LESSONS LEARNED FROM CHALLENGER

HEADQUARTERS
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

SAFETY DIVISION

OFFICE OF SAFETY, RELIABILITY,
MAINTAINABILITY AND QUALITY ASSURANCE

WASHINGTON, DC 20546

FEBRUARY 1988

Foreword

The expression Lessons Learned has been an important concept in NASA and aerospace industries for many years. It was conceived as a tool to perpetuate experience and keep from repeating costly mistakes. If this is to be done, the lessons must not only be learned - they must be remembered. Experience has shown that as management systems and key people change the lessons are forgotten. The crucial messages generated from the review of the Challenger accident must not be lost. We must keep them alive and readily retrievable to:

- Help engineers build safety into their basic designs.
- Provide check lists for trade studies and for development testing.
- Help structure verification and validation plans and procedures.
- Focus attention on high risk areas in management systems.
- Provide punch lists for real-time risk assessment to be used in consideration of deviations and waivers.
- Identify and develop detailed remedial actions to correct weaknesses in management evidenced by mistakes, failures, accidents, mishaps and safety problems.
- Assist in prioritizing management attention in areas particularly vulnerable to critical oversights and human errors.
- Help evaluate safety risk conditions.

If all of these objectives are to be accomplished effectively, the lessons learned information must be entered in computer files with insight into its many eventual uses, and once retrieved, it must be recast to fit the specific application at hand. This task is not easy, but it is possible with skilled and dedicated people. The uses of these materials are limited only by the creativity and determination of the lessons learned practitioner. The payoff - to keep from repeating costly mistakes - is worth the effort.

George A. Rodney
Associate Administrator for
Safety, Reliability, Maintainability and Quality Assurance
National Aeronautics and Space Administration

Preface

Results of this lessons learned study of the Space Shuttle Challenger accident is documented in two reports: Lessons Learned From Challenger and Space Station Lessons Learned From Challenger. The first report records problems, causes and generic lessons learned for potential application to all ongoing and future programs and will be used by the Office of Safety, Reliability, Maintainability and Quality Assurance Code Q, as part of the lessons learned transfer process. The second report extends the developed lessons learned to specific recommended applications for the Space Station Program and will be used in its ongoing program planning and implementation.

This study was performed for the Safety Division, Code QS, by a contractor team headed by Planning Research Corporation. Supporting team members were JLC Aerospace Corporation and Risk Management Associates, Inc. In process study review was provided by both Code Q and the Space Station Program, Code S.

Successful transfer of lessons learned necessitates joint study team efforts of this type, but specific continuing emphasis is required to assure that lessons are retained and applied to all programs. The format of the lessons learned portion of this report has been prepared to permit incorporation in computer files for tracking and reporting of applications. These active files with associated checklists and periodic reviews is a primary method to assure retention of lessons learned.

Robert H. Thompson
Director, Safety Division
Office of
Safety, Reliability, Maintainability and Quality Assurance
National Aeronautics and Space Administration

Contents

Section I – Introduction

1.1 Background

After the loss of the Space Shuttle Challenger on January 28, 1986, extensive governmental investigations were conducted, primarily by two groups: The Presidential Commission on the Space Shuttle Challenger Accident and the U. S. House of Representatives Science and Technology Committee. Their purpose was to identify the causes of the accident and to make recommendations regarding a safer Space Shuttle and a more effective NASA.

In late 1986 after publication of reports from these investigating groups, it was recognized by both the Space Station Program management and the newly appointed NASA Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance (AA/SRM&QA), that future application of lessons learned from the accident would be of significant value to the agency and especially the Space Station Program. This belief coincided with that of the House Committee:

> *"Although the Committee's concern and evaluation in this report are specifically related to the effective functioning of NASA's Space Shuttle Program, it should be understood that the larger objective and the greater responsibility are to insure that NASA, as the Nation's civilian space agency, maintains programmatic excellence across the board.*
>
> *"What we as a Committee, NASA as an agency, and the Nation as a whole, also must realize is that the lessons learned by the Challenger accident are universally applicable, not just for NASA but for governments and for society....NASA and Congress must remember the lessons learned from the Challenger Accident."*

This Congressional interest combined with the fundamental benefit recognized by NASA to be derived from such an effort, resulted in the initiation of a task designed to answer the question: "What actions are necessary in Space Station development and operations to take advantage of the lessons learned from the Space Shuttle Challenger accident?" Four basic steps were identified as necessary for task completion:

1) Analyze the Challenger accident. Using the results of work performed by the Presidential Commission and the House Science and Technology Committee as primary source documents, analyze the events surrounding the accident. Where possible, use NASA internal reports and responses to the two primary group's own reports to supplement the lessons learned development.

2) Develop a set of consolidated lessons learned. Document results of this analysis in the form of generic program lessons learned.

3) Determine Space Station potential applications. Based upon an evaluation of Space Station development and operations planning, derive measures to apply the lessons learned.

4) Conduct follow-on implementation. When completed, the study would yield a basis for actual implementation actions on a detailed level showing traceability to specific lessons learned. Space Station Program management in conjunction with the AA/SRM&QA, would then decide appropriate follow-on actions.

The first three steps of the agreed-upon task were combined into a single study which is the subject of this report.

1.2 Study Approach

Implementation of the lessons learned application study was assigned to the AA/SRM&QA Safety Division; a contractor study team was selected; and a NASA review team was established with representatives from both SRM&QA and Space Station. Study task descriptions and milestones were finalized and work was initiated in June 1987. Primary source documents are listed in Figure 1-1. Related reference documents are listed in Figure 1-2.

As part of the first study task, Problem and Cause Analysis, program elements were identified and problem areas grouped within the elements illustrated by Figure 1-4. This organization provided the framework for identification of consolidated problems and their causes from which generic lessons learned and Space Station applications could be developed. This Final Report documents study results under the fifth study task.

Problems, causes, lessons learned and applications are provided in Section III of this report as items 1 through 29. Numbered references are listed in Appendix A keyed to corresponding paragraphs by the paragraph numbers.

Figure 1-1. Source Documents

Figure 1-2. Related Reference Documents

Figure 1-3. Program Element Organization for Lessons Learned

Section II – Lessons Learned Discussion

2.1 General

A single underlying and pervasive problem, and as a result some inescapable conclusions, emerge from discussion items in this analysis and from investigations and testimonies reviewed in the reference documents. While some critical voids in the overall management system existed at the time of the 51-L accident, the basic problem was not so much lack of management system definition as it was lack of management system control. Some requirements in the system were ignored by both management and the work force; a breakdown in communications existed from top-level management to workers on the floor; there was a willing abandonment of some critical management controls. Managers were pressuring the work force to break management rules in an attempt to maintain flight schedules.

To put this condition in proper perspective, it should be noted that the United States space program was built on innovation and willingness to circumvent or waive the rules to make productive things happen. It is impossible to conceive of a tight management system that would offer complete control over unforeseen problems and contingencies. There will be times when rules have to be circumvented or waived to accommodate urgent demands of the moment. Conversely, it should be recognized that this philosophy can promote ill-conceived judgements and human errors if uncontrolled or taken to extremes.

The Space Station Program should have a policy that management rules and requirements must be followed, unless to do so would cause greater problems and risks. If the rules must be broken, it must be accomplished in a manner which ensures that all people and organizations having critical inputs and oversight management responsibilities know about the deviations in time to make deliberate and prudent decisions. When rules are circumvented or waived, especially in a repetitive manner, assessments of the existing management system must be made to determine if changes to the system are required to eliminate the need for those deviations in the future. Also, it should be remembered that communication with the work force is crucial to the entire process. For in the end, it is people - down to those who are engaged in the most fundamental tasks - who ultimately control the success or failure of any complex endeavor.

2.2 Program Elements

Lessons learned and Space Station applications are summarized for discussion purposes under the seven basic program elements illustrated in Figure 1-3. A fundamental message for each element has emerged from the analysis. These messages are axiomatic, even philosophical, but need to be documented as a reminder of the 51-L accident and as a stimulus to prevent future occurrences.

> *Provide continual, independent, program oversight and program review functions that emphasize safety.*
>
> *Ensure quality program and safety management that have clear definition of authority and responsibility and have resources commensurate with requirements.*
>
> *Maintain comprehensive and effective program processes and systems that support the safety risk management function.*
>
> *Maintain realistic plans that have provisions for flexibility, minimize outside pressures and stress flight and ground safety.*
>
> *Control effectively the development of critical items with respect to performance, environments, tolerances, margins, manufacturing processes, testing and safety.*
>
> *Implement the transition from development to operations with careful attention to criteria establishment, management structure, management systems, enhancements and safety.*
>
> *Ensure quality performance of work force involved in safety critical operations including adherence to required procedures and constraints.*

Subsequent paragraphs of this discussion expand these basic messages and introduce the individual lessons learned contained in Section III.

2.3 Program Oversight

Emphasize SRM&QA at all levels.

SRM&QA efforts were curtailed and manpower was reduced because of the perception that the NSTS had reached an operations phase. It was not recognized that the very nature of any space venture dictates a measure of assurance efforts that continue throughout program life to maintain a healthy balance between safety, performance, costs and schedules. The Space Station with its many interfaces between nations, organizations, R&D projects and various types of operations from ground operations to logistics, to fabrication in space, to on-board experimenting and to space-launch, will need considerable SRM&QA resources to maintain acceptable safety risks. Due to the dynamic nature of the Space Station and the continuing change in configuration and operations profiles, SRM&QA resources will have to be continually assessed to ensure the proper levels of effort and efficacy of the assurance functions at all program levels.

Provide independent SRM&QA oversight.

The 1986 Shuttle accident and the 1967 Apollo accident both have confirmed that without independent SRM&QA oversight, sooner or later, the urgent demands of meeting costs and schedules will lead to imprudent decisions affecting safety risks. This was recognized by the 51-L Presidential Commission and Congressional Committee and is now a part of the NASA management policy expressed in the responsibilities of the Associate Administrator for SRM&QA. With the advent of this new policy it was recognized also that this independence would be a difficult accomplishment in light of the workload necessary to carry out the primary SRM&QA responsibilities of the programs and the limited number of skilled assurance discipline people available. The complexity of the Space Station program will make this task of maintaining independent oversight a difficult job. Oversight functions which lead to independent assessments for safety critical operations will have to be factored into both on-board and ground design and operations review processes. In turn, this will necessitate many dual-role SRM&QA position responsibilities both on orbit and ground.

Base safety risk determinations on hard facts.

The decisions leading to go-ahead for 51-L launch were not based on valid environmental and performance analyses and test data. Instead, the decisions were made to fit the expediency of launch schedules. Questions were constituted in the form which elicited answers fitting a why we should not launch rather than why we should launch philosophy. The schedule type of pressures are indemic to space operations. There will be times in the Space Station Program where situations similar to the 51-L launch operations decision process will occur. Go-ahead for all hazardous operations must be based on hard facts and deliberate analyses. In turn, acceptance of safety risks must be determined formally and at the proper level of management.

Audit for compliance periodically.

One of the consequences of perceiving the NSTS to be in an operations phase and the subsequent reduction of SRM&QA resources was the drastic reduction of assurance audits by NASA and its contractors. In turn, this led to an inordinate reliance on paper verifications of requirements compliance rather than physical validation checks. Many of the critical non-compliance deficiencies pointed out by the 51-L investigation reports were the type that are routinely highlighted and corrected as a result of SRM&QA audits. Space Station must maintain a vigorous audit program throughout its life to avoid the consequences of non-compliance.

Ensure effective problem resolution.

The NSTS problem resolution system did not identify the SRB aft seal joint and other safety critical problems above Level III management review. While this was not the total cause of the improper dispositioning of the aft-seal joint problem, it did lead to a lack of visibility and focus of top-level management in addressing and resolving the problem. To avoid these mistakes, Space Station must maintain a comprehensive problem reporting and corrective action

(PRACA) system which includes all critical safety problems and establishes criteria for resolution of these problems at each level of management review.

2.4 Program Management

Define clearly authority, responsibility and interfaces.

There were many changes in the NSTS program, contractor and SR&QA organizations prior to the 51-L launch. In turn, authorities, roles, responsibilities and interface relationships were changed and transitioned to new operations contractors from NASA internal organizations and its development contractors. While reorganization was necessary because of changing requirements, there were some responsibilities that were lost in the handover and other responsibilities that lost their specific definition, especially in interface areas. In SSP the problems of evolving and changing authorities, responsibilities and interfaces will be continual and will increase significantly with first integration, launch and on-orbit assembly of Station elements. The impacts must be minimized by careful and judicious planning of changes at non-critical points in the Program. In addition, there must be a constant vigilance and meticulous reconciliation of authorities, responsibilities and interfaces to assure that critical management functions are covered during any change in content or organizational elements throughout the program.

Include definition of dual responsibilities.

Many dual responsibility roles for in-line program and assurance management systems are necessary due to limitations in availability of technical or specialist personnel. Part of the confusion in responsibilities that existed prior to 51-L was a result of these dual roles being inadequately defined. Personnel were required in some cases to perform work and then were required to make judgements on how well it was done. While this task is not impossible, it is one that is contrary to human nature. Meticulous attention must be given to the definition of dual-role responsibilities to preserve independence for both program and technical review processes through various levels of management and SRM&QA oversight.

Maintain adequate SRM&QA skills and resources.

NASA and its contractor SR&QA resources (both funding and personnel) atrophied over a period of years prior to the 51-L launch. In addition, many professionals filling the limited positions did not understand the complex engineering and operations details necessary for effective performance. Also, many of the more experienced professionals left the agency and its contractors during this time. While presently the budget for SRM&QA has been augmented to restore needed fiscal resources, a serious problem still remains, that of acquiring all the skilled professionals needed to fill the added positions available and those planned with the growth of Space Station. Entry-level and new hire training will be necessary by both SSP and its contractors. In addition, there should be infusion of program design and operations engineers into the SRM&QA disciplines and cross training of experienced assurance engineers in the program line-engineering disciplines. Due to the present scarcity of aerospace assurance engineering talent, recruiting and training programs should be continual and rigorous.

Manage deviation and waiver process effectively.

The deviation and waiver process was not adequately defined prior to the 51-L launch. Some policies and decision criteria for acceptance were unclear and ambiguous. As a result, decisions leading to launch were made without adequate consideration of available engineering data or the consequences of incomplete critical data on performance and margins. Also, no provisions were made for independent assessment in the decision process. The SSP must develop and maintain an effective definition of roles and responsibilities for organizations and personnel involved in the deviation and waiver process. Rigorous methods must be provided for resolution of issues and avenues of appeal for higher-level management decisions.

Ensure that program management is skilled and motivated.

At the time of the 51-L accident, NSTS management had little understanding of the mechanics or principal instruments of safety risk management. Also, many factors contributed to a tired and unmotivated work force with lack of personal commitment to excellence. As a result, launch processing errors were not reported including failure to follow procedures for critical operations. SSP must establish and maintain effective safety risk management which is understood and practiced by both program management and the work force. Criteria should be defined to reduce risks and should be monitored for compliance. The pursuit of excellence which characterized NASA's early space ventures should be revitalized and a vigorous effort maintained to monitor and correct those conditions which lead to demotivation and lowered morale.

Ensure that program critical knowledge is maintained.

Despite the presence of significant amounts of information on the SRB aft field joint problems, both NASA and Thiokol managers failed to understand or accept the seriousness of the situation. In retrospect, the data was there but it was not properly analyzed and packaged to focus the attention of upper management. SSP must not only gather and retain critical information, it must also analyze and package the information so that it facilitates management decision processes including safety risk assessments. The database must also permit recall for addressing repetitive and generic problems. Previous lessons learned must be included.

2.5 Program Processes

Maintain an effective problem reporting and corrective action system.

The NSTS Level II Problem Reporting and Corrective Action (PRACA) System in place at the time of the 51-L launch did not include all of the associated safety problems (e.g., SRB aft field joint was not included). The criteria for selection of reported items was limited to specific categories of failures, anomalies and problems. The system was not designed to report and track corrective actions for all safety problems. SSP must maintain criteria for selection of safety problem reporting that will include all problems involving hazardous operations and mission critical components. PRACA action items should identify effective management review requirements for accepted resolution of each problem.

Include trend analysis and safety risk assessment.

There was no organized trend analysis and safety risk assessment system prior to the 51-L launch. Adverse trends indicating increases in safety risk were prevelant throughout the NSTS system. Also, there was no stated requirement for a safety risk assessment although much of the engineering review process, including the prelaunch operations reviews, addressed some of the issues which might normally be covered in a formal safety risk assessment. SSP must establish and maintain an effective trend analysis system and provide an organized approach to safety risk assessment. All of the incremental parts of the total risk assessment system must be carefully developed so that the inputs from all the NASA and contractor organizations are compatible and facilitate an organized routine and accelerated real-time safety risk dispositioning.

Maintain an effective flight readiness review system.

At the time of the 51-L launch, the flight readiness review system had deteriorated to a quick review of those items which were perceived to be new issues or anomalies from the previous launch. In some cases reviews were conducted by teleconference in the absence of key personnel with presentations curtailed by time constraints. Often there was no record made of other key prelaunch meetings. SSP must provide a rigor in its flight readiness reviews to assure that the consequences of all modifications and changes to Station elements, including processes and test/checkout procedures, are adequately evaluated against the baseline. All organizations and personnel required to validate readiness decisions should be identified and their comments formally recorded.

Maintain an effective assurance information system.

Information necessary to analyze risks and validate the launch decision were either not available or only accessible with great difficulty at the time of the 51-L launch. Performance margins and factors of safety for critical components were not recallable in real time, and in the aftermath of the accident investigation, it was apparent that decisions were made on what was remembered of some critical test data. The SSP planned critical information system must include all information needed to make risk decisions, such as environmental certification limits, operational constraints, performance margins and safety factors. It is imperative that this information be recallable in real time to support critical operations reviews and decision processes.

Maintain an effective engineering change system.

The NSTS change system was basically sound prior to 51-L, however, it was overloaded, and as the flight rate increased, the ability to evaluate, test, certify and implement changes was seriously curtailed. Configuration management was inconsistent and critical Shuttle modifications were backlogged. There were problems also in assigning the proper priorities to complete change items. SSP must provide a system for engineering changes that can keep up with the workload. Provisions should be made to augment the system and personnel necessary to evaluate, test, certify and implement peak change traffic. Backlog trends should be analyzed and the information made available for program schedule and management review.

2.6 Plans

Maintain adequate crew safety planning.

The crew had no escape provisions for the 51-L failure mode even if ejection seats, which were removed after the R&D flights, had been retained. It is well known that no quick and easy solutions to this problem currently exist. Any feasible crew escape system for the boost phase would be limited without a major Shuttle redesign. Space Station has more potential options and some added crew safety risks. Crew emergency situations must be identified and a concerted effort made to provide safe havens in orbit or safe returns for likely emergencies. Those situations where crew safety cannot be ensured should be described in detail and dispositioned through the safety risk management process.

Maintain adequate contractual safety requirements.

The NSTS contracts provide greater incentives to contractors for minimizing costs and meeting schedules than for performance and safety. Also, in many contracts the factors relating to grading of safety and safety deliverables were not properly defined. As a result, there was very little incentive to excel in the safety tasks. SSP must assure that safety is properly incentivized in its contracts; planned contracts should be structured to provide realistic weighting factors. Government and contractor personnel involved in incentive/award fee contract planning and implementation should be trained to assure adequate understanding and expertise in the methods of providing necessary safety incentives. Recently completed SSP Phase C/D procurements should be reviewed to ensure adequate contractual safety requirements.

Maintain adequate safety emphasis in the contractor selection process.

In NSTS many of the contract awards were made with cost as the paramount weighting factor. Generally, SR&QA was evaluated as a part of each of the engineering, manufacturing, support and management factors. This resulted in safety being a non-discriminator or at best a nearly indiscernable weighting factor in the contractor selection process. SSP must provide for proper consideration of SRM&QA when evaluating potential contractors as part of the procurement process. Weighting factors should be commensurate with the safety risks and potential accident costs involved in completion of the contract.

Maintain realistic program plans including critical redesign provisions.

Inordinate schedule pressure brought about by unrealistic planning was probably the most pervasive cause of the 51-L accident. In the zeal to achieve compressed flight schedules, managers ignored the impact on safety risks due to backlog in engineering changes, shortages in spares, elimination of mandatory inspections, deleterious results of worker fatigue and violations of launch constraints. SSP must provide policy and the management climate which assures considered and prudent judgements in balancing safety with schedules, performance and costs. Schedules must be realistically planned to minimize safety risks.

2.7 Development

Control critical environmental and performance specifications.

The SRM aft seal joint assembly was not properly qualified or certified for unusual weather and launch operations environment at KSC. There were failures to define the integrated environmental and performance criteria, to quantify the ambient conditions, to design and test for all expected launch weather conditions and to identify all SRM performance limitations and safety margins. SSP must assure that environmental and performance envelopes for both ground and flight are adequately developed, incorporated and controlled in design and performance specifications for all critical items including distributed systems and integrated station elements.

Control critical tolerances and margins.

The SRM O-ring assembly was not designed with realistic tolerances and margins necessary to sustain operational integrity under actual flight loads, off nominal weather conditions or the degradation associated with reuse requirements. The dimensional tolerances of SRM cases were exceeded with planned reuse; unusually precise tolerances and measurement accuracies were required during assembly; tolerances were routinely waived in launches without an understanding of the consequences of environmental and flight loads; and the degradation effects due to reuse were not analyzed. SSP must assure that the design verification process includes effective analysis and testing to characterize the limits of safe performance and operational environments for all operations critical components. Design tolerances must be compatible with expected process controls and operating conditions including those associated with reuse of these components.

Control critical test specifications.

Parts and material performance and environmental test specifications for the SRM aft field joint assembly were not properly defined. The SRM O-ring specifications did not contain realistic performance or temperature requirements for test and they did not specify certification tests to verify design margin integrity with the expanded case dimensions resulting from reuse. In addition, the putty used in the SRM aft seal joint was not properly specified and certification testing was inadequate. SSP must provide a system to control test specifications for critical components. Operating conditions including likely off-nominal conditions and resulting stress profiles must be accurately transposed into test specifications which will result in validation of all critical margins.

Control critical design characterization and verification.

The parts and materials used in the SRM aft seal joints were not properly characterized and their design margins were not properly verified in qualification and certification testing. In addition, the specifics and extent of the test verification could not be traced through the NSTS management system. SSP must provide a system to assure that critical components and materials are accurately characterized and that critical properties are verified by test and inspection. This must include meticulous accounting to ensure that operations, environmental and performance requirements have been realistically verified and that traceability of data is provided to allow ready access for engineering review and assurance oversight.

Control critical qualification testing.

SRM and SSME qualification testing did not adequately cover conditions of performance and operations specified. In addition, some specifications themselves were incomplete. SSP requirements and procedures documentation must be developed and maintained to ensure comprehensive qualification testing to complete specifications. Integrated testing should include dynamic considerations, environmental conditions, functions and time, duplicating those to be encountered in mission operations to the maximum extent feasible.

Control critical manufacturing and assembly processes.

Neither NASA or its contractors had adequate controls on the quality, consistency or critical manufacturing processes associated with the SRM aft seal joint O-rings and putty. The proprietary nature of these products resulted not only in a lack of understanding of the basic properties, but also resulted in changes in ingredients without certification and approval. SSP must provide a system to adequately control materials, manufacturing and assembly processes for critical components. Processes involving critical items should be prominently labeled critical to assure the proper level of care and a highly disciplined review mechanism should be maintained to ensure compliance with requirements. Proprietary materials should be avoided. Where this is infeasible, tight specifications must be established to ensure that all critical properties can be controlled and verified by nondestructive evaluation and sample testing.

2.8 Transition

Define transition carefully.

NSTS transition from the development phase to the operations phase came suddenly and not enough time, opportunity or resources were programmed to complete the many activities necessary to make the transition successful. Increasing flight rate was given priority over streamlining the management and work processes through automation, standardizing and centralizing management and carefully evaluating the impact of eliminating quality inspections, tests and verification procedures. Transition to operations cannot be accomplished by edict, it must be planned meticulously and accomplished deliberately step by step. SSP must carefully define requirements and provide sufficient time and resources to bring about an orderly transition.

Establish transition criteria.

There were no comprehensive criteria or conditions stated in NSTS to determine the merit of the decision to go from the deliberate "fix-it-before fly" philosophy in the development phase to the operations phase that normally reflects a condition where the risks are acceptable without any major concerns for design imperfections or the ability to meet planned schedules. This transition cannot be made unless there is a yardstick of stated criteria to measure the degree of accomplishment which connotes acceptable safety and mission success risk conditions. SSP must establish these transition criteria for all management processes to assure that conditions or procedures essential to safety or mission success are not modified or deleted.

Transition program management and management systems.

There was no visible effort in NSTS to provide an orderly transition of the management concepts and processes to provide efficient management of the operations phase. All management processes including plans, procedures, support systems, standards and requirements must be reviewed and revised to meet the change in concept and increased tempo of activities. SSP must provide the policy, direction and oversight to assure that the necessary changes in the management systems are implemented at the proper time and are functioning in a manner which promotes efficiency without incurring undue safety risks.

2.9 Operations

Maintain effective operations and maintenance documentation.

The NSTS OMIs were not current, there were numerous errors in procedures and there were improper deviations from approved technical operating procedures during 51-L prelaunch operations, which resulted in significant damage to a SRM segment and to an orbiter payload door. In addition, at launch all OMRSD's were not met, waived or accepted. SSP must maintain an effective operations and maintenance documentation system. There should be sufficient time and resources to develop accurate baseline requirements and documentation and maintain the system current. There should be CDR's and follow-on audits to assure compliance. In turn, operations readiness reviews must include assurance that the requirements are correctly reflected in the appropriate OMI's and other technical procedures. In addition, there must be an OMI review and update prior to any change or modification close-out.

Control critical operating constraints.

The launch constraints and commit criteria were poorly defined and many constraints were improperly removed prior to the 51-L launch. The ambient and component temperatures were outside of the stated certification range of the SRMs. Also, there was a launch constraint on the aft seal joint imposed by MSFC that was removed without proper analysis and review of the anomalous conditions which were exhibited in previous flights. SSP must ensure that realistic operating performance envelopes with reasonable margins and confidence levels are established for critical components. Constraints and limit criteria must be clearly defined and traceable to hardware/software specifications and to environmental and operational stress profiles. Constraints must not be removed without a thorough technical analysis and approval of both the appropriate program and the independent assurance managements.

Maintain quality work force performance.

There were careless mistakes and other evidences of substandard workmanship at the time of the 51-L launch. Some required quality verifications were not being made and some inadvertent damage sustained during pre-launch processing went unreported because of a lack of confidence in company forgiveness policy and workers' consequent fear of losing their jobs. SSP must maintain coordinated personal and team motivation programs. A spirit of pride of accomplishment, the need for excellence and a sense of personal and collective responsibility for all Space Station activities are essential attributes for success. In addition, a free flow of information, mutual trust between management and the work force, well defined work standards and stringent verification of work accomplishment will be required.

Section III – Lessons Learned

3.1 Lessons Learned Organization

This section of the report provides 67 individual lessons learned grouped within 29 potential problem/lesson learned areas and seven typical (generic) program elements, as illustrated in Figure 1-3. This lessons-learned organization was developed by first identifying problem areas from the source documents and then categorizing them in a typical program breakdown. The breakdown into program primary elements not only indicates where problems occurred, but also provides a road map for development of program lessons learned applications.

As illustrated in Figure 1-3, the four program elements related to oversight, management, processes (or systems) and plans extend throughout the program,and corresponding lessons learned end-to-end. The remaining program elements of early plans (including Phase B definition), development, transition and operations are time-phased; their lessons learned primarily apply in the phase indicated in Figure 1-3, however, applications to other phases must be considered.

Subsequent paragraphs of this section are organized by these program elements and the 29 problem/lesson learned areas. Within each area, problems and causes are defined from review of the source documents, corresponding lessons learned are identified and potential applications to Space Station are recommended. The numbering system permits traceability from causes to lessons learned to applications and can be used to create computer files for tracking and statusing during program implementation.

3.2 Program Oversight

1. Safety Emphasis

1.1. Problem

Safety considerations were de-emphasized and resources were reduced unrealistically. Prior to 51-L the NASA SR&QA organizations, both at Headquarters and at the field centers, had atrophied to a level which seriously limited their capability to perform effectively.

1.2. Causes

1.2.1. Vacillating emphasis on safety. NASA has a history of vacillating emphasis on safety. Generally the emphasis wanes during periods of mission success and peaks just after a serious accident. Prior to 51-L there were a series of successes (24 STS missions).

1.2.2. SR&QA functions were reduced to an ineffectual level. The SR&QA work force at some field centers was decreased as the flight rate increased, further degrading the ability to perform the already unsatisfactory assurance function. The results of insufficient resources were evidenced in the following four critical SR&QA functions:

1.2.2.A. Problem reporting was inadequate. Safety problem reporting was not concise in forwarding critical risk factors to the proper levels of management. (Ref. 4.2.1.C.)

1.2.2.B. Trend analysis was inadequate. Very few trend analyses were being performed to identify, validate and categorize safety risks.

1.2.2.C. Safety risk assessments were diminished. The original Mission Safety Assessment Report (MSAR) listed and provided a measure of risk assessment of identified hazards based on safety related critical item list

(CIL) factors and non-CIL causes with some traceability to the CIL factors. After the STS-4 flight, the resources to maintain the MSAR were diminished. To compensate, the ensuing MSARs had the CIL factors and their traceability removed, considered only the differences between the last flight and the next scheduled flight, and provided neither continuity between change publications nor to the original MSAR. Thus, the MSAR was reduced to a minimal, profunctory publication with little substance or value, providing managemnt with no reason to heed it in decision making processes.

1.2.2.D. Audits were curtailed. SR&QA audits of support and element contractors were curtailed after the declaration of operational status for the NSTS.

1.2.3. Cost and schedule performance was the primary measure of management effectiveness. In one NASA handbook for project managers, it was stated that their effectiveness would be judged on cost, schedules and some reliability factors. No mention was made of safety.

1.3. Lessons Learned

1.3.1. Commitment needed for safety emphasis. A firm commitment must be maintained to emphasize the need for safety during periods of success as well as adversity. The resources to maintain this commitment must not be diminished without justification to assure that safety risks will not be unknowingly increased. The commitment also needs certain tangible evidence of the commitment. The following are essential to prevent commitment deficiencies of the pre-Challenger accident environment: (Ref. 4.)

1.3.1.A. Safety requires a vital concern at all levels. A policy must be maintained to assure there is a vital concern for safety at all levels from top management to the workers at the processing level.

1.3.1.B. Career development programs should be maintained. Career development programs should be provided to assure safety competency in the SRM&QA and in program/project engineering and operations. Specific guidelines and criteria should be maintained to assure that safety is given proper emphasis along with cost, performance, schedule and mission success in the hazardous operations decision process.

1.3.1.C. Excellence required for safety. The importance of following procedures and the need for technical excellence and its relationship to safety must be emphasized by all levels of management.

1.3.1.D. Safety motivation programs needed. Vigorous programs should be instituted to improve individual and organizational safety motivation. These motivation programs must emphasize the importance and relationship of self-discipline, following procedures and the need for technical excellence to the safe achievement of program objectives.

1.3.2. SRM&QA capabilities must be acquired and maintained. Programs must acquire the capability to perform the functions early in the program, develop it with the program and adjust it as the program matures. While the SRM&QA functions need infusions of new personnel from other disciplines to assure it technical competence is maintained, they also must maintain a minimum core of skilled professionals to guide the management of the functions. Adequate personnel and other resources are required to perform both the program in-line and the assurance functions. Although not all inclusive for an SRM&QA program, the following four areas need special attention: (Ref. 4.3.1.A.)

1.3.2.A. Comprehensive safety problem resolution needed. Effective problem reporting systems must be maintained that identify all safety problems emanating from design deficiencies, ground and flight anomalies and adverse trends. These reporting systems must be capable of tracking categorization of problems, assignments of responsibilities and recommended remedial actions including verification and validation necessary to clear the problems.

1.3.2.B. Adequate trend analyses needed. Adequate trend analyses must be provided in support of problem reporting systems.

1.3.2.C. Expanded Mission Safety Assessment Report needed. An expanded MSAR for NSTS should be maintained to reflect aggregate risks including special emphasis on safety effects of modifications, trends, mission anomalies and failures and critical margins. Where necessary, mission pertinent operations and maintenance analyses should be included to substantiate risk assessments. After a baseline document is published, it is acceptable to publish mission unique supplements and change pages providing full

traceability is maintained. A similar reporting system should be developed for Expendable Launch Vehicles (ELV) and other high resource/risk programs throughout NASA.

1.3.2.D. SRM&QA periodic audits must be maintained. Audits should be made periodically throughout the life of a program to verify safety management proficiency and compliance with policies and requirements in both NASA internal and contractor organizations. Special audits should be made to follow up on corrective actions taken to resolve safety deficiencies, problems and adverse trends. Special attention should be focused on critical components and mission critical safety problem areas. In addition, frequent walk-throughs in the processing and operations areas should be made to assess compliance with safety requirements.

1.3.3. Safety performance should be linked with job effectiveness. Management instructions and program manager handbooks should reflect that safety performance will be a prime consideration of job effectiveness.

1.3.3.A. Safety performance evaluations needed. Safety performance should be made a part of performance evaluations and promotion criteria for managers and supervisors.

1.4. Space Station Applications

1.4.1. Commitment needed for safety emphasis. A firm commitment must be maintained to emphasize the need for safety during periods of SSP success as well as adversity. Resources (skills, staffing, systems) to maintain this commitment must not be diminished without justification to assure that safety risks will not be unknowingly increased. The commitment also needs certain tangible evidence of the commitment. The following are essential to prevent commitment deficiencies of the pre-Challenger accident environment: (Ref. 4.)

1.4.1.A. Safety requires a vital concern at all levels. An SSP policy must be maintained to assure there is a vital concern for safety at all levels and throughout all phases of the program, from top management to the workers at the processing level and the crew on-orbit.

1.4.1.B. Career development plans should be maintained. Career development plans should be maintained to assure safety competency in program/project engineering and operations. Specific guidelines and criteria should be maintained to assure that safety is given proper emphasis along with cost, performance, schedule and mission success in the hazardous operations decision process.

1.4.1.C. Excellence required for safety. The importance of following procedures and the need for technical excellence and its relationship to safety must be emphasized by all levels of management throughout SSP, both on the ground and on orbit.

1.4.1.D. Safety motivation programs needed. Vigorous programs should be maintained to improve individual and organizational safety motivation throughout the SSP. These motivation programs must emphasize the importance and relationship of self-discipline, following procedures and the need for technical excellence to the safe achievement of program objectives.

1.4.2. SRM&QA capabilities must be acquired and maintained. SSP programs must acquire the capability to perform the functions early in the program, develop it with the program and adjust it as the program matures. While the SRM&QA functions need infusions of new personnel from other disciplines to assure it technical competence is maintained, they also must maintain a minimum core of skilled professionals to guide the management of the functions. Adequate personnel and other resources are required to perform both the program in-line and the assurance functions. Although not all inclusive for an SRM&QA program, the following four areas need special attention: (Ref. 4.3.1.A.)

1.4.2.A. Comprehensive safety problem resolution needed. The established SSP problem reporting system must be effectively maintained to assure that it identifies all safety problems emanating from design deficiencies, ground and flight anomalies and adverse trends. Problem reporting must include tracking categorization of problems, assignments of responsibilities and recommended remedial actions including verification and validation necessary to clear the problems.

1.4.2.B. Adequate trend analyses needed. Adequate trend analyses must be provided in support of established problem reporting systems.

1.4.2.C. An aggregate safety risk assessment report should be maintained. Safety risk assessment reports should be developed and maintained to document safety analyses and aggregate risk assessments associated with major mission and hazardous operations events (e.g. block and mission set changes, Orbital Maneuvering Vehicle (OMV) activities, etc.). Each reissue should provide special emphasis on safety effects of modifications, ongoing trends, mission anomalies and failures and critical margins. After a baseline document is published, it is acceptable to publish mission unique supplements and change pages providing full traceability is maintained. The reports should be formally dispositioned through each level of management in both SSP in-line and independent assurance management systems.

1.4.2.D. SRM&QA periodic audits must be maintained. Audits should be made periodically throughout the life of the SSP to verify safety management proficiency and compliance with policy and requirements in both NASA internal and contractor organizations. Special audits should be made to follow up on corrective actions taken to resolve safety deficiencies, problems and adverse trends. Special attention should be focused on critical components and mission critical safety problem areas. In addition, frequent walk-throughs in the ground processing and operations areas should be made to assess compliance with safety requirements. Since this will be more difficult on orbit and since there will be limited crew, there should be some structured SRM&QA training for each crew member to enhance recognition of the assurance disciplines and awareness of unsafe actions and procedures.

1.4.3. Safety performance should be linked with job effectiveness. SSP management should ensure that safety performance is a prime consideration of job effectiveness at all levels and throughout the life of the program, in accordance with established requirements.

1.4.3.A. Safety performance evaluations needed. SSP management should ensure that safety performance is a part of line-managers and supervisors performance evaluations and promotion criteria.

2. Assurance Reviews

2.1. Problem

There was a lack of independence in assurance reviews. The SRM joint-seal problem was not reviewed independently by NASA SR&QA organizations and no action was taken to identify the safety risks inherent with the STS-program-identified solutions to the problem.

2.2. Causes

2.2.1. Lack of independence of SR&QA organizations. The MSFC SR&QA organization was closer to the joint-seal problem than any of the other NASA organizations. They reported to the MSFC Director of Science and Engineering who had the responsibility for developing Shuttle hardware. While in fact no attempt at independent assessment was made by MSFC SR&QA, their "chain of command" in itself would have made any such attempt suspect.

2.2.2. Deficient safety problem reporting criteria. Criteria prescribed by Level II for reporting flight safety problems from Level III upward was restrictive to the point that it resulted in no identification of open problems from MSFC during 1984 and 1985. As a consequence of this and other pertinent factors (Ref. Problem 1 and 4), NASA assurance organizations outside of MSFC had no reason to undertake independent assessment action even though, in retrospect, trend data on the progressive severity of the problem was available. "Even the most cursory examination of failure rate should have indicated that a serious and potentially disastrous situation was developing on all Solid Rocket Booster joints."

2.3. Lessons Learned

2.3.1. Critical problems must have independent assessment. Safety-critical problems and proposed corrective actions shall be evaluated by the independent safety assessment organizations and recommendations made which are consistent with overall risk criteria. Where necessary, independent reviews will be convened to develop consensus assurance opinions, characterize the safety risks, structure and galvanize assurance

actions and provide progress updates of program corrective actions. Accurate records of proceedings shall be documented and submitted to both program and assurance managements.

2.3.2. Critical problems must be made visible for independent assessment. A comprehensive safety problem reporting system must be maintained. There must be well defined reporting criteria and requirements, timely and accurate record keeping and real-time visibility of problem disposition status for all levels of program and assurance managements. In turn, assurance organizations must analyze flight and ground processing data to identify adverse safety trends, assess the validity of actions proposed to solve safety problems and track the efficacy of safety problem corrective action.

2.4. Space Station Applications

2.4.1. Critical problems must have independent assessment. Safety-critical problems and proposed corrective actions shall be evaluated by the independent safety assessment organizations and recommendations made which are consistent with overall risk criteria. Where necessary, independent reviews will be convened to develop consensus assurance opinions, characterize the safety risks, structure and galvanize assurance actions and provide progress updates of SSP corrective actions. Accurate records of proceedings shall be documented and submitted to both program and assurance managements. SSP Level I/II and Code Q requirements documentation including the Program Requirements Document (PRD) and the Program Definition and Requirements Document (PDRD) should be reviewed and revised where necessary to reflect these concepts.

2.4.2. Critical problems must be made visible for independent assessment. A comprehensive safety problem reporting system must be maintained. There must be well defined reporting criteria and requirements, timely and accurate record keeping and real-time visibility of problem disposition status for all levels of SSP and assurance managements. In turn, assurance organizations must analyze flight and ground processing data to identify adverse safety trends, assess the validity of actions proposed to solve safety problems and track the efficacy of safety problem corrective action. SSP Level I/II and Code Q requirements documentation including the PRD and PDRD should be reviewed and revised where necessary to reflect these concepts.

3.3 Program Management

3. Authority and Responsibility

3.1. Problem

Lines of authority and responsibility and interfaces between SR&QA, programs, center support offices and contractors were poorly and sometimes improperly defined.

3.2. Causes

3.2.1. NASA assurance management deficiencies. Much of the NASA SR&QA requirements documentation, including those defining roles and responsibilities, was inconsistent and out of date; the assurance integration requirements were not clearly defined; and the NASA assurance requirements which were imposed on the contractors were not uniformly applied to the NASA internal organizations.

3.2.1.A. Integration assurance role changed with SPC. The Shuttle Processing Contract (SPC) by intent removed much of the NASA SR&QA integration assurance role from the NSTS program, however, not all of the responsibility reduction was assigned by contract to the SPC. In the handover process, some vital interface requirements were not accurately defined, or were inappropriate, which left voids in the interface functions among NASA, the SPC and the development contractors. (Ref. 2.1.)

3.2.1.B. Risk management inconsistencies. Inconsistencies between NASA center and contractor risk management systems which existed prior to the SPC award were magnified and became serious because now the program risk management system could not be accurately integrated. In addition, there was a serious loss

of "corporate knowledge" when the existing contractor SR&QA personnel departed for other assignments and the NASA SR&QA functions were scaled back. (Ref. 7.1 and 8.1.)

3.2.1.C. Safety panel review system poorly understood. Many of the Level IV contractors did not fully understand the mechanics and function of the safety panel review system resulting in poor communications and inconsistencies in safety risk disposition records.

3.2.1.D. Adverse trend monitoring inadequate. There was no requirement to monitor safety related adverse trends in prelaunch and flight operations.

3.2.2. Inconsistencies in SR&QA roles and responsibilities. There was a lack of consistency in the SR&QA roles and responsibilities between NASA Headquarters and field centers which contributed to confusion in resolving safety issues.

3.2.2.A. No Headquarters SR&QA commitment. There was no commitment for the Headquarters SR&QA organizations to be involved in the resolution of safety problems or in an independent assurance assessment during launch.

3.2.2.B. Independent assessment role inadequate. Several of the field center assurance offices reported to program offices which negated any independent assessment role. (Ref. 4.2.1.D)

3.2.2.C. Assurance function inadequate. There were many positions in SR&QA that required individuals to perform an assurance function and then make a judgement on how well their own function had been done.

3.2.2.D. Avenues of appeal not clearly defined. Avenues of appeal to contest changes and to voice independent safety concerns in risk assessments were not clearly defined.

3.3. Lessons Learned

3.3.1. Program and agency SRM&QA relationships must be defined. Program and agency SRM&QA organizational and functional relationships must be accurately defined and periodically reviewed to provide the most efficient methods of operating within the context of identifying safety risks, making balanced schedule, performance and risk decisions and providing assurance oversight. Roles, responsibilities, authorities and interfaces between NASA organizations and their contractors must be clearly defined in the areas of hazard identification and controls; risk assessment processes; audit policy and requirements; appeal for reversals of risk assessment judgements in the program review process and in the deviation and waiver and launch decision processes.

3.3.2. Organization must accommodate any revised roles and responsibilities. The management of SRM&QA, program offices and field centers should be reorganized as necessary to efficiently carry out any redefinition of roles, responsibilities and authorities elicited from periodic reviews. Where necessary, organizational responsibilities should be changed; position descriptions should be revised; the safety risk review process redefined including the charters and ground rules for operating safety review panels; basic requirements for risk assessment and criteria for acceptance or rejection or risks should be changed to provide consistency in review and record keeping.

3.3.2.A. Assurance decision flow process needs identification. A decision flow diagram and a matrix of responsibilities for assurance functions should be maintained to assure that the proper responsibility assignments are made and that each organization involved understands its specific role in both the primary and independent risk assessment processes.

3.3.2.B. Independent safety assessment plan needed. An implementation plan should be maintained for the independent safety assessment management system defining the activities, products, information requirements and criteria for assessments at each level of review (Level I through IV). All events to be supported (such as operations or flight readiness reviews) that require independent assessment must be identified, evaluation criteria defined and protocols established to resolve conflicting judgements. Schedule milestones for implementation should be included to assure that the management system is in place when needed.

3.3.2.C. Dual assurance responsibilities must be defined. Memoranda of understanding should be maintained for organizations involved in furnishing matrixed support and for each individual involved in a matrixed function to assure that dual responsibilities are understood and the concept of independent safety assessment is preserved.

3.3.2.D. Avenues of appeal must be defined. Clear avenues of appeal to contest changes and voice independent safety concerns in risk assessments must be defined including specific and unambiguous statements of roles and responsibilities for in-line assurance and matrixed personnel.

3.4. Space Station Applications

3.4.1. SSP and agency SRM&QA relationships must be defined. SSP and agency SRM&QA organizational and functional relationships must be accurately defined and periodically reviewed to provide the most efficient methods of operating within the context of identifying safety risks, making balanced schedule, performance and risk decisions and providing assurance oversight. Roles, responsibilities, authorities and interfaces between SSP organizations and their contractors must be clearly defined in the areas of hazard identification and controls; risk assessment processes; audit policy and requirements; appeal for reversals of risk assessment judgements in the program review process and in the deviation and waiver and on-orbit hazardous operations decision processes. The on-board assurance relationships between crew members, flight operations and ground management should be defined also. Special attention should be given to oversight roles and responsibilities.

3.4.2. Organizations must accommodate any revised roles and responsibilities. The management of SRM&QA, program offices and field centers should be reorganized as necessary to efficiently carry out any redefinition of roles, responsibilities and authorities illicited from periodic reviews. Where necessary, organizational responsibilities should be changed; position descriptions should be revised, the safety risk review process redefined including the charters and ground rules for operating safety review panels, basic requirements for risk assessment and criteria for acceptance or rejection or risks should be changed to provide consistency in review and record keeping.

3.4.2.A. Assurance decision flow process needed. A decision flow diagram and a matrix of responsibilities for the SSP assurance function for both ground and flight should be maintained to assure that the proper responsibility assignments are made and that each organization involved understands its specific role in both the primary and independent risk assessment processes.

3.4.2.B. Independent safety assessment needs. An SSP implementation plan should be maintained for the independent safety assessment management system defining the activities, products, information requirements, and criteria for assessments at each level of review (Level I through IV). All events to be supported (such as ground operations and on-orbit operations readiness reviews) that require independent assessment must be identified, evaluation criteria defined and protocols established to resolve conflicting judgements. Schedule milestones for implementation should be included to assure that the management system is in place when needed.

3.4.2.C. Dual assurance responsibilities must be defined. Memoranda of understanding should be maintained for SSP organizations involved in furnishing matrixed support and for each individual involved in a matrixed function to assure that dual responsibilities are understood and the concept of independent safety assessment is preserved.

3.4.2.D. Avenues of appeal must be defined. Clear avenues of appeal to contest changes and voice independent safety concerns in risk assessments must be defined including specific and unambiguous statements of roles and responsibilities for in-line assurance and matrixed personnel.

4. SRM&QA Resources

4.1. Problem

Neither NASA nor its contractor organizations had sufficient resources to perform their SRM&QA assurance functions properly.

4.2. Causes

4.2.1. Management perception of diminished risk. Management perceived that the safety risks for the STS had diminished after the first four flights. It was perceived also that the SR&QA community was not needed to be actively engaged in safety critical problem resolution or the launch decision waiver process. (E.g., there was no safety representative on the Mission Management Team that made key decisions during 51-L countdown; no SR&QA representative at teleconference between MSFC and Thiokol on January 27, 1986.)

4.2.1.A. Reduced SR&QA participation in the program. The conclusion that the safety risks had diminished was not based on an objective, factual assessment of the true situation (assessment of the aggragate of anomalies, problems, close calls, trends, etc.), but was based on the fact that a catastrophic vehicle failure had not occurred. This resulted in an imprudent decision to reduce SR&QA participation in the program. Such SR&QA tasks as testing, analysis and instrumentation were reduced or reassigned and SR&QA research and technology development was reduced and facilities to accomplish this were shut down.

4.2.1.B. Pressure to reduce costs and turnaround time reduced SR&QA resources. Pressure to reduce costs and turnaround time eliminated mandatory inspection requirements for the SRB and ET and resulted in further reduction of quality control resources. (Ref. 17.2.1.)

4.2.1.C. Safety critical problems not identified. Safety critical problems were not identified as evidenced by the lack of visibility, resolution and tracking. (Ref. 1.2.2.A.)

4.2.2. Lack of confidence in SR&QA functions. Management lacked confidence in the capability of SR&QA functions to provide meaningful inputs in the engineering processes necessary to solve difficult problems and evaluate launch and flight risks. This lack of confidence was due, in part, to a lack of skilled personnel assigned to the assurance functions.

4.2.2.A. Insufficient advice. The STS Program Manager received insufficient advice from the SR&QA functions.

4.2.2.B. Incorrect criticality categories. Critical components were incorrectly categorized and tracked (e.g., the criticality category for the O-ring redundancy).

4.2.3. The "Silent Safety Program." The perceptions in Causes 4.2.1 and 4.2.2 were heightened by and in turn exacerbated the "Silent Safety Program."

4.2.4. Inadequate reliability analysis and record keeping. The SRM aft joint seal assembly was not recognized as a single failure point (criticality category 1) under nominal operating conditions until 1982. While this component was reclassified from category 1R to category 1 at that time, there were some information systems that continued the category 1R classification until five weeks after the 51-L accident.

4.3. Lessons Learned

4.3.1. Safety risk must not be diminished by decree. Decisions relating to SRM&QA resource allocations at any phase of a program (including skills, staffing and systems) must be made based on objective, factual assessments of the degree of safety risk and must not be skewed by schedule or operational expediency. Consideration should be given to the number and severity of safety related problems, the status of adverse trends, the effectiveness of controls of known hazards and the residual and aggregate risk assessments.

4.3.1.A. Baseline sustaining core of skills resources needed. There must be a baseline sustaining core of skilled SRM&QA professionals and resources to manage an active assurance effort throughout all phases of the program and to provide for a "corporate knowledge" base for these functions. Augmentation of this sustaining core should be provided based on a continual calculated assessment of safety risks and management effectiveness. Adequate facilities and resources also must be provided to support SRM&QA testing, analysis, instrumentation and research and development.

4.3.2. The SRM&QA work force must be competent and be involved. To assure the effectiveness of the SRM&QA function there must be an infusion of technically skilled design, systems and operations engineering personnel. The assigned SRM&QA work force must not only be skilled, it also must be directly involved in program processes. Personnel must understand the issues, take well-founded technical and managerial positions on them and participate with program management in their timely and effective

resolution. In addition, there should be a structured career path for each of the assurance disciplines; a rotation of people between the SRM&QA disciplines and other disciplines; and structured professional and technical training programs to improve individual and assurance management performances.

4.3.3. Periodic SRM&QA reviews needed. Periodic reviews of the SRM&QA work effectiveness (including skills, staffing and systems) should be made by the NASA Associate Administrators to assure that resources provided for assurance functions at all levels are appropriate, based on technical levels, complexity and phase of programs, and safety risk factors. The reviews should also determine if the assurance management is adequately performing its in-line and independent functions.

4.3.3.A. Effective safety advisory panel needed. "NASA should establish an STS Safety Advisory Panel reporting to the STS Program Manager. The charter of this panel should include Shuttle operational issues, launch commit criteria, flight rules, flight readiness and risk management. The panel should include representation from the safety organization, mission operations and the astronaut office." (Recommendation from Ref.1 p. 199) Also, the panel should periodically evaluate efficacy of in-place management systems critical to safety; review close-out recommendations and other dispositions of safety problems; and recommend courses of action to decrease safety risks and to rectify any deficiencies noted.

4.3.4 Critical components must be analyzed to assure redundancy. Resources must be provided to assure that all criticality category 1R components are analyzed to determine the failure modes which can result in loss of redundancy due to a single possible event, due to a generic fault, due to off-nominal coupling effects from adjacent systems and due to likely environmental or operating conditions. Specifications for the elimination or control of these failure modes must be stipulated and validated. The results of this process must be accurately and consistently recorded throughout the program and assurance management systems.

4.4. Space Station Applications

4.4.1. Safety risk must not be diminished by decree. Decisions relating to SRM&QA resource allocations at any phase of the SSP (including skills, staffing and systems) must be made based on objective, factual assessments of the degree of safety risk and must not be skewed by schedule or operational expediency. Consideration should be given to the number and severity of safety related problems, the status of adverse trends, the effectiveness of controls of known hazards and the residual and aggregate risk assessments. There should be specific evaluations of these principles during planning of SSP phase transitions and a documented affirmation of any conclusions relating to changes in existing resources. SSP should consider the requirement for separate identification of SRM&QA resources in development of periodic Program Operating Plan (POP) submittals.

4.4.1.A. Baseline sustaining core of skills and resources needed. There must be a baseline sustaining core of skilled SRM&QA professionals and resources to manage an active assurance effort throughout all phases of the SSP and to provide for a "corporate knowledge" base for these functions. Augmentation of this sustaining core should be provided based on a continual calculated assessment of safety risks and management effectiveness. Adequate facilities and resources also must be provided to support SRM&QA testing, analysis, instrumentation and research and development. Code S and Code Q should jointly evaluate the baseline resource needs for each phase of the SSP.

4.4.2. The SRM&QA work force must be competent and be involved. To assure the effectiveness of the SRM&QA function there must be an infusion of technically skilled design, systems and operations engineering personnel. The assigned SRM&QA work force must not only be skilled, it also must be directly involved in program processes. Personnel must understand the issues, take well-founded technical and managerial positions on them and participate with program management in their timely and effective resolution. In addition, there should be a structured career path for each of the assurance disciplines; a rotation of people between the SRM&QA disciplines and other disciplines; and structured professional and technical training programs to improve individual and assurance management performances. SSP and the NASA centers should jointly develop a plan to implement these policies.

4.4.3. Periodic SRM&QA reviews needed. Periodic reviews of the SRM&QA work effectiveness (including skills, staffing and systems) should be made by the NASA Associate Administrators to assure that resources provided for assurance functions at all levels are appropriate, based on technical levels,

complexity and phase of the SSP, and safety risk factors. The review should also determine if the assurance management is adequately performing its in-line and independent functions.

4.4.3.A. Effective safety advisory panel needed. SSP should establish a safety advisory panel reporting to the SSP manager. The charter of this panel should include SSP operational issues, flight and hazardous operations commit criteria, flight rules, flight readiness and risk management. The panel should include representation from the SRM&QA organization, mission operations, design engineering and the Space Station crew. Also, the panel should periodically evaluate efficacy of in-place SSP management systems, both ground and on-board, critical to safety; review close out recommendations and other dispositions of safety problems; and recommend courses of action to decrease safety risks and to rectify any deficiencies noted.

4.4.4. Critical components must be analyzed to assure redundancy. Resources must be provided to assure that all Classification A mission critical assets are analyzed to determine the failure modes which can result in loss of redundancy due to a single possible event, due to a generic fault, due to off-nominal coupling effects from adjacent systems and due to likely environmental or operating conditions. Specifications for the elimination or control of these failure modes should be stipulated and validated. The results of this process should be accurately and consistently recorded throughout the SSP and assurance management systems.

5. Deviation and Waiver Management

5.1. Problem

Deviation and waiver management, including the review and decision process and associated risk assessments at all levels, were inadequate for flight critical components. The SRM joint seal waiver violated existing management requirements and pointed to some serious deficiencies in the deviation and waiver system.

5.2. Causes

5.2.1. Management discipline breakdown. There were numerous violations of existing deviation and waiver requirements resulting from the compelling urge to preserve the launch schedule. This situation led to inadequate consideration of engineering concerns for launch conditions beyond those which were verified by qualification tests and analyses. It also led to inadequate understanding of the measured effects of temperature and case dimension tolerances on the SRM joint assembly.

5.2.1.A. Deviation and waiver management system not effectively defined. The deviation and waiver management system was not effectively defined to allow adequate review by NASA top management.

5.2.1.B. Relaxed management attitude. Management at all levels failed to comprehend the seriousness of the problem, particularly at Level I and Level II. There was a relaxed attitude in repeatedly waiving the joint-seal problem at launch.

5.2.1.C. Ambiguous decision criteria. There were ambiguities in critical launch constraints and the incremental go/no-go decision process, as evidenced by the technically unsupportable safety risk decision on ice conditions.

5.2.1.D. No independent assessment. There was no independent assessment of the safety-related problem analysis conducted by the NSTS program. Adverse trends, as evidenced by case joint "blow-by" in previous STS launches, were ignored. The increased risk imposed by the increased SRM case proof pressure testing was not recognized.

5.2.2. NASA management pressure for a favorable launch decision. Thiokol management was pressured by the SRB Project Manager to reverse their no-go position. The position reversal was not made on a sound technical basis.

5.3. Lessons Learned

5.3.1. Standards for consideration of deviations and waivers must be maintained. Minimum standards and requirements for presentation and consideration for waivers must be maintained, reviewed periodically and

updated, including required information defining deviations from operational constraints; impact on safety and mission performance; status of prior analyses and risk assessments; critical assumptions in modeling or test verifications; effects on stated safety margins; critical history or pedigree of component; and any perceived uncertainties or unknowns in the information presented.

5.3.1.A. Deviation and waiver management system must be effectively defined. The organizational management system involved in the deviation and waiver process must be effectively defined at all levels. The organization should be formally constituted for the specific purpose of dispositioning deviations and waivers and should address all interface requirements between programs, NASA Headquarters, NASA centers, element contractors and support contractors. Criteria, ground rules and information necessary for critical decisions, including guidelines for resolution of issues and avenues of appeal for higher management decision, should be defined, periodically reviewed and updated. Key roles and responsibilities of organizations and people involved in the deviation and waiver process must be clearly defined. Principals should be identified by name.

5.3.1.B. Deviation and waiver process must be reviewed. The deviation and waiver process must be periodically reviewed to identify and correct deficiencies in requirements and procedures from Level I through Level IV. All previous lessons learned relating to these deficiencies must be addressed and used as a check list to validate the revised system. Similarly, the SRM&QA management systems, requirements and documentation must be reviewed periodically to assure that the independent safety assessment function is adequate.

5.3.1.C. Safety critical information must be accessible at decision points. Information relating to factors of safety, performance margins, safety problem status and resolutions, critical item status, residual risk dispositions, launch and operational constraints including environmental limits and operational red-lines, safety critical trends and hazard controls, must be readily accessible to both program and independent assessment organizations at decision points in the deviation and waiver process.

5.3.1.D. Deviations and waivers must be independently evaluated. All deviations and waivers for launch or hazardous operations decisions must be independently evaluated by SRM&QA. Evaluations must be recorded and must be available for review in the decision process throughout all levels of management.

5.3.2. Violations of deviation and waiver requirements must be prevented. SRM&QA independent assessment must ensure that violations do not occur. NASA must provide continual policy enforcement stating that "schedules" shall never drive operational decisions where critical safety issues are involved.

5.3.2.A. Technical decision criteria must be maintained. NASA must provide continual policy enforcement stating that no actions shall be taken by management which could be perceived as forcing a contractor into a position which appears to have an unsound technical basis. Technical decision criteria, including those relating to justification for risk acceptance, must be maintained, reviewed periodically and updated. For the waiver decision process such criteria should be stated in terms of why the waiver should be accepted rather than why the waiver should not be accepted.

5.4 Space Station Applications

5.4.1. Standards for consideration of deviations and waivers must be maintained. Minimum SSP standards and requirements for presentation and consideration for waivers must be maintained, reviewed periodically and updated, including required information defining deviations from operational constraints; impact on safety and mission performance; status of prior analyses and risk assessments; critical assumptions in modeling or test verifications; effects on stated safety margins; critical history or pedigree of component; and any perceived uncertainties or unknowns in the information presented.

5.4.1.A. Deviation and waiver management system must be effectively defined. The organizational management system involved in the deviation and waiver process must be effectively defined at all levels. The organization should be formally constituted for the specific purpose of dispositioning deviations and waivers and should address all interface requirements between SSP, NASA Headquarters, NASA centers, SSP element contractors and SSP support contractors. Criteria, ground rules and information necessary for critical decisions, including guidelines for resolution of issues and avenues of appeal for higher

management decision, should be defined, periodically reviewed and updated. Key roles and responsibilities of organizations and people involved in the deviation and waiver process must be clearly defined. Principals should be identified by name.

5.4.1.B. Deviation and waiver process must be reviewed. The SSP deviation and waiver process must be periodically reviewed to identify and correct deficiencies in requirements from Level I through Level IV. All previous lessons learned relating to these deficiencies must be addressed and used as a check list to validate the revised system. Similarly, the SSP SRM&QA management systems, requirements and documentation must be reviewed periodically to assure that the independent safety assessment function is adequate.

5.4.1.C. Safety critical information must be accessible at decision points. SSP information relating to factors of safety, performance margins, safety problem status and resolutions, critical item status, residual risk dispositions, launch and operational constraints including environmental limits and operational red-lines, safety critical trends and hazard controls, must be readily accessible to both program and independent assessment organizations at decision points in the deviation and waiver process.

5.4.1.D. Deviations and waivers must be independently evaluated. All deviations and waivers for launch or hazardous operations decisions must be independently evaluated by SSP SRM&QA. Evaluations must be recorded and must be available for review in the decision process throughout all levels of management including agency SRM&QA.

5.4.2. Violations of deviation and waiver requirements must be prevented. Agency and SSP SRM&QA independent assessment must ensure that violations do not occur. NASA must provide continual policy enforcement stating that "schedules" shall never drive operational decisions where critical safety issues are involved.

5.4.2.A. Technical decision criteria must be maintained. SSP must provide continual policy enforcement stating that no actions shall be taken by management which could be perceived as forcing a contractor into a position which appears to have an unsound technical basis. Technical decision criteria, including those relating to justification for risk acceptance, must be maintained, reviewed periodically and updated. For the waiver decision process such criteria should be stated in terms of why the waiver should be accepted rather than why the waiver should not be accepted.

6. Management Performance

6.1. Problem

Some NASA and contractor management lack motivation, experience and/or skills to manage the program effectively.

6.2. Causes

6.2.1. Deterioration of the pursuit of excellence. There was a lack of personal commitment to and identification with the NSTS program by some assigned personnel. Some individuals working on the NSTS program lost their motivation for excellence.

6.2.2. Premature phase transition. The management decision to transition the Space Shuttle from the development phase to the operational phase was premature. (Ref. 26.1.)

6.2.3. Flawed decisions in developing Shuttle Processing Contract. Problems associated with consolidating fifteen development contractors into one Shuttle Processing Contract and the method in which it was accomplished involved flawed management decisions. (Ref. 3.1 and 26.1.)

6.2.4. Lack of excessive overtime policy. Field centers lacked enforceable policies relating to the amount of overtime allowed. The application of excessive overtime leading to personnel fatigue increased accident risk. (Ref. 29.1.)

6.2.5. Questionable work error forgiveness policy. NASA has no work error forgiveness policy, and policies of the contractors vary. Therefore, the forgiveness policy is questionable as perceived by some technicians who were hesitant to report problems. (Ref. Problem 29.1.)

6.2.6. Failure to benefit from astronaut experience in management. NASA departed from the use of astronauts in management positions to the extent they previously had in the 1960's and 1970's. As a result, management failed to benefit from the participation of responsible individuals having considerable flight experience and a greater appreciation of operation problems and flight safety.

6.2.7. Confusion over safety management. Some NSTS managers are unversed in the mechanics or the principal instruments of risk assessment used in safety management. Roles and responsibilities of each organizational element regarding accomplishment of the total safety assurance effort is generally unclear to NSTS management.

6.2.7.A. Insignificant safety input. There was a feeling among some managers that safety input to the program in the past had been insignificant so there was no need to understand the function or the process.

6.2.7.B. Little incentive to understand safety. Center project managers have little incentive to understand the safety function or its principals. One Project Manager Handbook states that project managers will be judged for effectiveness on many factors, none of which indicate the need for safety awareness or understanding of safety principals.

6.3. Lessons Learned

6.3.1. Management dedication is required. Agency and program management must ensure that only highly motivated personnel who demonstrate a personal commitment are brought into key positions. Periodic evaluations must be made and when personnel are found who lack dedication, they should be re-dedicated or moved to other positions. Management must also ensure that continuing and innovative motivation programs are in place for all program phases and disciplines.

6.3.2. Effective transition planning is required. The operational status of a very complex, high-technology, high-risk system that is basically developmental in nature and objective, must be carefully defined and transition carefully planned to preclude operational complacency. Unique requirements, such as technology transparency, long-duration operation and follow-on development, should be emphasized. (Ref. 26.3.)

6.3.3. Effective contractor transition is required. When transitioning work between contractors, the transition must be accomplished in an orderly and well planned manner with close program supervision to ensure that expertise, experience and technology are not lost in the process. (Ref. 7.3 and 26.3.)

6.3.4. Effective overtime policies must be maintained. Program management must maintain established policies relating to the amount of overtime allowed where personnel fatigue decreases performance or increases safety risk. Program SRM&QA musts assure compliance with these policies.

6.3.5. Work error forgiveness policies must be maintained. Agency and program management must encourage/require contractors to devise policies for forgiving or mitigating truly accidental damage. Program SRM&QA must assure that effective policies are developed and maintained.

6.3.6. Management flight experience is encouraged. Experienced astronauts who have demonstrated good management capability and have an in-depth appreciation of the technical side of a program should be encouraged by policy to move into agency and program management positions at some time during their career.

6.3.7. Management safety commitment is mandatory. The commitment to safety must be made a stated and integral part of each supervisor's and manager's career development plan and the safety performance of each supervisor and manager must be evaluated as part of the annual appraisal process. Safety commitments must be incorporated in all contract procurements in a similar manner.

6.4. Space Station Applications

6.4.1. Management dedication is required. Agency and SSP management must ensure that only highly motivated personnel who demonstrate a personal commitment are brought into key positions. Periodic evaluations

must be made and when personnel are found who lack dedication, they should be re-dedicated or moved to other positions. Periodic audits of program and contractor activities should include specific examination of how the Space Station requirement for product-oriented motivation (awareness) activity is being implemented as an integral part of existing motivational activities. Management must also ensure that continuing and innovative motivation programs are in place for all program phases and disciplines.

6.4.2. Effective transition planning is required. The operational status of Space Station must be carefully defined and transition carefully planned to preclude operational complacency. Unique requirements, such as technology transparency, long-duration operation and follow-on development, should be emphasized. (Ref. 26.4.)

6.4.3. Effective contractor transition is required. When transitioning work between contractors, the transition must be accomplished in an orderly and well planned manner with close program supervision to ensure that expertise, experience and technology are not lost in the process. (Ref. 7.4 and 26.4.)

6.4.4. Effective overtime policies must be maintained. SSP management must maintain established policies relating to the amount of overtime allowed where personnel fatigue decreases performance or increases safety risk. SSP needs to be particularly sensitive to excessive individual and crew overtime in the on-orbit construction, activation and operation of the Space Station. Planning must allow time for contingency responses. SSP SRM&QA must assure compliance with these policies.

6.4.5. Work error forgiveness policies must be maintained. SSP management must encourage/require contractors to devise policies for forgiving or mitigating truly accidental damage. SSP SRM&QA must assure that effective policies are developed and maintained.

6.4.6. Management flight experience is encouraged. Experienced astronauts who have demonstrated good management capability and have an in-depth appreciation of the technical side of a program should be encouraged to move into SSP management positions.

6.4.7. Management safety commitment is mandatory. The commitment to safety must be made a stated and integral part of each SSP supervisor's and manager's career development plan and the safety performance of each supervisor and manager must be evaluated as part of the annual appraisal process. Safety commitments must be incorporated in all contract procurements in a similar manner.

7. Program Critical Knowledge

7.1. Problem

Focus and management of critical knowledge including previous lessons learned were inadequate.

7.2. Causes

7.2.1. Failure to understand or fully accept seriousness of safety critical problem. Despite the presence of significant amounts of information and the occurrence of at least one detailed briefing at Headquarters on the difficulties with the O-rings, the NASA and Thiokol technical managers failed to understand or fully accept the seriousness of the problem.

7.2.1.A. Poor technical decision-making. There has existed over a period of several years a syndrome of poor technical decision-making by NASA and contractor personnel who failed to act decisively to solve the increasingly serious anomalies in the SRM joints. This situation has been considered the result of poor communication and inadequate procedures.

7.2.2. Previous lessons were forgotten. Although the system of coming to conclusions and recording lessons that can be learned appears to be adequate, there is no effective system in place to ensure that lessons learned are not forgotten.

7.3. Lessons Learned

7.3.1. Program critical knowledge must be retained. NASA and contractor management must recognize that a key to avoiding future mishaps is the solution to the problem of communicating critical knowledge effectively. Inherent in the solution are complete and periodic reviews of decision-making processes. A

comprehensive initial review should be accomplished before processes are established for the development phase of a program.

7.3.2. Lessons learned assurance is required. The system for lessons learned development, retention and dissemination should be periodically reviewed to verify applicability and effectivity. Features should be incorporated to strengthen the system when deficiencies are found. SRM&QA should ensure that lessons are not forgotten through independent oversight.

7.4. Space Station Applications

7.4.1. Program critical knowledge must be retained. Program upper management should make an early and continuing effort to foster, throughout Space Station and contractor management, the absolute necessity to understand, track and retain critical knowledge as it is gained. Every effort must be made to see that critical knowledge is adequately reflected in decision-making processes and that poor communication is recognized and eliminated. SSPO should consider expansion of the "Design Knowledge Capture" requirements documentation and program support task to include lessons learned and other program critical knowledge.

7.4.2. Lessons learned assurance is required. SSP management, in conjunction with SSP SRM&QA, should periodically review the lessons learned system for applicability to requirements and processes. Agency SRM&QA should periodically and independently review effectivity of the operating system including specific lessons applied.

3.4 Program Processes

8. Safety Risk Management

8.1. Problem

Policies, criteria, requirements and management systems were inadequate to assure complete review and assessment of safety risks. There were inconsistencies in all of these areas between NASA Headquarters, field centers, prime contractors and support contractors.

8.2. Causes

8.2.1. Safety risk management policies, criteria and requirements changed. Changes in policies, criteria and requirements were dictated by the various parent organizations to which Safety was assigned. This deprived Safety of its independence, removed it from the program review process and limited participation in audit and review.

8.2.1.A. Headquarters safety management structure changed. During Shuttle development and operations phases, there were numerous changes in the NASA Headquarters safety management structure.

8.2.1.B. Changes confused field centers and contractors. The changes in safety management at Headquarters led to confusion in the NASA centers and contractors. Their efforts to follow and duplicate the perceived changes in basic safety policy were not possible, or in many cases, undesirable due to contractual commitments and unacceptable perturbations to their management systems.

8.2.2. System safety procurement directives fluctuated. One of the more significant changes in NASA Headquarters direction is illustrated by the several iterations in the procurement directives which alternately required system safety efforts in NASA contracts and then deleted them. These fluctuations occurred several times in the 15 years prior to 51-L and contributed to the de-emphasis of safety. The effort to keep up with the fluctuating policies was ineffective and resulted in a backlog of documentation changes and significant conflicts in definitions of risk categories, hazard closures and waiver/deviation processes. (Ref. 15.2.1.B and 16.2.1.)

8.2.3. Safety risk assessment process was confused. Changes to organizational, safety management and procurement directives added significant confusion to the safety risk assessment process.

8.2.3.A. Headquarters safety role diminished. There was a diminished assertion of the Headquarters safety assessment role in all programs.

8.2.3.B. Requirements documented inconsistently. There was a ripple of inconsistencies throughout the requirements documentation which could not be dealt with adequately due to the atrophy of safety resources throughout NASA and its contractors. (Ref. 1.1 and 4.1.)

8.2.3.C. SR&QA failed to assess seal problem. The resulting confusion contributed to, but cannot fully explain, the failure of safety management along with reliability and quality control management to critique "the engineering analysis advanced as an explanation of the SRM seal problem."

8.2.4. Tracking and verification of hazard controls were inadequate. There was no system to track and verify that hazard controls were being maintained.

8.3. Lessons Learned

8.3.1. Safety risk management policies, criteria requirements, and structure must be maintained. Policies, criteria and requirements for safety risk management in both program organizations and SRM&QA organizations must be periodically reviewed for inconsistencies in definition, purpose and effectiveness and weaknesses in supporting the aggregate safety risk assessments; priority must be given to correcting deficiencies and monitoring the corrected system to assure that inconsistencies are caught before they cascade into the various tiers of requirements documentation. A periodic review and update of the entire safety risk assessment capability must be performed (including skills, staffing and systems). Structured and well defined roles, authorities and responsibilities between the safety and program management organizations must be maintained (Ref. 3.3). Resources must be provided to assure an adequate baseline capability throughout NASA to support the safety risk management function for all programs (Ref. 4.3).

8.3.2. System safety procurement emphasis must be maintained. The Safety Division, NASA Headquarters, must periodically review procurement directives and delineate changes required to assure that the proper system safety efforts and sufficient resources are provided in contract to support independents safety risk assessment in accordance with current policy. (Ref. 15.3.)

8.3.3. Effective safety risk assessment process must be maintained. The safety risk assessment process must consider the impact of: safety related problems (both identified by the program and conceived by independent assessment); status and quality of hazard identification and controls; and safety related trends in workmanship, schedule pressures, procedures integrity and the status of the disposition of identified safety risks. A discrete safety risk assessment must be provided for each operations event in which an overall aggregate risk assessment is required or a mission constraint is considered for waiver. Each such assessment, along with any meetings where key decisions are made leading to these risk assessments, must be properly recorded. Any conflict in fact or judgement between program and safety inputs should be resolved through an independent risk assessment management system with meticulously documented approval/disapproval decision procedures.

8.3.3.A. Headquarters risk management lead role is mandatory. NASA Headquarters must maintain policies and requirements for safety risk management and take the lead role in its implementation.

8.3.3.B. SRM&QA requirement documents must be maintained. SRM&QA requirements documentation must be reviewed periodically and changed as necessary to provide consistent risk assessment criteria, risk category definitions, hazard closure criteria and deviation/waiver criteria.

8.3.3.C. Safety risk assessment function must be objective and in-depth. There should be at least one safety professional working directly for each program manager at each major review level and one for the assurance manager tasked to provide independent safety assessment. (i.e., whenever possible, the conflict of interest combination of "doing" and "oversight" safety functions should be avoided by not assigning both functions to one person.) Where this approach is not possible due to matrixed responsibilities or shortage

of qualified people there must be a clear definition of the function so that the "dual-role" person and both managers involved understand their individual and collective roles and each can maintain objectivity.

8.3.4. Tracking and verification of hazard controls must be maintained. The risk management process must be maintained to include tracking and periodic reverification of hazard controls for safety critical systems, components and operations. Processing of changes to these critical items must include a review and revalidation of the original hazard controls and a reverification that the stipulated controls are being maintained.

8.4. Space Station Applications

8.4.1. Safety risk management policies, criteria requirements, and structure must be maintained. Policies, criteria and requirements for safety risk management in all SSP organizations must be periodically reviewed for inconsistencies in definition, purpose and effectiveness and weaknesses in supporting the aggregate safety risk assessments; priority must be given to correcting deficiencies and monitoring the corrected system to assure that inconsistencies are caught before they cascade into the various tiers of requirements documentation. A periodic review and update of the entire SSP safety risk assessment capability must be performed (including skills, staffing and systems). Structured and well defined roles, authorities and responsibilities between the safety and program management organizations must be maintained. (Ref. 8.4.) Resources must be provided to assure an adequate baseline capability throughout the SSP to support the safety risk management function (Ref. 4.4). Reviews should be provided for all documentation levels (I through IV) including the PRD and PDRD. NHB 1700 and 5300 series documentation should be reviewed for inconsistencies.

8.4.2. System safety procurement emphasis must be maintained. SSP procurement emphasis must be reviewed periodically and changed as necessary to assure that the proper system safety efforts and sufficient resources are provided in contracts to support independent safety risk assessment. (Ref. 15.4.)

8.4.3. Effective safety risk assessment process must be maintained. An effective SSP safety risk assessment process must be maintained and must consider the impact of: safety related problems (both identified by the program and conceived by independent assessment); status and quality of hazard identification and controls; and safety related trends in workmanship, schedule pressures, procedures integrity and the status of the disposition of identified safety risks. A discrete safety risk assessment must be provided for each operations event in which an overall aggregate risk assessment is required or a mission constraint is considered for waiver. Each such assessment, along with any meetings where key decisions are made leading to these risk assessments, must be properly recorded. Any conflict in fact or judgement between program and safety inputs should be resolved through an independent risk assessment management system with meticulously documented approval/disapproval decision procedures.

8.4.3.A. Headquarters risk management lead role is mandatory. NASA Headquarters (Code Q and SSP Level I/II) must maintain effective and comprehensive policies and requirements for safety risk management and take the lead role in its implementation.

8.4.3.B. Effective SRM&QA requirements documentation must be maintained. SSP SRM&QA requirements documentation including applicable sections/paragraphs of the PDRD, must be reviewed periodically and changed as necessary to assure consistent risk assessment criteria, risk category definitions, hazard closure criteria and deviation/waiver criteria.

8.4.3.C. Safety risk assessment function must be objective and in-depth. There should be at least one safety professional working directly for each SSP manager at each major review level and one for the SSP assurance manager tasked to provide independent safety assessment. (i.e., whenever possible, the conflict of interest combination of "doing" and "oversight" safety functions should be avoided by not assigning both functions to one person.) Where this approach is not possible due to matrixed responsibilities or shortage of qualified people, there must be a clear definition of the function so that the "dual-role" person and both managers involved understand their individual and collective roles and each can maintain objectivity. This policy should be included in appropriate SSP Safety documentation.

8.4.4. Tracking and verification of hazard controls must be maintained. The risk management process must be maintained to include tracking and periodic reverification of hazard controls for safety critical systems, components and operations. Processing of changes to these critical items must include a review and revalidation of the original hazard controls and a reverification that the stipulated controls are being maintained.

9. Problem Resolution

9.1. Problem

The problem resolution process including definition and tracking, corrective action, risk assessment and assurance management were inadequate for some flight critical components.

9.2. Causes

9.2.1. Erroneous criticality assessments. O-rings were first assessed as criticality category 1R and reclassified to category 1 in 1982. The problem assessment system failed to change from 1R, possibly resulting in confusion and the erroneous closing of the erosion problem.

9.2.2. Lack of independent problem assessment. Potential "show stopper" problems (major impacts to budget/schedule) were assessed only by in-line personnel dependent on the program for their immediate future career.

9.2.3. Inadequate trend analyses. Trend analyses were not extensive enough to project adverse trends that in hind sight appear obvious. (Ref. 10)

9.2.4. Deliberately ignoring the problem. Flight Readiness Reviews discouraged flagging repetitive problems including criticality category 1 problems.

9.2.5. Inconsistent handling of critical problems. The SSMEs had many critical problems resolved and planned the resolution of many more while others remained unresolved.

9.2.6. Lack of critical component qualification data. Qualification data deficiencies such as safety margins, failure rate and predicted life may have prevented engineers from reaching the best, most cost/safety/reliability effective solution for the expended resources.

9.3. Lessons Learned

9.3.1. Standard program-wide requirements, definitions and procedures needed. Program-wide procedures for both hardware and software must define minimal approval authority and required concurrences for risk and criticality identification, change, acceptance, elimination and closure (temporary and permanent). There should be program wide definitions and preparation and use instructions for all Failure Modes and Effects Analyses (FMEAs), hazard analyses, critical items list, criticality determinations and problem reporting and closure. Tracking and assuring compliance are necessary. The NASA Headquarters safety policy and requirements documents including NHB 1700 and 5300 series, must be standardized in content including definitions.

9.3.2. Complete and independent critical problem assessment needed. Disposition of critical problems (hardware and software) must not be made until an independent assessment is conducted. Safety risk issues must be clearly stated, impediments to problem resolution highlighted, realistic schedules defined for disposition of problems, risks for meeting launch commitments stated and progress towards resolution monitored by both program and assurance management.

9.3.3. Complete and accurate trend data needed for problem resolution. A structured, disciplined system for the collection, storage and use of data in trend analyses in the identification of problems and in their resolution should be required for each program. Care must be exercised to prevent the use of erroneous or out-of-date data in the formulation of solutions. (Ref. 10.)

9.3.4. Priority consideration for critical problem resolution required. Criticality category 1 and 1R problems must have priority consideration for resolution and implementation of remedial actions. They should be highlighted in Flight Readiness Reviews (FRRs) and program reviews at all levels of management.

Criticality ground rules, management requirements and criteria for analysis must be adhered to rigidly. Status and problem resolution records in all program and assurance management systems must be consistent. Acceptance of criticality category 1 and 1R risks temporarily and permanently must be reviewed by senior safety personnel who are not responsible for/to the program.

9.3.5. Tightly controlled critical problem resolution procedures required. All critical problems (hardware and software) must be resolved consistently using tightly controlled procedures systematically prioritizing problems for resolution based on risk, benefit to the program, and other factors will help assure the most critical problems are worked first. If there is a deviation, a risk assessment with justification must be included in the documentation of the problem.

9.3.6. Complete and accurate qualification data needed. Complete qualification data including performance and environmental envelopes and safety margins must be provided for critical problem resolution.

9.4. Space Station Applications

9.4.1. Requirements should be reviewed for uniformity. Program wide definitions and assignments of authority, definitions of terms, preparation and use instructions, reporting, tracking and closure (including acceptance of risk) requirements, and the system for assuring compliance with instructions pertaining to safety problems and SRM&QA activities should be continually reviewed to ensure they are clearly delineated (hardware and software).

9.4.2. Independent problem assessment needed. Disposition of critical problems (hardware and software) must not be made until an independent assessment is conducted. Safety risk issues must be clearly stated, impediments to problem resolution highlighted, realistic schedules defined for disposition of problems, risks for meeting launch commitments stated and progress towards resolution monitored by both program and assurance management.

9.4.3. Complete and accurate trend data needed for problem resolution. A structured, disciplined system for the collection, storage and use of data in trend analyses in the identification of problems and in their resolution should be required for each program. Care must be exercised to prevent the use of erroneous or out-of-date in the formulation of solutions. The program support task to identify and analyze safety critical trends should be closely monitored to ensure management awareness of adverse trends so that timely corrective action may be taken. (Ref. 10.)

9.4.4. Management awareness of critical problems required. Criticality category 1 and 1R problems must have priority consideration for resolution and implementation of remedial actions. They should be highlighted in Operational Readiness Reviews (ORRs) and other program reviews at all levels of management. Criticality ground rules, management requirements and criteria for analysis must be adhered to rigidly. Status and problem resolution records in all program and assurance management systems must be consistent. Acceptance of criticality category 1 and 1R risks temporarily and permanently must be reviewed by senior safety personnel who are not responsible for/to the program.

9.4.5. Resolution of critical problems must be consistent. All critical problems (hardware and software) must be resolved consistently using tightly controlled procedures. Systematically prioritizing problems for resolution based on risk, benefit to the program, and other factors will help assure the most critical problems are worked first. If there is a deviation, a risk assessment with justification must be included in the document of the problem.

9.4.6. Complete and accurate qualification data needed. The Space Station requirement for complete qualification data including performance and environmental envelopes and safety margins must be closely monitored during critical design and testing to ensure satisfactory problem resolution.

10. Trend Analysis

10.1. Problem

There was a failure to trend all critical performance anomalies, understand existing trend data and take timely management action to resolve unfavorable trends. Little or no trend analysis was performed on O-

ring erosion and blow-by problems, on statistics relating to human errors and on configuration management and schedule related adverse trends.

10.2. Causes

10.2.1. Inconsistent nonconformance trend analysis. Nonconformance trend analysis was inconsistently performed within NASA.

10.2.1.A. Inadequate requirements for trend analysis. Requirements for the performance of trend analysis were inadequately defined.

10.2.1.B. Adverse trends not identified. Trends for the O-ring thermal distress events, which appear obvious in hindsight, were not identified. There was an increase in the frequency of O-ring incidents after several changes were made on the SRB processing procedures, including an increase in leak check pressures. The SR&QA program failed to track and discover the reason for the increased frequency of O-ring erosion and blow-by events. Other adverse trends included an increase in workmanship errors and an increasing backlog of engineering modifications.

10.2.1.C. Trend analysis incomplete. The trend analysis of the temperature dependence of the O-ring incidents was performed incompletely and failed to identify the correlation.

10.2.2. Safety critical trend data was ignored. There was insufficient follow up to characterize trends in repeated performance anomalies and implement corrective action. Some trend data presented was insufficiently communicated or misunderstood.

10.3. Lessons Learned

10.3.1. Trend analysis is mandatory. Requirements for the performance of problem and other adverse trend analyses must be standard elements of program and SRM&QA management systems. Critical systems (hardware and software) should be subjected to a continuing analysis of performance and operating trends to identify increased safety risks and impending failures. In addition, data reflecting states of quality of workmanship, status of modifications that are designed to decrease risks, status of configuration controls and other key data should be monitored and analyzed for adverse trends.

10.3.2. Response to adverse trends required. When repeatability of flight/operations anomalies on critical systems is demonstrated by trend analysis, limitations or constraints must be imposed to accommodate the anomaly, and testing and analysis should be used to positively characterize it with recommendations for elimination or mitigation of the deficiency. Prompt action must be taken to correct the deficiencies which cause the adverse trends. Proposed resolution of the attendant remedial actions must be independently assessed.

10.4. Space Station Applications

10.4.1. Trend analysis is mandatory. Requirements for the performance and reporting of trend analyses must be included in SSP requirements documentation, and in all appropriate contract data requirements as well as in agreements between SSP organizations including Level II, Level III, the international partners and the SRM&QA. Critical systems (hardware and software) should be subjected to a continuing analysis of performance and operating trends to identify increased safety risks and impending failures. In addition, data reflecting states of quality of workmanship, status of modifications that are designed to decrease risks, status of configuration controls and other key data should be monitored and analyzed for adverse trends.

10.4.2. Response to adverse trends required. When repeatability of flight/operations anomalies on critical systems is demonstrated by trend analysis, constraints should be imposed to accommodate the anomaly and testing and analysis should be used to positively characterize it with recommendations for elimination or mitigation of the deficiency. Prompt action must be taken to correct the deficiencies which cause the adverse trends. Proposed resolution of the attendant remedial actions must be independently assessed.

11. Flight Readiness Reviews

11.1. Problem

There was a degradation of the Flight Readiness Review process.

11.2. Causes

11.2.1. FRR procedures were ignored. Defined FRR procedures were not followed adequately.

11.2.1.A. FRR reduced importance. FRRs had been reduced in importance. Reviews in some cases were conducted only by teleconference, incomplete attendance of key personnel and presentations curtailed by time constraints.

11.2.1.B. Requirements for readiness statements not enforced. There was a failure to enforce a clear requirement for definite readiness statements.

11.2.1.C. Key meetings not recorded. Review procedures and communications used to assure flight readiness were systematic, thorough and comprehensive and provided ample opportunity for surfacing hardware problems prior to flight. FRRs were usually recorded (audio); however there was often no record made of other key prelaunch meetings.

11.2.2. Failure to communicate critical concerns. The decision to launch 51-L was based on incomplete and at times misleading information.

11.2.2.A. Communication to responsible management. There was a failure to adequately communicate concerns to the responsible Level I and Level II management within the FRR process.

11.2.2.B. Communication by delta reviews only. Coverage of critical issues was reduced to "delta reviews," with data presented covering only elements on the previous flight that fell outside of expected performance.

11.2.2.C. Teleconference data not reported. Results of a January 27 teleconference were not reported to Level I. This teleconference was between engineers from MSFC and Thiokol who argued hours into the night regarding the effect of temperature on the performance of the seals. Thiokol engineers' concerns were not conveyed to Level I during the FRR process.

11.2.3. Inadequate SR&QA representation. There was inadequate SR&QA representation at key meetings, and in some cases, none.

11.3. Lessons Learned

11.3.1. Flight readiness review process must be maintained. The FRR process must be maintained rigorously to assure that all critical issues relative to readiness and safety are identified and reviewed. FRRs must include assurance that all previous operational anomalies have been reviewed and properly dispositioned. The importance of FRRs must be reinforced. Readiness statements, including specific information on concerns about capability of the system elements to perform required functions safely, must be mandatory from contractors and from organizations within NASA responsible for specific systems. NASA should ensure that complete written records of critical meetings (e.g., FRRs and associated meetings) are accurately maintained.

11.3.2. Clear and accurate communications vital. Critical decisions surrounding hazardous flight operations must be based on clear communications conveyed through established channels. All critical concerns must be fully communicated to all appropriate levels of management so that critical decisions can be made based on complete information.

11.3.3. Independent SRM&QA participation needed. Independent SRM&QA personnel must be active participants and an effective integral part of the program structure, review processes, and key management organizations responsible for determining flight readiness.

11.4. Space Station Applications

11.4.1. Rigorous maintenance of flight readiness review process required. The FRR process as defined in SSP requirements documentation, must be maintained rigorously to assure that all critical issues relative to readiness and safety are identified and reviewed. FRRs must include assurance that all previous flight anomalies have been reviewed and properly dispositioned. The importance of FRRs must be emphasized. Readiness statements, including specific information on concerns about capability of the system elements

to perform required functions safely, must be mandatory from contractors and from organizations within the Program responsible for specific systems. Assurance is required that complete written records of critical meetings (e.g., FRRs and associated meetings) are accurately maintained.

11.4.2. Clear and accurate communications vital. SSP systems and documentation must be reviewed and changed as necessary to assure that critical decisions related to flight operations are based on clear communications conveyed through established channels. All critical concerns must be fully communicated to all appropriate levels of management so that critical decisions can be made based on complete information.

11.4.3. Independent SRM&QA participation required. The Space Station Program requires that independent SRM&QA personnel be active participants and an effective integral part of the program structure, review processes, and key management organizations responsible for determining flight readiness. The integrity of this independent and vital role must be maintained.

12. Assurance Information System

12.1. Problem

Assurance information system criteria, requirements and management were inadequate.

12.2. Causes

12.2.1. Lack of appropriate data to support safety risk decisions. Critical data necessary to support safety risk decisions relative to the launch of STS 51-L were either not available, or accessible only with great difficulty, effectively making it unavailable.

12.2.1.A. Environment, launch and flight data. Environmental certification, launch constraints and flight experience data were not easily accessible at the time of launch.

12.2.1.B. SRM performance data. Information on test and performance which supported safety margins on the SRM field joint were not readily available.

12.2.2. Inadequate definition of data requirements. The information needed to perform systems assurance, problem tracking and safety assessments was not defined.

12.2.2.A. Safety data. Requirements for data and criteria to evaluate safety problem areas and adverse trends were not defined.

12.2.2.B. Launch decision data. Information requirements for each level of review in the launch decision process were not defined.

12.2.3. Data not ranked and sorted to indicate importance. Large amounts of information were disseminated on a routine basis, often with little or no indication of its importance to all recipients. Providing wide distribution for information of minor importance contributed to an "information glut" with the net effect of increasing the chance that important information would not receive adequate scrutiny.

12.3. Lessons Learned

12.3.1. Assurance information system required. An information system should be maintained to provide environmental certification, launch and operational constraints and flight experience data to support the launch or operations decision process and to be readily available to designers, planners and operational personnel on a real time basis, as well as being available for independent safety assessment. Examples of data include range of environments specified for each element and subsystem, method of certification, flight exposure, waivers granted and their justification.

12.3.2. Information requirements must be defined. The basic information requirements needed to support operational decision making and SRM&QA assurance and assessment functions must be defined and maintained. The requirements should identify what the data needs are, how the data is to be generated or extracted from other data systems, when the data is needed and in what form.

12.3.3. Priority information must be identified. Program management must identify priority information. It also must establish the criteria and procedures for processing priority information and make these criteria and procedures available for SRM&QA review.

12.4. Space Station Applications

12.4.1. Assurance information system required. SSP information systems should support operational decision making by tracking and making accessible data such as environmental certification limits, method of certification, operational constraints, waivers granted and their justification and flight experience. The information should also be readily available to designers, planners and SRM&QA for independent safety assessment.

12.4.2. Information requirements must be defined. The basic information requirements needed to support operational decision making and SRM&QA assurance and assessment functions must be defined, incorporated in SSP information systems requirements documentation and maintained throughout all SSP phases. The requirements should identify what the data needs are, how the data is to be generated or extracted from other data systems, when the data is needed and in what form. Attention should be given to identifying data that must be collected during the current phase of the SSP which will be required during later phases.

12.4.3. Priority information must be identified. Priority information should be identified within the SSP. Level II should establish the criteria and procedures for processing priority information and make these criteria and procedures available for SRM&QA review.

13. Engineering Change Process

13.1. Problem

The method used to prioritize changes based on criticality was inadequate for the engineering change system.

13.2. Causes

13.2.1. Inadequate change evaluation due to schedule pressures. Schedule pressures from the increased flight rate adversely affected the ability to implement, evaluate, test and certify changes in hardware design.

13.2.2. Inadequate prioritization of changes. Inadequate prioritization of changes contributed to pressures on the engineering change system and increased the potential that important changes to mission critical elements received inadequate attention.

13.3. Lessons Learned

13.3.1. Schedule pressures must not impact the engineering change process. Schedule pressures must not be allowed to "short circuit" the change process. The process must ensure that important changes are given high priority within the system and receive adequate scrutiny and management attention. Consideration should be given to procedures to reduce the number of minor changes requiring high level attention while avoiding the greater risk of inadvertently filtering important information from management attention. (Ref. 17.3.1.)

13.3.2. Prioritization of engineering changes needed. Categories of importance must be maintained and applied consistently to permit highlighting of critical changes. The highest priority changes should be those which involve significant changes to mission critical elements crucial to flight safety. The criteria for prioritizing changes should be maintained by the programs and reviewed by program SRM&QA with independent overview by agency SRM&QA.

13.4. Space Station Applications

13.4.1. Schedule pressures must not impact the engineering change process. Schedule pressures must not be allowed to "short circuit" the SSP change process. The process must ensure that important changes are given high priority within the system and receive adequate scrutiny and management attention. Consideration should be given to procedures to reduce the number of minor changes requiring high level

attention while avoiding the greater risk of inadvertently filtering important information from management attention. Space Station requirements documentation requires that program SRM&QA review proposed engineering changes for identification and resolution of hazards that may be introduced into the system and provide concurrence or non-concurrence based on each review. SSP management should consider expanding this change processing role to include analysis to assure that proposed changes and the change system itself are not being adversely impacted by schedule pressures.

13.4.2. Prioritization of engineering changes needed. Categories of importance must be maintained and applied consistently to permit highlighting of critical changes in the SSP. The highest priority changes should be those which involve significant changes to mission control elements crucial to flight safety. The criteria for prioritizing changes should be maintained by appropriate SSP organizational elements and reviewed by SSP SRM&QA. Agency SRM&QA should review the change processing system independently to assure that assigned priorities are commensurate with safety objectives.

3.5 Plans

14. Crew Safety

14.1. Problem

There were no crew escape options during Shuttle first stage operation.

14.2. Causes

14.2.1. Management decisions to exclude crew escape options during first stage operation. The Shuttle Program management considered first stage abort options and crew escape options several times during the history of the program but opted not to implement any of the systems considered despite the fact that first stage operation is probably the most hazardous phase of the mission.

14.2.1.A. Limited utility options. No one solution covered a wide range of abort and crew escape scenarios.

14.2.1.B. Limited program funds. Funds were limited and management was forced to make compromise decisions regarding the best use of funds available.

14.2.1.C. Potentially greater risks. Some technically feasible options were undesirable because the risk that would have been introduced to the program was potentially greater than having no abort capability. Other options were not technically feasible.

14.2.1.D. Further schedule delays. Implementation of feasible, desirable options would have further delayed the first Shuttle flight which was already far behind its original schedule.

14.3. Lessons Learned

14.3.1. Crew safety critical to program success. Requirements concepts and implementation planning for manned-flight programs must provide for adequate crew safety in emergency situations, including early detection (caution and warning) and either avoidance, safe haven mode(s), escape or rescue, or combinations thereof. Limits and constraints must be developed for each category of emergency situation.

14.3.1.A. Crew safety early planning a must. Requirements implementation and plans, including funds, must be established early in manned-flight programs to preclude later schedule and funding impacts that prove to be unfeasible.

14.3.1.B. Crew safety assurance required. SRM&QA must provide periodic reviews over the life of the program to assure that adequate crew safety planning and implementation is maintained.

14.4. Space Station Applications

14.4.1. Periodic review of crew safety requirements essential. Current SSP documentation specifies a variety of requirements levied to ensure crew safety, such as safing capabilities, safe haven concepts, conservative factors of safety related to pressurized elements, fire suppression capability, extravehicular activities safety concerns, etc. These program and related documents should be periodically reviewed by SSP management and SRM&QA and updated to assure that requirements, concepts and implementation provide for all crew emergency situations, and that crew safety is a reality which will remain throughout the life of the program.

15. Contract Safety Requirements

15.1. Problem

Existing contract requirements and incentives used by NASA do not adequately address or promote safety and quality concerns.

15.2. Causes

15.2.1. Contracts emphasize schedule and cost, little safety. Key Shuttle contracts provide greater incentives to contractors for minimizing costs and meeting schedules than for features related to safety and performance. The Shuttle Processing Contract (SPC) is cost-plus, incentive/award fee. The amount of incentive fee is based on contract costs (lower cost yields a larger incentive fee) and on safe and successful launch and recovery of the Orbiter. The award fee portion permits focus on areas not sensitive to incentive provisions, including the safety record of the contractor. However, the incentive fee portion is 14 percent maximum and the award fee portion is one percent maximum. The SRM contract is cost-plus, incentive-fee since July 1983 and is based strictly on costs, although penalties may be invoked for delays in delivery or for Shuttle accidents due to SRM failure.

15.2.1.A. Safety incentives inconsistent and deficient. Contracts vary in the extent of their safety incentives and such variances can contribute to differences in system safety and operational safety. SPC was graded high in the "Fair" range despite serious processing problems, especially with respect to the Orbiter. "Fair" definition: "Effective performance; responsive to contract requirements; adequate results. Reportable deficiencies with identifiable, but not substantial, effects on performance."

15.2.1.B. Safety requirements inconsistent and deficient. System safety plans are used primarily to fill an initial contract deliverable requirement and are not updated or used in contract management. Most contracts require that a system safety plan be submitted and approved, but in at least one case, this plan was the primary output of the system safety program because the contract did not specify that the plan be implemented. There was no evidence that any system safety plans were used during contract management. In addition, the plans contained no specific information upon which the contractor could be evaluated for award fee purposes. This lack of emphasis in properly specifying system safety contract requirements can be, to some degree, attributed to changes and resulting deletion of system safety requirements in procurement regulations. (Ref. 8.2.2.)

15.3 Lessons Learned

15.3.1. Contract safety and quality emphasis is mandatory. Agency and program policies, directives and processes must be maintained to reflect appropriate and continuing emphasis, guidance and direction on safety and quality content of procurement planning and implementation, including procurement regulations and award fee evaluation plans.

15.3.1.A. Balanced contract incentive structure required. Contract incentive structure must be carefully studied during procurement planning to assure proper balance between safety, performance, cost and schedule features. Meaningful amounts of safety and quality incentive/award fee must be incorporated.

15.3.1.B. Contract incentives review required. Agency SRM&QA must maintain a specific and continuing independent review to assure that necessary policies, directives and processes related to contractual safety and quality incentive features are in place, are effective, are being interpreted properly and are being implemented properly, including procurement regulations and award fee evaluation plans.

15.3.1.C. Contract incentive/award fee training required. A required formal training system must be maintained to assure that both government and contractor involved in incentive/award fee planning and implementation have an adequate understanding and expertise.

15.3.1.D. Effective contractual safety plans required. Program SR&QA must: 1) assure that adequate and effective safety plans are included in ongoing and planned contracts; and 2) periodically review contractual safety plans and their implementation and assure corrective action where deficiencies are found. The requirement for a System Safety Management Plan must be included in the planning of all incentive/award fee contracts. Deliverables included in this plan shall be used to evaluate safety and quality activities and related fee performance. All safety plans must be included in the contractor configuration management process to assure that change control and reporting is maintained.

15.3.1.E. SRM&QA involvement required. Program SRM&QA must be involved specifically and continually in the incentive/award fee process, both to establish reasonable guidelines and rewards in new contract planning and to judge performance of active contracts.

15.4. Space Station Applications

15.4.1. Contract safety and quality emphasis is mandatory. Space Station Program policies, directives and processes must be maintained to reflect appropriate and continuing emphasis, guidance and direction on safety and quality content of procurement planning and implementation.

15.4.1.A. Balanced contract incentive structure required. Space Station Program SRM&QA must review all ongoing and planned SSP contracts to assure that adequate safety and quality content is provided. The emphasis and weighting of SRM&QA disciplines in development of evaluation criteria must be assessed for consistency and level of importance. The same balance of SRM&QA emphasis and weighting must be incorporated in the re-assessment process for each evaluation period over the life of contracts.

15.4.1.B. Contract incentives review required. Agency SRM&QA must maintain a specific and continuing independent review of SSP ongoing and planned contracts to assure that necessary policies, directives and processes related to contractual safety and quality incentive features are in place, are effective, are being interpreted properly and are being implemented properly, including procurement regulations and award fee evaluation plans.

15.4.1.C. Contract incentive/award fee training required. Space Station Program must maintain/require a formal training system for government and contractor personnel involved in incentive/award fee planning and implementation to assure adequate understanding and expertise.

15.4.1.D. Effective contractual safety plans required. Space Station Program SRM&QA must: 1) assure that adequate and effective safety plans are included in ongoing and planned contracts; and 2) periodically review contractual safety plans and their implementation and assure corrective action where deficiencies are found. The requirement for a System Safety Management Plan must be included in all ongoing and planned incentive/award fee contracts; deliverables must be included to permit evaluation of safety and quality activities for fee determination. All safety plans must be included in the contractor configuration management process to assure that change control and reporting is effectively maintained.

15.4.1.E. SRM&QA involvement required. SSP SRM&QA must be involved specifically and continually in the incentive/award fee process as it relates to the assurance disciplines, both to establish reasonable guidelines and rewards in new contract planning and to judge performance of active contracts (Ref. 15.4.1.A.).

Content of active Phase C/D contracts should be reviewed to ensure that SRM&QA requirements were adequately established in view of the low emphasis placed on some SRM&QA evaluation factors in recently concluded Phase C/D Procurements. (Ref. 16.4.2.)

16. Contractor Selection Emphasis

16.1. Problem

Evaluation factors and criteria for competitive contract award were not structured to provide adequate safety and technical consideration.

16.2. Causes

16.2.1. Cost overrode all other contract selection factors. Cost consideration overrode any other objections in the selection of Thiokol as the Shuttle SRM contractor. As part of the SRM proposal evaluation, suitability factors were used for grading: 1) Design, Development and Verification; 2) Manufacturing, Refurbishment and Support; and 3) Management. Cost was evaluated separately. (Ref. 8.2.2.)

16.2.1.A. Thiokol low cost. Thiokol was first (lowest) under Cost. Thiokol was last (of four) under Factor One, second under Factor Two and first under Factor Three.

16.2.1.B. Technical deficiencies correctable. The Source Evaluation Board (SEB) concluded that the main criticisms of the Thiokol proposal were technical in nature, were readily correctable and the costs to correct did not negate the sizeable Thiokol cost advantage. Any selection other than Thiokol would give rise to an additional cost of appreciable size.

16.2.2. SRM&QA factors not considered at same level as other factors. Neither safety or quality was identified uniquely at a level even comparable to "Support".

16.2.2.A. Safety sub-factors. Logically, safety sub-factors (criteria) were contained within the three main, graded factors, however, safety was not considered at the same level as Design, Refurbishment, etc.

16.2.2.B. Quality sub-factors. Quality relates to technical excellence which was graded last (Factor One) and second (Factor Two).

16.3. Lessons Learned

16.3.1. Emphasis of SRM&QA evaluation factors in the contractor selection process is required. Appropriate consideration of SRM&QA and technical factors must be maintained when evaluating potential contractors as part of the procurement process.

16.3.2. SRM&QA assurance of the contractor selection process is required. The SRM&QA function must provide assurance that necessary program policies, directives, plans and procedures contain adequate SRM&QA evaluation factors and weighting of factors, that this documentation is being applied correctly to specific procurements and that the SEB process accurately reflects consideration of SRM&QA evaluation results. SRM&QA must also periodically review procurement regulations to determine deficiencies in SRM&QA coverage, make recommendations for changes and follow-up on corrective measures.

16.4. Space Station Applications

16.4.1. Emphasis of SRM&QA factors in the contractor selection process is required. The Space Station Program must maintain appropriate consideration of SRM&QA and technical factors when evaluating potential contractors as part of the procurement process.

16.4.2. SRM&QA assurance of the contractor selection process is required. SSP SRM&QA must provide assurance that necessary policies, directives, plans and procedures contain adequate SRM&QA emphasis, evaluation factors and weighting of factors, that this documentation is being applied correctly to specific procurements and that the process accurately reflects consideration of SRM&QA evaluation results.

Content of planned SSP Phase C/D procurements should be reviewed to ensure that SRM&QA requirements are adequately established in view of the low emphasis placed on some SRM&QA evaluation factors in recently concluded Phase C/D procurements. (Ref. 15.4.1.) This effort should include involvement in the development of changes to procurement regulations currently being considered to assure adequate SRM&QA emphasis.

17. Schedule Pressures

17.1. Problem

Schedule pressures degraded safety through the overtaxing of resources, facilities, processes and personnel.

17.2. Causes

17.2.1. Pressure to cut costs by flying more frequently. The most pressing reason for compressing the flight schedule to permit the maximum number of launches per year was the NASA promise made to Congress and the White House to minimize the cost per launch.

17.2.1.A. Striving to reduce launch unit costs. Annual sustaining program costs were so much greater than the added cost of an individual launch that doubling the launches per year would almost half the cost per launch.

17.2.1.B. Overly optimistic schedules. The optimistic schedules would have been most difficult to meet if all endeavors were completely successful, which they were not.

17.2.2. Success oriented planning ignored the real world. In the zeal to achieve the compressed flight schedule, planners failed to consider the impact of engineering changes, problems, lack of spares, mission changes and therefore failed to provide for contingencies. This planning failure led in turn to other management discipline failures and compromised the already weak risk management function. (Ref. 8.2.3 and 18.2.1.)

17.2.2.A. Payload manifest changes. The payload manifests were not frozen prior to the initiation of flight preparation. Modifications to planning, hardware, Operations and Maintenance Instructions (OMIs) and software were required when complex payloads changed flights or additions were made to the on-orbit activities. Though a credit to the personnel working these changes that their work did not cause a catastrophic failure, the personnel resource was hard pressed to the point where safety of the missions was in jeopardy.

17.2.2.B. Inadequate contingency planning. No planning had been made for modifications, problem resolution and unscheduled maintenance so that these functions had to be worked into the tight schedule, usually on overtime, or deferred with no assessment of the increased risk involved.

17.2.2.C. Spares shortage. The shortage of spares forced the more time- consuming and risky practice of cannibalization.

17.2.2.D. Non-standard launch pads. Pad A and Pad B of LC 39 were not identical, adding to paperwork, training, learning curve and the spares problem. Switching people between the pads greatly increased the risk of human error.

17.2.2.E. Planned landings at KSC. Planning identified most Shuttle landings for KSC. However, weather and Orbiter steering and brake deficiencies caused the landing to be switched to Edwards, lengthening the turnaround time and tightening the schedule even more.

17.3. Lessons Learned

17.3.1. Realistic and flexible schedules are mandatory. Realistic and flexible schedules must be maintained; success-oriented schedules must not be permitted. A variation of the Program Evaluation Review Technique (PERT) should serve as a starting point for developing a system to exploit successes without having a perturbation to the optimistic time appear as a gross failure in the schedule, i.e., have a best possible, worse possible, and most likely event time. Operations and SRM&QA must have detailed involvement in the preparation of master flight schedules.

17.3.2. Real world planning is mandatory. Program planning should use previous experience including lessons learned to schedule and control tasks. Payload users must define firm support and schedule requirements prior to inclusion in approved schedules. Established safety criteria must be enforced for overtime work; any plans that exceed these criteria must be submitted for approval to Level I/II and assurance management. Safety should consider excessive overtime as a justification to hault critical operations. Modifications, problem resolution and unscheduled maintenance are tasks that are difficult to define in a long range plan, but there must be schedule flexibility, such as designated contingency periods or non-scheduled periods (off shifts, weekends, holidays), that will allow these types of work to be completed without impacting the flight schedule. Either spares must be on hand or sufficient time must be allocated to cannibalize and restore a system to an operable condition without impacting the flight schedule adversely (e.g., excessive overtime, undue pressure).

17.4. Space Station Applications

17.4.1. Realistic and flexible schedules are mandatory. Realistic and flexible schedules must be maintained; success-oriented schedules must not be permitted. SSP should review and change, as necessary, currently established schedule systems and schedules to ensure that realism and flexibility is maintained (including Program/Project Controlled Milestones and the Engineering Master Schedule). SSP Operations and SRM&QA must have detailed involvement in the preparation of master flight schedules.

17.4.2. Real world planning is mandatory. SSP planning should use previous experience including lessons learned to schedule and control tasks. Payload users must define firm support and schedule requirements prior to inclusion in approved schedules. Safety criteria must be maintained for overtime work; any plans that exceed these criteria must be submitted for approval to Level I/II and assurance management. Safety should consider excessive overtime as a justification to halt critical operations. Modifications, problem resolution and unscheduled maintenance are tasks that are difficult to define in a long range plan, but there must be schedule flexibility, such as designated contingency periods or non-scheduled periods (off shifts, weekends, holidays), that will allow these types of work to be completed without impacting the flight schedule. Either spares must be on hand or sufficient time must be allocated to cannibalize and restore a system to an operable condition without impacting the flight schedule adversely (e.g., excessive overtime, undue pressure).

18. Critical Redesign

18.1. Problem

Resources for some critical redesign efforts were inadequate.

18.2. Causes

18.2.1. Poor planning for potential design problems. Funds allocated for redesigns were inadequate for design, demonstration and qualification of all SSME and SRB deficient critical items.

18.2.1.A. Insufficient resources. High-technology, complex, advance state-of-the-art programs usually plan for initial design problems and some redesign effort, but the Shuttle Program's problems in developing the Thermal Protection System, SRBs, ET disconnects and SSMEs were more costly than anticipated.

18.2.1.B. Incomplete redesign and testing. Failure to adequately plan for and fund critical redesign problems resulted in some selected redesigns, having incomplete qualification testing.

18.3. Lessons Learned

18.3.1. Effective contingency planning is required. High-technology, advanced state-of-the-art programs must provide means in early planning to accommodate uncertainties, design and qualification problems, and operational problems that could result in critical and/or expensive redesign and requalification. The Agency must review and maintain established policies and planning to ensure adequate planning for program contingencies.

18.4. Space Station Applications

18.4.1. Effective contingency planning is required. SSP must provide means to accommodate uncertainties, design and qualification problems and operational problems that could result in critical and/or expensive redesign and requalification. SSP should review established program/agency planning methods and Program Operating Plans to ensure adequate consideration of contingencies related to potential critical redesign and requalification.

3.6 Development

19. Environmental and Performance Specifications

19.1. Problem

Environmental and performance specifications for some critical flight components and GSE were not properly defined. The SRM aft joint seal assembly, including the O-ring and putty materials, was not compatible with the winter operations environment at KSC.

19.2. Causes

19.2.1. Failure to account for and explicitly define integrated environmental and performance criteria. Criteria for design, performance, launch and other processes and operations have used "ambient" as a reference base.

19.2.1.A. Quantification of ambient conditions. No quantification of "ambient" conditions expected to be encountered was described as measured at specific locations and interpreted in terms of effects of time of day, wind velocity, temperature, humidity, period of exposure and other parameters.

19.2.1.B. Cold soak analysis. The integrated analysis of the stacked vehicle did not account for induced environments such as the cold soak of the aft SRB joint from the ET Liquid Hydrogen (LH2) load.

19.2.1.C. Winter performance specifications. In turn, the NASA performance specifications did not adequately address the known Florida winter weather conditions or set use limits.

19.2.1.D. Joint assembly not qualified. The entire joint assembly including the O-rings and putty were not qualified for the low temperature environment encountered on January 28, 1986 because of inadequate criteria definition.

19.2.1.E. Failure to account for weather phenomena. The design of the SRB joint caused retention of rainwater. There was no weather seal. There were suspicions after the 51-L accident, based on observed anomalies on other SRB stack sets, that rainwater had intruded into the joint, frozen due to the environment on 51-L and thereby prevented the aft joint seals from functioning properly.

19.3. Lessons Learned

19.3.1. Complete environmental and performance definition required. Complete environmental envelopes of ground and flight operations, including weather related conditions, must be developed and maintained for safe flight. These requirements must be included in design and performance specifications, operations commit criteria, qualification and certification testing and Operations and Maintenance (O&M) procedures for critical flight components.

19.3.1.A. Test data should confirm critical operations criteria. All critical operations commit criteria should have direct-measurement data available to confirm adherence to the specified criteria. Instrumentation and sensors should be installed as necessary to measure performance and limits of critical components. Caution and warning devices and damage control procedures should be provided to assure that positive action can be taken in time to prevent dangerous coupling and cascading effects leading to catastrophic accidents.

19.3.1.B. Interface functional analysis essential to requirements development. Engineering and Safety should conduct an Element Interface Functional Analysis (EIFA) as early as feasible in the design process to identify normally expected conditions which result in changes across the interface and result in a hazard (i.e., venting, thermal soak, dynamic load and/or configuration changes, etc.). The results of the EFIA should be factored into the specification for performance of the materials and components.

19.3.1.C. Critical testing and certification needed. Criticality category 1 and 1R components and materials should be tested and certified over the entire operating range of environment (natural, induced and combined). Limitations must be clearly identified and strictly adhered to in processing, operating, and maintenance documents and procedures.

19.3.1.D. Critical material properties must be verifiable. Criticality category 1 and 1R materials must be specified in a manner which guarantees that constituency and critical properties can be measured, tested or inspected to verify acceptability.

19.3.1.E. Identification of critical limitations necessary. Performance specifications for criticality category 1 and 1R components and materials must include all known operating environment limitations plus adequate margins for contingencies and likely anomalous operations.

19.4. Space Station Applications

19.4.1. Complete environmental and performance definition required. Complete environmental envelopes of ground and flight operations, including weather related conditions and on-orbit environmental effects, must be developed and maintained for safe flight. These requirements must be included in design and performance specifications, operations commit criteria, qualification and certification testing and O&M procedures for critical mission components. Where possible, "off-limits" or over-stress testing should be conducted to establish margins and safety factors on mission critical assets.

19.4.1.A. Test data should confirm critical operations criteria. All critical operations commit criteria should have direct-measurement data available to confirm adherence to the specified criteria. Instrumentation, sensors and built-in test features should be installed as necessary to measure performance and limits of critical components; and caution and warning devices and damage control procedures should be provided to assure that positive action can be taken in time to prevent dangerous coupling and cascading effects leading to catastrophic accidents.

19.4.1.B. Interface functional analysis essential to requirements development. SSP Engineering and Safety should conduct an Element Interface Functional Analysis (EIFA) as early as feasible in the design process to identify normally expected conditions which result in changes across the interface and result in a hazard (e.g., venting, thermal soak, on-orbit internal and external environmental effects dynamic loads and/or configuration changes). The results of the EFIA should be factored into the specification for performance of the materials and components.

19.4.1.C. Critical testing and certification needed. Criticality category 1 and 1R components and other Classification A mission critical assets should be tested and certified over the entire operating range of environment (natural, induced and combined) for ground, flight and orbital operations. Limitations must be clearly identified and strictly adhered to in processing, operating, and maintenance documents and procedures.

19.4.1.D. Critical material properties must be verifiable. Criticality category 1 and 1R materials and other Classification A mission critical assets must be specified in a manner which guarantees that constituency and critical properties can be measured, tested or inspected to verify its acceptability.

19.4.1.E. Identification of critical limitations necessary. Performance specifications for criticality category 1 and 1R components and other Classification A mission critical assets must include all known operating environment limitations plus adequate margins for contingencies and likely anomalous operations.

20. Critical Item Tolerances and Margins

20.1. Problem

Critical reuse flight hardware was inadequately designed to maintain required tolerances and margins within its performance envelope over its specified life cycle. The SRB segment O-ring assembly was not properly designed, including necessary tolerances and margins, to sustain operational integrity under actual flight loads, off nominal weather conditions or the degradation associated with the reuse requirements.

20.2. Causes

20.2.1. Failure to maintain tolerances and margins over life cycle. Failure of the SRB aft segment O-ring assembly to maintain its dimensional integrity was a major contributor to the 5l-L accident.

20.2.1.A. Unusually precise tolerances needed for assembly. To provide an effective seal, the O-ring seal assembly on the SRM requires unusually precise tolerances and measurement accuracies during assembly.

20.2.1.B. Tolerances routinely waived for launch. Some of the tolerances were routinely waived in launches prior to 51-L despite the fact that the environmental effects and flight dynamic loads on these dimensional tolerances were not adequately characterized.

20.2.1.C. SRM case growth from reuse. Case growth brought about by reuse of case segments added to the difficulty of maintaining specified tolerances.

20.2.2. Failure to determine degradation of margins due to criticality recategorization and reuse. The loss of O-ring redundancy in several flights resulted in the recategorization of the O-ring assembly from criticality category 1R to category 1. The recategorization should have dictated a vigorous effort to more accurately determine the degradation due to reuse of components, determine the environmental and operating margins and impose appropriate launch constraints. This did not happen.

20.3. Lessons Learned

20.3.1. Operations critical verification must include analysis and testing. The design verification process must include effective analysis and testing to characterize the limits of safe performance and operational environment for all operations critical components. The characterization should include degradation limits over the entire life cycle for reuse items. (Ref. 19.3.1.)

20.3.1.A. Design tolerances must be realistic. Design specifications must stipulate tolerances which are compatible with realistic requirements for expected process controls and operating conditions (producibility and operability).

20.3.1.B. Deviation and waiver process must not be used to resolve tolerance and margin deficiencies. The waiver and deviation process must not be used as a substitute for solving those critical item tolerance and margins deficiencies which relate to safety risk. Repeated requests for deviations and waivers for the same problem on a critical item must be flagged as an adverse trend and the deviations and waivers dispositioned through the independent safety assessment and program decision management systems.

20.3.1.C. Original specifications must apply to reused components. Any used critical components shall be refurbished and tested to the same operations/flight worthiness specifications required for original mission critical components, or characterized by expected change such as wear, dimensional variation, fatigue life, etc. versus usage factors such as numbers of times used, length of use, cycles etc.

20.3.2. Off-nominal limits for critical item tolerances and margins must be specified. Precise tolerance and margin limits must be prescribed for both nominal and likely off-nominal (or anomalous) conditions relating to hazardous operations. These limits shall be stipulated in process controls, red-line specifications, operations commit criteria and operations rules. Limits must be verified and validated by test. Out of specification measurements must be highlighted in both in-line and assurance management reviews. Any deviations in limits must be flagged, evaluated against standards for risk assessment and dispositioned through the independent safety assessment and program decision management systems. Where necessary, analytical models including dynamic loads impacts should be developed to more accurately predict wearout characteristics; instrumentation should be developed to assure measurement of critical wearout tolerances; and trend criteria stipulated to flag items approaching dangerous operating conditions. Also, any anomalous or overstress condition should be reported and dispositioned through a formal safety problem and corrective action system.

20.3.3. Tolerance and margin verification process must be periodically reviewed. Modifications and enhancements as a result of technology improvements, work experience and special analyses (e.g., Non-destructive Evaluation (NDE) innovations, maintenance, life cycle modeling) must be periodically evaluated for possible improvements in the tolerance and margin verification process; such improvements must be incorporated where appropriate.

20.3.4. Flightworthy certification test results must be evaluated. Hardware and software flightworthy certification test results shall be routinely evaluated to verify that critical components tolerances and margins meet operations requirements. In turn, operations procedures and performance profiles shall be reviewed to assure that flight qualification and certification test specifications which verify critical item tolerances and margins reflect realistic operations stress and process requirements (including changes in requirements since last review) and anticipated operations conditions (including emergency operations).

20.4. Space Station Applications

20.4.1. Operations critical verification must include analysis and testing. The design verification process must include effective analysis and testing to characterize the limits of safe performance and operational environment for all operations critical components. The characterization should include degradation limits over the entire life cycle for reuse items. (Ref. 19.4.1.)

20.4.1.A. Design tolerances must be realistic. Design specifications must stipulate tolerances which are compatible with realistic requirements for expected process controls and operating conditions (producibility and operability). The practicality of tolerance controls should be evaluated in design reviews and verified in combined-elements integrated system verification processes.

20.4.1.B. Deviation and waiver process must not be used to resolve tolerance and margin deficiencies. The deviation and waiver process must not be used as a substitute for solving those critical item tolerance and margins deficiencies which relate to safety risk. Repeated requests for deviations and waivers for the same problem on a critical item must be flagged as an adverse trend and the deviations/waivers dispositioned through the independent safety assessment and program decision management systems.

20.4.1.C. Original specifications must apply to reused components.

Any used critical components shall be refurbished and tested to the same operations/flight worthiness specifications required for original mission critical components, or characterized by expected change such as wear, dimensional variation, fatigue life, etc. versus usage factors such as numbers of times used, length of use, cycles etc.

20.4.2. Off-nominal limits for critical item tolerances and margins must be specified. Precise tolerance and margin limits must be prescribed for both nominal and likely off-nominal (or anomalous) conditions relating to ground and flight hazardous operations. These limits shall be stipulated in process controls, red-line specifications, operations commit criteria and flight operations rules. Limits must be verified and validated by test. Out of specification measurements must be highlighted in both SSP in-line and assurance management reviews. Any deviations in limits must be flagged, evaluated against standards for risk assessment and dispositioned through the independent safety assessment and program decision management systems. Where necessary, analytical models including dynamic loads impacts should be developed to more accurately predict critical item wearout characteristics; instrumentation should be developed to assure measurement of critical wearout tolerances; an on-board inspection and measurement capability should be developed and trend criteria stipulated to flag items approaching dangerous operating conditions. Also, any anomalous or overstress condition should be reported and dispositioned through a formal safety problem and corrective action system.

20.4.3. Tolerance and margin verification process must be periodically reviewed. Modifications and enhancements as a result of technology improvements, work experience and special analyses (e.g., NDE innovations, maintenance, life cycle modeling) must be periodically evaluated for possible improvements in the tolerance and margin verification process; such improvements shall be incorporated where appropriate.

20.4.4. Flightworthy certification test results must be evaluated. Hardware and software flightworthy certification test results shall be routinely evaluated to verify that critical components tolerances and margins meet operations requirements. In turn, operations procedures and performance profiles shall be reviewed to assure that flight qualification and certification test specifications which verify critical item tolerances and margins reflect realistic operations stress and process requirements (including changes in requirements since last review) and anticipated operations conditions (including EVA, payload deployment, Station reboost, Orbiter maneuvering and docking, OMV operations and contingency operations for each of these activities).

21. Test Specifications

21.1. Problem

Qualification, certification and other test specifications for some flight critical components were not properly defined.

21.2. Causes

21.2.1. Inadequate performance and verification specifications. Component and material performance specifications were not adequate to assure required performance with an acceptable margin of safety.

21.2.1.A. Inadequate O-ring specifications. The SRM O-ring specification did not contain realistic performance or temperature requirements, nor did they require performance under all potential conditions of case out-of-roundness and dynamic loads.

21.2.1.B. Inadequate putty specifications. The proprietary putty lacked requirements for a specific material or for defined acceptability. Procuring a proprietary product forces NASA to: buy rights to proprietary data and even contract for in-process inspection agreements; accept the manufacturer's certification that the material complies with specifications; or fully define the technical requirements and means of verifying compliance.

21.2.2. Interaction between systems not thoroughly assessed. Interaction between systems was not thoroughly assessed for impact of the system, component and part specifications as the total integration of the Shuttle took place. Therefore, comprehensive qualification test specifications were not prepared for the SRMs, O-rings, putty or the SSMEs although no other method of qualification appears justifiable.

21.3. Lessons Learned

21.3.1. Comprehensive performance, process and material specifications needed. Every acceptable performance or material specification must contain provisions for assuring that the performance or material will satisfy all required conditions. To assure this, the required performance must be defined in detail and the operating and non-operating environment specified. The quality assurance requirements must provide for verification of the compliance with each requirement.

21.3.1.A. Critical items must be fully qualified. All critical items must be fully qualified by testing or other means. New materials and new designs must require thorough testing to determine all technical characteristics, environmental effects, stress margins, and failure rates prior to introduction into critical usage. Test specifications must assure that testing will provide these data. (Ref. 19.3.1. and 23.3.1.)

21.3.1.B. Proprietary product specifications must be adequate. Proprietary critical products must be described by adequate performance, process and material specifications despite restricted data problems. The use of such products should be avoided where data is not available. (Ref. 22.3.1.B.)

21.3.2. Interactions between systems must be accommodated. As designs approach the critical design review point, the systems engineering function for the program integrator must review all potential physical and functional interactions possible between systems, equipment, and facilities, and initiate updating of the affected specifications.

21.4. Space Station Applications

21.4.1. Comprehensive performance, process and material specifications needed. Every acceptable SSP performance or material specification must contain provisions for assuring that the performance or material will satisfy all required conditions. Even proprietary items and materials must have specifications defining performance, environmental and testing (or other assurance) requirements. Proprietary components and materials should be avoided if required data is not available. Qualification testing must not only assure the ability to meet all performance and environmental requirements, they should also furnish data on design and safety margins, initial data on failure rates, most likely failure modes and expected life.

21.4.2. Interactions between systems must be accommodated. Interactions between systems/equipment must be accommodated. As Space Station designs approach the critical design review point, the systems engineering function for the program integrator must review all potential physical and functional interactions possible between systems, equipment, and facilities, and initiate updating of the affected specifications.

22. Design Characterization and Test Verification

22.1. Problem

Design characterization and test verification of some critical flight components and materials were inadequate.

22.2. Causes

22.2.1. Lack of traceability of performance and environmental requirements. Sound program practice requires performance and environmental requirements to be traceable from the program requirements documents through system, equipment, component, piece part and material specifications; this traceability with the accompanying additional definitive details was missing in critical areas required to assure successful verification/qualification testing. The SRM field joint design failed to consider all potential stress combinations.

22.2.A. Incomplete test verification. Testing to verify actual requirements was incomplete. The requirements from Design and Quality Assurance sometimes were not enforced during operations.

22.3. Lessons Learned

22.3.1. Program requirements must be traceable. Program requirements must be specifically defined and controlled as early as possible in a program and must be continuously reflected throughout all levels of specifications during development and operations. Specifications for critical items must be so identified and completely traceable to corresponding program requirements. (Ref. 19.)

22.3.1.A. Compliance verification is required. Compliance with each requirement under environmental extremes must be verified. Verification of critical items is mandatory, preferably by testing. (Ref. 21.)

22.3.1.B. Proprietary items should be avoided. Proprietary items should be avoided where practical. If proprietary items are selected, requirements and verification must be definitive as necessary to assure that all requirements are satisfied. (Ref. 24 and 21.3.1.A.)

22.3.1.C. OMRSD/OMI must meet original intent. OMRSD and OMI must meet the original intent. That is, the designer must specify in the OMRSD each requirement of the design to ensure proper performance and the operator or maintainer must reflect in the OMI each OMRSD requirement and specify, step by step, the process and tolerances of compliance and the verification of critical functions and characteristics. (Ref. 27.)

22.4. Space Station Applications

22.4.1. Program requirements must be traceable. SSP should assure that program requirements contained in the PDRD and related documents are specifically defined, are controlled and are continuously reflected throughout all levels of specifications. Specifications for critical items must be so identified and completely traceable to corresponding program requirements.

22.4.1.A. Compliance verification is required. Compliance with each SSP requirement under environmental extremes must be verified. Verification of critical items is mandatory, preferably by testing.

22.4.1.B. Proprietary items should be avoided. SSP proprietary items should be avoided where practical. If proprietary items are selected, requirements and verification must be definitive as necessary to assure that all requirements are satisfied.

22.4.1.C. OMRSD/OMI must meet original intent. OMRSD and OMI must meet the original intent. That is, the designer must specify in the OMRSD each requirement of the design to ensure proper performance and the operator or maintainer must reflect in the OMI, each OMRSD requirement and specify, step by step, the process and tolerances of compliance and the verification of critical functions and characteristics.

23. Qualification Testing

23.1. Problem

Qualification testing to verify performance/operations including performance margins was inadequate for some flight critical components.

23.2. Causes

23.2.1. Tests did not duplicate flight environments. Specifications for parts, materials and assemblies for both propulsion systems were not adequate to perform comprehensive qualification tests that would permit certification by analysis, sub-scale tests or similarity.

23.2.1.A. SRM testing. The SRM static test stand did not duplicate flight attitude, dynamic stresses, minimum/maximum ignition environments or flight temperature extremes.

23.2.1.B. SSME testing. The SSME tests were not able to successfully demonstrate reliability, safety margins, and full performance capability.

23.3. Lessons Learned

23.3.1. Comprehensive qualification testing needed. To assure a successful program as stated in the NASA Engineering Experience Bulletin No. 1 released in the 1977 time frame:

"Qualification testing on all systems over the full range of possible environments shall be conducted in the future to the maximum extent feasible. Operational procedure documentation must be complete and must be checked for consistency with engineering and test data. Qualification testing and/or preflight integrated testing should include dynamic considerations and conditions of environment, functions, and time duplicating those to be encountered in mission operations to the maximum extent feasible."

For sound decisions in handling unplanned or marginal conditions, each manager should know the limits of performance, reliability and environment; the remaining useful life; factors of design safety; and the confidence level for the combinations of these parameters for critical systems and their components. This information must be made available also to assurance management. When test planning or test results are deficient, these deficiencies must be input to appropriate problem resolution systems. When qualification testing does not duplicate the actual operational environment, extensive and careful analysis must be performed before the item or system is certified. Additional testing or redesign must be undertaken when any question arises relative to marginal test results before certifying any critical item.

23.4. Space Station Applications

23.4.1. Comprehensive qualification testing needed. SSP requirements and procedures documentation must be reviewed and maintained to ensure comprehensive qualification testing, including the following considerations. Each critical system, equipment item and component must be qualified to perform under all environments that may be encountered during its planned useful life. Because tests are the most objective and least controversial method of qualification, they should be specified to the maximum extent feasible. Test specifications must be traceable from program requirements through design and verification specifications. The tests should be used to determine all critical parameters including performance envelopes, safety margins, environments limits, likely failure modes, failure rate and predicted life. When test planning or test results are deficient, these deficiencies must be input to appropriate problem resolution systems. When qualification testing does not duplicate the actual operational environment, extensive and careful analysis must be performed before the item or system is certified. Additional testing or redesign must be undertaken when any question arises relative to marginal test results before certifying any critical item.

24. Critical Process Control

24.1. Problem

Not all critical processes are formally identified and controlled. Neither NASA nor its contractors can adequately control the quality or consistency of critical materials which are manufactured with ingredients known only to the manufacturer.

24.2. Causes

24.2.1. NASA lacked control of some critical processes. It is evident that there is inadequate review by NASA to ensure that all manufacturing processes involving criticality category 1 and 1R components of all prime and subcontractors are appropriately designated as "critical processes".

24.2.1.A. Unknown putty behavior. Because original O-ring putty contained carcinogenic material (asbestos), it became necessary to procure a new putty when the original supplier stopped production. Performance of the new putty was highly unpredictable. Because the new putty was proprietary, there was no control on its process. Also, requalification testing was not adequate because characteristics of the new putty changed substantially as a function of humidity. It was difficult to apply in both the dry climate of Utah and dampness of Florida.

24.2.1.B. Unknown O-ring behavior. The behavior of fluorocarbon elastomer O-Rings was something of a mystery to NASA and its contractor because the material was "proprietary".

24.2.1.C. Critical change without approval. Changes in ingredients of the O-Ring and putty materials could be made without certification and approval, further compounding the problem of inadequate evaluation and testing.

24.3. Lessons Learned

24.3.1. Control of critical processes required. Manufacturing processes involving criticality category 1 and 1R items of all NASA contractors and subcontractors must be designated "critical" where appropriate and incorporated in the change management process. A highly disciplined review mechanism must be maintained to ensure that the process of identifying and controlling category 1 and 1R processes is effective. (Ref. 19.3.1.C.)

24.3.1.A. Review and verification essential. The use of materials in criticality category 1 and 1R applications, whose characteristics and fabrication processes are not well understood, must not only be tested and certified, but also provisions must be made for in-depth independent reviews of the test and certification results prior to approval. All lots of materials procured for use in category 1 and 1R applications must be subjected to sample testing or other verification of acceptability.

24.3.1.B. Change control required. Changes in critical materials with respect to ingredients, proportions and manufacturing processes must be considered "new" material and only be permitted after adequate retesting and recertification including the specific approval of the project and other appropriate review functions. (Ref. 13.3.2.)

24.3.1.C. Criticality awareness important. Employees of NASA contractors, including venders furnishing basic materials and manufacturers working on critical processes, must be made aware of the serious consequences of failure or malfunctioning of criticality category 1 and 1R components through formal awareness programs or comparable activity.

24.4. Space Station Applications

24.4.1. Control of critical processes required. SSP should review current materials manufacturing/processing reliability/control documentation to ensure that critical process control is understood and that specific guidance is included. Manufacturing processes involving criticality category 1 and 1R items of all contractors and subcontractors must be designated "critical" where appropriate and incorporated in the change management process. A highly disciplined review mechanism must be maintained to ensure that the process of identifying and controlling the category 1 and 1R processes is effective. (Ref. 19.4.1.C.)

24.4.1.A. Review and verification essential. The use of materials in criticality category 1 and 1R applications, whose characteristics and fabrication processes are not well understood, should not only be tested and certified, but also provisions should be made for in-depth independent reviews of the test and certification results prior to approval. All lots of materials procured for use in category 1 and 1R applications must be subjected to sample testing or other verification of acceptability.

24.4.1.B. Change control required. Changes in critical materials with respect to ingredients, proportions and manufacturing processes must be considered "new" material and only be permitted after adequate retesting

and recertification including the specific approval of the project and other appropriate review functions. (Ref. 13.4.2.)

24.4.1.C. Criticality awareness important. Employees of SSP contractors, including venders furnishing basic materials and manufacturers working on critical processes, must be made aware of the serious consequences of failure or malfunctioning of criticality category 1 and 1R components through formal awareness programs or comparable activity.

25. Monitoring and Control of Critical Operations

25.1. Problem

Redundancy considerations for monitoring and control of some critical operations were inadequate.

25.2. Causes

25.2.1. Lack of redundancy for monitoring and control of critical operations.

25.2.1.A. Loss of capability to detect potential propellant leaks and fire. Failure of a Hardware Interface Module (HIM) supporting the Main Propulsion System (MPS) ground support equipment propellant loading system caused a 2-hour, 20-minute delay while repairs were made, which resulted in the loss of all fire detection and hazardous gas measurements in the MPS ground support equipment with propellant on board during this time. Loss of this vital capability precluded adequate visibility of potential propellant leaks and fire.

25.2.1.B. Lack of Mission Control Center backup. A similar situation existed at Mission Control Center, Houston (MCC-H) although it was not a consideration in the 51-L incident. It was not considered necessary to have real time backup for MCC-H. There was some facility and equipment backup capability at GSFC but it would have taken days to bring the GSFC Control Center on line. Presumably this was not considered to be a significant risk due to the redundancies in the critical information, monitoring, control and power systems at MCC-H. Nevertheless a recent incident at MCC-H demonstrates its vulnerability. A failure because of a ruptured water line makes the decision not to have real time backup for STS missions questionable.

25.3. Lessons Learned

25.3.1. Monitoring and control of critical operations required. Baseline monitoring and control systems and safety devices used to provide warning and control of critical functions during hazardous and mission operations must be reviewed periodically to verify accepted safety risks attendant with loss of function. Where it is determined that the safety risks or the down-time necessary to replace or repair the systems (or provide suitable backup) are no longer acceptable, redundant systems must be installed.

25.4. Space Station Applications

25.4.1. Monitoring and control of critical operations required. Space Station Program requirements documentation requires subsystem design which will provide redundancy verification, redundancy management, failure propagation avoidance, separation of redundant paths and safe untended operations for long periods of time without monitoring. Baseline monitoring and control systems and safety devices used to provide warning and control of critical functions during hazardous and mission operations must be reviewed periodically to verify accepted safety risks attendant with loss of function. Where it is determined that the safety risks or the down-time necessary to replace or repair the systems (or provide suitable backup) are no longer acceptable, additional redundant systems must be installed.

3.7 Transition

26. Operations Transition

26.1. Problem

The scheduled flight rate did not accurately reflect the capabilities and resources. "...the system was trying to develop its capabilities to meet an operational schedule but was not given the time, opportunity or resources to do it."

26.2. Causes

26.2.1. The lack of capabilities and resources to transition to operational status. The transition from the development phase to the operations phase came suddenly, and in some cases, there was not enough preparation to become operational. Preparation for operational status involved many planned activities to accomplish the transition, including streamlining the processes through automation, standardizing components and centralizing management, all without compromising safety and quality. However, increasing flight rate had priority, only the time and resources left after supporting the flight schedule could be directed towards the preparation activities. Leftover time and resources were inadequate.

26.3. Lessons Learned

26.3.1. Operations transition must be carefully defined. The operational status of high-technology, complex aerospace systems must be carefully defined, planned and implemented to assure that any "residual R&D nature" of the system is considered and that adequate time and resources are made available for transition. (See 17.3.)

26.3.1.A. Specific transition criteria must be established. Systems or programs must have specific criteria established, reviewed, approved and maintained for achieving operational status. SRM&QA must be involved in criteria development and assurance that criteria are being satisfied.

26.3.1.B. Management and its processes must be transitioned. Management processes, systems and procedures which were modified in writing or by practice in transitioning from the NSTS R&D phase to the operations phase should be reviewed to determine the safety risk effects considering 51-L lessons learned. Program plans, procedures and requirements documentation should be revised to incorporate necessary changes.

26.4. Space Station Applications

26.4.1. Operations transition must be carefully defined. Space Station operational status must be carefully defined, planned and implemented to assure that any "residual R&D nature" of the systems are considered and that adequate time and resources are made available for transition.

26.4.1.A. Specific transition criteria must be established. Specific criteria must be established, reviewed, approved and maintained for achieving Space Station operational status. SSP SRM&QA must be involved in criteria development and assurance that criteria are being satisfied.

26.4.1.B. Management and its processes must be transitioned. Space Station management processes including plans, procedures and requirements must be reviewed for transition impact, including increased user requirements, parallel growth development, long-term O&M and logistics requirements, system technology improvements and restructuring of contractor involvement.

3.8 Operations

27. Operations and Maintenance

27.1. Problem

Compliance with the operations and maintenance documentation was inadequate for some flight critical systems.

27.2. Causes

27.2.1. Errors in technical operating procedures. The SSME/MPS orbiter paper work contained a large number of errors. OMIs were in need of review and update.

27.2.2. Improper deviations from approved technical operating procedures. Failure to follow OMIs contributed to damage to a SRM segment and to significant damage to an orbiter payload bay door. At launch all OMRSDs were not met, waived or accepted.

27.3. Lessons Learned

27.3.1. OMD requirements review and update necessary. Requirements placed by the designer (OMRSDs) must be correctly reflected in the pertinent OMIs (or other technical operating procedures) with responsibilities assigned for verification of compliance. Safety must review and approve all OMIs containing critical and hazardous operations. OMRSDs, manufacturer's data and other pertinent information must be part of the review. OMI review and update must be completed prior to any change or modification close-out.

27.3.2. OMD compliance essential. All critical requirements, regardless of source, must be readily traceable through to compliance or non-compliance. All critical open items must be satisfied prior to exposure of personnel or critical flight hardware to risk. Close-out of all open items must require action by Quality or the verifier.

27.4. Space Station Applications

27.4.1. OMD requirements review and update necessary. Early in Space Station development of orbital elements and GSE, there must be concerted effort to develop OMRSDs based on sound engineering principals through critical design reviews and follow-on audits. Subsequent Operational Readiness Reviews must include assurance that these requirements are correctly reflected in the corresponding OMIs or other technical operating procedures with responsibilities assigned for verification of compliance. During or subsequent to these reviews SRM&QA must approve all OMIs containing critical and hazardous operations. OMRSDs, manufacturer's data and other pertinent information must be part of the review. OMI review and update must be completed prior to any change or modification close-out.

27.4.2. OMD compliance essential. All SSP critical requirements, regardless of source, must be readily traceable through to compliance or non-compliance. All critical open items must be satisfied prior to exposure of personnel or critical flight hardware to risk. Close-out of all open items must require action by Quality or the verifier.

28. Operational Constraints

28.1. Problem

Some launch constraints were poorly defined and management of them was deficient. Challenger launched outside of SRM qualification temperatures. The launch of Challenger was allowed to proceed despite the fact the ambient and component temperatures at time of launch were outside the qualification range of the solid rocket motors (i.e., 40 degrees F to 90 degrees F). The coldest point on the right aft field joint was 28 degrees + or - 5 degrees F, at the 300 degree position.

28.2. Causes

28.2.1. Inadequate launch commit criteria. Launch commit criteria did not properly address cold temperature impacts upon SRM performance.

28.2.1.A. SRM not adequately certified. The environment was outside the performance envelope because the SRM had not been adequately certified to meet the induced environmental conditions that are stated in NASA design standards.

28.2.1.B. Lack of understanding design performance limitations. The NASA and contractor management who participated in the decision to launch 51-L did not understand or ignored specific design performance limitations and proceeded to launch without waiving limitations based on a sound technical basis.

28.2.2. Contractor forced into illogical position. NASA and contractor management failed to ensure strict conformance to SRM design and prelaunch temperature specifications. Thiokol management reversed its

position and recommended launching at the urging of MSFC and contrary to the view of its own engineers in order to accommodate a major customer.

28.2.3. Failure to identify hazards of extreme environments. NASA and contractor analyses failed to identify the hazards which would be created on the launch pad because of extreme cold weather. Thus constraints and other mitigation measures were not identified via contingency plans and implemented.

28.3. Lessons Learned

28.3.1 Operational constraints and limit criteria must be clearly established. Imposed constraints and limit criteria (e.g., launch commit criteria) must be clearly defined and traceable to hardware/software specifications ensuring conformance to operational parameters for that hardware/software.

28.3.1.A. Certification testing must consider margins. To establish the operating performance envelopes with reasonable margins and confidence levels, design qualification/certification should require testing to limits beyond established design limits. Limits should be specific for environmental conditions and stress loads that can be encountered during processing, vehicle build up and mission operations.

28.3.1.B. Design performance limits must be recognized. When considering the acceptability of technical requirements for tests, launch or operations, NASA and contractor management must understand the basis for specific design performance limitations and must either conform to the limitations or have a sound technical basis for any deviation or waiver.

28.3.2. Preconceived management decisions must be avoided. NASA and contractor management must avoid even the appearance of forcing the technical community into preconceived management positions.

28.3.3. Extreme environmental hazards must be identified. NASA and contractor analyses of potential hazards must include the effects of extreme environments, both nominal and off-nominal. Necessary constraints and other mitigating measures when can be identified and implemented through approved planning.

28.4. Space Station Applications

28.4.1. Operational constraints and limit criteria must be clearly established. SSP must ensure that imposed constraints and limit criteria are clearly defined and traceable to hardware/software specifications requiring conformance to operational parameters for that hardware/software.

28.4.1.A. Certification testing must consider margins. To establish the operating performance envelopes with reasonable margins and confidence levels, SSP documentation should be reviewed and updated to require, whenever feasible, that design qualification/certification testing to limits be done beyond established design limits. Limits should be specific for environmental conditions and stress loads that can be encountered during preparations for launch of Station elements, on-orbit assembly and mission operations.

28.4.1.B. Design performance limits must be recognized. When considering the acceptability of technical requirements for tests or on-orbit operations, Space Station Program and contractor management must understand the basis for specific design performance limitations and must either conform to the limitations or have a sound technical basis for any deviation or waiver.

28.4.2. Preconceived management decisions must be avoided. SSP policy guidance must be maintained to ensure that program and contractor management avoid even the appearance of forcing the technical community into preconceived management positions. Current and planned SSP documentation should be reviewed for this guidance and any deficiencies corrected.

28.4.3. Extreme environmental hazards must be identified early in the program. To ensure that system and component design is compatible with the anticipated environment early in the Space Station program, requirements documents must be carefully prepared to include complete and accurate environmental operating parameters.

29. Work Force Performance

29.1. Problem

Performance of some of the work force was substandard and unmotivated.

29.2. Causes

29.2.1. Management failure to motivate personal commitment. A lack of personal commitment to and identification with the NSTS Program was found during interviews. Management failed to maintain a high degree of motivation for excellence with many individuals working on the NSTS Program.

29.2.1.A. Lack of confidence in forgiveness policy. Orbiter technicians cited examples of employees being punished after acknowledging they had accidentally caused some damage. Inconsistent reporting occurred because of lack of confidence in the company's forgiveness policy and technicians' consequent fear of losing their jobs.

29.2.1.B. Assembly procedure violation. An SRB segment was used in violation of the assembly procedure, which might have, but was judged not to have, directly contributed to the failure.

29.2.1.C. Careless mistakes and quality inspections. There is evidence that careless mistakes are still being made in workmanship in NSTS processing and not all required quality checks are being made.

29.2.1.D. Lack of program team spirit. Personnel involved with the NSTS primarily identify with their own organization, element, project or function rather than with the program as a whole.

29.2.1.E. Frustrated safety personnel. Many safety personnel involved with the NSTS are frustrated and lack motivation for strong, dedicated commitment to the mission.

29.3 Lessons Learned

29.3.1. Work force motivation required. NASA and its contractors must maintain emphasis on well-coordinated personal and team motivation programs. A team spirit and pride of accomplishment must be infused in the programs by whatever extraordinary means is necessary.

29.3.1.A. Work error forgiveness policies must be maintained. The fear that punishment will result from an employee reporting a problem, as well as all other obstacles to proper problem reporting, must be minimized. NASA must encourage its contractors to devise effective policies for forgiving or mitigating truly accidental damage. All operations and assurance personnel must understand that their contributions are vital to a safe and successful program. Problem reporting and good procedural discipline must be rewarded.

29.3.1.B. Close monitoring and control of critical operations required. NASA and contractor quality and safety personnel must oversee and monitor operations closely to ensure that procedures are not violated. Procedures pertaining to critical hardware operations must be followed or appropriate procedures or assembly operations must be officially changed. Stringent surveillance/verification over critical operations must be maintained. Personnel charged with the responsibility to accomplish critical operations must be provided sufficient information to be able to understand the potential consequences of deviations from procedural safeguards.

29.4. Space Station Applications

29.4.1. Work force motivation is required. SSP requirements documentation specifies that product-oriented motivation (awareness) activity shall be implemented as an integral part of and making maximum use of existing motivational activities, the objective being to prevent human error by instilling in personnel an awareness of personal responsibility for Space Station mission success. SSP management and contractors must maintain this emphasis on personal and team motivation programs. A team spirit and pride of accomplishment must be maintained. SRM&QA must include this important aspect of work performance during safety audits.

29.4.1.A. Work error forgiveness policies must be maintained. The fear that punishment will result from an employee reporting a problem, as well as all other obstacles to proper problem reporting, must be minimized. SSP management must encourage/require contractors to devise effective policies for forgiving or mitigating truly accidental damage. All operations and assurance personnel must understand that their

contributions are vital to a safe and successful program. Problem reporting and good procedural discipline must be rewarded.

29.4.1.B. Close monitoring and control of critical operations required. Program and contractor quality and safety personnel must oversee and monitor operations closely to ensure that procedures are not violated. Procedures pertaining to critical hardware operations must be followed or appropriate procedures or assembly operations be officially changed. Stringent surveillance/verification over critical operations must be maintained. Personnel charged with the responsibility to accomplish critical operations must be provided sufficient information to be able to understand the potential consequences of deviations from procedural safeguards.

Appendix A – References

Supporting references are keyed to corresponding paragraph numbers in the text. Primary document references are listed below.

Study Source Documents from Figure 1-1

Ref. 1 Report of the Presidential Commission on the Space Shuttle Challenger Accident, June 6, 1987, Volume I.

Ref. 2 Investigation of the Challenger Accident, Report of the Committee on Science and Technology, House of Representatives, Ninety-ninth Congress, October 29, 1987.

Ref. 3 Lessons Learned Report, STS 51-L Data and Design Analysis Task Force, NASA, June 1986.

Ref. 4 Final Report of the STS Safety Risk Assessment Ad Hoc Committee, SRM&QA, NASA, August 1987.

Related Reference Documents from Figure 1-2

Ref. 5 STS Management and Communications Study, NASA, August 1986.

Ref. 6 SRM&QA Organization Task Team Review Report, Office of AA/SRM&QA, September 1986.

Ref. 7 Lessons Learned: An Experience Data Base for Space Design, Test and Flight Operations, Aerospace Safety Advisory Panel, November 1986.

Ref. 8 Response to Recommendations of the House of Representatives Committee on Science and Technology Report of the Investigation of the Challenger Accident, NASA, February 1987.

Ref. 9 Report to the President, Implementation of Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident, NASA, June 1987.

1. Safety Emphasis

1.2.1.	Ref. 4, Section IV, pp 12-16
1.2.2.	Ref. 2, p 4
	Ref. 4, Section IV, pp 12–16
1.2.2.A.	Ref. 1, pp 154-155
1.2.2.B.	Ref. 1, p 155
1.2.2.C.	Ref. 4, p 44
1.2.2.D.	Ref. 2, p 20
	Ref. 4, p 42
1.2.3.	Ref. 2, p 9
	Ref. 4, p 15

2. Assurance Reviews

2.2.1.	Ref. 1, pp 155, 161
2.2.2.	Ref. 1, pp 154-155

3. Authority and Responsibility

3.2.1.	Ref. 1, p 153
	Ref. 2, p 29
	Ref. 4, pp 18, 34
3.2.1.A.	Ref. 4, pp 18, 30
3.2.1.B.	Ref. 1, p 153
	Ref. 4, p 30
3.2.1.C.	Ref. 4, pp 18, 45
3.2.1.D.	Ref. 1, p 156 - inferred
3.2.2.	Ref. 4, pp 18, 22
3.2.2.A.	Ref. 1, p 153
3.2.2.B.	Ref. 1, p 153
3.2.2.C.	Ref. 4, p 22
3.2.2.D.	Ref. 4, p 30

4. SRM&QA Resources

4.1.	Ref. 1, p 199, Rec. IV
4.2.1.	Ref. 1, pp 152, 160-161, findings 1 and 5
4.2.1.A.	Ref. 2, p 176, findings 1 and 2
	Ref. 4, p 29
4.2.1.B.	Ref. 1, p 161
	Ref. 2, pp 22, 31, finding 1; 132
4.2.1.C.	Ref. 1, pp 154, 155
	Ref. 2, p 11
4.2.2.	Ref. 4, p 18

4.2.2.A.	Ref. 1, p 152
4.2.2.B.	Ref. 1, p 156 Ref. 2, p 9
4.2.3.	Ref. 1, p 152
4.2.4.	Ref. 1, pp 156-159 Ref. 4, pp 47-48

5. Deviation and Waiver Management

5.2.1.	Ref. 1, pp 95, 104, findings 1 and 3, 156
5.2.1.A.	Ref. 1, p 104, finding 2 Ref. 4, pp 10, 51, 52
5.2.1.B.	Ref. 1, pp 148, finding 3, 160 Ref. 2, pp 25, 214
5.2.1.C.	Ref. 1, pp 117-118, 148, finding 4 Ref. 2, p 25 Ref. 4, p 44
5.2.1.D.	Ref. 1, pp 155-156 Ref. 2, p 11
5.2.2.	Ref. 1, pp 95, 104, 114-117 Ref. 2, p 122

6. Management Performance

6.2.1.	Ref. 4, p 40
6.2.2.	Ref. 2, p 22
6.2.3.	Ref. 1, pp 170, 171
6.2.4.	Ref. 2, p 20
6.2.5.	Ref. 1, p 194
6.2.6.	Ref. 1, p 199, Rec. IIb
6.2.7.	Ref. 1, p 199, Rec. IIa
6.2.7.A.	Ref. 4, p 30
6.2.7.B.	Ref. 4, p 15
6.4.1	JSC 30000, Sec. 9, para. 1.5 [Jan. 15, 1987]
6.4.7	JSC 30000, Sec. 9 [Jan. 15, 1987]
6.4.7	JSC 30000, Sec. 9 [Jan. 15, 1987]

7. Program Critical Knowledge

7.1.	Ref. 1, p 135 Ref. 2, pp 4-5
7.2.1.	Ref. 2, p 5
7.2.1.A.	Ref. 2, p 4
7.2.2.	NASA Management Instruction, Mishap Reporting and Investigation, NMI 8610.1E NASA Handbook, Guidelines for Mishap Investigations, NHB 1700.1 (V2)
7.4.	SSP PSC RFP, SOW para. 5.4.1.5

8. Safety Risk Assessment

8.2.1.	Ref. 4, pp 12-13
8.2.1.A.	Ref. 4, pp 12-13
8.2.1.B.	Ref. 4, p 13
8.2.2.	Ref. 4, pp 12-13
8.2.3.	Ref. 2, p 25 Ref. 4, p 13
8.2.3.A.	Ref. 1, p 153
8.2.3.B.	Ref. 4, Section VI, pp 33-37
8.2.3.C.	Ref. 1, pp 155-158
8.2.4.	Ref. 4, p 48

9. Problem Resolution

9.2.1.	Ref. 1, pp 152, 156, 158, 161 finding 6
9.2.2.	Ref. 1, p 153 Ref. 2, pp 56-57, 172 discussion
9.2.3.	Ref. 1, pp 152, 156, 161, finding 4 Ref. 2, pp 56-57, 70
9.2.4.	Ref. 2, pp 70, 216-217
9.2.5.	Ref. 1, p 192 Ref. 3, P-4, p 17
9.2.6.	Ref. 1, pp 152-153 Ref. 2, pp 56-57, 172 discussion Ref. 4, p 37, Rec. VI.3.g
9.3.1.	Ref. 1, pp 152-153 Ref. 4, p 37, Rec.VI.3.g
9.3.2.	Ref. 4, p 37, Rec.VI.3.h
9.3.3.	Ref. 1, p 198, Rec. Ia
9.4.1	JSC 30000, Sec. 3, para. 2.1.11.[Jan. 15, 1987] SSP PSC RFP, p 364, SOW para. 7.1.5.1
9.4.2.	Ref 4, p 37, Rec. VI.3.h
9.4.3.	JSC 30000, Sec. 9, para. 1.8 [Jan. 15, 1987] SSP PSC RFP, p 364, SOW para. 7.1.5.2
9.4.4.	SSP PSC RFP, p 364, SOW para. 7.1.5.1
9.4.5.	SSP PSC RFP, p 362, SOW para. 7.1.4.6
9.4.6.	JSC 30000, Sec. 9, para. 2.4.1, 2.4.2 [Jan. 15, 1987]

10. Trend Analysis

10.1	Ref. 1, pp 71,145-146, 155-156, 159, 161, finding 4 Ref. 2, p 138
10.2.1.B.	Ref. 1, pp 65-66, 155
10.2.1.C.	Ref. 1, p 145
10.2.2.	Ref. 1, p 148, finding 5, 159 Ref. 3, P-4, p 17
10.3.1.	Ref. 4, pp 45-46, Rec. IX.3.d

11. Flight Readiness Reviews

11.2.1	Ref. 1, p 85 Ref. 2, p 69

	Ref. 3, P-4, p 17
11.2.1.A.	Ref. 1, p 200, Rec. V
	Ref. 2, p 53
	Ref. 3, P-2, p 14
11.2.1.B.	Ref. 2, p 69
11.2.1.C.	Ref. 2, p 26
11.2.2.	Ref. 1, pp 82, 200, Rec. V
	Ref. 2, pp 53, 69-70
11.2.2.A	Ref. 2, p 71
11.2.2.B	Ref. 2, p 70
11.2.2.C	Ref. 2, p 11
11.4.3	JSC 30000, Sec. 9, para. 2.1.4 [Jan. 15, 1987]
11.4.3	JSC 30000, Sec. 9, para. 2.1.4 [Jan. 15, 1987]

12. Assurance Information System

12.2.1.	Ref. 3, A-11, p 35
12.2.2.	Ref. 4, pp 57-58, Rec. XIII.3.a
12.2.3.	Ref. 2, p 171 Issue 2

13. Engineering Change Process

13.1.	Ref. 2, pp 28, 161-165, 171
13.2.1.	Ref. 2, p 161 Issue 1, finding l
13.2.2.	Ref. 2, p 162, Issue 2, 165
13.4.1.	JSC 30000, Sec. 9, para. 2.2.10 [Jan. 15, 1987]
13.4.2.	JSC 30000, Sec. 9, para. 2.2.10 [Jan. 15, 1987]

14. Crew Safety

14.2.1.	Ref. 1, pp 180, 200, Rec. VII
	Ref. 3, M-4, p 41
14.4.1	JSC 30000, Sec. 3 [Jan. 15, 1987]

15. Contract Safety Requirements

15.2.1.	Ref. 2, p 32, finding 1, 33, finding 2
	Ref. 4, p 54
15.2.1.A.	Ref. 1, p 195
	Ref. 2, p 180, Discussion, Rec. 1
	Ref. 4, p 54
15.2.1.B.	Ref. 4, pp 53-54

16. Contractor Selection Emphasis

16.1.	Ref. 2, pp 51-52, 255-259
16.2.1.	Ref. 1, pp 120-121

17. Schedule Pressures

17.2.1.	Ref. 2, pp 22, 119, 122
17.2.1.A.	Ref. 1, p 164
	Ref. 2, p 119
17.2.1.B.	Ref. 1, p 164
	Ref. 2, p 22
17.2.2.	Ref. 1, pp 167, 176
	Ref. 2, pp 22, 122
	Ref. 3, D-6, p 9
17.2.2.B.	Ref. 1, pp 64, 171, 177, 201, Rec. VIII
17.2.2.C.	Ref. 1, p 176
	Ref. 2, pp 21, 116
	Ref. 3, P-1, p 13
17.2.2.D.	Ref. 3, P-6, p 19
17.2.2.E.	Ref. 1, p 200, Rec. VI
17.3.1.	Ref. 1, p 201, Rec. VIII
	Ref. 3, M-1, p 38
17.3.2.	Ref. 1, p 171

18. Critical Redesign

18.2.1.	Ref. 1, p 192
	Ref. 2, p 9, Issue 1, finding 2
	Ref. 3, A-2, p 25
18.2.1.A.	Ref. 1, p 148
18.2.1.B.	Ref. 1, p 192

19. Environmental and Performance Specifications

19.2.1.	Ref. 1, pp 95, 98
19.2.1.A.	Ref. 3, A-1, p 24
19.2.1.B.	Ref. 1, p 98
19.2.1.C.	Ref. 2, p 50, discussion 1
19.2.1.D.	Ref. 2, p 50, discussion 2
19.2.1.E.	Ref. 2, p 63

20. Critical Item Tolerances and Margins

20.2.1.	Ref. 1, p 70, finding 5
	Ref. 2, p 19
	Ref. 3, A-8, p 32
20.2.1.A.	Ref. 1, pp 70-73
20.2.1.B.	Ref. 1, p 159
	Ref. 2, p 26, finding 2
20.2.1.C.	Ref. 1, p 70, finding 5
20.2.2.	Ref. 1, p 156

21. Test Specifications

21.2.2.	Ref. 1, pp 95, 192
	Ref. 2, p 9, finding 2, 61, finding 2, pp 250-251
21.3.1.	Ref. 2, p 10 Rec. 1, 61 Rec. 1

22. Design Characterization and Test Verification

22.2.1.	Ref. 1, pp 64, 70, 71
	Ref. 3, D-4, A-1, A-4, pp 7,24, 28
22.2.1.A.	Ref. 1, pp 60, 64, 65
22.3.1.	Ref. 2, p 9, Rec. 1

23. Qualification Testing

23.2.1.	Ref. 1, p 148 finding 1
	Ref. 2, p 50 discussion 1
23.2.1.A.	Ref. 1, p 148, finding 1
	Ref. 2, p 50 discussion 1

	Ref. 3, D-3, A-1, pp 6, 24
23.2.1.B.	Ref. 1, p 148, findings 1 and 2, 192
	Ref. 3, D-1, D-5, pp 4, 8
23.3.1.	Ref. 3, D-1, p 4

24. Critical Process Control

24.1.1.	Ref. 2, p 9
24.2.1.	Ref. 2, p 18
24.2.1.A.	Ref. 1, p 125
	Ref. 2, p 62
24.2.1.B.	Ref. 2, p 62
24.2.1.C.	Ref. 2, p 62
	Ref. 3, A-7, p 31
24.3.1.A.	Ref. 2, p 18

25. Monitoring and Control of Critical Operations

25.2.1.A.	Ref. 3, A-5, p 29
25.2.1.B.	Ref. 4, p 50
25.4.1	JSC 30000, Sec. 3, para. 2.1.10.B [Jan. 15, 1987]

26. Operations Transition

26.2.1.	Ref. 1, p 170

27. Operations and Maintenance

27.2.1	Ref. 1, p 193
27.2.2.	Ref. 2, p 21
27.3.1.	Ref. 1, pp 193, 219-220
27.3.2.	Ref. 1, pp 192, 219-220
	Ref. 2, p 21

28. Operational Constraints

28.1.1.	Ref. 2, p 11
28.2.1.	Ref. 2, p 11
28.2.1.A.	Ref. 3, D-1, p 4
28.2.1.B.	Ref. 1, p 156
28.2.2.	Ref. 1, p 104
28.2.3.	Ref. 1, p 117
	Ref. 2, p 11

29. Work Force Performance

29.2.1.	Ref. 4, p 40
29.2.1.A.	Ref. 1, p 194
29.2.1.B.	Ref. 2, p 67
29.2.1.C.	Ref. 4, p 41
29.2.1.D.	Ref. 4, p 40
29.2.1.E.	Ref. 4, p 42
	JSC 30000, Sec. 9, para. 1.5 [Jan. 15, 1987]

Appendix B – Reference Matrices

Matrices are provided in this appendix to show interrelationships between lessons learned of this report and traceability to study source documents:

- Figure B-1. Lessons Learned Cross Reference Matrix
- Figure B-2. Study Source Reference Matrix
- Figure B-3. Commission Report Recommendation Matrix
- Figure B-4. House Report Recommendation Matrix
- Figure B-5. Crippen Report Recommendation Matrix
- Figure B-6. McDevitt Report Recommendation Matrix

B-2

B-3

B-4

B-5

B-6

B-7

B-8

B-9

B-10

B-11

B-12

B-13

Appendix C – Acronyms

AA	Associate Administrator
ASAP	Aerospace Safety Advisory Panel
CDR	Critical Design Review
CIL	Critical Items List
Code S	Office of Space Station, NASA Headquarters
Code Q	Office of SRM&QA, NASA Headquarters
Code QS	Safety Division, NASA Headquarters
EIFA	Element Interface Functional Analysis
ELV	Expendable Launch Vehicle
ET	External Tank
EVA	Extravehicular Activity
F	Fahrenheit
FMEA	Failure Modes and Effects Analysis
FRR	Flight Readiness Review
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HIM	Hardware Interface Module
JSC	Lyndon B. Johnson Space Center
KSC	John F. Kennedy Space Center
LC	Launch Complex
LH2	Liquid Hydrogen
MCC-H	Mission Control Center-Houston
MPS	Main Propulsion System
MSAR	Mission Safety Assessment Report
MSFC	George C. Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NDE	Non-destructive Evaluation
NHB	NASA Handbook
NMI	NASA Management Instruction
NSTS	National Space Transportation System
O&M	Operations and Maintenance
OMD	Operations and Maintenance Documentation
OMI	Operations and Maintenance Instruction
OMRSD	O&M Requirements and Specification Documentation
OMV	Orbital Maneuvering Vehicle
ORR	Operational Readiness Review
PDRD	Program Definition and Requirements Document (Level II SSP)
PERT	Program Evaluation Review Technique
POP	Program Operating Plan
PRACA	Problem Reporting and Corrective Action
PRD	Program Requirements Document (Level I SSP)
R&D	Research and Development
SEB	Source Evaluation Board
SPC	Shuttle Processing Contract
SR&QA	Safety, Reliability and Quality Assurance
SRB	Solid Rocket Booster
SRM	Solid Rocket Motor
SRM&QA	Safety, Reliability, Maintainability and Quality Assurance
SSME	Space Shuttle Main Engine
SSP	Space Station Program
SSPO	Space Station Program Office

STS Space Transportation System