



Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management

Committee on Shuttle Criticality Review and Hazard Analysis Audit, Space Applications Board, Commission on Engineering and Technical Systems, National Research Council

ISBN: 0-309-54234-0, 154 pages, 8 1/2 x 11, (1988)

This free PDF was downloaded from:

<http://www.nap.edu/catalog/10616.html>

Visit the [National Academies Press](http://www.nap.edu) online, the authoritative source for all books from the [National Academy of Sciences](http://www.nap.edu), the [National Academy of Engineering](http://www.nap.edu), the [Institute of Medicine](http://www.nap.edu), and the [National Research Council](http://www.nap.edu):

- Download hundreds of free books in PDF
- Read thousands of books online, free
- Sign up to be notified when new books are published
- Purchase printed books
- Purchase PDFs
- Explore with our innovative research tools

Thank you for downloading this free PDF. If you have comments, questions or just want more information about the books published by the National Academies Press, you may contact our customer service department toll-free at 888-624-8373, [visit us online](http://www.nap.edu), or send an email to comments@nap.edu.

This free book plus thousands more books are available at <http://www.nap.edu>.

Copyright © National Academy of Sciences. Permission is granted for this material to be shared for noncommercial, educational purposes, provided that this notice appears on the reproduced materials, the Web address of the online, full authoritative version is retained, and copies are not altered. To disseminate otherwise or to republish requires written permission from the National Academies Press.

Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management

Prepared by the
Committee on Shuttle Criticality
Review and Hazard Analysis Audit

of the
Aeronautics and Space Engineering Board

with staff support from the
Space Applications Board
Commission on Engineering and Technical Systems
National Research Council

NATIONAL ACADEMY PRESS
January 1988

ONPI ARCHIVES

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Frank Press is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Robert M. White is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of

appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Samuel O. Thier is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Frank Press and Dr. Robert M. White are chairman and vice chairman, respectively, of the National Research Council.

This study was conducted under Contract No. NASW-4003 between the National Academy of Sciences and the National Aeronautics and Space Administration.

Available from:

Aeronautics and Space Engineering Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418.

Printed in the United States of America

COMMITTEE ON SHUTTLE CRITICALITY REVIEW AND HAZARD ANALYSIS AUDIT

ALTON D. SLAY, Gen., (USAF, Retired), Slay Enterprises, Inc., McLean, VA (former Commander, USAF Systems Command), *Chairman*

GERARD W. ELVERUM, JR., Vice President and General Manager, Applied Technology Division, TRW, Inc., Redondo Beach, CA.

B. JOHN GARRICK, President, Pickard, Lowe and Garrick, Newport Beach, CA (from September 22, 1986 to February 19, 1987)

GRANT L. HANSEN, retired Vice President, Systems Development Corporation, San Diego, CA

WILLIS M. HAWKINS, Senior Advisor, Lockheed Corporation (former Senior Vice President), Calabasas, CA

I. GRANT HEDRICK, Senior Management Consultant, Grumman Corporation (former Senior Vice President), Bethpage, NY

BRUCE HOADLEY, Division Manager, Analytical Methods and Software Systems, Bell Communications Research, Redbank, NJ

WILLIAM B. LENOIR, Principal, Space Systems Practice, Booz-Allen & Hamilton (former astronaut), Bethesda, MD

ARTUR MAGER, Consultant (retired Group Vice President, The Aerospace Corporation), Los Angeles, CA

NORMAN R. PARMET, retired Vice President-Engineering & Quality Assurance, Trans World Airlines, Fairway, KS

ROBERT E. UHRIG, Distinguished Professor of Engineering, Department of Nuclear Engineering, University of Tennessee, Knoxville, TN

JAMES J. KRAMER, Manager, Advanced Technical Programs, General Electric Company, Washington, DC (Ex Officio Member, Chairman, Aeronautics and Space Engineering Board)

Staff

David S. Johnson, Study Director

Robert H. Korkegi, Director, Aeronautics and Space Engineering Board

William H. Michael, Jr., Director, Space Applications Board

Courtland S. Lewis, Consultant

Vki Marrero, Administrative Assistant

Amy Janik, Administrative Secretary

PREFACE

The President of the United States approved the Space Shuttle program in 1972, to become the heart of the National Space Transportation System (NSTS) and provide routine, economical access to space. The launch of Columbia in 1981—the first reusable vehicle to be launched and orbit the earth—opened a new era. The development of the Space Shuttle and its operation and maintenance have involved several National Aeronautics and Space Administration (NASA) centers, their industrial prime contractors, and scores of subcontractors, including tens of thousands of people. This must be considered one of the most complex technical undertakings of all time.

After 24 successful Shuttle flights, the Space Shuttle Challenger accident of January 28, 1986, stunned the entire nation and indeed the world. In response to the accident President Reagan established the Presidential Commission on the Space Shuttle Challenger Accident (frequently called the Rogers Commission, after its chairman) to investigate the accident and make recommendations for the safe recovery of the Space Transportation System (STS). Among its recommendations, the Rogers Commission called upon NASA to review certain aspects of its STS risk assessment effort and to “identify those items that must be improved prior to flight to ensure mission success and flight safety.”* It further recommended that an audit panel be appointed by the National Research Council (NRC) to verify the adequacy of the effort and report directly to the Administrator of NASA. The Committee on Shuttle Criticality Review and Hazard Analysis Audit was established in response to the recommendation. Beginning with the Committee’s first meeting on September 22, 1986, this report is the culmination of 14 months of investigation, study, and deliberation.

While the Committee recognizes that it is not possible, a priori, to *guarantee* mission success and flight safety, we hope the Committee’s conclusions and recommendations will assist NASA in taking those prudent additional steps which will provide a reasonable and responsible level of flight safety for the Space Shuttle. As the Challenger accident made painfully obvious, no probe into space is

routine, and the Space Shuttle is still a developmental vehicle. The risks of space flight must be accepted by those who are asked to participate in each flight as well as by those who are responsible to the nation for achieving its goals in space. Such risks should also be recognized by Executive Branch officials and Congress in their review and oversight of NASA endeavors.

The Committee has been favorably impressed by the dedicated effort and beneficial results obtained thus far by NASA and its contractors from the STS risk assessment and risk management system. The Committee is also gratified by the progress NASA is making in strengthening this system. We appreciate the close collaboration the Committee had with NASA and contractor personnel, the interest they showed, and their responsiveness to the Committee’s suggestions. Nevertheless, although our general impressions are favorable, we do have suggestions for improvement. It is against this background that the recommendations in this report should be judged.

The Committee recognizes that the NSTS risk assessment and risk management activities, both existing and with the modifications proposed here, are large and complex. This means that change should be introduced with care. A systematic examination of the entire set of processes supporting risk assessment and management in order to optimize the total ensemble may be appropriate. Such an examination may be particularly useful in conjunction with implementation of a new program such as the Space Station.

Although this report and its recommendations are directed to the NSTS Program, they are of broader applicability. It certainly would be wise to consider the lessons learned when structuring any risk assessment and management system for other programs having attributes similar to the NSTS Program, such as the Space Station Program. It, too, is a large program involving highly complex technology which requires the major participation of several NASA centers and prime contractors for its execution.

Acknowledgments

In conducting its work, the full Committee met an average of once a month for over a year, and individual and groups of members conducted ad-

* Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident, William P. Rogers, Chairman (June 1986).

ditional site visits, research, and writing on behalf of the Committee. This intense dedication and the resulting contributions of the highly competent members of the Committee are acknowledged with great appreciation. I also would like to express the Committee's appreciation for the excellent support of the National Research Council staff in all aspects of its work. While this report represents the contributions by and deliberations of all members of the Committee, I would especially like to note the contributions to its writing by David S. Johnson and Courtland S. Lewis. Mr. Johnson, in particular, was extraordinarily effective as Study Director. His organizational skills, technical knowledge, and hard work were central to our effectiveness as a committee. The peer review by the National Research

Council also made a key contribution to the quality of our reports.

In closing, we wish to thank the many NASA and contractor employees who facilitated the work of the Committee, often extending their already heavy workloads in the aftermath of the Challenger accident. Of special note was the assistance provided during the study by the two NASA liaison persons, E. William Land, Jr. and Charles S. Harlan.

Alton D. Slay
Chairman,
Committee on Shuttle Criticality
Review and Hazard Analysis Audit

Contents

	<i>Page</i>
1. EXECUTIVE SUMMARY	1
1.1 NASA's Safety Policy and Process	1
1.2 The Committee's View	3
1.3 Findings and Recommendations	4
1.4 Closing Remarks	9
2. INTRODUCTION	10
2.1 Purpose of Study	10
2.2 Study Approach	10
2.2.1 Interpretation of Task	10
2.2.2 Plan and Structure	11
2.2.3 Meetings and Site Visits	12
2.2.4 Interim Reports of the Committee	12
2.3 Organization of the Report	13
3. NASA'S SAFETY PROCESS FOR THE NATIONAL SPACE TRANSPORTATION SYSTEM PROGRAM	15
3.1 Policy on Safety	15
3.2 Management Structure	16
3.2.1 Program Management	16
3.2.2 Review Boards	17
3.3 Organizational Roles	17
3.3.1 Engineering Project Offices	17
3.3.2 Safety, Reliability, Maintainability, and Quality Assurance	17
3.3.3 Engineering Integration Office	19
3.4 Safety Analyses	20
3.4.1 The Failure Modes and Effects Analysis and Critical Items List	20
3.4.2 Hazard Analysis	22
3.4.3 Element Interface Functional Analysis	23
3.4.4 Other Analyses	23
3.4.5 Overall Scope of Analyses	25
3.5 Post-51L Reevaluation/Review	29
3.5.1 NASA Management Directives	29
3.5.2 Process	29
3.5.3 Relation to Engineering Redesign Activity	31
3.5.4 Relation to Flight Readiness Process	31
3.5.5 Data Input and Output	32

	<i>Page</i>
4. RISK ASSESSMENT AND RISK MANAGEMENT: THE COMMITTEE'S VIEW	33
4.1 General Concept	33
4.2 NASA's Process: Overall Comments	34
4.2.1 NASA Risk Assessment	34
4.2.2 NASA Risk Management	37
4.3 Summary	37
5. SPACE TRANSPORTATION SYSTEM RISK ASSESSMENT AND RISK MANAGEMENT: DISCUSSION AND RECOMMENDATIONS	40
5.1 Critical Items List Retention Rationale Review and Waiver Process	40
5.2 Critical Items List Prioritization and Disposition	45
5.3 Hazard Analysis and Mission Safety Assessment	47
5.4 Relationship of Formal Risk Assessment Process to Space Transportation System Engineering Changes	51
5.5 Timely Feedback of Data into the Risk Assessment and Management Processes	52
5.6 The Need for Quantitative Measures of Risk	55
5.7 The Need for Integrated Space Transportation System Engineering Analysis in Support of Risk Management	57
5.8 Independence of the Space Transportation System Certification and Software Validation and Verification Program	59
5.9 Operational Issues	63
5.9.1 Launch Commit Criteria Waiver Policy	63
5.9.2 Human Factors as a Contributor to Risk	64
5.9.3 Cannibalization of Spare Parts	65
5.10 Other Weaknesses in Risk Assessment and Management	68
5.10.1 The Apparent Reliance on Boards and Panels for Decision Making	68
5.10.2 Adequacy of Orbiter Structural Safety Margins	70
5.10.3 Software Issues	71
5.10.4 Differences in Procedures among NASA Centers	72
5.10.5 Use of Non-Destructive Evaluation Techniques	73
5.11 Focus on Risk Management	74
6. LESSONS LEARNED	79
6.1 Elements of and Responsibilities for Risk Assessment and Risk Management	79
6.2 Establishment of Responsibility for Program Direction and Integration	80
6.3 The Need for Quantitative Measures of Relative Risk	81
6.4 The Need for Integrated Review and Overview in the Assessment of Risk, and in Independent Evaluation of Retention Rationale	81
6.5 Independence of the Certification of Flight Hardware and of Software Validation and Verification	81
6.6 Safety Margins for Flight Structures	81
6.7 Other	81

APPENDICES:		<i>Page</i>
A	Acronyms and Definitions	83
B	Establishing Reports and Documents	87
C	Letter Reports to the Administrator of NASA and NASA Response	97
D	Probabilistic Risk Assessment	115
E	An Improved Critical Item Risk Assessment Procedure for the National Space Transportation System	125
F	Description of Proposed Systems Safety Engineering Functions in Support of the National Space Transportation System Risk Assessment and Risk Management	139

1 Executive Summary

The Shuttle Criticality Review and Hazard Analysis Audit Committee (SCRHAAC) was formed by the National Research Council (NRC), at the request of the National Aeronautics and Space Administration (NASA), in response to a recommendation of the Presidential Commission on the Space Shuttle Challenger Accident (also known as the Rogers Commission). That Commission had recommended that NASA review and evaluate certain aspects of its process for ensuring the safety of the National Space Transportation System (NSTS), and that an NRC panel be appointed to audit the NASA review effort and verify its adequacy.

The Committee monitored the overall NASA review and evaluation effort while performing detailed on-site reviews of its implementation for selected elements and subsystems¹ (e.g., the Space Shuttle Main Engine, Solid Rocket Booster, Auxiliary Power Unit). As areas of particular concern emerged, such as software issues, the adequacy of Orbiter structural margins, integrated Space Transportation System (STS) analysis in support of risk assessment, and Orbiter steering on landing, the Committee pursued those concerns in greater detail. Various operational issues affecting Shuttle safety (e.g., the application of Launch Commit Criteria and the “cannibalization” of spare parts) were also examined. Each of these audits was conducted through a series of meetings with NASA and contractor personnel on-site at the contractor facilities and NASA centers, and by reviewing available documentation. In addition, two NASA liaison persons provided direct input on questions raised

by the Committee on an ongoing basis and provided substantial reports on certain points of concern.

The Committee appreciates that NASA has accomplished the design, development, verification, and certification of the STS utilizing a management approach and procedures that have been, in large part, most successful. The Committee also recognizes that the risk assessment and management recommendations made in this report will only be useful if they are introduced in rational, practical stages. The Committee believes, however, that the safety of continuing operations of the STS can be improved by creating an integrated risk assessment and management program which builds on the largely qualitative methods used previously. The totality of the recommendations, once such a system is implemented, should be extremely valuable in the accomplishment of the NSTS Program in the future, and should serve as a prototype for similar programs in NASA as well.

During the course of its work, the Committee produced two interim progress reports to the Administrator of NASA in which more than a dozen recommendations and suggestions were made. Some of the concerns expressed in the interim reports have been resolved since the reports were presented; others remain at issue. All of the concerns identified in those reports are reflected in the Findings and Recommendations summarized in Section 1.3.

1.1. NASA'S SAFETY POLICY AND PROCESS

NASA policy regarding safety is established by the Administrator; its essence (as stated in NASA Policy Directive 1701.1) is to:

- “a. Avoid loss of life, injury of personnel, damage and property loss.

¹ There are four major flight “elements” in the Space Shuttle (Orbiter, Space Shuttle Main Engines, Solid Rocket Boosters, and External Tank), each of which is composed of several subsystems.

- "b. Instill a safety awareness in all NASA employees and contractors.
- "c. Assure that an organized and systematic approach is utilized to identify safety hazards and that safety is fully considered from conception to completion of all agency activities.
- "d. Review and evaluate plans, systems, and activities related to establishing and meeting safety requirements both by contractors and by NASA installations to ensure that desired objectives are effectively achieved."

Every manager throughout the organization is responsible for systematically identifying risks, hazards, or unsafe situations or practices, and for taking steps to assure adequate safety in the activities and products under his supervision. Out of this broad policy framework are derived the more specific safety requirements that are implemented in successively greater detail down through Headquarters, program, and project organizations at the NASA centers and contractors. **The Committee finds that the basic documents setting forth these policies are complete and do establish a firm foundation for the NASA-wide safety program.**

Central to NASA's analyses to ensure reliability of the Shuttle system is the Failure Modes and Effects Analysis (FMEA). FMEAs are performed on all STS flight hardware as well as Ground Support Equipment (GSE) which interfaces with flight hardware at the launch sites to identify hardware items that are critical to the performance and safety of the vehicle and the mission, and to identify items that do not meet design requirements. Each possible failure mode is identified and then analyzed to determine the resulting performance of the system and to ascertain the *worst-case* effect that could result from a failure in that mode. All the identified "critical items" are then categorized according to the worst-case effect of the failure on the crew, the vehicle, and the mission. If the worst-case effect is loss of life or vehicle, the item is categorized as Criticality 1 (1R if there are redundant units, and 1S if it would result from the failure of a piece of ground support equipment). In the same manner, Criticality 2 and 2R are cases where loss of mission could result.

The result of this classification is a "Critical Items List" (CIL) which includes for each item the rationale for its retention on the STS, thus requiring a waiver of the NASA policy against flying with such items present. The retention rationale is the primary input to NASA waiver decisions to fly the Shuttle, exposing the STS and its crew to the risk

implicit in the use of the analyzed critical item. **The retention rationale is used to justify accepting the design "as is," in the Committee's view; its audits of the NASA review process discovered little emphasis on creative ways to eliminate potential failure modes.**

The hazard analysis is another analytical tool used to identify and, if possible, resolve hazardous conditions that could develop while operating and maintaining STS hardware and software. Hazard analyses consider not only the failures identified in the FMEA process, but also other potential threats posed by the environment, crew-machine interfaces, and mission activities. Identified hazards and their causes are analyzed to find ways to eliminate or control the hazard. A hazard is said to be "eliminated" when its source has been removed. A "controlled hazard" is one that has effectively been controlled by a design change, addition of safety or warning devices, procedural changes, or operational constraints. Any hazard that cannot feasibly be eliminated or controlled is termed an "accepted risk."

There are many other analysis and assessment tools used by NASA. This complex mosaic of analysis techniques is intended to provide an all-encompassing approach to ensuring the design reliability and safety of the STS. Some of the techniques, such as the hazard analyses, tend to be "top-down" approaches that examine certain cross-systems causes and effects. Others, such as FMEA/CIL, are narrower "bottom-up" analyses that pursue a specific event to its conclusion—but only with respect to the subsystem involved.

In March 1986, soon after the Challenger accident, direction was issued within NASA to reevaluate the FMEAs on all critical items on the STS, "... to affirm the completeness and accuracy of the FMEA/CIL for the current National STS design." Following reevaluation of the FMEA, each Criticality 1 and 1R item, along with any new items, or items for which the reevaluation had led to a change in classification, was to be resubmitted for review and approval of the waiver permitting the item to be flown aboard the STS. Those items not revalidated by the review were required to be redesigned, certified, and qualified for flight. In addition to the FMEA/CIL reevaluation, the directives stipulated that the hazard analyses and a set of special Element Interface Functional Analyses (EIFAs) were also to be reviewed for completeness and accuracy.

Since the Challenger mission 51-L accident, a substantial number of engineering changes have been undertaken to improve Shuttle safety prior to resumption of flight. The redesign activity has, for the most part, preceded the FMEA/CIL and hazard analysis reevaluations. However, as the reevaluations proceeded, they disclosed a number of additional items which are being addressed before the next flight.

1.2 THE COMMITTEE'S VIEW

As the Challenger accident made very evident, space flight is not routine. Its risks must be accepted by those who are asked to participate in each flight as well as by those who are responsible to the nation for achieving our goals in space. The Committee believes that the basis for NASA's acceptance of those risks should, as far as possible, stem from rationally derived criteria. This acceptance also should depend very heavily on the quality of the methodology and the degree of objectivity by which the risks are determined, as well as the rigor by which the risks are controlled (i.e., managed).

Very early in the work of the Committee, it became clear that NASA's processes for analyzing failure modes, effects, and hazards could only be understood and evaluated intelligently when viewed as elements of an overall program of risk assessment and risk management. In the Committee's view, any such program should include the following basic elements:

Risk assessment:

—A comprehensive method for identifying potential failure modes and hazards associated with the system.

—A specific, quantitative methodology for identifying and assessing (or estimating) the safety risks of the system.

Risk management:

—A management process by which the safety risks can be brought to levels or values that are acceptable to the final approval authority. Risk management includes establishment of acceptable risk levels; the institution of changes in system design or operational methods to achieve such risk levels; system validation and certification; and system quality assurance. The basic organizational

elements are in place within NASA for assessing and managing risk; however, there is a need for a change in the scope of functions and the way that they are carried out.

The Committee believes that the *management* of the risks of the STS must be the responsibility of line management (i.e., the NSTS Program Manager, the Associate Administrator for Space Flight and, ultimately, the Administrator of NASA). Only this program management, *not the safety organizations*, can make judicious use of the means available to achieve operational goals while controlling the safety risks at acceptable levels throughout the evolution of the program. The safety organizations at NASA centers and Headquarters are staff organizations—as such, they can and should be responsible for providing *assessments* of the system's risks. They should also be responsible for assuring that the activities associated with controlling the risks to the specified levels have been carried out and documented. Safety organizations cannot, however, assure *safe operation*.

Certain shortcomings in process and methodology exist which are discussed in Section 5 and summarized in Section 1.3 below. In particular, there is a fundamental problem in the nature of and the methods used to develop the overall assessments on which NASA line management bases its decisions about how to reduce and control risk in the STS.

Risks in STS operations now are assessed based on subjective judgments and accepted on the basis of *qualitative* rationales, although many *quantitative* engineering analyses and test data relevant to risk assessment are available and often are used in arriving at what are finally qualitative, subjective judgements. With such a non-specific (i.e., non-value based) risk acceptance process there is little basis for making objective comparisons of the several major risk categories associated with the STS, nor for carrying out risk evaluations by independent agencies. Neither can one systematically track the efforts to reduce the risk or impact of the various possible failures. Without more objective, quantifiable measures of relative risk it is not clear how NASA can expect to implement a truly effective risk management program. However, the Committee does not wish to suggest that NASA subordinate sound technical judgement to numerical analysis. Such an approach would be, in our opinion, unrewarding and counterproductive.

1.3 FINDINGS AND RECOMMENDATIONS

Following are the major findings of the Committee and the specific recommendations associated with them. The summary findings and recommendations are extracted from Section 5 of the report, which includes a discussion of each one. The subsection numbering here parallels that in Section 5. For example, Subsection 1.3.1 corresponds to Subsection 5.1, 1.3.2 corresponds to 5.2, and 1.3.9.1 corresponds to 5.9.1. In addition, the recommendations are numbered sequentially and identically in both sections. It should be noted that *the recommendations are not listed in any priority order.*

1.3.1 Critical Items List Retention Rationale Review and Waiver Process

The Committee views the NASA critical items list (CIL) waiver decision making process as being subjective, with little in the way of formal and consistent criteria for approval or rejection of waivers. Waiver decisions appear to be driven almost exclusively by the design-based FMEA/CIL retention rationale, rather than being based on an integrated assessment of *all* inputs to risk management. The retention rationales appear biased toward proving that the design is “safe,” sometimes ignoring significant evidence to the contrary (see Section 5.1).

Although the Safety, Reliability, and Quality Assurance (SR&QA)² organizations of NASA collect, verify, and transmit all data related to FMEA/CIL and hazard analysis results, the Committee has not found an independent, detailed analysis or assessment of the CIL retention rationale which considers all inputs to the risk assessment process.

Recommendations (1):

The Committee recommends that NASA establish an integrated review process which provides a comprehensive risk assessment and an independent evaluation of the rationale justifying the retention of Criticality 1 and 1R items. This integrated review should include detailed consideration of the results of hazard analyses and all other inputs to the risk

² As of September 1987, the NASA Headquarters organization is called Safety, Reliability, *Maintainability*, and Quality Assurance (SRM&QA), while the similar organizations at the NASA centers are still named SR&QA. In this report, SR&QA also is used to refer generically to this function.

assessment process, in addition to the FMEA/CIL retention rationale. Further, the review process should assure that the waivers and supporting analyses fully reflect current data and designs. Finally, NASA should develop formal, objective criteria for approving or rejecting proposed critical item waivers.

1.3.2 Critical Items List Prioritization and Disposition

At present, in NASA instructions all Criticality 1 and 1R items are formally treated equally, even though many differ substantially from each other in terms of the *probability* of failure or malperformance, and in terms of the potential for the worst-case effects postulated in the FMEA to be seen if the particular failure occurs.

The large number of Criticality 1 and 1R items at the time of the 51-L accident has since been *substantially increased* due to changes in ground rules for classification and the complete reevaluation of the entire STS.

The Committee believes that giving equal management attention to all Criticality 1 and 1R potential failures could be detrimental to safety if, as is the case, some are extremely unlikely to occur, or if the probability is very low that the postulated worst-case consequences of the failures will result. Treating all such items equally will necessarily detract from the attention senior management can give to the *most* likely and *most* threatening failure modes.

Recommendations (2):

The Committee recommends that the formal criteria for approving waivers include the probability of occurrence and probability that the worst-case failures will result. We further recommend that NASA establish priorities now among Criticality 1 and 1R items, taking care not to use ambiguous measures of risk and probability. NASA should also modify the definitions of criticality in terms of the probability of failure and probability of worst-case effects. Finally, we recommend that NASA Level I management pay special attention to those items identified as being of highest priority, along with the rationale that produced the priority rating. Responsibility for attending to lower-priority items within the present Criticality 1 and 1R categories, when reclassified, should be distributed to Levels II and III for detailed evaluation and decision.

1.3.3 Hazard Analysis and Mission Safety Assessment

NASA hazard analyses currently do not address the relative probabilities of a particular hazardous condition arising from failure modes, human errors, or external situations.

The hazard analysis and the mission safety assessment do not: address the relative probabilities of the various consequences which may result from hazardous conditions; provide an independent evaluation of the retention rationales stated in the input CILs; or provide an overall risk assessment on which to base the acceptance and control of residual hazards.

Recommendations (3):

The Committee recommends that the FMEA/CILs be used as one of many inputs considered in the hazard analysis and system safety assessment. We also recommend that the overall system safety assessment encompass a quantitative risk assessment which in turn uses the CILs and hazard analyses as input. Finally, the Committee recommends that this risk assessment be the primary basis for retention or rejection of residual hazards as well as critical items.

1.3.4 Relationship of Formal Risk Assessment Process to Space Transportation System Engineering Changes

Elements of formal risk assessment, such as FMEA/CILs and hazard analyses (HAs), appear to have had little direct impact on the STS recovery engineering process, as they have not figured prominently in the majority of engineering change decisions made by NASA management.

Recommendation (4):

The Committee recommends that NASA take firm steps to ensure a continuing and iterative linkage between the formal risk assessment process (e.g., FMEA/CIL and HA) and the STS engineering change activities.

1.3.5 Timely Feedback of Data Into the Risk Assessment and Management Processes

The Committee has found many indications that data from STS inspection, test and repair, and in-flight operations do not always feed back rapidly enough or effectively enough into the risk assessment and management processes.

Recommendations (5):

The Committee recommends that high-level NASA management attention and priority be given to increasing the efficiency of the flow, analysis, and use of inspection, test and repair, test results, and in-flight operations data throughout the decision-making process. The Committee also recommends that full implementation of the System Integrity Assurance Program (SIAP), including its Program Compliance Assurance Status System (PCASS), be given a high priority. Diverse professionals (e.g., design and development engineers, operating personnel, statistical analysts) should be used in the development of this program, with maximum possible early involvement by potential users and key decision makers. The Committee further recommends that procedures be implemented to ensure that all mission anomalies detected in real time and from recorded events, and those detected during the near-term inspection of recovered hardware, also are fed into the formal risk assessment and management processes for action prior to committing to the next flight. Finally, the Committee recommends that all such anomalies be called to the immediate attention of launch decision makers who will justify in writing their decisions regarding the disposition of the anomalies.

1.3.6 The Need for Quantitative Measures of Risk

Quantitative assessment methods, such as probabilistic risk assessment, have not been used directly to support NASA decision making regarding the STS, although quantitative analyses and test data often are used in arriving at qualitative, subjective judgments upon which decisions are based. Powerful methods of statistical inference are now available which allow the integration of all sources of information on risk, including data on partial degradations and failures as well as engineering models of failure modes.

NASA is not adequately staffed with specialists and engineers trained in the statistical sciences to aid in the transformation of complex data into information useful to decision makers, and for use in setting standards and goals.

Recommendations (6):

The Committee recommends that probabilistic risk assessment approaches be applied to the Shuttle risk management program at the earliest possible

date. Data bases derived from STS failures, anomalies, and flight and test results, and the associated analysis techniques, should be systematically expanded to support probabilistic risk assessment, trend analyses, and other quantitative analyses relating to reliability and safety. Although the Committee believes that probabilistic risk assessment approaches will greatly improve NASA's risk assessment process, it recognizes that these approaches should not substitute for good engineering and quality control practices in design, development, test, manufacturing, and operations, all of which must continue to receive high priority emphasis by NASA and its contractors. The Committee further recommends that NASA build up its capability in the statistical sciences to provide improved analytical inputs to decision making.

1.3.7 The Need for Integrated Space Transportation System Engineering Analysis in Support of Risk Management

NASA safety-related analyses tend to focus primarily on single-event, worst-case failures to the relative exclusion of possible multiple and synergistic failures in different subsystems or elements of the STS. In addition, the connection between the various analyses appears tenuous. There does not appear to be an adequate integrated-system view of the entire STS.

Recommendation (7):

A "top-down" integrated system engineering analysis, including a system safety analysis, that views the sum of the STS elements as a single system should be performed to help identify any gaps that may exist among the various "bottom-up" analyses centered at the subsystem and element levels.

1.3.8 Independence of the Space Transportation System Certification and Software Validation and Verification Program

In general, hardware certification and verification, and software validation and verification³ in STS are managed and conducted primarily by the same organizational elements responsible for the design and fabrication of the units. Thus, the

³ See Appendix A for definition of these terms.

independence of the certification, validation, and verification processes is questionable. For example:

—The contractor that builds the Orbiters (Rockwell International, STS Division) is also responsible for preparing the documentation and performing the work involved in certification, but does not answer to an entity independent of the NSTS Program with regard to the certification function.

—At Marshall Space Flight Center (MSFC), the Engineering Directorate has the prime responsibility for design requirements for the propulsion elements of STS and also has responsibility for the review and approval of their certification. The Program Office is responsible for the design and development phase as well as for performing the certification activities.

—At the Johnson Space Center (JSC), prime responsibility for design requirements, design and development, and certification for the Orbiter all rest with the Program Office, supported by the Engineering and Operations Directorates of the Center.

—"Independent" validation and verification (IV&V) of software is carried out by the same contractor (IBM) that produces the STS software, with some checks being made by the Johnson Space Center (JSC).

Recommendation (8):

Responsibility for approval of hardware certification and software IV&V should be vested in entities separate from the NSTS Program structure and the centers directly involved in STS development and operation. However, these organizations should continue to conduct activities supporting certification and IV&V.

1.3.9 Operational Issues

1.3.9.1 Launch Commit Criteria Waiver Policy

An average of two Launch Commit Criteria (LCCs) are waived by NASA in the course of each launch. The Committee questions the validity of an operational procedure that "institutionalizes" waivers by routinely permitting established criteria to be violated.

Recommendation (9a):

The Committee recommends that NASA establish a list of mandatory LCCs which may NOT be

waived by anyone. This should comprise the bulk of the LCCs. A limited number of criteria would be separately listed, for special cases, together with a discussion of the circumstances under which they may be waived and who may make the waiver decision.

1.3.9.2 Human Factors as a Contributor to Risk

Human factors, which are considered in some of the STS hazard analyses, do not appear to be taken into account as the cause of failure modes in the FMEAs. Since the FMEA is one of the principal safety tools used in the evaluation of the STS design, the Committee believes that the STS design process should explicitly consider and minimize the potential contribution of humans to the initiation of the defined failure modes.

Recommendation (9b):

The Committee recommends that the NASA FMEA include human factors among the recognized sources of potential causes of failure modes. This step would provide another valid link between the FMEA and the hazard analysis, which are now, in our view, too tenuously connected.

1.3.9.3 Cannibalization of Spare Parts

By the time of the Challenger accident, "cannibalization," the removal of parts at the Kennedy Space Center (KSC) from one operational STS element to fulfill spares requirements in another, had become a prevalent feature of STS logistics, thus introducing a variety of failure potentials associated with human error. Cannibalization is not evaluated as a producer of potential failure in either the hazard analysis (where it would be most appropriate) or the FMEA.

Recommendations (9c):

The Committee recommends that NASA maintain its current intense attention toward reducing cannibalization of parts to an acceptable level. We further recommend that adequate funds for the procurement and repair of spare parts be made available by NASA to ensure that cannibalization is a rare requirement. Finally, we recommend that NASA include cannibalization, with its attendant removal and replacement operations, as a potential producer of failure in the integrated risk assessment recommended earlier (Section 1.3.1).

1.3.10 Other Weaknesses in Risk Assessment and Management

1.3.10.1 *The Apparent Reliance on Boards and Panels for Decision Making*

The multilayered system of boards and panels in every aspect of the STS may lead individuals to defer to the anonymity of the process and not focus closely enough on their individual responsibilities in the decision chain. The sheer number of STS-related boards and panels seems to produce a mindset of "collective responsibility."

Recommendation (10a):

The Committee recommends that the Administrator of NASA periodically remind all NASA personnel that boards and panels are advisory in nature. He should specify the individuals in NASA, by name and position, who are responsible for making final decisions while *considering* the advice of each panel and board. NASA management should also see to it that each individual involved in the NSTS Program is completely aware of his/her *responsibilities* and *authority* for decision making.

1.3.10.2 *Adequacy of Orbiter Structural Safety Margins*

The primary structure of the STS has been excluded, by definition, from the FMEA/CIL process, based on the belief that there is an adequate positive margin of safety. However, the Committee questions whether operating structural safety margins have actually been proven adequate.

Completion of the Model 6.0 loads study and the reevaluation of margins of safety based on these loads will significantly improve NASA's grasp of actual operating margins of safety.

Recommendations (10b):

The Committee recommends that NASA place a high priority on completion of the Model 6.0 loads, the reevaluation of safety margins for these loads, and the early verification and continued monitoring of the model 6.0 loads by permanently instrumenting and calibrating at least the next full scale STS vehicle to fly. We further recommend that NASA complete and implement a comprehensive plan for conducting periodic inspection and maintenance of the structure of the Orbiters throughout the service life of each vehicle.

1.3.10.3 Software Issues

NASA FMEAs do not assess software as a possible cause of failure modes.

There is little involvement of JSC Safety, Reliability, and Quality Assurance in software reviews, resulting in little independent quality assurance for software.

A large amount of data—much of it flight specific—must be loaded for each Shuttle mission but it is not subjected to validation as rigorous as that for the software.

Recommendations (10c):

The Committee recommends that NASA: explore the feasibility of performing FMEAs on software, including the efficacy of identifying and predicting fault and error modes; request JSC SR&QA to provide periodic review and oversight of software from a quality assurance point of view; provide for *validation of input data* in a manner similar to software validation and verification.

1.3.10.4 Differences in Procedures Among NASA Centers

Differences in the procedures being used by the main NASA centers involved in the NSTS Program may reflect an imbalance between the authority of the centers and that of the NSTS Program Office. The Committee is concerned that such an imbalance can lead to serious problems in large programs where two or more centers have major roles in what must be a tightly integrated program, such as the NSTS and Space Station. Without strong, central program direction and integration, the success and safety of these complex programs can be placed in jeopardy.

Recommendation (10d):

The Administrator should ensure that strong, central program direction and integration of all aspects of the STS are maintained via the NSTS Program Office.

1.3.10.5 Use of Non-Destructive Evaluation Techniques

Non-destructive evaluation (NDE) tests on the Solid Rocket Motor (SRM) are performed at the manufacturing plant. Subsequent transportation and assembly introduce a risk of debonding and

other damage which may not be apparent upon visual inspection. No NDE is done on the SRMs in the “stacked” configuration at the launch facility.

New NDE techniques now being developed have potential applicability to the STS.

Recommendation (10e):

The Committee recommends that NASA apply all practicable NDE techniques to the SRM at the launch facility, at the highest possible level of assembly (e.g., SRMs in the “stacked” configuration), and emphasize development of improved NDE methods.

1.3.11 Focus on Risk Management

The current safety assessment processes used by NASA do not establish objectively the levels of the various risks associated with the failure modes and hazards.

It is not reasonable to expect that NASA management or its panels and boards can provide their own detailed assessments of the risks associated with failure modes and hazards presented to them for acceptance.

Validation and certification test programs are not planned or evaluated as quantitative inputs to safety risk assessments. Neither are operating conditions and environmental constraints which may control the safety risks adequately defined and evaluated.

In the Committee’s view, the lack of objective, measurable assessments in the above areas hinders the implementation of an effective risk management program, including the reduction or elimination of risks.

Recommendations (11):

The Committee recommends that NASA consider establishing a focused agency-wide Systems Safety Engineering (SSE) function, at both Headquarters and the centers, which would:

- be structured so as to be integrally involved in the entire set of design, development, validation, qualification, and certification activities;

- provide a full systems approach to the continuous identification of safety risks (not just failure modes and hazards) and the objective (quantitative) evaluation of such safety risks;

- provide the output of this function to the NASA Program Directors in support of their risk management; and

—support the Program Directors by providing assurance that their systems are ready for final safety certification to the risk levels established by the NASA Administrator.

The Committee also recommends that the STS risk management program, based in part on the definition of the potential to reduce the level of risk developed by the system safety risk assessment, include a concerted effort to remove or reduce the risks.

1.4 CLOSING REMARKS

Although this report and its recommendations are directed to the NSTS Program, most of them are of broader applicability. It would be wise to consider the lessons learned here when structuring

a risk assessment and management system for other programs which have similar attributes, such as the Space Station. The safety of other large systems involving highly complex technology, and requiring major participation by several NASA centers and prime contractors, could benefit from an integrated risk assessment and management program based on the current NASA procedures supplemented by those recommended in this report. For any new program, such as the Space Station, there is the opportunity to structure an optimum risk assessment and management program at the outset by assembling those elements of risk assessment and management which will be most effective in establishing, monitoring, and controlling safety risks to accepted levels. (See Section 6.)

2 Introduction

“Criticality Review and Hazard Analysis. NASA and the primary Shuttle contractors should review all Criticality 1, 1R, 2, and 2R items and hazard analyses. This review should identify those items that must be improved prior to flight to ensure mission success and flight safety. An Audit Panel, appointed by the National Research Council, should verify the adequacy of the effort and report directly to the Administrator of NASA.”

2.1 PURPOSE OF STUDY

The Space Shuttle Challenger disaster of January 28, 1987, stunned NASA and the entire nation. As the shock of the accident began to subside, NASA initiated a wide range of actions designed to ensure greater safety in various aspects of the Shuttle system and an improved focus on safety throughout the National Space Transportation System (NSTS) Program. A number of these actions were prompted by recommendations of the Presidential Commission on the Space Shuttle Challenger Accident (also known as the Rogers Commission).

Recommendation III of the Presidential Commission (see box above) directed NASA to review certain safety-critical items on the Shuttle as well as the existing analyses of hazards that could affect Shuttle operations and system safety, and to identify needed improvements in the Shuttle system. It also recommended the establishment of an audit panel, under the auspices of the National Research Council (NRC), to monitor that review effort and verify its adequacy. At NASA's request, the NRC formed the Committee on Shuttle Criticality Review and

Hazard Analysis Audit to conduct this audit. The Committee consisted of 12 people with expertise in a range of relevant areas: space system development and operations, aircraft development and operations, propulsion systems, avionics, structures, statistics, reliability and safety, and risk assessment and management of complex technological systems. They were asked to evaluate NASA's effort in response to the Rogers Commission recommendation and to report their findings and recommendations directly to the NASA Administrator.

See Appendix B for the full text of the pertinent establishing documents.

2.2 STUDY APPROACH

2.2.1 Interpretation of Task

Following its charge from the Rogers Commission and NASA, the Committee planned initially to focus its audit strictly on certain specific features of the NASA safety process:

- the Critical Items List (CIL) and the NASA review of those Shuttle primary and backup units whose failure might result in loss of life, the Shuttle vehicle itself, or the mission (i.e., the Criticality 1, 1R, 2 and 2R items⁴);
- the Failure Modes and Effects Analyses (FMEA) on which the criticality determinations are largely based; and
- the hazard analyses and their review.

(See Section 3 for a description of these activities and their interrelationships.)

⁴ See Table 3-1 for definitions of Criticality levels.

Early in its study, the Committee recognized that to fulfill its charge to “verify the adequacy of the effort” it must broaden the scope of its audit to include an assessment, from a risk management point of view, of NASA’s overall process for identifying, assessing, reviewing, and implementing changes in the Space Shuttle system. That broader scope would include not only other safety analyses and functions, but also the relationship of safety elements and organizations to the continuing process of Space Shuttle design and engineering. (See Appendix B for the resulting Statement of Task.)

Thus, in the context of evaluating NASA’s procedures for detecting, assessing, and dealing with hazards and potential failure modes in the Shuttle system, the Committee would seek to determine:

- What has NASA done in the past?
- What is it doing differently now?
- How adequate are these procedures?
- Where are the flaws in the process, if any?

2.2.2 Plan and Structure

The Committee began with a general review of NASA’s policies and procedures for reviewing safety-critical items and analyzing hazards. This process overview, provided in briefings by and discussions with NASA officials and managers of the NSTS Program and its component projects, provided not only a general overview but also the status of the reevaluation which NASA had undertaken of the FMEA/CIL and hazard analyses. The general review also included briefings and studies on the ways in which other organizations and industries (e.g., U.S. Air Force, nuclear power, and commercial aviation) accomplish similar safety analyses and reviews.

The Committee decided to conduct its audit of the reevaluation on several levels. First, it would conduct a detailed review of one or two major Space Transportation System (STS) elements⁵, and the reevaluation process and its results. The Space Shuttle Main Engine (SSME) and the Solid Rocket Booster/Solid Rocket Motor (SRB/SRM) were selected for this audit, since the Committee felt that

the greatest hazards are in propulsion. During its work, the Committee identified other areas of concern which led to a detailed examination of a number of different aspects of the STS safety-related activities. Each of these audits was conducted through a series of meetings with NASA and contractor personnel on-site at contractor facilities and NASA centers.

Concern about the potential weakness of NASA’s “top-down” analyses to complement the “bottom-up” FMEA/CILs (which seemed to be the dominant safety evaluation tool) led the Committee to initiate audits related to the integrated system safety assessments across all of the elements of the STS. For example, it examined interactions arising from the generation and distribution of electrical power and fresh water aboard the STS, and the generation and distribution of hydraulic power in the Orbiter and the SRB. This work is reflected particularly in Section 5.7 of this report.

The 17-inch diameter fuel and oxidizer disconnect valves between the Orbiter and the External Tank (ET) were selected for detailed examination of the preparation and role of hazard analyses in STS risk assessment to complement the broader, more general treatment of this subject obtained in briefings, discussions, and written answers to Committee questions. This audit contributed significantly to Sections 5.3 and 5.11.

The Committee discovered early in its work that the large number of Criticality 1 and 1R items on the STS are not ranked by priority of their importance and that NASA did not appear to be making much use of modern analytical techniques in quantitatively assessing probabilities of failures and their effects, and levels of risk in the program. This led to a special investigation of the extent to which such techniques are used in the NSTS program, and of methods which might be of special value to the program. (See especially Sections 5.2 and 5.6, and Appendices D and E.)

Since the STS structure was excluded by NASA from the FMEA/CIL process, and since there were concerns about the actual margins of safety, the Committee examined in some detail the past history and current activity of NASA in this critical area (see Section 5.10.2). The safety/risk assessment for Orbiter software also is handled in a very different manner than hardware (e.g., no FMEA/CIL). Therefore, it too was subjected to a special audit, the results of which are reflected primarily in Sections 5.8 and 5.10.3.

⁵ NASA terminology generally refers to the entire Space Shuttle as a “system” composed of four major flight “elements”: Orbiter, Space Shuttle Main Engines, Solid Rocket Boosters/Solid Rocket Motors, and External Tank. Each of these elements is composed of major systems which are, in turn, made up of subsystems, units, and components or piece parts.

Finally, because of significant problems in the past, the Committee examined in some detail, from a safety standpoint, the history and current redesign of the Orbiter nose wheel steering system, and the main wheels and brakes.

These more detailed audits of selected subsystems, when coupled with the broader investigations of the SSME and SRB elements and the STS as a whole, provided the basis for the Committee's findings, conclusions, and recommendations in Section 5 and supporting material in Appendices D through F. The Committee did not examine the interfaces between the STS and its payloads to the extent that the members were comfortable in making any specific conclusions and recommendations beyond those for the NSTS Program in general.

2.2.3 Meetings and Site Visits

Apart from the meetings and site visits conducted by individual and groups of Committee members, the full Committee held a total of 12 meetings. Nine meetings were largely fact-finding with NASA and contractor personnel; three were devoted to formulating conclusions and recommendations, and preparation of this final NRC report (see Table 2-1). The Committee met with a large number of NASA personnel representing Headquarters management, as well as program and project management at all three of the NASA field centers having primary involvement in the NSTS Program. Safety, Reliability, and Quality Assurance (SR&QA) organizations⁶ were heavily represented among those presenting briefings and working with the Committee. Prime contractors for STS elements, and contractors for several subsystems and STS integration activities were also extensively represented, both at NASA centers and at their own facilities. In addition, independent contractors involved in the FMEA/CIL reevaluation were heard from.

In addition to the meetings and site visits, input was provided by NASA in two other very important ways. First, two NASA liaison persons representing Headquarters management and the NSTS Program (SR&QA Office) facilitated the Committee's audit and provided direct input on specific questions on

⁶ As of September 1987, the NASA Headquarters organization is called Safety, Reliability, *Maintainability*, and Quality Assurance (SRM&QA), while the similar organizations at the NASA centers are still named SR&QA. In this report, SR&QA also is used to refer generically to this function.

an ongoing basis. Secondly, a series of documents were provided giving detailed answers to lists of questions developed by the Committee on a wide range of subjects. These "Q&A" documents were supplemented by substantial reports from NASA on certain points of concern.

It should be noted here that the Committee was at all times impressed and gratified by the excellent support that was consistently provided by NASA management and staff to accommodate the Committee's audit and its inquiries.

2.2.4 Interim Reports of the Committee

In accordance with its charge, the Committee issued two interim progress reports in the form of letters to the NASA Administrator (see Appendix C). The first letter report was dated January 13, 1987, some four months after the Committee first met. Presented in person by Committee Chairman Alton D. Slay to the Administrator and his key deputies, it presented four specific suggestions for improvement in aspects of the FMEA/CIL and hazard analysis processes, based on the initial phase of the Committee's audit. The Administrator discussed these matters with Chairman Slay, and then responded formally to SCRHAAC on April 22, 1987, to describe actions taken with regard to the Committee's concerns. As following sections will detail, specific changes in procedure and approach have already been made in response to two of the four suggestions (see NASA response to the first letter report, in Appendix C).

In addition, Committee Chairman Slay appeared before the House Subcommittee on Space Science and Applications (Committee on Science, Space and Technology) on April 29, 1987, to discuss the findings contained in the first letter report.

The Committee's second letter report was issued July 22, 1987, and was again delivered personally by the Chairman and discussed with the Administrator. It summarized SCRHAAC's continuing activities and findings, also commenting on the actions taken by NASA in response to the first letter report. In this second report, eight new topics were addressed, some of them expressing approval of particular aspects of the STS risk assessment and management process, and planned changes, and others highlighting areas of concern on the part of the Committee.

Some of the concerns expressed in the interim reports have been resolved since the reports were

TABLE 2-1 Meetings of the Committee on Shuttle Criticality Review and Hazard Analysis Audit

Date	Location	Participants	Purpose
1. 9/22–23/86	NRC, Washington, DC	NASA Headquarters, JSC, MSFC & KSC staff Boeing Comm'l Aircraft representatives	Process overview, Committee planning
2. 10/27–28/86	Rockwell STS Div. Rocketdyne Div. Los Angeles, CA	Rockwell STS Div., Rocketdyne Div, NASA HQ, JSC, MSFC, USAF Space Div. and Aerospace Corp. staff	SSME, Orbiter FMEA/CIL & hazard analysis audit
3. 11/10/86	NRC, Washington, DC	NASA Assoc. Admins. for Space Flight & SRM&QA, NSTS Program Manager	Discussion of concerns; draft first interim report
4. 12/15–16/86	NASA JSC, Houston	NSTS and JSC personnel (including Mission Operations & Astronaut personnel)	Review STS risk management and operations
5. 1/14–16/87	MSFC Huntsville, AL KSC FL	MSFC and KSC leaders and staff related to STS	Overview of MSFC & KSC FMEA/CILs & hazard analyses
6. 2/10–11/87	NRC, Washington, DC	MSFC & JSC Indepndnt contractor staff, Quant. Risk Assess. (QRA) consultants	QRA, Independent contractor FMEA/CIL reviews
7. 3/18/87	Rocketdyne Div. Canoga Park, CA	Rockwell STS Div., Rocketdyne Div., NASA HQ, JSC, and MSFC staff	SSME: STS integration activities
8. 4/24–25/87	NRC, Washington, DC	NASA HQ & JSC NSTS personnel SRM&QA personnel	SRM&QA status and functions STS integration & software
9. 5/28–29/87	NRC, Washington, DC	NSTS Dep. Dir., Operations JSC, HQ personnel	STS oprns, payloads, PCASS, system engineering, draft second interim report
10. 7/13 -14/87	NRC, Woods Hole, MA	Executive session	Review & discuss information collected
11. 9/3 4/87	NRC, Washington, DC	Executive session	Formulate conclusions, recommendations; review drafts
12. 10/12/87	NRC, Washington, DC	Executive session	Review & approve final text

ACRONYMS:

CIL	Critical Items List	NSTS	National Space Transportation System
FMEA	Failure Modes and Effects Analysis	PCASS	Program Compliance Assurance and Status System
HQ	Headquarters (of NASA)	QRA	Quantitative Risk Assessment
JSC	Johnson Space Center	SRM&QA	Safety, Reliability, Maintainability & Quality Assurance
KSC	Kennedy Space Center	SSME	Space Shuttle Main Engine
MSFC	Marshall Space Flight Center	STS	Space Transportation System
NASA	National Aeronautics & Space Administration	USAF	United States Air Force
NRC	National Research Council		

presented; others remain at issue. All of the concerns identified in those reports are discussed in Section 5 of this report. It should be noted that NASA's safety process in general, and the current reevaluation in particular, have been undergoing considerable change following the Challenger accident and during the Committee's audit. Indeed, some of the changes have resulted from the Committee's discussions with NASA officials and from its interim reports. Thus, many of the subjects covered by this report have been "moving targets" that continued to change as this report was being prepared. However, the Committee believes that the report reflects the facts and circumstances as of September 1987.

2.3 ORGANIZATION OF THE REPORT

Following this introduction is Section 3, which presents an overview of NASA's safety process for

the NSTS Program as the Committee understands it. That section is provided as a tutorial for those who may not be familiar with this complex process. Section 4 briefly describes the Committee's conception of modern risk management, including the essential element of objective risk assessment, and contrasts it with NASA's safety process in general terms.

The heart of the report is Section 5, which presents discussion, findings, and recommendations regarding particular aspects of NASA's STS safety assurance process. It comprises the results of the Committee's audit. The section is divided into 11 subsections, each dealing with a different aspect of the process (with some encompassing related but distinct topics).

Section 6 is a brief summary of the main "lessons learned" by SCRHAAC in the course of its audit. These lessons, derived from the STS review, are

considered to be applicable to other large and complex technological systems which, by their size and complexity, require the involvement of several major centers and organizations for their execution.

Finally, a series of appendices are provided.

Some, like Appendix A (“Acronyms and Definitions”), are intended as useful tools for the reader. Others are provided as amplification or background on various subjects addressed in the report. See the Table of Contents for a complete listing.

3 NASA's Safety Process For The National Space Transportation System Program

Before entering into a discussion of the Committee's findings regarding various specific aspects of the process that NASA relies on to ensure the safety of the Space Transportation System (STS), it may be useful to provide a basic overview of the elements and purposes of that process. Readers who are already familiar with the structure and purposes of NASA's present safety process may wish to skip over this "orientation" section and begin reading at Section 4.

The measures taken to ensure safety follow basic NASA policy issued at the Administrator level. The implementation of that policy is guided and overseen by descending levels of management throughout NASA Headquarters and the NASA field centers and their contractors involved in STS development and operation. Various organizations within NASA have different and overlapping sets of responsibilities with respect to safety of the STS. At the heart of the safety process is a set of analyses of the system configuration and function. NASA's activities in the safety area since the Challenger (51-L) disaster occurred have centered on these analyses and on the needed engineering changes in the STS system which the analyses have helped to identify.

This section is intended to be only a factual description of NASA's safety process, with emphasis on policy and structure (as perceived by the Committee). The Committee's analysis and comments are presented beginning in Section 4.

3.1. POLICY ON SAFETY

NASA policy regarding safety is established by the Administrator through NASA Policy Directive

(NPD) 1701.1, "Basic Policy on Safety." The purpose of this document is to prescribe "the basic policy for planning, developing, conducting, and evaluating agency activities to ensure the highest practicable standards of safety in all NASA programs." The essence of the policy is to:

- "a. Avoid loss of life, injury of personnel, damage and property loss.
- "b. Instill a safety awareness in all NASA employees and contractors.
- "c. Assure that an organized and systematic approach is utilized to identify safety hazards and that safety is fully considered from conception to completion of all agency activities.
- "d. Review and evaluate plans, systems, and activities related to establishing and meeting safety requirements both by contractors and by NASA installations to ensure that desired objectives are effectively achieved."

The accompanying NASA handbook (NHB 1700.1 [VI]) states that "... the steps necessary to achieve safety of operations begin with initial planning and extend through every facet of NASA's activities. Under this concept, every manager throughout the organization is responsible for systematically identifying risks, hazards, or unsafe situations or practices, and for taking steps to assure adequate safety in the activities and products under his supervision."

Out of this broad policy framework are derived the more specific safety requirements that are implemented in successively greater detail down through Headquarters, program and project organizations at the NASA centers, and contractor organizations.

3.2 MANAGEMENT STRUCTURE

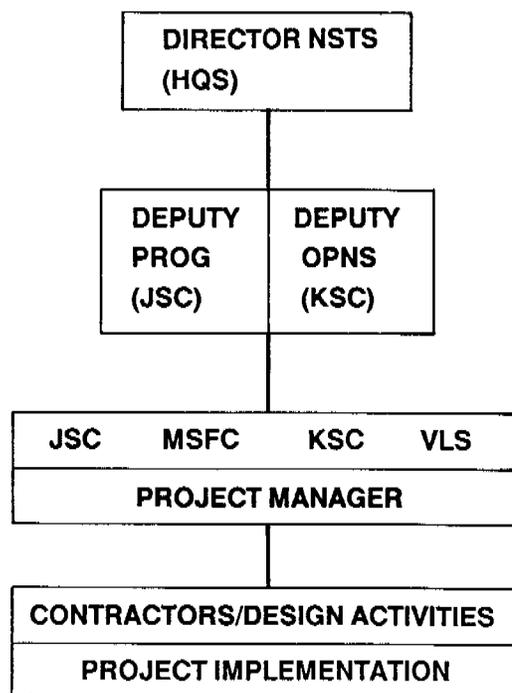
3.2.1 Program Management

The development and operation of the STS is carried out through a National Space Transportation System (NSTS) Program. This Program draws on resources functionally located at three of the NASA field centers. Prior to the Challenger mission 51-L the NSTS Program was managed out of Johnson Space Center (JSC), in Houston; JSC is also responsible for the Orbiter element of the STS as well as the integration of all STS elements. Marshall Space Flight Center (MSFC), in Alabama, is responsible for the propulsion elements of the STS: the Space Shuttle Main Engine (SSME), Solid Rocket Booster (SRB), which includes the Solid Rocket Motor (SRM), and External Tank (ET). Kennedy Space Center, in Florida, is responsible for major ground support equipment (GSE), and launch and landing operations.

After mission 51-L, the NSTS Program Director was brought to NASA Headquarters (Level I) to manage the program from a location closer to top agency officials and at a level which has oversight of all three field centers. The Deputy Director (Program) of the NSTS Program remains at JSC; the recently established position of Deputy Director

(Operations) is located at KSC. At each NASA center there are Project Managers responsible for the particular elements and systems. These Project Managers, in a matrix organizational arrangement, report functionally to the NSTS Program Director as well as organizationally to the center management. Reporting to the Project Managers are various Subsystem Managers who are directly responsible for the engineering effort on their subsystems. Thus, within the center organization there are engineers and other personnel supporting the NSTS Program.

Management levels within the NSTS Program are referred to as "Level I, Level II", and so on according to the hierarchy shown in Figure 3-1. Each level of management has a specific scope of responsibility, as described in the figure. Basically, Level I is Headquarters, primarily concerned with policy and broad program formulation and management; Level II is the major program management level; and Level III is the project management level. The Level I Program Director is at Headquarters, and reports to the Associate Administrator for Space Flight. Level II for development resides at JSC (viz., the Deputy Director [Program]) and at KSC for operations (the Deputy Program Director [Operations]), while Level III is dispersed across all of the participating NASA centers.



LEVEL I:
TOP LEVEL PROGRAM REQUIREMENTS, BUDGETS AND SCHEDULES. CONTROL OF CHANGES ABOVE \$1 MILLION/YEAR OR TWO MILLION TOTAL, OR THOSE IMPACTING LEVEL I REQUIREMENTS OR SCHEDULES.

LEVEL II:
MANAGEMENT AND INTEGRATION OF ALL ELEMENTS OF THE PROGRAM. INTEGRATED FLIGHT AND GROUND SYSTEM REQUIREMENTS, SCHEDULES AND BUDGETS; CONTROL OF PROJECT INTERFACES; CONTROL OF CHANGES EXCEEDING PROJECT BUDGETS, OR THOSE IMPACTING LEVEL II REQUIREMENTS, INTERFACES, OR SCHEDULES.

LEVEL III:
PROJECT ORIENTED FLIGHT AND GROUND SYSTEM REQUIREMENTS, SCHEDULES, AND BUDGETS; CONTROL OF CHANGES WITHIN PROJECT LEVEL BUDGETS, SCHEDULES, AND SPECIFICATIONS.

LEVEL IV:
DETAILED FLIGHT AND GROUND SYSTEM REQUIREMENTS WITHIN ASSIGNED PROJECT. CONTROL AND IMPLEMENTATION OF DETAILED DESIGN.

FIGURE 3-1 National Space Transportation System Program management relationships (after NASA).

3.2.2 Review Boards

Each of the management levels has associated with it one or more boards or panels that review and approve or disapprove the actions proposed by technical and other groups at the levels below. The most important of these boards are the two Program Requirements Control Boards (PRCBs). One PRCB is at Level II and the other at Level I, chaired respectively by the NSTS Deputy Director (Program) and the NSTS Program Director. These boards meet together to review FMEA/CILs. The main Level III boards are the Configuration Control Boards (CCBs), one for each STS element and the two launch sites (KSC and Vandenburg AFB); each of the CCBs is supported by a number of Configuration Control Panels (CCPs). (See Figure 3-2.)

Each of these boards and panels has controlling authority for “dispositioning” (deciding upon or recommending) proposed changes to its documentation, hardware, and software—to the extent that the change does not conflict with requirements, schedules, budgets, etc., established by a higher-level board. Level II/I PRCB approval is required for all changes to flight hardware after delivery to NASA and for all changes to flight hardware that interfaces with GSE.

There are a considerable number of other Level II and III boards that are responsible for review of specific technical and management aspects of STS design, development, and operation. All of them feed, ultimately, through the Level II/I PRCBs, which are the highest boards for configuration control. These boards and their functions (some of which are shown in Figure 3-2) will be described further in Section 3.3, and from a different standpoint in Section 5.10.1.

3.3 ORGANIZATIONAL ROLES

As was noted in Section 3.1, in theory, safety in all its forms is equally the responsibility of all NASA managers and workers, as well as those of their contractors. In practice, roles and responsibilities are necessarily defined and allocated across various functional organizations. Within the NSTS Program, these safety-related roles are shared by the engineering organizations in the project offices; the Safety, Reliability, Maintainability, and Quality Assurance (SR&QA) organization at Headquarters and the corresponding SR&QA organizations at the centers; the NSTS Engineering Integration

Office; and, to a lesser extent, the operations organizations (i.e., the Astronaut Office and Mission Operations Directorate).

3.3.1 Engineering Project Offices

The engineering organization within each element project office at the centers is responsible to a Project Manager and the Program Director for the performance and reliability of hardware/software systems they develop. Safety is thus an inherent feature of the system design, development, testing, and production processes. Since it is engineers who design the unit or system, test it, certify it for operation, and inspect it after flight, it is they who have the greatest ability to understand and anticipate the ways in which the unit or system might fail.

For that reason, NASA engineers have primary responsibility for carrying out the most technical of the safety analyses described in Section 3.4 (i.e., the Failure Modes and Effects and Analysis [FMEA]) and for establishing the rationale for retaining critical items identified through the FMEA. They participate secondarily in other safety analysis efforts. However, few of the engineers have any formal grounding in safety engineering techniques and methodologies.

3.3.2 Safety, Reliability, Maintainability, and Quality Assurance

Safety, Reliability, and Quality Assurance (SR&QA) Offices (the maintainability function was added at Headquarters in 1986) have long existed in one form or another within the various NASA centers as staff organizations reporting to the center director. (See Figure 3-3, for example.) The corresponding Headquarters organization has existed as a policy-setting group reporting, until 1986, to the NASA Chief Engineer.

Center SR&QA staff are detailed to programs such as the NSTS Program, where they develop functional units of staff dedicated to various aspects of Safety, Reliability, and Quality Assurance.⁷ Their role is to provide oversight of the engineering design and development activities, and to advise the Project Manager and the various configuration control boards on the safety and other relevant aspects of systems under review. They are also responsible

⁷ The center SR&QA organizations have, as of the time of writing, not adopted the “M” in their organization name. We have elected to adhere to current NASA practice to avoid confusion.

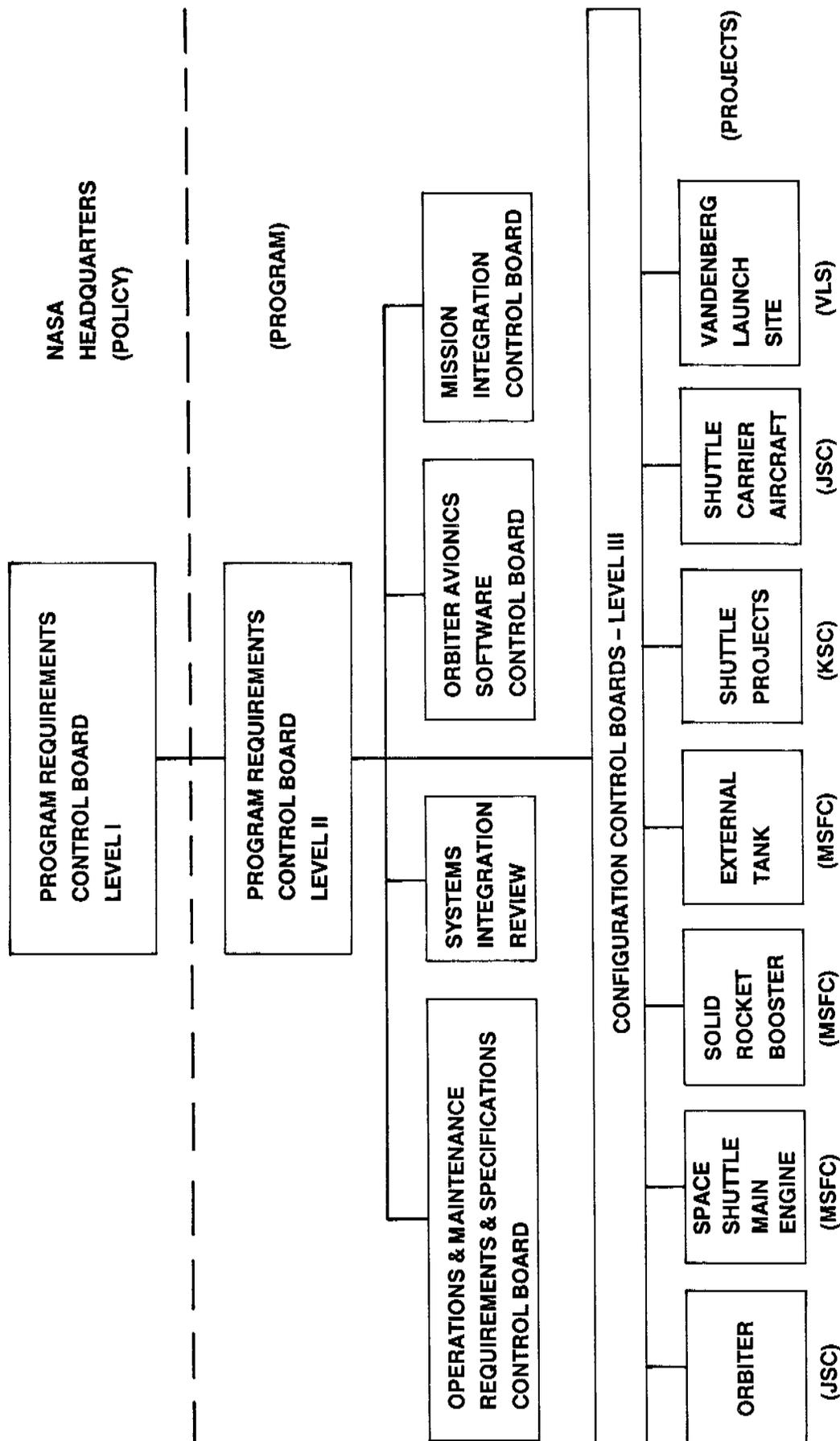


FIGURE 3-2 Structure of NSTS Program Requirements Control Boards and Configuration Control Boards (after NASA).

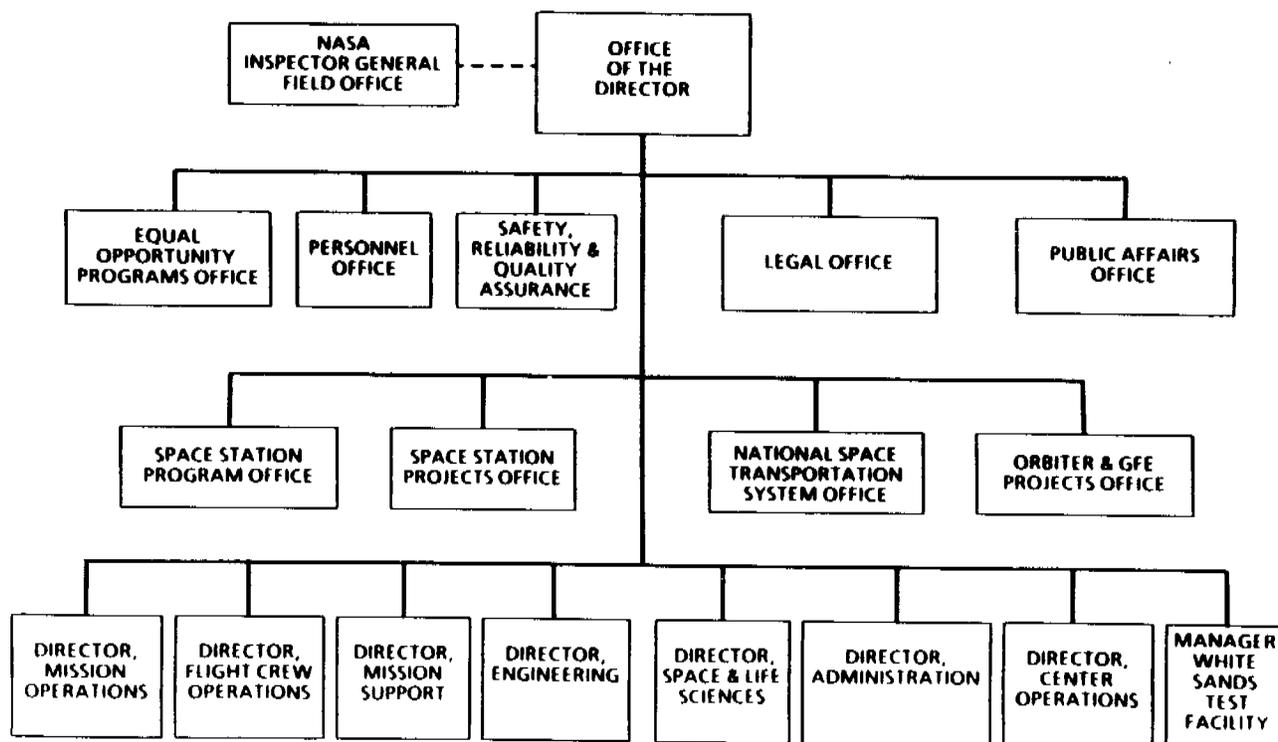


FIGURE 3-3 Organization of NASA Johnson Space Center (NASA).

for keeping records on problems and anomalies encountered in the development and operation of the STS.

SR&QA, through its Safety Divisions, has primary responsibility for conducting hazard analyses of the STS (see Section 3.4.2 for a description). This is one of the most important safety-related analyses conducted on the STS, in many ways complementing the FMEA.

In the wake of the Challenger accident, the functions and authority of SR&QA were expanded in scope, and the Headquarters organization was restructured. A new position of Associate Administrator for SRM&QA was established, with appeal rights to the Administrator of NASA on any decision relevant to the safety of the STS and its crew. The new Associate Administrator intends to establish the SRM&QA function as an effective check and balance to the overall NASA operation, one that will provide a “second-look assessment” of the entire process from design through operations. Figure 3-4 depicts the new SRM&QA organization at Headquarters.

3.3.3 Engineering Integration Office

The NSTS Engineering Integration Office is located at JSC, where it handles certain special aspects

of STS design and development that are crucial to the safe functioning of the overall system. These include: systems integration and interface design between the different STS elements, analyses of integrated structural loads and thermal effects, software requirements and configuration control, and ground systems and operations requirements. Shuttle avionics and ascent flight systems—two systems involving electronics and software functions which cut across various STS elements—are also among the responsibilities of this office.

The organization of the office is shown in Figure 3-5. Note that the figure identifies a separate review structure for systems integration and software. The Systems Integration Review (SIR) Board is a Level II board that supports the Level II and I PRCBs in all the integration areas, including ascent and entry, flight control, and thermal design. The Shuttle Avionics Software Control Board (SASCB) is the controlling authority for avionics software. Additionally, a Mission Integration Control Board (MICB), shown in Figure 3-2, is the controlling authority for changes to delegated mission integration requirements that do not affect other Level II requirements, budgets, or schedules.

The Engineering Integration Office is also responsible for carrying out a series of Element

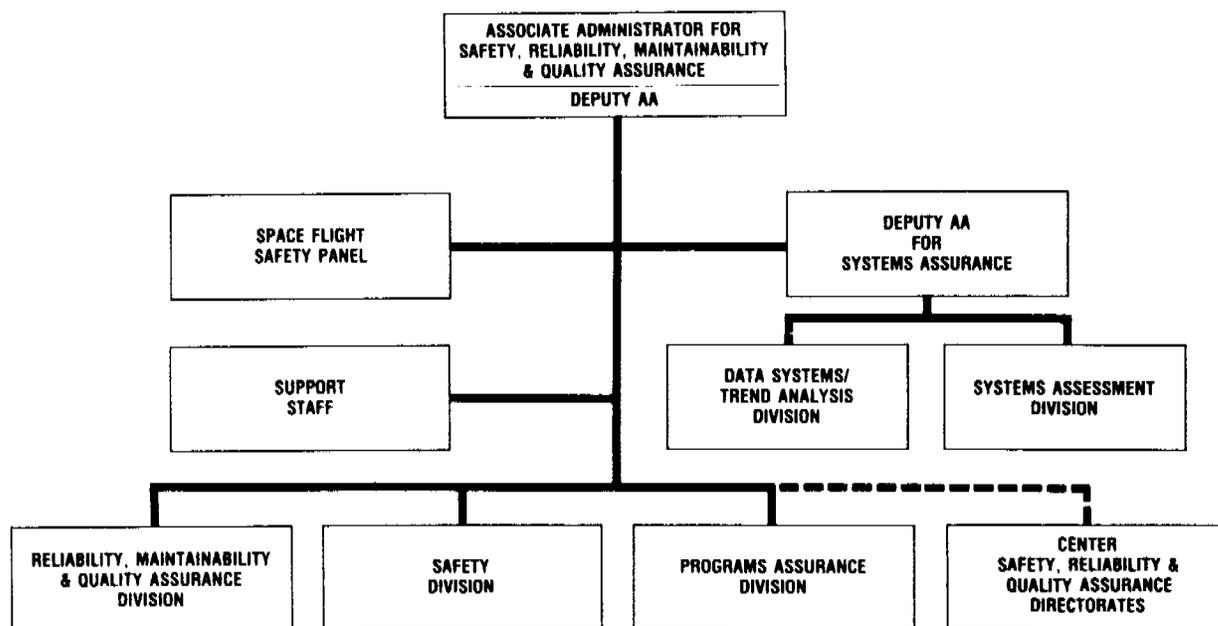


FIGURE 3-4 Organization of the new office of Safety, Reliability, Maintainability, and Quality Assurance at NASA Headquarters (NASA).

Interface Functional Analyses (EIFA), described in Section 3.4.3 below.

3.4 SAFETY ANALYSES

3.4.1 The Failure Modes and Effects Analysis and Critical Items List

At the heart of NASA's effort to ensure reliability of the Shuttle system is the Failure Modes and Effects Analysis. FMEAs are performed on all STS flight hardware as well as Ground Support Equipment which interfaces with flight hardware at the launch sites to identify hardware items that are critical to the performance and safety of the vehicle and the mission, and to identify items that do not meet design requirements. (NASA does not perform FMEAs on software; also excluded from the FMEA by definition are STS primary structure and, originally, pressure vessels.) This analysis, carried out by the element contractor, begins with an identification of the functional units of each system and a determination of the potential modes of failure for each unit. Each possible failure mode is then analyzed to determine the resulting performance of the system and to ascertain the *worst-case* effect that could result from a failure in that mode. All the identified items are then categorized according to the worst-case effect of the failure on the crew, the vehicle, and the mission.

Table 3-1 shows the FMEA/CIL criticality clas-

sifications, which are based on severity of effect. Items in the top four categories—Criticality 1, 1R, 2, and 2R—comprise a Critical Items List (CIL). Essentially, this is a listing of all hardware items and their failure modes which do not meet certain design and reliability requirements (related to safety) set for the Shuttle system by Level I management. Those requirements (specified in JSC 07700, Vol. I, Appendix A, para. 2.8) are as follows:

- "Redundancy requirements for all flight vehicle subsystems . . . [with specific exceptions] . . . shall be established on an individual basis, but shall be no less than fail-safe.
- "Redundant systems shall be designed so that their operational status can be verified during ground turnaround and to the maximum extent possible while in flight."

Therefore, in addition to single-point failures, the CIL also includes items that could fail in one mode and result in loss of the capability of redundant (backup) systems, items whose status is not readily detectable in flight, and redundant systems in which a single failure under certain conditions may result in loss of the total system capability.

Critical items with these failure modes must be subjected to design improvements or to corrective action to meet the fail-safe and redundancy requirements, before the Shuttle can fly with them present. If that is not feasible, a waiver request

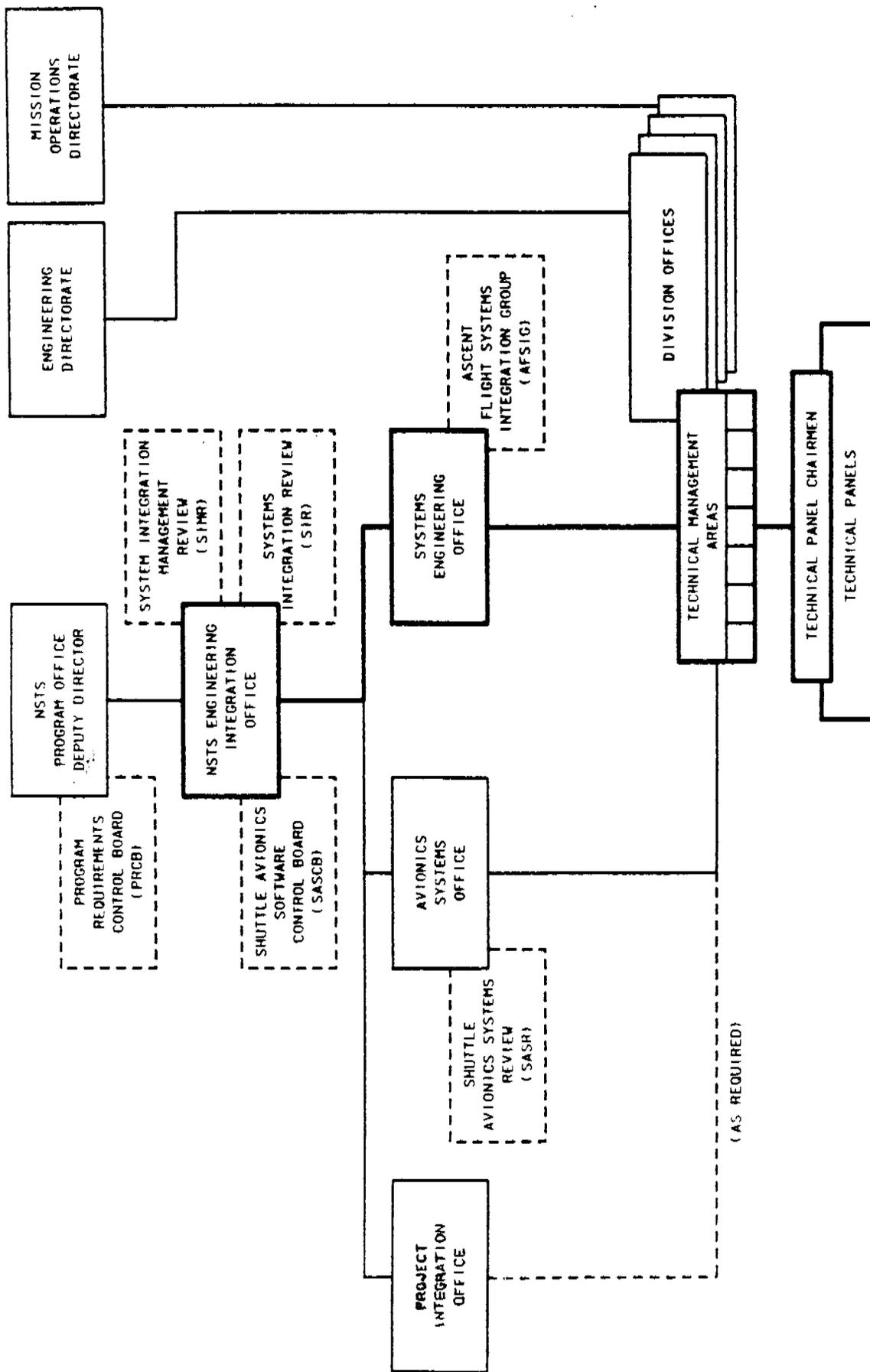


FIGURE 3-5 Organization and review structure of the National Space Transportation System Engineering Integration Office (NASA NSTS).

TABLE 3-1 FMEA/CIL Criticality Classification

Criticality Category	Potential Effect of Failure
1	Loss of life or vehicle
1R	Redundant hardware element, failure of which could cause loss of life or vehicle
2	Loss of mission
2R	Redundant hardware element, failure of which could cause loss of mission
3	All others
For Ground Support Equipment only:	
1S	Failure of a safety or hazard monitoring system to detect, combat, or operate when required and could allow loss of life or vehicle
2S	Loss of vehicle system

must be submitted to NASA management to present the rationale for retaining an item that does not meet the requirements. Types of data included in this “retention rationale” include design, test, and inspection data, failure history, and operational experience. Figure 3-6 shows an example of a CIL document, including the retention rationale.

An approved waiver must support the decision to accept the risk represented by the critical item and ensure that maintenance, test, or inspection procedures will minimize the potential for the failure to occur. Figure 3-7 depicts the review and approval process for critical items. Note that the key approval reviews are done by the CCB and PRCB review boards described in Section 3.2.2. After the PRCB meets, a directive is issued that documents items for which waivers have been granted and lists actions assigned by the Board. Each critical item, along with its approved waiver, is maintained by the NSTS Program, and any subsequent changes affecting the CIL must be approved by the NSTS Program Director.

The FMEA/CIL was originally conceived as a design tool, used to ensure the early identification and disposal of critical failure modes, as well as to support other reviews of the STS design. Since mission 51-L it is now also an operational and management tool, used for problem analysis, to assess the efficacy of corrective actions, to identify maintenance checkout requirements and inspection points, and to reflect trends in failure history.

3.4.2 Hazard Analysis

Hazard analysis is another analytical tool used to identify and, if possible, resolve hazardous conditions that could develop while operating and maintaining STS hardware and software. Hazard

identification is performed collectively by the NSTS engineering, safety, and operations organizations. Sources of information used to identify hazards include the FMEA/CIL, as well as various design reviews, safety analyses, crew procedures development, flight anomaly reports, and other sources. Hazard analyses thus consider not only the failures identified in the FMEA process, but also other potential threats posed by the environment, crew/machine interfaces, and mission activities. There are several different types of hazard analyses, as listed in Table 3-2. A typical Hazard (analysis) Report (HR) is shown as Figure 3-8.

Identified hazards and their causes are analyzed by Safety Division staff of the SR&QA offices at the NASA centers (and their contractors) to find ways to eliminate or control the hazard. A hazard is said to be “eliminated” when its source has been removed. A “controlled hazard” is one that has effectively been controlled by a design change, the addition of safety or warning devices, procedural changes, or operational constraints. Any hazard that cannot feasibly be eliminated or controlled by these means is termed an “accepted risk”, and requires review and approval by Level III and II management boards and their chairmen. SR&QA maintains a closed-loop tracking system for hazard documentation, resolution, and approval. The basic steps in hazard processing and review are depicted in Figure 3-9 and Figure 3-10.

Indicated in both of the latter figures is a Mission Safety Assessment (MSA). This is a report, prepared by the Safety Division for each STS flight mission, which provides an integrated and comprehensive assessment of all activities and hazards associated with a mission, including turnaround activities. It also provides a way to identify and “baseline”

SHUTTLE CRITICAL ITEMS LIST - ORBITER						
SUBSYSTEM	:LANDING DECELERATION	FMEA NO	02-1	-001	-1	REV:02/09/82
.ASSEMBLY	:MAIN LANDING GEAR	ABORT:				CRIT. FUNC: 1
.P/N RT	:MC621-0011					CRIT. HDW: 1
.P/N VENDOR:	1170100 MENASCO	VEHICLE	102	099	103	104
.QUANTITY	:2	EFFECTIVITY:	X	X	X	X
.	:LEFT HAND	PHASE(S)	PL	LO	OO	DO X LS
.	:RIGHT HAND					
.		REDUNDANCY SCREEN:	A-N/A	B-N/A	C-N/A	
.PREPARED BY:		APPROVED BY:		APPROVED BY (NASA):		
.DES	L L RHODES	DES		SSM		
.REL	A L DOBNER	REL		REL		
.						
.ITEM:	MLG STRUT					
.	MLG SHOCK STRUT INNER AND OUTER CYLINDER AND LOAD CARRYING MEMBERS.					
.FUNCTION:						
.	MLG LOAD CARRYING MEMBERS CYLINDER - DAMPER, WHERE A PASSAGE OF HYDRAULIC FLUID THROUGH AN ORFICE ABSORBS THE ENERGY OF IMPACT AND WHERE DRY NITROGEN IS USED AS THE ELASTIC MEDIUM TO RESTORE THE UNSPRING PARTS TO THEIR EXTENDED POSITION.					
.FAILURE MODE:	STRUCTURAL FAILURE					
.						
.CAUSE(S):						
.	STRESS CORROSION. PIECE-PART STRUCTURAL FAILURE. OVERLOAD.					
.EFFECT(S) ON	(A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:					
.	(A) LOSS OF SUBSYSTEM FUNCTION. (B) NONE. (C) NONE. (D) PROBABLE LOSS OF VEHICLE IF MAIN STRUT FAILS ON LANDING.					
.DISPOSITION & RATIONALE	(A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:					
.	(A) UNDER WORST CASE LOADING (FLAT STRUT) THE STRUT IS CAPABLE OF WITHSTANDING ONE LANDING AT THE NORMAL LANDING DESIGN GROSS WEIGHT OF 207,000 LBS. AND SINK SPEED OF 9.6 FEET PER SECOND WITH CORRESPONDING LANDING ROLLOUT AND BRAKING CONDITIONS, WITH NO YIELDING OF THE STRUCTURAL MEMBERS. (B) ACCEPTANCE INCLUDES VERIFICATION THAT CERTIFIED MATERIALS AND PROCESSES WERE USED. CERTIFICATION INCLUDES A FATIGUE LOAD TEST SPECTRUM (REF MC62-0011 TABLES 10-11) REPRESENTING THE EQUIVALENT LOADING FOR THE LIFE OF EACH LANDING GEAR WITH A SCATTER FACTOR OF 4.0. THE STATIC LOAD TESTS INCLUDED A TAXI BUMP (65K PAYLOAD), VEHICLE WEIGHT 227 KIIPS/AND A RIGHT TURN/WHICH IS THE WORST CASE CONDITIONS WITHOUT FAILURE. (C) DURING TURNAROUND-VISUALLY INSPECT FOR DAMAGE. USE NDE TO SPOT SUSPECT AREAS. AT MANUFACTURER-RAW MATERIAL VERIFIED-VISUALL INSP./ID PERFORMED-PARTS PROTECTION, COATING AND PLATING PROCESSES VERIF. BY INSPECTION.-MANUF., INSTL. AND ASSY. OPERATIONS VERIF. BY SHOP TRAVELER MIPIS-CORROSION PROTECTION PROVISIONS VERIF. NDE OF SURFACE AND SUB-SURFACE DEFECTS VERIF. BY INSPECTION. PROPERLY MONITORED HANDLING AND STORAGE ENVIRONMENT VERIFIED. MATL. AND EQUIPMENT CONFORMANCE TO CONTRACT REQMS. VERIFIED BY INSP.-FINDINGS VERIFIED BY AUDIT 9-25-78. (D) DURING DROP TEST PROGRAM, THE OUTER GLAND NUT FAILED. MENASCO REDESIGNED AND CHANGED FROM ALLUMINUM TO STEEL MATL. THE SNUBBER RING P/N 1170134-1 WAS REDESIGNED. UPPER BEARING 1170107-1 WAS REPLACED BY A SOLID ALLUMINUM-BRONZE BEARING.					

FIGURE 3-6 An example of a Critical Items List document (NASA).

hazards (i.e., to establish their “normal”—accepted—state or level) for future flights.

3.4.3 Element Interface Functional Analysis

Provision is made in NASA’s risk management process for checking cross-element interface failure modes and effects by a number of means. One method used is the Element Interface Functional Analysis, prepared by the NSTS Engineering Integration Office with the support of Rockwell International. EIFAs are analyses of various functional failure modes that can occur at element-to-element interfaces as a result of a hardware failure in either element. There are three EIFAs: Orbiter/ET, Orbiter/SSME, and Orbiter/SRB-ET. (A fourth EIFA,

on ground/flight systems, is now being generated.)

The purpose of these analyses is to correlate element hardware failures with failure modes at the element interface to determine the effect on the mission, vehicle, or crew safety. EIFAs also look for failure propagation across interfaces. The EIFA activity helps to ensure that FMEA items are correctly classified as to their criticality.

3.4.4 Other Analyses

Providing basic input to the hazard analysis is a diverse group of safety analyses. NHB 5300.4 (ID-2) describes these analyses as follows:

“Safety analyses are performed at the integrated and element (SIS) levels and down to the component level to assure

TABLE 3-2 Types of Hazard Analyses

Type of Analysis	Program Phase	Why Used
Preliminary Hazard Analyses	Concept/design and development	Allows top level hazard definition by generic hazard and lends itself to expansion as the program progresses.
Fault Tree Analyses	Concept/design and development/operations	Allows in-depth analysis of selected critical areas and relationships among events.
Sneak Analysis	Design and development phase (when detailed design available)/operations	Allows identification of latent nonfailure conditions that may allow undesired conditions or prevent desired conditions.
Software Hazard Analysis	Design and development phase/operations	Allows independent verification that software code implements approved requirement.
Operations Hazard Analysis	Design and development phase/operations	Allows identification of hazardous conditions during operations caused by such things as out-of-sequence operation, omitted steps, and interaction of elements.
Mission Level Hazard Analysis	Design and development phase/operations	Allows detailed analysis of mission events considering hardware, crew, ground operations, and software interactions.
Mission Safety Assessment	Design and development phase/operations	Allows assessment of previously conducted analyses for completeness and accuracy, provides analyses and provides visibility of hazards by mission phase and event.

(Source: NASA JSC)

identification of hazardous conditions, hazard causes, hazard effects, hazard levels, corrective actions, and rationale for hazard closure.”

An important subset of safety analyses are the systems safety analyses, defined as follows (in NHB 1700.1 (V3), System Safety):

“Systems safety analyses are performed for the purpose of identifying hazards and establishing risk levels . . . in support of this concept the analyses perform five basic functions:

- “a. Provide the foundation for the development of safety criteria and requirements.
- “b. Determine both whether and how the safety criteria and requirements provided to engineering have been included in the design(s).
- “c. Determine whether the safety criteria and requirements created for that design have provided for adequate safety for the system.
- “d. Provide part of the means for meeting pre-established safety goals.
- “e. Provide a means of demonstrating that safety goals have been met.”

Two other important safety analyses are the Integrated Hazard Analysis (IHA) and Critical Functions Assessment (CFA). The NSTS Engineering Integration Office, with the support of Rockwell International (the integration support contractor) produces an IHA when a potential risk situation or unsafe condition is perceived, the resolution of which involves two or more STS elements. These

analyses are reviewed by the System Integration Review Board (SIR), described earlier.

The CFA, a one-time effort completed in 1978, examined critical functions during each mission phase and identified hardware and software changes which would improve safety. The CFA included certain multiple and cascading failure combinations; it is currently being reexamined by Rockwell International to verify the results of the initial assessment and provide an update to the current STS configuration.

3.4.5 Overall Scope of Analyses

The various analysis techniques employed by NASA are intended to provide an all-encompassing approach to ensuring the design reliability and safety of the STS. Some of the techniques, principally the hazard analyses and EIFA, tend to be “top-down” approaches that examine certain cross-systems causes and effects. Others, such as FMEA/CIL, are narrower “bottom-up” analyses that pursue a specific event to its conclusion—but only with respect to the piece of hardware involved. In a briefing to the Committee, Rockwell International presented its view of this interaction, summarized in Figure 3-11.

The FMEA/CIL, EIFA, and other safety analyses feed into the various hazard analyses in a one-way flow culminating in the Mission Safety Assessment.

PHA NO. ORBI-024

SPACE SHUTTLE PRELIMINARY HAZARD ANALYSIS

MISSION PHASE: Prelaunch Through Landing ENGINEER: J. Rallsback

SUBSYSTEM OR OPERATION: Environmental/Consumables DATE: 07/15/86

EFFECTIVITY: All Flights SHEET 1 OF 3

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	HAZARD LEVEL	SAFETY REQUIREMENTS	HAZARD CONTROL
Loss of electrical power (total loss of Space Shuttle power).	Contamination of H ₂ or O ₂ system.	Loss of crew and Shuttle.	CA	<ol style="list-style-type: none"> 1. The cryogenic system is to be verified clean during acceptance and reverified each time system is opened for maintenance. 2. The GSE cryogenic supply is to be sampled to verify purity prior to each service operation. 3. Provide individual fuel cell contaminant detection. 4. Provide filters prior to each interface. 5. Materials shall be selected that are compatible with reactants. 	<ol style="list-style-type: none"> 1. Fuel cells were certified to operate at a specific level of purity during qualification testing. 2. Preload sampling of cryogenics and cleaning and sampling each time it is opened verifies contamination is controlled to within specifications. 3. -----

FIGURE 3-8 Excerpt from a sample Space Shuttle preliminary hazard analysis report (NASA).

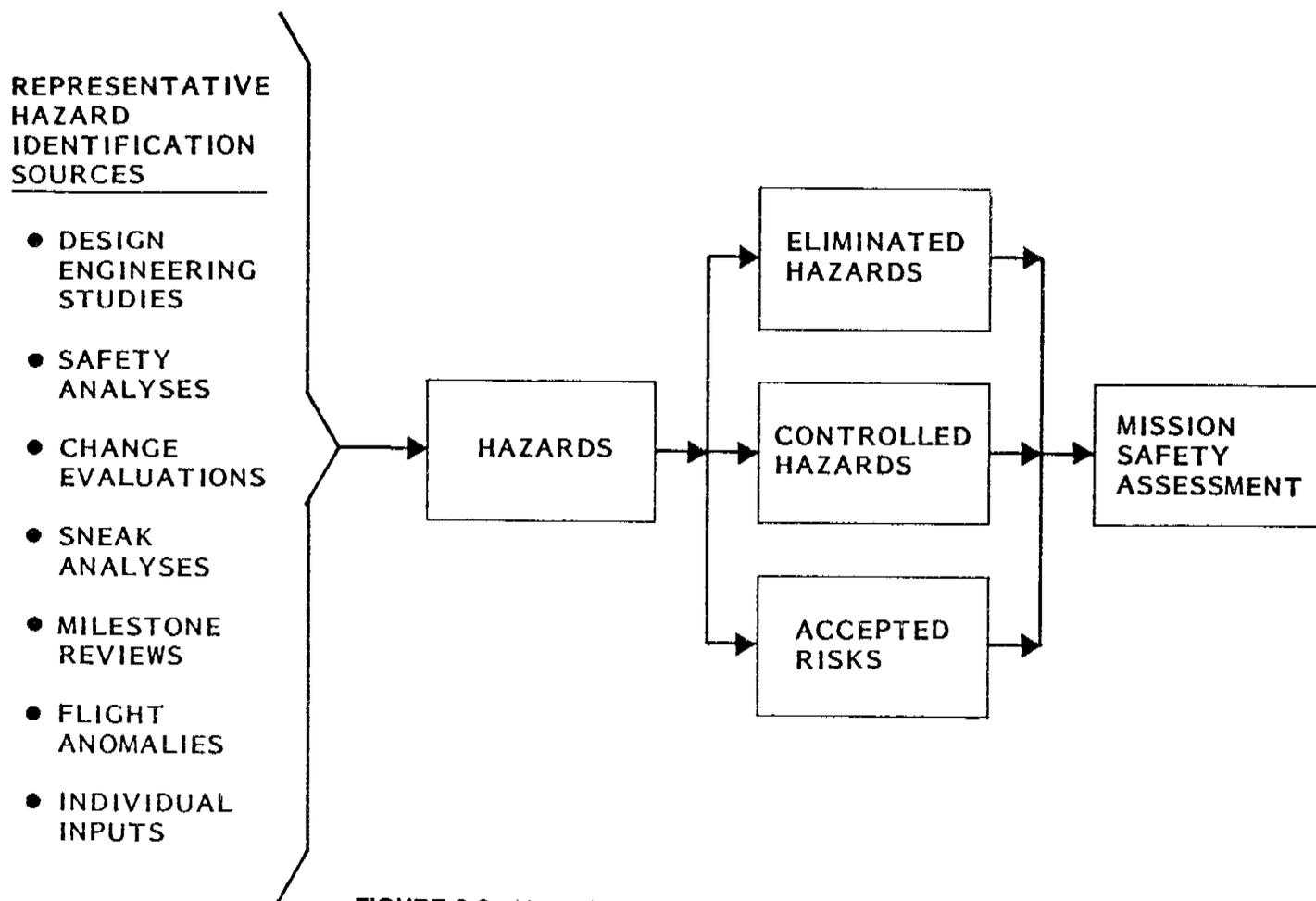


FIGURE 3-9 Hazard processing steps (NASA JSC).

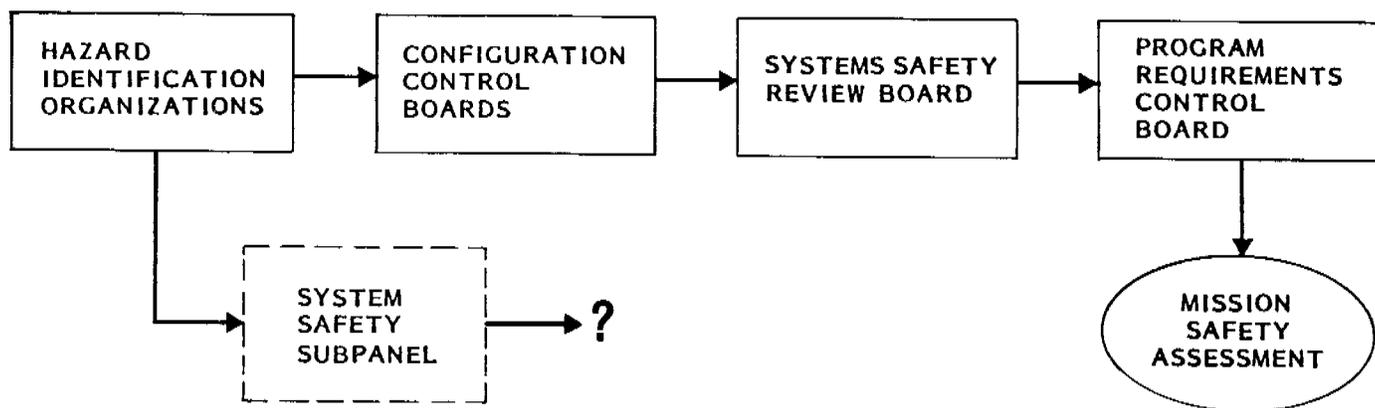


FIGURE 3-10 Hazard analysis review process (NASA JSC).

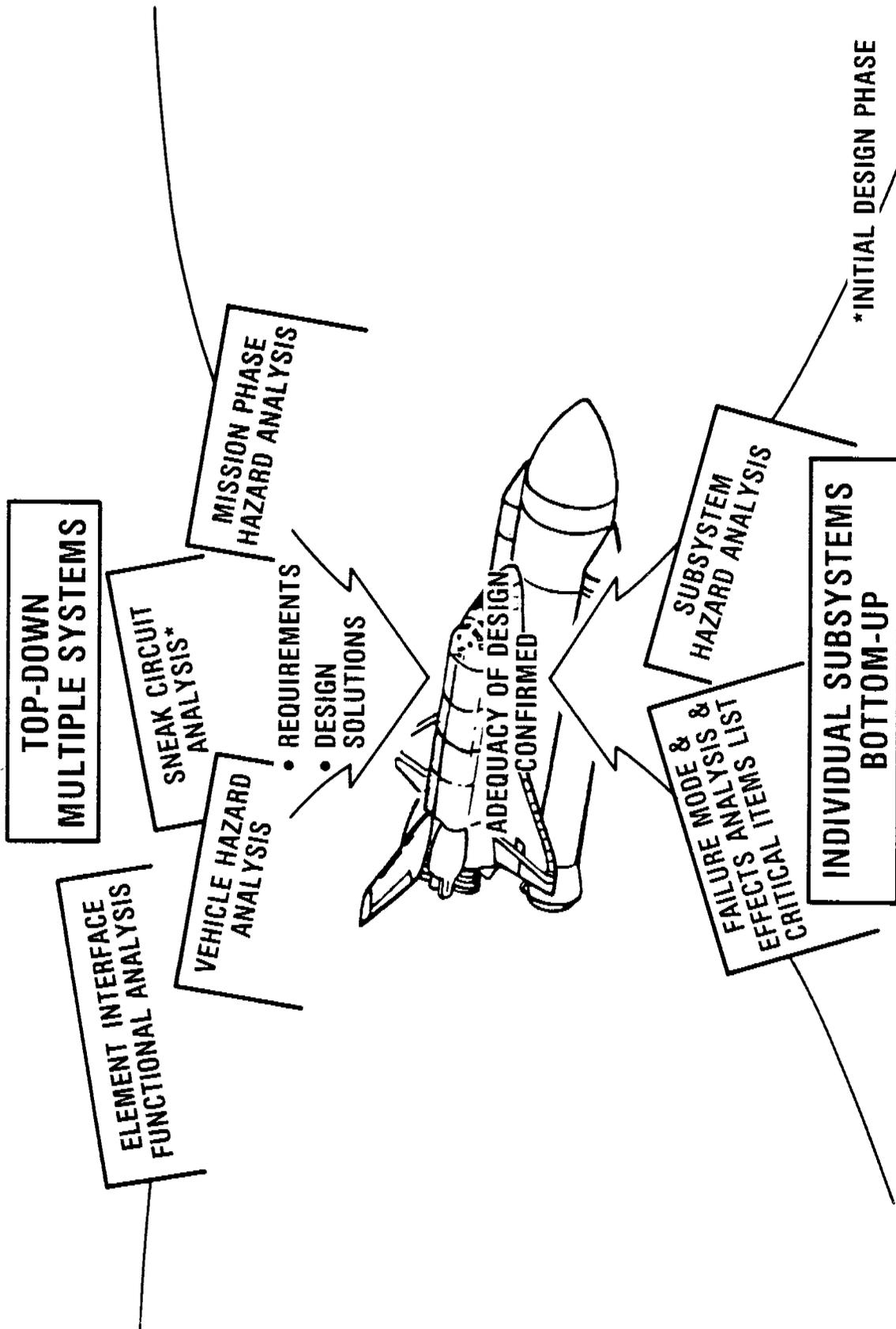


FIGURE 3-11 Interaction of top-down and bottom-up analysis techniques used in STS reliability and safety assessments (Rockwell STS Division).

TABLE 3-3 Critical Item Review Teams

Shuttle Element	Prime Contractor	Independent Review Contractor
Orbiter (JSC)	Rockwell International, STS Division	McDonnell Douglas Astronautics Co., Houston Division
External Tank (MSFC)	Martin Marietta, Michoud Aerospace Div.	Rockwell International, Space Transportation Systems Division
Solid Rocket Motor (MSFC)	Morton Thiokol, Inc., Wasatch Operations	Martin Marietta, Denver Aerospace Division
Solid Rocket Booster (MSFC)	United Technologies Corp., United Space Boosters, Inc.	Martin Marietta, Denver Aerospace Division
Space Shuttle Main Engine (MSFC)	Rockwell International, Rocketdyne Division	Martin Marietta, Denver Aerospace Division

(Source: NASA)

As a practical matter (as discussed in Sections 5.1 and 5.3) the FMEA/CIL, with its retention rationale, appears to be the dominant analysis, on which the waiver and some of the engineering change decisions are primarily based.

3.5 POST-51L REEVALUATION/REVIEW

3.5.1 NASA Management Directives

In March 1986, soon after the Challenger accident, direction was sent out from the Associate Administrator for Space Flight and the NSTS Program Director to the NSTS Project Offices to reevaluate (“re-review”) the FMEAs on all critical items on the STS. The Program Director described the purpose of the reevaluation as: “. . . to affirm the completeness and accuracy of the FMEA/CIL for the current National STS design.”⁸ Following reevaluation of the FMEA, each Criticality 1 and 1R item, along with any new items, or items for which the reevaluation had led to a change in classification, was to be resubmitted for review and approval of the waiver permitting the item to be flown aboard the STS. Authority for approval of these waivers resides at the Level I PRCB, with the NSTS Program Director having final sign-off authority.

Those items not revalidated by the review were required to be redesigned, certified, and qualified for flight. In addition to the FMEA/CIL reevaluation, the directives stipulated that the hazard analyses and EIFAs also be reviewed.

⁸ Memorandum of March 13, 1986.

3.5.2 Process

FMEA/CIL. Each NSTS project and its prime contractor carried out the FMEA/CIL reevaluation, usually doing two separate reviews. In addition, independent contractors not otherwise involved in working on that element were selected to conduct parallel reviews of the FMEA/CIL for each element and to report the results of their assessments to NASA’s review team. These independent reviews emphasized any analysis results that differed from those identified by NASA or the element prime contractor. The FMEA/CIL review participants are listed in Table 3-3.

The processing flow for the reevaluation initially varied somewhat from center to center, but was essentially like that shown in Figure 3-12 (from JSC). During the reevaluation, special effort has been directed to identifying design enhancements, operational and procedural checkout changes, or software additions that reduce the criticality and/or minimize the chance that the potential failure mode will occur.

The main difference between the re-review and the “normal review process” is the conduct of the independent reviews. Another significant difference is that the groundrules for determining Criticality 1 status were changed: FMEAs are now carried down to the individual component level (even where multiple identical components are involved), and pressure vessels (formerly excluded) are now included. These and other changes in procedure are specified in a new document, NSTS 22206, “Instructions for Preparation of Failure Modes and Effects Analysis and Critical Items List,” which

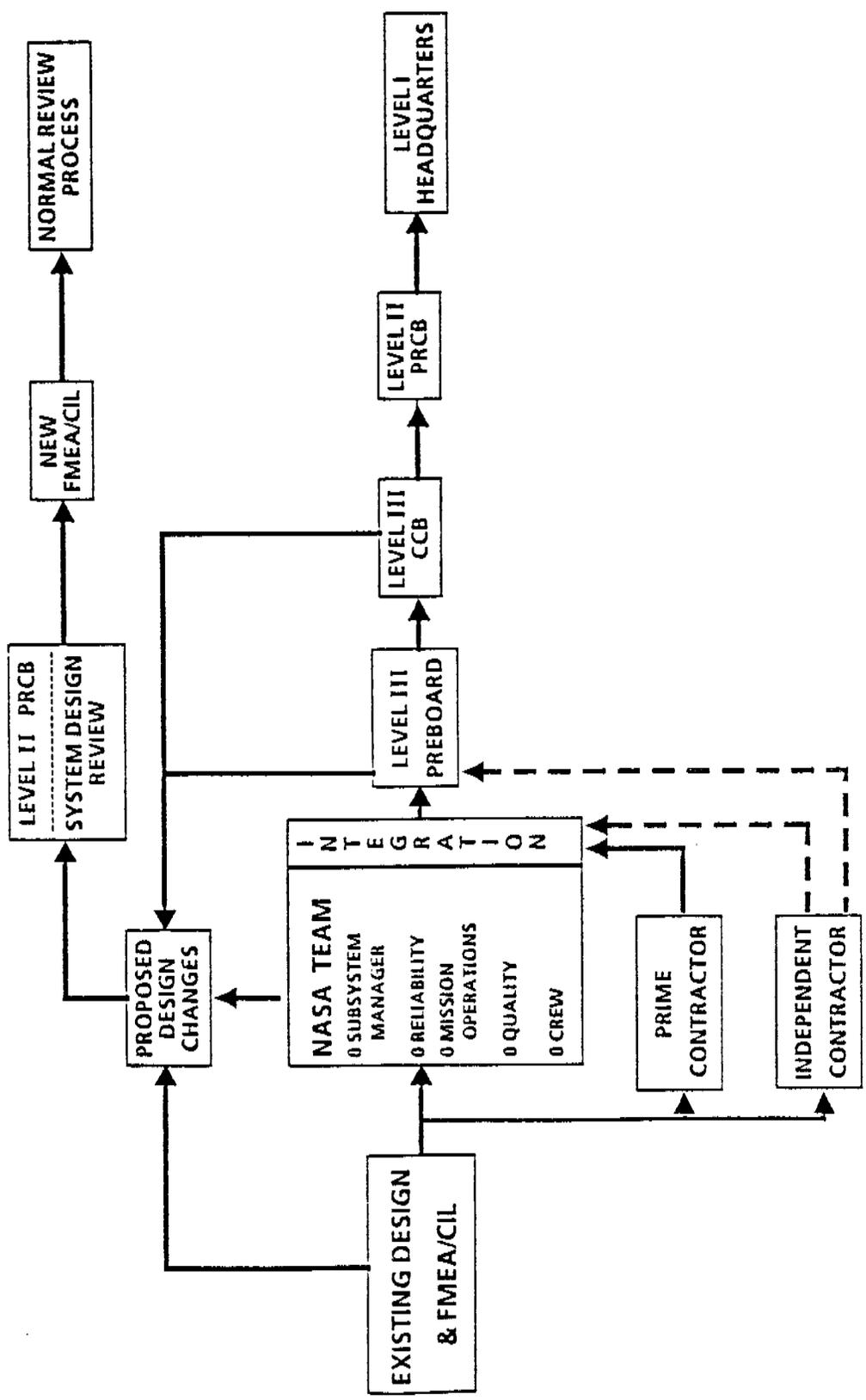


FIGURE 3-12 Typical processing flow for the current reevaluation of STS FMEA/CILs (NASA NSTS).

was issued in October 1986 to standardize the process across the program.

Hazard Analysis. A similar review of all element and integrated system-level hazard analyses is being undertaken in response to the Challenger accident. As in the case of FMEA/CIL, each project office, its prime contractor, and the independent contractor are evaluating all hazard analyses and Hazard Reports to verify their completeness and accuracy. Figure 3-13 illustrates the current review process.

Each hazard analysis assessment is being conducted in accordance with the guidance provided in a new document, NSTS 22254, "Methodology for Conduct of NSTS Hazard Analyses." This document defines the policy and procedures required for preparing hazard analyses, Hazard Reports, and Mission Safety Assessments.

The current review consists of a technical safety evaluation of the source material used for all analyses, studies, and investigations conducted from the beginning of STS flight. Each subsystem assessment is expected to ensure that all hazards have been identified, that dispositions are accurate, and that identified risks are acceptable.

3.5.3 Relation to Engineering Redesign Activity

Since the mission 51-L accident, a substantial number of engineering changes have been undertaken to improve Shuttle safety prior to resumption of flight. Shortly after the Challenger accident, groups representing various organizational elements of NASA (design centers, Astronaut Office,

etc.) presented the NSTS Program Director with lists of items which they considered as needing attention. All were Criticality 1 or 1R items. From these lists, a special Level II senior management PRCB known as the System Design Review Board recommended the selection of 90 items (consisting of hardware, software, and procedures) to undergo redesign, test, or analysis before the next flight of the Shuttle. Other items were categorized as near-term and "opportunity" actions. Since that time, the number of mandatory next-flight changes across the STS system has grown to 159.

The redesign activity has, for the most part, preceded the FMEA/CIL and hazard analysis reevaluations. Relatively few of the early items identified for next-flight change derived from the reevaluation activity. However, as the reevaluations proceeded they did disclose a number of items which are being worked before the next flight. FMEA/CILs and hazard analyses are being generated for all STS elements and modifications. The PRCB constitutes itself as the System Design Review Board to review all waiver recommendations on critical items.

3.5.4 Relation to Flight Readiness Process

The results of the various safety-related analyses feed into the flight review and readiness processes. By the time of the Design Certification Review (DCR), three months before launch, all FMEA/CIL waiver decisions, Hazard Reports, and the Mission Safety Assessment are available for review by the relevant readiness review boards.

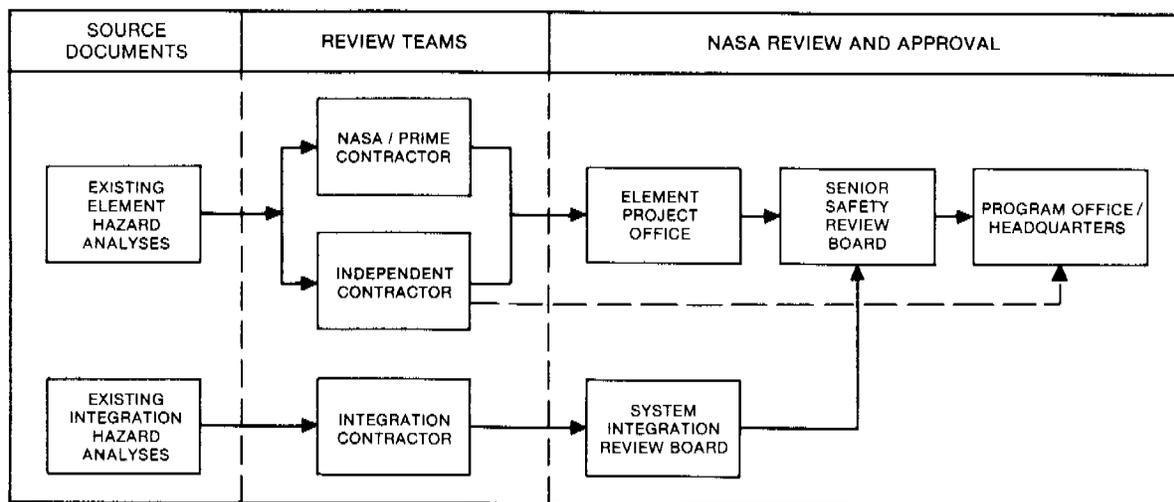


FIGURE 3-13 Steps in the current hazard analysis reevaluation process (NASA).

3.5.5 Data Input and Output

Among the most important types of data for use in developing and updating the CIL retention rationale and conducting hazard analyses is feedback from actual use of the hardware. STS equipment tests, preflight checkout, postflight inspections, and inflight operational experience and data are all crucial sources of this type of data. NASA uses a number of special reports and reporting systems to collect and integrate such data. They include the following, whose names are self-explanatory:

- Problem Reporting and Corrective Action (PRACA) System
- Problem Reports (PRs)
- Discrepancy Reports (DRs) [for software]
- Unsatisfactory Condition Reports (UCRs)
- Failure Reports

The PRACA system is a large, distributed data base (one for each STS element and one for KSC ground support equipment) that contains all of the reports listed above, along with data on corrective actions taken. PRACA is the basis for many design changes. Problems found in a postflight assessment are logged into the PRACA system at the design center for that element, and all problems are tracked by JSC/NSTS via a flight anomaly report, or Failure Report. The Failure Report is cross-correlated with the FMEA/CIL number.

Steps are being taken to ensure that the results of safety analyses are available to NASA managers in a more thorough and timely fashion. For example, NASA is setting up a closed-loop accounting and review system, by which all Criticality 1, 1R,

and 1S items are being tied to problem reports and their resolutions. This new System Integrity Assurance Program (SIAP), being developed under the NSTS Engineering Integration Office, is intended to ensure that STS flight and ground systems retain their design performance, reliability, and safety. It draws on the FMEA/CIL, hazard analyses, and other existing safety analysis systems.

A major component of the SIAP is its Program Compliance Assurance Status System (PCASS)—essentially a computer-based management information system. The PCASS will serve as a central data base integrating a number of existing information systems and sources across the NSTS. For example, the PRACA will be a part of it, facilitating the reduction and presentation of data on flight anomalies. It will provide in near real-time, to users such as the participants in Flight Readiness Reviews, an integrated view of the status of problems with the STS, including trends, anomalies and deviations, and closure information. One of the major advantages of PCASS is that it will give SR&QA staff an easy route of access into the entire system of data bases dealing with the STS. Eventually, it will provide automated information on critical item status and hazard data, with a computerized FMEA planned as one of the inputs.

NASA Headquarters SRM&QA is also planning an extensive system for the documentation, reporting, review, and assessment of safety information. The NASA Safety Information System (NSIS) and the Shuttle Hazards Information Management System (SHIMS)—an STS hazards data base—are two examples.

These input and output mechanisms provide the essential connectivity of the safety analyses to the continuing development, improvement, and operation of the STS within the NSTS Program.

4 Risk Assessment and Risk Management: The Committee's View

4.1 GENERAL CONCEPT

Almost lost in the strong public reaction to the Challenger failure was the inescapable fact that major advances in mankind's capability to explore and operate in space—indeed, even in routine atmospheric flight—will only be accomplished in the face of risk. The risks of space flight must be accepted by those who are asked to participate in each flight as well as by those who are responsible for the program. The Committee believes that the basis for NASA's acceptance of those risks should stem as much as possible from rationally derived criteria. This acceptance also should depend very heavily on the quality of the methodology and the degree of objectivity by which the risks are determined, as well as the rigor by which the risks are controlled (i.e., managed).

The Committee began its audit activities by focusing specifically on the FMEA, the CIL, and the hazard analysis process. However, very early in the data gathering phase it became clear that NASA's processes for analyzing failure modes, effects, and hazards could only be understood and evaluated intelligently when viewed as elements of an overall program of risk assessment and risk management. In the Committee's view, any such program should include the following basic elements:

1. A comprehensive method for identifying potential failure modes and hazards associated with the system.
2. A specific, quantitative methodology for identifying and assessing (or estimating) the safety risks of the system.

3. A risk management process by which the safety risks can be brought to levels or values that are acceptable to the final approval authority. Risk management includes:
 - establishment of acceptable risk levels;
 - institution of changes in system design or operational methods to achieve such risk levels;
 - system validation and certification; and
 - system quality assurance.

In this usage, we define a "safety risk" as the probability (likelihood or chance) of suffering a particular *consequence* of a failure mode, mishap, or hazard. For a large, complex system such as the STS, there is a set of system risks each of which is comprised of many contributing risks. Thus, we use the plural "safety risks" of the system, since one may choose to manage these risks to different levels.

There are actually two major functions present in the listing above. *Risk assessment* is comprised of the first two elements, identification and assessment of both the failure modes and hazards, and the safety risks associated with them. Risk assessment is or should be a staff function, the results of which are provided as input to management. *Risk management*, on the other hand (the third element above), must primarily be a line management function. Within NASA, SRM&QA at Headquarters and SR&QA at the centers are staff organizations. The Associate Administrator for SRM&QA reports to the NASA Administrator. Line management authority for NSTS extends from

the Administrator to the Level I Associate Administrator for Space Flight to the NSTS Program Director and thence through the Level II Program Office to the Level III project managers.

The concept of risk assessment and risk management is employed very explicitly within some private industries and public enterprises engaged in the engineering development of complex systems. The nuclear power industry is one such, and the commercial aerospace industry is another. Within the USAF Systems Command (including the Space Division, which develops military launch vehicles and spacecraft), risk assessment consists of a wide range of qualitative and quantitative tools, including the FMEA and hazard analysis. Risk management is viewed as a formal process involving the establishment, assessment, and control of risk to predetermined acceptable levels.

Figure 4-1 illustrates a generic type of program planning and tracking chart that is used in risk management by the USAF. Levels of risk in the system, as evaluated by a specific risk assessment methodology, are plotted against time (and the cost) to correct the problems contributing to risk. In this generic example, actual risk lags and exceeds the planned levels of risk for each category of risk, and throughout most of the program. The planned risk presents a target toward which the system risk is actively managed. The risk levels assessed at the conceptual design stage must eventually be evolved, through engineering, down to levels acceptable to the approval authority (i.e., high level, program line management). This is accomplished through a "systems safety engineering" function that is an integral part of the engineering design and development process from its inception.

4.2 NASA'S PROCESS: OVERALL COMMENTS

The fundamental view of risk assessment and management discussed above took shape over the first few months of the Committee's activities. It formed a framework within which the Committee could conduct the subsequent stages of the audit and more confidently evaluate NASA's STS safety program—of which the FMEAs, CILs, and hazard analyses are only a few important parts. Much of the remainder of this report reflects the results of our inquiry into specific aspects of the ways in which NASA assesses and manages risks in the NSTS program. But we believe it is important,

before plunging into specifics, to provide a sense of the "big picture" within which the Committee conducted its audit, and to give a general assessment of how NASA's current process (as described in Section 3) relates to that picture.

4.2.1 NASA Risk Assessment

NASA defines *risk* as: "the chance (qualitative) of loss of personnel capability, loss of system, or damage to or loss of equipment or property." [NHB 5300.4 (1D-2), p. a-4]

To identify potential failure modes and hazards, NASA uses input from many different sources: analyses, data gathering processes, design reviews, etc. Figure 4-2, obtained from the SR&QA Office at JSC, lists most of these sources for the NSTS. (However, the Committee is not aware of any FMEAs or hazard analyses being conducted on software.) If employed rigorously, these tools provide a good basis for achieving element 1 of the three specified in Section 4.1. However, this list of sources might more appropriately be titled "Identify Potential Failures and Hazards," because most of the activities listed do not deal with *risk*. For example, the failure modes analysis identifies possible hardware failure modes, but usually says little about the risk associated with each of them. When the effects analysis is added in, then part of the input needed to establish risk has been gained, but still nothing is inferred about the probability of occurrence of either the failure itself or the various possible effects that might result. A similar situation occurs in the identification of hazards.

One can categorize failure modes on the basis of the *consequences* of their worst-case effects, as is done in a very rough way in the Critical Items List, for failure modes whose worst-case effects lead (for example) to loss of life or vehicle. Such a categorization is useful for calling urgent attention to certain failure modes and their attendant hazards. Nevertheless, the listing of such items does not establish their contribution to the various *risks* of the system. In the NASA safety process, each item on the CIL has a retention rationale written for it. These retention rationale statements usually contain information which could, if used properly, contribute to a process for estimating the associated risk. However, the rationales appear to be used strictly as arguments for a waiver of the NSTS requirement that no single-point Criticality 1 or

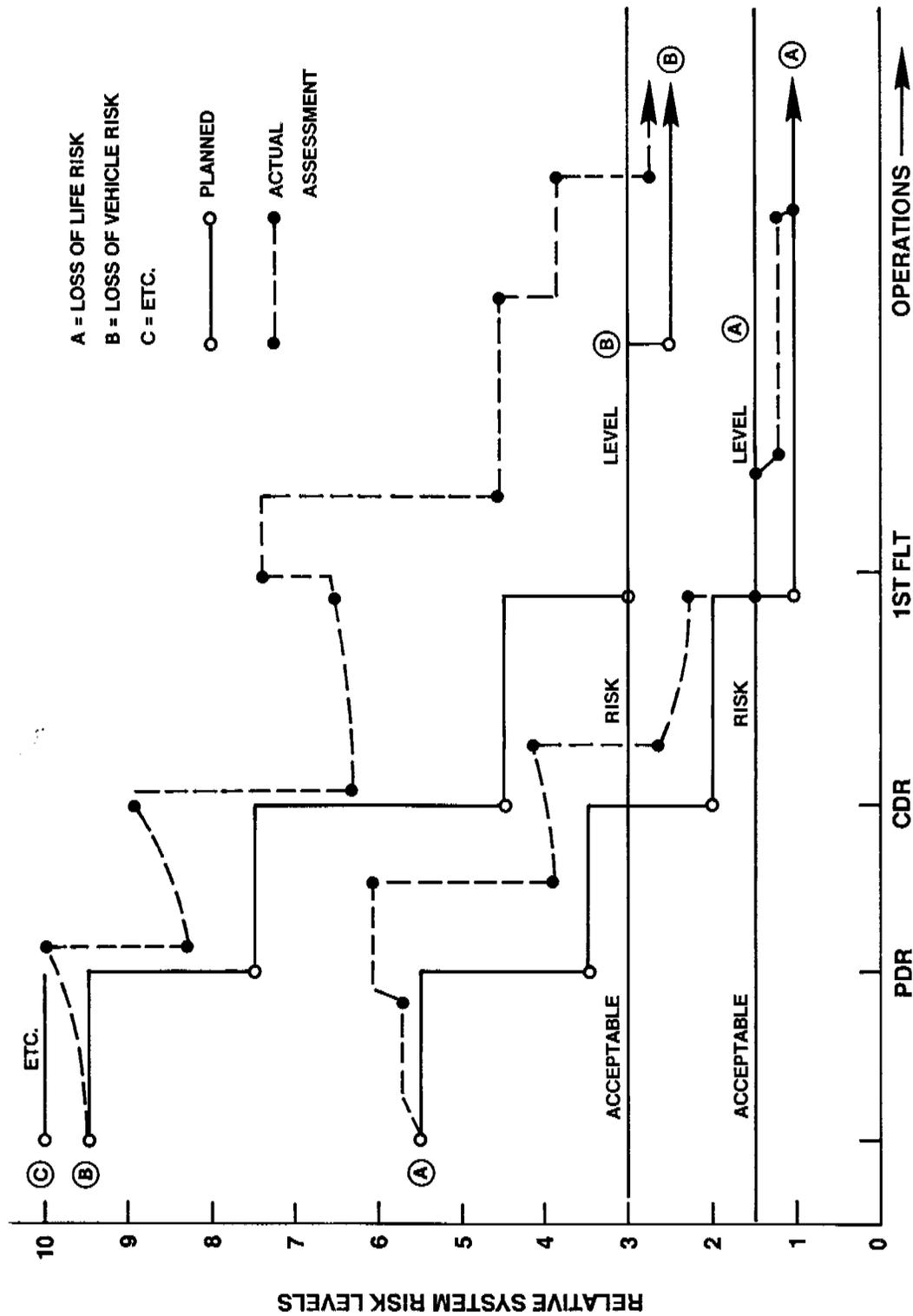


FIGURE 4-1 Conceptual diagram of risk management involving iterative steps taken to achieve specified levels of acceptable risk.

HAZARD ANALYSES	AEROSPACE SAFETY ADVISORY PANEL
DESIGN & ENGINEERING STUDIES	LESSONS LEARNED—OTHER PROGRAMS
DEVELOPMENT & ACCEPTANCE TESTING	ALERTS
SAFETY STUDIES AND ANALYSES	CRITICAL FUNCTIONS ASSESSMENT
FMEAs, CILs, & EIFA	INDIVIDUAL CONCERNS
CERTIFICATION TEST AND ANALYSIS	HOT LINE
SNEAK CIRCUIT ANALYSES	PANEL MEETINGS
MILESTONE REVIEWS	SOFTWARE HAZARD ANALYSIS
FAILURE INVESTIGATIONS	FAULT TREE ANALYSIS
WAIVERS AND DEVIATIONS	INSPECTIONS
WALK-DOWN INSPECTIONS	CHANGE EVALUATION
MISSION PLANNING ACTIVITIES	REVIEW OF MANUFACTURING PROCESS
SOFTWARE REVIEWS	HUMAN FACTORS ANALYSIS
ASTRONAUT DEBRIEFINGS AND CONCERNS	SIMULATIONS
OMRSD/OMI	PAYLOAD HAZARD REPORTS
FLIGHT ANOMALIES	REAL TIME OPERATION
FLIGHT RULES DEVELOPMENT	PAYLOAD INTERFACES

FIGURE 4-2 Techniques for the identification of potential sources of risk in the NSTS Program (after NASA JSC SR&QA).

1R failure modes be present when a mission is launched (see Sections 3.4.1 and 5.1).

Similarly, in NASA's hazard analysis process, hazards are categorized as to level and status. Hazards are defined as either critical or catastrophic, depending on whether or not there is time for any possible emergency action to be taken. Each "closed" hazard is categorized as being eliminated, controlled, or an "accepted risk." Rationales are written to justify accepting the uncontrolled hazards; many times the same rationale is employed that was used for retaining the critical failure modes (see Section 5.3 for elaboration). However, as in the case of the CILs, these justifications do not establish the *risk* levels of the hazards. Thus, although the term "risk assessment" is used in many different ways and places in NASA documents and presentations, the Committee found that nowhere was the total activity described that is needed to accomplish element 2 in Section 4.1 above (i.e., a quantitative methodology for assessing safety risks).

In NASA's definition of risk (above), the word "chance" is used as the measure (or basis of comparison) of the risk. The definition clearly implies evaluation of a set of risks based on the chance of occurrence of each of the various consequences described. However, NASA acknowledges, and our reviews have confirmed, that these "chances" are not formally or specifically estimated; nor are they documented. Rather, STS risks are assessed based on subjective judgments and the approval of *qualitative* rationales by various board and panel chairmen, and Level II and I authorities, as described in Section 3. However, many *quantitative* engineering analyses and test data relevant to risk assessment are available and often are used in arriving at what are finally qualitative subjective judgements. With such a non-specific (i.e., non-value based) risk acceptance process there is little basis for making objective comparisons of the several major risk categories associated with the STS, nor for carrying out risk evaluations by independent agencies. Neither can one systemati-

cally evaluate the results of efforts to reduce the risk of the various possible losses. **Without more objective, quantifiable measures of relative risk it is not clear how NASA can expect to implement a truly effective risk management program.**

4.2.2 NASA Risk Management

The various NASA documents identified in Sections 3.1 and 3.4, with some of their key provisions noted, basically describe a framework within which to operate an effective risk management program. At the core of such a program is the idea of risk management through the control of hazards. Residual hazards (risks) that cannot be designed away would be controlled at least to levels consistent with program objectives and cost constraints. The definition and analysis of hazards and levels of risk associated with a system and its operation was to be performed within a system *safety* function. Since the effective level of hazard control was not always expected to be perfect, a “residual hazard risk analysis” would be performed to provide the retention rationale for accepting such hazards and for continuing to operate (perhaps with constraints).

In parallel with and providing inputs to this system safety function is a *reliability* activity. This function was to be basically concerned with establishing a data base for selection of components which would meet allocated failure probability requirements; performing failure mode and effects analyses; establishing redundancy criteria and configuration definitions, maintainability criteria, and life limits; and preparing critical items lists containing items with single-point failure modes which could cause catastrophic results.

A third element in the overall safety and risk management program is *quality assurance*. This function, as defined by NASA, would be responsible for assuring that the hardware and software produced for the system was produced in a controlled way and met all requirements of the quality control criteria documents. This assurance role also includes supervision of personnel certification and establishment of non-destructive testing methods to detect flaws in components and non-conforming materials.

These functions provide the basic staff capability which line management can bring to bear on the management of risk in the NSTS Program. NASA’s own explicit view of risk management for the NSTS

was described to the Committee at JSC. It is conceived to be a synthesis of activities in four broad categories:

- Programmatic
- Engineering/development
- Mission operations
- Product assurance

As depicted in Figure 4-3, activities in all categories are conducted throughout all phases of the NSTS Program, from concept definition to flight operations. The risk management process is said to be characterized by top-down direction and control, with “bottom-up” response and accountability from the staff organizations and line management at the NASA centers. The process of risk assessment and management is described as one of “independent but integrated participation” by Program management, design/development (project engineering), operations (Astronaut Office and Mission Operations Directorate), and SR&QA. These terms are key: the degree of independence and integration of organizations and functions within the overall process comprise a major, recurring theme of the discussion presented in the following Section 5.

4.3 SUMMARY

The basic organizational elements are in place within NASA for assessing and managing risk; however, there is a need for a change in the scope of functions and the way that they are carried out. Certain shortcomings in process and methodology exist which are discussed in the following section. In particular, there is a fundamental problem in the nature of and the methods used to develop the overall assessments on which NASA line management bases its decisions about how to reduce and control risk in the STS. Also, it appears to the Committee that there is no clear, formal, and *rigorous* view among NASA line managers—at least on any consistent basis—of the nature and goals of risk management.

To reiterate what was said earlier, the Committee believes that risk management for any system involving complex engineering must be the responsibility of line management—i.e., (in the case of the NSTS) the system Program Manager, the Associate Administrator for Space Flight and, ulti-

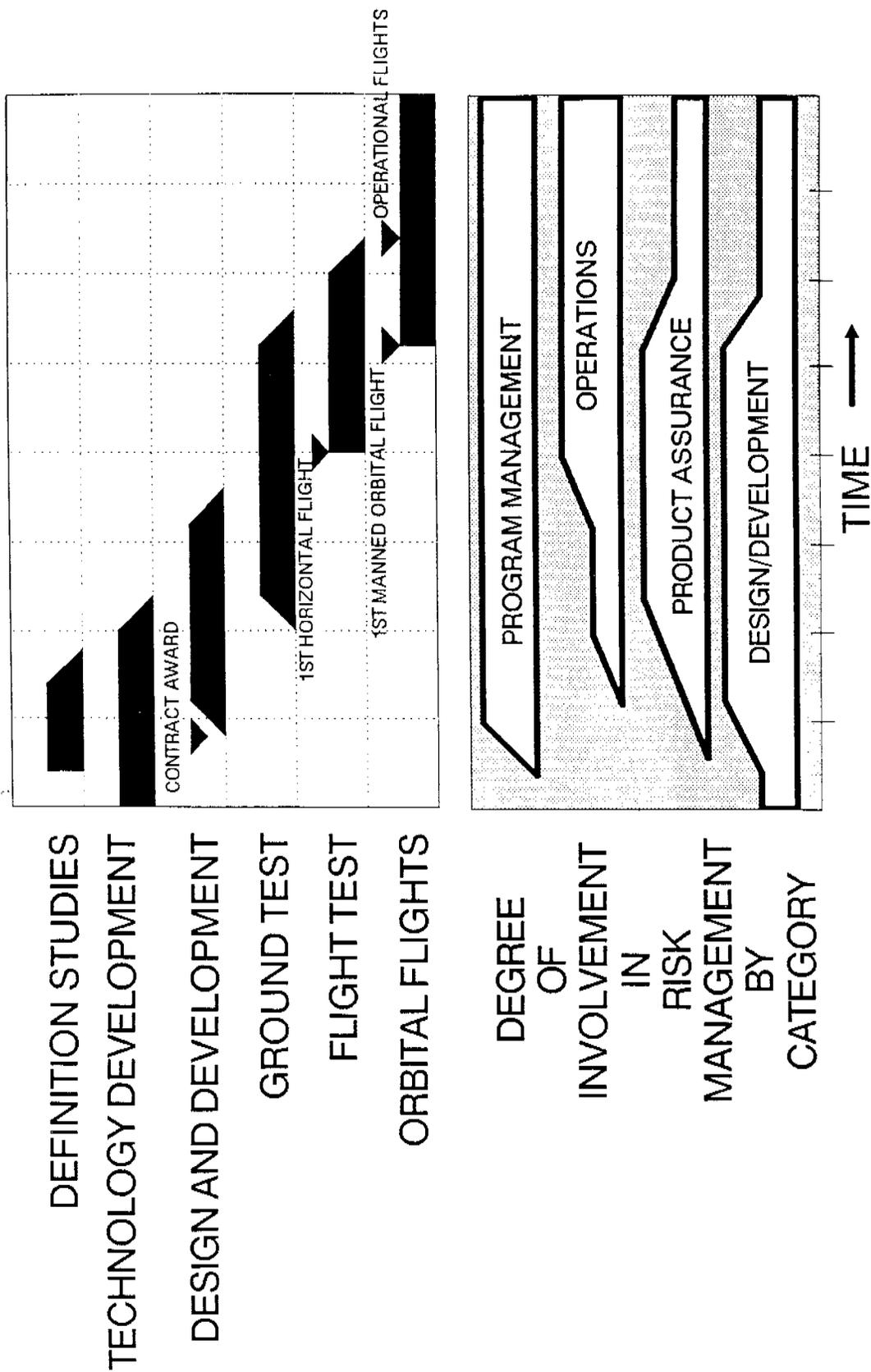


FIGURE 4-3 Phases in the Space Shuttle program and the degree of involvement in risk management in each phase (NASA JSC).

mately, the Administrator of NASA. Only this program management, not the safety organizations, can make judicious use of the means available to achieve the operational goals while evolving the safety risks down to acceptable levels, as described earlier. The safety organizations at NASA centers and Headquarters are staff organizations—i.e., they can and should be responsible for providing the assessments of the system's risks. They should also

be responsible for assuring that the activities associated with controlling the risks to the levels assessed have been carried out and documented. Safety organizations cannot, however, assure safe *operation*; they can only assure that the safety risks have been evaluated by approved, proper, rigorous, quantitative, and objective methods, and that the system configuration and its operation are being controlled to those risk levels.

5 National Space Transportation System Risk Assessment and Risk Management: Discussion and Recommendations

5.1. CRITICAL ITEMS LIST RETENTION RATIONALE REVIEW AND WAIVER PROCESS

The Committee views the NASA critical items list (CIL) waiver decision making process as being subjective, with little in the way of formal and consistent criteria for approval or rejection of waivers. Waiver decisions appear to be driven almost exclusively by the design-based FMEA/CIL retention rationale, rather than being based on an integrated assessment of *all* inputs to risk management. The retention rationales appear biased toward proving that the design is "safe," sometimes ignoring significant evidence to the contrary.

Although the Safety, Reliability, and Quality Assurance (SR&QA) organizations of NASA collect, verify, and transmit all data related to FMEA/CIL and hazard analysis results, the Committee has not found an independent, detailed analysis or assessment of the CIL retention rationale which considers all inputs to the risk assessment process.

As set forth in the NASA documents identified in Section 3.1, both the performance of the Failure Modes and Effects Analysis (FMEA) and the identification of critical items are intended to be carried out under the aegis of the reliability function. In principle, the FMEA should be both a design tool to provide an impetus for design change, and a tool for the evaluation of the final configuration in order to define the necessary control points on the

hardware. The identified critical items would require supporting retention rationale and waivers as appropriate in order to be included in the overall as-flown system configuration. How this retention rationale was to be generated, who developed it and who evaluated it against what safety criteria became crucial questions for the Committee's review of the whole process.

According to prescribed procedures, the hazard analyses being performed by the safety function of SR&QA, and the FMEA and CIL identification performed by the reliability function, were to come together in the generation of Mission Safety Assessment (MSA) reports which would contain analyses and justification of the retention rationale for the critical items and their associated "hazards", as well as a safety-risk assessment of the resulting units, subsystems, and systems. The hazard analysis and Mission Safety Assessment parts of this overall safety and risk assessment process as it was supposed to be done prior to 1986 are shown in Figure 5-1, obtained from JSC's SR&QA.

As Figure 5-1 indicates, according to specified NASA procedure the CIL retention rationale is to be used as one of many inputs to the more comprehensive hazard analysis. In reality, however, the hazard analysis is often simply a derivative of the CIL and its retention rationale, and is not used as a major basis for waiver decisions. Examination by the Committee showed that often these retention rationales were simply discussions of the hardware's specifications, design, and testing. They were generated primarily by the functional development engineers responsible for the design. They are intended to be justifications, and do not, in our

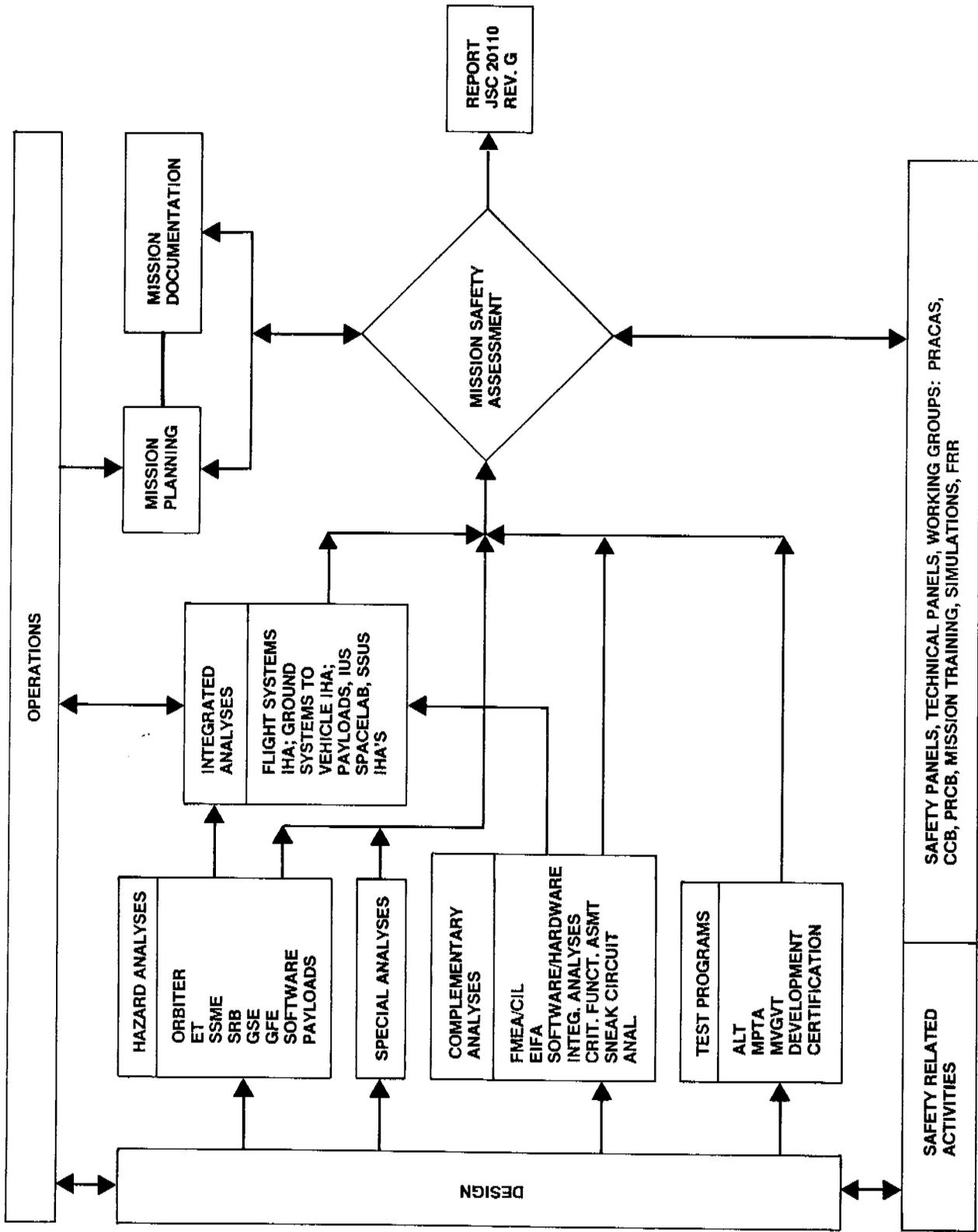


FIGURE 5-1 Hazard identification and documentation activities for STS as prescribed by NASA policy prior to the Challenger accident (NASA JSC SR&QA).

view, provide a true assessment of the risk of the hazards.

Sometimes the rationale appears to be simply a collection of judgments that a design should be safe, emphasizing positive evidence at the expense of the negative, and thus does not give a balanced picture of the risk involved. For example, the CIL retention rationale of December 1982, for the Solid Rocket Motor (SRM) indicated in support of retention that: there had been no failures in three qualification, five development, and ten flight motors; there had been no leakage in eight static firings and five STS flights; 1076 Titan III joints (presumably of similar design) were tested successfully; etc. Missing from the retention rationale was, among other points, any discussion of the dissimilarities between the SRM and Titan III (e.g., insulation design and combustion pressure on the O-ring); the O-ring erosion observed in the Titan III program and on the second STS flight; a failure during an SRM burst test; and, since the rationale was not updated, all of the O-ring anomalies seen after December 1982. Furthermore, in many cases we reviewed:

- No specific methodology or criteria are established against which these justifications can be measured.
- The true margins against the failure modes often are not defined or explicitly validated.
- The probability of the failure mode is never established quantitatively.
- Design “fixes” are accepted without being analyzed and compared with the configuration they are replacing on the basis of relative risk.

The point is worth reiterating: **The retention rationale is used to justify accepting the design “as is”;** Committee audits of the review process discovered little emphasis on creative ways to *eliminate* potential failure modes.

Since 51-L, there has been a major increase in the attention and resources given to STS SR&QA and risk assessment and management functions at all levels of NASA and its contractors. In 1986, NASA appointed an Associate Administrator at Headquarters for Safety, Reliability, Maintainability, and Quality Assurance (SRM&QA) and charged him with establishing a NASA-wide safety and risk management program. To implement this program, policy directives are being developed relating to

various procedures and operational requirements. Specific instructions and methodologies to be used in the conduct of various analyses and assessments, such as hazard analyses, are being developed. Independent institutional assessments and audits will be made of SR&QA activities and technical effectiveness at each NASA center.

Some important elements of this revamped NASA safety program—including hazard analysis and mission safety assessment—are depicted in Figure 5-2, which was obtained from the JSC SR&QA organization in May 1987. Several things shown in the figure should be noted. First, there is now a specific new set of NSTS instructions to all contractors and NASA organizations for conducting hazard analyses, and for preparing FMEAs and CILs for the NSTS (these new instructions affect the activities in the boxes in Figure 5-2 marked *). Second, it can be seen that the FMEA/CIL documents are intended to be one of many inputs into the hazard analysis and Hazard Report, which in turn are shown as an input into the Mission Safety Assessment.

However, since (as discussed in Section 4.2) the Hazard Reports do not provide a comprehensive risk assessment, nor are they even required to be an independent evaluation of the retention rationale stated in the CILs, the Committee believes that NASA plans—at least for the near term—to continue using the retention rationale of the CILs directly and individually as the basis for Criticality 1 and 1R waiver justifications to Levels II and I. We have indicated this by adding the Criticality 1 and 1R waiver path within the dashed lines on the left side of Figure 5-2. The current plan is to take the critical item waiver requests to the PRCB and Level I via a data package prepared by JSC SR&QA. It is our impression, however, that most of the arguments in this data package will still basically be those contained in the original CIL retention rationale. **Thus, we see too little in the way of an independent detailed analysis, critique, or assessment of the risk inherent in Engineering’s rationale.**

Since mid-1986, NASA and its contractors have been performing a massive rework of all STS program FMEAs, updating the resulting CILs, and reviewing all prior HAs. This new FMEA/CIL effort has had value in identifying new failure modes that were missed earlier or introduced through past changes, and those resulting from new changes made mandatory before next flight. However, the new NSTS instructions for preparing FMEA/CILs

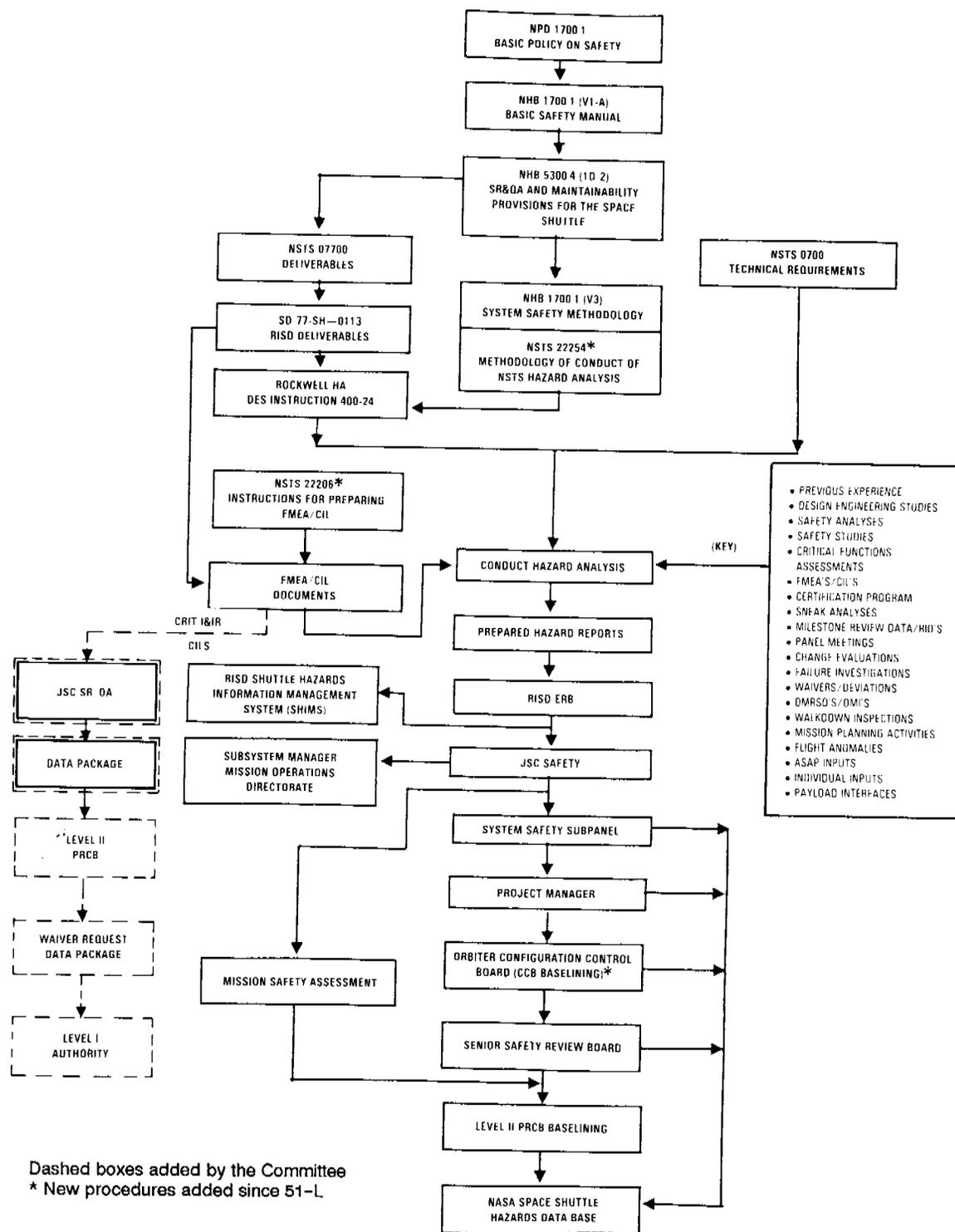


FIGURE 5-2 NASA JSC safety analysis, hazard reports, and safety assessment process in 1987, as modified by the Committee (adapted from NASA JSC SR&QA).

(NSTS 22206) have also resulted in a large increase in the number of Criticality 1 and 1R items. The Committee believes this new complexity will pose additional severe problems for both the mechanics and credibility of the CIL and waiver processes.

The strong dependence on the CIL retention rationales in waiver decisions makes it critical that they be comprehensive and up to date. It is not clear to the Committee whether, in the pre-51L environment, changes in the STS configuration or

the operational experience base led directly and surely to review and appropriate updating of the relevant CIL retention rationale. In the wake of the 51-L accident, the NSTS program issued a document (NSTS 22206) which is intended to strengthen the process for updating the retention rationale. Once a retention rationale has been accepted and a waiver granted for a critical item, any changes to the item itself, the FMEA, or the CIL that could affect the retention rationale mean that the CIL must be resubmitted to the Level II/PRCB for its approval (NSTS 22206, p.2-7, para.2.2.6). Any change, whether it be to the test environment, level, procedures, methods, or frequency, is to be reflected in changes to the retention rationale. If crew procedures are changed to reduce risk, corresponding changes are also to be made in the retention rationale.

The question is whether this updating is conducted regularly and in a consistently rigorous fashion. Although this policy is new and may not yet have been fully imposed in all quarters, NASA and contractor personnel interviewed by the Committee seemed variously uncertain about or unaware of these requirements and how they are met. **Updating the retention rationale seems to many to be considered a routine bookkeeping chore, of secondary importance, yet these rationales are the primary basis for granting waivers.**

During its audit the Committee developed a concern that the FMEA and associated retention rationale on a given critical item may sometimes fail to provide data in various important categories of information, such as the effects of environmental parameters. The lack of data in a certain case may or may not be significant with respect to the threat that item represents. Yet the absence of such data, even though it resulted in uncertainty, in the past has sometimes had the effect of bolstering the rationale for retention and providing unwarranted confidence in readiness reviews. This problem was especially in evidence with Mission 51-L. Data suggesting that temperature was a factor in the erosion of the O-rings did exist, but (according to the Rogers Commission) the relevant analyses apparently were considered to be inconclusive by those responsible, and these data did not appear in the retention rationale. Thus, the rationale implied that there were no data to suggest that temperature was a problem. Strengthening and closing the problem reporting loop since the accident may well reduce the likelihood of similar

future occurrences. Still, we note that the “negative answer” indicates uncertainty about the issue at hand. If the uncertainty is crucial to the decision process, then it implies the need for more experiments, tests or analyses to reduce the uncertainty. (Appendix E includes an analysis of the O-ring temperature effect and the uncertainty implied by extrapolation to low temperatures.)

Thus, the Committee’s central concerns here are the reliance on and quality of the retention rationale, and the fact that we can perceive no documented, objective criteria for approving or rejecting proposed waivers. CIL waiver decision making appears to be subjective, with no consistent, formal basis for approval or rejection of waivers. All items are considered and discussed at length during the CCB and PRCB reviews. It appears that, if no action item is generated as a result of the review, the critical item waiver is approved. There was no formal “approved or disapproved” step in meetings audited by the Committee, although we are informed that such approvals do appear in the minutes of the meetings. NASA managers emphasize that Level III engineers and their “Level IV” contractors are accorded a high level of responsibility and accountability throughout the program, and that their opinions and analyses are the real bases for making retention decisions; these engineers bear the burden of proving that the rationale is strong enough to justify retention and waiver of the item.

However, the Committee believes that engineering judgment on these matters is not enough. Such judgment is crucial, but it is often too susceptible to vagaries of attention, knowledge, opinion, and extraneous pressures to be the sole foundation for decision making. We are concerned that, for all the reasons discussed above, without professional, detailed evaluation against specific criteria for reducing risk (not just review by panels and boards), the retention rationales can be misleading or even incorrect regarding the true causes and probabilities of the failure modes for which retention waivers are being requested (see discussion of probabilistic risk assessment in Section 5.6).

Recommendations (1):

The Committee recommends that NASA establish an integrated review process which provides a comprehensive risk assessment and an independent evaluation of the rationale justifying the retention

of Criticality 1/1R and 2/2R items. This integrated review should include detailed consideration of the results of hazard analyses and all other inputs to the risk assessment process, in addition to the FMEA/CIL retention rationale. Further, the review process should assure that the waivers and supporting analyses fully reflect current data and designs. Finally, NASA should develop formal, objective criteria for approving or rejecting critical item waivers.

5.2 CRITICAL ITEMS LIST PRIORITIZATION AND DISPOSITION

At present, in NASA instructions all Criticality 1 and 1R items are formally treated equally, even though many differ substantially from each other in terms of the *probability* of failure or malperformance, and in terms of the potential for the worst-case effects postulated in the FMEA to be seen if the particular failure occurs.

The large number of Criticality 1 and 1R items at the time of the 51-L accident has since been *substantially increased* due to changes in ground rules for classification and the complete reevaluation of the entire STS.

The Committee believes that giving equal management attention to all Criticality 1 and 1R potential failures could be detrimental to safety if, as is the case, some are extremely unlikely to occur, or if the probability is very low that the postulated worst-case consequences of the failures will result. Treating all such items equally will necessarily detract from the attention senior management can give to the *most* likely and *most* threatening failure modes.

Critical items in the Shuttle system are categorized according to the consequences of worst-case failure of that item. However, it has been the case that within each criticality category no further ranking is formally made. In practice, managers do sometimes discriminate within a category, e.g., in their decisions regarding those STS items which should be fixed prior to next flight. Prior to the 51-L accident there were already 2369 Criticality 1 and 1R items (the most critical) present in the Shuttle system. There has been a substantial in-

crease in the number of such items, now estimated by NASA to be 4686, of which 2148 have been approved by the PRCB (Director, JSC/SR&QA, personal communication, November 10, 1987). This increase resulted from the reevaluation of the entire Space Shuttle system and the new ground rules specified for the preparation of FMEAs—e.g., the carrying of analyses down to the individual component level (even where multiple, identical components are involved) and the inclusion of pressure vessels which were formerly excluded (see Section 3.5.2). To take just one example, the number of Criticality 1 and 1R items in the SSME turbomachinery rose from 8 to 67 under the new ground rules. In view of this problem, NASA is now taking steps to prioritize the most critical items and will reevaluate the current scheme for defining levels of criticality.

Initially, the reassessment process seemed to the Committee to be too heavily focused on Level I. The presence of a very large number of Criticality 1 and 1R items—even admitting that many are clustered with identical items—obviously places a heavy demand on the time and attention of key NASA decision makers and could prevent their penetrating deeply enough into the analyses surrounding each item to make a valid decision on all of them. We were concerned not only about the workload placed on Level I management, but also about the danger that crucial technical details might be lost or obscured as the rationale for retention was presented at successively higher levels. Although the same information is presented at the Level II and I PRCBs, it seemed entirely possible that technical debates occurring at lower levels might not be adequately relayed to Level I.

A post-51L organizational change that shifted the Level II NSTS Program Director at JSC to Level I at Headquarters has alleviated these concerns to some extent. NASA recognized that the waiver decision-making flow was not ideal—especially from Level II to Level I. Consequently, the Level I NSTS Director (who also chairs the Level I PRCB) now participates in the Level II reviews as a basis for sign-off at Level I. Thus, there is now a more direct “hand-off” of concerns and rationales from Level III to Level I, via Level II. Nevertheless, the process still places a heavy workload on Level I, and there is still a danger that important technical information might be lost in transmission.

The organizational change streamlined the waiver decision-making process, but it did not help in

handling the large number of Criticality 1 and 1R items. Many of these items differ substantially from each other in terms of the *probability* of failure or malperformance, and in terms of the possibility that the worst-case effects postulated in the FMEA will be seen in the event the particular failure does occur. (In this connection it might be noted that, prior to 51-L, 56 Criticality 1 failures occurred on the *Orbiter* during flight without any of the postulated worst-case effects resulting.) Thus, the items vary considerably in their potential impact on Shuttle operational safety—i.e., on risk.

Early in its audit the Committee began urging NASA to find a way to prioritize the Criticality 1 and 1R items (see Appendix C, first interim report). NASA managers tended to assert that, since all Criticality 1 and 1R items are (by definition) equally catastrophic in their consequences, all should be treated equally—and, indeed, we saw evidence in our audits that they were handled with equal attention. But it is the position of the Committee that giving equal management attention to all such items could be detrimental to safety if (as is the case) some are extremely unlikely to fail, or the probability is very low that the postulated worst-case consequences of the failures will result. **The most likely and most threatening failure modes merit the most attention. It is illogical to dissociate the probability of an event or its consequences from decisions about the management of risk.**

For example, in the development of a probabilistic risk assessment for a modern nuclear power plant, fault tree and event tree analyses typically identify several million potential sequences of events (including multiple independent failures and cascading failures) that can lead to core melt-down. However, only 20 to 50 of these sequences contribute significantly to the risk, with five to ten of them contributing 90% of the risk. These particular sequences are exhaustively analyzed to identify ways to substantially reduce the overall risk.

A secondary consideration of the Committee was the possible impact of the disclosure that, as the resumption of Shuttle operations nears, there are more Criticality 1 and 1R items (with all of them being waived) than there were before the accident. That perception would not be justified by, and would not fairly reflect, the real strides in system safety that have been made since 51-L.

Responding to suggestions on the part of the Committee, NASA developed and tested a number of techniques that could be used to prioritize the

CIL on the basis of the relative risk each item represents. One such scheme—termed the Critical Item Risk Assessment (CIRA) procedure—was selected and instructions for its implementation have now been promulgated throughout the NSTS program (NSTS 22491, June 19, 1987).

The CIRA procedure is currently qualitative in nature—although it employs reliability and test data to some extent. It is based instead on judgments about the *degree* of threat inherent in different risk factors. The Committee is concerned about the potential negative impact on the CIRA of ambiguous measures of risk and probability. However, the technique does lend itself to the incorporation of more rigorous quantitative measures of risk and probability of occurrence as these measures are developed for use within NASA. (See Appendix E for a discussion of CIRA and one approach to quantitative measures suggested by the Committee.)

Current plans for the implementation of CIRA, spelled out by the NSTS Deputy Director (Program) in a memorandum dated July 21, 1987, are for STS project managers to prioritize the Criticality 1, 1R, and 1S items in each project *after* completing the FMEA/CIL reevaluation and presenting the CIL at the Level III CCB. By two weeks before Design Certification Review, each project manager will provide the NSTS Deputy Director (Program) with a list of “the 20 items in his project that represent the greatest risk to the program.” The Deputy Director will then compile and distribute a report. This assessment effort will run parallel to, and may not actually affect, the preparations for STS-26 (the next scheduled Shuttle flight). However, “an alternate course of action” may be chosen for subsequent missions. The Committee views this implementation procedure with concern. It does not appear to reflect a serious concern on the part of the NSTS Program for the need to prioritize the CIL by assessing relative risks.

Recommendations (2):

The Committee recommends that the formal criteria for approving waivers include the probability of occurrence and probability that the worst-case failures will result. We further recommend that NASA establish priorities now among Criticality 1 and 1R items, taking care not to use ambiguous measures of risk and probability. NASA should also modify the definitions of criticality in

terms of the probability of failure and probability of worst-case effects. Finally, we recommend that NASA Level I management pay special attention to those items identified as being of highest priority, along with the rationale that produced the priority rating. Responsibility for attending to lower-priority items within the present Criticality 1 and 1R categories, when reclassified, should be distributed to Levels II and III for detailed evaluation and decision.

5.3. HAZARD ANALYSIS AND MISSION SAFETY ASSESSMENT

NASA hazard analyses currently do not address the relative probabilities of a particular hazardous condition arising from failure modes, human errors, or external situations.

The hazard analysis and the mission safety assessment do not: address the relative probabilities of the various consequences which may result from hazardous conditions; provide an independent evaluation of the retention rationales stated in the input CILs; or provide an overall risk assessment on which to base the acceptance and control of residual hazards.

Hazard analysis (HA) is intended to be a key part of NASA's safety and risk management process. Because it considers hazardous conditions, whatever their source, it is a top-down analysis that should encompass the FMEA and other bottom-up analyses and cover the safety gaps that these other analyses might leave. In reality, however, the HA has not played the central role it was designed to play. Instead, the main focus has been on the FMEA and its corresponding CIL retention rationale. These are design-based analyses, prepared by the project engineering staff. (See Section 5.1.)

The Committee's audit of the FMEA/CIL re-evaluation and hazard analysis review produced, at first, a somewhat confusing and contradictory set of perceptions about the relationships between these safety analyses and the nature of the overall risk assessment and management process of which they are a part. Gradually, it became clear that there were differences between the officially prescribed process and the real process, as well as differences in the way the process is perceived by

various NASA personnel, depending on their function and point of view. Beyond that, there were also differences among the NASA centers in the implementation at the detail level.

Figure 5-1 (shown earlier), which was prepared by the Safety Division at JSC, depicts fairly accurately the process, as the Committee has come to understand it, that was prescribed by NASA policy at the time of the Challenger accident. Here, the HA is clearly an important element, buttressed by a number of complementary analyses including the FMEA/CIL. The ultimate product of the safety analysis is the Mission Safety Assessment (MSA), feeding into the deliberations of the various engineering and readiness review boards. Figure 5-3, also prepared by the Safety Division at JSC, shows the process from the perspective of that Division, focusing on the HA as the central activity. Note that the FMEA/CIL is listed as one of many inputs to the hazard analysis. The actual process appears to be quite different from the one suggested by the preceding two figures.

During the latter part of 1986 and the first few months of 1987, our audit led to the impression that, although some of the FMEA/CILs were inputs into the HA function, the *real* risk acceptance process within NASA operated essentially as shown in Figure 5-4 (obtained from JSC). One can see from the diagram that the "Hazard Analysis As Required" is a dead-end box, with *inputs* but *no output* with respect to waiver approval decisions. Our impression was supported by subsystem project managers, engineers and their functional management at JSC. Many of them believed that the CIL path shown in Figure 5-4 was the actual approval route for retention of designs with Criticality 1 and 1R failure modes.

A key problem, in our view, is that the risk assessment shown in the box entitled "Retention Rationale and Risk Assessment" was not really an independent assessment of the risk levels by professional system safety engineers; such individuals (and they are few in number within NASA) were "left out of the loop." Neither did the assessment contain an evaluation of how system hazards resulting from critical item failure modes would be controlled. In practice, in most cases reviewed by the Committee, the retention rationales written on the CIL forms were simply transferred to the hazard analysis reports and became the basis for final acceptance of residual hazards, and for decision-making at Flight Readiness Reviews (FRRs).

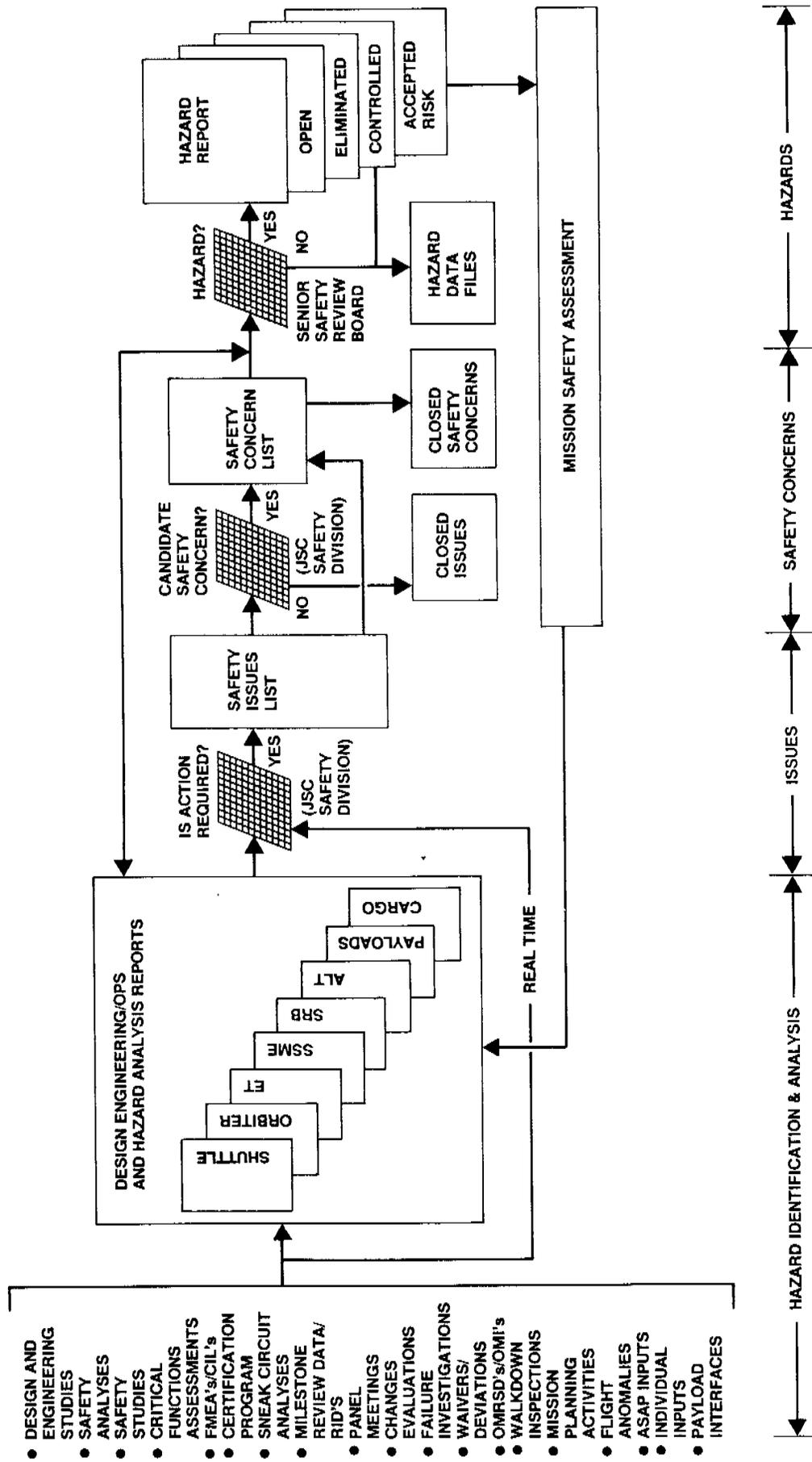


FIGURE 5-3 Processing of identified safety issues, concerns, and hazards; and the documentation in the Mission Safety Assessment (NASA JSC SR&QA).

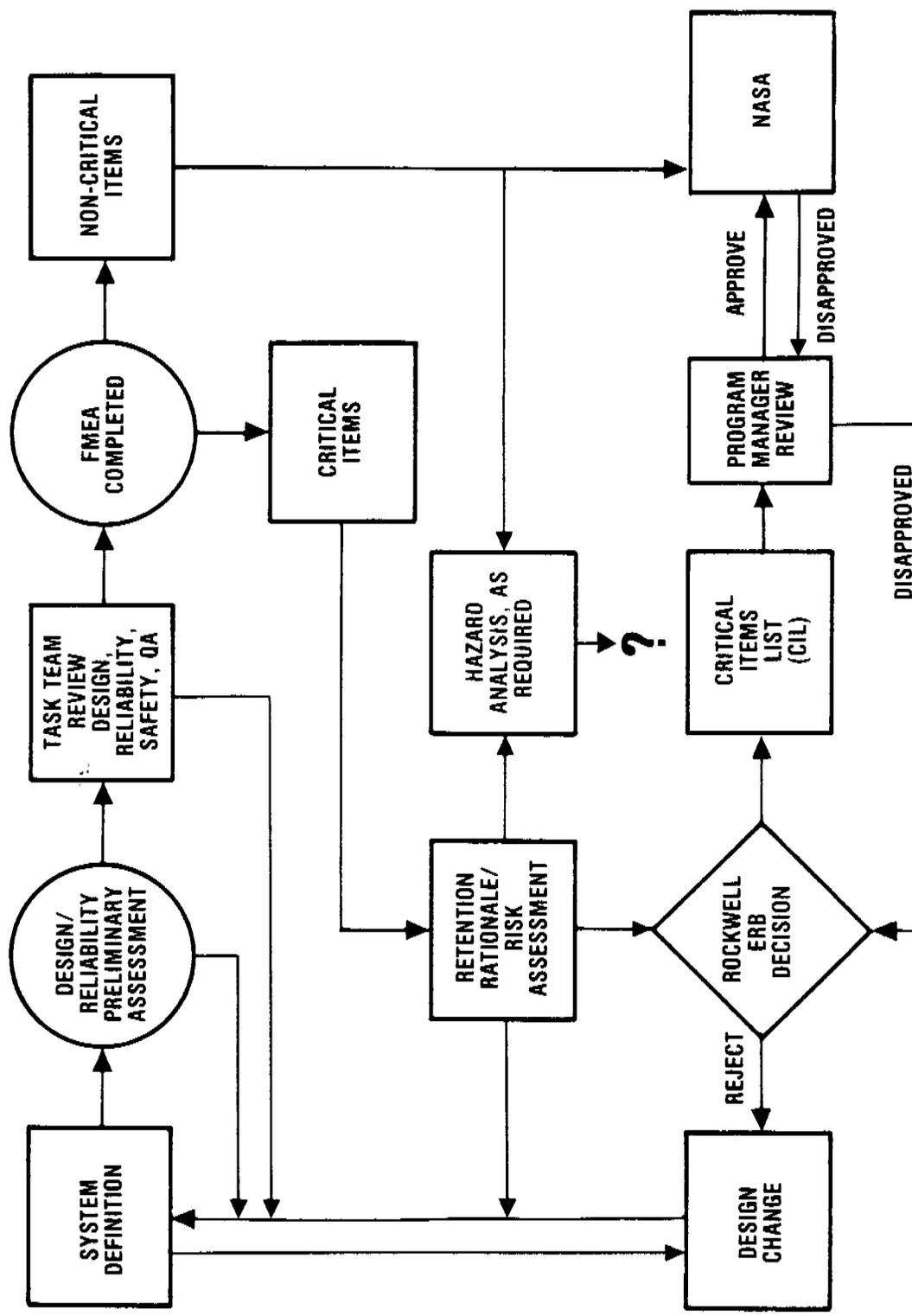


FIGURE 5-4 The STS FMEA/CIL closed loop process provides for feedback on actions—the actual process (after Rockwell STS Div.).

NASA does not use the HAs and (in turn) the MSAs as the basis for the Criticality 1 and 1R waivers. In fact, HAs for some important subsystems were not updated for years at a time even though design changes had occurred or dangerous failures were experienced in subsystem hardware. (An example is the 17-inch disconnect valves between the ET and Orbiter.) The Committee's audit showed that standards and detailed instructions for the conduct of HAs were not found to be consistent throughout the STS program; NSTS 22254 was issued to correct that problem.

In summary, the Committee found in its review of the HA process that:

1. HAs were done for only the largest subsystems of the STS; they addressed certain overlays of hazards but were not traceable to all failures in units within the subsystems.
2. HAs were not done routinely for each major subsystem.
3. The HA assumed worst-case consequences and simply categorized hazard levels (catastrophic or critical) based on whether there was time for counter-actions.
4. The HA process called for an independent evaluation of the HA results. Analyses of catastrophic and critical hazards were to be verified using risk assessment techniques. However, the HAs did not address the relative probability of occurrence of various failures, based on actual flight and test information, nor did they evaluate the validity of the CIL retention rationale against any formal set of criteria.

We found that many engineering personnel, functional managers, and some subsystem managers were unaware of what tasks must be done to complete the hazard analysis, did not know whether they had actually been done, and did not contribute to them. Some, in fact, believed that HAs were just an exercise done by reliability and/or safety people and that they were redundant to the FMEA/CILs. **Their belief appears to be justified, in that these HA activities did not seem to be authoritatively in-line as part of a true hazard control and risk management process. It appears they were carried out in a relatively sterile environment outside the mainstream of engineering.**

The safety personnel did use the HAs along with the FMEA/CILs to create Mission Safety Assessments for the major elements of the STS and for the overall missions. These MSAs were to provide "a formal, comprehensive safety report on the final design of a system." However, in practice, the MSA reports essentially served as process assurance reports. They listed the hazards and stated whether they were eliminated or controlled; compared hardware parameters with safety specifications; specified precautions, procedures, training or other safety requirements; and generally documented compliance with the various reliability and safety tasks. They did not provide in-depth quantitative risk assessments, and relied almost exclusively on the CILs and HA reports for justification of acceptable risks.

New design changes and/or flight data were "examined" and "judged" for safety by various personnel and boards at NASA Levels III, II, and I; the vehicles for the approval of changes appear to have been the FRRs and various special reviews. The HA and MSA reports were not viewed as controlling documents on a specific system configuration which was judged to be safe by the safety organizations. The initial waivers to fly Criticality 1 and 1R items were not always redone in a timely way after new data were obtained. Thus, our audit supports the impression that the hazard analysis is not used to its fullest advantage and that overall system safety assessments, based on test and flight data and on quantitative analyses, are not a part of the process of accepting critical failure modes and hazards.

Since the Hazard Report does not provide a comprehensive risk assessment, or even an independent evaluation of the retention rationale stated in the input CILs, we believe the overall process shown in Figure 5-2, representing NASA's current plans, has serious shortcomings. The isolation of the hazard analysis within NASA's risk assessment and management process to date can be seen as reflecting the past weakness of the entire safety organization. For that reason, this issue of the role of hazard analysis drives to the heart of our most sweeping conclusion, which is that the information flow, task descriptions, and functional responsibilities implied by Figure 5-2 must be modified if NASA is to achieve a truly effective risk management process. The reordering of functions which the Committee recommends is described in detail in Section 5.11.

Recommendation (3):

The Committee recommends that the FMEA/CILs be used as one of many inputs considered in the hazard analysis and system safety assessment. We also recommend that the overall system safety assessment encompass a quantitative risk assessment which in turn uses the CILs and hazard analyses as input. Finally, the Committee recommends that this risk assessment be the primary basis for retention or rejection of residual hazards as well as critical items.

5.4 RELATIONSHIP OF FORMAL RISK ASSESSMENT PROCESS TO SPACE TRANSPORTATION SYSTEM ENGINEERING CHANGES

Elements of formal risk assessment, such as FMEA/CILs and hazard analyses, appear to have had little direct impact on the STS recovery engineering process as they have not figured prominently in the majority of engineering change decisions made by NASA management.

The foregoing sections have addressed the relationship between FMEA/CIL and hazard analysis, and their relationship to the CIL retention rationale review and waiver decision-making process. It is important also to take a broader perspective and examine the relationship of the risk assessment process, as a whole, to the actual STS engineering redesign activity and recovery process.

Shortly after the Challenger accident, groups representing various parts of NASA (design centers, Astronaut Office, etc.) presented the NSTS Program Manager at JSC with their lists of items deemed to require attention. All were Criticality 1 or 1R items. From these lists, the JSC Level II Program Requirements Control Board selected 90 (consisting of hardware, software, and procedures) to undergo redesign, test, or analysis before the next flight of the Shuttle.

These decisions were made without formal reference to the FMEA. Since that time, the number of mandatory next-flight changes across the STS system has grown to 159. Of these, only a handful have the FMEA/CIL/retention rationale (or the hazard analysis) listed as the original source of the

change (e.g., 1 out of 23 on the SSME, 4 out of 48 on the Orbiter). Only a few of the mandatory changes have arisen out of the current FMEA/CIL reevaluation. Indeed, the redesign activity has, for the most part, preceded these reevaluations. Most of the mandatory changes were longstanding concerns, identified before the 51-L accident, which were derived from flight experience, engineering analysis, etc.

NASA and contractor personnel told the Committee that the stand-down provided an opportunity to address known hazards—things that were already “in the mill” before the accident. Thus, the FMEA/CIL and hazard analyses seem not to have affected STS engineering very significantly. Yet the FMEA/CIL reevaluation and the hazard analyses were the heart of the mandate the Committee (via NASA) received from the Rogers Commission in its recommendation III (see Appendix B).

For this reason, the Committee was concerned as it gained an increasing impression that the FMEA/CIL and hazard analyses are fairly narrow parts of the overall STS risk management/reliability picture. The special System Design Review Boards established in March 1986 to review design changes slated for completion before the next flight apparently did not take the FMEA/CILs formally into account. As discussed in Section 5.3, the hazard analyses in actual practice appear to have little or no influence on the waiver decisions to accept Criticality 1 and 1R designs for flight. Also, the original scheduling of the first flight some six months after completion of the FMEA/CIL and hazard analysis reevaluations seemed to presuppose that no substantial design change requirements would result from the process.

NASA and contractor personnel explained to the Committee that the FMEA/CIL is primarily a *design tool*, used as an input to Preliminary Design Review in the early days of the Shuttle program. In their view, the current reevaluation is essentially a design validation effort; thus, they say, the fact that it has disclosed few new critical items confirms the strength of the original design. Furthermore, they assured the Committee, engineering changes are processed through the same configuration control boards that review the FMEA/CIL, and the total process is not complete until the last change to be implemented before flight has undergone a FMEA and been dispositioned by the board.

The Committee accepts this explanation. However, accepting it forces us to conclude that NASA

may have overemphasized the importance of the FMEA/CIL reevaluation while simultaneously not giving sufficient attention to its results. Also of concern is the Committee's continuing impression that the extensive FMEA/CIL effort has focused on a "moving target," as the redesign work goes forward without adequate feedback into that process. For example, the contractor conducting an independent FMEA on the Orbiter (McDonnell Douglas) reported—and JSC confirmed—that personnel conducting the FMEAs have had to utilize old "as-built" hardware drawings as a data base, telephoning engineers whenever they believe an item might have been modified since the original design.

In its first interim report to NASA (see Appendix C), the Committee recommended that NASA take steps to ensure a close linking between the STS engineering change activities and the FMEA/CIL-hazard analysis processes. A subsequent revision in the change review procedure appears to be helping in that regard. It requires an assessment of each proposed design change to determine if any Criticality 1 or 2 hardware is affected. Furthermore, NASA's Administrator has assured the Committee that flight schedule considerations will not be allowed to reduce the rigor with which reviews and analyses are conducted. The Committee is substantially reassured regarding the strengthened relationship between the risk assessment process and STS engineering changes. However, concerns remain regarding the long-term outlook for a strong connection between these activities, as Shuttle operations resume and engineering improvements continue.

Recommendation (4):

The Committee recommends that NASA take firm steps to ensure a continuing and iterative linkage between the formal risk assessment process (e.g., FMEA/CIL and HA) and the STS engineering change activities.

5.5 TIMELY FEEDBACK OF DATA INTO THE RISK ASSESSMENT AND MANAGEMENT PROCESSES

The Committee has found many indications that data from STS inspection, test and repair,

and inflight operations do not always feed back rapidly enough or effectively enough into the risk assessment and management processes.

One of the key failures that led to the Challenger disaster was that data regarding O-ring erosion in earlier flights had not surfaced with enough visibility or in a timely enough fashion to impact the O-ring CIL retention rationale or the Flight Readiness Review for that ill-fated mission. The Committee has found numerous indications that data from STS inspection, test and repair, and inflight operations do not always feed back rapidly enough or effectively enough into the risk management process. For example, with a high Shuttle flight rate (such as the rate of one per month being experienced just prior to 51-L), there may be a lag of two or more flights before in-flight anomalies are reviewed by the responsible NASA managers.

A primary issue here is the feedback of operational experience, inspection, test and repair reports, data and anomalies into the FMEA and the CIL retention rationale, and their impact on waiver and commit-to-launch decisions. Information that could affect the CIL waiver retention rationale often appears in other parts of the system long before it finds its way into the rationale for retention. For example, the SSME prime contractor has set up a board (Rocketdyne's Engineering Review Board) to disposition every item identified as troublesome by the project engineers. However, the relevant CIL number and document is identified only *after* disposition is made. Similarly, the effects of activities such as inspection, test and repair, and inflight operations appear not to be adequately accounted for in hazard analyses.

Furthermore, it is not clear to the Committee what processes exist for methodically incorporating operational experience into performance analysis programs and the system change process, or into the FMEA/CIL. Mission Operations Directorate (MOD) personnel at JSC have been heavily involved in the FMEA/CIL and hazard analysis reevaluations, and 14 astronauts have been assigned to safety functions such as FMEA/CIL. This involvement in reviews leads to the development of flight rules, which, as one astronaut noted, is an effort to address a problem through procedural changes when it is too late for design changes. However, flight rules and procedures development often do lead to system design changes. (The Director of

MOD described 28 such changes made during 1985 and 1986.)

Another critical problem is the need to provide rapid feedback of information on anomalies detected during inspections, tests, and repairs as well as those occurring in flight, into the Flight Readiness Review (FRR) and the commit-to-launch decision. For example, in the past, information from the previous STS flight was not available in time to influence the decision to launch the next mission.

There is a well-established process for handling and reporting in-flight anomalies. Once detected, an anomaly is evaluated and tracked by a Mission Evaluation Team (MET) (or the equivalent). A Problem Report (PR) is prepared on each anomaly which includes data and analysis regarding the fault isolation and its possible resolution, and potential effects on future flights and schedules. The PR is then reviewed, evaluated, and approved by the relevant project organizations, SR&QA, and the NSTS Deputy Director (Program). The PRs and the status of their resolution are tracked in the Problem Reporting and Corrective Action (PRACA) System. Finally, all reported anomalies and other concerns are compiled into a list which is made available to the FRR Board for the next scheduled flight.

The problem has been the delays in the feedback from anomaly detection on one flight to the FRR for the next flight. NASA has a "quick look" procedure for expediting the reportage of significant anomalies up the management chain, but some data will simply entail an irreducible lag. NASA intends, for the initial flights of the Shuttle after its resumption, to reduce *all* the data from each flight before launching the next one. However, after the first few flights, NASA plans to increase the flight rate to a point where the data stream from postflight activities will once again lag. Although vigilance will certainly remain higher for some time in the wake of the Challenger accident, the Committee is nonetheless concerned that the same dangerous preconditions will once again be present.

NASA is now establishing a new closed-loop accounting and review system known as the System Integrity Assurance Program (SIAP). (See Figure 5-5). Among other things, this system will tie all Criticality 1, 1R, and 1S items (defined in Section 3.4.1 and Table 3-1) to findings in the field. A key feature of SIAP is its Program Compliance Assurance Status System (PCASS). This is essentially a computer-based information system for the SIAP. Still being developed, the PCASS will function as

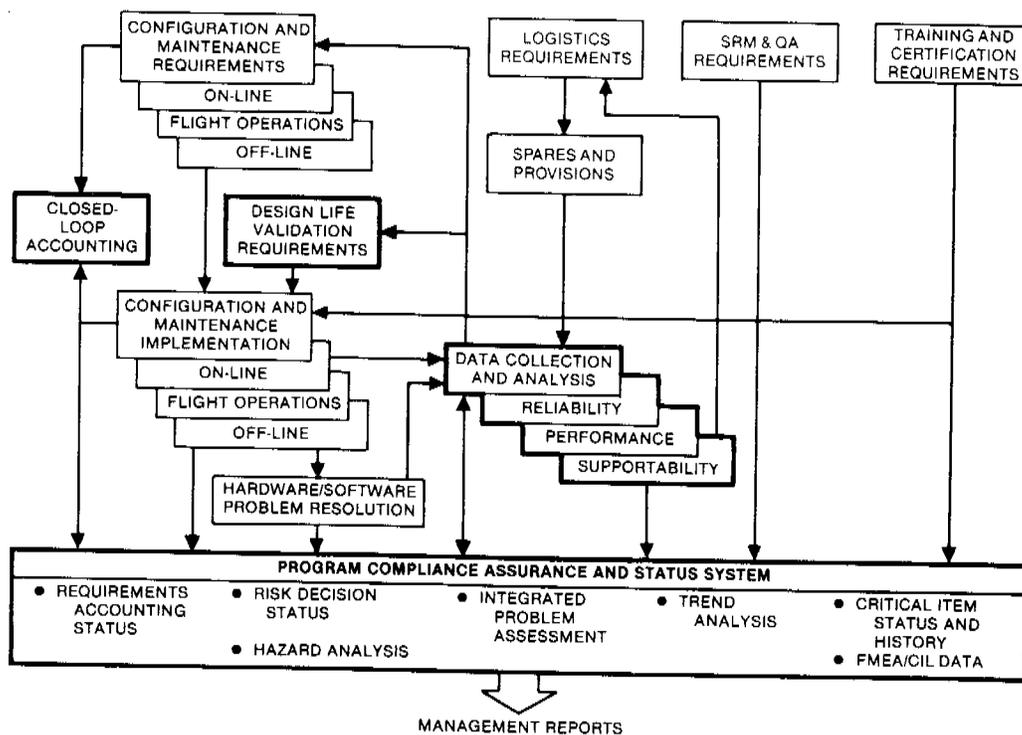


FIGURE 5-5 The NASA NSTS System Integrity Assurance Program (NASA).

a central data base that integrates a number of existing information systems and sources across the NSTS (Figure 5-6). For example, the PRACA system mentioned above will be a part of it, speeding the transmission of data on flight anomalies.

The PCASS has the potential to provide in near real-time, to decision makers such as the participants in the FRRs, an integrated view of the status of problems with the STS, including trends, anomalies and deviations, and closure information. However, the PCASS will be ineffective unless inspection, repair, test, flight, and other data are fed into the system in a timely manner, and the data are available promptly in convenient, usable form. For example, delays in reporting on anomalies and trends from previous flights can jeopardize proper decisions to launch the next flight.

The Committee believes that the SIAP, including the PCASS as an integrated data base, can and should become a central element of STS risk assessment and management. However, great care must be taken to assure that the data base is correctly and adequately maintained.

Essential to the successful assessment and management of risk is the certain and timely feedback of preflight, flight, and postflight system performance data; along with inspection, test and repair data; test results; and failure or degradation reports. Thus, a prime need recognized by NASA managers is to ensure that all problem actions are promptly placed in the PRACA/PCASS system. In many cases this involves a strong reliance on the

thoroughness of maintenance and handler personnel as well as project engineers. The paperwork burden on NASA technical and safety personnel is already enormous. But the timely and diligent reporting and the proper evaluation of such data are among the most important tasks they can perform. It is precisely where the system broke down in the months preceding 51-L.

Recommendations (5):

The Committee recommends that high-level NASA management attention and priority be given to increasing the efficiency of the flow, analysis, and use of inspection, test and repair, test results, and in-flight operations data throughout the decision-making process. The Committee also recommends that full implementation of the System Integrity Assurance Program (SIAP), including its Program Compliance Assurance Status System (PCASS), be given a high priority. Diverse professionals (e.g., design and development engineers, operating personnel, statistical analysts) should be used in the development of this program, with maximum possible early involvement by potential users and key decision makers. The Committee further recommends that procedures be implemented to ensure that all mission anomalies detected in real time and from recorded events, and those detected during the near-term inspection of recovered hardware, also are fed into the formal risk assessment and management processes for action prior to committing to the next flight. Finally, the Committee

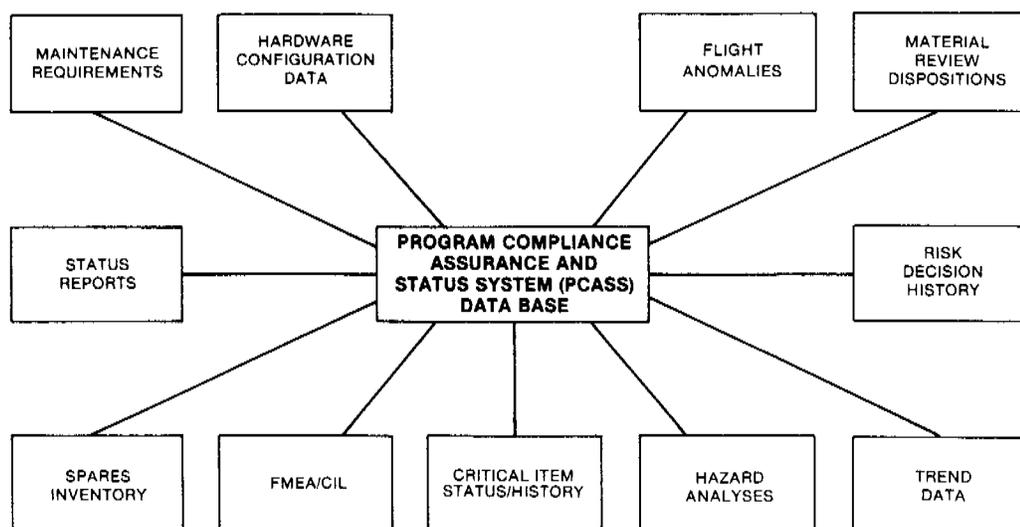


FIGURE 5-6 Data base elements of the NASA NSTS Program Compliance Assurance and Status System (NASA).

recommends that all such anomalies be called to the immediate attention of launch decision makers who will justify in writing their decisions regarding the disposition of the anomalies.

5.6 THE NEED FOR QUANTITATIVE MEASURES OF RISK

Quantitative assessment methods, such as probabilistic risk assessment, have not been used to directly support NASA decision making regarding the STS, although quantitative analyses and test data often are used in arriving at qualitative subjective judgments in reaching decisions. Powerful methods of statistical inference are now available which allow the integration of all sources of information on risk, including data on partial degradations and failures as well as engineering models of failure modes.

NASA is not adequately staffed with specialists and engineers trained in the statistical sciences to aid in the transformation of complex data into information useful to decision makers, and for use in setting standards and goals.

The key technical decision makers in NASA operate as chairmen of bodies that review relevant technical information. Their decisions involve requirements, design, waivers, launch decisions, etc. Much of this information is in the form of complex engineering data. Data are routinely collected from flight and ground tests, part changeout and failure histories, anomaly reports, computer simulations, and other sources. Some of these data are used in various ways for design qualification, system certification, and configuration control. They are also used to establish or verify redlines and safety margins. They are sometimes employed in the FMEA to support rationales for retention, and in the hazard analyses to support classification of a hazard. They may come into play in the waiver process and the Flight Readiness Reviews. In other words, numbers and statistics appear throughout the risk management process, but they are generally used as raw data, and in a qualitative way. Numerical data have not normally been used *directly* to generate indicators of risk or reliability. Even

trend analysis, a relatively simple statistical technique for anticipating failures, has not been employed routinely or to maximum effectiveness.

The Committee was informed by a number of NASA persons during discussions that early in the history of the Apollo program a decision was made not to use numerical probability analyses in NASA's decision-making process. This disinclination still prevails today. As a result, NASA has not had the benefit of more modern and powerful analytical assessment tools that have been developed in recent years, and that are used by other high technology organizations, such as in the communications and nuclear power industries. Without such tools, it would be very difficult at best for safety engineers to transform the massive data base which has developed in the STS program into specific information regarding what was truly known and what was not known. In addition, the failure to use numerical probability analyses had the unfortunate effect of denying NASA designers the required statistical data base on various types of failures, along with the better understanding of the mechanisms of failures that can be obtained from such data.

Quantitative approaches to the overall analysis of risk in complex systems are known by various names, such as quantitative risk assessment and probabilistic risk assessment (PRA); we use the latter here. Using modern techniques of statistical inference in combination with engineering models of failure modes and system models, these approaches have become sophisticated and powerful in recent years. They are employed by the nuclear power, aircraft, and communications industries, the military aerospace sector, and other developers and operators of complex systems. While these quantitative approaches are not a panacea, since not everything affecting flight safety can be rigorously quantified, they can permit more objective assessment of the varying types and quality of information and data which are available as well as reflect the uncertainties introduced by incomplete data or knowledge.

An approach to statistical inference that is particularly useful for assessing risk is the Bayesian approach (using, for example, Weibull, binomial, or Poisson likelihood functions). This allows the integration of information from a variety of sources, such as industrial data on components and materials, test data, analytical engineering models, field data, and qualitative engineering judgment. The

Bayesian approach (see Appendix D for more details) produces a “State of Knowledge Curve” (technically a probability density) for the parameter of interest, such as the frequency of a Criticality 1 failure. The curve provides an estimate of the frequency and measures the uncertainty in the estimate. If only the data from the few or zero observed failures during flights were used, then the uncertainty would be too large to be useful. But the relevant information goes well beyond that scant data base. For example, it may include a model of the mechanism which would cause the failure mode. This cause model may involve loads and safety margins whose uncertainties have been well characterized by existing engineering data bases or carefully designed margin validation tests. Suppose, however, that after a complete analysis, the uncertainty about the frequency spans both the safe and unsafe regions of the frequency scale. This is not a sign that the analysis has failed, but it is an indicator that more (carefully designed) tests are needed. The experience and intelligence of the subject matter experts has already been fully reflected in the Bayesian analysis; so it is inappropriate to ask them now to resolve the uncomfortable uncertainty. Only new information will do. If the State of Knowledge Curve spans primarily the unsafe region of the frequency scale, then a design or procedure change is required. But if the safe region of the frequency scale carries all the uncertainty, then the uncertainty itself is of little consequence because the risk is now low enough to fly.

Probabilistic risk assessment identifies all possible failure scenarios along with their probabilities of occurrence and their consequences. The methods used in PRA to identify and organize these scenarios into a structured pattern variously include the use of master logic diagrams, fault trees, event trees, and FMEAs, among others. Since NASA has a great deal of experience with FMEAs in the design process, it is logical that they be a principal input to the PRA. Among the pay-offs to NASA from using PRA is that literally thousands of scenarios and their associated risks can be eliminated from further consideration in the hazard analysis and other risk assessment processes, if their contributions to total risk and/or their probability of occurrence are extremely low. (The specific limits should be set by the top management of NASA. However, failure scenarios that contribute less than 0.01 percent of the total risk or have a probability

of occurrence of less than 10^{-7} per flight would appear to be reasonable candidates for removal from further consideration.) Thus the proper use of PRA methods could significantly reduce the time and effort expended on risk assessment activities while, at the same time, identifying in a quantitative manner the most important contributors to overall risk. By concentrating on these priority items, NASA can reduce the overall risk and perhaps the total cost of risk assessment.

Quantitative methods of analysis rely on the modeling of statistical data of many kinds. For an example of the application of a statistical technique called logistics regression to reveal a statistically significant trend and predict the probability of an STS event while specifying the prediction uncertainty, see Appendix E. It is essential that such analyses be performed with the advice of professionals who understand the full range of analytic tools available through the modern statistical sciences. There currently are not enough professionals in the statistical/analytical sciences among NASA’s civil service and contractor personnel to fully analyze such data on a regular basis. One result of NASA’s early decision not to use a specific reliability or risk analysis approach (apparently because of the lack of a large statistical data base) was that NASA safety organizations were not staffed with professional statisticians or safety-risk analysts, and project engineers were not trained in modern statistical analysis techniques.

Partly in response to the Committee’s interim reports (Appendix C), NASA has begun taking tentative steps toward the use of modern probabilistic analysis and other analysis techniques. A NASA handbook on PRA is being written. Contractor studies have been initiated to conduct trial PRAs of the Orbiter Auxiliary Power Unit and the similar Hydraulic Power Unit in the SRB, as well as on the Shuttle main propulsion pressurization system. In addition, the Jet Propulsion Laboratory is conducting for NASA a study of ways to improve the SSME certification process. They are using a Bayesian approach with a Weibull likelihood function. The prior distribution is derived from engineering models of failure mode life. The idea of integrating engineering models with techniques of statistical inference is very promising. Based on the results of these studies, NASA plans to assess the benefits and applicability of PRA to the STS risk management process. The new Associate Administrator for SRM&QA has indicated that he will

personally evaluate the technique and develop and pursue a strategy for introducing it throughout NASA.

The Committee is concerned that the test with this *very* limited sample—particularly with the evaluation criterion stated in the NASA response to our first interim report (see Appendix C), namely comparison of the PRA results with the (current) “mainline FMEA/CIL activity”—could give a distorted result and lead NASA not to introduce PRA. We have cautioned NASA not to evaluate PRA merely by comparing the results of two or three disparate tests of PRA with the results obtained earlier through the FMEA/CIL process. The criterion should not only be whether a significant new problem is identified by the PRA. What should be asked is whether PRA would have helped in making NASA’s *original* decisions (e.g., regarding the waiver on a Criticality 1 item), or would have given increased confidence in the decisions that were made. The PRA also should improve the understanding of the nature of the failure modes, and increase the confidence in and objectivity of the assessment of risk.

The judgment of experienced engineering practitioners is crucial for ensuring system safety. However, a complex risk assessment process can actually obscure some of the prime contributors to risk. Probabilistic risk-analytic modeling techniques can provide decision makers with an input that clarifies the key choices facing them. Numbers and accompanying analyses should not drive decisions directly, but they can help ensure that system weaknesses and problems “bubble up” for consideration and decision. Also, having available a detailed quantitative breakdown of risk does provide experienced decision makers with a better basis for intelligently managing risk. Clearly, however, the Committee does not wish to suggest that NASA subordinate sound technical judgement to numerical analysis. Such an approach would be, in our opinion, unrewarding and perhaps counterproductive.

Recommendations (6):

The Committee recommends that probabilistic risk assessment approaches be applied to the Shuttle risk management program at the earliest possible date. Data bases derived from STS failures, anomalies, and flight and test results, and the associated analysis techniques, should be systematically ex-

panded to support probabilistic risk assessment, trend analyses, and other quantitative analyses relating to reliability and safety. Although the Committee believes that probabilistic risk assessment approaches will greatly improve NASA’s risk assessment process, it recognizes that these approaches should not be a substitute for good engineering and quality control practices in design, development, test, manufacturing, and operations, all of which must continue to receive high priority emphasis by NASA and its contractors. The Committee further recommends that NASA build up its capability in the statistical sciences to provide improved analytical inputs to decision making.

5.7 THE NEED FOR INTEGRATED SPACE TRANSPORTATION SYSTEM ENGINEERING ANALYSIS IN SUPPORT OF RISK MANAGEMENT

NASA safety-related analyses tend to focus primarily on single-event, worst-case failures to the relative exclusion of possible multiple and synergistic failures in different subsystems or elements of the STS. In addition, the connection between the various analyses appears tenuous. There does not appear to be an adequate integrated-system view of the entire STS.

NASA’s risk management process provides some mechanisms for identifying cross-element interface effects and failure modes, including propagation of failure modes to interfacing or physically adjacent modules or subsystems. One mechanism is the Element Interface Functional Analysis (EIFA), described in Section 3.4.3. There are three EIFAs: Orbiter/ET, Orbiter/SSME, and Orbiter/SRB-ET (a fourth EIFA, on ground/flight systems, is now being generated). The hazard analysis is intended to be a top-down analysis that addresses cascading failures. Interface Control Documents are a third mechanism concerned with safety at the subsystem interfaces. Finally, a Critical Functions Assessment (CFA), conducted initially in 1978 to identify critical functions during each mission phase, is currently being reevaluated by Rockwell International. The CFA can include multiple and cascading failure combinations.

The NSTS Engineering Integration Office at JSC is responsible for managing system integration activities, the systems analysis and interface design effort, and analysis of integrated structural loads and thermal effects. As part of this responsibility, a series of Level II Systems Integration Review (SIR) panels are assigned to review the FMEAs on both sides of an interface. The Office is supported by Rockwell International in the provision of Space Shuttle integration analyses—although Rockwell's support responsibility apparently does not extend to some areas (e.g., on-orbit or reentry phases) or elements. The Engineering Integration Office, with the support of Rockwell, also produces Integrated Hazard Analyses (IHA) bridging two or more STS elements.

To the extent that the hazard analysis is a top-down analysis, it is important that its output lead to the generation or modification of the FMEAs. But there is no indication that this is happening. For example, a member of the Committee audited the FMEA/CILs and hazard analyses related to potential interactions between the Orbiter fuel cells, water management, active thermal control, and life support subsystems; in particular, he looked for indications of possible effects of the presence of hydrogen in the cooling or potable water which would result from a failure of the hydrogen separator. The FMEA/CILs identified only two possible effects: degradation of the performance of the flash evaporator and a reduction of water storage capability. Other, potentially more damaging effects not covered in the FMEA include: the effect of the possible shutdown of flash evaporators between 140,000 and 100,000 feet on the active thermal control system; the violation of water quality standards, with resultant crew discomfort; and the inability to accurately assess the amount of water onboard. It should be noted that no hazard analysis seems to exist related to the potential presence of hydrogen in water; the Element Interface Functional Analysis is not applicable because all of the subsystems of concern are within the same element (the Orbiter).

Although the FMEA/CIL is a bottom-up analysis, it should be able to expose cascading failures initiated by the subject failure. However, at present the FMEA process usually does not consider the cascading of failures beyond the first occurrence. For example, it will not consider propagation of a failure in the hydrogen separator into the flash evaporator and the subsequent propagation into

the thermal protection subsystem. The FMEA/CIL ground rules restrict the analysis to individual subsystems. Contractor personnel do analyze the effects of a failure in the *subject* subsystem on other subsystems, but no further.

External failures are considered in the redundancy screen,⁹ but not in the FMEA. The Committee notes the dichotomy between the concern with failure of redundant items, contrasted with the lack of concern in the FMEA over nearly simultaneous failures in *separate* subsystems which could have an equally critical effect.

The prevailing impression of the Committee is that, although there are several mechanisms that take a partial systems view, and although the level of effort is much greater than it was prior to 51-L, the various analyses do not add up to a truly integrated, total-systems analysis in support of risk assessment. Nor are they linked to the FMEA/CIL in such a way as to compensate for its limitations. The existing risk management process consists primarily of separate, bottom-up lines of analysis, without a thorough top-down, integrated systems analysis.

The Associate Administrator for SRM&QA has been directed by the Administrator to develop a new agency-wide risk management system that integrates the various parts of the risk assessment and management process. This is a promising development. It is important for NASA to call attention to the totality of "risk management" as the sum of various processes, including total STS risk assessment, that ultimately must be considered on an integrated basis by line management as well as by SRM&QA.

It may be noted that, of all the organizations and groups observed by the Committee, operations personnel (astronauts and flight controllers) appear to have the broadest and most integrated perspective of the Shuttle system. Flight controllers in training have actually found real problems on spacecraft while performing cross-element analyses. The continuous development and updating of flight rules and procedures is an important source of this perspective. For example, the Mission Operations Directorate (MOD) flight rules sheet now

⁹ The redundancy screen is a method for documenting the capabilities for redundancy verification: A—capable of checkout during normal ground turn-around between flights. B—loss of redundant element is readily detectable in flight. C—there is a possible single event (e.g., contamination or explosion) which can cause loss of all redundancy.

lists the relevant hazards, FMEAs, and CILs in a matrix format. An experimental system being developed by MOD—the Shuttle Configuration Analysis Program (SCAP) and Failure Analysis Program (FAP)—is able to simulate multiple failures and their effects. This system could be useful in integrated risk analysis.

Another strong example of the integrated, systems engineering approach is the Avionics Audit, a series of studies performed by Rockwell since 1979 on selected avionics hardware, software, and Orbiter functions. An audit looks at failures across the STS, including cascading failures and interactions. The output of the audit is fed back into the FMEA/CIL/retention rationale, hazard analysis, etc., to ensure that they are consistent and complete or that a design change is implemented, with all relevant documents being revised accordingly. Both the Avionics Audit and the Critical Functions Assessment are promising techniques. However, they are presently not scoped broadly enough, nor are there enough highly skilled engineers available, with an understanding of both the STS and the audit techniques, to do the job. (We understand that there are tentative plans to expand the Avionics Audit to embrace the entire STS.)

The expansion of effort on integrated analysis is a positive sign. However, **the Committee remains concerned that we have not found at Level II a consolidated, integrated STS systems engineering analysis, including system safety analysis, that views the sum of the Shuttle elements as a single system.** We hope that, in attempting to develop an agency-wide risk management system, NASA will devise an integrated STS system analysis and assessment process which is closely coupled with the FMEA/CIL and other components of risk management, to ensure assessment of the truly critical safety items in the STS. This would include all combinations of hardware, software, and procedural failures and malperformances, and cascading failures. Operations personnel should be brought heavily into play in the development of such an integrated system evaluation. Finally, the safety/risk management process should be reviewed to identify ways to improve both the coordination of analysis efforts and the efficiency of the overall process. Care must be taken to assure that each part of the process is necessary and contributes significantly to the overall STS risk management system.

Recommendation (7):

A “top-down” integrated system engineering analysis, including a system safety analysis, that views the sum of the STS elements as a single system should be performed to help identify any gaps that may exist among the various “bottom-up” analyses centered at the subsystem and element levels.

5.8 INDEPENDENCE OF THE SPACE TRANSPORTATION SYSTEM CERTIFICATION AND SOFTWARE VALIDATION AND VERIFICATION PROGRAM

In general, hardware certification and verification, and software validation and verification of STS components are managed and conducted primarily by the same organizational elements responsible for the design and fabrication of the units. Thus, the independence of the certification, validation, and verification processes is questionable. For example:

- The contractor that builds the Orbiters (Rockwell International, STS Division) is also responsible for preparing the documentation and performing the work involved in certification, but does not answer to an entity independent of the NSTS Program with regard to the certification function.
- At Marshall Space Flight Center (MSFC), the Engineering Directorate has the prime responsibility for design requirements for the propulsion elements of STS and also has responsibility for the review and approval of their certification. The Program Office is responsible for the design and development phase as well as for performing the certification activities.
- At the Johnson Space Center (JSC), prime responsibility for design requirements, design and development, and certification for the Orbiter all rest with the Program Office, supported by the Engineering and Operations Directorates of the Center.
- “Independent” validation and verification (IV&V) of software is carried out by the

same contractor (IBM) that produces the STS software, with some checks being made by the Johnson Space Center (JSC).

STS certification methods and responsibilities are described in the Shuttle Master Verification Plan (NSTS-07700-10-MVP-01). This plan now is being revised to define reverification requirements which must be met prior to the return to flight. Figure 5-7 depicts the phases of the process and responsibilities for preparation, review, and approval (i.e., by the contractor or NASA). Figure 5-8 shows the time sequence for the various aspects of the certification-verification process for a subsystem, from the establishment of requirements to operations.

According to the NASA Associate Administrator for SRM&QA, his office is responsible for developing certification plans, reviewing the results, and approving the certification of STS. However, as the following discussion points out, the certification process is actually carried out by the NASA centers and their contractors who are building the STS. Although the general approach to certification is the same at the three centers involved in the STS program (JSC, MSFC, and KSC), there are several differences in detail, especially with respect to the degree of involvement of the SR&QA organizations (Director, JSC SR&QA, personal correspondence).

At MSFC, the Engineering Directorate has the prime responsibility for establishing design requirements and also for reviewing and approving certification. The Program Office has responsibility for the design and development phase as well as for the performance of certification activities. Under the cognizance of the MSFC Chief Engineer, a lead engineer is designated for each element (ET, SRB, SSME) to oversee the certification activity. The MSFC SR&QA office reviews and approves all certification and verification documentation, and performs an independent verification assessment to insure that all STS elements for which MSFC is responsible are properly certified and qualified for flight.

For the Orbiter, the JSC Program Office subsystem managers (supported by the Engineering and Operations Directorates of the Center) have prime responsibility for design requirements, design and development, and also the review and approval of all aspects of certification of hardware. However, the JSC SR&QA office is responsible for assuring the adequacy of all flight equipment through review and approval of all certification requirements, plans,

and test reports. In the case of unresolved differences between the Orbiter Project Manager and the JSC Manager of SR&QA regarding a certification issue, the appeal route is to the Director of JSC. As shown in Figure 5-7, the Orbiter element contractor (Rockwell International, STS Division) is responsible for preparing the documentation and performing the work involved in certification.

At KSC, the verification program used during the establishment of the Shuttle Launch and Landing Site (LLS) was, because of the nature of that facility, quite different from that used for flight hardware. The LLS project at KSC certified that critical ground systems meet design performance requirements. KSC SR&QA and operating personnel also participate in facilities, systems, and equipment certification.

STS Orbiter flight *software* is developed by IBM under contract to NSTS/JSC. Another group of the same contractor, but not reporting to the development manager, carries out the independent validation and verification (IV&V) of the software produced by the development group. NASA personnel consider the multi-organizational, multi-facility participation in software testing and verification to be a strong feature of their procedure. They consider that IV&V is adequately performed in two stages: (1) by a group in IBM separate from the development group, and (2) through testing in the Shuttle Avionics Integration Laboratory (SAIL) at JSC. However, the Committee noted very close collaboration at JSC among NASA personnel and support contractors involved in software development, with little clear differentiation of roles and responsibilities. While such an atmosphere promotes teamwork and cooperation, it does not tend to promote the maintenance of adequate checks and balances required for truly independent IV&V.

The Committee agrees that the existing software validation and verification process is well run, with good quality control, and we believe it should be retained. Indeed, performance of STS software has never created a problem in STS operations. However, **the Committee questions whether independent validation and verification by a second group within the development contractor is sufficiently independent.** The degree of independence certainly would lead to serious questioning by outsiders if significant problems were to develop in the flight software. The Committee further believes that the SAIL, while it may be a good end-to-end test, is not adequate to fulfill the purposes of IV&V. Also,

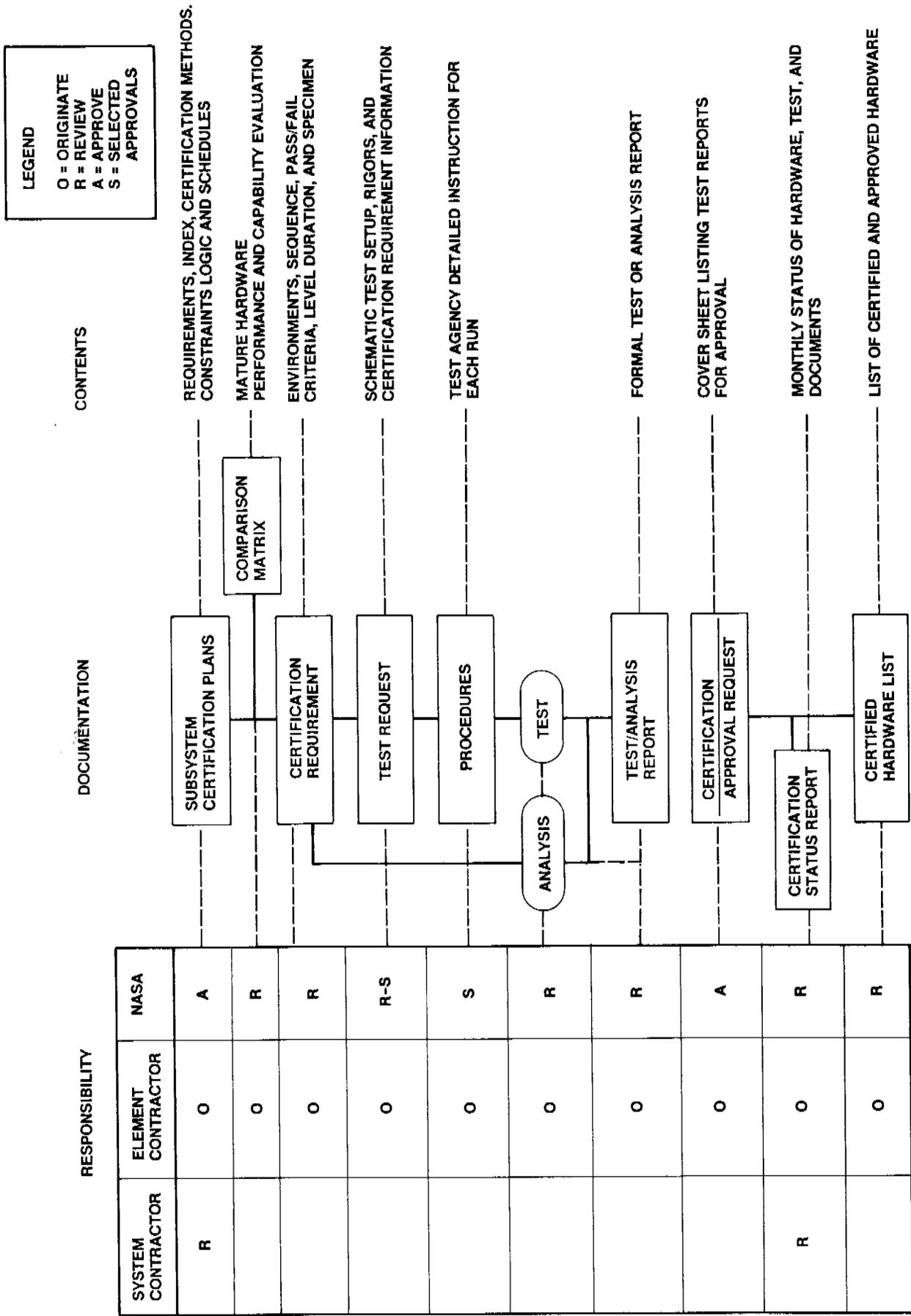


FIGURE 5-7 Phases of the STS certification process and associated organizational responsibilities (NASA).

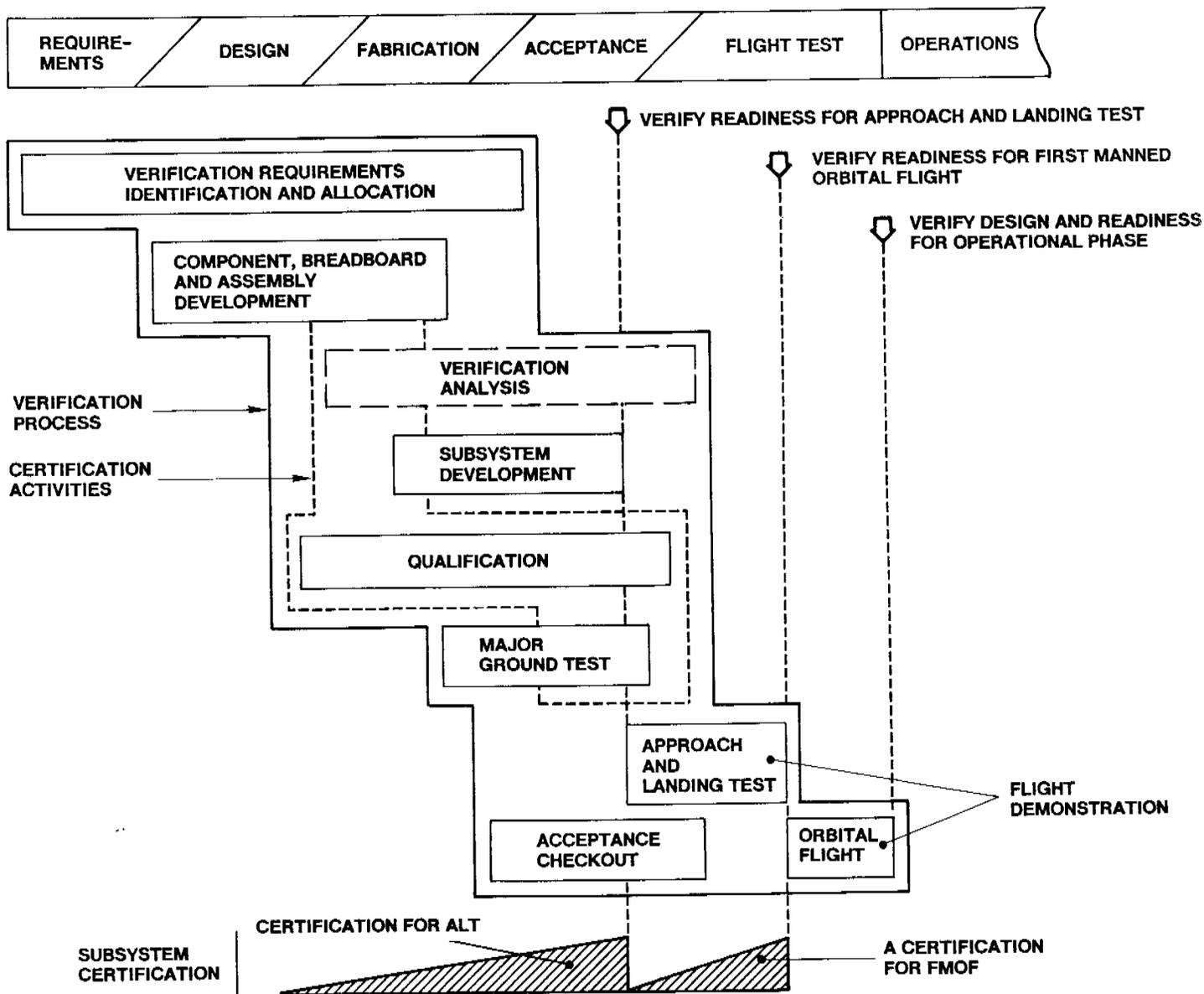


FIGURE 5-8 The time sequence for the hardware certification-verification process in the NSTS Program (NASA).

members of the Committee were told by JSC representatives that, because of limited staff, the JSC SR&QA organization now provides little independent review and oversight of the software activities in the NSTS program.

Based on the Committee's review of STS certification-validation-verification processes, it appears that the work is managed and conducted primarily by the same organizational elements responsible for the design and fabrication of the STS units. The SR&QA organizations seem to have a secondary role. Thus, the degree of independence of the SR&QA hierarchy in the certification process is questionable. This situation is in stark contrast to

that which prevails for military aircraft, in which a totally separate organization is responsible for both certification and software IV&V. It also is in contrast with the process prevailing in the commercial aircraft industry, where the Federal Aviation Administration is responsible for certification. The FAA uses "Designated Engineering Representatives" (DERs) who are employed by the airframe manufacturer but are responsible to the FAA while serving as DERs. This approach provides for independence of the certification process from the design, development and production of the airplanes, while bringing to bear the experience of hands-on engineering practitioners.

Recommendation (8):

Responsibility for approval of hardware certification and software IV&V should be vested in entities separate from the NSTS Program structure and the centers directly involved in STS development and operation. However, these organizations should continue to conduct activities supporting certification and IV&V.

5.9 OPERATIONAL ISSUES

Operational aspects of the NSTS program require considerable attention in risk assessment and management. Three aspects are focused on here: Launch Commit Criteria waiver policy, human error as a contributor to risk, and cannibalization of spare parts at KSC.

5.9.1 Launch Commit Criteria Waiver Policy

An average of two Launch Commit Criteria (LCCs) are waived by NASA in the course of each launch. The Committee questions the validity of an operational procedure that “institutionalizes” waivers by routinely permitting established criteria to be violated.

Launch Commit Criteria (LCCs) are technical requirements and conditions pertaining to the STS system, ground systems, and the physical environment that must be met before a launch can proceed. NASA divides LCCs into three classes: mandatory, highly desirable, and desirable. However, all LCCs are subject to waiver based on the judgment of responsible NASA managers, and typically a few (an average of two) are waived for each launch.

To date, no LCC waiver has ever produced a problem on a Shuttle mission. However, **Committee members questioned the validity of an operational procedure that “institutionalizes” waivers by routinely permitting established criteria to be violated.** There was a general feeling that “waivable” criteria are not valid criteria.

NASA officials told the Committee that an average of 2,000 LCCs come into play on a given Shuttle launch, so that the number waived per launch is an insignificant percentage of the total. The great majority of these are apparently not critical. Furthermore, they explained, in most cases

NASA engineers know that there is some extra margin of safety between the LCC and the actual reasonable limits of safety, because they have learned more about the systems involved since the time the LCC was established. Thus, a typical LCC waiver represents fine-tuning—for example, a slight deviation in leak rates or pressurization rates. Few such waivers have ever led to design changes. The Committee is not persuaded by these arguments.

As a result of the 51-L accident, NASA has begun revising the ground rules for waivers and reassessing the LCCs across the board. A time will be selected (probably launch minus 5 min.) beyond which waiver of an LCC cannot be executed unless contingency procedures are prescribed in advance, thus forcing a launch scrub. Furthermore, each waiver will now trigger a formal reassessment of the particular LCC that was waived, perhaps resulting in a change to it.

Although these changes in policy are appropriate, there are aspects of LCC policy that the changes do not address. The Committee is uncertain about what criteria are used to establish LCCs initially, especially in the weather and environmental area. For example, ice on the pad at the time of mission 51-L was later shown by films to be a serious hazard; yet there was no LCC governing icing. Similarly, there was not an LCC on temperature at the SRB O-rings—only an unrealistic (as it turned out) LCC on ambient air temperature. The Flight Readiness Review Board for that mission was aware of SRB O-ring erosion on past flights, but did not recognize the effects of temperature on the O-ring.

At the same time, there is a concern that too much faith may be placed in the LCCs. A possible case in point is the Atlas Centaur launch failure of March 1987, in which a decision was made to launch the vehicle into a storm because lightning strikes at the time of launch appeared to be beyond the 5-mile range permitted by the LCCs. The Atlas was destroyed by lightning shortly after launch, and observers (including NASA personnel) later said that conditions were clearly not suitable for launch.¹⁰ In the view of the Committee, LCCs are designed to *permit* launch; they should not be allowed to *force* a launch. Experienced judgment must continue to be exercised. But it would be useful in this regard if LCCs were more accurate and more comprehensive in their definition of

¹⁰ NASA: Report of the Atlas Centaur—67/FLTSATCOM F-6 Investigation Board, 15 July 1987.

allowable limits; in that case they would not be so subject to waiver.

We note the U.S. Air Force system for indicating the criticality of flight equipment by a "red cross" (a mandatory NO-GO), "red diagonal" (system not fully operational, but safe to fly), and "red dash" (some inspection not done). A comparable prioritization would be appropriate for NASA's LCCs. Loss of an STS may be much more costly in dollars and lives than loss of any USAF system, and any means of focusing judgment should be welcome. There must be room for experienced judgment; but there must also be inviolable rules that prevent errors in judgment being made under pressure of time on certain critical LCCs. We recognize the objections of launch directors to inviolable criteria; but in our view the best launch director is one who is willing to be conservative and to live with a conservative system.

The Committee welcomes the present review of LCC waiver policy. We believe that the presence of the newly appointed NSTS Deputy Director (Operations) will also help to ensure the application of experienced judgment and knowledge whenever LCC waiver decisions are being made.

Recommendation (9a):

The Committee recommends that NASA establish a list of mandatory LCCs which may NOT be waived by anyone. This should comprise the bulk of the LCCs. A limited number of criteria would be separately listed, for special cases, together with a discussion of the circumstances under which they may be waived and who may make the waiver decision.

5.9.2 Human Factors as a Contributor to Risk

Human factors, which are considered in some of the STS hazard analyses, do not appear to be taken into account as the cause of failure modes in the FMEAs. Since the FMEA is one of the principal safety tools used in the evaluation of the STS design, the Committee believes that the STS design process should explicitly consider and minimize the potential contribution of humans to the initiation of the defined failure modes.

NASA's risk assessment and risk management process for the STS focuses primarily on failure of hardware, and secondarily on software faults and errors. Human error, which can be a major contributing factor in accidents, is accorded relatively little attention in the present risk management system although it is considered in some of the hazard analyses. While procedural aspects of STS operations are regularly relied upon to justify the retention of critical items, human factors do not appear to be taken into account as a source of failure modes in the preparation of the FMEAs. Human error can affect both flight operations (through crew operations and flight controller procedures) and ground operations (testing, certification, maintenance, assembly, etc.). Hazard analyses can consider human error in both types of operations activities; but the Committee has not found that hazard analysis is regularly used to assess this element of risk.

Procedures utilized in both ground and flight operations are controlled by formal Configuration Control Boards. Personnel are, of course, trained and certified for the operations that they will carry out. Procedures are verified by a variety of methods, including trainers, simulators, mockups, engineering models, and analysis tools.

The Committee initially had some concerns regarding the lack of involvement of flight operations personnel in engineering redesign decisions and safety reviews, but through discussions with NASA personnel these concerns were largely resolved. However, we remain troubled by aspects of *ground* operations, with respect to their human error potential. We note that two of the three fatal spacecraft accidents in the U.S. manned space program to date occurred on the ground, of which one was caused by procedural errors on the part of the ground crew.¹¹ Removal and replacement of parts, test, repair, and all the various ground operations provide enormous potential for error that can lead to serious problems. The potential may be exacerbated by the fact that, at KSC, ground personnel are relied upon to report any errors they make which could induce damage; there is little incentive for self-reporting.

A draft NASA Handbook on Systems Assurance, recently prepared by the Safety Risk Management

¹¹ Two Shuttle processing workers were asphyxiated and killed in late 1986 during a test involving nitrogen gas. (The Apollo fire in 1967 was not caused by human error, but by a shorted wire which initiated a fire in the pure oxygen atmosphere.)

Program Office of Headquarters SRM&QA Safety Division, places new emphasis on human error in risk assessment. In a proposed risk assessment model (Figure 5-9), sensitivity to human error is presented as one factor that contributes to the likelihood of a failure mode occurring. This is a positive sign, but it now is far from being implemented in the fabric of NASA system design and safety assurance.

Recommendation (9b):

The Committee recommends that the NASA FMEA include human factors among the recognized sources of potential causes of failure modes. This step would provide another valid link between the FMEA and the hazard analysis, which are now, in our view, too tenuously connected.

5.9.3 Cannibalization of Spare Parts

By the time of the Challenger accident, "cannibalization," the removal of parts at the Kennedy Space Center (KSC) from one operational STS element to fulfill spares requirements in another, had become a prevalent feature of STS logistics, thus introducing a variety of failure potentials associated with human error. Cannibalization is not evaluated as a producer of potential failure in either the hazard analysis (where it would be most appropriate) or the FMEA.

NASA initiated a spares program in 1981, as Shuttle test flights began. Early flights were supported with spare parts produced on order, a source of trouble since parts were often not available in a timely fashion. After other Shuttles came on line and as the flight rate increased, parts shortages became increasingly severe. Cannibalization was often the only answer to meet the flight-rate demand.

As the President of Rockwell International STS Division said to the Committee, "In the last year of flight, cannibalization was the name of the game. We were robbing Peter to pay Paul all throughout the system." With budgetary constraints and cost overruns a chronic reality, NASA apparently decided to emphasize STS fabrication and launchings

over purchasing adequate spare units; the result was logistics problems.

From a safety standpoint, cannibalization raises many problems. First, having workers enter one vehicle and remove a part presents the danger that they will inadvertently (and perhaps unknowingly) damage an adjacent part of the vehicle. Second, there is the risk that the part itself will be damaged upon removal and transport. Third, there is the chance that the part will be improperly replaced in the vehicle for which it was cannibalized as well as in the original vehicle when the part is returned or replaced. The latter two possibilities are theoretically covered by post-installation checkout and inspection, but the risk of error increases as the incidence goes up. Workers are required to report any possible damage they cause, but the "honor system" may not be 100% reliable. Finally, cannibalization per se is *not* explicitly evaluated within the hazard analysis process.

Figure 5-10 shows the incidence of cannibalization over approximately the last year before the accident. It can be seen that at least one-third of the Orbiter Line Replaceable Units (LRUs) flown on some missions were obtained through cannibalization. A NASA official at KSC told the Committee that the problem of spares had become so acute that, if Shuttle flights had continued uninterrupted, KSC would not have been able to sustain STS operations.

The flight hiatus has given NASA time to improve the spares inventory and to make some needed changes in logistics management. Responsibility for Orbiter logistics has been assigned to KSC. The spares budget has been increased. Furthermore, there has been a sharp drop in planned flight rate, which should reduce the requirement for cannibalization. Also, stricter management controls have been placed on cannibalization, making it unlikely that personnel will readily resort to this practice. The program hopes to achieve a level of support in which lack of spares would delay processing no more than 5 percent of the time (the aerospace industry standard). The new NSTS System Integrity Assurance Program specifically prohibits cannibalization except by approval of the chairman of the PRCB, and requires the collection and analysis of supportability trend data in support of logistics management.

Reducing the repair time for spare parts is the fastest way to improve the inventory and reduce cannibalization. The repair processing time is cur-

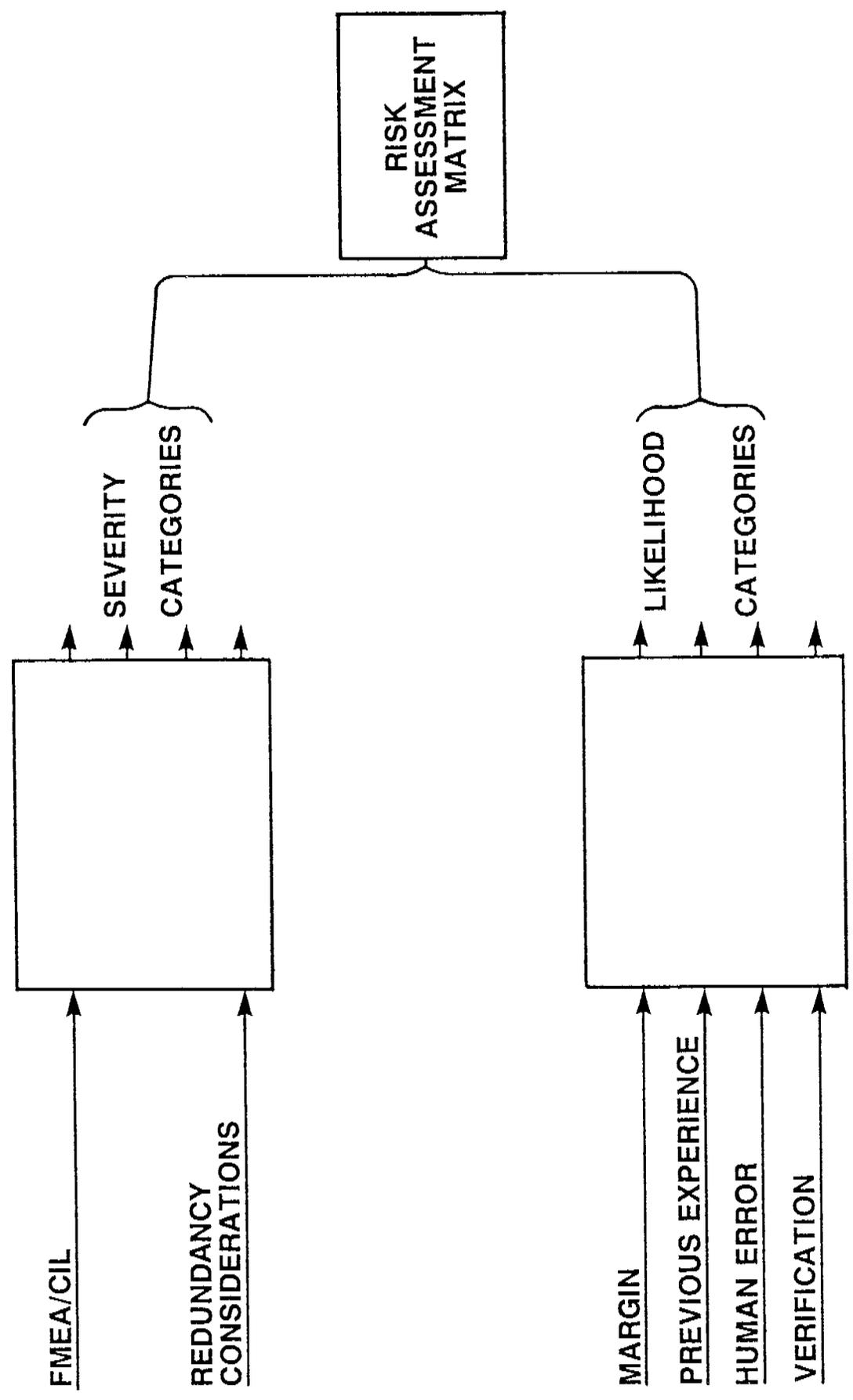


FIGURE 5-9 Human error would be taken into account in this risk assessment model proposed by NASA Headquarters office of SRM&QA (NASA)

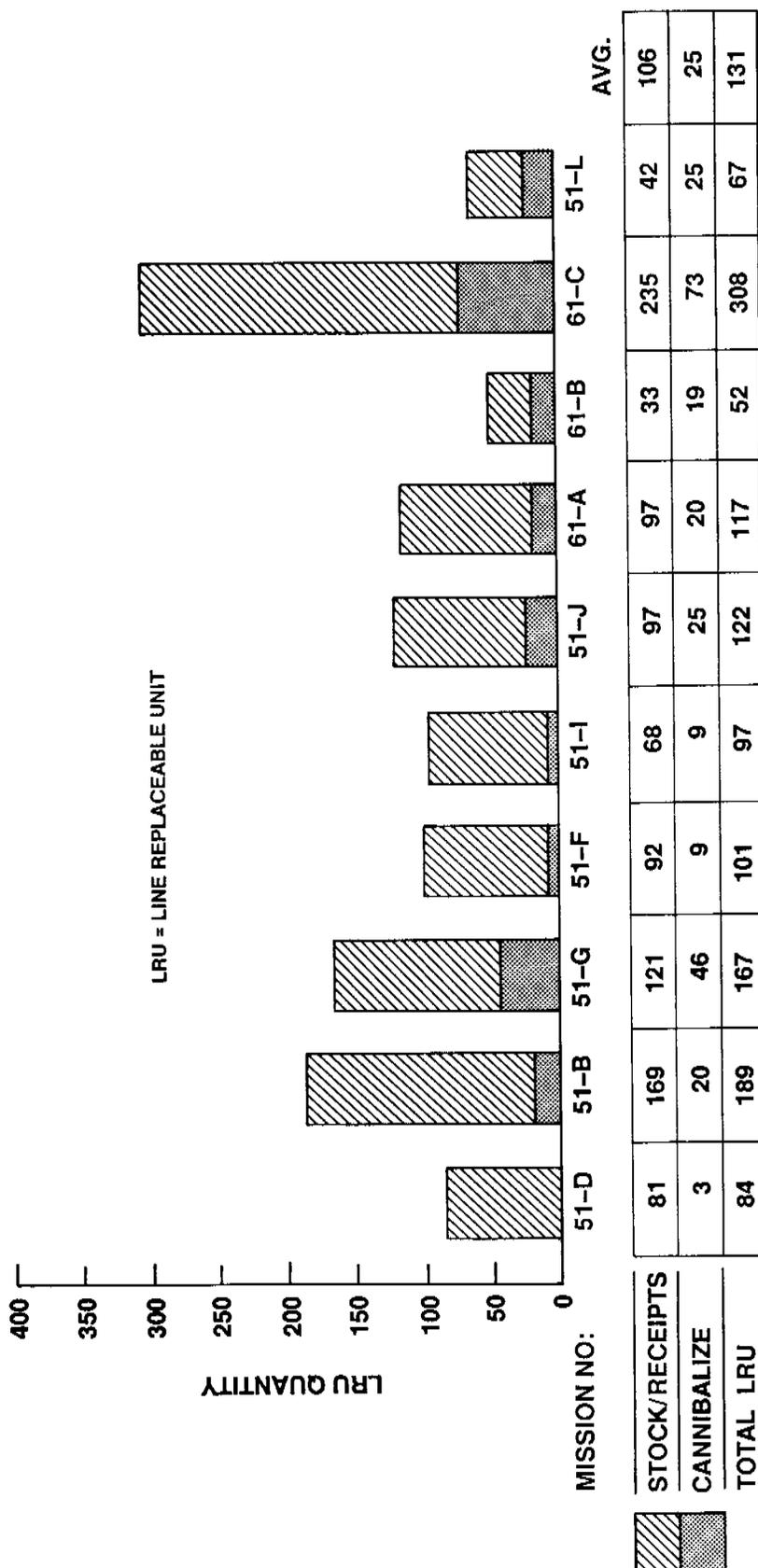


FIGURE 5-10 Analysis of the trend in replacement of STS Orbiter Line Replaceable Units (LRUs) from spares in stock and by "cannibalization" of units from other Orbiters (after NASA KSC).

rently too long, but a gradual reduction in flow time is expected to occur.

Recommendations (9c):

The Committee recommends that NASA maintain its current intense attention toward reducing cannibalization of parts to an acceptable level. We further recommend that adequate funds for the procurement and repair of spare parts be made available by NASA to ensure that cannibalization is a rare requirement. Finally, we recommend that NASA include cannibalization, with its attendant removal and replacement operations, as a potential producer of failure in the integrated risk assessment recommended earlier (Section 5.1).

5.10. OTHER WEAKNESSES IN RISK ASSESSMENT AND MANAGEMENT

5.10.1 The Apparent Reliance on Boards and Panels for Decision Making

The multilayered system of boards and panels in every aspect of the STS may lead individuals to defer to the anonymity of the process and not focus closely enough on their individual responsibilities in the decision chain. The sheer number of STS-related boards and panels seems to produce a mindset of “collective responsibility.”

The NSTS Program is a large organization whose mission involves the development, deployment, and operation of a complex space vehicle in a wide range of missions. Associated with each milestone in the development of any NASA space system and its constituent parts, or in the preparation for a space mission, are one or more reviews. These reviews may be made from the standpoint of requirements, engineering design, development status, safety, flight readiness, or resource requirements. Conducting each review is a team, panel, or board, which may or may not be permanently empaneled. As described in Section 3.2.2, in the NSTS Program there are review groups at every level of management, including the contractor organizations.

Figure 5-11 depicts the review groups associated with the NSTS FMEA/CIL and hazard analysis

processes alone. There are also boards to review design requirements and certification, software, the Operations and Maintenance Requirements and Specifications Document (OMRSD) and the Operations and Maintenance Instructions (OMI), the Launch Commit Criteria, and mission rules. There are flight readiness reviews at each stage of preparation, with a Launch System Evaluation Advisory Team to assess launch conditions and a Mission Management Team to oversee the actual mission.

The Committee developed a concern about a possible attitudinal problem regarding the decision process on the part of the NASA personnel engaged in it. **Given the pervasive reliance on teams and boards to consider the key questions affecting safety, “group democracy” can easily prevail, with the result that individual responsibility is diluted and obscured.** Even though presumably the chairman of each group has official responsibility for the decision, most decisions appear to be highly participatory in nature. In a CCB review audited by the Committee, for example, there were 25–35 people present and the role of the chairman was not especially distinct. Each action appeared to be a consensus action by the board.

It is possible that this is a factor in the problem identified by the Rogers Commission: “. . . a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers” (Vol. I, p. 82). For example, the Level II PRCB conducts daily and weekly meetings—usually via teleconference—in which as many as 30 people participate. It is certainly conceivable that individuals might be reluctant to express their views or objections fully under such circumstances. Also, passing decisions upward through the ranks of review boards may reduce each chairman’s sense that his decisions are crucial. As a case in point, it is clear from the report of the Rogers Commission, and from statements made to the Committee by NASA personnel involved, that the lines of authority and responsibility in the flight readiness review decision-making chain had become vague by the time of mission 51-L.

In discussing this issue, NASA’s Associate Administrator for SRM&QA pointed to the SR&QA directors at the field centers as the individuals with primary responsibility for the safety of the Shuttle system. They are said to have full “responsibility, authority, and accountability.” Nevertheless, these individuals do make inputs to larger and higher boards, so that in the end all decisions become

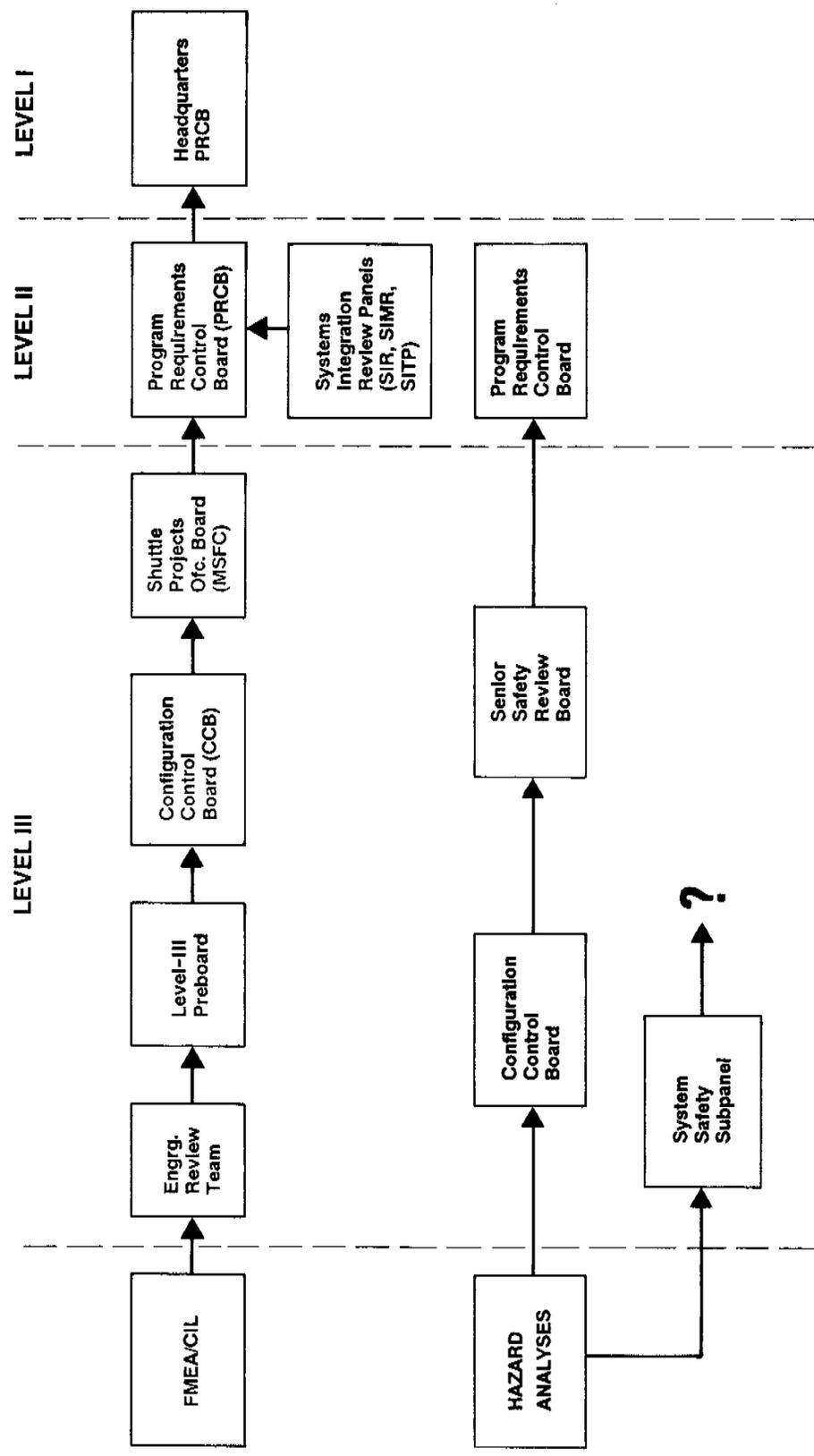


FIGURE 5-11 NASA relies on a multilayered system of panels and boards for decisions on engineering design and safety matters.

collective ones, lacking the crucial mindset of individual accountability.

It is possible that a semantic problem is partly at fault here, in that NASA managers often refer to "the board" as being synonymous with its chairman, with respect to decision authority. Nevertheless, a mindset is thereby established in which it is not clear whether these are individual or group decisions.

The Committee contrasted the NSTS system with that of the U.S. Air Force, in which the board (including its chairman) makes recommendations to the decision maker. One positive point in favor of NASA's system is that, there, the chairman (who is the decision maker) is required to listen "in public" to all dissenting views.

The Committee recognizes the important role played by the many panels and boards in the NSTS program in providing coordination, resolving problems and technical conflicts, and reviewing and recommending actions. These entities allow the different interests and skill groups to bring forward their inputs, contribute their knowledge, and thus minimize the risk that a proposed action will negatively affect some aspect of the STS.

Recommendation (10a):

The Committee recommends that the Administrator of NASA periodically remind all NASA personnel that boards and panels are advisory in nature. He should specify the individuals in NASA, by name and position, who are responsible for making final decisions while considering the advice of each panel and board. NASA management should also see to it that each individual involved in the NSTS Program is completely aware of his/her responsibilities and authority for decision making.

5.10.2 Adequacy of Orbiter Structural Safety Margins

The primary structure of the STS has been excluded, by definition, from the FMEA/CIL process, based on the belief that there is an adequate positive margin of safety. However, the Committee questions whether operating structural safety margins have actually been proven adequate.

Completion of the Model 6.0 loads study and the reevaluation of margins of safety based on these loads will significantly improve NASA's grasp of actual operating margins of safety.

NASA groundrules exclude primary structure from the FMEA/CIL process. NASA has apparently assumed that the structural reliability of the STS (including the Orbiter, External Tank, and Solid Rocket Boosters) is close to 1.00, because the operating loads are believed to be less than the proof load to which the vehicle has been subjected. It is true that some structures have reliability approaching 1.00; examples include bridges, buildings, and even commercial airliners. But there is a considerable difference between the Shuttle, a first-of-its-kind vehicle operated under unique conditions and challenging environments, and a commercial airliner, which is designed and tested to loads and conditions that are well understood. In addition, in the case of a commercial airliner the certifying agency (FAA) and operator organizations act as independent rule makers and auditors. No such independent check and balance exists for the STS, where NASA controls all functions in-house (including requirements, analysis methods, testing, and certification)—primarily within the NSTS program.

The original development plans for the Orbiter—the most complex and vulnerable element, and the only manned element—included a conventional structural test program for certification of the structural integrity. A complete, full-scale structural test article (an Orbiter vehicle) was to be included which was to be loaded to 1.4 times the operating limit load in the most critical conditions. (This compares to the conventional value of 1.5 used by the military and the FAA.) Due to budget problems NASA decided to eliminate one of the planned flight vehicles and convert the static test article (#099, Challenger) to a flight vehicle after a series of proof tests to only 1.20 times the limit load. Some loading conditions actually did not exceed 1.15 times the limit load. Therefore, the tests did not even verify a 1.4 strength margin over limit loads. Subsequent flight test data and calculations show that in some areas the maximum operating loads are actually 15% to 20% higher than those originally postulated, so that the static proof loading tests demonstrated only approximate limit conditions. Thus, today there is no *demonstrated*

verification of safety margins for critical elements of the Orbiter.

The model of loads and stresses on the Orbiter used in its original design has been revised once. By 1983 even these data had become suspect, and another complete revision of loads using the latest test and analysis data was begun. Calculated strength margins from this study (called Model 6.0) are expected to be available by November 1987.

The Committee believes that the margin of actual strength over maximum expected limit load for critical areas of the Orbiter structure is not well known. Partly this is because loading conditions are complex and unprecedented, and partly it is because very little (if any) of the flight structure was actually tested to failure. The Committee agrees with the decision not to use the FMEA/CIL process on STS structures. However, we remain concerned about the uncertainty in the actual strength margins of safety. The Model 6.0 loads calculation now nearing completion should correct the known discrepancies in external loads. Verification of the Model 6.0 loads by data routinely gathered from an instrumented and calibrated flight vehicle, beginning with the next flight, can help verify the model and establish the margins of safety more definitively. This knowledge will greatly improve NASA's ability to keep Shuttle operations within a safe envelope of structural loads.

Implicit in the safe operation of any such structure is a monitoring system to assure that deterioration of structural integrity does not occur. An effort now underway could add materially to NASA's ability to operate the Orbiter's structure safely over its service life. People with airline experience, working under Rockwell International, are developing a maintenance and inspection plan for the structure. A well-planned periodic inspection of this sort is essential, and is the best preventive for unpleasant occurrences due to structural deterioration or other causes.

Recommendations (10b):

The Committee recommends that NASA place a high priority on completion of the Model 6.0 loads, the reevaluation of safety margins for these loads, and the early verification and continued monitoring of the model 6.0 loads by permanently instrumenting and calibrating at least the next full scale STS vehicle to fly. We further recommend that NASA complete and implement a comprehensive plan for conducting periodic inspection and main-

tenance of the structure of the Orbiters throughout the service life of each vehicle.

5.10.3 Software Issues

NASA FMEAs do not assess software as a possible cause of failure modes.

There is little involvement of JSC Safety, Reliability and Quality Assurance in software reviews, resulting in little independent quality assurance for software.

A large amount of data—much of it flight specific—must be loaded for each Shuttle mission but it is not subjected to validation as rigorous as that for the software.

The Shuttle onboard data processing system consists of five general purpose computers (GPCs) with their input and output devices, and memory units. Four of the five GPCs contain the primary software system, known as the Primary Avionics System Software (PASS); the fifth is a redundant computer which contains the Backup Flight System (BFS). The PASS is developed by IBM, and the BFS is built by Rockwell.

In addition to flight software code, there are also flight software initialization data, called "I-loads", which are mission-unique parameter values. The basic code is reconfigured for specific missions, with about two such "reconfigured flight loads" per flight. After the software requirements are approved, three levels of development tests are performed leading to the First Article Configuration Inspection, or FACI. At the FACI milestone, the software package is handed off to the *contractor's* verification organization for independent testing, called Independent Validation and Verification (IV&V), which leads to the Configuration Inspection (CI) and delivery to NASA. (The degree of independence of the IV&V was discussed in Section 5.8.) Following mission-specific reconfiguration and testing in the SAIL and other JSC laboratories, the package is ready for Flight Readiness Review.

A Shuttle Avionics System Control Board (SASCB) is the Level II flight software control board, to which the Program Requirements Control Board has delegated responsibility for software configuration control. The Manager of the NSTS Engineering Integration Office chairs this board and signs the flight readiness statement on software; thus he is the focus of configuration control and

management authority for software. At Level III there is a Software Control Board, corresponding to the Configuration Control Board for hardware issues.

The testing, control, and performance of STS software seem quite good. Out of some half-million lines of code in the Shuttle flight software, typically an average of one error is discovered beyond the CI. With the emphasis placed on early detection of errors, error rates are quite low throughout the total 10 million-line Shuttle software system. Only once has a software problem disrupted a mission (on STS-7, uncertainty about the effect of installed software code on a particular abort scenario caused a launch scrub). Both the developers and the "independent" certifiers perform their own inspections of the code. Special "code audits" are also carried out to reinspect targeted aspects of the code on a one-time basis, based on criticality, complexity, Discrepancy Reports (DRs), and other considerations. Software quality control includes weekly tracking of DRs through the Configuration Management database (which tracks all faults, their causes and effects, and their disposition); trends of DRs are reported quarterly.

Although generally impressed with the Shuttle software development and testing process, the Committee made a number of specific findings. First, we note that software is not a FMEA/CIL item. NASA personnel state that all software is considered to be Criticality 1, with each problem being fixed as soon as it is detected through testing and simulation. The Committee believes that identification and prediction of software faults or error modes may be feasible by dividing the software into functional modules and then considering the various possible failures (e.g., improper constants, discretes or algorithms, missing or superfluous symbols).

There is little involvement of the JSC SR&QA organization in software reviews, due to the limitations on staff. As a result, there is little independent quality assurance for software.

Finally, we note that a large amount of data—much of it flight specific—must be loaded for each Shuttle mission. However, the data and its entry are not validated with the same rigor as in the IV&V of the software.

Recommendations (10c):

The Committee recommends that NASA: explore the feasibility of performing FMEAs on software,

including the efficacy of identifying and predicting fault and error modes; request JSC SR&QA to provide periodic review and oversight of software from a quality assurance point of view; provide for validation of input data in a manner similar to software validation and verification.

5.10.4 Differences in Procedures Among NASA Centers

Differences in the procedures being used by the main NASA centers involved in the NSTS Program may reflect an imbalance between the authority of the centers and that of the NSTS Program Office. The Committee is concerned that such an imbalance can lead to serious problems in large programs where two or more centers have major roles in what must be a tightly integrated program, such as the NSTS and Space Station. Without strong, central program direction and integration, the success and safety of these complex programs can be placed in jeopardy.

In March 1986, the NASA Associate Administrator for Space Flight and the Manager of the Level II NSTS Program issued memoranda setting forth NASA's strategy for returning the Space Shuttle safely to flight status. Their orders rescinded all Criticality 1, 1R, and 1S waivers and required that they be resubmitted for approval. The process also required the reevaluation of all FMEA/CILs and retention rationales, as well as hazard analyses. Other instructions required that a contractor be selected for each STS element (that contractor not otherwise being involved in work on the element) to conduct an independent FMEA/CIL. No specific guidelines were issued by the NSTS Office for the conduct of the independent evaluations; the methods to be used were determined by the NASA centers concerned. Also, the FMEA/CIL reevaluations were initiated using pre-51L FMEA/CIL instructions, in which there were differences in ground rules between JSC and MSFC. (In October 1986, the NSTS Program Office issued new uniform instructions, NSTS 22206, for the preparation of FMEA/CILs, but it took several months for revised directions to reach the STS contractors.) Thus, some differences emerged in the nature and results of the reevaluation conducted by different contractors.

These differences are especially noticeable with respect to the FMEA/CIL reevaluation procedures. The Committee found that, at MSFC, all contractors had been instructed to conduct a new FMEA, "from scratch." At JSC, the independent contractors were told to prepare a new FMEA, but the prime contractors were instructed to reevaluate the existing FMEA. At KSC, where FMEAs are conducted only on ground support equipment, a single group (not the original designer) was reevaluating each category of FMEA, working with the existing FMEA. Procedures with respect to the independent reviews also differed. At MSFC, the independent contractor first performed its FMEA and developed any necessary retention rationales; it then compared those results with the FMEAs and retention rationales prepared by the prime contractor and wrote specific Review Item Discrepancies (RIDs) on points of difference or disagreement. At JSC, no RIDs were written and no retention rationales were prepared by the independent contractor. Furthermore, some Orbiter subsystems were initially excluded from the review.

Initially, the Committee was concerned that these differences in procedure might reduce the validity and effectiveness of the FMEA/CIL reevaluation process. However, an audit by the Committee of the documentation and review process used by JSC in the case of the Orbiter indicated that it is a reasonable alternative to the RID process employed by MSFC. Nevertheless, the Committee suggested in its second interim report to NASA (see Appendix C) that the NSTS Program Office "review the FMEA/CIL reevaluation processes as implemented for each STS element to assure itself that any differences will not compromise the quality and completeness of the overall STS FMEA/CIL effort."

This more specific concern for procedural differences led, moreover, to a broader concern over the nature of management control within NASA. Differences in procedures used by the NASA centers in this context and others (e.g., with respect to the independence of STS certification, as discussed in Section 5.8) lead the Committee to suspect that an imbalance may exist between the authority of the centers and that of the NSTS Program Office. The Committee is concerned that such an imbalance can lead to serious problems in large programs where two or more centers have major roles in what must be a tightly integrated program, such as the NSTS and Space Station. Without strong, central program direction and integration, the suc-

cess and safety of these complex programs can be placed in jeopardy.

Recommendation (10d):

The Administrator should ensure that strong, central program direction and integration of all aspects of the STS are maintained via the NSTS Program Office.

5.10.5 Use of Non-Destructive Evaluation Techniques

Non-destructive evaluation (NDE) tests on the Solid Rocket Motor (SRM) are performed at the manufacturing plant. Subsequent transportation and assembly introduce a risk of debonding and other damage which may not be apparent upon visual inspection. No NDE is done on the SRMs in the "stacked" configuration at the launch facility.

New NDE techniques now being developed have potential applicability to the STS.

Problems have been detected by NASA and its contractor on the STS Solid Rocket Motor (SRM) with debonding between the propellant, liner, insulation, and case. In April 1986, a USAF Titan 34D (comparable in design to the SRM) experienced a destructive failure shortly after launch, due to debonding. No such severe consequences have been seen from SRM debonding, but bond line problems are nevertheless viewed as critical failure modes, especially given the redesign of the SRM joints. Voids within the propellant mass are also of concern. Destructive inspection of the SRM (e.g., cutting and probing) is not feasible, so non-destructive methods must be used. On the SRM, most of these tests are performed at the manufacturing plant; later transportation and assembly introduce a risk of debonding and other damage which may be more difficult to detect at the launch site.

There are essentially two issues here: the techniques employed and the location where inspection is done. Shuttle SRM NDE assessment to date has employed a combination of visual, ultrasonic, and radiographic techniques. The range of NDE techniques considered by NASA (but not necessarily tested) as of January 1987 is shown in Table 5-1. According to NASA's Aerospace Safety Advisory Panel, acoustic and thermographic techniques are

TABLE 5-1 Non-Destructive Evaluation Methods Considered By NASA

Method	Looks For	Remarks
Ultrasonics	Unbonds: case/insulation, inhibitor/propellant, and propellant/liner	Propellant/liner to be confirmed.
Radial radiography	Propellant voids/inclusions	
Tangential radiography	Gapped unbonds: Propellant/liner, flap bonds, and flap bulb configuration	
Thermography	Unbonds: case/insulation inhibitor/propellant, and propellant/liner	Limited experience base; prop./liner to be confirmed
Mechanical	Unbonds: near joint end case/insulation	Complex insulation geometry
Oblique-light video	Gapped edge unbonds: case/insulation and inhibitor/propellant	Magnifies and automates visual unbond inspection
Computed tomography	Gapped unbonds: all intersecting interfaces, propellant voids/inclusions	Long term
Holography	Unbonds: near joint end case/insulation	Excitation and scale concerns
Acoustic emission	Unbonds: case/insulation	Long term

(Source: NASA MSFC)

thought to be those with the greatest near-term potential for improving NDE capabilities with respect to the SRM.¹² Another promising group of techniques is based on X-ray technology. The USAF, in its Titan recovery program, has emphasized NDE techniques including ultrasonic, thermographic, and X-ray.¹³ Similar efforts are being pursued in the Navy's Trident program.¹⁴

With respect to the issue of location, NASA has determined that the "stacked" configuration of the SRM is not amenable to NDE of critical areas using available methods. However, NASA engineers believe that the assembly, rollout, and pad hold-down loads on the SRM will not cause debonding. Therefore, inspections are conducted at key processing points in the plant and at critical SRM segment locations before stacking at Kennedy Space Center. Nevertheless, the Committee remains concerned about the possibility of damage resulting from transportation, assembly, and rollout.

We recognize that NASA is (and has been) paying serious attention to the NDE issue. However, we believe that the technologies are developing rapidly enough that continued close attention is warranted.

Recommendation (10e):

The Committee recommends that NASA apply all practicable NDE techniques to the SRM at the launch facility, at the highest possible level of assembly (e.g., SRMs in the "stacked" configura-

tion), and emphasize development of improved NDE methods.

5.11 FOCUS ON RISK MANAGEMENT

The current safety assessment processes used by NASA do not establish objectively the levels of the various risks associated with the failure modes and hazards.

It is not reasonable to expect that NASA management or its panels and boards can provide their own detailed assessments of the risks associated with failure modes and hazards presented to them for acceptance.

Validation and certification test programs are not planned or evaluated as quantitative inputs to safety risk assessments. Neither are operating conditions and environmental constraints which may control the safety risks adequately defined and evaluated.

In the Committee's view, the lack of objective, measurable assessments in the above areas hinders the implementation of an effective risk management program, including the reduction or elimination of risks.

Throughout its audit the Committee was shown an extensive amount of information related to program flow charts, organizations, review panels and boards, information transmission, and reports. But the Committee did not become aware of an organization and safety-engineering methodology that could effectively provide an objective assessment of risk, as described in Section 4. Throughout the flow of NASA reports and approvals, both

¹² NASA: Aerospace Safety Advisory Panel, Annual Report for 1986 (February 1987).

¹³ Lt. Col. Frank Gayer, USAF Space Division, personal communication.

¹⁴ Dale Kenemuth, SP-273, Dept. of the Navy, personal communication.

before the 51-L mission and after, judgments are made and statements of assurance given by persons at every level which are based on data and assertions having a wide range of validity. The Committee believes that it is not reasonable to expect program management or NASA Level I management to provide its own in-depth evaluation of presented hazard risks. Nor will other panels or boards be able to do so without the necessary professional staff work being done. That work, in turn, cannot be performed without methods for assessing risk and controlling hazards. The methods must include the establishment of criteria for design margins which are consistent with the acceptable levels of risk.

The Associate Administrator for SRM&QA, in his new plan for management of NASA's SR&QA activities, stipulates that the SR&QA directors of the NASA centers are responsible for *assuring the safety* of their Center's products and services. However, we conclude that unless the safety organizations at the centers have (1) the appropriate methodology and tools (both analysis programs and personnel), and (2) the *authority* to establish criteria for safety margins, specific requirements on verification test programs, environmental constraints on operations, and total flight configuration validation, they *cannot* be held responsible for assuring an acceptable level of safety of flight systems. (In fact, they can never "assure safety," but only assure that the risks have been assessed objectively by approved methodologies, and that they are being controlled to the levels accepted by the appropriate NASA authorities.)

Figure 5-12 shows that even in the current post-51-L planning, the final result of the hazard analysis and safety assessment process is a NASA Space Shuttle Hazards Data Base. Having an approved list of accepted, identified hazards and a sophisticated closed-loop accounting and review system (the SIAP) may be useful. However, nearly every catastrophic accident since the beginning of the missile and space programs was caused by some already-identified hazard related to potential failure modes. The essence of safety-risk management, in the Committee's view, is not just the identification and acceptance of potential hazards, nor even the performance of a risk assessment for each failure mode and hazard; it is getting *control* of the conditions which turn potential into real. The FMEAs, CILs, hazard reports, and safety assessments identify risks, summarize information, ref-

erence data, provide status, etc. They do not analyze or establish the risk levels. Neither do they assess quantitatively the *validity* of the test programs in establishing failure margins, or define the operating conditions or environmental constraints which affect the risk levels.

We believe that the key requirements and concepts contained in various relevant NASA documents (see Section 3, for example) provide a good overall framework within which a comprehensive systems safety and risk management program could be defined and implemented. It is the opinion of the Committee that such a program would require bringing together appropriate activities into a focused "Systems Safety Engineering" (SSE) function at both Headquarters and the centers. This SSE function would apply across the entire set of design, development, qualification and certification, and operations activities of the NSTS. These activities would be an integral engineering element of the NSTS Program. They would involve more than just the preparation of reviews, reports, or data packages. Instead, systems safety engineering would combine the functions of reliability and systems safety analysis. It should be responsible for defining the requirements and procedures, and performing or managing, as appropriate, at least the following functions which comprise the basis of a risk assessment and risk management system:

1. Identification of failure modes and effects
2. Establishment of design criteria for redundancy
3. Identification of hazards and their potential consequences
4. Identification of critical items
5. Evaluation of the probability of occurrence of causes and consequences of failure modes and hazards
6. Establishment of safety-risk level criteria for design margins and hazard controls
7. Design of qualification and certification test programs
8. Objective assessment of safety risks
9. Development of acceptance rationale for retained hazards and hazard reports
10. Specification of environmental and operating constraints at all levels (parts, subsystem,

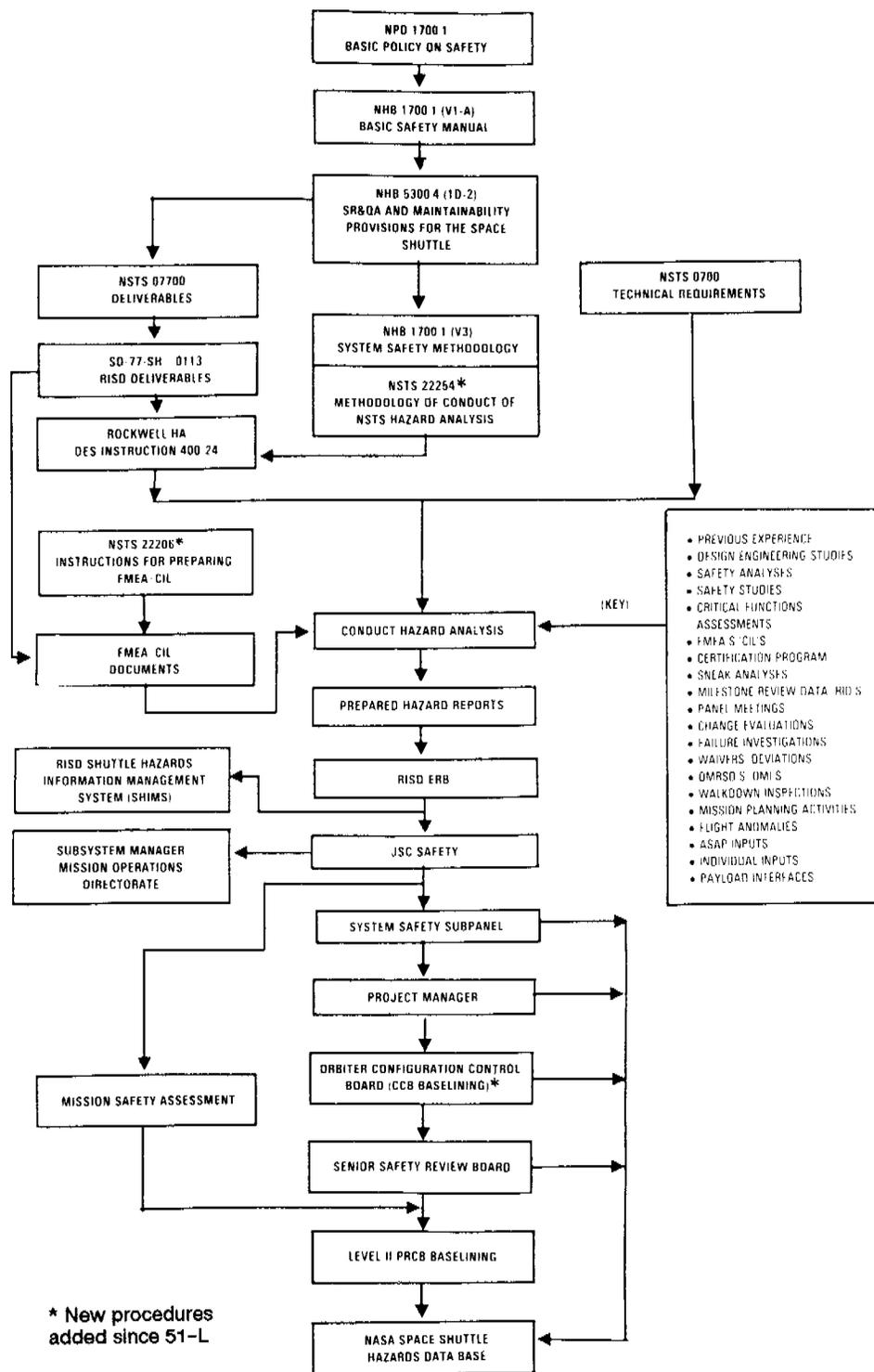


FIGURE 5-12 NASA NSTS safety analysis, Hazard Reports, and safety assessment process in 1987 (NASA JSC SR&QA).

- 11. Quantitative evaluation of flight data to update safety margin validations
 - 12. Oversight of quality assurance functions to control safety risks
 - 13. Overall system safety risk assessment and definition of the potential to reduce the level of risk.
- All of the above systems safety engineering functions (elaborated upon in Appendix F) are necessary both for achieving credible risk assessment and for

defining the risk controls required to justify acceptance of critical failure modes and other hazards. During design and development, the quantitative evaluation of relative risks for each design against acceptable criteria for levels of risk should be considered as an integral part of the systems engineering activity. These activities also would provide a definitive basis for establishing the design margins and operational constraints needed to reduce the overall risk to the accepted level and subsequently control the risk.

Function 13 above (definition of the potential to *reduce* the level of risk) is an essential input to risk management. The Committee has the impression that changes to the STS often are considered only if they will improve its performance or reduce risks to that level which has previously been accepted in the program. **The Committee believes that such risks, accepted in the past, logical as that may have appeared to be at the time, should not continue to be accepted without a concentrated effort to plan and implement a program to remove or reduce these risks.**

The magnitude of the preceding tasks point to the need for a large number of highly qualified professional systems safety engineers (i.e., systems engineers with a safety orientation) at NASA and at its major contractors. We were disturbed to learn from the Director of the Safety Division at Headquarters SRM&QA that, as of April 25, 1987, he had only *one* professional systems safety engineer in his division, and that he expects to add only two more in the near term and four additional ones in the long term. It is troubling to the Committee that this important and extremely complex systems engineering function should be so severely constrained by staff limitations, in light of the cost of the Shuttle and the risk to its crew.

Taken together, the tasks listed above have the highest leverage on overall risk assessment and the control of the causes of hazard. Only professionally dedicated systems safety engineers working together can develop the expertise and motivation to carry out these functions properly. They can perform their control of *validation* and *certification* programs in an objective way (if not functionally assigned to program organizations). The need for independent entities to perform certification and software IV&V to provide substantiation and confidence was discussed in Section 5.8. This risk-managed approach to the validation and certification functions, including the feedback of flight

data, should not be done by those responsible for design and development. They are *performance* oriented; they generally do not design hardware configurations to facilitate margin validation, and their proposed certification programs usually are not oriented to the demonstration of failure margins.

Finally, it seems to the Committee that it is not managerially reasonable to make an organization responsible for holding system safety to an agreed level of risk without according it responsibility and authority over all of the above functions, which actually control the risks.

Another major element of an overall risk management program is the quality assurance (QA) function. Quality assurance certifies that the hardware and software have been produced to the exact designs which describe the *validated* and *qualified* system. The "configuration" includes all aspects of the hardware and software, including the environments which in any way influence the properties of materials, stress margins, or temporal behavior of parts, subsystems, and elements.

In 1986, responsibility for policy and oversight of the quality assurance function was assigned to the new office of the Associate Administrator for SRM&QA. This is appropriate, because overall risk management and total systems safety are dependent on the quality assurance function throughout NASA. The QA function should be performed separately from the systems safety engineering functions (although there is certainly a strong oversight interaction between the two). Quality assurance should be a responsibility of each NASA center (and, of course, each contractor). Its purpose is not to design but to control and assure. As part of this function it should control the entire set of final released engineering documents describing the complete configuration of the system. As the Committee understands it, that is precisely NASA's current practice.

Recommendations (11):

The Committee recommends that NASA consider establishing a focused agency-wide Systems Safety Engineering (SSE) function, at both Headquarters and the centers, which would:

- be structured so as to be integrally involved in the entire set of design, development, validation, qualification, and certification activities;*
- provide a full systems approach to the continuous*

- identification of safety risks (not just failure modes and hazards) and the objective (quantitative) evaluation of such safety risks;*
- provide the output of this function to the NASA Program Directors in support of their risk management;*
 - support the Program Directors by providing assurance that their systems are ready for final*

safety certification to the risk levels established by the NASA Administrator.

The Committee also recommends that the STS risk management program, based in part on the definition of the potential to reduce the level of risk developed by the system safety risk assessment, include a concerted effort to remove or reduce the risks.

6 Lessons Learned

Although this report and its recommendations are directed to the NSTS Program, they are of broader applicability. It would be wise to consider the lessons learned by the Committee when structuring a risk assessment and management system for other programs with similar characteristics, such as the Space Station Program. These characteristics would include large size, use of highly complex technology, and major participation by several NASA centers and prime contractors. The following are generalized conclusions derived from the preceding sections. Numbers in parentheses refer to the principal sections of the report from which the conclusions were derived.

6.1 ELEMENTS OF AND RESPONSIBILITIES FOR RISK ASSESSMENT AND RISK MANAGEMENT

In the Committee's view, any large, complex, multi-center program should entail an overall risk assessment and risk management process which includes the following basic elements:

Risk assessment:

—A comprehensive method for identifying potential failure modes and hazards associated with the system.

—A specific, quantitative methodology for identifying and assessing (or estimating) the safety risks of the system.

Risk management:

—A management process by which the safety risks can be brought to levels or values that are

acceptable to the final approval authority. Risk management includes establishment of acceptable risk levels; the institution of changes in system design or operational methods to achieve such risk levels; system validation and certification; and system quality assurance. (4.1)

The Committee believes that *risk management* must be the responsibility of line management (i.e., the program manager and, ultimately, the Administrator of NASA). Only this program management, not the safety organizations, can make judicious use of the means available to achieve the operational goals while reducing the safety risks to acceptable levels. The safety organizations at NASA centers and Headquarters are staff organizations—i.e., they can and should be responsible for providing the *assessments of a system's risks*. They should also be responsible for assuring that the activities associated with controlling the risks to the levels assessed have been carried out and documented. Safety organizations cannot, however, assure safe *operation*; they can only assure that the safety risks have been properly evaluated, and that the system configuration and operation is being controlled to those risk levels which have been accepted by top management. (4.1, 4.3)

In each such major program, the risk assessment and management processes should be supported by a focused agency-wide Systems Safety Engineering function, at both Headquarters and the centers involved in the program, which would:

—be structured so as to be integrally involved in the entire set of design, development, validation, and qualification activities;

—provide a full systems approach to the continuous identification of safety risks (not just failure

modes and hazards) and the objective (quantitative) evaluation of such safety risks;

—provide the output of this function to the program director in support of his risk management process;

—support the program director by providing assurance that his system is ready for final safety certification to the risk levels established by the NASA Administrator. (5.11)

This focused systems safety engineering would combine the functions of reliability and systems safety analysis. It should be responsible for defining the requirements and procedures, and performing or managing, as appropriate, at least the following functions which should comprise the basis of a risk assessment and risk management system:

1. Identification of failure modes and effects
2. Establishment of design criteria for redundancy
3. Identification of hazards and their potential consequences
4. Identification of critical items
5. Evaluation of the probability of occurrence of causes and consequences of failure modes and hazards
6. Establishment of safety-risk level criteria for design margins and hazard controls
7. Design of qualification and certification test programs
8. Objective assessment of safety risks
9. Development of acceptance rationale for retained hazards and hazard reports
10. Specification of environmental and operating constraints at all levels (parts, units, subsystem, element, and system) to assure that validated margins are not violated
11. Quantitative evaluation of flight data to update safety margin validations
12. Oversight of quality assurance functions to control safety risks
13. Overall system safety risk assessment and definition of the potential to reduce the level of risk.

All of these systems safety engineering functions (elaborated upon in Appendix F) are necessary

both for achieving credible risk assessment and for defining the risk controls required to justify acceptance of critical failure modes and other hazards. During design and development, the quantitative evaluation of relative risks for each design against acceptable criteria for levels of risk should be considered as an integral part of the systems engineering activity. Finally, these activities would provide a definitive basis for establishing the design margins and operational constraints needed to reduce the overall risk to the accepted level and subsequently to control the risk. They also can provide a rational basis for decisions on which risks should be *reduced* through changes in design or procedures. (5.11)

In controlling risks, there must be a formal, continuing, and iterative linkage between the risk assessment and risk management processes, on the one hand, and the system's engineering change activities, on the other. (5.4)

As a program moves toward its operational phase, a system should be established for the rapid and effective feedback of inspection and test results, and repair and flight data into the risk assessment, risk management, and decision making processes. In the case of flight programs, this should include ensuring that all mission anomalies detected in real time and from recorded events, as well as those detected during the near-term inspection of any recovered hardware, are promptly fed into the formal risk assessment and management processes for action prior to committing to the next flight; all such anomalies should be called to the immediate attention of launch decision makers. (5.5)

6.2 ESTABLISHMENT OF RESPONSIBILITY FOR PROGRAM DIRECTION AND INTEGRATION

An imbalance between the authority of the NASA centers and that of the Program Office could lead to serious problems in a large program where two or more centers have major roles in what must be a tightly integrated program, such as the STS and Space Station. Without strong, central direction and integration, the success and safety of these complex programs can be placed in jeopardy. The Administrator of NASA should ensure that strong direction and integration of all aspects of such a program are maintained at Level I via the Program Office. (5.10.4) There also must be clear and unambiguous direction of the program at all levels.

Those responsible for decisions should be designated and known to all. Boards and panels should be advisory to these persons and not decision making bodies in themselves. (5.10.1)

6.3 THE NEED FOR QUANTITATIVE MEASURES OF RELATIVE RISK

Top management and program attention should be focused on those items with the greatest risk to the safety of a system by means of a prioritization of all contributors to the overall risk. (5.2) Acceptable levels of risk in each program should be set by the Administrator of NASA. However, suitable quantitative measures of risk, such as probabilistic risk assessment, are required to objectively define the acceptable levels, track progress toward achieving these levels, and evaluate alternate courses of action to reduce risk. (5.6, 5.11)

6.4 THE NEED FOR INTEGRATED REVIEW AND OVERVIEW IN THE ASSESSMENT OF RISK, AND IN INDEPENDENT EVALUATION OF RETENTION RATIONALES

There should be an *integrated* review process which provides a comprehensive, overall assessment of risk (including an *independent* evaluation, constantly updated, of retention rationales) upon which to base any decisions to grant waivers which permit operating with items that appear on the Critical Items List. (5.1, 5.3, 5.11) A balance is needed between "bottom-up" assessment tools (e.g., FMEA/CIL) and "top-down" analyses (e.g., hazard analyses). In particular, the "top-down" analysis processes must encompass an *integrated* system-wide engineering analysis, including a system safety analysis. (5.7)

6.5 INDEPENDENCE OF THE CERTIFICATION OF FLIGHT HARDWARE AND OF SOFTWARE VALIDATION AND VERIFICATION

Responsibility for approval of hardware certification and software Independent Validation and Verification (IV&V) should be vested in entities separate from the program management structure and the centers directly involved in the program's development and operation. However, the latter organizations should continue to conduct activities supporting certification and IV&V. (5.8)

6.6 SAFETY MARGINS FOR FLIGHT STRUCTURES

Safety margins for flight structures should be established which are in consonance with the accepted levels of safety risk for the program. However, great care is needed to properly verify that the margins have been achieved *and are maintained* in the flight structures. Verification can include the use of analytical models, but should be supported by static tests before flight, and—in the case of reusable flight hardware—continued monitoring in flight by permanently instrumenting, calibrating, and analyzing data from a representative flight system. Also, in the case of reusable hardware and man-rated systems destined to remain in orbit for long periods of time, comprehensive plans should be developed and implemented for conducting periodic inspection and maintenance of the structure of each system throughout the service life of each vehicle or platform. (5.10.2)

6.7 OTHER

There are other important factors in risk assessment and management which have been discussed in this report with respect to the STS as it existed following the Challenger accident. However, they are items which are considered to be less important than those enumerated above or not generally applicable to several other programs. Where applicable, they certainly should be given serious consideration in structuring the risk assessment and management program. These other factors are listed here by title and section reference:

Operational Issues (5.9)

—Launch Commit Criteria Waiver Policy (5.9.1)

—Human Factors as a Contributor to Risk (5.9.2)

—Cannibalization of Spare Parts (5.9.3)

Other Weaknesses in Risk Assessment and Management (5.10)

—Software Issues (5.10.3)

—Use of Non-Destructive Evaluation (NDE) Techniques (5.10.5).

For any new program, such as the Space Station, there is the opportunity to structure an optimum risk assessment and management program at the outset which builds on the experience gained in the NSTS Program and assembles those techniques which will be most effective in establishing, monitoring, and controlling risks to accepted levels.

APPENDIX A ACRONYMS AND DEFINITIONS

Acronyms:

AFSIG	Ascent Flight Systems Integration Group
ALT	Approach and Landing Test
APU	Auxiliary Power Unit (in the Orbiter)
ASAP	Acrospace Safety Advisory Panel
BFS	Backup Flight System
CB	Control Board (generic)
CCB	Configuration Control Board
CCP	Configuration Control Panel
CDR	Critical Design Review
CFA	Critical Functions Assessment
CI	Configuration Inspection
CIL	Critical Items List
CIRA	Critical Item Risk Assessment
CR	Change Request
DCR	Design Certification Review
DER	Designated Engineering Representative (for the FAA)
DES	Data Exchange System
DR	Discrepancy Report
ERB	Engineering Review Board
EIFA	Element Interface Functional Analysis
EMF	Electromotive force
ET	External Tank
FAA	Federal Aviation Administration
FACI	First Article Configuration Inspection
FAP	Failure Analysis Program
FMEA	Failure Modes and Effects Analysis
FMEA/CIL	Failure Modes and Effects Analysis, and Critical Items List
FRR	Flight Readiness Review
GFE	Government Furnished Equipment
GPC	General Purpose Computer (on the Orbiter)
GSE	Ground Support Equipment
HA	Hazard Analysis
HPU	Hydraulic Power Unit (in the SRB)
HQ	Headquarters (of NASA)
HR	Hazard Report
IBM	International Business Machines
IHA	Integrated Hazard Analysis
IUS	Inertial Upper Stage
IV&V	Independent Validation and Verification
JSC	Johnson Space Center
KSC	Kennedy Space Center

LCC	Launch Commit Criteria
LLS	Launch and Landing Site
LRU	Line Replaceable Unit
LOV	Loss of Vehicle
MET	Mission Evaluation Team
MFG	Manufacturing
MICB	Mission Integration Control Board
MOD	Mission Operations Directorate (at JSC)
MPTA	Main Propulsion Test Article
MSA	Mission Safety Assessment
MSFC	Marshall Space Flight Center
MVGVT	Mated Vehicle Ground Vibration Test
NASA	National Aeronautics and Space Administration
NDE	Non-Destructive Evaluation
NHB	NASA Handbook
NMI	NASA Management Instruction
NPD	NASA Policy Directive
NRC	National Research Council
NSIS	NASA Safety Information System
NSTS	National Space Transportation System
OASCB	Orbiter Avionics Software Control Board
OMI	Operations and Maintenance Instructions
OMRS	Operations and Maintenance Requirements and Specifications
OMRSD	Operations and Maintenance Requirements and Specifications Document
PASS	Primary Avionics Software System
PCASS	Program Compliance Assurance Status System
PDR	Preliminary Design Review
PR	Problem Report
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action (system)
PRCB	Program Requirements Control Board
QA	Quality Assurance
QRA	Quantitative Risk Assessment
QRM	Quantitative Risk Model
RID	Review Item Discrepancy (report)
RISD	Rockwell International, Space Division
RMPP	Risk Management Program Plan
SAIL	Shuttle Avionics Integration Laboratory
SASCB	Shuttle Avionics Software Control Board
SASR	Shuttle Avionics Systems Review
SCA	Shuttle Carrier Aircraft
SCAP	Shuttle Configuration Analysis Program
SCRHAAC	Shuttle Criticality Review and Hazard Analysis Audit Committee
SHIMS	Shuttle Hazard Information Management System
SIAP	System Integrity Assurance Program
SIMR	Systems Integration Management Review
SIR	Systems Integration Review (board)
SR&QA	Safety, Reliability, and Quality Assurance

SRB	Solid Rocket Booster
SRM	Solid Rocket Motor (of the SRB)
SRM&QA	Safety, Reliability, Maintainability, and Quality Assurance
SSE	Systems Safety Engineering
SSM	Subsystem Manager
SSME	Space Shuttle Main Engine
SSUS	Space Shuttle Upper Stage
STS	Space Transportation System
UCR	Unsatisfactory Condition Report
USAF	United States Air Force
VLS	Vandenberg Launch Site

Definitions:

Certification	—consists of qualification tests, major ground tests, and other tests and/or analyses required to determine that the design of hardware from component through subsystem level meets requirements; a part of verification.
Qualification	—is used in terms of qualification tests (see certification), to establish that an item meets requirements.
Validation	—the confirmation of some state or condition determined earlier.
Verification	—the process of planning and implementing a program that determines that Shuttle systems meet all design, performance, and safety requirements. The verification process (for both hardware and software) includes all development, certification and acceptance testing, flight demonstration, appropriate pre-flight checkout, post-flight activities, and analyses necessary to support verification.

APPENDIX B

ESTABLISHING REPORTS AND DOCUMENTS

The Shuttle Criticality Review and Hazard Analysis Audit Committee of the National Research Council held its opening meeting on September 22, 1986, in Washington, D.C. This appendix contains the following key references leading up to its establishment.

	<i>Page</i>
<i>Report of the Presidential Commission on the Space Shuttle Challenger Accident</i> , William P. Rogers, Chairman, June 6, 1986. Excerpt: Vol. I, pp. 198–199, Recommendations: introduction and Recommendation III.	88
Letter from the President of the United States to the Administrator of the National Aeronautics and Space Administration, June 13, 1986, directing that the recommendations of the Presidential Commission be implemented.	90
Letter from the Administrator of NASA to the Chairman, National Research Council, July 3, 1986, requesting the NRC to form an audit panel as called for in Recommendation III of the Presidential Commission.	91
Letter from the Chairman of the National Research Council to the Administrator of NASA, July 15, 1986, agreeing to establish an audit panel under the National Research Council.	93
Report to the President: <i>Actions to Implement the Recommendations of The Presidential Commission on the Space Shuttle Challenger Accident</i> , NASA, July 14, 1986, excerpt from p. 19.	94
<i>Statement of Task</i> , Committee on Space Shuttle Criticality Review and Hazard Analysis Audit, November 12, 1986 (revision).	95



Presidential Commission
on the
Space Shuttle Challenger Accident

June 6, 1986

Dear Mr. President:

On behalf of the Commission, it is my privilege to present the report of the Presidential Commission on the Space Shuttle Challenger Accident.

Since being sworn in on February 6, 1986, the Commission has been able to conduct a comprehensive investigation of the Challenger accident. This report documents our findings and makes recommendations for your consideration.

Our objective has been not only to prevent any recurrence of the failure related to this accident, but to the extent possible to reduce other risks in future flights. However, the Commission did not construe its mandate to require a detailed evaluation of the entire Shuttle system. It fully recognizes that the risk associated with space flight cannot be totally eliminated.

Each member of the Commission shared the pain and anguish the nation felt at the loss of seven brave Americans in the Challenger accident on January 28, 1986.

The nation's task now is to move ahead to return to safe space flight and to its recognized position of leadership in space. There could be no more fitting tribute to the Challenger crew than to do so.

Sincerely,

A handwritten signature in black ink, appearing to read "William P. Rogers", written in a cursive style.

William P. Rogers
Chairman

The President of the United States
The White House
Washington, D. C. 20500

600 Maryland Avenue, S.W.

Washington, D.C. 20024

(202)453-1405

EXCERPTS FROM:

*Report of the Presidential Commission on the
Space Shuttle Challenger Accident*

William P. Rogers, Chairman
June 6, 1986

Pages 198–199

Recommendations

The Commission has conducted an extensive investigation of the Challenger accident to determine the probable cause and necessary corrective actions. Based on the findings and determinations of its investigation, the Commission has unanimously adopted recommendations to help assure the return to safe flight.

The Commission urges that the Administrator of NASA submit, one year from now, a report to the President on the progress that NASA has made in effecting the Commission's recommendations set forth below:

— III —

Criticality Review and Hazard Analysis. NASA and the primary Shuttle contractors should review all Criticality 1, 1R, 2, and 2R items and hazard analyses. This review should identify those items that must be improved prior

to flight to ensure mission success and flight safety. An Audit Panel, appointed by the National Research Council, should verify the adequacy of the effort and report directly to the Administrator of NASA.

THE WHITE HOUSE

WASHINGTON

June 13, 1986

Dear Jim:

I have completed my review of the report from the Commission on the Space Shuttle CHALLENGER Accident. I believe that a program must be undertaken to implement its recommendations as soon as possible. The procedural and organizational changes suggested in the report will be essential to resuming effective and efficient Space Transportation System operations, and will be crucial in restoring U.S. space launch activities to full operational status.

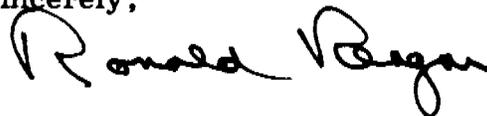
Specifically, I would like NASA to report back to me in 30 days on how and when the Commission's recommendations will be implemented. This report should include milestones by which progress in the implementation process can be measured.

Let me emphasize, as I have so many times, that the men and women of NASA and the tasks they so ably perform are essential to the nation if we are to retain our leadership in the pursuit of technological and scientific progress.

Despite misfortunes and setbacks, we are determined to press on in our space programs. Again, Jim, we turn to you for leadership. You and the NASA team have our support and our blessings to do what has to be done to make our space program safe, reliable, and a source of pride to our nation and of benefit to all mankind.

I look forward to receiving your report on implementing the Commission's recommendations.

Sincerely,



The Honorable James C. Fletcher
Administrator
National Aeronautics and
Space Administration
Washington, D.C. 20546



National Aeronautics and
Space Administration

Washington, D C
20546

Office of the Administrator

JUL 3 1986

Dr. Frank Press
Chairman
National Research Council
2101 Constitution Avenue
Washington, DC 20418

Dear Frank:

On May 20, 1986, I wrote to you requesting that the National Research Council (NRC) form an oversight committee to review the work of NASA and our contractors in the necessary redesign, retest, and recertification of the Solid Rocket Motor (SRM). Your letter of June 2, 1986, provided NRC acceptance of this request, and the committee is now heavily involved in its work. I believe that a very effective relationship has been established among the parties involved. These actions are consistent with the first recommendation of the Presidential Commission on the Space Shuttle Challenger Accident.

I must now, however, ask you for further assistance as we take the actions necessary to return the Shuttle to flight status. Recommendation III states that NASA and the primary Shuttle contractors should review all Criticality 1, 1R, 2, and 2R items and hazard analyses and that the review should identify those items that must be improved prior to flight to ensure mission success and flight safety. The Commission also recommends that "An audit panel appointed by the National Research Council should verify the adequacy of the effort and report directly to the Administrator of NASA." This letter is to request that the NRC form such an audit panel, verify the adequacy of the effort, and report to me.

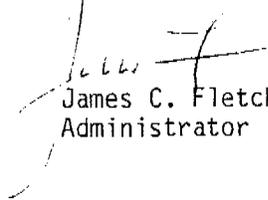
The review of these criticality items is under way within the STS program at this time and is anticipated to be completed in early 1987. The current review is being conducted at the individual project level with program level reviews scheduled to begin in the fall. A review of our approach by your panel would be most helpful prior to the beginning of the program level reviews. Subsequent plans for participation by the panel in the process and the reviews will be developed following this initial review.

NASA will provide the audit panel with access to all information and technical data necessary to perform the functions of the review. Background and orientation briefings will be provided by NASA and appropriate contractor personnel to permit the panel to proceed with their assessment. Additional meetings and data exchanges with NASA and/or contractor personnel will be arranged as requested by the panel.

The principal NASA contact during the course of the review will be Mr. Jay F. Honeycutt of the Office of Space Flight, telephone 453-1261. The expense of the work of the committee will be covered by an addition to NASW-3511.

I appreciate the willingness of the National Research Council to undertake this audit responsibility.

Sincerely,



James C. Fletcher
Administrator

NATIONAL RESEARCH COUNCIL

2101 CONSTITUTION AVENUE WASHINGTON, D. C. 20418

July 15, 1986

OFFICE OF THE CHAIRMAN

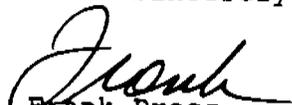
The Honorable
James C. Fletcher
Administrator
National Aeronautics and Space Administration
Washington, D.C. 20546

Dear Jim:

I write in response to your letter of July 3, 1986, requesting that the National Research Council appoint an audit panel to review the NASA approach to resolving flight-critical items. The National Research Council will undertake this task, and will work to get started expeditiously. As you know, members of the NRC staff have already met with NASA headquarters management to discuss the scope of this effort.

We will begin by having a one or two day scoping effort to better understand the NASA criticality review system as well as alternative review and evaluation procedures that are used in analogous situations. Upon conclusion of this first discussion, we should be ready to select a panel and proceed with the effort.

Yours sincerely,



Frank Press
Chairman

cc: Philip E. Culbertson
Jay F. Honeycutt

THE NATIONAL RESEARCH COUNCIL IS THE PRINCIPAL OPERATING AGENCY OF THE NATIONAL ACADEMY OF SCIENCES AND THE NATIONAL ACADEMY OF ENGINEERING
TO SERVE GOVERNMENT AND OTHER ORGANIZATIONS.



National Aeronautics and Space Administration

Report to the President

Actions to Implement the Recommendations

*of The Presidential Commission
on the Space Shuttle Challenger Accident*

EXCERPT FROM PAGE 19:

The Commission recommended that the National Research Council (NRC) appoint an Audit Panel to verify the adequacy of this effort and report directly to the Administrator of NASA. This request has been made by NASA and accepted by the NRC. The NRC is forming the panel and NASA will support them as required.

July 14, 1986
Washington, D.C.

Code Designator for Group: _____

Commission on Engineering and
Technical Systems
ASSEMBLY OR COMMISSION

Committee on Space Shuttle Criticality
Review and Hazard Analysis Audit
COMMITTEE

Aeronautics and Space Eng'g. Board
DIVISION, OFFICE OR BOARD

SUB-UNIT

STATEMENT OF TASK

(Make clear what is expected of the group described and by whom the project is sponsored. Limit to not more than this page.)

As recommended in the report of the Presidential Commission on the Space Shuttle Challenger Accident, the Committee will audit the review by NASA and its primary Shuttle contractors leading to the identification by NASA of those items that must be improved prior to resumption of flight to ensure mission success and flight safety. Particular attention will be given to the Failure Modes and Effects Analyses (FMEA), Critical Item Lists (CIL), and Hazard Analyses. The audit will concentrate on procedures, techniques, and a sampling of specific actions taken by NASA and the contractors in order to verify the adequacy of the effort. The results of the audit will be reported directly to the Administrator of NASA by a series of letter reports and a final report.

The Executive Committee of the Governing Board of the National Research Council approved this effort at its meeting on August 26, 1986

The work of the Committee is carried out under Contract No. NASW-3511 with the National Aeronautics and Space Administration.

November 14, 1986
Date of Statement

September 5, 1986
(Date of previous statement if applicable)

COMMITTEE RECORDS FORM #1

APPENDIX C

LETTER REPORTS TO THE ADMINISTRATOR OF NASA AND NASA RESPONSE

Prior to this final report, the Shuttle Criticality Review and Hazard Analysis Audit Committee issued two interim letter reports to the Administrator of the National Aeronautics and Space Administration. The Administrator of NASA provided a response to the Committee regarding the first interim report. It also was referenced in NASA's Report to the President of June 1987. These documents are contained in this appendix.

	<i>Page</i>
First interim letter report to the Administrator of NASA from Committee Chairman Alton D. Slay, January 13, 1987, 4 pp.	98
Reply to Committee Chairman Alton D. Slay from the Administrator of NASA regarding the first report, April 22, 1987	102
Report to the President: <i>Implementation of the Recommendations of The Presidential Commission on the Space Shuttle Challenger Accident</i> , NASA, June 1987, excerpts from pp. 41-42	104
Second interim letter report to the Administrator of NASA from Committee Chairman Alton D. Slay, July 22, 1987, 8 pp.	107

NATIONAL RESEARCH COUNCIL
COMMISSION ON ENGINEERING AND TECHNICAL SYSTEMS
2101 Constitution Avenue Washington, D. C. 20418

AERONAUTICS AND SPACE
ENGINEERING BOARD

January 13, 1987

The Honorable James C. Fletcher
Administrator
National Aeronautics and Space Administration
Washington, D.C. 20546

Dear Jim:

This is an interim progress report of the Shuttle Criticality Review and Hazard Analysis Audit Committee. The National Research Council formed this committee in response to your request for an audit of the NASA response to the Presidential Commission Recommendation III regarding criticality review and hazard analysis.

The Committee has been a functioning entity since its first meeting on September 22, 1986. We have thus far received presentations from and engaged in detailed discussions with NASA Headquarters, the National Space Transportation System program office, Johnson Space Center, Marshall Space Flight Center, and Kennedy Space Center. Similar meetings were held at Rocketdyne (Space Shuttle Main Engine) and Rockwell International (Orbiter), and by a working group at Morton Thiokol (Solid Rocket Motor). All of the participants described their efforts and progress in reevaluating the Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL) status and in reassessing hazard analysis and risk management. The Committee also has received a briefing on and discussed the process being used by the U.S. Air Force Systems Command-Space Division to determine launch readiness and safety status. The Titan 34D Recovery Program was described as an example.

The Committee has been favorably impressed by the dedicated effort and extremely beneficial results obtained thus far from the FMEA/CIL and hazard analysis processes. We are very appreciative of the frank and open manner in which NASA and contractor personnel have worked with the Committee. Our suggestions have been received in a very responsive manner in all quarters. We wish to commend Admiral Truly, Arnold Aldrich and the NASA Shuttle team involved in the FMEA/CIL-hazard analysis processes for the significant work they have performed so far. Although our general impressions are favorable, we do have some suggestions for improvement. In summary, they are:

- o Criticality 1 and 1R items should be assigned priorities based on the probability of occurrence.
- o Since many of the Criticality 1 and 1R items differ substantially in terms of the probability of failure, NASA should consider modifying the definition of critical items to account for these differences.

The National Research Council is the principal operating agency of the National Academy of Sciences and the National Academy of Engineering to serve government and other organizations

Letter to the Honorable James C. Fletcher

- 2 -

- o NASA should incorporate its present total system review procedures in an integrated systems assessment process coupled closely with the FMEA/CIL reevaluation now being undertaken.
- o Linkage between the STS engineering change activities and the FMEA/CIL-hazard analysis processes should be assured.

SETTING PRIORITIES FOR CRITICALITY 1 AND 1R ITEMS

NASA does not now set priorities for Criticality 1 and 1R items nor does it consider the probability of occurrence of an event in the treatment of these items. The Committee recommends that NASA devise some mechanism for and assign priorities to the Criticality 1 and 1R items. It suggests that probability of occurrence should be an important element of any such priority reasoning. Basing priorities on this fundamental measurement of risk will help NASA and those interested in its progress to evaluate the adequacy of changes being made to Shuttle hardware, software, or procedures in the interest of enhancing safety.

Essential to the success of any risk assessment process is the certain and timely feedback of preflight and postflight system performance data, along with test data and failure or degradation reports. Such inputs are critical to any successful FMEA/CIL and hazard analysis program and can form the basis for more precise evaluation of risk. While it is clear to the Committee that these data are used in readiness reviews and other NASA activities, it is not clear that they are used in the FMEA/CIL or hazard analysis processes. The Committee believes that this information can, if properly used, assist greatly in the FMEA/CIL and hazard analysis processes and in the determination of priorities.

The present decision-making process within NASA with regard to FMEA/CIL appears to be based on the judgment of experienced practitioners and has received very little contribution from quantitative analysis. We believe that the failure of NASA to use numerical techniques as an input to decision-making detracts from the overall effectiveness of the FMEA/CIL and hazard analysis processes. Such techniques could provide a more realistic assessment of risk, at least on a relative basis. We do not wish to suggest that NASA subordinate technical judgment to numerical analysis. Such an approach would be, in our opinion, unrewarding and perhaps counterproductive.

Currently waiver authority for all Criticality 1 and 1R items rests with NASA Level I. The Committee believes that Level I should focus its attention on the highest priority items resulting from the

Letter to the Honorable James C. Fletcher

- 3 -

suggested selection process, along with the rationale that produced the priority rating. The waiver decision authority for the remainder of the Criticality 1 and 1R items should be delegated to Levels II and perhaps III.

DEFINITION OF CRITICALITY CATEGORIES

The Committee notes that the dedicated response of the entire NASA organization and its contractors has produced a variety of items which, by precise definition, must be placed in the Criticality 1 or 1R categories. Many of the items differ substantially from one another in terms of the probability of failure or malperformance and thus their potential impact on Shuttle operational safety. The Committee suggests that NASA consider a modification of the Critical Items List to account for these differences, help the priority selection process, and better focus present or future efforts to achieve safer Shuttle operations.

INTEGRATED SPACE TRANSPORTATION SYSTEM ANALYSIS

The Committee understands that various mechanisms are being used by NASA to examine total system operation, including propagation of failure modes to interfacing or physically adjacent modules or subsystems. The Committee does not perceive, however, any formal relationship of such evaluation methods to the ongoing FMEA/CIL process. The Committee suggests that NASA devise an integrated STS systems assessment process which is closely coupled with the FMEA/CIL activity to assure assessment of the truly critical safety elements in the STS. This includes all combinations of hardware/software/procedural failures and cascading failures.

RELATION BETWEEN FMEA/CIL-HAZARD ANALYSIS AND DESIGN CHANGES

We note that many engineering changes have been undertaken since the 51-L accident to improve Shuttle safety prior to resumption of flight, now scheduled for February 1988. In parallel, the FMEA/CIL and hazard analysis reevaluations are under way with completion expected during the summer of 1987. Thus, the FMEA/CIL reevaluation may not adequately reflect all of the engineering changes, nor will there be time to incorporate any substantial design changes that may be indicated by the outcome of the FMEA/CIL reevaluation, hazard analyses, and related activities. The Committee recommends that NASA assure a close linking between the STS engineering change activities and the FMEA/CIL-hazard analysis processes.

Letter to the Honorable James C. Fletcher

- 4 -

FUTURE WORK

The Committee is continuing its effort to audit the FMEA/CIL, hazard analysis, and related processes dealing with risk assessment. We have planned additional visits to NASA centers and contractor facilities where we will continue to examine the mechanisms used by NASA and its contractors to provide for the overall safety of the STS as an integrated system. We also will further refine some of the points raised here in future reports to you. While we recognize that it is not possible a priori to ensure mission success and flight safety, through this review and audit we hope to assist NASA in taking those prudent steps which will provide a reasonable and responsible level of assurance of flight safety. We will, of course, remain in close contact with your staff throughout this activity.

Sincerely yours,



Alton D. Slay
Chairman
Committee on Shuttle Criticality
Review and Hazard Analysis Audit

cc: Admiral Richard H. Truly



National Aeronautics and
Space Administration

Washington, D.C.
20546

Office of the Administrator

APR 22 '87

General Alton D. Slay
National Research Council
National Academy of Engineering
2101 Constitution Avenue, NW (NAS 307)
Washington, DC 20418

Dear Al:

In reply to your January 13, 1987, interim progress report of the Committee on Shuttle Criticality Review and Hazard Analysis, your four suggestions are repeated, along with NASA's response to each.

NRC Comment: "Criticality 1 and 1R items should be assigned priorities based on the probability of occurrence." (This comment also suggested the use of probability analysis techniques and the delegation of certain criticality items to lower levels of the organization.)

NASA Response: The National Space Transportation System is in the process of selecting and implementing a critical items prioritization technique for the Shuttle program. Five different techniques have been evaluated by review teams at JSC, MSFC, and KSC. One of these techniques has been selected to be presented to the program manager at a Program Requirements Control Board (PRCB) for baselining as a formal program requirement. The chosen approach will overlay the existing Failure Mode and Effects Analysis/Critical Items List (FMEA/CIL) activity with minimum perturbation, yet provide an effective measure of relative risk in order to focus future review emphasis and resource allocations. In parallel with the prioritization technique development, an effort is also under way to assess the utility of probabilistic risk assessment in the NSTS FMEA/CIL process. Activities have been initiated to engage two independent firms with expertise in probabilistic risk assessment to perform detailed reviews of the orbiter auxiliary power unit and the shuttle main propulsion pressurization system. A decision to apply such probabilistic risk assessment techniques to other elements of the Shuttle will depend upon assessments of the results and impacts of those efforts and comparison of these results with the results of the mainline FMEA/CIL activity. Delegating the review and approval of certain critical items will be decided after the results of the prioritization and risk assessment activities have been thoroughly assessed.

NRC Comment: "Since many of the Criticality 1 and 1R items differ substantially in terms of the probability of failure, NASA should consider modifying the definition of critical items to account for these differences."

NASA Response: We expect the FMEA/CIL prioritization process will provide the necessary definitions and program focus in this regard.

NRC Comment: "NASA should incorporate its present total system review procedures in an integrated systems assessment process coupled closely with the FMEA/CIL reevaluation now being undertaken."

NASA Response: Since the Challenger accident, NASA has reemphasized its risk management effort. An important feature of the revised effort must be a "systems engineering" approach that integrates the various elements of the risk management process to assure assessment of the combinations of hardware, software, procedures, and cascading failures. NASA's new Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance has been tasked to develop a new agencywide risk management system.

NRC Comment: "Linkage between the STS engineering change activities and the FMEA/CIL hazard analysis processes should be assured."

NASA Response: Engineering changes are processed through the same Space Shuttle configuration control boards that conduct the review of the FMEA/CIL. A recent change to the procedure requires an assessment of each change request to determine if it affects any Criticality 1 or 2 hardware. The nature of the combined change control and FMEA/CIL processes is such that the total process cannot be completed until the last change to be implemented before flight has itself undergone a FMEA and been dispositioned by the board. Regardless of the timetable established by the NSTS working schedule for FMEA/CIL preparation and review, the changes that result will be dealt with in the same manner as the generating FMEA items. All changes mandatory for first flight will undergo the same rigor, even if this results in a flight schedule impact. The NSTS Systems Design Reviews which began early last year have significantly reduced the likelihood of new changes being identified that have major schedule impacts.

The dedication of your committee and the sincerity of its comments are very much appreciated by NASA. I hope you find our actions in response to your suggestions to be both appropriate and timely. Thank you again for your help.

Sincerely,


James C. Fletcher
Administrator

Report to the President

IMPLEMENTATION
of the
RECOMMENDATIONS

of the Presidential Commission
on the Space Shuttle
Challenger Accident

June 1987



EIFA's have been conducted on ET/orbiter, SSME/orbiter, and SRB/ET/orbiter interfaces. These analyses have been reviewed by NASA and the systems integration contractor, and the results are under evaluation by the element project offices and the NSTS Engineering Integration Office. When this review is completed, the finalized EIFA's will be presented to the PRCB for formal approval.

NATIONAL RESEARCH COUNCIL AUDIT

The Shuttle Criticality Review and Hazard Analysis Audit Committee of the National Research Council (NRC), chaired by retired USAF General Alton Slay, reports directly to the NASA Administrator and is responsible for verifying the adequacy of the proposed actions for returning the Space Shuttle to flight status (see Appendix F for panel membership and a summary of responsibilities).

The committee has discussed the FMEA/CIL/HA reevaluation process with representatives from NASA Headquarters, JSC, KSC, and MSFC. Meetings have been held at the centers and at Rockwell International's Space Transportation Systems and Rocketdyne divisions; Morton Thiokol; United Space Boosters, Inc.; Sundstrand Corporation; and NRC Headquarters. The committee is evaluating the adequacy of the review process, checking for continuity across all elements of the program, and reviewing changes that NASA and its contractors have made since the accident.

A preliminary report was submitted to the NASA Administrator on January 13, 1987, indicating that the committee has been favorably impressed with the results obtained from the FMEA/CIL and hazard analysis processes. While the committee's general impressions were favorable, it did make some suggestions for improvements. In summary, these suggestions are: (1) Criticality 1 and 1R items should be assigned priorities based on the probability of occurrence; (2) since many of the Criticality 1 and 1R items differ substantially in terms of the probability of failure, NASA should consider modifying the

definition of critical items to account for these differences; (3) NASA should incorporate its present system review procedures into an integrated system assessment process coupled closely with the FMEA/CIL reevaluation now being undertaken; (4) linkage between the STS engineering change activities and the FMEA/CIL/HA processes should be provided.

NASA has responded to these suggestions in the following manner:

1. Several candidate systems for prioritizing critical items have been evaluated by each of the projects. A hybrid system has been developed that incorporates the positive features of the candidate systems and specifically addresses probability of occurrence. The approach can be overlaid on the existing FMEA activity with minimum perturbation, providing an effective measure of relative risk.
In parallel with the development of prioritization techniques, an effort is under way to determine the applicability of probability risk assessment to the FMEA/CIL process. This technique is used in the nuclear power industry to provide relative-risk assessments. Two firms with expertise in probability analysis have been selected to perform detailed assessments of the orbiter auxiliary power unit and the main propulsion engine pressurization system. A decision to apply probability analysis techniques to other systems of the program will depend on the results of these assessments.
2. The FMEA/CIL prioritization process will provide the necessary program focus and more definitive definitions in response to the committee's concern expressed in their second suggestion.
3. Since the accident, NASA has reemphasized its risk management effort. An important feature of the revised effort is a "systems engineering" approach that integrates the various elements of hardware and software failure analysis. Further discussion of risk management is included in the response to Recommendation IV.
4. Engineering changes are processed through the same project and program control boards that conduct and approve the reviews of the FMEA/CIL. Each

change request will be assessed to determine if it affects any Criticality 1 or 2 hardware to ensure that the required linkage is provided.

The NRC audit committee is reviewing additional areas to identify potential methods of reducing risk. These include the design qualification and flight certification processes, launch commit criteria and waiver policy, and the generation, review, and approval of retention rationale for waivers to critical items.

Also being reviewed are the overall safety, reliability, maintainability, and quality assurance program, the definition of struc-

tural analysis requirements, the establishment and verification of analyses for margins of safety, the risk management processes for software, and the processes for analyzing payload safety.

Interim findings and recommendations from these reviews will be submitted to the NASA Administrator through letter reports, as required. The final report, anticipated in 1987, will include an assessment of the procedures reviewed and recommendations for improving the Shuttle risk management system. As reports are received, any recommendations included will be reviewed by NASA and responses will be provided to NRC.

NATIONAL RESEARCH COUNCIL
COMMISSION ON ENGINEERING AND TECHNICAL SYSTEMS
2101 Constitution Avenue Washington, D C 20418

AERONAUTICS AND SPACE
ENGINEERING BOARD

July 22, 1987

The Honorable James C. Fletcher
Administrator
National Aeronautics and Space Administration
Washington, D.C. 20546

Dear Jim:

I am pleased to provide this second interim progress report of the National Research Council's Committee on Shuttle Criticality Review and Hazard Analysis Audit. I wish to thank you for your letter of April 22, 1987, in which you summarized the steps that the National Aeronautics and Space Administration (NASA) is taking in response to the suggestions in our first report to you of January 13, 1987. The Committee is indeed gratified by the progress NASA is making in strengthening the Space Transportation System (STS) risk management program. We also appreciate the continued close collaboration with NASA and contractor personnel, and note the interest they show and their responsiveness to the Committee's suggestions. The purpose of this letter is to react to the actions of NASA taken in response to our first letter, and to comment on some additional aspects of STS risk management.

Since our last report, the full Committee has met six more times, including visits to Marshall Space Flight Center, Kennedy Space Center, again to Rocketdyne on the Space Shuttle Main Engine (SSME), and with Rockwell Space Transportation System Division on STS integration. Working groups of the Committee also met at appropriate NASA centers and contractors to review the risk management aspects of the Solid Rocket Booster (SRB); Orbiter Auxiliary Power Unit (APU) and SRB Hydraulic Power Unit (HPU); Shuttle structural analysis, margins and verification; Orbiter nose wheel steering; software; and Space Shuttle Main Engine. This continued audit has allowed the Committee to evaluate the changes NASA is making in the STS risk management processes and to identify some additional views which we thought would be useful to share with you in this interim report.

Regarding the response of NASA to the first report, the Committee's reaction is, in summary:

- o The work under way to assign priorities to Criticality 1 and 1R items appears to be a significant step forward. We also are pleased to note the tests of Probabilistic Risk Assessment (PRA) now being conducted.
- o The Committee looks forward to learning how the prioritization process will be used to redefine the critical items by taking into account the differences in the probability of occurrence.

The National Research Council is the principal operating agency of the National Academy of Sciences and the National Academy of Engineering to serve government and other organizations

Letter to the Honorable James C. Fletcher

- 2 -

- o We enthusiastically support the agency-wide risk management system now being developed. However, we are still concerned with the apparent lack of consideration of the STS as a single, complex system rather than a collection of subsystems.
- o The steps taken to link the engineering change control and the Failure Modes and Effects Analyses/Critical Items List (FMEA/CIL) processes are both appropriate and welcome. We are also reassured by your statement that the flight schedule will not be allowed to reduce the rigor with which the risk management tasks will be conducted.

The Committee's continuing audit since our last interim report leads us to provide initial comments on the following topics:

- o Persons involved in the STS program frequently give the impression that decisions are made collectively by panels, boards, etc., rather than by the responsible individuals. We believe that the Administrator of NASA should periodically remind the NASA organization of the specific individuals responsible for final decisions based on the advice received from each advisory body.
- o The new System Integrity Assurance Program (SIAP), especially its Program Compliance Assurance and Status System (PCASS), now being implemented by the National Space Transportation System (NSTS) Program office, will be invaluable as a tool in support of STS risk management. The STS failures data base, when completed, can be of major importance in determining the probability that the worst case effect postulated in the FMEA will actually occur.
- o The progress being made in improvements to the SSME as a result of the FMEA/CIL reevaluation is very encouraging.
- o The changes being introduced in NASA Headquarters Safety, Reliability, Maintainability and Quality Assurance (SRM&QA) appear to be well planned and in the right direction. However, we are concerned that it is not adequately staffed to cope with the demands placed upon it, and recognize that close collaboration with the centers and program offices is necessary to improve risk management in NASA.
- o A risk assessment report, based upon both the FMEA/CIL/retention rationale and a comprehensive hazard and safety assessment, should be the basis for the acceptance rationale in considering waivers to fly Criticality 1 components.

Letter to the Honorable James C. Fletcher

- 3 -

- o There appear to have been unexplained differences among the STS elements in the approach to and the rigor of the FMEA/CIL reevaluations. The methods being used should be reviewed to assure that any differences which exist will not compromise the FMEA/CIL reevaluation process.
- o The panels and boards (Program Requirements Change Board, Flight Readiness Review, etc.) that advise key NASA decision makers are not adequately staffed with people skilled in the statistical sciences of data analysis, statistical inference, and probabilistic risk assessment; persons with such skills should be added to provide improved support of the decision making process.
- o A greater effort is needed to plan for additional elimination or reduction of risks in the STS.

Following is an elaboration on these topics.

COMMENTS ON NASA RESPONSE

Setting priorities for Criticality 1 and 1R items

We are pleased to see the steps being taken to assign priorities to the critical items. The Committee notes that the technique proposed for implementation lends itself to the incorporation of quantitative measures of risk and probabilities of occurrence as these measures are developed. However, the Committee urges that care be taken to assure that over simplified but potentially inaccurate quantitative measures are not used. We have been assured by a representative of the NSTS office that the prioritization process can be completed well before the next Shuttle launch, which we believe to be an important consideration. We look forward to learning how NASA plans to use the results of this process. I can understand your desire to defer a decision to delegate from Level I of NASA the review and approval of waivers on certain critical items until you have assessed the results of the new prioritization and risk assessment processes. However, the Committee believes that before the next launch some method should be used to assure that NASA Level I gives special attention to the highest priority items identified through the prioritization process.

The Committee is delighted to learn that NASA is testing the use of Probabilistic Risk Assessment (PRA) on the APU and HPU, and the Shuttle main propulsion pressurization system. We also are aware of the SSME certification process assessment study being conducted at the Jet Propulsion Laboratory, which includes a PRA of the SSME. The Committee cautions NASA on its intention to evaluate PRA by comparing the results of only two or three disparate tests of PRA with the results obtained earlier by the FMEA/CIL process. The criterion should not only be whether a significant new problem is identified by the PRA. The PRA test results should be used by NASA to answer the questions: Would the PRA have helped

Letter to the Honorable James C. Fletcher

- 4 -

in making NASA's original decisions, e.g., on a Criticality 1 waiver? Would it have given more confidence in the decisions that were made? The current sample size is too small to judge its merits when applied to the entire STS or even a complex element such as the Orbiter. The PRA should increase in value as the scope of its coverage of the STS is widened. It also should be useful in better understanding the nature of the failure modes.

Integrated Space Transportation System analysis

The Committee is pleased to note that the NASA Associate Administrator for SRM&QA has been directed to develop an agency-wide risk management system. We believe that it is important to call attention to the totality of "risk management" as the sum of a number of separate processes which ultimately must be considered on an integrated basis.

The Committee is still concerned that at the NSTS office at JSC we have not found a consolidated, integrated STS systems engineering analysis, including system safety analysis, that views the sum of the STS elements as a single system. Such a "top-down" engineering analysis would help avoid potential gaps which may exist as a result of the present very thorough "bottom-up" analyses centered at the subsystem and element project levels.

We have recently become aware of the Avionics Audit which is conducted by Rockwell International-STS Division for the NSTS Program office. We understand that this audit process will be expanded to embrace eventually the entire STS. The Committee believes that an expanded audit of this type could serve as the nucleus of the needed integrated STS engineering analysis in support of risk management.

Relation between FMEA/CIL-Hazard Analysis and design changes

The Committee is reassured by the steps NASA has taken to tighten the procedure for assessing the impact of any proposed design change on Criticality 1 or 2 hardware; by the requirement that all changes introduced before a flight must undergo a FMEA which also must be accepted by the change board; and by your statement that the flight schedule will not be permitted to reduce the rigor with which these risk management tasks are conducted.

COMMENTS ON NEW TOPICS

Role of panels and boards in STS decisions

The Committee recognizes the important role played by the many panels and boards in the NSTS program in providing coordination, resolving problems and technical conflicts, and reviewing and recommending actions. These

Letter to the Honorable James C. Fletcher

- 5 -

entities allow the different interests and skill groups to bring forward their inputs, contribute their knowledge, and thus minimize the risk that a proposed action will negatively affect some aspect of the STS. We presume that each of these entities recommends an action to an appropriate official, such as a project manager at Level III or the Deputy Director of the NSTS Program at Level II, who actually makes and takes responsibility for the decision.

The Committee is concerned about a possible attitudinal problem regarding the decision process on the part of the NASA personnel engaged in it. When we ask a NASA manager about how a decision is made, often we are told that it is made by such-and-such a board. We are concerned that there may be a tendency for those involved in the multi-layered review and decision process to hide in the anonymity of panels and boards, and that each person who must sign off on an item may not be inclined to concentrate enough on his or her individual responsibility in light of the number of levels of group reviews involved in the decision process. The Committee recommends that the Administrator of NASA periodically remind all of the NASA organization of the specific individuals by name and position who are responsible for final decisions (and the organizational relationships among them) based on the advice coming from each panel and board. This would not detract from the important role played by all members of the panels and boards in providing advice to the decision maker.

Potential of the Program Compliance Assurance Status System (PCASS)

The Committee is enthusiastic about the potential of the PCASS, which is being established as a major part of the new System Integrity Assurance Program (SIAP) of the NSTS. It should improve the quality of information available to key decision makers (e.g., at Flight Readiness Reviews) by providing in near real-time an integrated view of the status of problems with the STS, including trends, anomalies and deviations, assessments, and closure information. Plans to keep up to date and computerize the FMEA will provide a very useful input to PCASS. The Committee also has learned of the data base maintained by the Johnson Space Center (JSC) SR&QA office which documents in one place the failures which have occurred on the Orbiter during ground testing and in flight. It is encouraging to note that of those failures of components on the Orbiter categorized as Criticality 1 which have occurred during flight, none resulted in the worst-case effect postulated in the FMEA. These failure data can be very valuable in connection with the new CIL prioritization system in establishing the probability that the postulated effects will actually occur, given the failure in flight. We understand that this, and similar data bases for the other STS elements, will be integrated into the PCASS. We believe that PCASS, as a real-time data base, has the potential to become a key element of the STS risk management, and thus its full and timely development should be encouraged and supported. The Committee recommends that this development be given a high priority and that the potential users of PCASS, including key decision makers, be involved closely now in its development.

Letter to the Honorable James C. Fletcher

- 6 -

Progress on the SSME as a result of the FMEA/CIL reevaluation

Based on its second visit to Rockwell International - Rocketdyne Division, the Committee is encouraged with the progress being made in improving the SSME as a result of the FMEA/CIL reevaluation. We also applaud the improvements in the test program which are designed to validate the reliability of the modified SSME before first flight. The SSME is one of the few cases in which the Committee has found that changes have been made as a result of the FMEA/CIL. In most other cases, the Committee observes that the initiation of changes has not originated with the FMEA/CIL process.

NASA Headquarters Safety, Reliability, Maintainability and Quality Assurance (SRM&QA) program.

In April, the Committee received a comprehensive briefing regarding the status and plans for the NASA Headquarters SRM&QA program. We are encouraged by the progress that has been made. The Committee believes that the program is going in the right direction. We recognize the magnitude of the task ahead; however, the goals and the program plans developed so far appear to be sound. The Committee is concerned that SRM&QA (at Headquarters and the centers) is not adequately staffed to cope with the demands being placed upon it, perhaps necessitating the additional use of contract personnel in order to carry out their functions before the launch of the next Shuttle. The Committee also believes that it will be particularly important to develop close collaboration with the NASA centers as well as other program offices in order to do those things which are needed to create a total risk management system augmenting the independent check and balance role of SRM&QA.

Input to waiver decisions

The Committee understands that FMEAs, CIL determinations, and their retention rationale are developed by the STS design and development people. The SRM&QA, operations and other relevant personnel contribute as appropriate. The FMEA/CIL and retention rationale so produced are among the inputs to the hazard analyses which are done by the safety people. In this case, design, development, operations and other relevant personnel contribute as appropriate. The output of these two processes (FMEA/CIL/retention rationale on the one hand, and hazard analyses on the other) are individually approved by the Program Requirements Control Board (PRCB). However, the Committee is concerned that the FMEA/CILs with their design-based retention rationale have become the only effective input to Levels II and I in their waiver decisions to accept the designs as safe enough to fly.

The Committee recommends that the present design-based retention rationale should be only one part of the rationale required to accept the hazards which can result from each critical failure mode. The other part should

Letter to the Honorable James C. Fletcher

- 7 -

be the output of the hazard and safety assessments, including evaluations of the probability that the hazardous conditions will actually develop and the probability that these conditions will lead to a Criticality 1 consequence. A risk assessment report, embracing the design retention rationale and the hazards/safety assessment, should provide the acceptance rationale for consideration by Level II and I managers in reaching their decisions on the granting of waivers.

Differences in FMEA/CIL reevaluation process among STS elements

In the Committee's audit of the reevaluation of the FMEA/CILs, a number of differences were found in the process being used by different element project offices and contractors. In some cases, we were unable to ascertain the reasons for the observed differences. For example, the independent contractors evaluating the FMEA/CILs for the STS elements managed by the Marshall Space Flight Center are required to review all subsystems and to file a Review Item Discrepancy (RID) when they differ with the results of the element contractor's analysis. On the other hand, the independent contractor for the Orbiter evaluation was not directed to review all parts of the Orbiter and does not file RIDs. We understand that JSC now has directed the contractor to review all subsystems in the Orbiter. An audit by the Committee of the documentation and review process used in the case of the Orbiter indicates that it is a reasonable alternative to the RID process. Nevertheless, the Committee suggests that the NSTS program office review the FMEA/CIL reevaluation processes as implemented for each STS element to assure itself that any differences will not compromise the quality and completeness of the STS FMEA/CIL effort as a whole.

Expertise in Statistical Sciences

The key technical decision makers in NASA operate as chairmen of bodies that review relevant technical information. The decisions involve design, requirements, waivers, launch decisions, etc. Much of this information is in the form of complex engineering data, such as test, inspection, flight, and weather data. These bodies draw upon experts in many engineering disciplines to deal with the complexities. Indeed, it is important that there be close ties among the design engineers, test and analysis people, and decision makers throughout the process of designing, building, certifying, and using components and systems. However, the Committee finds that these bodies are not adequately supported by people skilled in the statistical sciences to aid in the transformation of complex data into information useful for decision making.

The Committee recommends that NASA build up its staff of experts in the statistical sciences (civil servants and contract support) to provide improved analytical support of risk management and of key decision makers by the application of modern statistical analysis, inference and assessment techniques.

Letter to the Honorable James C. Fletcher

- 8 -

Reducing the risk in the Space Transportation System

Even with the current FMEA/CIL and hazard analysis efforts which are supported thoroughly within NASA and by its contractors, the Committee receives the impression that changes often may only be considered which will reduce risks to that level which has been previously accepted in the STS program. The Committee believes that such risks, accepted in the past, logical as that may have appeared to be at the time, should not now be accepted without a concentrated effort to plan and implement a program to remove or reduce these risks.

FUTURE WORK

The Committee is continuing its audit by examining other aspects of the STS risk management process. Among these are the design qualification and flight certification processes; a further look at integrated systems analysis; launch commit criteria and waiver policy; the process for generating, reviewing, revising and approving the retention rationale for waivers to permit flight of the Shuttle with critical items that affect safety; the process for structural analysis, establishment of margins, and verification of analyses and margins; the risk management process for STS software; and the process for analyzing the effect of payloads on the safety of the Shuttle, ground personnel, and flight crews.

We plan to issue a final report of the Committee late this year. It will include our assessment of all of the procedures reviewed and recommendations for improvement of the STS risk management system. If it should appear desirable, we will provide another interim letter report to convey findings and recommendations which may emerge from the reviews now under way.

Sincerely yours,



Alton D. Slay
Chairman
Committee on Shuttle Criticality
Review and Hazard Analysis Audit

cc: Admiral Richard H. Truly

APPENDIX D

PROBABILISTIC RISK ASSESSMENT

1. THE APPROACH TO QUANTITATIVE RISK MANAGEMENT

The output of a quantitative risk management function is a quantification and prioritization of issues, the controlling of which leads to optimal decisions involving safety, reliability, quality, performance, and cost. The approach is to implement a methodology that interprets, synthesizes, and integrates all elements of a product assurance program into a form suitable for decision making. The input would be the results from the various safety, reliability, and quality assurance programs of the field offices. The transformation of this information into a useful basis for decision making is the step that enables meaningful risk management to occur.

The National Aeronautics and Space Administration (NASA) has a variety of documents covering the approach to be taken in the discipline areas of safety, reliability, maintainability, and quality assurance. These documents, subject to revisions, would be the basic guides to be implemented by the various centers. It is the task of the risk assessment function to systematically process the output of the centers into a form suitable for meaningful risk management. The key requirements for this critical information processing and assessment step are as follows:

- The figures of merit must be explicit and quantitative.
- The information processing must be based on an integrated systems engineering approach (see also Section 5.11).
- The quantification of uncertainty must be an integral part of the information processing (see also Appendix E).
- The contributors to risk must be explicit, prioritized, and defined in terms that enable measurable corrective actions.
- Finally, the results should provide the basis for rational analysis of alternatives for reducing and controlling risk.

The logic engine for carrying out the information processing is a risk-based model of each space

system. The model should be structured to give perspective to the importance of the various tasks associated with the product assurance activity. The model must be a living model with continuous input into and from the design process. While this approach probably is not warranted in many cases, such as small automated spacecraft, it should be considered in large, complex programs—especially those with potential risk to human life—such as the STS or the Space Station.

2. TWO KINDS OF CONFIDENCE

The essential objective of the risk management effort is “confidence”—confidence that each space mission will perform substantially as planned, and confidence that it will not be destroyed or rendered significantly less useful by accidents or unforeseen problems (including excessive cost). Now, what is meant by confidence? One way we humans increase our confidence is to believe that we are highly competent. We shall call this “psychological” confidence. It can be extremely important for the effectiveness of an organization. NASA has done an excellent job in this area in the past, and this needs to continue.

There is another kind of confidence that we shall call “engineering” confidence. This comes from in-depth understanding of the system under consideration, from deep knowledge of the design and testing program, and from knowing how to achieve quality in manufacturing, maintenance, operation, and flight readiness.

There is another dimension to this notion of gaining engineering confidence. This comes from acknowledging that nothing ever built by man is 100% reliable. It comes from knowing that risks are always present. The objective, therefore, is to know just how large the risk is. Thus, engineering confidence and success come not from eliminating risk, which is impossible, but from controlling it and managing it. That means knowing what it is—measuring it, knowing its size, shape, structure, etc.—and taking steps to reduce the risk to acceptable levels. Thus, the idea of engineering confidence is essentially equivalent to the quantification of risk. This equivalence makes engineering confi-

dence an objective quantity, as distinct from psychological confidence, which is subjective. Psychological confidence is a matter of good feeling. Engineering confidence is objectively and logically related to the evidence available—to the information, experience, test data, calculations, and, indeed, to the consensual judgments of the experts involved. Engineering confidence is the quantitative expression of that evidence. That expression is formulated according to strict, logical, invariable rules. It is not a matter of opinion or mood.

When a satisfactory level of engineering confidence has been established, then those involved in the program indeed will have a “good feeling.” Therefore, engineering confidence produces psychological confidence. The reverse, as we know too well, is not necessarily true.

3. HOW IS CONFIDENCE GAINED OR REGAINED?

The public and Congress, based on past technological failures in the nation’s space programs, are probably not going to be moved by psychological confidence in the future. Engineering confidence needs to be created. The issue of quantification needs to be faced. Those responsible for a program such as the NSTS need to be willing to ask themselves: “How confident are we that this design, this mission, this launch will succeed?” This is a powerful question, if it is properly used. How is this question used properly? The first step is to provide the format in which the answer is to be given. This makes the question into a workable tool.

The proposed format is as follows, taking the STS as an example: Let us project ourselves into the future to a time when we can imagine that many thousands of Shuttle missions have been launched. One can now look back at the record and ask the following question: “In what fraction of these launches was the vehicle lost?” Let this fraction be ϕ_{LOV} . This parameter would then be a very meaningful figure of merit describing the success, safety, and effectiveness of the program.

At the present time, of course, the numerical value of this parameter is not known. One can only tell the state of knowledge about what this value will be. This is done in the form of a probability density curve against ϕ_{LOV} , using a logarithmic scale, as shown in Figure D-1.

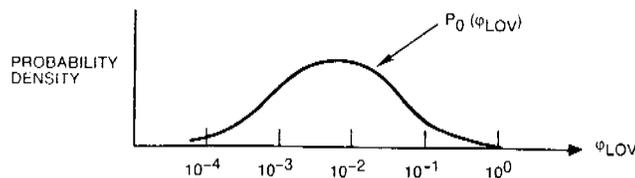


FIGURE D-1 State of knowledge probability curve for frequency of loss of vehicle.

This curve expresses the current knowledge about ϕ_{LOV} based on all the information and evidence available. The width of the curve reflects the degree of uncertainty about the value of ϕ_{LOV} . The whole shape and location of the curve is a portrayal of the current state of confidence in the vehicle. Therefore, this “state of knowledge” curve can be adopted as the format for quantitative expression of confidence. This curve is also the bottom-line output of a risk analysis of the vehicle.

With curves of this type, together with an orderly compilation of the evidence on which the curve is based, NASA can build confidence in a tangible form. They can then communicate it convincingly to the whole technical and management team, and also to Congress, to review committees, and to the public at large.

4. DOCUMENTING CONFIDENCE THROUGH A QUANTITATIVE RISK MODEL

At any point during the life of a project it is desirable to be able to reach for a document that presents the current risk status of the project in a compact, succinct, and quantitative form. This document should contain the bottom-line figures of merit and the numbers, tables, graphs, and diagrams that would capture and characterize the risk of the project. It also should make clear the main contributors to risk and the main sources of unreliability, doubt, and uncertainty at that time.

The document, which might be called the Risk Summary Report, would be updated regularly and might be the basic document upon which the risk management function would draw. It would contain in an organized way the combined knowledge of the entire technical team on issues of risk. It would spell out what is known and not known on each point and would quantify all uncertainties so that decision makers could clearly understand the trade-offs among costs, benefits, and risks.

Such a document can only be generated as the summary output report of an ongoing quantitative

risk model (QRM) of the project. This model and this report, properly handled, could become an extremely useful mechanism, a primary channel for communication between management and the technical team. Indeed, it could become an important framework and mechanism for communication and coordination among all parts of the technical team. If used in this way, the report would make a major contribution to the success of the project.

The Risk Summary Report may be thought of as the final stage of an information machine. This machine is depicted in Figure D-2 as a kind of megaphone. At the right end in the figure are represented the working levels of the project and the design, fabrication, testing, and research organizations. The information from all these activities, relevant to risk, is continually gathered into the machine at the right. This information is digested and processed, through the logic of the QRM, and emerges finally as the Risk Summary Report.

The primary information flow is thus from right to left in this figure. However, there is also a very important reverse flow, a kind of “back EMF.” The fact that this machine exists, that it is organizing and processing the information in certain ways, and that people are reading the output in certain ways, exerts a valuable orderly discipline on the working levels. Questions move from left to right, forcing the working levels to continually structure and organize their data and their thinking about risk.

If the information machine is properly constructed, it establishes not only an orderly calcu-

lating and recording mechanism but, perhaps even more importantly, it establishes a language and a conceptual framework that unifies and organizes the thinking, communication, and decision making of the whole project. Not only are better design decisions thus made, but enormous savings in time and talent can result simply from the fact that everybody is using the same language so that, to a great extent, all participants mean the same things by the same words.

The QRM approach can provide an extremely valuable integrating framework for the Safety, Reliability, and Quality Assurance (SR&QA) activities. This framework would include the Failure Modes and Effects Analyses (FMEA) and hazard analysis work, which would become in effect part of the QRM. Indeed, one of the benefits of the QRM approach is that it would help to ensure that the results of the FMEA and hazard work are fully recognized and acted on at the decision level. One of the ways this benefit is achieved is through the discipline of quantification, which forces the major items to the surface, where attention must be paid to them. A second way is through the quantification of uncertainty, an even more stringent discipline, which forces an organization (for example), before it dismisses an item as an “acceptable” risk, to show quantitatively that the evidence available provides sufficient confidence to support that decision. The quantification of uncertainty also helps decision makers to know when a change in the hardware is needed or when the problem is just lack of confidence—so that perhaps more testing is needed, rather than new designs.

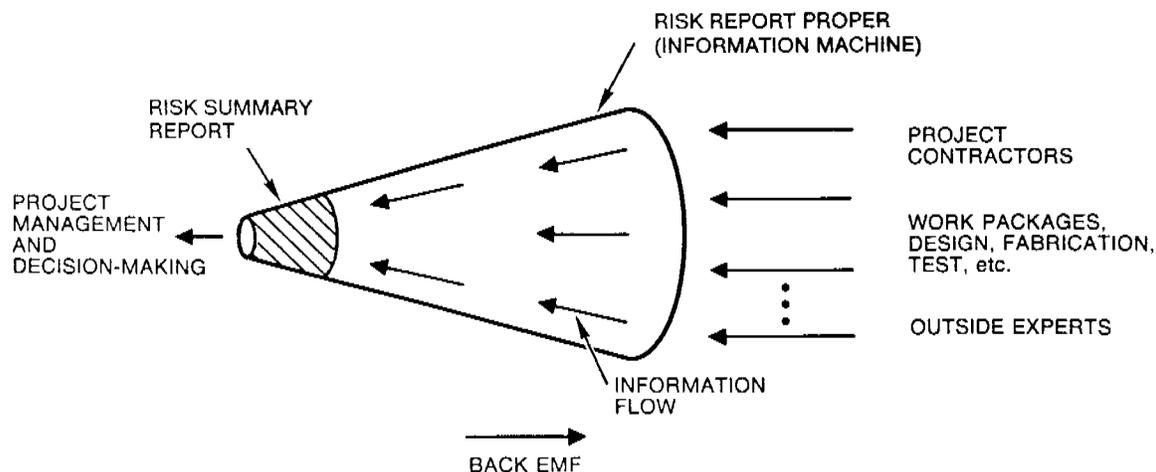


FIGURE D-2 The Risk Summary Report as the final stage of an information machine.

5. THE ELEMENTS OF PROBABILISTIC RISK ANALYSIS

5.1 The "Set of Triplets" Definition of Risk

In contemplating the design or operation of a project, those involved should say to themselves: "We know how things are supposed to work out; we know our plan. Now we would like to know what are the possible departures from that plan." Specifically, they would ask three questions:

- What can go wrong?
- What is the likelihood of that happening under the current plan?
- If it does happen, what are the consequences; i.e., what is the damage?

The answers to these questions constitute a risk and reliability analysis. The answers might be arranged in a table as in Figure D-3. The first column contains descriptions and names of scenarios. This is the answer to the first question above. The second column contains the likelihoods, l_i , of the scenarios, s_i . Here we use the word likelihood in a generic sense. How to quantify likelihood will be discussed in Section 5.2. The third column contains "damage index," x_i , which is a measure of the consequences of the i th scenario.

Each row of the table thus constitutes a triplet

$$\langle s_i, l_i, x_i \rangle$$

giving a scenario, its likelihood, and consequences. This triplet constitutes then one answer to the three questions. The table itself, i.e., the set of all triplets

ANSWERS TO: (1) WHAT CAN GO WRONG?
 (2) WHAT IS THE LIKELIHOOD?
 (3) WHAT IS THE DAMAGE?

SCENARIO	LIKELIHOOD	DAMAGE
s_1	l_1	x_1
s_2	l_2	x_2
s_3	l_3	x_3
.	.	.
.	.	.
.	.	.
.	.	.
s_N	l_N	x_N

$$R \equiv \text{RISK} = \{ \langle s_i, l_i, x_i \rangle \}$$

FIGURE D-3 Quantitative definition of risk.

denoted by the outer brackets, provides the total risk; in particular,

$$R = \{ \langle s_i, l_i, x_i \rangle \}$$

is the complete answer to the questions. Therefore this set of triplets is adopted as the definition of risk, R .

This definition becomes the organizing principle for the QRM and, thus, for the SR&QA work on the project. What is being sought in this work is the identification of all possible significant scenarios and the characterization of their likelihood and consequences.

5.2 Quantifying Likelihood

The idea of likelihood can be expressed quantitatively in different ways. For NASA-type risk work the most useful way might be what is called the "probability of frequency" approach. In this approach, one can imagine a "model" in which a vehicle is launched, or a facility operated under specified conditions many, many times. In this thought experiment the scenario, s_i , will occur with a certain "frequency," which is denoted ϕ_i , and which is measured in occurrences per mission, per launch, per year, or other appropriate unit.

These frequencies ϕ_i may be thought of as abstract in the sense that, since the experiment cannot be run completely, the ϕ_i cannot be measured precisely. The ϕ_i actually are parameters of the model and they can be usefully adopted as figures of merit indicating the safety and reliability of the system.

We would like then to know the numerical values of these parameters, ϕ_i . As mentioned above, these values will never be known precisely. However, we are not totally at a loss either. There is always a certain body of evidence and information relevant to these values. So now one can ask, "What inferences can be drawn from this evidence about the values of these parameters, and with what degrees of confidence can those inferences be drawn?"

The answers to this question can be expressed in the form of probability curves against the possible values of the parameters (as in Figure D-1). These curves are called state of knowledge curves. They become the final quantitative expression of risk and reliability.

The remaining question is how these curves are developed from evidence available, considering that the evidence may be of very differing types: test data, actual flight experience, calculations, judgment of experts, experience of other similar equipment, etc. The answer is that the development of these curves makes heavy use of the fundamental theorem of inference, Bayes theorem. The use of this theorem is partly art and partly science, but it always can be done in a way that is meaningful for decision making purposes.

In order for the individual state of knowledge curves on the ϕ_i 's to be a complete specification of the knowledge available, certain assumptions must be made. One is that the scenarios are *approximately* mutually exclusive; i.e., only one can happen at a time. Another is that conditional on the data, different ϕ_i 's are statistically independent. If these assumptions are not satisfied, more complex applications of Bayes theorem are required. However, for this discussion, we make these simplifying assumptions.

5.3 Structuring and Categorizing the Triplets

Since the number of possible scenarios for a system can be very large, it is important in carrying out a Probabilistic Risk Assessment (PRA) to organize and categorize the set of triplets. This can be done in many ways.

Perhaps the most important categorization of triplets is by the magnitude of the consequent damage. For this, one wants to know what scenarios lead to destruction or inactivation of the space mission. What is the total probability of such scenarios? What scenarios lead to substantial decreases in the system's performance or usefulness? What is the probability of that outcome?

A second way would be to categorize scenarios by the part of the system complex in which they originate. This would give us a picture of the risk of the various elements and subsystems. Another important way of looking at the problem is to categorize the triplets by the phase of the flight in which they take place, thus making visible the risks attendant on each flight phase.

5.4 Pictorial Representation of Risk

It may be useful for some purposes to express the damage x_i on an index scale, [0, 100]. The

value $x_i = 0$ represents no damage and the value $x_i = 100$ represents loss of vehicle (LOV). Intermediate values of x_i represent partial loss of mission or vehicle. With this idea a useful pictorial presentation of risk can be developed in the following way: In the risk table, Figure D-3, the scenarios can be numbered in order of increasing damage; that is, such that

$$x_{i+1} \geq x_i$$

and let N be the total number of scenarios. Then we can define

$$\Phi(x_i) = \sum_{j=i}^N \phi_j .$$

Thus defined, $\Phi(x_i)$ is the total frequency of all scenarios having damage level x_i or greater.

If these $\Phi(x_i)$ are plotted on a log scale versus x_i and the resulting step-function is smoothed, a curve, $\Phi(x)$ vs. x , is obtained which is known variously as the "risk curve", the Rasmussen curve, or the "frequency of exceedance" curve as in Figure D-4. Its ordinate over any x is the frequency with which scenarios occur having damage equal to or greater than x . This curve also may be viewed as a figure of merit of the system.

As before, since the ϕ_i is not known exactly, one will not know the risk curve exactly. But from the uncertainty in the individual ϕ_i , the uncertainty in

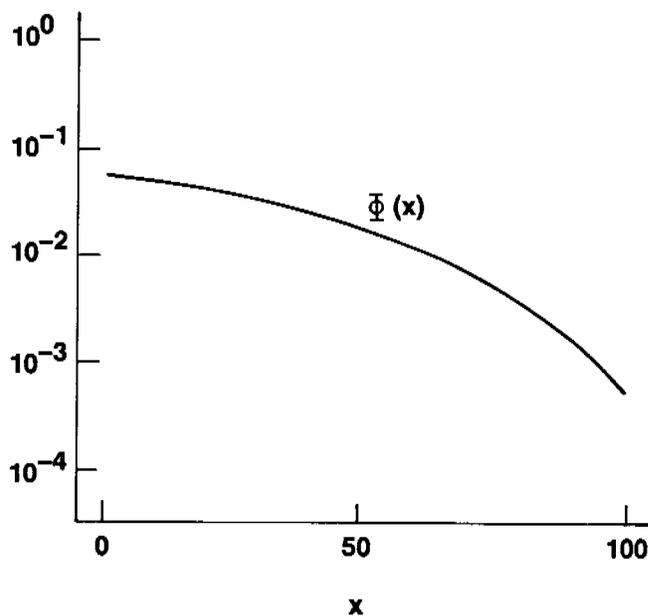


FIGURE D-4 Risk curve.

$\Phi(x)$ can be calculated. This uncertainty can then be presented in the form of a family of risk curves

$$\{\Phi_p(x): 0 \leq P \leq 1\},$$

shown, for example, in Figure D-5. This graph is called a "risk diagram." For a fixed x , the uncertainty about $\Phi(x)$ can be quantified by

$$Pr\{\Phi(x) \leq \Phi_p(x)\} = P.$$

Suppose, for example, that $\Phi_{.99}(100) = 10^{-2}$. This means a confidence level of 99% that the frequency of LOV [i.e., $\Phi(100)$] is less than or equal to .01.

From a portrayal of such risk diagrams one can gain a rapid understanding of the contributions that various sources make to the overall risk of a system or program.

5.5 Use of Risk Diagrams in Decision Making

Like everything else in life, large engineered systems, such as the SIS, necessarily involve a degree of risk. In the case of engineered systems, however, intelligent design decisions can control the amount of risk. Sometimes through a flash of insight it is possible to change or simplify a design in a way that not only reduces risk but also improves performance and reduces the cost. This does happen, and these are happy occasions. More often, however, the situation is that risk can be made, in principle, as small as one likes, but the price for this is diminished performance and increased cost of the system.

The task of management, therefore, is to strike an optimal balance between risk, cost, and per-

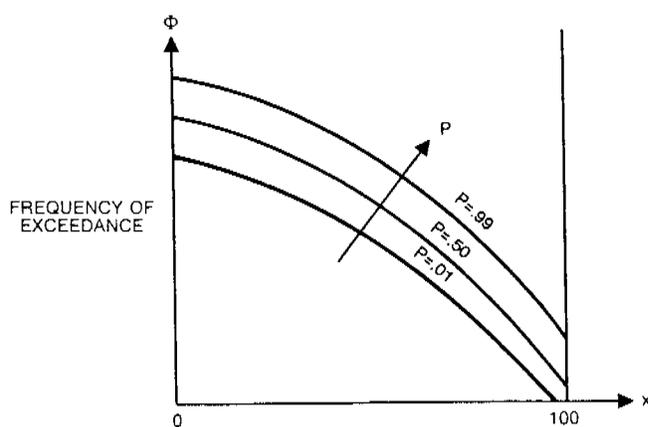


FIGURE D-5 Risk diagram.

formance. The balance is struck and fine-tuned continuously through day-to-day decisions, as the design evolves. In the "flash of insight" cases, the decisions are easy to make. In the more usual case, trade-offs are required. In these situations, it is useful and necessary to have quantitative input so that the amount of risk can be weighed against the levels of cost and performance.

The situation in such cases is portrayed in Figure D-6, which shows the anatomy of a general decision problem. Each option brings with it a certain risk, cost, and performance. If these three factors were precisely known, it would be easy to make the decision. What makes that problem interesting in real life is that these factors are never known with complete certainty. It is important, then, to quantify these uncertainties as part of the input to the decision analysis.

Figure D-6 shows the uncertainties in cost and performance quantified in the form of probability curves. Each option, therefore, can be characterized by triplet $\langle C, B, R \rangle$ diagrams. The decision maker must then choose which triplet (i.e., which option) he prefers. In the language of decision theory his degree of preference, as a function of the triplet, is called a utility function, U .

The rule of quantitative risk analysis, as shown, is to provide the assessment of risk, including uncertainty, as part of the input to decision problems. Strictly speaking, PRA per se is limited to the risk part of the problem, but the same quantitative way of thinking, the same probabilistic methodology, can be and should be applied to the cost and performance factors as well.

5.6 Assembly and Disassembly of Risk

5.6.1 Identifying Scenarios

According to the definition of risk noted above, the first and most important step in risk assessment is to identify the scenarios. In this connection, the following are some key ideas. First of all, note that any scenario that can be described is actually a category of scenarios. Thus, "the pipe breaks" is a category that includes as sub-categories, "the pipe breaks longitudinally," "there is a double-ended guillotine break," "the pipe breaks in such and such location," etc.

A second point is that since the objective is to identify all possible significant scenarios, any method

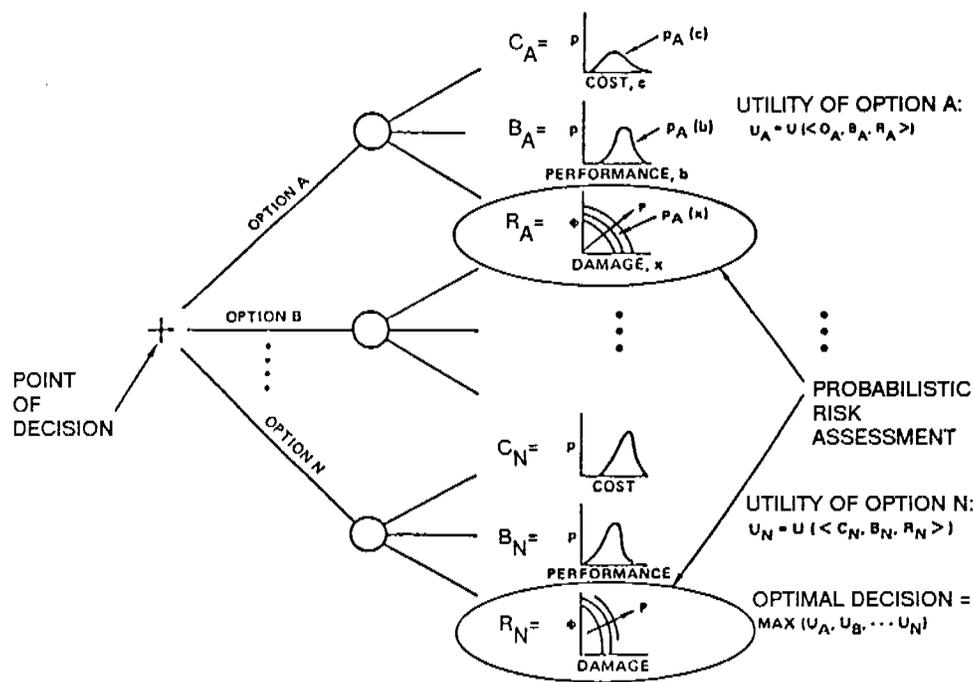


FIGURE D-6 Decision model.

that helps one do that is good. Any new way of looking, any new way of categorizing that helps to be sure that no significant scenarios have been overlooked is good, so it is perfectly acceptable to use more than one approach to scenario identification.

One approach that is quite useful is to break the overall engineered system into parts and subparts. Each part can be examined in detail and the questions asked: “What can go wrong with this part? What scenarios can originate here?” This approach would seem to be particularly appropriate for space systems. “Parts” could be interpreted successively as physical segments of the total system, as functional subsystems in the system; they could also mean different phases of the system’s mission life. Again, all different ways are helpful.

Another point of interest is that some scenarios are single-event scenarios. Something fails and the system is damaged or destroyed. Other scenarios require several different events to happen coincidentally, sometimes referred to as multiple failures. Other scenarios are “chains” of events. These are “cascade” or “domino” scenarios. Something happens initially and because of that something else fails, which causes a chain of propagating events resulting in overall system failure.

Each of these types of scenarios requires its own type of analytical tools. Failure modes and effects analyses (FMEAs) are useful for single-event scenarios; event trees and event sequence diagrams for chains of event-type scenarios; and fault trees for coincident failures. In space systems and missions, one can expect all these types of scenarios to be present and expect all these analytic tools, and others, to be useful. The specific mix of methods and approaches should be determined by what is contributing to the risk.

5.6.2 Quantification of Scenarios

In a methodology that has worked well, long run frequency is used as the measure of likelihood of the scenario. Thus, an underlying Poisson-type random process model is used as the framework for discussing the risk and reliability behavior of the system. The scenario frequencies are then viewed as parameters in the Poisson model, and these parameters are used as figures of merit to indicate the safety and reliability of the system.

The values of these scenario frequencies are determined from the frequencies of all the component events (the “elemental” events) in the scenario, such as failure of valves, pumps, human errors, etc. The results of the modeling logic are thus to

express the frequencies of the scenarios in terms of the frequencies, λ_j , of these elemental events,

$$\phi_i = F_i(\lambda_1, \lambda_2, \dots, \lambda_j, \dots) \quad (1)$$

Now, the discipline of data analysis and statistical inference is applied. The question is asked: How big are the numbers λ_j ? Again, the state of knowledge probability curves are used to provide the answer (see Figure D-7).

These curves must reflect all of the evidence and information available which are relevant to the λ_j : all operating experience, test data, calculations, etc. In putting together this information, the logic of Bayes theorem is used to help evaluate and combine the various types of evidence correctly. The discipline of this theorem forces one to organize and codify the evidence and helps to curb wishful thinking.

To apply Bayes theorem one needs two basic ingredients. The first ingredient is a "prior" state of knowledge curve $P_{0j}(\lambda_j)$ which quantified the available qualitative information about λ_j . Qualitative information may be in the form of precise knowledge of related components or expert engineering judgement. The fact that this qualitative information can be quantified as a probability density is the major result of the theory of subjective probability that has been developed since the 1950's.

The second ingredient is the "likelihood function" associated with the available data that contains information about λ_j . These data could be industry data, test data, and/or field data. Let $D = (D_1, D_2, \dots)$ be the vector of data available. The likelihood function, $L(\lambda_j, D)$, is proportional to the conditional probability of observing the data D given λ_j . For example, if the data are observed defects, then the likelihood function may be derived from the Poisson distribution.

Bayes theorem integrates these sources of infor-

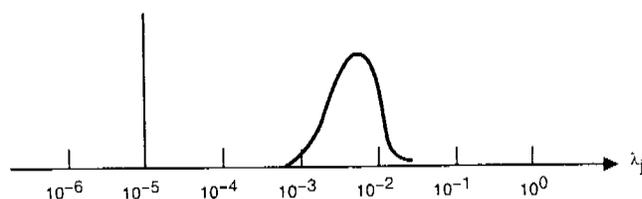


FIGURE D-7 State of knowledge probability curve for elemental parameter λ_j .

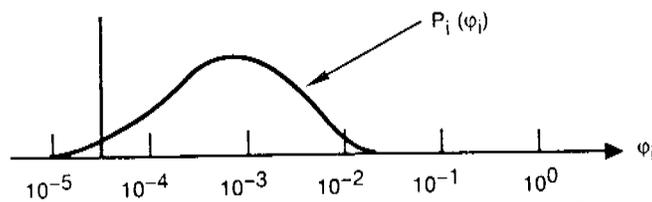


FIGURE D-8 State of knowledge probability curve for scenario frequency.

mation. The state of knowledge curve for λ_j given all information is $P_j(\lambda_j)$, which is proportional to

$$P_{0j}(\lambda_j) L(\lambda_j, D) .$$

The proportionality constant is chosen so that $P_j(\lambda_j)$ is a probability density (i.e., it integrates to 1).

Having the curves $P_j(\lambda_j)$, they can now be "propagated" through equation (1) to obtain curves for the ϕ_i (Figure D-8). Finally, since the total loss-of-vehicle frequency is the sum of the ϕ_i ,

$$\phi_{LOV} = \sum \phi_i ,$$

the curves $P_i(\phi_i)$ (through a mathematical convolution) are simply aggregated to obtain a new curve, $P_1(\phi_{LOV})$, for the LOV frequency. This curve, in relation to the initial curve, $P_0(\phi_{LOV})$ from Figure D-1, might appear as in Figure D-9. Curve P_1 is a more satisfactory state of knowledge than P_0 and thus is a better basis for a "go" decision.

This aggregation should be done in stages, so they can be viewed at various levels of aggregation such as system, subsystem, unit. In this way, one could answer macroscopic questions like: "What is the total frequency of events that could destroy or inactivate the system?" By proceeding downward in the aggregation, one could then see, at successively greater levels of detail, where the bulk of this frequency is coming from. This draws management's attention to the aspects of the design needing further attention.

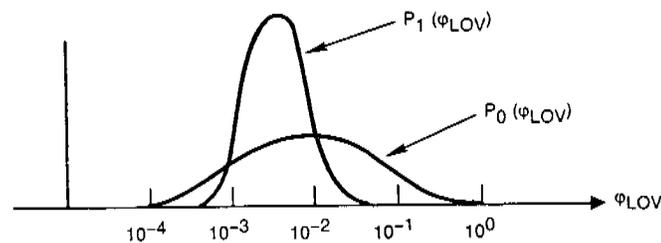


FIGURE D-9 States of knowledge (confidence) before and after PRA.

5.6.3 Design Improvement

The improvement between curves P_0 and P_1 in Figure D-9 is simply an improvement in knowledge and confidence coming from study and analysis (PRA). It does not reflect any actual changes to the design of the system. If one now recognizes that, in the course of such a study and analysis, many areas of the design or maintenance/operation practices will surely be discovered where we can do

better, and if those improvements are then implemented, the probability curve will change again, hopefully to something like the curve P_2 in Figure D-10.

With repeated cycles of this type of analysis and with continued experience and technology improvement, one may hope ultimately to achieve something like curve P_3 , which perhaps is what is needed to support a viable manned space program.

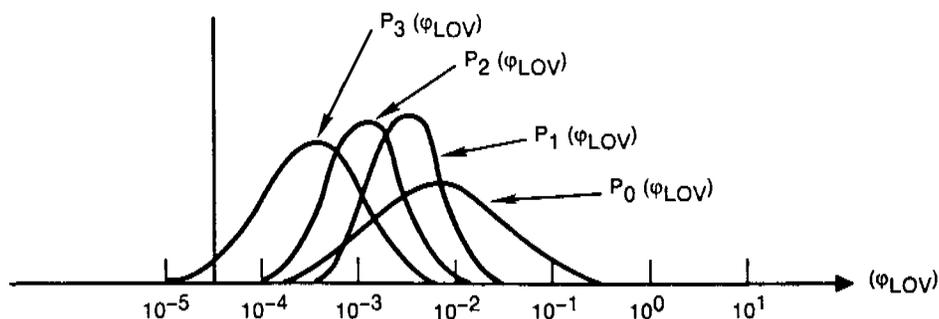


FIGURE D-10 Evolutionary system improvements are reflected in changes in the state of knowledge curves.

APPENDIX E

AN IMPROVED CRITICAL ITEM RISK ASSESSMENT PROCEDURE FOR THE NATIONAL SPACE TRANSPORTATION SYSTEM

(With an Example of Application to the 51-L Field Joints)

1. INTRODUCTION

On May 28, 1987, a NASA representative made a presentation to the Committee on Shuttle Criticality Review and Hazard Analysis Audit entitled, "Critical Items List (CIL) Prioritization." The method discussed was subsequently issued in modified form as NSTS Instruction 22491, Reference [3]. This Instruction for the preparation of Critical Item Risk Assessments (CIRA) provides a method for prioritizing the failure modes in the CIL. It contains many excellent ideas and is a significant step forward. However, the Committee has some concerns and some related suggestions on how to simplify and clarify the method.

This Appendix also contains in Section 5 an example of the application of trend analysis and Probabilistic Risk Assessment (PRA) to the pre-Challenger O-rings. This application, included here *only as an example of some applicable analysis techniques*, makes heavy use of modern statistical science and Bayesian ideas.

2. CONCERNS WITH THE CURRENT METHOD

The Committee's concerns with the CIRA method, as currently formulated, can be summarized as follows:

1. In Table 1 of Reference [3] (shown here in Attachment 1) the column labeled "SEVERITY" DEFINITIONS really contains worst-case damage states.
2. In Table 1, the columns labeled SUCCESS PATHS and STATUS CODE FOR REDUNDANCY/BACKUP are really descriptions of system or subsystem architectures. They affect risk by affecting the probabilities in the last

two columns. However, the relevant information is in the probabilities themselves—not in the architecture. Any guidelines written on how to assess the probabilities, either empirically or subjectively, should contain much discussion on how success paths, redundancy structure, and periodic checking strategy affects the probabilities in columns 4 and 5.

3. The probabilities in the last two columns of Table 1 are qualitative and open to interpretation as to what the terms "Very Likely," "Likely," "Unlikely," and "Very Unlikely," mean. The two columns, which have the same qualitative scale, appear to have different quantitative scales associated with them. In column 4, "Very Unlikely" appears to mean something like $\leq 10^{-6}$ and "Very Likely" means something like 10^{-1} . In column 5, the scale depends on whether or not there is redundancy. If there is no redundancy, then "Very Unlikely" means something like 10^{-2} and "Very Likely" means something like greater than .95. But if there is redundancy, then "Very Unlikely" may mean 10^{-6} . With the qualitative definitions of probability, it is quite possible that two engineers working on two failure modes with the same severities and probabilities would assign them to different probability categories and therefore produce inconsistent priorities. It is very important that the probabilities have operational definitions. Terms like "Unlikely" are not operational definitions.
4. There is no way to produce a unique priority. Suppose there are two failure modes, and Table 1 is filled out as follows:

Failure Mode	Severity Definition	Success Paths	Redundancy/ Backup	Design Confidence	Likelihood of Worst Case
1	(A)—Loss of Life	0	(a)—None	(II)—Likely	(iv)—Unlikely
2	(A)—Loss of Life	0	(a)—None	(IV)—Unlikely	(ii)—Likely

Which one should have the highest priority? Suppose that the last two columns were replaced by the following structure:

Failure Mode	Probability of Failure	Probability of Worst Case Given Failure	Probability of Worst Case
1	Likely = .01	Unlikely = .01	.0001
2	Unlikely = .00001	Likely = .5	.000005

Now it is clear that failure mode 1 presents a higher risk.

3. PROPOSED IMPROVEMENTS

As an improvement to Reference [3], the Committee proposes the procedure described in Table E-1 below:

All failure modes with the same **Worst Damage State Given Lack of Redundancy or Redundancy Failure** would be ranked by column Z.

The probabilities shown in Table E-1 are for illustration only and do not reflect any specific example. In actual application, it would be highly desirable for the analyst to include confidence limits (or the equivalent) for each of the probabilities listed in the tables produced through the CIRA. The Committee recommends strongly that such probabilities be documented by a rationale. Many of the facts mentioned in the current CIL "Rationale for Retention" would be cited in the probability rationale—but in the quantitative manner illustrated by the example in Section 5. In addition, facts that imply higher probabilities would also be analyzed. For example, the long-run frequency of catastrophic failure for solid rocket motors of a

mature design is 1/50; and therefore 1/25 for two solid rocket motors. A dis-aggregation of this frequency by failure mode would be a useful baseline for an analysis. How are our design and failure modes different from history? For example, the field joint is similar to Titan III, but also different. The redundant O-ring points to a smaller probability, but the insulation geometry points to a higher probability.

In Table E-1, failure mode 3 has the most risk, even though it is only a Criticality 1R item. For this case, the computation of column W uses the following estimates:

- (i) There is one success path remaining after the primary failure.
- (ii) The availability of the backup is not readily detectable and is checked every third flight; and the estimated availability is .99.
- (iii) The probability of a secondary failure is .05.

The formula for column W is

$$\begin{aligned}
 W &= \Pr\{\text{Backup Available}\} \times \Pr\{\text{Secondary Failure}\} \\
 &+ \Pr\{\text{Backup not Available}\} \\
 &= (.99)(.05) + (.01) \\
 &= .0595
 \end{aligned}
 \tag{1}$$

For failure mode 1, there is no backup; but, it is a relatively rare (probability = .001) failure mode and infrequently (probability = .01) causes the worst damage state.

Failure mode 2 is much less risky. The computation of column W uses the following estimates:

- (i) There is one success path remaining after the first failure.

TABLE E-1 Improved Risk Assessment Procedure

T	U	V	W	X	Y	Z = (V)(W)(Y)
Failure Mode	Criticality	Probability of Primary Failure During Mission	Probability of Redundancy Failure, Given Primary Failure	Worst Damage State, Given Lack of Redundancy or Redundancy Failure	Probability of Worst Damage State, Given Lack of Redundancy or Redundancy Failure	Probability of Worst Damage State Event
1	1	.001	1	(A)—Loss of Life and/or Vehicle	.01	.00001
2	1R	.001	.001999	(A)—Loss of Life and/or Vehicle	.1	.000001999
3	1R	.01	.0505	(A)—Loss of Life and/or Vehicle	1	.000595

- (ii) The backup is readily detectable and fixed when failed and the availability of the backup is .999.
- (iii) Given the backup, the probability of secondary failure is .001—the same as the primary.

Use of equation (1) in this case yields

$$W = (.999)(.001) + (.001) = .001999$$

4. RELATIONSHIP BETWEEN IMPROVED PROCEDURE AND TABLE E-1

There is a strong relationship between the improvements described in Section 3 and NASA's Table 1 (Attachment 1 here). From the "SEVERITY" DEFINITIONS in column 1 of Table 1, we can deduce the following Worst Damage States:

- A. Loss of Life and/or Vehicle
- B. Mission is Aborted
- C. Degraded Operational Capability or Early Mission Termination or Damage to a Vehicle System
- D. Loss of Some Operational Capability of Vehicle, but Full Mission Duration.
- E. No Operational Effect

The probability scales could be set up as categories with the definitions given in Table E-2.

The Committee urges the use of quantitative definitions of probability. Even though for some failure modes the probabilities will be assessed subjectively, it is very important that the analyst have an operational definition. To reiterate, terms like "Unlikely" are not operational definitions. In

addition, use of a quantitative probability scale will augment the pure engineering judgment approach.

The factors in Reference [3], Section 3.4, are very relevant to assessing the **Probability of Primary Failure During Mission** in Table E-1. Other factors include:

- Product design certification test results
- Manufacturing process qualification test results
- Engineering analytical models
- Related industry data
- Etc.

The number of **SUCCESS PATHS** and the **REDUNDANCY/BACKUP** scenarios given in NASA's Table 1 (Attachment 1 to this appendix) are very relevant to assessing the **Probability of Redundancy Failure Given Primary Failure** in Table E-1.

The factors relevant to assessing the **Probability of Worst Damage State Event** in Table E-1 are very similar to those listed in Reference [3], Section 3.5. As part of the exercise of assessing this probability, one could list all the events subsequent to redundancy failure that do not lead to the worst damage state.

5. APPLICATION TO THE O-RINGS

Only as an example to illustrate the foregoing proposal, consider the field joint O-rings prior to the Challenger flight 51-L at a joint temperature of 31°F, which was predicted for the Challenger flight. It is based only on a limited knowledge of the subject derived from References [1] and [2],

TABLE E-2 Probability Scales For Improved Risk Assessment Procedure

Description	Center Point of Ranges of Probability Values		
	Probability of Primary Failure During Mission	Probability of Redundancy Failure Given Primary Failure	Probability of Worst Damage State Given Lack of Redundancy or Redundancy Failure
Very Likely	10 ⁻¹	10 ⁻¹	1.0
Likely	10 ⁻²	10 ⁻²	.5
Possible	10 ⁻³	10 ⁻³	10 ⁻¹
Unlikely	10 ⁻⁵	10 ⁻⁵	10 ⁻²
Very Unlikely	10 ⁻⁷	10 ⁻⁷	10 ⁻³

and thus must be viewed ONLY AS AN ILLUS-
 TRATION OF A PROCESS.

To keep things simple, only one failure scenario is considered. In the language of Table E-1 we have:

TABLE E-3 Application of Table E-1 to the SRM Field Joint

Language of Table E-1	Application to Field Joint
Primary failure during mission	Erosion and blowby of the primary O-ring
Redundancy failure given primary failure	Failure of the secondary O-ring given erosion and blowby of the primary O-ring
Worst damage state	Loss of life and vehicle

The reason for considering this scenario is that data are readily available. Also, in Reference [1], p. 135, it is stated that bypass erosion or blowby was considered much more serious than just impingement erosion.

The data set used in this analysis (see Attachment 2) is taken from pages 129–131 of Reference [1]. The subset of these data used here involves only the actual flights and only the field and nozzle joints. A useful organization of this subset is shown in Attachment 3. In the columns labeled “erosion,” “blowby,” and “erosion or blowby,” the blanks mean that the event did not occur. In the column labeled “blowby given erosion,” the blank means there was no erosion and the zero means that there was erosion but no blowby. Most of the data are for the primary O-rings; but the data with an asterisk are for the secondary O-rings.

5.1 Primary Failure

For primary O-ring failures, we consider the scenario of erosion and blowby. The primary failure probability is:

$$\Pr\{\text{Primary Failure}\} = \Pr\{\text{Primary Erosion}\} \\
 \times \Pr\left\{\begin{matrix} \text{Primary} \\ \text{Blowby} \end{matrix} \middle| \begin{matrix} \text{Primary} \\ \text{Erosion} \end{matrix}\right\}. \quad (2)$$

The vertical bar in the probability expression (2) reads “conditional on.” So, for example,

$$\Pr\{\text{Blowby} | \text{Erosion}\}$$

would read, “probability of the event Blowby, conditional on the event Erosion occurring.” For

two events A and B, a fundamental law of probability is

$$\Pr\{A \text{ and } B\} = \Pr\{A\} \times \Pr\{B | A\} .$$

5.1.1 Primary Erosion

A plot of the incidents of field joint primary O-rings with erosion is shown in Attachment 4. For example, flight 51–C, in January 1985, had two field joints with primary O-ring erosion; this mission experienced a joint temperature of 53° F and a leak check pressure of 200 psi. The fitted curves are derived from a statistical model which allows for possible joint temperature and leak check pressure effects.

Flight 51-C experienced both erosion and blowby of the field joint. At a subsequent Flight Readiness Review where 51-C was discussed, there was a concluding statement, “Low temperature enhanced probability of blow-by” (Reference [1], p. 147). On page H-73 of Reference [2], it is stated that, “Frequency of O-ring damage has increased since the incorporation of . . . higher stabilization pressures in leak test procedures . . .”. So it is of interest to statistically model the effect of temperature and leak check pressure on O-ring anomalies.

Let

$$p(t, s) = \text{Probability of erosion per field joint primary O-ring,}$$

where

$$t = \text{Joint temperature} \\
 s = \text{Leak check pressure.}$$

The assumptions for this statistical model are:

1. The model for $p(t, s)$ is:

$$\ln \left\{ \frac{p(t, s)}{1 - p(t, s)} \right\} = \alpha + \beta t + \gamma s . \quad (3)$$

This is called a Logistic Regression model. The variables α, β, γ are unknown parameters to be estimated from the data. Different values of these parameters represent different relationships between erosion probability and (temperature, pressure). For example, if $\beta < 0$, then probability decreases with temperature; but if $\beta > 0$, then probability increases with temperature. We will let the data determine which of these is most likely.

2. Given $p(t, s)$, the field joints are statistically independent.

Let

$x(t, s)$ = Number of field joint primary O-rings with erosion for a launch with joint temperature t and leak check pressure s .

Under these assumptions, the probability distribution of $x(t, s)$ given $p(t, s)$ is binomial with parameters $n = 6$ (i.e., 6 field joints) and $p = p(t, s)$. So for $k = 0, 1, \dots$, or 6,

$$\Pr \left\{ x(t, s) = k \mid p(t, s) \right\} = \binom{6}{k} [p(t, s)]^k [1 - p(t, s)]^{6-k}$$

Let the subscript i represent the i th launch in Attachment 3. So $i = 1, 2, \dots, 23$. Let

x_i = Number of field joint primary O-rings with erosion
 t_i = Joint temperature
 s_i = Leak check pressure
 $p_i = p(t_i, s_i)$

Also let

$$\begin{aligned} x &= (x_1, x_2, \dots, x_{23}) \\ t &= (t_1, t_2, \dots, t_{23}) \\ s &= (s_1, s_2, \dots, s_{23}). \end{aligned}$$

The likelihood function, L , given the data x , is defined as the probability of observing x conditional on t, s , and (α, β, γ) . The variables t and s are regarded as known variables (in standard regression analysis they are called independent variables); and (α, β, γ) are the unknown parameters. The likelihood function is regarded as a function of (α, β, γ) and is

$$L(\alpha, \beta, \gamma) = \prod_{i=1}^{23} \binom{6}{x_i} p_i^{x_i} (1 - p_i)^{6 - x_i}.$$

Recall that p_i is a function of (α, β, γ) .

The maximum likelihood estimates of the (α, β, γ) are those values that maximize the likelihood function. In effect, they are the values of (α, β, γ) that make the observed value of x the most probable under our model.

There is a close relationship between maximum likelihood estimation and least squares. The least squares estimates of (α, β, λ) are those values that minimize

$$\sum_{i=1}^{23} (x_i - 6p_i)^2,$$

where $6p_i$ is the expected value of x_i under our model. If the x_i 's had a Gaussian (normal) distribution with common variance, then the maximum likelihood estimates and the least squares estimates would be the same. This is because the Gaussian probability density would then be monotonically related to the sum of squares above. However, the probability densities of the x_i 's in our problem are binomial and not Gaussian. And it is a well established fact in statistical science that maximum likelihood estimation is usually more efficient (closer to the truth) than least squares; so we use maximum likelihood.

The results of a maximum likelihood analysis of these data under the above model yields the values in Table E-4.

TABLE E-4 Maximum Likelihood Analysis of the SRM Field Joint Primary O-Ring Erosion Data

Parameter	Maximum Likelihood Estimate	90% Confidence Interval
α	7.8	[-.1, 15.7]
β	.17	[-.28, -.06]
γ	.0024	[.012, .016]

The **90% Confidence Interval** reveals the fact that from our data we cannot learn the "true" value of (α, β, λ) with great precision. For example, a Bayes interpretation of the interval $[-.28, -.06]$ for the temperature effect, β , is that given our data, there is a .9 probability that the "true" value of β lies in the interval $[-.28, -.06]$. Note that this interval does not include the value $\beta = 0$ (i.e., no effect). **This means that the temperature effect is "statistically significant;" or that there is only a very small probability that the true value of β is greater than or equal to zero.**

Also note that there is no statistically significant pressure effect on field joint erosion. That is because most of the variation is explained by temperature variation. This is curious, because in Reference [1], blow-holes caused by high pressure were cited as a cause of erosion.

Plugging the maximum likelihood estimates into equation (3) yields

$$\begin{aligned} \ln \left[\frac{p(t, 200)}{1 - p(t, 200)} \right] &= 7.8 - (.17)t + (.0024)(200) \\ &= 8.3 - (.17)t. \end{aligned}$$

This implies

$$p(t,200) = \frac{e^{[8.3 - (.17)t]}}{1 + e^{[8.3 - (.17)t]}} \quad (4)$$

The curve for 200 psi (plotted in Attachments 4 and 5) is $(6)p(t,200)$, because there are 6 field joints.

The predicted probability per joint of primary O-ring erosion at 31° F joint temperature and 200 psi leak check pressure is

$$p(31,200) = .95 \left[\begin{array}{l} \text{Probability of} \\ \text{Primary Erosion} \end{array} \right] \quad (5)$$

The 90 percent confidence interval for the “probability of primary O-ring erosion” is shown in Attachment 5 and is [.5, 1.0]. This shows that the extrapolation to 31° F introduces considerable uncertainty in the estimate. The propagation of this uncertainty to the final result will be discussed in Section 5.5.

5.1.2 Primary Blowby Given Primary Erosion

The frequencies per primary O-ring of blowby given erosion were extracted from Attachment 3 and are given in Table E-5. An analysis of the blowby given erosion data shows no statistically significant effects of joint type, joint temperature, or leak check pressure. So we use the estimate

$$\begin{aligned} & \Pr \left\{ \begin{array}{l} \text{Primary Blowby} \\ \text{for Field Joint} \end{array} \middle| \begin{array}{l} \text{Primary Erosion} \\ \text{for Field Joint} \end{array} \right\} \\ &= \Pr \left\{ \begin{array}{l} \text{Primary Blowby} \\ \text{for Field or} \\ \text{Nozzle Joint} \end{array} \middle| \begin{array}{l} \text{Primary Erosion} \\ \text{for Field or} \\ \text{Nozzle Joint} \end{array} \right\} \\ &= .292 \end{aligned} \quad (6)$$

TABLE E-5 Frequency per Primary O-Ring of Blowby Given Erosion

Joint	Frequency per O-Ring
Field	$\frac{2}{7} = .286$
Nozzle	$\frac{5}{7} = .291$
Field plus Nozzle	$\frac{7}{24} = .292$

Plugging (5) and (6) into (2) yields

$$\begin{aligned} \Pr\{\text{Primary Failure}\} &= (.95) (.292) \\ &= .277 \end{aligned}$$

It is revealing to look at the frequency of primary O-ring blowby, given no erosion, in Table E-6.

TABLE E-6 Frequency per Primary O-Ring of Blowby Given No Erosion

Joint	Frequency per O-Ring
Field	$\frac{1}{2} = .50$
Nozzle	$\frac{1}{5} = .20$
Field plus Nozzle	$\frac{2}{7} = .286$

Comparison with Table E-5 shows that there is a strong statistical dependence between primary O-ring erosion and blowby—particularly for the field joint. For the field joint, blowby was rare (frequency = .015) when there was no erosion, but not rare (frequency = .286) when there was erosion. So

$\Pr\{\text{Blowby} \mid \text{Erosion}\} \gg \Pr\{\text{Blowby} \mid \text{No Erosion}\}$,
 which implies strong statistical dependence. If blowby and erosion were statistically independent, then these two conditional probabilities would be the same.

The strong statistical dependence shown above suggests that erosion might be a causal factor for blowby. This idea is born out by field data and various experiments. Experiments (reference [2], p. H-82) showed that an O-ring will fail to seal with an erosion depth of 0.15 inches. In flights 51-C and 51-B, there was both erosion and blowby of the field primary O-ring, and a heat effect or erosion of the secondary O-ring. In both cases, the erosion of the primary O-ring was among the worst erosions experienced (reference [2], p. H-71, H-72) as measured by cross-sectioned depths of 0.038 and 0.171 inches, cross-sectioned perimeters of 130° and 360°, and a top view of affected lengths of 58.75 and 12 inches. This implies that blowby can be caused by excessive erosion. So our model that the higher the probability of primary O-ring erosion, the higher the probability of primary O-ring blowby, is plausible.

5.2 Probability of Secondary Failure

Next we consider the **Probability of Redundancy Failure Given Primary Failure** in Table E-1. This would be failure of the secondary O-ring. Our model of secondary failure is secondary erosion and failure given primary erosion and blowby. Therefore,

$$\begin{aligned} & \Pr \left\{ \begin{array}{l} \text{Secondary} \\ \text{Failure} \end{array} \middle| \begin{array}{l} \text{Primary Erosion} \\ \text{and Blowby} \end{array} \right\} \\ &= \Pr \left\{ \begin{array}{l} \text{Secondary} \\ \text{Erosion} \end{array} \middle| \begin{array}{l} \text{Primary Erosion} \\ \text{and Blowby} \end{array} \right\} \\ &\times \Pr \left\{ \begin{array}{l} \text{Secondary} \\ \text{Failure} \end{array} \middle| \begin{array}{l} \text{Secondary} \\ \text{Erosion} \end{array} \right\}. \end{aligned} \quad (7)$$

A statistical analysis of secondary erosion given primary erosion and blowby shows no statistically significant effects of joint type, joint temperature, or leak check pressure. So we use the estimate from Table E-7 below:

$$\begin{aligned} & \Pr \left\{ \begin{array}{l} \text{Secondary Erosion} \\ \text{for Field Joint} \end{array} \middle| \begin{array}{l} \text{Primary Erosion and} \\ \text{Blowby} \\ \text{for Field Joint} \end{array} \right\} \\ &= \Pr \left\{ \begin{array}{l} \text{Secondary Erosion} \\ \text{for Field or} \\ \text{Nozzle Joint} \end{array} \middle| \begin{array}{l} \text{Primary Erosion and} \\ \text{Blowby for Field} \\ \text{or Nozzle Joint} \end{array} \right\} \\ &= .286 . \end{aligned} \quad (8)$$

TABLE E-7 Frequency per SRM Joint of Secondary O-Ring Erosion Given Erosion and Blowby of the Primary O-Ring in 23 Flights Prior to Challenger 51-L

Joint	Secondary Erosion Given Primary Erosion and Blowby
Field	$\frac{1}{2} = .50$
Nozzle	$\frac{1}{5} = .20$
Field plus Nozzle	$\frac{2}{7} = .286$

The estimation of

$$\Pr \left\{ \begin{array}{l} \text{Secondary} \\ \text{Failure} \end{array} \middle| \begin{array}{l} \text{Secondary} \\ \text{Erosion} \end{array} \right\}$$

in equation (7) presents some difficulties because there were no secondary failures before 51-L. So we shall express the solutions parametrically in terms of the parameter

$$\lambda_4 = \Pr\{\text{Secondary Failure}|\text{Secondary Erosion}\} \quad (9)$$

The state of knowledge curve (described in Appendix D) for λ_4 could be determined on the basis of engineering information. Examples of relevant engineering information which was available before 51-L are:

1. Joint rotation created doubt about the ability of the secondary O-ring to seal. In fact the O-ring failure mode was considered Criticality 1, not Criticality 1R. So, officially, the FMEA did not recognize the secondary O-rings as providing redundancy. However, according to Reference [1], p. 126, NASA management and Thiokol still considered the joint to be a redundant seal because there were flights where the primary O-ring failed and the secondary O-ring sealed in accordance with its design intent.
2. In July 1985, a Thiokol engineer, in light of the 51-B nozzle joint secondary O-ring erosion, expressed his concern that if the same scenario should occur in a field joint (and he believed it could), then it would be a "jump ball" as to the success or failure of the joint because the secondary O-ring could not respond to the clevis opening rate and might not be capable of pressurization (i.e., in the 51-L design, which has been changed in the redesigned joint). (See Reference [1], p. 139.)
3. The qualitative assessment (Reference [2], p. H-84, Chart 166) of the probability that the field joint secondary O-ring will fail given erosion penetration of the primary O-ring seal is listed in Table E-8.

TABLE E-8 Qualitative Probability of SRM Secondary O-Ring Failure Given Erosion Penetration of Secondary O-Ring

Time After Ignition	Qualitative Probability of Secondary O-Ring Failure
Ignition Transient: 0 to 170 ms 170 to 330 ms 330 to 600 ms	low medium high
Steady State: 60 ms to 2 min	high

4. There were only two incidents of secondary O-ring erosion in a field joint. So there was no solid statistical evidence that the secondary O-ring would work given primary O-ring failure; i.e., nothing like 1,000 successes without a failure. Also, as seen in Table E-8, the probability of secondary O-ring failure depends on time after ignition.
5. The night before the Challenger launch, a chart provided to NASA by a Thiokol engineer about the possible temperature effect on the O-rings (Reference [1], p. 89, Chart 2-2) included concerns that: (i) lower temperature of the O-rings would result in a change in their sealing timing function which would result in higher O-ring pressure actuation time; (ii) if the actuation time increases, threshold of secondary seal pressurization capability is approached; (iii) if threshold is reached, then secondary seal may not be capable of being pressurized.

Plugging (8) and (9) into (7) yields

$$\Pr \left\{ \begin{array}{l} \text{Secondary} \\ \text{Failure} \end{array} \right\} = (.286)\lambda_4 \left(\begin{array}{l} \text{Probability of} \\ \text{Secondary Failure} \end{array} \right) \quad (10)$$

5.3 Probability of Worst Damage State Given Redundancy Failure

If the field joint seal were to fail, there is some possibility that the crew and vehicle would survive. For example, the seal might fail right before the solid rocket motors completed their burn. However, the chances are very high that such a failure, should it occur, would be earlier in the flight. This suggests a value approaching 1 for the probability of loss of life and vehicle given total seal failure. Thus, the closest probability value of 1 from Table E-2, column **Probability of Worst Damage State**, is selected in this example.

5.4 Probability of Worst Damage State Event

Using the estimates derived above, the value for column Z in Table E-1 is

$$Z = (.277)(.286)\lambda_4 \left(\begin{array}{l} \text{Probability per Joint} \\ \text{of Worst Damage} \end{array} \right) = (.0792)\lambda_4 \quad (11)$$

5.5 Probability of At Least One Field Joint Failure

The estimated probability in Section 5.4 is for only one field joint. The estimated probability of field joint failure for the mission is

$$\begin{aligned} \Pr \left\{ \begin{array}{l} \text{Mission Field} \\ \text{Joint Failure} \end{array} \right\} \\ = 1 - \Pr \left\{ \begin{array}{l} \text{No Field} \\ \text{Joint Failures} \end{array} \right\} \\ = 1 - [1 - (.0792)\lambda_4]^6 \\ \text{(Probability of Failure)} \end{aligned} \quad (12)$$

It is clear from the statistical analyses that there is uncertainty in the estimates of the probabilities used. For example, the 90 percent confidence intervals in Table E-4 show that the parameter estimates are uncertain. Also, the .286 estimate in equation (8) was based on two failures out of seven, and is therefore uncertain. The uncertainty associated with equation (12) is quantified in Attachment 6. The two almost linear curves form a 90 percent confidence interval for the "probability of mission field joint failure," conditional on the value of λ_4 . So if the value of λ_4 is .25, for example, then the conditional 90 percent confidence interval is [0.010, .118].

A subject matter expert could analyze the relevant engineering information and assess a state of knowledge curve for 4. If this curve were centered on $\lambda_4 = .25$ with a considerable variance, then the unconditional 90 percent confidence interval for the "probability of mission field joint failure," would be much wider than the [0.010, .118] interval cited above.

The 90 percent confidence intervals in Attachment 6 were derived by a Bayesian analysis (see Appendix D for more discussion). For the 51-L environment (e.g., 31° F), we define the following long run "true" frequency probabilities:

- θ = Probability of mission field joint failure per mission; and for a given field joint,
- ϕ = Probability of failure
- λ_1 = Probability of primary O-ring erosion
- λ_2 = Probability of primary O-ring blowby given primary O-ring erosion
- λ_3 = Probability of secondary O-ring erosion given primary O-ring erosion and blowby
- λ_4 = Probability of secondary O-ring failure given secondary O-ring erosion.

$$\text{Our model is that } \theta = 1 - (1 - \phi)^6 \quad (13)$$

$$\phi = \prod_{i=1}^4 \lambda_i \quad (14)$$

$$\text{Let } \Lambda = \lambda_1 \lambda_2 \lambda_3 \quad (15)$$

$$\text{then } \theta = 1 - [1 - \Lambda \lambda_4]^6 \quad (16)$$

In the Bayesian analysis we assume that, conditional on our data, λ_1 , λ_2 , and λ_3 are statistically independent. This is reasonable because the λ_i 's are successive conditional frequencies. The state of knowledge curves for the individual λ_i 's were derived from Bayesian analyses assuming "flat" a priori state of knowledge curves. This means that we did not use much information external to the data in Attachment 3. For example, we made no attempt to use the engineering models described in, e.g., Reference [2], p. H-60. This may have been possible by modeling the uncertainties in the variables of the engineering models. This idea was suggested by Feynman (Reference [2], Appendix F). The uncertainties in the engineering models are a possible explanation as to why the models did not predict very well.

Finally, the state of knowledge curve for Λ was derived by propagating the state of knowledge

curves for the λ_i 's through equation (15). This was done by a discrete probability approximation technique. The implied 90 percent confidence interval for Λ is [.007, .082].

The upper and lower curves in Attachment 6 are derived from equation (16) and are

$$\begin{aligned} \theta_u(\lambda_4) &= 1 - [1 - (.082) \lambda_4]^6 \\ \theta_l(\lambda_4) &= 1 - [1 - (.007) \lambda_4]^6 \end{aligned} \quad (17)$$

REFERENCES

- [1] Report of the Presidential Commission on the Space Shuttle Challenger Accident, Volume 1, June 6, 1986, Washington, D.C.
- [2] Report of the Presidential Commission on the Space Shuttle Challenger Accident, Volume 2, June 6, 1986, Washington, D.C.
- [3] National Space Transportation System, "Instructions for Preparation of Critical Item Risk Assessment (CIRA)," NSIS 22491, June 19, 1987.

ATTACHMENT 1 NASA's Proposed CIRA Technique.

TABLE 1
CRITICAL ITEM RISK ASSESSMENT PROCEDURE DEFINITIONS MATRIX

"SEVERITY" DEFINITIONS	SUCCESS PATHS	STATUS CODE FOR REDUNDANCY/BACKUP	"DESIGN CONFIDENCE" DEFINITIONS	LIKELIHOOD OF WORST CASE FAILURE EFFECT
A - FIRST FAILURE RESULTS IN LOSS OF LIFE AND/OR VEHICLE	LIST NUMBER OF SUCCESS PATHS REMAINING AFTER FIRST FAILURE	a - NO BACKUP AVAILABLE (OR BACKUP NOT VERIFIABLE AS OUTLINED IN b THRU e)	I - FAILURE MODE CONSIDERED VERY LIKELY WITHIN LIFE OF SYSTEM	i - WORST CASE EFFECT IS VERY LIKELY
B - FIRST FAILURE RESULTS IN IMMEDIATE ABORT TO AVOID LOSS OF LIFE AND/OR VEHICLE (E.G. PAD & INTACT ABORTS)		b - BACKUP AVAILABLE, NOT DETECTABLE WHEN FAILED, BUT CHECKED PERIODICALLY FOR FAILURE MODE UNDER CONSIDERATION (E.G. EVERY 3RD FLIGHT, EVERY 3RD VEHICLE FLOW FOR GSE, ETC)	II - FAILURE MODE CONSIDERED LIKELY WITHIN LIFE OF SYSTEM	ii - WORST CASE EFFECT IS LIKELY
C - FIRST FLIGHT HARDWARE FAILURE RESULTS IN DEGRADED OPERATIONAL CAPABILITY OR UNACCEPTABLE FAILURE TOLERANCE MODE WHICH LEADS TO EARLY MISSION TERMINATION (E.G. PLS, SLS) OR FIRST GSE FAILURE RESULTS IN DAMAGE TO A VEHICLE SYSTEM		c - BACKUP AVAILABLE, NOT DETECTABLE WHEN FAILED, BUT CHECKED BETWEEN EACH FLIGHT/VEHICLE FLOW FOR FAILURE MODE UNDER CONSIDERATION	III - FAILURE MODE CONSIDERED POSSIBLE WITHIN LIFE OF SYSTEM	iii - WORST CASE EFFECT IS POSSIBLE
D - FIRST FAILURE RESULTS IN LOSS OF SOME OPERATIONAL CAPABILITY OF VEHICLE, BUT DOES NOT AFFECT MISSION DURATION		d - BACKUP AVAILABLE, READILY DETECTABLE WHEN FAILED, AND CHECKED PERIODICALLY FOR FAILURE MODE UNDER CONSIDERATION (E.G. EVERY 3RD FLIGHT, EVERY 3RD VEHICLE FLOW FOR GSE, ETC)	IV - FAILURE MODE CONSIDERED UNLIKELY WITHIN LIFE SYSTEM	iv - WORST CASE EFFECT IS UNLIKELY
E - FIRST FAILURE DOES NOT AFFECT OPERATIONAL CAPABILITY OF VEHICLE		e - BACKUP AVAILABLE, READILY DETECTABLE WHEN FAILED, AND CHECKED BETWEEN EACH FLIGHT/VEHICLE FLOW FOR FAILURE MODE UNDER CONSIDERATION	V - FAILURE MODE CONSIDERED VERY UNLIKELY WITHIN LIFE OF SYSTEM	v - WORST CASE EFFECT IS VERY UNLIKELY

ATTACHMENT 2 O-Ring Anomalies Compared with Joint Temperatures and Leak Check Pressure

Flight or Motor	Date	(Solid Rocket Booster)	Joint/ O-Ring	Pressure (In psi)				Joint Temp. °F
				Field	Nozzle	Erosion	Blowby	
DM-1	07/18/77	-	-	NA	NA	-	-	84
DM-2	01/18/78	-	-	NA	NA	-	-	49
DM-3	10/19/78	-	-	NA	NA	-	-	61
DM-4	02/17/79	-	-	NA	NA	-	-	40
QM-1	07/13/79	-	-	NA	NA	-	-	83
QM-2	09/27/79	-	-	NA	NA	-	-	67
QM-3	02/13/80	-	-	NA	NA	-	-	45
STS-1	04/12/81	-	-	50	50	-	-	66
STS-2	11/12/81	(Right)	Aft Field/Primary	50	50	X	-	79
STS-3	03/22/82	-	-	50	50	-	-	69
STS-4	06/27/82	unknown: hardware lost at sea		50	50	NA	NA	80
DM-5	10/21/82	-	-	NA	NA	-	-	58
STS-5	11/11/82	-	-	50	50	-	-	68
QM-4	03/21/83	-	Nozzle/Primary	NA	NA	X	-	60
STS-6	04/04/83	(Right)	Nozzle/Primary	50	50	(1)	-	67
		(Left)	Nozzle/Primary	50	50	(1)	-	67
STS-7	06/18/83	-	-	50	50	-	-	72
STS-8	08/30/83	-	-	100	50	-	-	73
STS-9	11/28/83	-	-	100(2)	100	-	-	70
STS 41-B	02/03/84	(Right)	Nozzle/Primary	200	100	X	-	57
		(Left)	Forward Field/ Primary	200	100	X	-	57
STS 41-C	04/06/84	(Right)	Nozzle/Primary	200	100	X	-	63
		(Left)	Aft Field/Primary	200	100	(3)	-	63
		(Right)	Igniter/Primary	NA	NA	-	X	63
STS 41-D	08/30/84	(Right)	Forward Field/Primary	200	100	X	-	70
		(Left)	Nozzle/Primary	200	100	X	X	70
		(Right)	Igniter/Primary	NA	NA	-	X	70
STS 41-G	10/05/84	-	-	200	100	-	-	78
DM-6	10/25/84	-	Inner Gasket/ Primary	NA	NA	X	X	52
STS 51-A	11/08/84	-	-	200	100	-	-	67
STS 51-C	01/24/85	(Right)	Center Field/ Primary	200	100	X	X	53
		(Right)	Center Field/ Secondary	200	100	(4)	-	53
		(Right)	Nozzle/Primary	200	100	-	X	53
		(Left)	Forward Field/ Primary	200	100	X	X	53
		(Left)	Nozzle/Primary	200	100	-	X	53

Dash (-) denotes no anomaly; NA denotes not applicable.
 See end of attachment for footnotes.

ATTACHMENT 2 (continued)

Flight or Motor	Date	(Solid Rocket Booster)	Joint/ O-Ring	Pressure (in psi)		Erosion	Blowby	Joint Temp. °F
				Field	Nozzle			
STS 51-D	04/12/85	(Right)	Nozzle/Primary	200	200	X	-	67
		(Right)	Igniter/Primary	NA	NA	-	X	67
		(Left)	Nozzle/Primary	200	200	X	-	67
		(Left)	Igniter/Primary	NA	NA	-	X	67
STS 51-B	04/29/85	(Right)	Nozzle/Primary	200	100	X	-	75
		(Left)	Nozzle/Primary	200	100	X	X	75
		(Left)	Nozzle/Secondary	200	100	X	-	75
DM-7	05/09/85		Nozzle/Primary	NA	NA	X	-	61
STS 51-G	06/17/85	(Right)	Nozzle/Primary	200	200	X (5)	X	70
		(Left)	Nozzle/Primary	200	200	X	X	70
		(Left)	Igniter/Primary	NA	NA	-	X	70
STS 51-F	07/29/85	(Right)	Nozzle/Primary	200	200	(6)	-	81
STS 51-I	08/27/85	(Left)	Nozzle/Primary	200	200	X (7)	-	76
STS 51-J	10/03/85		-	200	200	-	-	79
STS 61-A	10/30/85	(Right)	Nozzle/Primary	200	200	X	-	75
		(Left)	Aft Field/Primary	200	200	-	X	75
		(Left)	Center Field/ Primary	200	200	-	X	75
STS 61-B	11/26/85	(Right)	Nozzle/Primary	200	200	X	-	76
		(Left)	Nozzle/Primary	200	200	X	X	76
STS 61-C	01/12/86	(Right)	Nozzle/Primary	200	200	X	-	58
		(Left)	Aft Field/Primary	200	200	X	-	58
		(Left)	Nozzle/Primary	200	200	-	X	58
STS 51-L	01/28/86			200	200			31

- (1) On STS-6, both nozzles had a hot gas path detected in the putty with an indication of heat on the primary O-ring.
- (2) On STS-9, one of the right Solid Rocket Booster field joints was pressurized at 200 psi after a destack.
- (3) On STS 41-C, left aft field had a hot gas path detected in the putty with an indication of heat on the primary O-ring.
- (4) On a center field joint of STS 51-C, soot was blown by the primary and there was a heat effect on the secondary.
- (5) On STS 51-G, right nozzle had erosion in two places on the primary O-ring.
- (6) On STS 51-F, right nozzle had hot gas path detected in putty with an indication of heat on the primary O-ring.
- (7) On STS 51-I, left nozzle had erosion in two places on the primary O-ring.

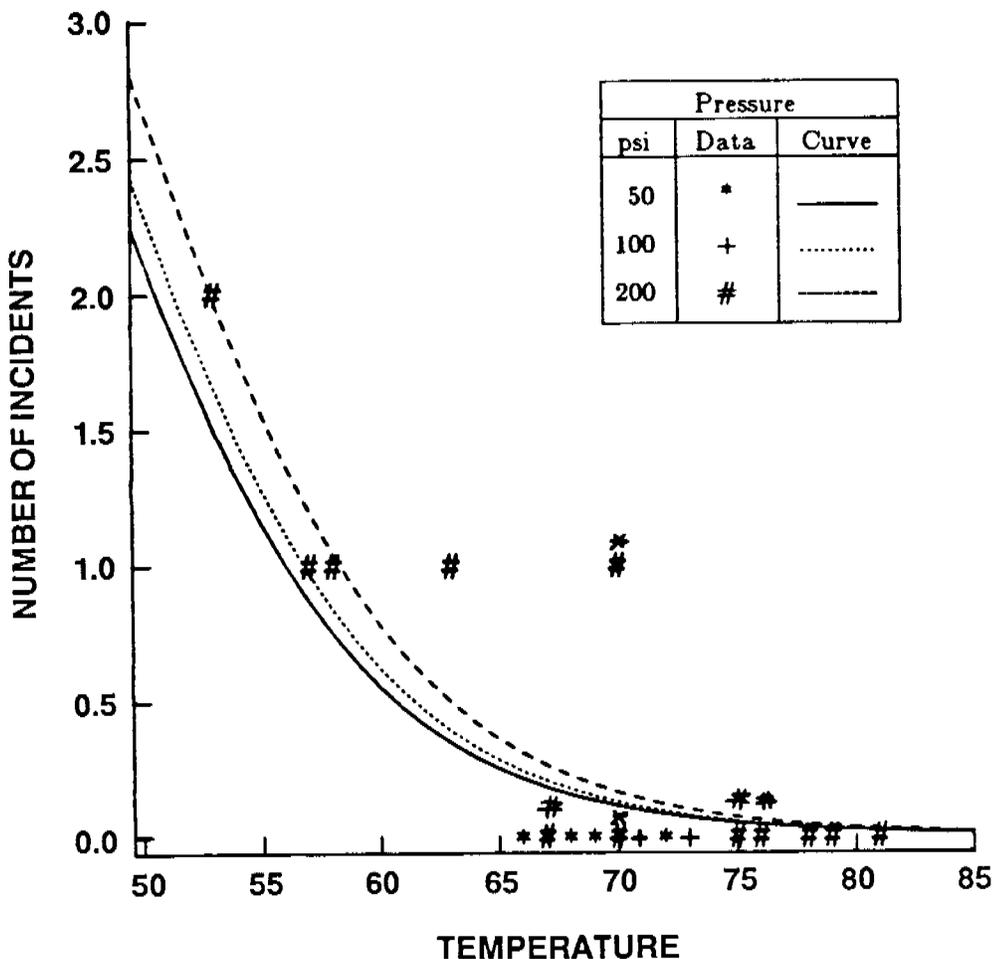
ATTACHMENT 3 O-Ring Anomalies Prior to Challenger

Flight	Date	Field		Nozzle		Field + Nozzle		Joint Temp.	Leak check** pressure		
		erosion or blowby	erosion or blowby	erosion or blowby	erosion or blowby	erosion or blowby	erosion or blowby				
1	04/12/81							66	50		
2	11/12/81	1	1	0		1	0	70	50		
3	03/22/82							69	50		
5	11/11/82							68	50		
6	04/04/83				2	2	0	67	50		
7	06/18/83							72	50		
8	08/30/83							73	100/50		
9	11/28/83							70	100/100		
41-B	02/03/84	1	1	0	1	1	0	57	200/100		
41-C	04/06/84	1	1	0	1	1	0	63	200/100		
41-D	08/30/84	1	1	0	1	1	1	70	200/100		
41-G	10/05/84							78	200/100		
51-A	11/08/84							67	200/100		
51-C	01/24/85	2,1*	2	2,1*	2	2	4,1*	53	200/100		
51-D	04/12/85				2	2	2	67	200		
51-B	04/29/85				2,1*	1	2,1*	75	200/100		
51-G	06/17/85				2	2	2	70	200		
51-F	07/29/85				1	1	1	81	200		
51-I	08/27/85				1	1	1	76	200		
51-J	10/03/85							79	200		
61-A	10/30/85		2	2	1	1	3	75	200		
61-B	11/26/85				2	1	2	76	200		
61-C	01/12/86	1	1	0	1	1	3	58	200		
51-L	01/28/86							31	200		
Total		7,1*	4	9,1*	2	17,1*	8	24,2*	12	29,2*	7

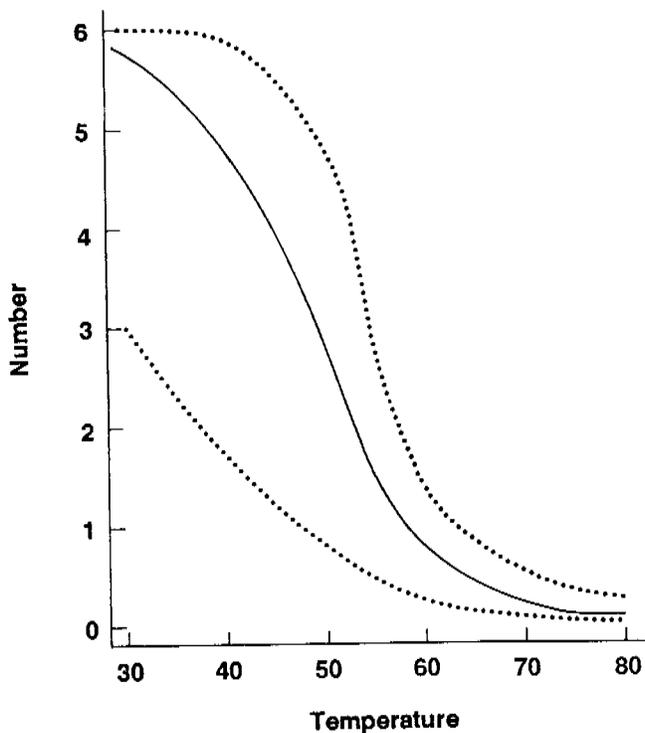
* Secondary O-ring

** Field/nozzle

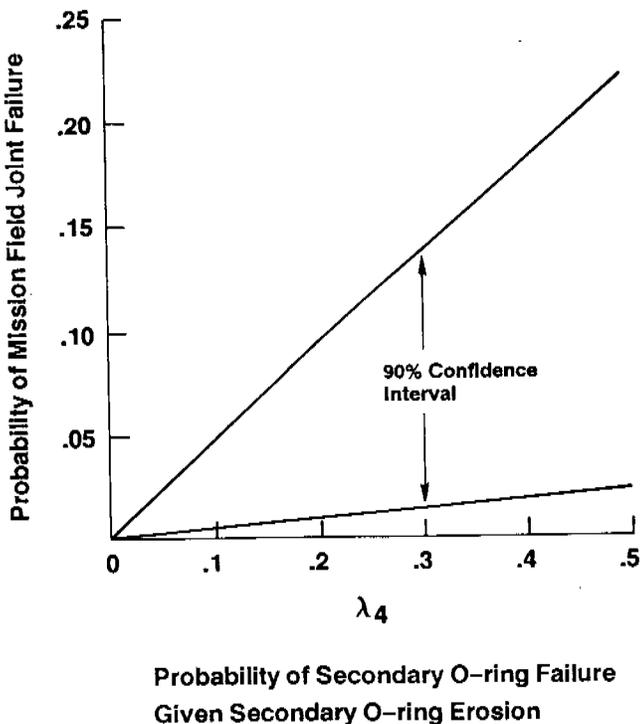
ATTACHMENT 4 Occurrence of Field Joint Primary O-rings with Erosion.



ATTACHMENT 5 Maximum Likelihood Estimate and 90% Confidence Interval for the Number of Field Joint Primary O-rings with Erosion at 200 psi.



ATTACHMENT 6 90 Percent Confidence Interval for the "Probability of Mission Field Joint Failure," as a Function of λ_4 .



APPENDIX F

DESCRIPTION OF PROPOSED SYSTEMS SAFETY ENGINEERING FUNCTIONS IN SUPPORT OF NATIONAL SPACE TRANSPORTATION SYSTEM RISK ASSESSMENT AND RISK MANAGEMENT

In Section 5.11 the Committee recommends that NASA consider bringing together appropriate activities into a focused "Systems Safety Engineering" function at both Headquarters and the centers. This activity would apply across the entire set of design, development, qualification and certification, and operations activities of the National Space Transportation System (NSTS) Program in support of risk assessment and risk management. Systems safety engineering would embrace the functions (listed in Section 5.11 and illustrated here in Figure F-1) which are described briefly in the following paragraphs.*

1. IDENTIFICATION OF FAILURE MODES AND EFFECTS

The failure modes of each hardware item can be identified at this step without addressing the probability of each failure mode occurring. All of the significant effects of each failure mode also would be identified. These effects (not just the estimated worst-case effect) are needed also for identification of hazards and for evaluating potential cascading influences on the failure modes of other parts of the system. All of the causes of each failure mode (including the feedback influences from the hazard analysis, step 3 below) should then be identified. The control of all causes of each failure mode by design margin, process controls, redundancy, and operating constraints would be defined. This information would be an input to the analysis of safety risks in steps 5, 8, and 9.

2. ESTABLISHMENT OF DESIGN CRITERIA FOR REDUNDANCY

Design criteria for redundancy would be based on functional and fail-operational requirements for components or units which do not have catastrophic single failure modes. These criteria would be based on reliability analyses of components using either statistical data bases where available or estimated failure rate functions.

* In Figure F-1, the thirteen functions discussed in this appendix are shown by the boxes which are numbered to correspond. This diagram can be compared to that currently described for the NSTS Program by the JSC SR&QA office, as shown in Figure 5-12 in Section 5.11.

3. IDENTIFICATION OF HAZARDS AND THEIR POTENTIAL CONSEQUENCES

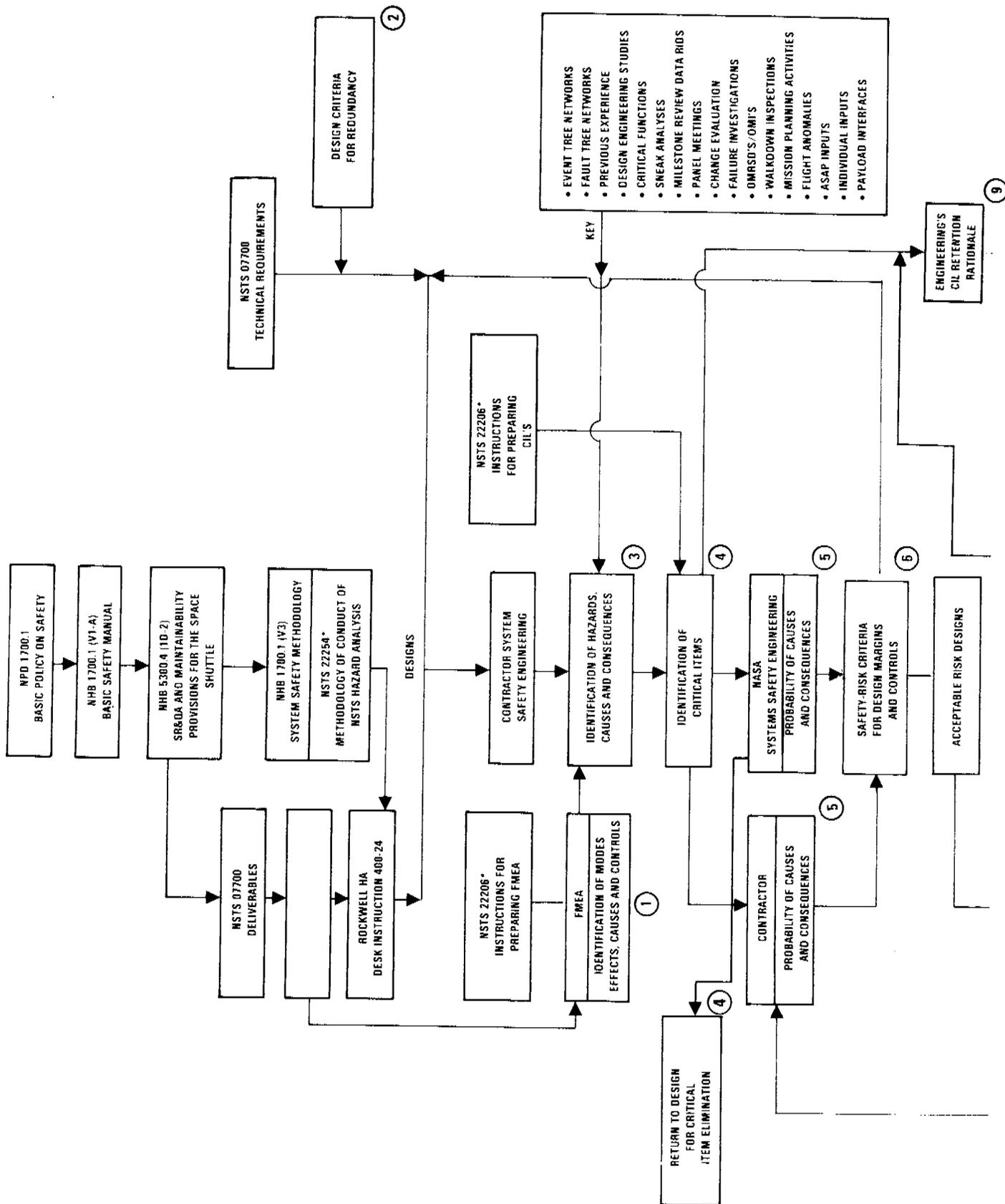
Hazards associated with the system can be systematically identified using various methods such as fault-tree or event-tree networks. Inputs will come from mission requirements, the system configuration, the applicable identified hardware failure effects, human factors and the expected environments. Potential consequences of the presence of each hazard can then be derived without regard for the probability of the events or mishaps occurring. (However, some screening out of *very* low probability failure events would simplify this effort.) Mishaps resulting from combinations of events and the impacts of created hazards on failure modes in other hardware can be identified. Each of the causes of the identified hazards, along with proposed controls, would be defined for later risk assessment in steps 5, 8, and 9.

4. IDENTIFICATION OF CRITICAL ITEMS

Using the set of information generated in the previous steps, hardware failure modes could be categorized on the basis of their potential consequences. Those designs having failure modes with consequences that could result in loss of vehicle or life would be returned to engineering for possible alternative concepts. Failure modes that remain after this cycle could be put into criticality categories to be prioritized based on severity of the failure effects and the probability of occurrence (steps 8 and 9). Those in prioritized categories which require Level I approval for either retention or a waiver authorization would be submitted through Level II PRCB along with a full safety-risk assessment produced under the direction of NASA systems safety engineers (step 13).

5. EVALUATION OF THE PROBABILITY OF OCCURRENCE OF CAUSES AND CONSEQUENCES OF FAILURE MODES AND HAZARDS

An evaluation can be made of the probability of occurrence of each of the causes and consequences for each retained failure mode and hazard. These



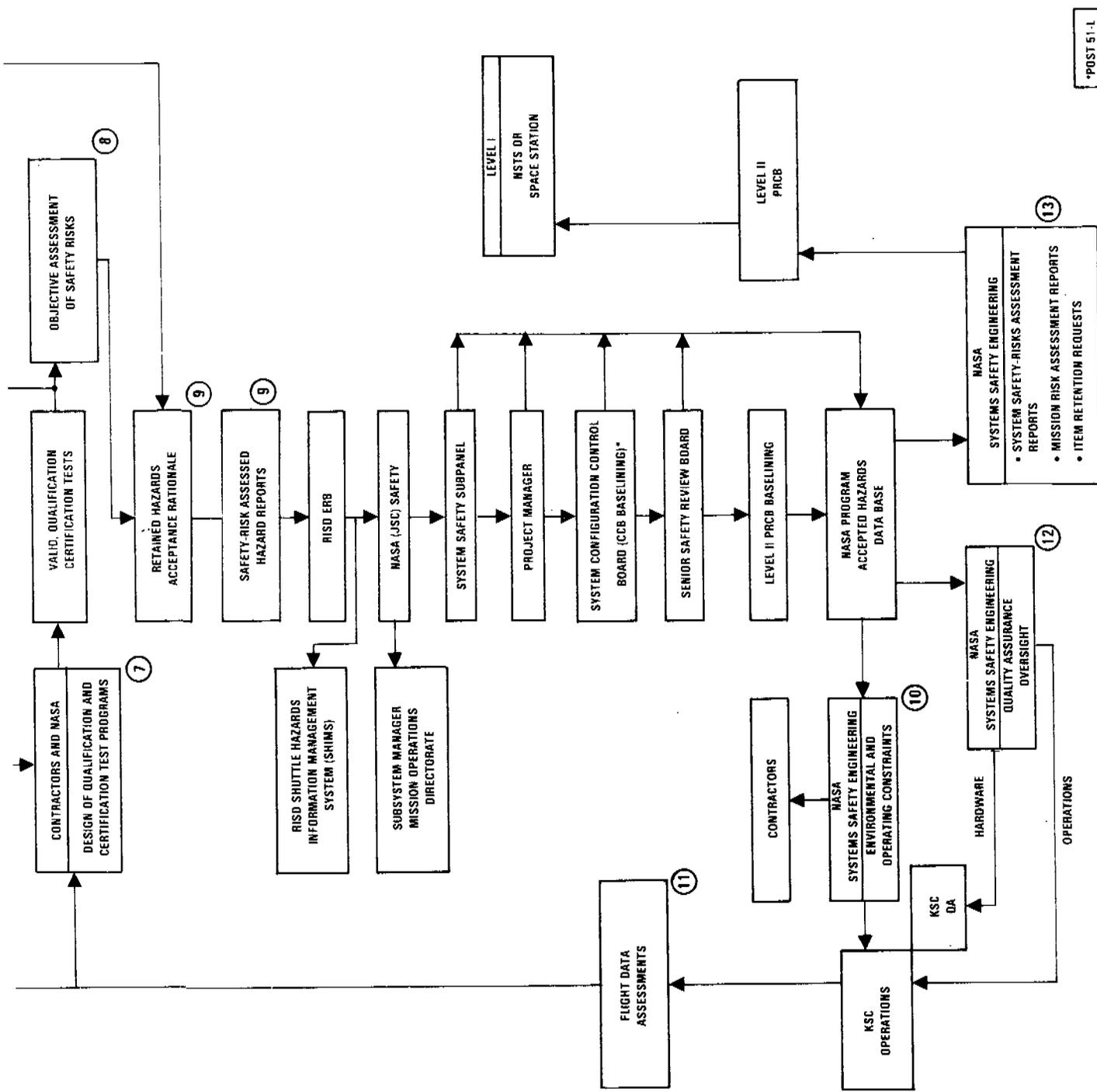


FIGURE F-1 Flow diagram of proposed systems safety engineering functions in support of risk assessment.

analyses could be performed by both the contractors' and NASA's systems safety engineers. A variety of tools can be used to perform these evaluations. The determination of probability of occurrence of the causes of failures would be expressed as a set of functions related to:

- a. Reliability data for hardware items having causes of failure modes that are statistical in nature, such as electronic boards.
- b. Wear-out functions for hardware line replaceable units where the causes of the failure modes are both statistical and have safety operating margins that are either time or cycle dependent.
- c. Operating margins required where the causes of the particular modes of hardware failure are dependent on stress, temperature, or other environmental factors to which the unit may be subjected.
- d. The control which can be exercised over the true configuration of the part, unit, subsystem, or system. This includes both the validation and control of manufacturing and integration processes, and the ability to explicitly verify the configurations prior to operations.

Evaluation of the probability of occurrence of each of the possible consequences of critical hardware failures or the presence of other severe hazards requires assessment of each path of the fault tree. The prevention of certain consequence paths would be evaluated relative to the system design and the specific operational hazard control techniques. Probability functions need to be determined for both the causes and consequences in order to provide inputs, both to the overall risk assessment which will guide the final design (or for the current STS, the proposed design changes), and to the criteria on which the validation and certification test programs should be based.

6. ESTABLISHMENT OF SAFETY-RISK LEVEL CRITERIA FOR DESIGN MARGINS AND HAZARD CONTROLS

Using relationships of the types derived under step 5 as a framework, risk levels can be allocated among the various subsystems, units, and components that would be consistent with the acceptable safety-risk requirements established by NASA for the overall NSTS program. Design criteria can then

be established for the margins required against each cause of a critical failure mode (using the functions developed in step 5) and for the controls required to limit the consequences of each hazard. This task is critical to providing assurance that the NSTS system has been configured to a given (acceptable) set of safety-risk levels. (Note that one *cannot assure* fully safe operations.) Those risk levels (which may be quite different for loss of hardware versus loss of life) must have a definable and objective set of measures that can be agreed upon by Level I and the Administrator of NASA. They must later be verified during the test programs. Without such quantitative safety-risk level assessments, *assurances* of acceptable safety are not meaningful and the fulfillment of responsibility is not measurable.

7. DESIGN OF QUALIFICATION AND CERTIFICATION TEST PROGRAMS

Once safety margins have been determined for each failure mode of the accepted designs, quantitatively significant validation, qualification, and (where required) time or cycle (reuse) dependent certification test programs can be designed. These test plans must be optimized to extract the maximum amount of information on operating margins against critical failure modes from the most cost effective quantity of hardware and the time period which can be allocated to tests. Design of the test programs is crucial to the viability of making risk assessments. The criteria for the tests should be established by reliability and/or systems safety engineers who specialize in test program design and statistical analysis of test data.

8. OBJECTIVE ASSESSMENT OF SAFETY RISKS

The test data should be statistically analyzed to establish credible validated margins against the causes of each significant potential failure mode. When these measured margins are compared with the margin criteria from step 6, and when the probability functions for configuration control (step 5.d) are derived, there will be a meaningful basis for making assessments of the probability of occurrence for each failure mode and its associated hazard. These probabilities of occurrence must be combined with the appropriate analyses of the probabilities of the consequences being realized for each failure at the subsystem and total system levels

to provide an objective measure of the portions of the overall safety-risks that are associated with each retained design and hazard.

9. DEVELOPMENT OF ACCEPTANCE RATIONALE FOR RETAINED HAZARDS AND HAZARD REPORTS

Rationales for accepting the safety risks associated with all created and intrinsic hazards would be developed. For those hazards caused by hardware failure modes, these rationales would embody the Critical Items List retention rationales developed by the various engineering groups and the test-based safety-risk assessments generated in step 8. This information would be published as a set of *risk assessed* hazard reports. These reports would go through the approval and data management process shown in Figure F-1. Upon approval by Level II PRCB, they would constitute the NSTS Accepted Hazards Data Base.

Those hazards in the data base which result from the currently defined Criticality 1 and 1R items could then be further classified and prioritized based on their assessed safety risks. Those requiring final acceptance at Level I would have special request packages prepared by NASA systems safety engineering. To avoid the misconceptions associated with thousands of waivers to an accepted system design, these requests should fall into two categories:

1. Items which met their specific design criteria, including safety-risk criteria (step 6). These items should *not* require a "waiver," but only Level I approval of the retention requests because of their perceived importance or risk contribution.
2. Items which *did not* meet their specific safety-risk design criteria as indicated by test margins or detailed risk analyses. These items would therefore require a "waiver" for retention.

These approval requests to Level I would be presented in conjunction with an overall System Safety Assessment Report and specific Mission Risk Assessment Reports (step 13 below).

10. SPECIFICATION OF ENVIRONMENTAL AND OPERATING CONSTRAINTS

Having accepted a residual hazard (whether contained or catastrophic) the NASA systems safety

engineers must specify very explicitly for all equipment levels (part, unit, subsystem, element, and full system) the environmental and operating constraints which will *assure* that the validated margins will not be violated. In this regard, this task also would have a major interface with the operations activities. The analysis of such things as the effect of environmental conditions on the validity of validations and certifications is usually not done by the quality assurance engineers; therefore, the systems safety engineers should be the responsible focus for this task.

11. QUANTITATIVE EVALUATION OF FLIGHT DATA TO UPDATE SAFETY MARGIN VALIDATIONS

By reviewing all flight data (or other off-line test data and even test data from other programs) for explicit information, updated quantitative assessments of the validated design criteria can be made. In order to retain the assured level of risk as new data become available, specifications may have to be changed for some hardware or new operational constraints may have to be defined.

12. OVERSIGHT OF QUALITY ASSURANCE FUNCTIONS TO CONTROL SAFETY-RISKS

In order to fulfill its responsibility to *assure* control to the accepted levels of risk, the systems safety engineers must oversee the appropriate quality assurance functions. This is essential because the validated margins and assessed risks of the retained hazards are dependent on total configuration verification of the overall system and each of its constituent parts. By "total" configuration one means all aspects of the hardware, software, external environments and operating constraints.

13. OVERALL SYSTEM SAFETY RISK ASSESSMENT AND DEFINITION OF THE POTENTIAL TO REDUCE THE LEVEL OF RISK

Using all of the above information, the NASA systems safety engineers can prepare a series of "System Safety Assessment Reports." These reports would continuously update overall system risk assessments against the safety-risk objectives established for the various phases of the NSTS Program by the risk management activity. The systems safety engineers also would define the potential to reduce the levels of risk in the program. Mission risk

assessment reports would also be prepared which would incorporate mission accomplishment risk assessments, of which the safety risks would be one input.

Where required, retention request packages generated in step 9 would be submitted through Level II to Level I along with the approved safety-risk assessments for each item and an appropriate

summary of the overall system safety-risks assessment report. Thus, the retention requests can be considered by Level I within the context of a definable and objective risk management process. The arguments for retention of prioritized critical items would be combined with objective assessments of safety-risks for each item's contribution to the overall system's safety risks.