements is enforced, with any deviations from normal operations receiving careful, thorough, formal, and documented consideration.

**"RESPONSIBILITY IS A UNIQUE CONCEPT"**

**It can only reside and inhere in a single individual.**
**You may share it with others, but your portion is not diminished.**
**You may delegate it, but it is still with you.**
**You may disclaim it, but you cannot divest yourself of it.**
**Even if you do not recognize it or admit its presence, you cannot escape it.**
**If responsibility is rightfully yours, no evasion, or ignorance, or passing the blame can shift the burden to someone else.**
**Unless you can point your finger at the man who is responsible when something goes wrong, then you have never had anyone really responsible."**

**ADM H.G. RICKOVER**

NR emphasizes individual ownership and the long view: the engineers who prepare recommendations and those that review and approve them must treat the requirements, the analyses, and the resolution of problems as responsibilities that they will own for the duration of their careers. They cannot stop at solutions that are good only for the short term, knowing that the plant and ship will need to operate reliably and safely for many years into the future. The historical stability of the NR organization has made this ownership a reality.

Additionally, Navy crews "own" their plants in that they are assigned to them and literally live with them for two to three years at a time. Even for a new construction plant, a crew is assigned to the ship years in advance of initial operation. The crews are intimately familiar with the operation of their propulsion plant and are a key resource in identifying problems, deficiencies, and acceptable corrective actions. They are the customer for the nuclear propulsion plant product, and they have an active voice in design and operations.

Recurrent Training Emphasis

The NR Program has never experienced a reactor accident, but nevertheless includes training based on lessons learned from program experiences. NR also looks outside its program for lessons learned from events such as Three Mile Island, Chernobyl, and the Army SL-1 reactor. The Headquarters staff receives frequent briefs on technical issues (e.g., commercial reactor head corrosion), military application of nuclear propulsion (e.g., aircraft carrier post deployment briefs), and even personal nutrition and health and professional development.

The importance of recurrent training cannot be overstated. NR uses the Challenger accident as a part of its safety training program, based in-part on Diane Vaughn's book, "The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA."

On May 15, 2003, the NNBE team, accompanied by 15 senior NASA managers attended a 3-hour NR training seminar entitled "The Challenger Accident Re-examined." The session was the 143rd presentation of the Challenger training event. Since 1996, the Knolls Atomic Propulsion Laboratory has provided this training for over 5,000 Naval Nuclear Propulsion Program personnel.

The seminar consisted of a technical presentation of the solid rocket motor O-ring failure and the timeline of events that led up to the accident. The presentation was followed by an open, structured discussion with Q&A of the lessons learned. The training focused on engineering lessons learned and the importance of encouraging differing opinions from within the organization. It was emphasized that minority opinions need to be sought out by management.

Embedded Safety Processes

NR integrates the safety process throughout its organization. Admiral Bowman expressed the "desired state" of an organization as one in which safety and quality assurance are completely mainstreamed.

**SAFETY CULTURAL EMPHASIS**

**"The only way to operate a nuclear power plant and indeed a nuclear industry--the only way to ensure safe operation, generation after generation, as we have--is to establish a system that ingrains in each person a total commitment to safety: a pervasive, enduring devotion to a culture of safety and environmental stewardship."**

**ADM F.L. BOWMAN**

Differing Opinions

As noted above, the NR organization encourages and promotes the airing of differing opinions. NR personnel emphasized that even when no differing opinions are present, it is the responsibility of management to ensure critical examination of an issue. The following quotation from Admiral Rickover emphasizes this point:

**"One must create the ability in his staff to generate clear, forceful arguments for opposing viewpoints as well as for their own. Open discussions and disagreements must be encouraged, so that all sides of an issue will be fully explored. Further, important issues should be presented in writing. Nothing so sharpens the thought process as writing down one's arguments. Weaknesses overlooked in oral discussion become painfully obvious on the written page."**

**ADM H.G. RICKOVER**

Key Knowledge, Processes, and Skills

NR's reliance on the in-depth technical knowledge of its personnel places a premium on the need to maintain that knowledge. The emphasis on continuing training is discussed above. To ensure that key technical requirements are not missed, a system of technical requirements captures previous design guidance and lessons and is re-evaluated periodically. Also, use of "Why?" documents is promoted as a means to document the reason for various technical decisions. Finally, retention of paper documentation in early years and, more recently, access to historical information in electronic form provides a means to ensure that engineering decisions can be based firmly on a foundation of past judgment and experience.

NR places great emphasis on process management and the key skills of those individuals performing within those processes. One laboratory is pursuing plans to videotape lectures and discussions by senior, retirement-eligible experts. Also, as an example in the materials area and a relatively recent initiative, the Process Sponsor Program identifies NR subject matter experts (typically highly experienced individuals) within specialized process areas (e.g., brazing, welding, heat treatment, software control, and others) who serve as NR corporate resources, mentoring and consulting across all NR facilities and contractors.

---

**Key Observations:**

- NR has total programmatic and safety responsibility for all aspects of the design, fabrication, training, test, installation, operation, and maintenance of all U.S. Navy nuclear propulsion activities.

- NR is a flat organization with quick and assured access to the Director – about 40 direct reports from within HQ, the field offices, and prime contractors. Communications between NR headquarters and prime contractors and shipyard personnel occurs frequently at many levels, and a cognizant engineer at a prime or shipyard may talk directly with the cognizant headquarters engineer, as necessary.

- The Naval Nuclear Propulsion Program (NNPP) represents a very stable program based on long-term relationships with three prime contractors and a relatively small number of critical suppliers and vendors.

- NR embeds the safety and quality process within its organization; i.e., the "desired state" of an organization is one in which safety and quality assurance is completely mainstreamed.

- NR relies upon highly qualified, highly trained people who are held personally accountable and responsible for safety.

- Recurrent training is a major element of the NR safety culture. NR incorporates extensive outside experience (Challenger, Chernobyl, Three Mile Island, Army SL-1 reactor) to build a safety training regimen that has become a major component of the NR safety record – 128,000,000 miles of safe travel using nuclear propulsion.

- NR promotes the airing of differing opinions and recognizes that, even when no differing opinions are present, it is the responsibility of management to ensure critical examination of an issue.

## 3.2 Safety Requirements

Technical authority is vested with the individual NR system and component managers. Technical Requirements are codified in a system of technical manuals and specifications.

Technical Requirements

NR sets detailed and specific top-level requirements via a uniform set of technical specifications. This is a system of many documents that represent top tier requirements for every aspect of reactor design, construction, operation, and maintenance. These specifications represent over 50 years of continuous learning and form the basis for NR technical requirements. Other documents address specific functional requirements for materials, systems and components. Through periodic updating, these specifications also serve as the repository of lessons learned derived from over 5,400 "reactor years" of operation (see figure 3.3). Other critical documents include those that identify requirements and methods for required safety analyses and engineering modeling, and those that describe detailed test procedures along with integrated hazards analyses and mitigation.

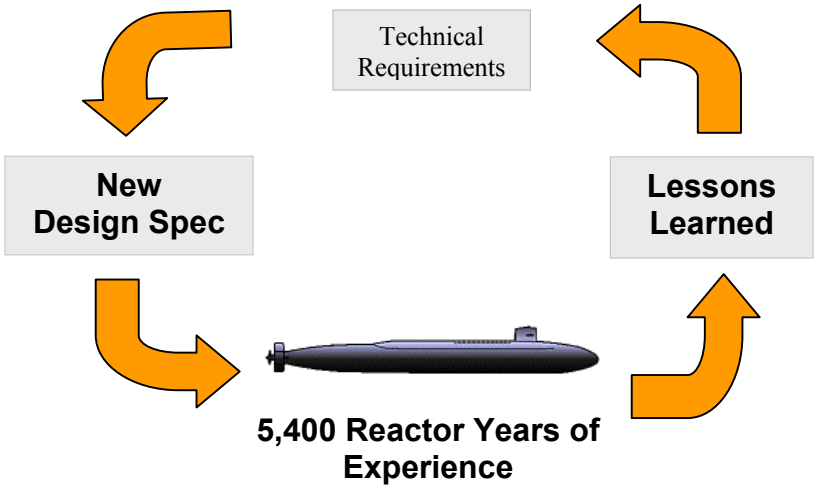



**Figure 3.3 Technical Requirements / Implementation Experience & Lessons Learned Closed Loop**

While most of NR's technical requirements are classified, it can be observed that they strongly emphasize the defense-in-depth approach (figure 3.5), where multiple problems and failures would have to occur to reach an actual unsafe condition. In particular, emphasis is placed on providing a design that allows time for operators to respond (and back each other up in responding) to casualties in order to re-establish stable and safe plant conditions. The technical requirements system explicitly requires several different analyses to show protection of the reactor and the public. This multiplicity in analyses, performed by different groups, provides different perspectives on the safety of design and operation, thereby reducing the chance that any major weakness is overlooked.

Overall Safety Requirements Approach - Embedded Safety Requirements

The philosophy that underpins the NR approach mandates that safety is embedded in the design requirements, the hardware, the implementing processes and most importantly the people. The NR technical requirements library houses the policies, requirements, procedures and manuals that implement the overall safety approach. Admiral F. L. Bowman summarizes below:

**"In the submarine environment, with these constraints, there is only one way to ensure safety: it must be embedded from the start in the equipment, the procedures, and, most importantly, the people associated with the work. Equipment must be designed to eliminate hazards and to be fault tolerant to the extent practical. Procedures must be carefully engineered so that the work will be conducted in the safest possible manner. And these procedures must be strictly adhered to, or work stopped and reengineered if conditions do not match the procedure."**

**ADM F.L. BOWMAN**

Requirements Flow-down

NR establishes specific top-level functional requirements (e.g., redundancy for safety-critical system elements, such as isolation valves, pumps, etc.) for new design reactors. The functional requirements are documented in a system specification that is then issued to the two NR laboratories. A single laboratory is selected as the lead design organization, but both laboratories are involved in the process. The non-lead laboratory has the lead for some components or sub-components, and each laboratory provides ideas on the components for which they have the lead, as well as for those for which they do not. A unique feature of the NR approach is the blending together of ideas (best of the best) from the two laboratories. As the lead laboratory proceeds with the detailed design of individual components or systems, the supporting laboratory serves in the role of independent review agent. NR accepts and approves the final design synthesis, and the

BPMI organization serves as the procurement agent for all hardware except for the reactor core, which is provided through Bettis.

Change Control and the Concurrence Process

As shown in Figure 3.1, there are four levels of responsibility/authority within Headquarters: the NR Director, Section Heads under the Director, Group Heads under each Section Head, and the Cognizant Engineers under each Group Head.

All actions and supporting information are required to be formally documented. No action is allowed to be taken via electronic mail. Telephone conversations may be used to exchange official information provided they are formally documented in writing, but all official business is conducted by exchange of letters. Technical recommendations and Headquarters response must be in writing. Emergent equipment problems may be handled through a specific process that, while not requiring the generation of a technical letter, is still documented in writing and obtains all requisite reviews.

Recommendations are prepared independently by the prime contractors and undergo extensive internal reviews by experts in all related technical disciplines. The management and personnel at the two NR laboratories are required to provide their technical recommendations independently without soliciting Headquarters advance agreement. This ensures that each laboratory retains its responsibility for providing its own technical assessment.

Any dissenting/alternate opinions are required to be documented in the recommendation with a discussion of the logic for not implementing them. When these involve reactor safety issues, they must be discussed with the submitting laboratory General Manager. The author at the prime contractor is expected to distribute the letter to all interested parties within the issuing prime contractor, at the other prime contractor, and at NR.

Upon submittal for action to Headquarters, the cognizant engineer routes the recommendation for comment to multiple interested parties. The cognizant engineer is responsible for determining the Headquarters response, after consultation with more experienced personnel within his/her group and evaluation of comments received from other reviewers. This frequently involves repeated technical exchanges with prime contractor staff, both those who prepared the recommendations and others. Once the cognizant engineer determines the response (e.g., approval, approval with comment, disapproval), he/she writes the response letter. The letter is then "tissued."

The term "tissued" refers sending the initial version of the letter (not a draft but the authoring engineer's best effort at the response) internally within Headquarters for review and concurrence. The author determines two lists of headquarters recipients: those who will concur in the action and those who just receive copies. A letter without concurrences is rare. In some cases, "copy to" recipients conclude that they or someone else should also be technically involved in the action and ask that the concurrence list be expanded.

This has the effect of backing up the author in ensuring the needed technical evaluations are performed, and it is one of the responsibilities of the Project Officers.

In addition, a pink tissue copy is sent to the Admiral, giving him the opportunity to review every item of correspondence when it is first created. This is another mechanism by which the Admiral becomes personally involved in technical actions. If for any reason, the Admiral questions the letter, it is placed on "hold." Then, before the letter can be sent, it must be cleared with the Admiral, usually by the author and his/her Section Head. The Admiral may direct additional persons in other disciplines to be involved.

To concur in a letter, an engineer reviews the proposed action. Since the head of the section received a "tissue" copy of the letter, the reviewing engineer may receive comments from the Section Head or others within the group. The review focuses on two questions: 1) is the action satisfactory in their technical discipline? and 2) is the overall action suitable? The engineer must be satisfied on both points. Concerns are worked out between the reviewing and authoring engineers. If the concerns cannot be resolved at the engineer level, Section Head interaction may be needed. If agreement still cannot be reached, then the parties not agreeing with the action of the letter will write a dissent. The proposed action and the dissent are then discussed with the Admiral, who will either direct further review (e.g., obtain specific additional evaluation) or decide on the appropriate course of action.

In a case where a recommendation involves a substantial change to fleet operator interface with equipment or procedures, fleet operator input is sought. At the very least, the section that includes current fleet operators on a shore-duty assignment will review and concur on the action. In some other cases, the action (e.g., approved procedure) may be sent first for fleet verification to check out its suitability under controlled conditions before issuing it for general use.

Actions can change substantially from what was originally conceived by the authoring engineer and documented in the "tissue." In this case, the author must return to people who have already concurred and identify substantive changes or re-tissue the letter complete with another pink. Sometimes, the Headquarters action may be substantially different from the original prime contractor recommendation. Even though Headquarters has provided direction, the prime contractors (or shipyards) receiving the letter are expected to identify technical objections to the Headquarters response, if appropriate.

---

**Key Observations:**

- NR has an institutionally embedded closed-loop process that begins with a technical requirements base built on lessons learned from more than 5,400 reactor years of experience, which in turn represents the foundation for the next-generation propulsion plant design specifications.

- There does not exist a single (stand-alone) document that prescribes NR design safety criteria or standards. The safety requirements are embedded in a uniform set of technical requirements.

- NR exercises rigorous change control through a process that ensures each recommended change is reviewed (and concurred in) by all the appropriate stakeholders. Managing change is frequently discussed at senior levels.

## 3.3 Implementation Processes

A Collaborative Safety Assurance Process

NR is a unique organization in many respects. There is no single individual who serves as a systems safety engineer or safety integrator.

Reactor safety is the primary responsibility of all NR personnel (see figure 3.4). While NR performs functions that are not traditionally associated with reactor safety, all of these functions ultimately support reactor safety. For example, by providing its own program management for reactor plant work, NR ensures that pressures from budgets and schedules do not impact reactor safety. Program managers' review of all work under their cognizance includes a strong emphasis on safety.

When the authoring (initiating) engineer recognizes that there is a safety attribute associated with his/her proposed Headquarters action, the Reactor Safety & Analysis section will be involved either by concurring or by being sent an information copy. That does not absolve the authoring and other section engineers of their responsibility for the safety of the action. Each of them must be satisfied that the action is safe from a reactor, ship, crew, and public safety standpoint. The role of the safety section is to provide advice, perspective based on NR and commercial experience, and an independent perspective. The safety section is one of many equals in the process, and does not have unique veto authority. A dispute over a safety issue is resolved as is any other technical dispute, eventually going to the Admiral if it cannot be settled at the lower management levels.

**COLLABORATIVE SAFETY MANAGEMENT APPROACH**

NR Systems Managers
- Fluid System
- Electrical Systems

NR Component Managers
- Primary Components
- Valves
- Reactor
- Physics

NR Support Managers
- Reactor Safety & Analysis
- Environmental Health and Safety
- Radiological Controls and Chemistry
- Refueling
- Materials
- Operations and Training
- Financial
- External Affairs

NR Program Managers

NR Field Offices
- Prime Contractors (Labs)
- Naval Shipyards

**Figure 3.4**

Reactor Safety and Analysis Director

There is a single individual among the 25 section managers who serves as the "Reactor Safety and Analysis Director," who is responsible for maintaining an overall perspective concerning reactor design safety. This individual does not have a specific operational system or sub-system to manage and is, therefore, relatively free from the direct responsibility and pressures to trade cost versus technical requirements.

The safety section also has responsibility for specific technical work, namely reactor safety analyses, which are used to demonstrate how the design is protective of the public. These safety analyses are summarized in classified safety analyses reports that are reviewed by the independent U.S. Nuclear Regulatory Commission (NRC) and its Advisory Committee on Reactor Safeguards for new plant designs. The safety section is responsible for coordinating the incorporation of conservative, technically correct safety policies, but the primary responsibility for safety issues remains with the cognizant engineers and their sections. Thus, the safety section primarily serves to review, consult, and concur in decisions regarding nuclear safety aspects of naval nuclear propulsion plant work and features of design, development, testing, construction, inspection, operation, refueling, and decommissioning.

As part of this responsibility, the safety section must maintain up-to-date knowledge of Department of Energy and NRC reactor safety requirements and issues. The prime contractors receive NRC bulletins and publications that evaluate certain commercial reactor components such as pumps, electrical circuit breakers, etc. The prime contractors have established a system to identify components that NRC has determined to have problems. If a naval plant is identified that employs that particular component, action is taken to correct the problem or replace the component.

Thus, Reactor Safety & Analysis is an independent and equal voice in design and operation decisions, and it does not impose after-the-fact safety requirements or interpretations. Additionally, it serves as a coordinator, interpreter, corporate memory, and occasionally, an advocate for specific capabilities in a system of interlocking responsibility in which everyone from the NR Director to the most junior operator is accountable for reactor safety.

Safety Management Philosophy

As shown in figure 3.5, safety of reactors is based upon multiple barriers or defense-in-depth, including self-regulating, large margins, long response time, operator backup, multiple systems (redundancy). The philosophy derives in part from NR's corollary to "Murphy's Law," known as Bowman's Axiom - "Expect the worst to happen." As a result, he expects his organization to engineer systems in anticipation of the worst.

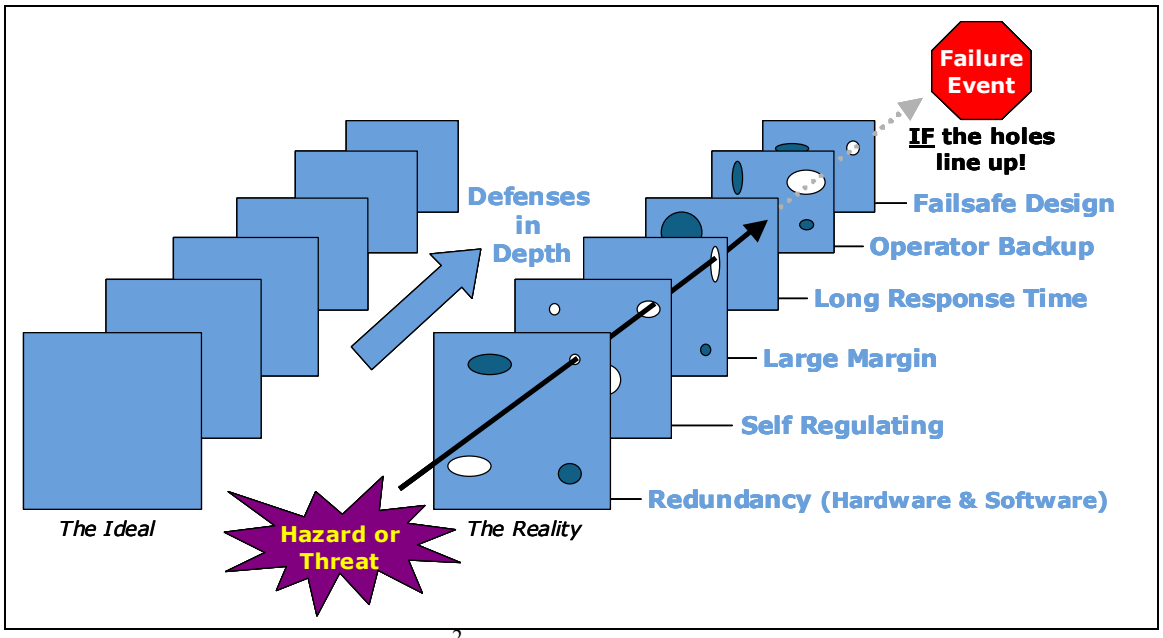



**Figure 3.5 Multiple Barriers to Failure**[2]

Safety Related Analysis

As part of the NR due diligence process, safety analyses are conducted to evaluate unlikely, worst-case event failure scenarios. Analyses are conducted to evaluate 1) potential damage to the reactor plant, 2) potential impact on people, and 3) potential impact to the environment.

The principal reactor plant safety analysis examines a host of scenarios derived from reactor operating experience and from Nuclear Regulatory Commission guidance for civilian power reactors. The scenarios fall into the overarching categories of 1) overpower and 2) under-cooling. Within each area a multitude of scenarios are examined that have the potential to contribute to an event.

The safety analysis report employs advanced analytical techniques to assess the likelihood of various system failure scenarios and then deterministically evaluate the potential impact on the public.

Systems Engineering

NR relies heavily on its two design laboratories' mechanical and electrical groups to perform systems engineering. These people are also responsible for the preparation of operating procedures, ensuring integration from both perspectives. NR Headquarters does not have a separate systems engineering group, nor an individual with the title "systems engineer." While the Fluid Systems sections and Electrical Section help to

[2] Graphic concept borrowed from James Reason's book, Managing the Risks of Organizational Accidents, 1977.

integrate the plants, all sections ensure their system level interfaces are addressed. Sections are also responsible for managing all external electrical and mechanical interfaces (e.g., interface with the SUBSAFE boundary or interfaces with main propulsion hardware). Finally, the program manager performs careful oversight of technical issues, not just of schedule and cost.

Quality of Work Principles

NR has an overall management philosophy and quality of work ethic that traces its origin and heritage back to Admiral H. G. Rickover, the founder and first director of the Naval Nuclear Propulsion Program. While the following list summarizes these embedded principles, several key attributes that characterize the organization and operation of NR require further comment:

- Individual Responsibility
- Product and Service Quality
- Appropriate Control
- Control of Interfaces
- Freedom to Dissent
- Formality and Discipline
- Protection of People and the Environment
- Validation of Work
- Managing Change
- Prevention
- Continuous Improvement
- Appropriate Design Conservatism and Cost Consciousness

As first introduced in section 3.1.2, personnel selectivity, training, communication, and open discussion are key enabling conditions for performance of quality work. The very best people are recruited, trained, and retained over their careers in NR. Everyone involved is required to understand and appreciate the technical aspects of nuclear power and have a deep sense of responsibility and dedication to excellence.

Secondly, communication is strongly emphasized. With a flat organization and with relatively quick and sure access to the top-most levels of the organization, up to and including the NR Director, everyone is encouraged to and takes responsibility for communicating with everyone else. An important aspect of this overall communication philosophy is the "freedom to dissent." The current NR Director, Admiral Bowman, has said that, when important and far-reaching decisions are being considered, he is uncomfortable if he does not hear differing opinions.

Operational Events Reporting Process

A major strength of the program comes from critical self-evaluation of problems when they are identified. NR has established very specific requirements for when and how to report operational events. This system is thorough, requiring deviations from normal operating conditions to be reported, including any deviation from expected performance of systems, equipment, or personnel. Even administrative or training problems can result in a report and provide learning opportunities for those in the program. Each reportable event is described in detail and then reviewed by NR Headquarters engineers. The

activity (e.g., ship) submitting the event report identifies the necessary action to prevent a recurrence, which is a key aspect reviewed by NR. The report is also provided to other organizations in the program so that they may also learn and take preventive action. This tool has contributed to a program philosophy that underscores the smaller problems in an effort to prevent significant ones. A copy of each report is provided to the NR Director.

During a General Accounting Office (GAO) review of the NR program in 1991, the GAO team reviewed over 1,700 of these reports out of a total of 12,000 generated from the beginning of operation of the nine land-based prototype reactors that NR has operated. The GAO found that the events were typically insignificant, thoroughly reviewed, and critiqued. For example, several reports noted blown electrical fuses, personnel errors, and loose wire connections. Several reports consisted of personnel procedural mistakes that occurred during training activities.

NR requires that events of even lower significance be evaluated by the operating activity. Thus, many occurrences that do not merit a formal report to Headquarters are still critiqued and result in identification of corrective action. These critiques are reviewed subsequently by the Nuclear Propulsion Examining Board and by NR during examinations and audits of the activities. This is part of a key process to determine the health of the activity's self-assessment capability.

This approach to capturing lessons learned and performing self-assessment is used for all NR program activities. The specific approach taken for radiological event reporting is discussed next.

Event Assessment Process

Problems are assessed using a variant of the classic Heinrich Pyramid[3]-approach with minor events at the base and major events at the top (see figure 3.6).

During training of prospective commanding officers, one instructor teaches about megacuries of radioactivity and then a second presenter addresses picocuries (a difference of $10^{18}$). The picocurie pitch is very effective because it emphasizes how little problems left uncontrolled can quickly become unmanageable. The point is to worry about picocurie issues, which subsequently prevents megacurie problems. Radioactive skin contamination is treated as a significant event at NR. The nuclear powered fleet has had very few skin contaminations in the past five years, and the total is comparably orders of magnitude lower than in some civilian reactor programs.

[3] H.W. Heinrich, Industrial Accident Prevention – A Scientific Approach, 1950.

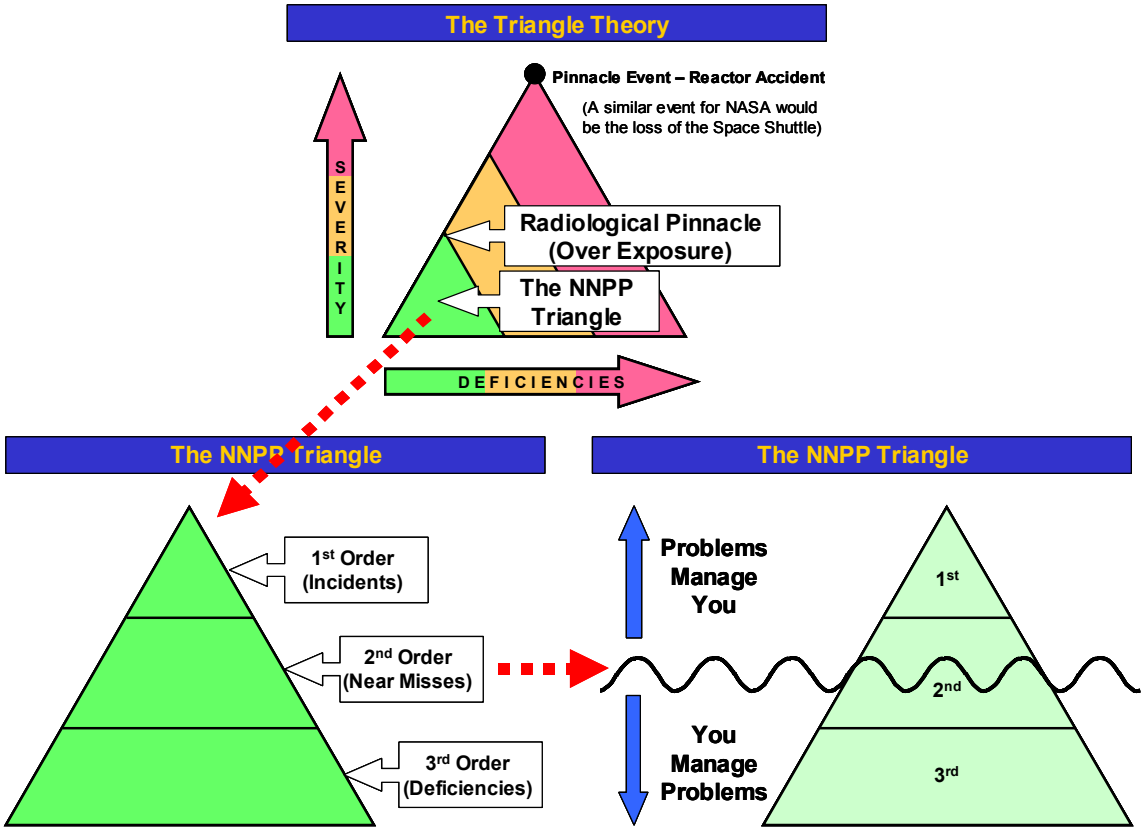



**Figure 3.6 NNPP Pyramidal Problem Representation**

The pyramid is layered into 1st, 2nd, and 3rd order problems with the threshold for an "incident" being the boundary between 1st and 2nd order problems. Any problem achieving 1st order status requires the ship's commanding officer or facility head to write a report that goes directly to the NR Director. This process encourages treatment of the lower level problems before they contribute to a more serious event. The Headquarters organization is involved in every report. Every corrective action follows a closed loop corrective action process that addresses the problem, assigns a corrective action, tracks application of the corrective action and subsequently evaluates the effectiveness of that action. A second order problem is considered a "Near Miss" and typically receives a formal management review. Headquarters gets involved with all first-order and some second-order problems. The visibility of issues available to the Admiral allows him to choose with which first, second, or sometimes third-order issues to get involved.

Root Cause Analysis Approach

The event reporting format uses a simple “four cause” categorization: procedures, material, personnel, and design. Each individual event is assessed for specific root causes (e.g., a material failure could be traced to excessive wear). More than one cause can be identified. Corrective actions are required to address both the root causes and contributing factors, since few events are the result of a single contributor given the use of the multiple barrier philosophy (figure 3.5).

A key aspect is a critique process where involved personnel are quickly gathered as soon as a problem is identified. Facts are obtained to allow assessment of causes and contributors. The emphasis is wholly on fact finding, not on assigning blame. Following the critique meeting, which (as noted) focuses on establishing the facts of an event (i.e., what happened), how those facts came about, and short term corrective actions, a separate meeting to establish root casues, long term corrective actions, and followup actions is usually held for the most significant events. Senior site management participates in this meeting, which starts with the what and how of the event established at the critique and focuses on understanding the root causes, establishing the long term corrective actions to address those root causes, and establishing followup actions to validate the effectiveness of the long term actions.

The method of analysis is primarily one of getting the right set of experienced personnel involved to gather and assess the facts and evaluate the context of the event. It is also worth noting that the laboratories maintain a current perspective on the many commercially available root cause analysis tools and techniques (e.g., the Kepner-Tregoe Method) to augment the critique activity. The laboratories are frequently asked to provide such training (and training on technical matters, too) to Headquarters personnel.

Quantitative/Predictive Methods

The NR organization relies principally on deterministic analysis and test in predicting performance of systems against design requirements. An important underlying perspective is that no single analytical "silver bullet" or method will ensure that there are no fundamental design defects or interactions missed in the deterministic engineering work. The approach is one of focus and emphasis on fundamental engineering rigor.

Human Factors

NR considers two basic facets of human factors, that which is incorporated in the design process and that which is applicable to operational aspects.

Reactor design activity incorporates a strong operator perspective emphasizing ergonomics. A principal consideration during the design process includes the requirement to avoid deviations or changes from existing designs unless a clear benefit is identified. The intent is to adopt a design approach that gives the crew a better, even more reliable warship when a change is made. To this end current operators are actively engaged in the design process via interactive visualization techniques to aid in the design and arrangement of equipment. NR also conducts a continuing review of commercial industry guidance that may have an impact on their design process.

A similar approach is taken relative to operational human factors. Again the intent is to minimize changes from past operational procedures unless there is a clear benefit. Laboratories prepare procedures, usually in terms of mark-ups from past projects; then

NR reviews these procedures again with experienced operator input. Fleet input is provided for verification.

One example of NR efforts to simplify the human-machine interface (interaction) is the careful design of annunciation and warning systems. In the case of Three Mile Island (TMI) commercial reactor, over 50 alarms or warnings were active prior to the mishap. At the onset of the TMI event, 100 more alarms were activated (a total of 150 of about 800 alarms active). In contrast, the total number of alarms and warnings in an NR reactor system is strictly limited to those needing an operator response. The Commanding Officer must be informed of unanticipated alarms that cannot be cleared. Naval nuclear power plants do not routinely operate with uncorrected alarms or warnings.

Laboratory Safety Committees

Each laboratory has independent safety committees that review select issues related to nuclear and reactor safety and report to the laboratory General Managers independently of the line organization responsible for the work. Major technical changes or policy changes generally receive committee review, as do technical decisions deemed to have a potential to affect safety. The approach for where safety responsibility resides and how these committees function within the laboratory organization can be summarized as:

- The General Manager is directly and personally responsible for the safety of the reactors and facilities under his/her cognizance.

- Reactors and nuclear facilities are designed, constructed, maintained, and operated in accordance with applicable requirements and in a manner that protects people, the environment, and property.

- Every employee is personally responsible for performing their duties in a manner that preserves the nuclear safety values of the NR program and maintains public confidence.

- Line organizations have the primary responsibility for reactor and nuclear safety. This responsibility is not diminished by reviews external to the line organizations.

- Reactor and nuclear safety-related activities are formally reviewed by subject matter experts who are independent of the line organizations.

The safety committees comment on line organization technical proposals but do not approve/disapprove them. If the line organization chooses not to incorporate (or cannot resolve) the comments, the difference of opinion is adjudicated by the laboratory General Manager.

**Key Observations:**

- Each independent lab general manager is required to be technically competent and is directly responsible for the safety of the reactors and facilities under his/her cognizance.

- The NR Director exercises (by law) direct supervision over the laboratories.

- Review by external organizations (such as Quality Assurance or Safety) does not diminish the responsibility of the line organization for program/product safety.

- Based on NR's organizational structure and culture of responsibility, there is not a separate systems engineering group or a job category of "systems engineer" within NR. While there is no single individual who serves as system safety engineer or integrator, there is, however, an individual (Reactor Safety and Analysis Director) responsible for maintaining an overall design safety perspective.

- Responsibility for safety of an action remains with the authoring engineer and his Section Heads. The Reactor Safety and Analysis Section reviews, consults and concurs in decisions on product nuclear safety aspects, but responsibility for product safety remains with the cognizant engineer and engineering organization.

- The Reactor Safety and Analysis Section has an independent and equal voice in design and operational decisions.

- Lessons Learned from more than 50 years of the NNPP have been documented and applied in an evolutionary fashion to each program to reduce operational risk and uncertainty.

- "Freedom to Dissent" is a primary element within NR.

- Emphasis on recruiting, training, and retaining the "very best people" for their entire careers is considered systemic to the success of NR.

- Critical self-evaluation of problems with strong Headquarters oversight is the tool of choice to isolate and control the small problems before they escalate into large problems.

- Closed loop corrective action is mandatory to NR's success. Problems must be identified, analyzed, and resolved and their resolutions proven successful.

- Cause analysis is performed via a formal fact-gathering critique, supplemented by expert assessment of root cause/corrective actions.

- Heavy emphasis is placed on ergonomics in reactor design through the use of various methods, such as interactive visualization techniques, walk-throughs, and discussion with operators. Operational human factors are also emphasized; but in both cases, change for the sake of change is not permitted.

## 3.4 Compliance Verification Processes

The NR Program (NR HQ, laboratories, field offices, contractors) has implemented a broad compliance assurance program that includes:

- Internal and external audit,
- Resident (field) offices,
- DCMA surveillance and inspection, and
- Operator continual training and recertification examinations.

Key players in the NR assurance process picture are identified in figure 3.7. The arrows indicate principal lines of oversight responsibility.

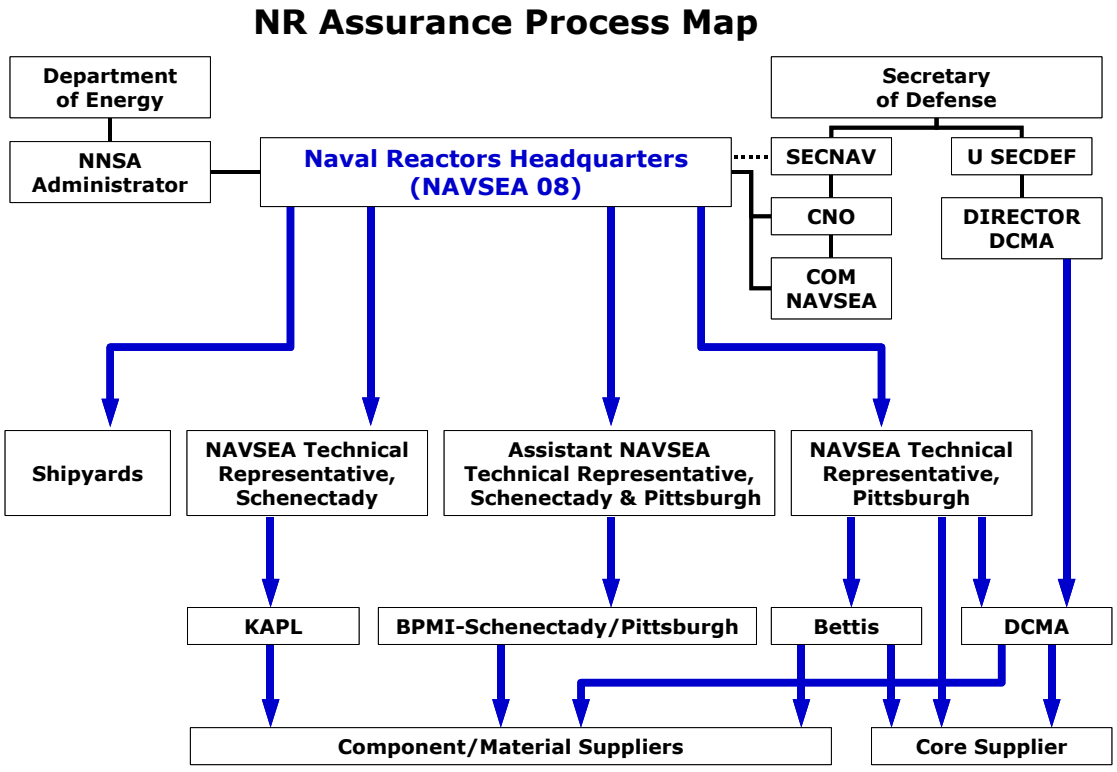



**Figure 3.7 NR Assurance Process Map**

Compliance Audits

Audits and inspections conducted by NR contractors, field, and Headquarters personnel have created an extensive oversight of program activities. The prime contractor laboratories and nuclear shipyards continuously conduct self-audits and inspections at almost every level of the organization. In addition, NR field office personnel routinely conduct numerous audits and inspections. NR Headquarters also conducts regular inspections of work, safety, environmental, and radiological controls (annually).

A key feature of NR audit activity is the composition of the audit teams. The requirement owner (technical authority for Headquarters, typically a senior executive plus the cognizant engineer) for a particular area is expected to participate in the audit process so that he/she can acquire a first-hand understanding of how their requirements are (or are not) being implemented. This method of closed-loop requirements verification also has the benefit of getting technical policy staff to go into the field and interact with the hardware as well as the implementation processes and personnel. The NR audit approach is a departure from the "auditor with a checklist" method where the individual may or may not have detailed knowledge of the requirements being verified. The activities being evaluated are required to prepare honest self-assessments that identify the weaknesses or deficiencies in their implementation of NR Program requirements and processes. Part of the Headquarters evaluation is weighing the validity and thoroughness of the self-assessment. NR evaluations comment negatively when a site self-assessment misses a problem, and NR would then review effectiveness of site management to critically assess their own activities. This encourages the activity to develop a self-assessment program that functions continually between the NR evaluations.

In addition, the NR field office evaluates the self-assessment and prepares its own view of the activity's performance. Thus, an evaluation is based on a combination of the activity's own self-assessment, that of the on-site field office, and that of the evaluation team itself. Findings are categorized as major or minor. Resolution of major findings must be formally closed out with NR Headquarters. The resolution of minor findings must be formally documented.

Biennial Evaluations

NR conducts biennial evaluations of shipyards performing nuclear work and training sites. These are broad audits of activities associated with work practices, safety, the environment, and health. Generally, 20 or so Headquarters senior personnel participate in each audit with the Director, NR conducting the close-out brief of findings. These audits include review of training activities, quality assurance programs, environmental protection, emergency preparedness, and physical security. Radiological controls compliance is audited at least annually (as part of the biennial evaluations in years when those are conducted).

Field Offices

The field offices at the laboratories and those at other sites differ some in function and structure. In all cases, one function is to facilitate communications between NR Headquarters and the field.

At the laboratories, the field offices provide regulation, oversight (including auditing), and contract administration. Audits are performed frequently and look at general and specific operational matters pertaining to program management, safety, the environment, and health. The findings or deficiencies noted in these audits require a response from the contractor as to the corrective action planned. The action planned must have the approval of the field office, which follows up to ensure each action is implemented. In addition to conducting formal audits and inspections, NR field personnel conduct routine inspections of activities and require contractors to correct any deficiencies that they find. When they record a deficiency, a report is filled out and the manager of the activity has 1 week to respond and identify actions to correct the deficiency. There are about 70 individuals in each of the two laboratory field offices.

For the shipyards, training reactor sites, and some naval nuclear maintenance facilities, field office personnel provide regulation and conduct audits and inspections. Field office personnel frequently monitor work activities on the site and within the propulsion plant. This surveillance is usually unannounced and may occur on any of the three daily shifts. The field office monitor interfaces with site management on a real-time basis regarding problems identified and actions to be taken. If necessary, the field office monitor has the authority to stop an unsafe operation. More routine matters are handled as described above, with issue of a deficiency report and requirement for the activity manager to respond by identifying corrective actions. These field offices are headed by senior personnel from the Washington Navy Yard headquarters and primarily staffed by naval officers with previous enlisted Naval Nuclear Propulsion Program operational experience.

Defense Contracts Management Agency (DCMA)

NR assigns delegations to DCMA to perform quality assurance surveillance and inspections at critical suppliers. NR has a unique relationship with DCMA. Individual inspectors are hand picked for their knowledge, skill, and experience, and they take technical direction directly from NR, via the responsible field office (not DCMA Headquarters). The key role of the DCMA inspector is to conduct surveillance of critical processes to ensure compliance with prime contractor approved requirements and procedures.

One field office has responsibility for periodically auditing DCMA performance to ensure that it meets NR unique requirements. The scope of compliance verification includes work control and review processes including quality assurance, inspection, and surveillance. In both cases, Objective Quality Evidence (OQE) forms the paper trail or documented basis to support certification decision makers.

Laboratory Internal Reviews and Audits

As an example, the contractors responsible for operations at the design laboratories conduct audits and inspections of all aspects of laboratory activities. The audits or inspections are directed toward ensuring compliance with written policies and procedures used to carry out the activities. They are conducted at all levels of the organization and performed by individuals at different levels.

Both KAPL and Bettis laboratories have implemented standing independent nuclear safety committees (reporting directly to the laboratory general manager) that conduct internal reviews and evaluate important aspects of reactor design and implementation safety.

As demonstrated in the following quotation, laboratory workers are cautioned not to let the presence of external audit or review teams diminish their sense of responsibility for safety.

**"Line organizations have the primary responsibility for reactor and nuclear safety. This responsibility is not diminished by reviews external to the line organization."**

**KAPL General Manager**

GAO Oversight of Laboratory Audit Activity

In the early 1990's the GAO performed an extensive and comprehensive 14-month investigation of environmental, health and safety practices at NR Facilities. The GAO had unfettered access to Program personnel, facilities and records. The review included documentation and operational aspects of the radiological controls protecting the environment and personnel, reactor design and operational history for full-size prototype nuclear propulsion plants, control of asbestos materials and chemically hazardous wastes, and NR internal oversight process. This included 919 formal audits by NR field offices at the laboratories over three years, 199 radiological deficiency reports generated by a laboratory over a month, and 28 NR audits at the laboratories over three years. The GAO noted that while these numbers may indicate major problems, virtually all of the issues were minor in nature. Rather, the numbers indicate the thoroughness of the audits and emphasize compliance with and awareness of requirements. The GAO testified before the Department of Energy Defense Nuclear Facilities Panel of the Committee on Armed Services in the U.S. House of Representatives that: "It is a pleasure to be here today to discuss a positive program in DOE. In summary, Mr. Chairman, we have reviewed the environmental, health, and safety practices at the NR laboratories and sites and have found no significant deficiencies."

Continuing Training & Biennial Recertification of Operators

Knowledge and operational skill degrade when not periodically recalled or used. The Continuing Training Program is in place on all naval nuclear vessels and nuclear training facilities to maintain and continually improve the knowledge, understanding, and skills to prevent this degradation of skills. A number of different activities are included under the Continuing Training Program (e.g., skill training, seminars, theory-to-practice exercises, casualty drills, and written and oral examinations). Most ships give written examinations, at least monthly, to all nuclear operators to check understanding and retention of material covered in the Continuing Training Program. All nuclear operators must comply with requirements to maintain watch-standing proficiency and, independent of any other considerations, must reestablish their qualification every 2 years. Requalification requires that the operator take a written examination and may include an oral board examination. The CO, XO, and Engineering Officer are exempt from the biennial requalification, but directly oversee the Continuing Training Program and teach many of the sessions. The ship's training program is covered in detail in the quarterly letter from the CO to the Admiral.

In order to provide independent oversight of the crew's training and operating capability, a Nuclear Propulsion Examining Board (NPEB) administers an Operational Reactor Safeguards Examination annually with emphasis on day-to-day operations and adherence to written procedures. The NPEB consists of four to seven people, including one or two senior officers (post-commanding officers), and oversees administration of written examinations to the entire engineering department, reviews all the engineering department records, conducts oral interviews with selected personnel, and observes casualty training in the power plant. At the conclusion of the ORSE, usually a 2- to 3-day period, the NPEB presents the results of its examination to the CO, emphasizing any weaknesses noted.

The NPEB reports directly to the command authority for that ship, and in parallel to NR Headquarters. The NPEB conducts its examination to standards established by the Director, NNPP.

Surveillance of Contractor Quality

NR exercises direct oversight over the prime contractors who operate the Bettis Atomic Power Laboratory, Knolls Atomic Power Laboratory, and Bechtel Plant Machinery, Inc. NR also oversees the relatively small number (30-35) of critical suppliers and sub-tier vendors. The long-standing knowledge, understanding, and shared responsibility that NR has developed with both prime contractors and lower-level vendors greatly facilitates management of quality and reliability of hardware. NR assigns the prime contractors broad responsibility for designing and approving critical processes implemented by the vendors and suppliers. NR has also developed and employs a suite of Facility and Quality Surveillance Plans that are designed, first, to ensure compliance with NR established procedures and second, to provide a process check that contractors and vendors are producing products that meet the required quality specifications.

Process Sponsor Program

NR has developed a Process Sponsor Program that identifies laboratory and contractor based technical and process experts representing a comprehensive range of critical process skills important to the NR mission. Specialty areas include:

- Automatic Soldering
- Brazing
- Casting
- Chromium Plating
- Cladding
- Cleanliness and Crevice Protection
- Detrimental Material Control
- Eddy Current
- Electrical Discharge Machining
- Software Control
- Electrolytic Nickel Plating
- Electropolishing
- Forging
- Fracture Toughness Testing
- General Welding
- Hard surfacing
- Heat Treatment
- Liquid Penetrant
- Magnetic Particle
- Melting
- Radiography
- Rolling
- Seal Welding
- Thread Rolling
- Tube Forming
- Tube making
- Ultrasound

As discussed in section 3.1, the Process Sponsor Program also provides the organization with a transfer of critical knowledge as personnel leave the program. The Process Sponsor Program identifies NR subject matter experts (typically highly experienced individuals) within specialized process areas (e.g., brazing, welding, heat treatment, software control, and others) who serve as NR program corporate resources mentoring and consulting across all NR facilities and contractors.

---

**Key Observations:**

- NR emphasizes that “Silver Bullet Thinking is Dangerous” -- "there is no silver bullet tool or technique.” All elements ("across the board") of quality assurance and compliance assurance must be rigorously implemented to ensure delivery and operation of safe, reliable, and high quality systems.

- NR audit teams include the requirement owner (technical authority) for a particular area. The owner participates in the audit process so that he/she can acquire a first-hand understanding of how the technical requirements are (or are not) being implemented.

- NR field offices act as day-to-day audit and inspection groups. Responses to their findings are required, and they must approve final actions in response to major comments.

- Functional audits of shipyards are supplemented by field office assessments and comparative evaluations of the site's own self-assessments.

- Qualification and biennial re-qualification of all nuclear operators by written examination and oral board examination assures currency of skills. In addition, the NPEB administers an annual examination to the entire engineering department of a ship and reports results to the ship's CO, the command authority for that ship, and NR Headquarters.

- DCMA is used by NR, but is given technical direction by NR directly rather than by DCMA Headquarters.

- NR maintains a Process Sponsor Program in which the engineering activity retains technical responsibility for its components but consults with process experts (sponsors) within their identified areas of responsibility, as necessary.

## 3.5 Certification Processes

NR employs a defense-in-depth approach to safety that involves rigorous quality control, comprehensive procedures, fail-safe design, and procedural compliance. In order to certify compliance, NR conducts incremental audits before key events, for example, initial reactor criticality. NR conducts an investigation of selected critical components in which compliance with requirements is tracked to the lowest level, as shown in the following notional example:

- Who installed the component?
- Who inspected the work?
- Where are the individuals' training and certification records?
- Where are the test data for the component?
- Where are the certification test records (objective quality evidence)?
- Who performed the tests, and what were the individuals' qualifications?
- Who witnessed the test?
- What is the material heritage?
- Where are the lot acceptance fracture toughness test data? etc.

The net result of the NR certification process is to continuously evaluate and correct any problems with work accomplishment or documentation required to validate the acceptability of prior work.

Functional audits are also performed at all executing activities by their local QA organization. Four levels of oversight are provided by the Type Commander, Squadron, the Naval Reactors Representative's Office (NRRO), and the NPEB. The Type

Commander and Squadron conduct assessments at the platform level. The NRRO provides oversight at the facility platform level. The NPEB performs detailed annual audits to examine the competency to operate. NPEB audits focusing on day-to-day operations are highly structured, employing a checklist process to assess safety records, self-assessment capability, training, crew level of knowledge, cleanliness, etc. NR employs several oversight methods, such as appraisals, evaluations, surveillance, program reviews, required submittals, critical item reports, and field representative reports.

Rigorous quality control includes on-site representatives, detailed specifications, a separate logistics/supply system, and Objective Quality Evidence (OQE) documentation. Executing organizations generate OQE, which is included in all Technical Work Documents (TWDs) in some form. Engineering Certification for the prime contractor is based on a Certification Checklist (CCL). Equipment certification packages are developed for the reactor core by the vendor and prime contractor, and the vendor provides detailed component history books to the prime contractor.

### 3.5.1 New Design Certification

NR performs a technical review of documentation received from the two dedicated nuclear laboratories. NR Headquarters in-depth technical review of all laboratory calculations is normally not required. When considered appropriate, NR will have one laboratory perform this in-depth peer review function on the other laboratory's documents. In addition, the NRC staff and the NRC Advisory Committee on Reactor Safeguards conduct a detailed, independent assessment of all new class reactor designs.

General Description of Naval Reactors Initial Test Program

The objective of the initial test program is to establish that the propulsion plant is installed and will perform as designed. Previous project tests have evolved over more than 50 years of NNPP design into a program that provides a high level of assurance that the nuclear propulsion plant will perform as designed. The new construction reactor plant testing process is outlined in figure 3.8.

The seven phases of the test program are:

1) Installation Check,
2) Calibration Testing,
3) Intra-System Test,
4) Inter-System Testing (Interface Testing),
5) Reactor Criticality Testing,
6) Final Calibration, and
7) Propulsion Underway (Sea Trial).

The installation check phase includes a visual inspection by system of all components and equipment to ensure that the installation is in accordance with design plans. Fluids systems will be checked for proper arrangement, such as the locating and mounting of components, hanging and anchoring of piping, alignment and bolting of machinery locking devices, verification of space envelopes required for maintenance, shock clearance, and the accessibility of operating parts of the system. Instrumentation and control systems will be checked for proper installation (including wrapping, servicing, sleeving, and marking). Circuit continuity, wiring, insulation, and proper ventilation (including heat dissipation features) will be checked.

The calibration tests are conducted prior to, and concurrently with, strength and tightness tests sequenced to meet test procedure requirements. Fluid systems are operated at minimum temperature and pressure in order to ensure, at the earliest date, that all components are operable and ready for further testing. Instrumentation and control testing proceeds concurrently, sequenced to meet test procedure requirements. Intra-system testing and inter-system operational testing begins in this phase and continues in subsequent test phases.

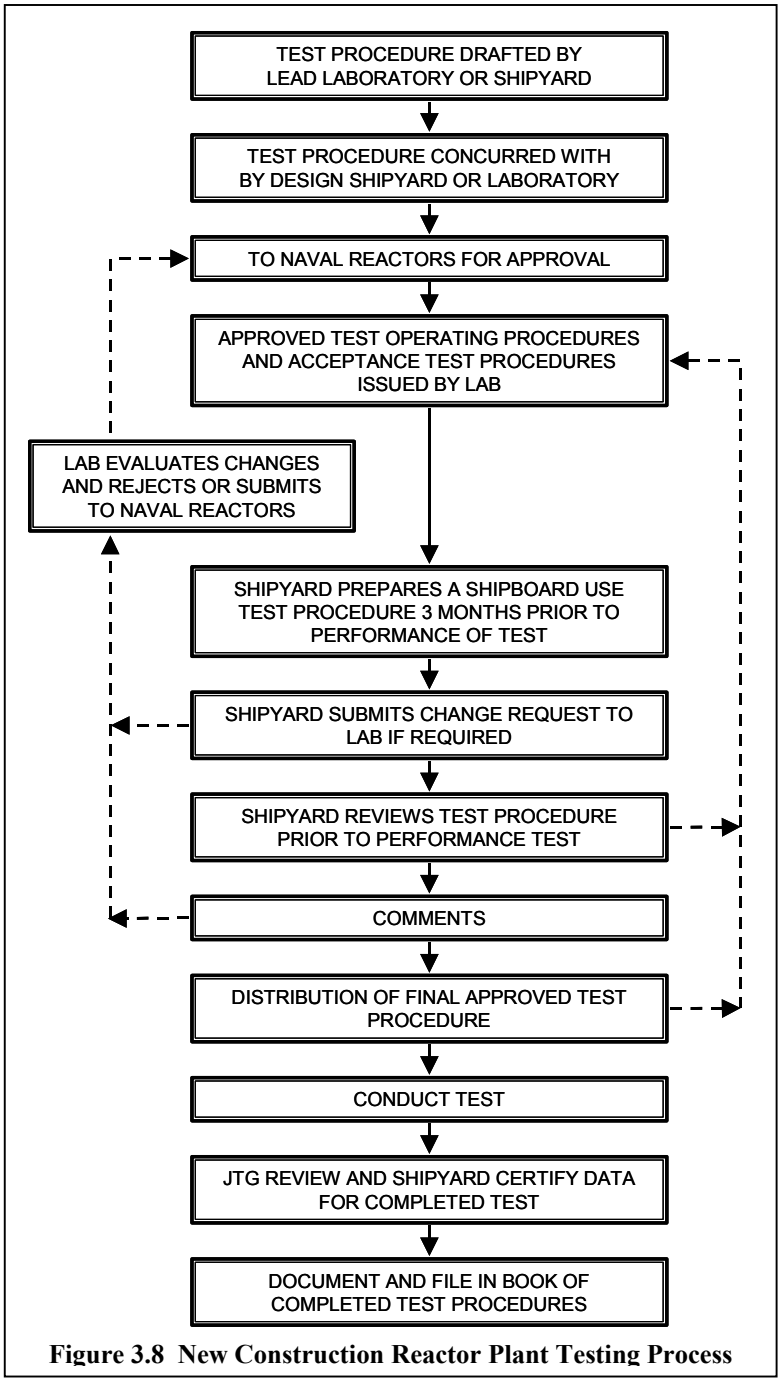


**Figure 3.8 New Construction Reactor Plant Testing Process**

When fluid systems have been tested adequately to indicate that operating pressures and temperatures can be reached, the systems are tested at designated higher pressures and temperatures. Safety and protection devices are tested as temperatures are increased. Besides normal hot operational testing, the tests are also performed in this phase to verify equipment response, performance characteristics, and maintainability.

After a rigorous examination of crew knowledge by a team from NR headquarters, authorization is obtained personally from the NR Director to take the reactor critical,

reactor criticality is achieved, and various physics and coolant radiochemistry parameters are measured to confirm that all acceptance requirements are met. Final testing and calibration of the nuclear instrument system is done. The plant is tested through various power levels and radiation shield surveys are performed. Steam transient testing, including testing under various steam plant lineups, is performed to demonstrate that plant parameters remain within acceptable limits. The intent of this phase is to ensure the readiness of the reactor plant for sea trials.

The new propulsion plant is then tested underway under the direct supervision of the NR Director in accordance with approved procedures and instructions. These test procedures include such things as final testing of cooling water systems and performance of propulsion plant heat balances.

Throughout the program described above, measured results are compared with previously established acceptance limits to assure the nuclear propulsion plant operation is consistent with design intent, safety, and protection analyses.

Joint Test Group Overview

The Joint Test Group (JTG) is a term used to describe collectively the persons assigned by their parent organizations to take local approval actions for a specific reactor plant test program. The JTG is composed of representatives of the following organizations participating in the test program:

- Construction Shipyard Nuclear Test Organization – The chief test engineer (CTE), appointed by the shipyard senior nuclear manager, is chairman of the JTG. The CTE is normally a senior individual who has been a shift test engineer on previously built nuclear submarines.

- Naval Reactors Representative's Office – A representative from the local NR field office is assigned as a JTG member.

- Ship's Force – A Ship's Force member is designated by the Commanding Officer and is normally a senior commissioned officer with several years of nuclear plant operations experience.

- Lead Design Laboratory (Knolls or Bettis Atomic Power Laboratory) – a KAPL or Bettis test engineer, generally with experience in nuclear propulsion plant design, operations, or both, is an assigned JTG member.

The members of the JTG must be qualified on the nuclear propulsion plant. The JTG facilitates local approval of documents for administration, performance, and acceptance of testing and communications among the responsible organizations involved in the test program. Decisions of this group must be unanimous. The JTG also monitors testing with emphasis on safety. The JTG members or parent organization representatives

assigned to monitor plant operations have the responsibility and authority to stop an operation at any time an unsafe or potentially unsafe plant condition arises.

Construction Shipyard Nuclear Test Organization

The Construction Shipyard Nuclear Test Organization is responsible for the overall administration, direction, and coordination of the reactor plant testing including scheduling and planning. Typical responsibilities include:

- Designating a Nuclear Chief Test Engineer who represents the shipyard as the Chairman of the Joint Test Group and is recognized as the authority responsible for ensuring that all aspects of reactor plant testing are accomplished in accordance with NR approved requirements.

- Providing qualified Shift Test Engineer (STE) personnel who, in conjunction with the ship's Engineering Officer of the Watch (EOOW), directs test operations and ensures all operations are performed in accordance with approved procedures or test documents. The STE is responsible for stopping a test or operation and requesting the EOOW to put the plant in a safe condition when problems develop that could result in an unsafe condition.

- Providing qualified personnel to prepare test documents (test sequence document, prerequisite lists, test procedures, etc.), to take data, and to evaluate test results.

- Keeping all interested and involved organizations and elements informed of the progress of and requirements for plant testing.

- Conducting a review of test procedures and operating procedures in advance of test performance.

- Preparing and recommending changes to test procedures and operating procedures for approval by members of the JTG.

- Preparing and issuing changes to test sequences.

- Preparing prerequisite lists for key events and requesting approval of these lists by members of the JTG for use.

- Evaluating problems during the test program and recommending possible courses of action for approval by members of the JTG.

- Reviewing all completed test procedures and certifying to the members of the JTG that the test has been satisfactorily completed.

- Ensuring that all preventive and periodic maintenance required by the reactor plant manual and component technical manuals are performed during the test program.

Ship's Force

Ship's Force has responsibility to operate the nuclear propulsion plant systems. All operations are performed by qualified personnel in accordance with approved operating procedures. In the event that abnormal or unexpected operating parameters occur, the Engineering Officer of the Watch (EOOW) shall promptly put the plant in a safe condition and notify the STE.

Naval Reactors Representative's Office

A representative from the Naval Reactors Representative's Office (NRRO) provides an independent review and surveillance of nuclear propulsion plant testing and operations, and concurs with test documents.

Lead Design Laboratory

The lead design laboratory is the organization responsible for the design of the reactor plant and for the preparation of detailed written procedures for testing and operating it. The Laboratory personnel provide surveillance over the testing of the reactor plant and tests of the safety related portions of the steam and electric plant. Qualified test engineers perform this function and are responsible for ensuring that testing and operations are being conducted in a safe manner and in accordance with approval procedures.

### 3.5.2 Engineered Refueling Overhaul (ERO) Certification

A high-level view of the Nuclear Maintenance Assurance process is shown in figure 3.9.

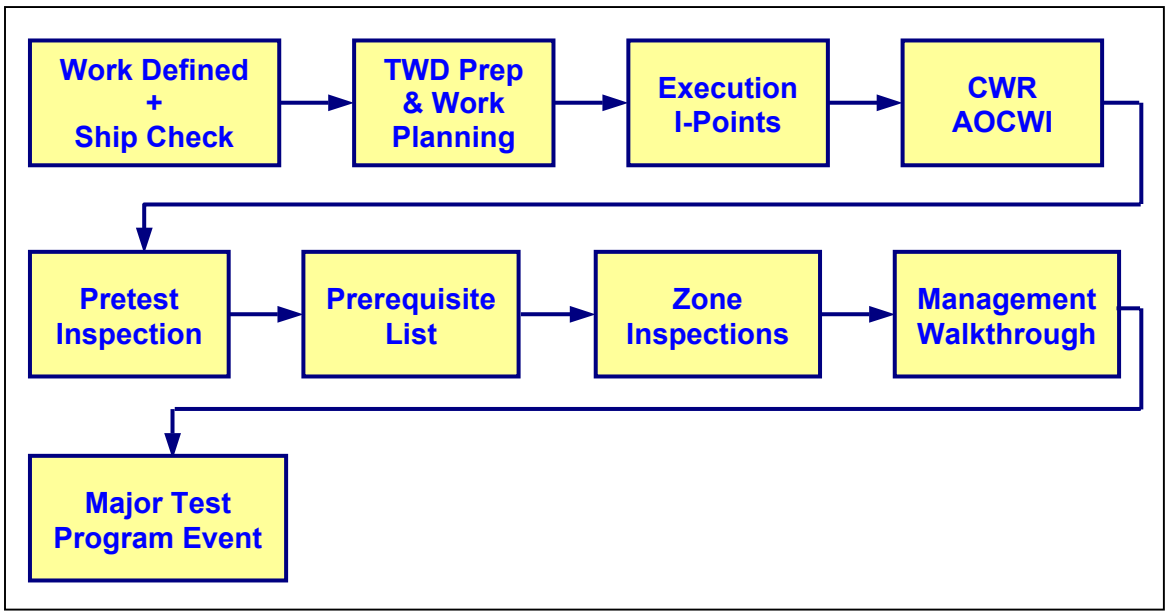



**Figure 3.9 High-Level View of Nuclear Maintenance Assurance Process**

The process begins with work definition and ship check. The nuclear engineering organizations prepare technical work documents (TWDs). The TWDs include various inspection points, including I-points and R-points. I-points specify nuclear inspection requirements at a given point in the process. R-points specify detailed steps that a radiological control technician must conduct at a given point. A Completion of Work Review (CWR) follows, which includes an Acceptance Of Completion of Work Inspection (AOCWI). The AOCWI is a paper inspection and may include a physical inspection of the completed work after engineering review (i.e., Pretest Inspection results) of the entire system in which all deviations are documented. Prior to operating the reactor, the OQE is reviewed in the Prerequisite List (PRL) activity. During the PRL, OQE is reviewed, and all discrepancies or incomplete items are either closed out or accepted as open. At this time, NR Headquarters conducts an examination to verify crew knowledge and proficiency. Subsequent to the PRL activity, Zone Inspections check for subsequent damage or discrepancies. Then, a Senior Management Walkthrough review is conducted by senior shipyard managers, the head of the NRRO, and the ship's Commanding Officer. Finally, after these steps are completed, a Major Test Program Event can be performed.

### 3.5.3 Maintenance

The above-described effort would be rendered irrelevant if components and systems were not properly maintained. A continuing maintenance program that fixes or prevents small discrepancies and does not allow for a prolonged backlog of maintenance is key. Availability of redundant components cannot be an excuse for delaying repair, since those redundant components are explicitly included in the design for ship and reactor safety and reliability. NR has detailed maintenance requirements and procedures for equipment, together with requirements and policies for a shipboard maintenance program. Routine preventive maintenance is essential to ensure the continued safety and reliability of plant operations, as is aggressive attention to prompt repair of deficient equipment. Maintenance is done by the crew or other qualified, nuclear-capable maintenance activities, depending on the level of skill or support equipment required. Corrective maintenance is also performed in accordance with detailed engineering work procedures, which include in-process quality checks and work certification to provide objective quality evidence (as described above). Work is then retested in accordance with engineering test procedures to verify proper component and system operation before being returned to normal operation. One focus area of assessment during external reviews, such as those done by the NPEB, is review of ships' maintenance programs. Additionally, ship material condition is periodically reviewed and assessed by NR Headquarters and by NR field activities.

Independent Assessment

External independent assessment for safety of naval nuclear propulsion plants is limited to reviews by the NRC and ACRS. The NRC conducts detailed reviews of particular aspects of new NR designs relative to state-of-the-art commercial plant designs.

In addition, where required, NR Headquarters prepares Environmental Impact Statements. Finally, in the environmental compliance area, NR is subject to audit by state and federal regulators in those areas not specifically assigned to NR by law.

---

**Key Observations:**

- NR performs incremental audits (similar to SUBSAFE) prior to key events to evaluate critical processes and to correct any problems with work accomplishment or critical documentation.

- A seven-phase test program begins with visual check of installation and progresses through higher levels of detail to actual operation of the reactor and delivery of power to assure readiness of the reactor plant for sea trials.

- A Joint Test Group (JTG), composed of representatives from the construction shipyard, NRRO, Ship's Force, and the cognizant laboratory, reviews and approves the administration and performance of test documents and acceptance of test results.

# 4.0 Comparative Context and Opportunities

## 4.1 Comparative Context

As noted in the introductory section of the December 20, 2002 NNBE Interim Report, the Navy's submarine and NASA's human space flight programs have a number of factors in common, the most important of which is a dedication and commitment to safety while conducting missions of national importance in very hostile and hazardous environments. However, a number of significant differences (e.g., managerial, organizational, and cultural) exist. It is necessary to examine and understand these key differences in detail to provide the proper contextual background against which the key observations and opportunities developed from this benchmarking exchange can be appropriately evaluated.

The following paragraphs are devoted to comparative discussions between the NASA Space Shuttle and the Navy NR programs. In selected cases the comparison is expanded to also include attributes of the NAVSEA 07, NAVSEA 05, and PEO organizations.

Organizations referenced in the following paragraphs include:

| | |
|---|---|
| NAVSEA 07: | Undersea Warfare Directorate (includes program managers for major overhaul activities) |
| NAVSEA 07Q: | SUBSAFE/Quality Assurance Division |
| NAVSEA 07T: | Submarine Hull Mechanical & Electrical Engineering Management Division |
| NAVSEA 08: | Naval Reactors (NR) |
| NAVSEA 05: | Ship Design, Integration and Engineering Directorate (Chief Engineer) |
| NAVSEA 04: | Logistics, Maintenance & Industrial Operations Directorate |
| NAVSEA 03: | Human Systems Integration in System Design Directorate |
| PEO/PMS: | Program Executive Office/Program Managers (includes program managers for new construction submarines) |
| ASN(RD&A): | Assistant Secretary of the Navy for Research, Development and Acquisition |

Operating Context

The degrees of complexity, challenge, and consequence for operating SSP systems, Navy submarines and reactor systems are comparable. The intrinsic, fail safe design of Naval nuclear reactors combines large margins of safety with long response times. As a result, Naval reactor failure modes are, by design intent, highly unlikely to lead quickly and directly to major damage. In contrast, failure modes on the Shuttle and submarines are more tightly coupled with relatively short response times that are more likely to result in catastrophe. Over the last 50 years, NR has built 27 different plant designs and installed them in 210 nuclear powered ships, accumulating over 5,400 reactor years of operating

experience from which to draw lessons learned and assist in uncovering latent design defects and manufacturing errors. On a comparative operating hour basis, the Shuttle Program has accumulated much less experience than submarines and naval reactor systems (i.e., operating hours) upon which to evolve and refine its design and manufacturing processes.

Requirements Philosophy

An overarching philosophy by which the Navy submarine force, and, in particular, the SUBSAFE and NR Programs, operates can be effectively summarized in two words: requirements and compliance, and is based on the narrowest and strictest interpretation of these terms. The focus and objective are to clearly define the minimum set of achievable and executable requirements necessary to accomplish safe operations. These requirements are coupled to rigorous verification and audit policies, procedures, and processes that provide the necessary objective quality evidence to ensure that those requirements are met. As expected, this approach results in an environment where tailoring or modification of the SUBSAFE and NR requirements is kept to an absolute minimum, and, when undertaken, is thoroughly vetted and very closely and carefully controlled.

The NASA approach is one in which requirements are defined in their broadest context and, in fact, result in what can be best described as requirement goals. The term goal is meant to show that the requirements are relatively difficult, and it is known in many instances they will be unachievable, as opposed to the NR and SUBSAFE approach of specifying achievable requirements. Thus, NASA's experience is to expect and allow lack of compliance with requirements by the individual project element designs, with the appropriate set of attendant waivers signed by the program manager, to document each deviation from the generally established goals. Two observations should be made on this approach. First, the approach necessarily requires discipline and rigor that accompanies the waiver (of the requirement goal) process, wherein rationale for acceptance of residual risk are thoroughly defined, documented, and reviewed by the entire program and engineering and safety communities. Secondly, the approach requires consideration and implementation of mitigation measures necessary to reduce the risk to an acceptable level.

Requirements Authority (Technical Authority)

Because of fundamental differences in organizational structures, one-to-one comparisons of specific manager roles and responsibilities are difficult to establish among the Space Shuttle, Navy submarine, and NR programs. The responsibilities for research and development, upgrades, life extension, new design, design verification, manufacturing, operations, and maintenance may be concentrated in an individual manager or shared by many organizations. Hierarchal reporting pathways differ, some are flat and direct, others are complicated with multiple responsibilities, and multiple indirect (i.e., dotted line) reporting relationships.

However, a narrow comparison has been developed in Table 4.1 related specifically to the resolution process for technical issues (including safety).

**Table 4.1 Program Manager (PM) Responsibility Comparison**

| | **Decision Authority To Resolve Technical Issues (including safety)** (ability to Trade Cost, Schedule & Make Risk Management Decision) | **Typical Resolution Process for Technical Issues (including safety)** | **Escalation Process for Technical Issues (including safety) If Required** |
|---|---|---|---|
| **Case-1:**<br><br>**Space Shuttle Program** | Program Manager in consultation with element project managers and center-based engineering experts<br><br>Project Manager (with matrixed engineering director support) seeks approval from the Program Manager. | Program Requirements Change Board (PRCB): SSP project managers present requests to the PRCB. Participants include <u>independent</u>: Engineering Director; Mission Operations Director; SMA Director; Flight Crew Operations Director. The Directors provide recommendations to the PM. If the PM does not accept their recommendation they can seek recourse with the appropriate Center Director. They <u>do not</u> have a veto in the PRCB forum. | *Multiple parallel pathways exist*<br><br>Institutional path: Center Director<br><br>Program Line Path: DAA for Space Flight (ISS and SSP); then AA for Space Flight<br><br>Functional path: AA for Safety & Mission Assurance |
| **Case-2:**<br><br>**Naval Reactors** | Lead Technical Section Head in consultation with appropriate system/sub-system discipline managers, project officers and laboratory personnel | Involved Technical Sections reach agreement and/or identify dissenting or differing opinions.<br><br>See Change Control and Concurrence Process<br>(see page 15) | NR Director |
| **Case-3:**<br><br>**PEO Submarines (new construction PMs)** | "Programmatic authorities select from among technically acceptable alternatives identified by cognizant technical authorities and request approval of engineering changes and non-conformances from them in accordance with reference." (NAVSEA INSTRUCTION 5400.97A) | PEO/PM reaches agreement with collocated Ship Design Manager - (NAVSEA 05 representative) | PEO/SEA 05 meeting with escalation to ASN(RD&A). |
| **Case-4:**<br><br>**NAVSEA 07 (overhaul and maintenance PMs)** | | NAVSEA 07-PM reaches agreement with Ship Design Manager - (NAVSEA 05 representative) and NAVSEA 07T (technical representative within NAVSEA 07) | SEA 07/SEA 05 meeting with escalation to COMNAVSEA. |

In the December 2002 NNBE Interim Report, it was noted that the Navy has (for non-reactor plant systems and areas) a central technical requirements authority (including SUBSAFE requirements) in the Chief Engineer (NAVSEA 05). This authority is separate from individual program and project managers, whereas individual NASA program or project managers have full engineering and technical requirements authority.

From an organizational perspective, the NR model is more similar to the way the Space Shuttle Program is organized than the SUBSAFE model. NR has integrated within its program structure a strong, centralized technical authority. Organizationally, NR has project officers (or program managers in NASA terminology) and technical directors that report directly to the NR Director.

In both the SSP and NR programs (cases 1 and 2) issues are resolved largely within their own line authority. In the case of PEO Submarines (case 3) and NAVSEA 07 (case 4) program managers must obtain approvals from the Chief Engineer (NAVSEA 05), the technical requirements authority. In the vast majority of cases, the escalation option is not required to resolve the issue.

Requirements Change Process

The NR approach is implemented as a collaborative, concurrent engineering process. The flat organization facilitates almost parallel review and assessment of proposed changes, with the NR Director serving as the final approval authority.

The Space Shuttle Program requirements change process is a structured, tiered process in which proposals are elevated from successive review boards eventually to the Program Requirements Control Board (PRCB), which is comprised of all program elements including engineering, operations and safety and is chaired by the program manager.

System Safety Integrator

Within the NR Program, the Reactor Safety and Analysis Director coordinates safety policies, acts as a resource to other organizations concerning reactor safety practices, and presents a safety perspective unbiased by responsibility for project schedule or budget. However, there is no single point or points of safety management responsibility; rather, each individual is held responsible for ensuring safety. Given a relatively flat organization with a strong safety culture, and a technical requirements system that has most safety provisions built in, NR has succeeded in mainstreaming safety implementation responsibility.

Much in the same way, NASA recognizes safety as a core value with each individual held responsible for safety. However, in the case of NASA, there does exist a safety functional manager. At the Agency level, that role is held by the NASA Office of Safety & Mission Assurance (OSMA), which is responsible for developing and implementing the overall agency safety program.

In the case of the Space Shuttle Program (SSP), a safety & mission assurance manager (Manager, Space Shuttle SR&QA Office) integrates SMA resources and activities for the program. This individual advises the SSP Program Manager concerning SMA requirements and issues, in consultation with SMA organizations at JSC, KSC, and MSFC. Each center provides safety, quality, and reliability engineering oversight and support to the SSP elements resident at the center. The Manager, Space Shuttle SR&QA Office, also works in close coordination with the Space Shuttle Flight Operations

Contractor (SFOC) SMA technical management representative to oversee SSP safety issues.

Systems Engineering Lead

Another point of contrast is the absence of an explicitly defined systems engineering function within the NR organization, although the two laboratories (and sometimes design shipyards) serve the system engineering function for the program as part of their routine responsibility to prepare and evaluate technical recommendations. NR retains, to this day, many of the management and organizational constructs introduced by Admiral Hyman Rickover in the 1950's.

NR achieves a high degree of systems engineering in general, and safety systems engineering specifically, without a position entitled "systems engineer." Everyone is responsible for ensuring that interface requirements and system-to-system interactions are addressed. The needed systems engineering is achieved very thoroughly because of the technical requirements, which result in a properly "systems engineered" and safe system. It was noted that a de-facto systems engineer has evolved in the role of the one (of three) Fluid Systems Section Head responsible for the particular design. Although functioning as such, it does not change the responsibilities of the individual engineers or the NR Director.

The NASA human space flight heritage has evolved, in part, from the 1960's Apollo program in which systems engineering was first developed and applied as a separate discipline to address the numerous interfaces and interactions inherent to complex systems. The Space Shuttle Program employs a formal systems engineering process headed by the SSP Chief Engineer, and supplemented by matrixed support from the center engineering directorates.

Independent Review

To avoid confusion and ensure clarity when discussing independent assessment or review, the NASA NNBE core team defined a framework to assist our discussions (see Appendix C). The framework provides examples of "independent assessment," recognizing that an accurate discussion requires understanding of degree of organizational separation from the program activity, funding source, reporting line, specific team knowledge and experience related to the activity, scope of review(s), depth of penetration, and frequency of review(s).

In the NNBE review it was evident that both the NR organization and the NASA SSP organization implement independent compliance assurance activities over government and contractor organizations. It is also the case that other organizations conduct various levels of independent review over the NR and SSP programs.

The NR program places emphasis on an annual/biennial functional audit of all major government and contractor organizations along with day-to-day observations of ongoing work. NR also plays strong roles in the verification of the product manufacturing and

ultimately the pre-operations certification. External independent review primarily involves the Nuclear Regulatory Commission assessment of new reactor designs as well as occasional, *ad ho*c reviews conducted by the General Accounting Office.

In the case of NASA, the three major Space Flight Centers have independent assessment offices resident in their SMA Directorates. They perform audits, assessments and other independent analysis functions using funds directly provided by NASA HQ, Office of Safety & Mission Assurance. Further, flight software is subject to independent verification and validation (IV&V), managed by the NASA IV&V Center in West Virginia. NASA Marshall Space Flight Center (MSFC) conducts periodic NASA Engineering & Quality Audit (NEQA) reviews of the MSFC provided Space Shuttle Program elements. Other organizations perform periodic independent assessments and spot audits of the Shuttle Program, including: Occupational Safety & Health Administration, NASA Inspector General, NASA Advisory Committee, General Accounting Office, and the Aerospace Safety Advisory Committee.

It should be noted that while NASA centers provide inline SMA support to the Space Shuttle Program and are funded by the program, they also report administratively to an independently funded and administratively controlled SMA Director. This organization has direct access to the Center Director (independent) and Code Q (independent). Assessment reports are reviewed and discussed both within the program community and independently within the SMA community. Key technical issues and assessments are reported to the SMA Director at the Center, the Center Director, and Code Q in addition to the Program or Project Manager.

Lessons Learned Emphasis

NR has "institutionalized" its lessons learned approaches. This has been accomplished by integrating within its program management structure a "centralized technical authority." This authority has the responsibility for establishing and maintaining functional technical requirements, as well as providing an organizational and institutionalized focus for capturing, documenting, and using operational lessons to improve safety of current and future reactor designs. These design safety improvements/changes are then incorporated into the next generation operational systems that in turn provide the next series of lessons learned – hence a tightly coupled, closed-loop process is established.

In the case of SUBSAFE, this central technical authority function is provided by the Chief Engineer. For NR the central technical authority (the NR Director) is supported by collaborative review and recommended approval by NR sections. NR technical requirements are captured in a suite of documents that represent critical requirements for every aspect of reactor design, construction, operation, and maintenance. This also serves as the repository of lessons learned derived from over 5,400 reactor years of experience, and it forms the basis upon which future reactor designs are promulgated.

The Space Shuttle and Space Station crews and operational personnel participate in extensive post-flight de-briefings with various organizations. At present, NASA has a

broad Lessons Learned Information System (LLIS) that program/project managers and their management teams are required (under recent policy revisions) to consult at various program and project milestones. Although NASA has made an effort to populate the LLIS with mishap investigation results and programmatic lessons learned, the Agency acknowledges that the currently implemented NASA LLIS has room for improvement.

Communications/Differing Opinion

Within NR, communication up and down is strongly emphasized with everyone taking personal responsibility for communicating across and through all levels of the organization. This is one of many continuing legacies traceable to Admiral Rickover. Problem reporting to the NR Director can be and is accomplished from everywhere in the organization. At the same time, line management (appropriate section heads and group heads) within NR is also notified that a problem is being reported. It should be noted that the flat organizational structure that exists at NR, as well as its heritage and culture, greatly facilitates this communication process. A further aspect of the NR communication culture is the strong encouragement for differing/dissenting opinions. In fact, NR personnel have commented that the NR Director requires that even when no differing opinions are present, it is the responsibility of management to ensure critical examination of all aspects of an issue.

NASA currently employs traditional, hierarchical, line management reviews leading up to the Flight Readiness Review in the Space Shuttle Program. The NASA SMA community implements the Pre-Flight Assessment Review (PAR) process. The Space Shuttle Program implements the Systems Safety Review (SSRP) process and the Payloads Safety Review Panel (PSRP) process. There also exists the anonymous NASA Safety Reporting System (NSRS) that provides a separate (last resort) path to the top of the organization available to all NASA and contractor employees who have a safety concern that they feel may not have otherwise been properly addressed. These processes provide avenues for people to raise technical issues.

Training Emphasis

NR has evolved a very strong training regimen and culture that specifically require mandatory and recurrent training based on both internal and external program experiences.

NR has a comprehensive training program for incoming headquarters engineering personnel, including a full-time, six-month resident curriculum covering all aspects of naval nuclear propulsion. NR draws on a number of outside programs and lessons learned, including Three Mile Island, Chernobyl, and the Army SL-1 reactor accident, and has developed a three-hour training seminar based on the Challenger accident. The Knolls Atomic Power Laboratory has conducted this seminar, entitled “The Challenger Accident Re-Examined” since 1996 during which time it has trained over 5000 program personnel. The seminar consists of a technical presentation of the Solid Rocket Booster joint failure and the timeline of events and decisions that led up to the accident. This

presentation is then followed by an open Q&A discussion of the lessons learned. The training focuses on engineering lessons learned and the importance of encouraging dissenting/differing opinions within the organization. Also, professional development training opportunities are strongly encouraged.

NASA has no formal, institutionalized, recurrent specific training requirement related to systems safety and safety-critical decision making as an underpinning for all program and project managers and project team personnel.

## 4.2 Opportunities

Notwithstanding the differences cited in section 4.1, there are indeed potential opportunities for improvement and enhancement that NASA may wish to consider as it seeks to continuously improve the safety of its programs, particularly its human space flight programs.

> Note: NR is a world-class "high reliability organization." The NR approach for managing and implementing safety has been examined in detail in this report. Opportunities discussed below draw on conceptual attributes of the NR example.

**Opportunity #1: Increase Capability and Functions of Current NASA Engineering Organizations**

The benchmarking activity (both NR and SUBSAFE) has brought into greater focus the importance of establishing and maintaining robust engineering and analysis capabilities to support the development and operation of complex, high technology systems.

It is envisioned that an enhanced independent NASA engineering organization would, as a minimum, be chartered to perform the following functions:

- conduct independent trending analysis and evaluation for recurrent flight safety issues;
- conduct independent testing and evaluation in specific areas not normally covered by the program;
- evaluate unexplained events ("known unknowns") with potential safety impact;
- develop and use NASA-wide collaborative engineering system(s) to enhance responsiveness and effectiveness;
- participate in independent compliance assurance and functional audits (along with independent safety assurance organization);
- manage (create) an integrated Lessons Learned Process for program/process enhancements and decision support;
- capture engineering knowledge relative to specific program/project designs - assemble archive material, interview original designers, operators - and present data in form suitable for long-term training and decision making.
- participate in NASA project management decision making *fora* (see Opportunity #3.)

This initiative would be coordinated by an enhanced NASA HQ engineering organization under the NASA Chief Engineer that would evolve into a technical authority serving all NASA programs and projects.

**Opportunity #2: Strengthen Independent Safety Compliance Assurance Function**

In the December 20, 2002 Interim Report, the importance of independent compliance verification was emphasized. The SUBSAFE organization serves as the independent compliance verification agent for submarines. For NR, resident on-site compliance verification is provided by the field offices, which function as independent agents reporting to the NR Director, providing ongoing surveillance and audit functions as discussed in section 3.4.

As NASA continues to examine Navy submarine safety assurance approaches (a process initiated in July of 2002), and in the wake of the Columbia accident, the issue of independent compliance verification remains prominent. NASA may wish to consider the SUBSAFE model (see appendix C discussion of independent assessment - SUBSAFE would be considered a Type-3 model). This model of robust independent audit capability may serve as an example for increasing the level of assurance currently provided to all NASA programs.

Prospective roles and responsibilities of the organization would complement those described in Opportunity #1, specifically collaborating with the independent engineering organizations in areas of trending and analysis and conducting independent compliance assurance and functional audits. It is envisioned that the independent safety compliance organization would have expanded role in NASA project management decision making *fora* (see Opportunity #3.)

An enhanced safety compliance organization must be independent, well-staffed, and adequately funded with robust audit and review capabilities and functions. In particular, NASA management should provide for an immediate infusion of systems engineers into the safety organizations and develop a structured system safety career path which can offer professional satisfaction, personal recognition, and focused training (see Opportunity 5.1) with well-defined promotion opportunities.

**Opportunity #3: Alternative Decision Making Approaches**

The NR and Navy submarine program decision processes stimulated considerable discussion within the NASA NNBE assessment team. One example is the NR approach of establishing the expectation for any member of the engineering team to dissent when a technical action is considered inappropriate. Another example, as discussed in section 4.1, is the Navy submarine program manager need to reach agreement with an independent technical authority for critical program decisions. A notional framework has been constructed (below) showing three models for safety critical decision making.

In Model A, the project manager has final authority. No one else has veto power, but it is possible for other participants to escalate issues (e.g., to line, institutional, functional, and management).

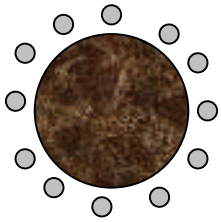
The project manager is represented by the dark circle

White circles represent participants in a decision forum with appeal options

**Model A: Long Table**
Centralized Decision Forum

In Model B (consensus driven) everyone has equal power to non-concur in a decision and escalate to the ultimate activity authority as necessary.

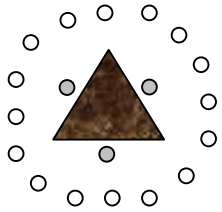
The project manager is equal to other participants



**Model B: Round Table**
Consensus Decision Forum

In Model C, a 3-way veto power decision board is identified wherein three selected managers must reach consensus on an issue to move forward. Appeals to upper line and organizational management exist.

The project manager (gray circle) is equal to the other two decision authorities



White circles represent participants in a decision forum with appeal options

**Model C: Triangle**
3-way Sharing of Decision Forum

A variant of Model C could be used for selected activity elements (e.g., a project within a program), and selected decision areas (e.g., waivers, deviations, critical design decisions, operational issues). Within this variant, the three decision authorities would be the project manager, an independent technical authority (see Opportunity #1) and an independent safety authority (see Opportunity #2) with appeal to in-line, functional, and/or institutional management.

In considering this example, it is important to note that with each additional "independent veto participant" in the process, the project manager's authority appears diminished and so accordingly his/her accountability. In the case of the SSP, each additional "independent veto participant" (independent of the SSP line organization) necessarily raises the ultimate accountability for safety to higher levels in the organization (i.e., the reporting path(s) convergent point). This "authority" versus "independence" tradeoff would necessarily be a critical part of any discussion of organizational changes contemplated by NASA.

**Opportunity #4: Enhance Management Structure of Future Human Space Flight Programs**

The NR example attests to the success of closely linking requirements ownership, design specification development, operational experience and utilization of lessons learned.

NASA has the opportunity to expand the functional closed-loop relationship (shown in Figure 3.3) into a notional management structure to provide greater requirements clarity and more effective organizational performance while ensuring organizational learning. It is envisioned that this model can be implemented for new programs within the NASA Human Space Flight Enterprise or used as a functional template to verify the potential effectivity of proposed management approaches. Closed-loop linkage should be demonstrable for the following key elements:

1) Technical Requirement Ownership (high-level functional requirements),
2) Technical Requirements Development for New Programs & Projects and continuous review and updating for operational systems,
3) Lessons Learned Utilization (acquisition, dissemination and incorporation) based on operational experience.

NASA may also wish to critically consider the basic approach toward requirements management for new Human Space Flight programs. As discussed in section 4.1 there are at least two schools of thought on this topic. The first approach, currently used by SSP, is to set high goals and issue waivers when the goals cannot be met, thereby simultaneously triggering a rigorous risk management process. The second approach is to establish achievable requirements through a traditional, up-front requirements/design tradeoff analysis process, thereby minimizing the number of waivers that result during design, development, and operational phases.

**Opportunity #5: Employ Selected NAVSEA Approaches to Create A Stronger NASA Systems Safety Performance**

While NASA has, over the years, provided extensive training in various (safety and risk management) tools and techniques and has indeed emphasized the need for all members of the NASA team (contractors as well) to continually place safety first there has been relatively little emphasis on system safety and programmatic (decision making) aspects of safety as a universal underpinning for all program and project managers. In addition, formal independent verification audits related to safety behavior implementation within programs and projects has been limited to periodic reviews and assessments, primarily at a safety process level.

### 5.1 Create Special Emphasis System Safety Training Programs

Implement training activity that is mandatory, recurrent, and has the presence and imprimatur of senior NASA leadership and management. The training must emphasize the themes of systems thinking, systems safety, and the individual responsibility for safety with each program or project team member. The responsibility to participate in the training must be incorporated, as a mandatory element into each employee's performance plan and training and development plans.

Proposed training themes include:

- *Safety Critical Decision Making* - Recognizing safety implications in decisions; balancing competing cost and schedule factors versus safety; recognizing "creep" or erosion of technical requirements or safety procedures (understanding past changes or relaxation of requirements that have affected safety); when and how to "push-back" against budget and schedule, recognizing and understanding group dynamics in decision making processes;

- *Complex System Failure Reviews* - Recurrent, mandatory safety training on highly complex, tightly coupled systems failures on NASA programs (e.g., Challenger Launch Decision), as well as experiences on other non-NASA programs (e.g., USS THRESHER, USS BONEFISH);

- *Critical Skill Certification* - Mandatory, recurrent system safety training for all civil servants and contractor personnel in their specialty or area of responsibility (decision makers, technicians, inspectors, test conductors, assurance personnel), leading to certification or authorization to perform specific safety-critical job responsibilities.

### 5.2 Establish Organizational Processes to Promote Better Communication and to Advance and Support Consideration of All Opinions

- *Differing Opinions:* NASA may wish to implement mandatory training for all managers that incorporates dynamic decision making role-playing scenarios in which different opinions are struggling for a voice. NR systematically promotes the airing of

all opinions and recognizes that, when no differing opinions are present, it is the responsibility of management to ensure critical examination of all aspects of an issue. Secondly, NR places emphasis on "over-communication" as a management/cultural approach to avoid under-communicating critical information.

- *Alternative/Differing Opinion Channels:* NASA currently employs traditional, hierarchical, line management reviews leading up to the Flight Readiness Review in the Space Shuttle Program. The formal FRR can be an intimidating venue in which to raise a technical issue not fully supported with data. This is especially true because the FRR is the culmination of numerous reviews leading up to the FRR. The Space Shuttle Program also implements the Systems Safety Review (SSRP) process and the Payloads Safety Review Panel (PSRP) process. The NASA SMA community implements the Space Shuttle Pre-Flight Assessment Review (PAR) Process. The PAR process provides a less intimidating route for personnel to raise issues. The PAR is primarily conducted within the S&MA community. Finally, there also exists the anonymous NASA Safety Reporting System (NSRS) that provides a separate path to the top of the organization available to all NASA and contractor employees who have a safety concern.

One possibility for NASA to consider is the introduction of an alternative technical "court of appeal" chaired by the IED (chartered by the Chief Engineer - see opportunities #1 and #3) in which safety critical engineering issues can be addressed. While requiring data to the extent possible, the forum would be open to engineering judgment and opinions not fully supported by data. This would serve as an intermediate communication forum to promote the necessary technical dialogue critical for success in high reliability organizations.

- *Review/Strengthen Existing Boards/Panels and Review Fora:* NASA should critically examine the numerous existing boards and panels to evaluate where improvements can be made to assure access and to more effectively drill down into safety issues.

### 5.3 Improve Functional Audit Processes to Independently Verify Safety Behavior

Cultural evolution and change require management leadership, time, repeating the message, training, and perhaps changes to processes. One important ingredient in facilitating change is the independent verification that the desired behaviors are taking root. Again borrowing from the NR and SUBSAFE cases, one observes a strong emphasis on both functional as well as certification audit. {See NNBE Interim Report pages 18-19.} The audit process is clearly the means of measuring (independently verifying) behavior and process discipline. The independent safety compliance organization identified in opportunity #2 should be tasked to recurrently verify the implementing organization's functional capabilities, and to verify compliance with the program/project baseline safety and mission assurance requirements. The functional audit results would be reported to the Program Manager and to the implementing center director.

**Opportunity #6: Implement a Process Sponsor Program**

NASA may wish to consider formal adoption of an analog to the NR Process Sponsor Program. This program formally identifies top technical and process experts representing a broad spectrum of safety critical disciplines in the materials and manufacturing arena. These individuals would represent a NASA-wide resource capability to support program/project managers, as well as a source of expertise to serve on technical committees, review boards, and audit teams.

It is envisioned that the program would be implemented as a collaboration between the NASA Office of Safety & Mission Assurance and the Chief Engineer's Office. Implementation may also involve participation of the NASA sponsored Quality Leadership Forum (QLF) and the NASA Engineering and Quality Audit (NEQA) Program. The activity is a potential element of the proposed NASA Engineering and Safety Center and would also be supported through the NASA Process Based Mission Assurance (PBMA) Knowledge Management System (KMS), Knowledge Registry, currently in development.

# Appendices

**Appendix A: NR Hosted Events & TIMs**
**Appendix B: Summary of Key Observations**
**Appendix C: Framework for Independent Assessment**
**Appendix D: NNBE Acronyms and Terms**

## Appendix A: NR Hosted Events & TIMs

| Date | Event Description | Event ID# |
|---|---|---|
| October 1, 2002<br>8:30 am – 4 pm | Nuclear Systems Theme Planning Meeting at Washington Navy Yard | 10A |
| January 30, 2003<br>9am – 12 pm | Follow-up Planning Discussions with NR | 10B |
| May 15, 2003<br>9 am –12 pm | Challenger Launch Decision Training at WNY | 40 |
| June 9, 2003<br>1 pm – 4:30 pm<br>June 13, 2003<br>8 am – 4:30 pm | NR Classified Discussions<br>1) Management / Organization / Culture<br>2) Requirements / Policy<br>3) Process Implementation<br>4) Verification<br>5) Certification | 10C |

### October 1, 2002 — Nuclear Systems Theme Planning Meeting at Washington Navy Yard

On October 1, 2002, the NNBE team met with NR to receive an overview briefing on the NR organization and discuss a framework for analysis to benchmark the nuclear systems theme of the benchmark exchange. The NR Director, Admiral Frank Bowman, addressed the group.

### January 30, 2003 — Follow-up Planning Discussions with NR

The NNBE met with NR again on January 30, 2003, to receive additional background information on the NR organization and to plan future benchmark exchange events.

### May 15, 2003 — Nuclear Systems Theme Planning Meeting at Washington Navy Yard

The NNBE team attended a 3-hour NR training seminar on the Challenger Launch Decision on May 15, 2003, at the Washington Navy Yard. ADM Frank Bowman kicked off the 143rd training seminar with introductory comments. Since 1996, the Knolls Atomic Propulsion Laboratory has provided this training for over 5,000 NR Program personnel. The seminar consisted of a technical presentation of the solid rocket motor O-ring failure and the timeline of events that led up to the accident entitled "The Challenger Accident Re-examined" given by Dr. Charlie Thompson, a materials engineering expert at KAPL. The presentation was followed by Q&A discussion of the lessons learned led by Mr. Mike Quinn, General Manager, KAPL. The training focused on engineering

lessons learned. Both ADM Bowman and Mr. Quinn emphasized that nothing was being changed in the standard seminar as a result of the loss of Columbia or for NASA's benefit.

## June 9 and 13, 2003 NR Classified Discussions

On June 9 and 13, 2003, the NNBE team met with NR to discuss in detail the five areas listed below. In addition, the team conducted classified discussions on specific tools, techniques, and processes that NR implements to ensure safety, including the effective results of implementing them.

1. NR management, organization, and culture from a safety perspective, including discussion of safety assurance processes implemented by prime contractors, how organizations interact in matters pertaining to reactor safety, and key contributors to success in ensuring reactor safety.

2. Discuss Uniform Technical Requirements System with special identification of safety documentation.

3. Discuss internal controls (e.g., concurrence process), important design assurance tools, and reporting of incidents and their corrective actions.

4. Discuss compliance verification, including functional audit, evaluation processes, and independent reviews.

## Appendix B: Summary of Key Observations

| Summary of Key Observations  | |
|---|---|
| **3.1** | **Management, Organization & Culture** |
| | • NR has total programmatic and safety responsibility for all aspects of the design, fabrication, training, test, installation, operation, and maintenance of all U.S. Navy nuclear propulsion activities.<br><br>• NR is a flat organization with quick and assured access to the Director – about 40 direct reports from within HQ, the field offices, and prime contractors. Communications between NR headquarters and prime contractors and shipyard personnel occurs frequently at many levels, and a cognizant engineer at a prime or shipyard may talk directly with the cognizant headquarters engineer, as necessary.<br><br>• The Naval Nuclear Propulsion Program (NNPP) represents a very stable program based on long-term relationships with three prime contractors and a relatively small number of critical suppliers and vendors.<br><br>• NR embeds the safety and quality process within its organization; i.e., the "desired state" of an organization is one in which safety and quality assurance is completely mainstreamed.<br><br>• NR relies upon highly qualified, highly trained people who are held personally accountable and responsible for safety.<br><br>• Recurrent training is a major element of the NR safety culture. NR incorporates extensive outside experience (Challenger, Chernobyl, Three Mile Island, Army SL-1 reactor) to build a safety training regimen that has become a major component of the NR safety record – 128,000,000 miles of safe travel using nuclear propulsion.<br><br>• NR promotes the airing of differing opinions and recognizes that, even when no differing opinions are present, it is the responsibility of management to ensure critical examination of an issue. |
| **3.2** | **Safety Requirements** |
| | • NR has an institutionally embedded closed-loop process that begins with a technical requirements base built on lessons learned from more than 5,400 reactor years of experience, which in turn represents the foundation for the next-generation propulsion plant design specifications.<br><br>• There does not exist a single (stand-alone) document that prescribes NR design safety criteria or standards. The safety requirements are embedded in a uniform set of technical requirements. |

| Summary of Key Observations | |
|---|---|
| | • NR exercises rigorous change control through a process that ensures each recommended change is reviewed (and concurred in) by all the appropriate stakeholders. Managing Change is frequently discussed at senior levels. |
| **3.3** | **Implementation Processes** |
| | • Each independent lab general manager is required to be technically competent and is directly responsible for the safety of the reactors and facilities under his/her cognizance.<br><br>• The NR Director exercises (by law) direct supervision over the laboratories.<br><br>• Review by external organizations (such as Quality Assurance or Safety) does not diminish the responsibility of the line organization for program/product safety.<br><br>• Based on NR's organizational structure and culture of responsibility, there is not a separate systems engineering group or a job category of "systems engineer" within NR. While there is no single individual who serves as system safety engineer or integrator, there is, however, an individual (Reactor Safety and Analysis Director) responsible for maintaining an overall design safety perspective.<br><br>• Responsibility for safety of an action remains with the authoring engineer and his Section Heads. The Reactor Safety and Analysis Section reviews, consults and concurs in decisions on product nuclear safety aspects, but responsibility for product safety remains with the cognizant engineer and engineering organization.<br><br>• The Reactor Safety and Analysis Section has an independent and equal voice in design and operational decisions.<br><br>• Lessons Learned from more than 50 years of the NNPP have been documented and applied in an evolutionary fashion to each program to reduce operational risk and uncertainty.<br><br>• "Freedom to Dissent" is a primary element within NR.<br><br>• Emphasis on recruiting, training, and retaining the "very best people" for their entire careers is considered systemic to the success of NR.<br><br>• Critical self-evaluation of problems with strong Headquarters oversight is the tool of choice to isolate and control the small problems before they escalate into large problems.<br><br>• Closed loop corrective action is mandatory to NR's success. Problems must be identified, analyzed, and resolved and their resolutions proven successful. |

| Summary of Key Observations | |
|---|---|
| | • Cause analysis is performed via a formal fact-gathering critique, supplemented by expert assessment of root cause/corrective actions.<br><br>• Heavy emphasis is placed on ergonomics in reactor design through the use of various methods, such as interactive visualization techniques, walk-throughs, and discussion with operators. Operational human factors are also emphasized; but in both cases, change for the sake of change is not permitted. |
| **3.4** | **Compliance Verification Processes** |
| | • NR emphasizes that "Silver Bullet Thinking is Dangerous" -- "there is no silver bullet tool or technique." All elements ("across the board") of quality assurance and compliance assurance must be rigorously implemented to ensure delivery and operation of safe, reliable, and high quality systems.<br><br>• NR audit teams include the requirement owner (technical authority) for a particular area. The owner participates in the audit process so that he/she can acquire a first-hand understanding of how the technical requirements are (or are not) being implemented.<br><br>• NR field offices act as day-to-day audit and inspection groups. Responses to their findings are required, and they must approve final actions in response to major comments.<br><br>• Functional audits of shipyards are supplemented by field office assessments and comparative evaluations of the site's own self-assessments.<br><br>• Qualification and biennial re-qualification of all nuclear operators by written examination and oral board examination assures currency of skills. In addition, the NPEB administers an annual examination to the entire engineering department of a ship and reports results to the ship's CO, the command authority for that ship, and NR Headquarters.<br><br>• DCMA is used by NR, but is given technical direction by NR directly rather than by DCMA Headquarters.<br><br>• NR maintains a Process Sponsor Program in which the engineering activity retains technical responsibility for its components but consults with process experts (sponsors) within their identified areas of responsibility, as necessary. |
| **3.5** | **Certification Processes** |
| | • NR performs incremental audits (similar to SUBSAFE) prior to key events to evaluate critical processes and to correct any problems with work accomplishment or critical documentation. |

| Summary of Key Observations | |
|---|---|
| | • A seven-phase test program begins with visual check of installation and progresses through higher levels of detail to actual operation of the reactor and delivery of power to assure readiness of the reactor plant for sea trials.<br><br>• A Joint Test Group (JTG), composed of representatives from the construction shipyard, NRRO, Ship's Force, and the cognizant laboratory, reviews and approves the administration and performance of test documents and acceptance of test results. |

## Appendix C: Framework for Independent Assessment

The NASA NNBE core team defined the following framework to assist our discussions of independent reviews:

Level of Independence – NASA NNBE Hierarchy

- Type 0 Independence: Program/Project Manager's In-Line Checking Functions / Reports Assessment to Program Manager (e.g., SSP/SMA managers, quality assurance, inspection, DCMA, KAPL and Bettis Lead Design Project Managers)

- Type 1 Independence: In-Line Resources for Assurance Activity / Reports Assessment to Authorities Within Upper Line Management (NASA/HQ OSF Review Team, KAPL and Bettis Managers not assigned lead design role)

- Type 2 Independence: Organizationally funded / Not In-Line / Reports Assessment to Upper/Top Program Line Management (e.g., NASA SMA Review Team, NASA HEDS Assurance Board, KAPL and Bettis Safety Review Organizations, NR Director for Reactor Safety & Analysis)

- Type 3 Independence: Organizationally funded / Not In-Line / Reports Assessment to Organizational Authority Outside (above) Program Line Management (e.g., NAVSEA 07Q, NASA Aerospace Safety Advisory Panel)

- Type 4 Independence: Organizationally Funded / Reports Assessment to Authorities Outside Organization (e.g., funded by NASA and reports to Congress or White House - Gehman Board, Rogers Commission, Nuclear Regulatory Commission and Advisory Committee on Reactor Safeguards review of NR designs)

- Type 5 Independence: Receives Resources From A Different Organization and Reports to a Different Organization (General Accounting Office).

In discussing degree of independence, it is also important to recognize that current and specific knowledge of a subject is often inversely correlated with degree of independence. Conversely, a more independent entity is often not current or well informed about a specific subject area.

Table C.1 Independence Dilemma

| | Lesser Current/Specific Technical Knowledge | Greater Current/Specific Technical Knowledge |
|---|---|---|
| Less Independence | | **X** |
| Greater Independence | **X** | **Desired State** *Difficult to achieve* |

**Framework for Independent Assessment (continued)**

Subject of Independent Assessment (examples)
- Government Program Management Capability (Functional Audits)
- Contractor Program Management Capability
- Contractor Implementation Processes
- Specific Technical or Management Decision
- Design Verification
- Manufacturing Verification
- Pre-Operations Safety Certification

Type of Independent Activity (examples)
- Focused Briefings
- Interviews
- Structured Surveys
- Inspection (process observation)
- Attending Meetings (process observers)
- Analysis and modeling

Strength of Independent Activity
- numbers of personnel
- experience of personnel
- knowledge of personnel

Frequency of Independent Review (examples)
- One-time Snap-shot
- Recurrent Snap-shots (longitudinal)
- Annual
- Biennial
- Ongoing (resident offices)

Scope of Independent Activity (singular or in combination)
- Technical performance
- Cost
- Schedule
- Safety/mission assurance

**Framework for Independent Assessment (continued)**

Another perspective on independence (spanning big "I" to little "i") is presented in Table C.2. mapping degree of independence versus organizational and funding factors.

| Independence | Organization | Different Internal Organization | External Organization | Independent Contractor | Independent Funding | External to Enterprise | External to Agency |
|---|---|---|---|---|---|---|---|
| i | Contractor SMA | X | | | | | |
| i | NASA Project SMA | X | X | | | | |
| i | Center (matrixed) SMA | X | X | X | | | |
| i | Center Independent Assessment; | X | X | X | X | | |
| I | HQ Code Q, NAC, ASAP, IV&V, NESC | X | X | X | X | X | |
| I | GAO, IG, Congress, OSHA | X | X | X | X | X | X |

## Appendix D: NNBE Acronyms and Terms

| | |
|---|---|
| AA | Associate Administrator |
| ACRS | Advisory Committee on Reactor Safeguards |
| ADDU | "Additional Duty" |
| AEC | Atomic Energy Commission |
| AOCWI | Acceptance of Completion of Work |
| ASAP | Aerospace Safety Advisory Panel |
| Availability | Availability of ship/depot for required maintenance |
| BPMI | Bechtel Plant Machinery, Inc. |
| BRES | Bettis Reactor Engineering School |
| CCL | Certification Checklist |
| CIO | Chief Information Officer |
| CNO | Chief of Naval Operations |
| CO | Commanding Officer |
| COMNAVSUP | Commander Navy Supply Systems Command |
| COMSPAWAR | Commander Space and Naval Warfare Systems Command |
| CTE | Chief Test Engineer |
| CWR | Completion of Work Review |
| DCMA | Defense Contract Management Administration |
| DOE | Department of Energy |
| EOD-TD | Explosive Ordnance Disposal-Training Department |
| EOOW | Engineering Officer of the Watch |
| *Fora* | Forums |
| FRR | Flight Readiness Review |
| GAO | General Accounting Office |
| HEDS | Human Exploration and Development of Space |
| HM&E | Hull, Mechanical and Electrical |
| IED | Independent Engineering Director |
| IG | Inspector General |
| ISD | Independent Safety Director |
| ISS | International Space Station |
| IV&V | Independent Verification and Validation (software) |
| JCS | Joint Chiefs of Staff |
| JSC | Johnson Space Center |
| JTG | Joint Test Group |
| KAPL | Knolls Atomic Power Laboratory |
| KMS | Knowledge Management System |
| KSC | Kennedy Space Center |
| LLIS | Lessons Learned Information System |
| MOA | Memorandum of Agreement |
| MSFC | Marshall Space Flight Center |
| NAC | NASA Advisory Council |
| NAVSEA 03: | Human Systems Integration in System Design |
| NAVSEA 04 | Logistics, Maintenance, & Industrial Operations |
| NAVSEA 05 | Ship Design Integration & Engineering |

| | |
|---|---|
| NAVSEA 07 | Undersea Warfare |
| NAVSEA 07Q | SUBSAFE / Quality Assurance Division |
| NAVSEA 07T | Submarine HM&E Management Division |
| NAVSEA 08 | Naval Reactors |
| NAVSEA 92Q | SUBSAFE/Quality Assurance |
| NAVSEA | Naval Sea Systems Command |
| NEQA | NASA Engineering and Quality Audit |
| NESC | NASA Engineering & Safety Center (proposed) |
| NNBE | NASA/Navy Benchmarking Exchange |
| NNPP | Naval Nuclear Propulsion Program |
| NNSA | National Nuclear Safety Administration |
| NOSSA | Navy Ordnance Safety and Security Activity |
| NPEB | Nuclear Propulsion Examination Board |
| NR | NAVSEA 08, Naval Reactors |
| NRC | Nuclear Regulatory Commission |
| NROTC | Navy Reserve Officer Training Corp |
| NRRO | Naval Reactors Representative Office |
| NSRS | NASA Safety Reporting System |
| NUWC | Naval Underwater Warfare Center |
| OPNAV | Office of Chief of Naval Operations |
| OQE | Objective Quality Evidence |
| OSF | Office of Space Flight |
| OSHA | Occupational Safety and Health Administration |
| OSMA | Office of Safety and Mission Assurance |
| ORSE | Operational Reactor Safeguards Examination |
| PAR | Pre-flight Assessment Review |
| PBMA-KMS | Process Based Mission Assurance - Knowledge Management System |
| PEO | Program Executive Officer |
| PEO SUB | Program Executive Officer - Submarines |
| PM | Program Manager |
| PRCB | Program Requirements Control Board |
| PRL | Prerequisite List |
| PSRP | Payloads Safety Review Panel |
| QLF | Quality Leadership Forum |
| RSRM | Reusable Solid Rocket Motor |
| SEALOGCEN | NAVSEA Logistics Center |
| SECNAV | Secretary of the Navy |
| SFOC | Shuttle Flight Operations Contractor |
| SMA | Safety and Mission Assurance |
| SR&QA | Safety, Reliability, and Quality Assurance |
| SRB | Solid Rocket Booster |
| SSME | Space Shuttle Main Engine |
| SSP | Space Shuttle Program |
| SSRP | System Safety Review Process |
| STE | Shift Test Engineer |

| | |
|---|---|
| SUBMEPP | Submarine Maintenance Engineering, Planning and Procurement |
| SUBSAFE | Submarine Safety |
| SUPSHIP | Supervisor of Shipbuilding, Conversion and Repair |
| SYSCOM | Systems Command |
| TIM | Technical Interchange Meeting |
| TMI | Three Mile Island |
| TWD | Technical Work Document |
| WNY | Washington Navy Yard |
| XO | Ships' Executive Officer |