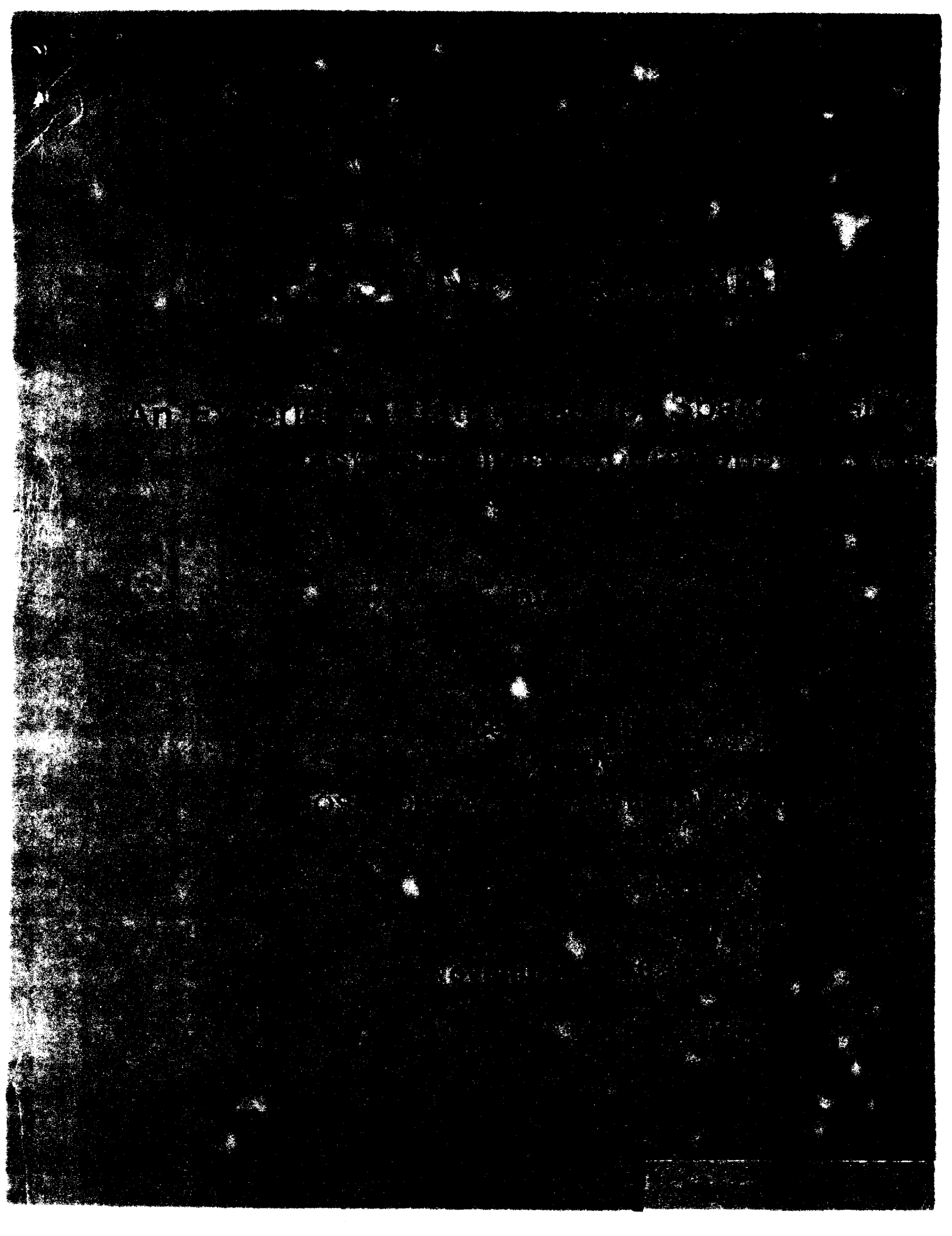

LESSONS LEARNED

An Experience Data Base for Space Design, Test and Flight Operations

by

Gilbert L. Roth
Staff Director
Aerospace Safety Advisory Panel

November 1986

---Special Note---

Even "Lessons Learned" can be overtaken by current events. Therefore, additions and modifications will be forthcoming on an "as needed" basis. Also, if readers have "Lessons Learned" that they would like to see included please send them to:

Gilbert L. Roth
Staff Director
Aerospace Safety Advisory Panel
NASA Headquarters
Washington, D.C. 20546

TABLE OF CONTENTS

I. INTRODUCTION

A. Preface

This document summarizes specific and generic lessons that have been "learned" as a result of the fact-finding activities of the Aerospace Safety Advisory Panel. As a program matures, it is advantageous to pause and reflect on the lessons learned during the conduct of the program and to record these reflections while they are fairly fresh in mind so that other programs can benefit from the experience. These lessons learned are intended primarily for use by those involved in any critical NASA program or project and who are somewhat familiar with the disciplines covered here. Thus the format used here favors brevity over excessive detail. In effect, it is an attempt to record some of the pitfalls a program has experienced, with a goal of alerting others to potential trouble spots and to suggest solutions which might improve the reader's program or project.

A candid treatment such as this may permit the drawing of incorrect inferences as to the general efficacy of NASA/industry management and technical proficiency, particularly by those uninitiated to the complexity of some of the "deficiencies" noted. Recommendations and actions described are not necessarily the only or best approaches. They reflect mainly the Space Transportation System experience (plus help from other ongoing aero and space work) which must be tailored to the "new" situation and should be accepted by the reader as one input to the many facets of both technical and management decisions. As such, they should be used to help identify potential problems in a timely manner and benefits should accrue when applied to projects in their early stages as well as the more mature ones.

Many of the lessons are somewhat subjective and represent individual opinions and therefore should not be interpreted as official statements of NASA positions or policies. The extent to which the problems described here repeatedly occur should eliminate any complacency or rationale on the part of any manager or designer that such shortcomings apply only to others.

Gerrard Bruggink, former deputy director of the U.S. National Transportation Safety Board's Bureau of Aviation Safety, in a paper entitled "Compromises Without Cause," says:

> With the hindsight of a thorough investigation, most accidents are foreseeable. While our accident data banks are bulging with this after-the-fact wisdom, we keep telling ourselves: we have to learn more about accident causes and human behavior before we can achieve greater safety. It is my contention that it is not the lack of knowledge but the reluctance to apply our present knowledge that limits the effectiveness of our efforts and expenditures."

B. Background

The Aerospace Safety Advisory panel members, consultants and staff occupy a unique position with regard to NASA, contractors, and other agencies. The Panel was established and continued by congressional statute, the personnel (with exception of staff) are non-NASA, the Panel reports to both the NASA Administrator and the Congress. They have "no axe to grind." This unique position allows them, through various modes of fact-finding, to look into and behind the many activities associated with large and small aerospace programs from concept through operations. The insight thus gained has been used to develop the findings, lessons learned, and recommendations here, and they represent a good cross-section of experiences that anyone can apply. Historically the Panel has been given unlimited scope in looking into NASA'S activities with an eye toward ground and flight safety as well as those program facets that make for mission success. The Panel has reviewed these data and is confident that NASA and its contractors will truly make constructive use of these "Lessons Learned".

C. Scope of This Work

The breadth of the Panel's work has, in fact, defined the scope of the lessons learned. This can be defined by the following statement made by a past Deputy Administrator of NASA:

> "Where do the Panel's interests lie? A safety review usually tends to concentrate on the engineering design and quality control aspects of safety. While these are important factors, they do not represent the total necessary for safe and reliable programs. Just as important are manufacturing practices, organizational structure, facilities, and human attitudes. Management approaches--and particularly management's ability to balance schedule, cost, design, development, and testing--often are the most important factors in the total success and safety of a program."

This certainly defines the Panel's role and the scope of the material covered here. An adjunct to this are the annual reports issued by the Panel and presented to the NASA Administrator and the Congress covering major NASA programs and projects--particularly those involving "manned systems." These annual reports provide further background on these and other lessons learned.

D. Source Data

Source material came from many activities beyond the Panel's own numerous factfinding work. These included:

1. Level III STS Change Control Boards at MSFC, JSC and KSC.

2. Level II STS Program Review and Control Board input/output at JSC
3. Level I STS Program Cost Review Board
4. Panel Annual Reports, 1973 to 1986
5. Panel Testimony to Congress during 1973-1986 period
6. Discussions with Shuttle Centaur personnel at NASA and Contractors between 1983-1986
7. Discussions with Space Station personnel at NASA and Contractors particularly at KSC, JSC and NASA Headquarters
8. Participation by Staff Director in NASA and Contractor working meetings at various sites
9. STS and Space Station Status reports from JSC and NASA Headquarters.

II. FINDINGS, LESSONS LEARNED, RECOMMENDATIONS

First, a few definitions so that we start off together:

o Findings - A management or technical deficiency which indicates a violation of an established policy, procedure, formal instruction, or of generally accepted good practice.

o Lessons Learned - One or more findings provides specific and/or generic practical benefits that can be retained for application to on-going and future programs and projects. Lessons learned when applied can help avoid pitfalls and problems that might otherwise occur.

o Recommendations - Indicates, where possible, how the lesson learned can be used or might be implemented . . . what actions should be considered to best meet the needs of a particular program or project.

A. Technical and Administrative Management Functions

1. Roles, Responsibilities and Relationships

Findings:

Relationships, e.g., communications, team spirit and responsiveness, between NASA Centers and Headquarters have altered over the years, becoming more impaired as resources, schedules and performance requirements have "tightened up." The Shuttle's unrelenting schedule pressure, combined with a host of engineering problems/modifications, and budget shortages, led to a good deal of "buckpassing" and an attitude of "its your problem, not mine." A secondary fallout has been the undue reliance upon an elaborate structure of review and oversight groups that has lead to the feeling that "not to worry, the safety and reliability guys will catch it down the road anyway!"

The review system leading to authorization to conduct major ground tests as well as those preceding flight has come under

close examination during the months following the Challenger accident. However, the Panel in examining this aspect of the total management system had this to say: "The Aerospace Safety Advisory Panel believes that the readiness process needs to be reconstituted before it is effective for operations. To the Panel it appears that:

- Reliability, safety, and quality organizations should be more clearly in the decision loops and the documentation process appears to be used more for post-operation justification of actions that for deciding readiness.

- The documentation used for summarizing risk and evaluation of readiness as represented by the safety assessment report, the accepted risk summary, and the critical issues summary all appear dedicated to listing every possible concern so that retrospective examination will find no basis for criticizing thoroughness. These procedural activities did not appear to represent a management level-by-level evaluation of risks and a summary of assessed total risk truly suitable for use by higher management.

- The inherent assurance of having separate operation teams independently assess readiness, as is the case with established transportation systems may not function adequately with NASA's present structure to assure independent readiness opinion.

Lesson Learned:

Historically, management of the Space Transportation System has developed a pattern whereby Headquarters balances input from the "program," the Centers, and the test community. Thus, no one organization within NASA has full responsibility for operations decisions. This must be modified before a routine and reliable operations function can achieve success. Policy-oriented goals, to make sense, should take account of technical realities. This suggests, in turn, the desirability of continuing interchange and communication between technical managers and policy-oriented administrators. Fragmentation and compartmentalization of information by the "competing" R&D Centers, and for that matter offices within a given Center, sours the needed team spirit and openness to assure the best solution for any given problem or concern and to give decision-makers the wherewithall to do their job correctly.

Recommendation:

First, the overall "system" (NASA and its contractors) has to take the time to assure that everyone is aware that the old philosophy that technical excellence is more important than schedule has not changed.

Second, The Space Shuttle is a development program--not an operational transportation system--at this time or in the near future. This must be understood to achieve "the return to safe flight in the shortest possible time."

Third, the primacy of NASA Headquarters must be reestablished in relation to the responsibilities and authority--both formal and informal--of the R&D Centers. This is a Presidential Commission recommendation as well. Beyond this, however, is the need for a tough-minded look at NASA's basic institutional structure and its established methods for carrying out complicated technical programs. Although it is not easy to change traditions and values that surround each of the NASA Centers (nor would it be wise to destroy entirely their loyalties and commitments), it is necessary to develop operating procedures and relationships that permit agency-wide priorities to be carried out successfully. To restate a jaded axiom: "One should strive for a structure that makes the whole greater than the sum of its parts."

2. STS Technical Audit Process

Findings:

Among the many successes of the early STS mission flight readiness process was a technical audit initiated at JSC to review and supplement the more routine sneak circuit analyses. This ad hoc function did not use "independent" evaluators or professional safety or quality assurance practitioners. It utilized the design team members who were responsible for major elements of the shuttle systems and therefore had familiarity with the fundamentals of the systems and their limitations. They were also familiar with the test successes and failures and the interface functions among the elements. The success of the ad hoc technical audit suggests that this process should be expanded in support of future shuttle and space station activities.

Lessons Learned:

Independent technical assessments are of particular value during the Phase B and Phase C periods of a program, that is, during the definition, preliminary design and detailed design periods. The technical assessment groups are in fact the technical conscience of the program and focus on identifying problems for program resolution and/or can take on the role of trouble shooter and work the resolution of the problem. Both roles are acceptable. Given the potential workload for such groups, one of their real problems is the establishment of priorities. These groups or small task teams support the mainline review system (such as the flight readiness review process) but add additional "insurance" and confidence in the ability to meet performance and safety requirements.

Recommendations:

Technical audit groups should be considered by the Space Station program as soon as practical to assure technical soundness of the design as it moves through the final stages of Phase B and into Phase C/D. It might also be fitting to constitute such audit teams to assess routine processes and procedures for operating the Shuttle and suggest new approaches which could save costs without increasing hazards. Keep in mind the success of such ad hoc teams stem from the currency of their technical or operational experience, their total familiarity with the system and their lack of dedication to any routine reporting or documentation discipline.

3. The Funding Trap

Findings:

The funding and management philosophy that has characterized the Shuttle program since its inception makes it considerably more difficult to maintain a "safety-first" commitment than one would desire. The funding constraints under which the Space Shuttle Program operated led to a reliance on a highly "success-oriented" philosophy. This now appears to be the case for the Space Station Program and may be exacerbated through results from the Phase B design period as well as reorganization and change in roles and responsibilities.

Lessons Learned:

There is no escaping the fact that doing things right the first time takes both time and money. The corollary is that underfunding or overambition requiring doing "it right" afterwards takes even more resources.

Unrealistic budgets and schedules place an extraordinary burden on program managers to minimize testing and rely on less than optimal system designs, which can lead to increased acceptance of risks and eventually jeopardize safety.

Shuttle Program experience suggests the wisdom of not trying to compensate for lack of executive, congressional, and public support by designing a program where everything is supposed to work the first time it is tried.

Recommendations:

Beginning a major aerospace program without the appropriate national support and resources commitment in place should not be attempted.

"Build-to-cost" should imply that the program management will match performance and safety with the resources available on a realistic schedule. Such schedules can be set as "goals" which are achievable without being completely out-of-reach.

Program specifications and contractual arrangements should be so structured as to promote constant reassessments of the baseline system design, development of back-up designs, and avoidance of a single-minded focus on meeting stringent initial requirements which exceed that which is possible. Maintenance of alternative designs and adherence to rigorous testing should be pursued to assure mission success and safety.

4. Aggregate Risk

Findings:

In all of the Panel's work there is a common thread, and that is risk--its identification and assessment. However, the concern of everyone is what is the true aggregate risk and how is it measured? In some form it is the composite result of all the individual risks that are identified, weighted or quantified, and accepted. Any complex undertaking wherein design is divided into systems, interfaces, subsystems, components all of which are handled by different groups geographically dispersed, poses extreme difficulties for the coordination of the effect of engineering and procedural tradeoffs that are constantly being made. In the case of most NASA programs, large and small, the process is further complicated by the fact that not only technology, but money and schedule pressures also drive the tradeoffs.

Lessons Learned:

There are many methods of identifying a risk, but it can only be quantified as the result of a test program and actual flight. Hence, the importance of the test programs that NASA stresses. In a large and complex program, e.g., Space Shuttle and Space Station as well as single aircraft R&D programs, the amount of testing that could be undertaken can be so great that the testing philosophy must be constantly reviewed to make sure of its pertinency and necessity. The critical focus must be on making sure that all risks inherent in the mission environment are accounted for within a test program. The time and funds available must be variables, allowed to increase as needed. In an evaluation of the adequacy of the test program for risk assessment, the tendency is to propose an outside entity to take a "fresh" look. This is difficult for two reasons: first, the people making such an assessment must have been involved virtually from "day one" so that they know the entire history and *modus operandi* and, second, this should not be an *ad hoc* effort, but a continuing part of the Management System. The same problems exist within individual functional subsystems (electric power distribution, hydraulic power and effector use, etc.) where design efforts and external influences have been traded off over a long period of time. Judgement alone is an inadequate assessment tool.

Recommendation:

The capability and funds to do an "aggregate risk" are within NASA, but it should be a discrete responsibility. It cannot be done by the engineering organizations as a part-time effort. Indeed, it might be well to bring in outside help who have been involved in nuclear power plant risk analyses to provide expertise on how NASA should use its own expertise in both probability risk assessments and an overall aggregate risks assessment. It should not be construed as part of an "engineering design function." In brief, it is suggested that there should be a formal effort within the program (Space Shuttle, Space Station or any other critical program or project) to quantify the aggregate risk of the total system and the impact of the changes that occur to it.

5. Design Management

Findings:

A basic design concept and requirement derived therefrom does not relieve the engineer from being sure that proper attention is given to the impact of environmental or induced loads. The Challenger accident which revolved around the solid rocket motor joints, is to a degree, a replay of a similar problem on the Skylab program. From the beginning of the Skylab program a basic design concept and requirement was that the meteoroid shield be tight against the basic vehicle skin. It was clearly stated that the meteoroid shield was to be structurally integral with the S-IVB tank (which was the basic Skylab vehicle) which itself was well proven in many previous flights. The auxiliary tunnel frames, the controlled torque on the trunnion bolts and the rigging procedure itself were all specifically intended to keep the shield tight against the Skylab basic structure. However, just as with Challenger, the question of whether the shield would stay in place under the dynamics of flight was simply not considered in any coordinated manner. That is, the aerodynamic loads on the shield and its external pressure environment during the launch did not receive the attention and understanding during the design and review process which in retrospect it deserved. So it is with Space Shuttle hardware, both ground and flight.

Lessons Learned:

Personal communications through program specifications, engineering and management reviews, safety overview, and engineering day-to-day activities are often not as rigorous as expected. Management must always be alert to the potential of its systems and take care that attention to rigor, detail and thoroughness does not inject an undue emphasis on formalism, documentation, and visibility in detail. Such an emphasis can suppress the concerns of lower level individuals and dismiss the value of the insights of an intuitive engineer or analyst. It is important to achieve a cross-fertilization and broadened experience of engineers and management to better understand the

interfaces between requirements (specifications) and hardware and software and the mission environment.

Recommendation:

Comprehensive configuration management implemented early is essential for any program, and particularly for one with complex interfaces and a variety of hardware and documentation sources. Positive steps must always be taken to assure that engineers become familiar with actual hardware, develop an intuitive understanding of computer-developed results, and make productive use of ground test and flight data in their continuing learning process, which to a degree begins anew for each new program.

An effective design review must emphasize hardware, but should also include the review of hardware impacts resulting from ambient conditions and mission-developed loads. Not only design personnel, but test and operations representatives should participate in design reviews.

6. Problem Reporting and Corrective Action System For Ground Support Equipment

Findings:

Data collection systems generally are utilized by management to identify: (1) problem areas; (2) need for modification/updates to equipment; (3) increased manpower or different skill levels; and (4) effectiveness of, or lack of, adequate supply support. Apparently none of this can be accomplished using the available PRACA data (or related system's data) at the KSC site. Across-the-board NSTS Safety data flow apparently does not currently exist that will rapidly and efficiently exchange information on documented hazards. Present information exchanges are accomplished by teleconference, datafax, mail, and through meeting minutes.

Lesson Learned:

In order to use problem and safety data by both management and working levels for design, test and decision-making there needs to be (1) an education program to assure proper data is prepared and presented to the "system" by all organizations (government and contractor) involved in the Shuttle Program and the Space Station Program, and (2) use of current technology, in this case computer data bases and transmission systems, is mandatory. Such programs can have a generic foundation that would be applicable to any program, large or small, now and in the future.

Recommendation:

First an education program should be initiated so that "all hands" the importance of an adequate, timely data collection and

assessment system followed by an orderly and timely distribution system. In the Space Station Program the TMIS (Technical Management Information System) could most likely serve in this capacity. To achieve the near real-time exchange of information which is required by users at all NASA Centers and appropriate contractors, there must be compatible software and hardware at all sites. Funding is a problem.

7. Achieving Adequate Safety Levels

Findings:

(1) Semantics is a significant factor in personal and organizational communications, which in turn affects the management and finally the success of a program. This was adequately demonstrated during the Presidential Commission hearings and as noted during many of the Panel's own activities. Attempts continue to be made to eliminate ambiguity of words and expressions used in the material which form the basis to accept or reject risks associated with Space Shuttle (and other) missions. The term "safety" is only one example. Risk Management is a more realistic term than safety. It implies that hazards are ever present, must be identified, analyzed and controlled or rationally accepted. It gets away from the "motherhood" ambiguity of safety: freedom from danger, a condition which rarely, if ever, exists. Acronyms which in many cases are used for two or more definitions. For example: "PCU" which stands for payload checkout unit, power control unit, pressure control unit, process control unit.

(2) The Shuttle/Centaur program, now cancelled, can provide additional insight or "lessons learned" that should not be lost to ongoing and future programs. Shuttle/Centaur was a program that had "a little bit of everything." For example, it started-stopped-started, went from an STS element to a payload, was greatly time and resource bounded, attempted to use "tried and true" or "off-the shelf" hardware with "minium changes," and other attributes which could be said to cover almost any management/safety condition to be experienced in the future.

(3) Actions speak louder than words: NASA places a great deal of emphasis on communications between employee, supervisor and upper levels of management, however, there appears to be a reticence on the part of many employees to speak up. Why? Because either they feel that they have not been "heard" before or that they will be considered "trouble-makers" by the next higher or greater levels of supervisions/management.

(4) When facilities and/or hardware are upgraded there are new possibilities of failure introduced which are not fully appreciated or understood at the time. A case in point, when the Mixing Facility at Morton Thiokol, Wasatch, Utah, was upgraded with a programmable controller, new possibilities of failure were introduced. A complete failure modes and effects analysis (FMEA)

should have been conducted not only on the mixer facilities, but also on all other hazardous operations to preclude the possibility of component failure or other failure modes from causing an impact on safety . . . lightning strikes should have been considered and were not.

(5) Hardware designs versus how they are used . . . when the payload bay access platforms in the Orbiter Processing Facility (OPF) at Kennedy Space Center (KSC) were designed, it was assumed that personnel operating them would be familiar with appropriate KSC and OSHA standards. However, at the time of the accident which resulted in the improper actuation of the access platforms and their subsequently damaging the Orbiter (March 8, 1985) most of the several hundred personnel who were certified to operate the platforms did so only incidentally to their primary duties.

(6) The view that product quality improvement and cost control are separate and conflicting goals exists in various areas within NASA and its contractors.

(7) Separating and defining "safety," "reliability," and "quality assurance" is a continuous management problem and often a working misconception for those involved. These are related disciplines, but are different and even unique unto themselves. Added to this problem are the associated activities of configuration management, interface control, and logistics which are inexoriably linked to "S,R&QA." It is the "lumping" together of these important management and engineering disciplines that leads to misunderstandings and possibly letting things "fall through the crack" thereby adversely affecting the goal of safe and successful missions.

Lessons Learned:

Lessons learned from the above findings are numerous and will be provided in a single narrative fashion.

The semantics involved with safety, reliability, and quality assurance leads to a great deal of misunderstanding and loss in effectiveness of the resources applied. Finding (1) is both the lesson learned and recommendation all combined. With regard to the specific meanings applied to safety, reliability and quality assurance, finding (7) above, the following may help:

Safety/Safe: For the Panel, safety is a judgement of the acceptability of risk, and risk, in turn, is a measure of the probability and the severity of damage to equipment and personnel resulting from failures or improper operations. Something is "safe" if its attendant risks are judged to be acceptable. "Systems Safety" encompasses a total view of all elements of a system which may include ground and flight aspects.

Reliability: This is a field of engineering with its own methodology derived from the basic sciences of statistics,

mathematics, physics and chemistry. It is an activity that deals with the frequency of failures to operate as specified and includes:

- o design criteria to meet reliability criteria
- o conduct of failure modes and effect analyses (FMEA's) definition of critical items, conduct of fault tree analyses to define hazards and general areas of concern,
- o interfaces directly with quality assurance and manufacturing process to provide "product assurance."

Quality Assurance: This is closely linked with configuration management and manufacturing activities which in turn provides the hardware and software that has been specified and designed to meet specific program requirements. It is, in some aspects, highly people-intensive since it deals directly with the hardware and software development, manufacture and installation. Its purpose is not to engineer but to control and assure. QA provides certified documentation that hardware and software have been produced to the exact designs (configuration control).

Although there is a tremendous interest in employee motivation and this is a vital part of achieving safety goals there is often a lack of communication. If there are numerous "memos for the record," which record an individual's feelings, then they generally are loath to bring such items to the attention of higher levels of supervision and/or management. Designers, procedures writers, safety auditors can not rely on the operators of equipment to implement their requirements on a continuous basis especially when new personnel are being added to the work cadre. Training and more training and expounding on the use of "common sense" becomes a necessity.

Recommendations:

o Communications must be open, continuous and in sufficient detail so as to ensure nothing required to safely get the job done is missed. Reviews by themselves, for example, are not enough. Personnel must feel that their views are wanted and that they will receive objective consideration. Telecons are fine, but they require a conscious effort to assure that everyone on the network is given the opportunity to partake.

o Terms used must be fully understood by all those on the project so nothing is lost in possible "translations." Uniformity of language across a sophisticated and geographically diverse program is mandatory.

o There are two major and complementary activities in the development of complex hardware. One is the production of the desired output and the other the identification of uncertainties

and the assessment of the associated risk. The two require different mental attitudes. At the operating levels results are most objective and complete if carried out by different groups supporting and complementing each other. At decisionmaking, the availability of two points of view of comparable competence, one focused on performance and the other on risk, is likely to prove of considerable value. It can be broadly said that the desire to complete a design makes it difficult to be objective about what may be wrong with it.

8. Designated Engineering/Quality Representatives

Findings:

The FAA practice of designating private-sector (contractor) individuals to act for it in certifying compliance with FAA regulations is followed by NASA in many non-critical hardware areas. NASA's contractors using such an arrangement call these personnel "Designated Engineering Representatives" (DER's). There has been some criticism of the DER system in which a "conflict of interest" is the general citation. The National Academy of Engineering/Science's National Research Council conducted a thorough examination of the FAA system and concluded that the DER system did not lack integrity. Further, in most instances there is no good alternative since the quality assurance (certification) functions are so numerous that they can not be managed or staffed by NASA and other government agencies.

Lessons Learned:

It is practical to use a DER arrangement, but it must be carefully planned to assure that only non-critical operations are conducted. Further, the personnel selected as DER's must be experienced, trained and properly motivated by both NASA and contractors.

Recommendation:

Continue this process as currently constituted. However, during the STS "downtime" period every effort should be made to maintain the high level of DER achieved prior to the Challenger accident. This may be difficult with a reduction-in-force now in process with the anticipated increase-in-force to come within a year's time. Plan ahead!

B. Ground Equipment and Facilities

1. General

Findings:

The KSC Uninterruptable Power Supply "(UPS)" failed a number of times causing delays in processing of flight equipment and affected the pressing workload leading to the "next" mission.

Failure of the Orbiter Processing Facility work stands inflicted damage to the inside of the Orbiter. Spillage of hypergolics affected Orbiter tile adhesive (RTV-Room Temperature Vulcanizing material) as has the use of supposedly "better" tile waterproofing materials.

Lessons Learned:

Ground Support Equipment and other ground facilities do not depend upon minimizing weight as does flight equipment, but the impact of cutting corners can be as severe as in-flight equipment. Causes of such failures as noted above were usually combinations of design deficiencies, operating procedures omissions, lack of auditing by the appropriate NASA and contractor organizations, and lack of personnel training. These types of problems will always be with us, but they can be minimized.

Recommendations:

Each of the lessons learned has to be treated by management. The old saw of "pay attention to the little things and the big ones will take care of themselves" is appropos. There is no desire here to give generic recommendations.

2. Welding

Findings:

Problems associated with welding apply to both ground and flight hardware, to both critical and non-critical areas. It is a past, present and future concern. A number of examples make this clear:

o The temperature sensor installation on the liquid oxygen interface between the launch pad tail service mast and the orbiter's main propulsion system ducting. This sensor's weldment failed causing the sensor pieces to enter the orbiter system and prevent closure of a critical orbiter value. Weld was found to be faulty.

o Weldments at Vandenberg Launch Site came under criticism causing the USAF Inspector General to conduct a thorough investigation. Apparently there were several thousand welds that had to be corrected.

Lessons Learned:

Welding technology, inspection procedures, personnel training continue to be a problem when viewed in the light of the millions of welds made on ground support equipment and facilities at many NASA and contractor sites and the criticality of many of those welds.

Recommendation:

For any continuing problem with a continuing process, such as welding, the tried and true approach of constant auditing of the personnel certification and work site activities is mandatory. Management is aware of this and the quality assurance agency at every site must do its own job and not assume "all is right with the welding."

3. Hoist Systems

Findings:

Single failure points exist on many of the major hoist systems at both KSC and VLS. These hoists are used to handle and move sophisticated and sometimes potentially dangerous hardware such as the Orbiter, the Solid Rocket Booster segments, and so on. In most cases waivers have been requested and granted, and in fact these have become deviations (not temporary as a waiver but permanant) to the specifications. JSC-07700, Volume X, paragraph 3.5.1.2.1.1 requires all ground support equipment to be designed to fail safe.

Lessons Learned:

Equipment is designed and manufactured without due regard of the environment in which the hoists will be working nor with the critical type of hardware involved. Much of this cannot be helped because equipment is not manufactured specifically for NASA's use, but must be modified to meet NASA's requirements. Waiving or accepting single failure points requires greater attention from management and the quality assurance/safety personnel.

Recommendations:

With known requirements it should be incumbant upon the KSC and VLS users to eliminate as many single failure points through very early knowledge of requirements and procurement actions. As with any other equipment, FMEA's and resultant critical items should be defined, hazards noted and a final risk assessment made. The risk assessment must include and be dependent upon impacts to the critical hardware that will interface with the hoist systems.

4. Procedures

Findings:

o The Presidential Commission investigating the Challenger accident noted, as has the Aerospace Safety Advisory Panel, that there have been numerous procedure violations, procedure deficiencies, and personnel training concerns associated with preparations for launching of the Space Shuttle. Examples

include the November 1985 handling incident with the Solid Rocket Booster, the access platform accident in the Orbiter Processing Facility, an inadequate GSE maintenance plan.

o Incremental delivery of Orbiter and payload integration modification kits has been a problem since the beginning of the STS program. There does not appear to be an orderly or timely system in place to identify to management the underlying causes of hardware delays and engineering data thoroughness and the resultant constraints for field operations.

o There is a lack of pre-developed trouble shooting procedures for critical (time) operations and associated ground support equipment which results in expending more resources in an inefficient manner. This affects serial-type operations at KSC.

o The STS-2 oxidizer (N_2O_4) leak mishap at LC-39A indicated the crew was conditioned to expect only a small leak by the history of having no major leaks (similar to Dr. Feynman's discussion about the solid rocket field joint in the Presidential Commission's report). There was a "mind-set" to avoid stopping the hypergol loading operation even though leak source and magnitude should have been identified visually. Emergency procedures were not adequate and there was a lack of crew familiarization with both the equipment and procedures.

Lessons Learned:

o It pays to go back and identify previous "lessons learned" and determine whether they have been incorporated into the current procedures. It is natural to see the level of attention paid to procedures to attentuate with time and repetition of the working procedure. A paper system by itself is, therefore, ineffective without continuous management and hands-on personnel attention and training.

o A computerized system is necessary to aid management in identifying, in a timely manner, problems and delays in the causes of hardware delivery problems and lack of sufficient engineering drawings/procedures to accomplish the many modifications made to flight hardware at the launch site.

o The lack of pre-developed trouble shooting procedures require the personnel on station to resolve the problem. This results in expended manhours to redocument trouble shooting, removal and replacement and retest procedures.

o There should be a single program wide identification or control number for changes. The present system has as many as three different control numbers for, say, a single Orbiter change. If the same change involves payload integration and KSC facilities, additional control numbers are assigned that differ from the Orbiter number. This practice results in many wasted resources involved in authorizing, identifying, distributing,

statusing, tracking and closing the same basic change.

o Two safety controlled activities have a substantial impact on processing times of flight and ground equipment. The first one is the designation of areas to be cleared for hazardous operations, and the second is the requirement for protective clothing (that is, escape suits, splash suits, Scott-Packs or face shields). Establishing the size of the area to be cleared and the protective clothing to be worn was based primarily on past experience of the personnel in charge. With experience gained, the requirements became less stringent and operational timelines improved. However, no data base is presently in existence or planned that would document the types of hazardous operations, the clearance, or clothing requirements, along with the yardsticks that formed the basis for these requirements. An exception to this is the Hypergolic Servicing Building.

Recommendations:

o A library and retrieval system should be developed that is readily available for NASA and non-NASA users. Lessons learned should be included in training courses and made a part of any significant contract in the future. Use of lessons learned as well as keeping a "running-log" of new lessons requires constant shoring-up by various motivational means.

o Pre-developed systems to aid management in identifying problems and developing resolutions should be instituted as soon as possible. Such computerized and manual feed programs may already be available and could be adapted to NASA use. For example, the FAA uses the Aviation Safety Analysis System which scans maintenance records to determine potentially dangerous trends. Further, field and hands-on personnel should be required to document and report periodically on the effectiveness of trouble-shooting procedures, hazard/problem identification procedures, and maintenance management.

o A single program-wide identification or control number for changes. The present system allows too many different numbers to be applied for a single orbiter change.

o Provide a computer base that shows the distances that must be cleared for hazardous operations, and the data that these distances are based upon (PPM levels of toxic materials or TNT equivalents of pressure vessels). List all the incidents/accidents during hazardous operations that verify or contradict the clearance on protective equipment requirements. This is not unlike the above mentioned library and retrieval systems for lessons learned.

5. Integrated Design and Modification Concerns

Findings:

There are a number of flight equipment design areas that affect ground operations and require better communications between ground and flight design and operations personnel. For example: Space Shuttle elements (Orbiter, Space Shuttle Main Engine, External Tank, Solid Rocket Booster) owing to weight and cost consciousness reduced the requirement for "ease of maintenance" which was originally a major driving force in the flight hardware design. This reduction in ease of maintenance resulted in increased resources being applied to KSC turnaround activities and has often adversely affected adjacent or peripheral hardware when hardware repair, replacement, checkout were and are required. A simple example is the breaking of electrical lines when "tramping around" in the Orbiter fuselage to remove and replace equipment. An example of a properly design item for ease of maintenance is the light-weight SSME heat shields which are segmented allowing easy removal and replacement without disturbing other hardware.

Lessons Learned:

Turnaround time reduction requires further advances in the ability of the technicians and engineers to troubleshoot ground and flight hardware and software.

Improper design, that is, not paying attention to the day-to-day operations needed to maintain flight hardware results in the need to design and fabricate special access devices and protective covers in areas that experience heavy personnel traffic. Furtner, it also means additional training of ground personnel to deal with hard to maintain hardware. Examples: design crew compartment panels such that they can be individually installed and removed, that is, it should not be necessary to remove adjacent panels or even impact them; wherever possible, standardize equipment which also helps the "sparing" requirements.

Electric and electronic boxes and cabling should have connectors designed to assure elimination of bent pins and proper keying of the connectors themselves.

Engineering/drawing change control and release system should be designed for the long range user and not the one-time designer/builder. The biggest problems today on Orbiter change control/modification incorporation are the result of the inflexibility of an engineering drawing system which has "evolved" from a production operations system to one that "happens" to cover field site modifications.

Recommendations:

o Weight and cost consciousness weakened the move toward building maintainability into the Orbiter. Maintainability, on future programs, must have its priority upgraded. Use of standard industry hardware where possible rather than unique

hardware since unique hardware limits the availability of spares and drives up the cost.

o Essential functions need to be completely independent of other functions and sub-systems (true maintainability/access) to reduce interfaces/interactions.

o Design protective (GSE) covers for exposed wiring and tubing runs at the time the original equipment is designed.

o Maintenance procedures should be programmed into a data base that would include trouble shooting and retest procedures for all sub-systems. Develop standard procedures across all sub-systems for maintenance and retest.

o Provide a defined maintainability design criteria at the inception of the program and a strong design review board to monitor adherence to these criteria.

o Future electronic/electric systems should have connector designs which eliminate bent pins and incorrect keying. Orbital replacement units cannot afford the luxury of down-time on this recurring problem.

C. Flight Hardware and Software

1. Welding

Findings:

The welding process, including inspection and correction, remains, to a great degree, an "art." The NASA Centers and their contractors continue to place great emphasis on welding techniques, personnel training and certification, and materials characterization. Of particular interest has been the weldments on the Space Shuttle Main Engine components such as the heat exchanger in the LOX side of the engine, and the large welds on the External Tank, and the Orbiter crew compartment welding. In the case of the SSME there are numerous areas that are extremely difficult to reach and can not be seen, which adds to the inspection problems. Robotic welders are being installed at the Rocketdyne facility's Turbopump Center and should reduce welding problems. In the case of the Orbiter, there have been delays as a result of difficulties in the weld rework of the canopy assembly where rework welds were resulting in additional cracks. The orbiter welding is forced to be done, in some instances, in a discontinuous manner. There have also been times that weld-rod mixups have occurred thereby using incorrect materials. In some instances difficult welds are being reinforced by means of nickel plating (Electrical Deposited Nickel, EdNi).

Lessons Learned:

A major point is: designers and manufacturing personnel do

not recognize, early enough, the difficulties to be encountered when doing assembly welding and repair welding. The "art" part of welding is underestimated. The ability to inspect many welds through non-destructive evaluation (NDE) is very limited.

Recommendations:

Continued support is required for both NASA and contractor research and development of welding methodology, welding materials and training associated with both welding and NDE operations. Hardware requiring weldments must be examined as early as possible in the design and development process to minimize adverse effects during manufacturing and flight use. Spending "up front" resources can save a great deal of resources and time during downstream activities.

2. Instrumentation

Findings:

Instrumentation which includes the sensors, transmission and distribution lines (if needed), readout devices and installation hardware are mandatory as both developmental and operational entities. There have been good and bad instrumentation experiences and those that have generic use are noted here:

o Instrumentation failures have occurred on every flight of the Space Shuttle. They have affected each of the Shuttle elements (Orbiter, External Tank, Solid Rocket Boosters, SSME's, ground launch system) and cargo carried in the payload bay. This has resulted in redesign of the instrumentation itself, reevaluation of the redlines used to define allowable operational boundaries, reevaluation of launch constraints, sensor voting systems and philosophy have come under review and modification, the location and numbers of sensors have been analyzed and modified. An idea of the problems or anomalies encountered during the past year are indicated by the following:

- Orbiter Auxiliary Power Unit #1 (APU #1) exhaust gas temperature number 1 sensor failed "low" just after the APU was shut down after ascent. The sensor was removed and examined and indicated an internal wire shorted. Occurred on STS 51-D.

- On STS 51-J the APU #1 gas generator valve module temperature failed during ascent with an off-scale low reading and followed by intermittent low readings. The measurement was intermittent and had been waived prior to the flight because a backup measurement was available. Troubleshooting isolated the failure to a bad wire splice.

- On STS 51-J, SSME #2 liquid hydrogen inlet temperature sensor failed off-scale high at T+235 seconds. Troubleshooting determined that the instrumentation transducer failed. This measurement was not required for launch commit criteria.

- On STS 51-B, SSME #2 gaseous hydrogen outlet pressure sensor failed off-scale high shortly before main engine cutoff. This same measurement had failed on a number of previous flights. A redesigned sensor was built and installed on all Orbiters and there were a few additional failures. The failures were tracked to wire problems.

- Orbiter smoke detector/alarm systems have experienced false alarms (STS 61-A). During the mission the crew, after the alarms sounded, could not isolate the cause. The smoke concentration output of all sensors remained at the normal background level which is well below the alarm trip point. Analysis of the flight data showed that there were five (5) alarms caused by the smoke detector #B in the avionics Bay #3. Since the redundant avionics bay smoke detector was operable, the 3B smoke detector was powered down for the remainder of the flight to prevent additional erroneous smoke alarms. A similar problem, which occurred on STS-3, was caused by contamination by loose gold particle in the large scale integrated circuit chip. There was no final determination of "why" the false alarms on 61-A.

- Investigation and analysis of the erratic Alpha Gimbal temperature measurement experienced on the Ku-band Deploy Assembly showed that a broken wire, due to flexing of such soft wire (26-agauge) at the connector interface. Flexing of such soft wire (copper) occurred during assembly and disassembly, not during use. It was noted that loss of either the "Alpha Encoder" or the "Gimbal Lock Sequencing switch" operation would represent a serious flight problem and could require the crew to jettison the deploy assembly in orbit.

o There were a number of "pluses" found in the instrumentation area which included:

- Accessibility to the instrumentation components was very good in such areas as the Dedicated Signal Conditioners, Multiplexer/Demultiplexers, Pulse Code Modulators, and the Payload Data Interleaver. All of these made it easier to assure proper working of the instrumentation system associated with these items.

- In some of the instrumentation three areas have been stressed: commonality, standardization, and self-diagnosis. Commonality and standardization provide designs that allow the sensors to fall within narrow calibration bands and thereby permit replacement without the necessity to update the sensor calibration curve data base. Self-diagnosis refers to having built-in testing equipment and fault detection methods. All of the above have led to some modularization of the instrumentation systems in some areas.

Lessons Learned:

o Flight instrumentation is one very important key to safe, successful flight, but usually does not receive the same degree of attention nor confidence that the hardware, whose state it monitors, enjoys.

o Instrumentation systems provide the operator with data and bounds (launch constraints, red line limits, voting systems to continue or shut-down systems, etc.) and when failures or anomalies occur the instrumentation systems provide the clues if not the reasons for hardware and software failures/anomalies. Without such sensors it is often difficult, if not impossible, to make modifications to enhance the safety of operations.

o Shuttle failures (SRM joints), Delta rockets, Titan rockets, Interum Upper Stage failures have been difficult if not impossible to determine because of the lack of instrumentation.

o Incipient failures and trends during test and flight depend upon the extent of instrumentation. This should be factored into the overall test and development programs so that the proper resources can be provided and applied in this area.

o NASA does not appear to have any particular emphasis on instrumentation design or standards, just that a false shutdown of good equipment should not occur as a result of instrumentation failure . . . more than that is needed.

Recommendations:

o NASA and its contractors should apply additional resources to match the flight vehicle (STS, Space Station, other) requirements with the appropriate instrumentation systems. This includes reliable, well-built sensors and transducers to meet the environmental demands under which they must work. This applies particularly to the SSME's and the Orbiter 102 which is to act as an extended R&D vehicle. There are many other programs and projects within NASA's purview that require better instruments as well . . . particularly the upcoming X-Wing vehicle.

o NASA needs to have a coordinated approach to:

- Instrumentation standards
- Instrumentation design
- Instrumentation logistics (spares, repair, etc.)

o Perhaps NASA should have a "Center of Excellence" for instrumentation . . . possibly LaRC.

3. Undersized Wiring and Cable Design

Findings:

There have been a number of areas in the Orbiter and the Solid Rocket Booster where "undersized wire" gauges have been used. Undersized refers to wire with little or no margin to conduct the electrical current required or its susceptibility to damage and/or breaking as a result of physical abuse. In most cases the wire gauge #2 has been designated as "undersized." Waivers have been approved relating to the NASA Standard JSCM 8080 (and others). Such waivers are extended from flight to flight when in fact the change to a large diameter wire might be practical and safer. This concern appears periodically over the past twenty years or more, since Apollo days. The usual wire gauge used for many instrument systems is #26, but the minimum for nearly all other uses is #22.

Lesson Learned:

Undersized wires are used to reduce "copper" weight but are susceptible to damage from normal vibration and movement as well as from impacts by personnel, and if an electrical short does occur the wire overheating can readily supply the energy or ignition sources to start a fire. This remains as a continuing concern which merits continued attention.

Recommendation:

Analyses must be made to assure that the use of undersized wire can NOT be the cause of shorting and a point of ignition within the hardware in which it is used. Designers and system safety engineers should pay close attention to the use of smaller gauge wire and if necessary the specifications or requirements documents should either be adhered to or changed. Waivers are a safety concern.

4. Hardware Contamination

Findings:

Contamination refers to a broad spectrum of undesireable elements that degrade or prevent the proper operation of hardware. Contaminants can be synthetics, metals, organic or inorganic particles or coatings. Some examples will indicate the breadth of this present concern:

o The presence of "black polymides" was found in the main propulsion lines of the Orbiter. The exact cause or originating site of these particles has not been determined, but it is believed to be the "scrappings" from the LOX and LH_2 detent rollers on prevalves. The contamination would appear to result from "wearing in" of these rollers with use of the valves when they are newly installed. They were replaced with new detent roller assemblies using a "better" material and contoured to the shape assumed by the "worn in" roller. In addition better inspection procedures and non-destructive evaluation methods are being used.

o There is a potential failure of the rotary switch located on crew compartment panel F9 as the result of contamination which can occur in the switch. Such an occurrence could short one or more of the orbiter AC busses causing transients which could be catastrophic to the Main Engine Controllers. All three AC busses are routed to this switch through a common connector and are protected by three 3 amp fuses each. The fuse-blow characteristics of the 3 amp fuses are such that AC transients could exceed 30 milliseconds allowing more that sufficient time for these transients to cause engine shutdown. It was decided that 0.5 amp fuses would be adequate for protection of the circuits and that they would not blow with normal AC bus transients and would eliminate the SSME controller problem.

o Hydraulic system contamination within Orbiter actuator servo control valve units and within the SSME actuators have been the cause of problems while the vehicle has been sitting on the launch pad. Delays and an abort were attributed to such hydraulic fluid contamination. Investigations showed that:

- The Orbiter hydraulic system(s), including those interfacing with GSE, are an order of magnitude cleaner than commercial or military aircraft, and generally exceed the Orbiter specifications themselves. HOWEVER, this apparently does not mean that the exisiting cleanliness requirements have been adequate, particularly when considering the SSME servo control valve's sensitivity to contamination (metal tolerances of one part in 100,000). Contamination Level Comparisons are shown in chart #1 on the next page.

- There has been no evidence of "silting" in any of the Orbiter hydraulic systems based on the analysis of all fluid samples taken from various Orbiters.

- There are criticality 1 items (failures of these are catastrophic) related to hydraulic contamination failure modes. Hydraulic supported subsystems have had a history of problems attributed to "transient hydraulic contamination." Chart #2 shows the number of criticality 1 items for which contamination has been identified as a potential failure mode on the Space Shuttle. Transient hydraulic contamination (intermittent) has been the most probable cause for problems/failures in the: Orbiter/8; SSME control valves/6; SRB thrust vector control valves/2.

Lessons Learned:

Contamination (particles, corrosion, etc.) are little things that speak softly and cause very large problems. Minute particles, molecular changes in materials can result in anomalous operations, failures, fires and worse. Usually a specific out of the ordinary event triggers a resolution of the problem rather than alleviating the problem by design, quality control, test, or operational procedures. Specific problems include: shorting of

CHART #1

CONTAMINATION LEVEL COMPARISONS

PARTICLE SIZE MICRONS	ORBITER SPECIFICATION GSE INFLOW	GSE OUT	MIL SPEC AIRCRAFT	BRAYCO HYD. FLUID UNFILTERED, ACTUAL	TAP WATER
5 - 15	19,331	36,200	87,000	877	1467
16 - 25	2,373	4,443	21,400	216	200
26 - 50	860	1,612	3,130	107	44
51 - 100	124	232	430	79	28
101 - and up	13	24	41	31	18

(JSC Shuttle Requirements SE-S-0073

CHART #2

NUMBER OF CRITICALITY 1 ITEMS FOR WHICH CONTAMINATION HAS BEEN IDENIFIED AS A POTENTIAL FAILURE MODE

SUBSYSTEM	MPS TVC ACTUATORS	STB TVC ACTUATORS	AERO ACTUATORS	BRAKES	NWS	SSME VLV ACTUATORS	HYD S/ COMP'NT
No.of crit 1 CIL items	4	4	7	2	0	1	0

MPS/SRB ACTUATOR

1. Stuck Power Spool
2. Clogged Filter Element
3. Stuck Lock Vlv
4. Closed Check Valve

AERO ACTUATORS

1. Stuck Power Spool Elevon
2. Stuck Power Spool Rud/SBk PDU
3. Jammed Body Flap Control Valve
4. Clogged PDU Filter Rud/SBk
5. Clogged Elevon Filter
6. Plugged Orifice Body Flap
7. Closed Check Valve Elevons

BRAKES

1. Brake/Skid Control Valve Jammed Open
2. Locked Switch Valve

SSME VLV ACT.

1. OPOV Valve failed

electrical and electronic components including computer circuits, cause of incomplete mechanical action as in valves and solenoids, fire/detonation in oxygen environments, detonation in hypergolic fuel systems, failure to seal close-tolerance joints, scouring and breakage of mating rotating parts, incomplete solder and weld joints.

Studies appear to indicate that hydraulic fluid cleanliness is NOT the issue but rather that component contamination (either self-generated or built-in) is the most likely cause of the problem. Vehicle experience at KSC and failure reports returned from the vendors tend to agree that the problem is within the components themselves.

Recommendations:

Designers, reliability engineers and safety engineers must give special attention to critical components with very close tolerances, components and systems that are difficult to clean and inspect, and proper placement of filters to alleviate the special problems caused by contaminants. The practical side of hardware operations which include the human side of the equation and how this can affect the degree of contaminates getting into a critical system. Redundancy will not increase reliability of the hardware if the above are not a part of the design, development and operational aspects of the program. Fluid filters then are not the only answer, but cleanliness of the finished and operating hardware. And last, but not least, it is best to NOT use Swiss watch tolerances for locomotive sized hardware.

5. Software/Computers

Findings:

o GAO activities provided the following information regarding software for aerospace programs: (Approximate numbers)

- 50% of contracts had cost overruns
- 60% had schedule overruns
- 45% of contracted software could not be used
- 19% of contracted software had to be reworked before use
- 29% of contracted software was never delivered
- 3% of contracted software had to be modified before use
- 2% of contracted software was useable as delivered

o Every attempt was made to standardize the design of

Orbiter software through the use of a common language (HAL/S) and the early development of a hierarchial system of standards and specifications. This attempt was only partially successful for several reasons. The most important reason was that the hardware and software design cycles came together quite late in the program. As a result, the software design was revised to be compatible with the hardware -- and, in some cases, supplier software -- and was not able to utilize many hardware built-in diagnostic and monitoring features, other reasons were:

- Early software operating system design used assembler language.

- Not all software designers were required to comply with common standards.

- Special test requirements needed special software.

o Orbiter software is modularized, but it is embedded in a relatively fixed structure. Some concepts, such as separate payload communications and data links are feasible and could be initiated.

o Both Orbiter and launch process software have had available only limited sets of memory configurations and telemetry formats which are capable of being run simultaneously. This was the result of restricted computer memory and restricted instrumentation data. Enhanced (really new) computers based on the USAF B-1 bomber types have been developed and are now in the final stages of certification for use on the Orbiter. These new computer systems have cut the weight in half, reduced the electrical power to one-half the wattage, have doubled the memory capability, and reduced the configuration envelope to about 70% of that for current orbiter computers.

Lessons Learned:

o Software specifications and the resulting contracts with software developers require greater understanding of the hardware interfaces and computer system capabilities early in the evolution of flight and ground software than has been exercised in the past.

o Real-life schedules and expectations must be set at the beginning of any program using expansive and expensive software to reduce the cost overruns, schedule delays, and particularly the inability to use delivered software. There is no point in being overly optimistic when the software programs are often used to make up for hardware deficiences.

o Although software maintainability is different from hardware maintainability in that software code does not wear out, tapes and disks do wear out. However, masters are retained from which new work copies are made. Software maintainability, then,

is measured by the time required to correct design errors, modify code, incorporate requirements changes and restore full operations of the software/hardware system.

o Individual sub-routines, modules and packages should be isolatable and reinstallable with total transparency so algorithms can be corrected, improved, or changed without bulk processing.

o Ground and flight software should employ compatible languages.

o Hardware and software development should be married during development of detailed design specifications so as to be without compromising basic design concepts.

Recommendations:

o Procurement of computers and development of software programs should not be undertaken until:

- There is a thorough review of the failure histories of prior used computers and software "glitches" to ensure that these same type of problems are understood (root causes) and that they are not introduced into the new-generation computers and software.

- Perform hardware and software detailed design as an integrated activity at the earliest opportunity.

- Maintain very close contact between NASA and the prime contractors involved in the major hardware and software . . . including systems engineering and integration contractors where used.

- Assess system architecture for impact on life cycle costs as well as for initial development costs.

- Management must understand that while the capabilities of the computer appear to be limitless there are some constraints to their use: they do not solve problems through the use of reasoning, systems are limited by the data supplied by man, and are incapable of manipulating this data in any way which it is not programmed to do.

6. Payloads and Upper Stage Propulsion Systems

Findings:

Payloads consist not only of the actual hardware to be delivered to low or high earth orbit but also the mission kit hardware which permits physical and functional accommodation of the cargo into the Orbiter Payload Bay. This is true of the upper propulsion stages (e.g., Payload Assist Modules, Inertial

Upper Stages, etc.) that are often used to place satellites in geosynchronous orbits or to place planetary vehicles on their way into space. Payload adjuncts include special software, fluid lines, attach systems, deploy systems, instrumentation, thermal protection, vehicle attitude requirements, and so on. Some items of note include the following:

o One of the significant factors that affects launch processing turnaround times is the lack of standardization between the many different payloads and the Orbiter. There are "difficult" payloads such as the Spacelab which require unique procedures, processing and interface hardware and software, and there are the "simpler" payloads such as communications satellites that are linked to Payload Assist Modules (PAM's).

o Integrating the payload into the bay often times takes unique patch panel configurations which are separately defined for each flight and therefore require relocation of the patch cabling. The longeron and keel bridges for each of the twelve Orbiter payload bays are unique, resulting in high usage of some bridges and little usage of others. Should a particular bridge be out of order or out of service, the lack of interchangeability could potentially impact vehicle processing or launch.

o Major problems have occurred when having to reconfigure cooling ducts and the payload ground handling mechanisms. Thus hardware and procedures must match. A typical example is cable connections which are located on the underside of the payload's wire tray interface panels. This requires loosening of the panels from the trays, removal of the panel shroud from the vehicle underside, connecting and routing the new cables and reversing the procedure for installation. In some cases, in order to route, secure and connect cables, thermal blankets must be removed and reinstalled, thus adding many manhours to the otherwise straightforward operation. This is particularly true in the aft flight deck where space limitations make it very difficult to get "hands-on" the hardware.

o Frequently there have been interfaces that prevent installation to the design drawings in use. For example, while using the payload ground handling mechanism, technicians must frequently work off a narrow extendable access platform as high as 65 feet above the floor. This situation is compounded by special payload requirements to access non-standard interface locations such as vertically installed side-mounted payloads or late change-out of hardware . . . some of which can be out of "range" of the access platform as designed. This was apparently the case with the Earth Observatory Satellite (EOS-1) filters.

Lessons Learned:

o There will always be some peculiar requirements for special payloads and resource allocations and schedules must be arranged to accommodate such requirements. Because of this the

installation and checkout procedures must be carefully prepared to preclude complacency on the part of the installation and checkout personnel.

o Payload integration personnel should be represented on all change control boards (CCB's) and where necessary the payload user should be made aware as soon as possible of changes that affect their interfaces.

o Ground Support facility and GSE designers should have the maximum information to properly design access to the payload to Orbiter interfaces, the use of hand tools and shop-aids should be certified and entered into the procedures once determined that their need is pointed out.

Recommendations:

Standardization between payloads and the GSE, ground facilities and the flight supporting equipment should be a design requirement for NASA and its customers. During the mission the payloads requiring EVA must also be designed to accommodate such EVA's. Installation of payloads into the Orbiter again should be made easier by looking into reliability of key components on both sides of the interface so that repairs and modification kits can be easily installed.

D. Space Transportation System/Centaur

1. Background

Although the Centaur project has been cancelled as far as flying them on the Space Shuttle, there is much to be learned from programs as complex and frought with technical, management and political problems as Centaur. There were many challenges associated with adapting the Centaur upper stage from an expendable launch vehicle environment for use as an integral part of the Space Shuttle. The first and foremost, the safety of the Orbiter crew and the protection of the Nation's investment in the Space Shuttle had to be assured. The Centaur is the first payload to use high energy cryogenic propellants and required the development of the necessary hardware and software to assure a safe system without unduly complicating (weight, reliability, maintenance, logistics) either the Centaur or the Orbiter or the ground support equipment.

Other items to keep in mind include:

o Originally the Centaur was conceived as an element of the Space Shuttle just as the Orbiter, SSME, SRB and ET were. Then well into the program it was changed to a payload which in turn changed the roles and responsibilities of the NASA Centers involved and to a degree the prime contractors as well.

o During the development of the Centaur there was the

continuing development of the Space Shuttle itself so that transmitted loads and other environments were shifting. This resulted in a large number of modifications to the design and test program.

Thus the Centaur was constantly living in an interactive environment which resulted in many problems encountered in climbing up the learning curve.

2. Establishment of Firm Program Goals

Findings:

The uncertainty of both the Shuttle/Centaur and the Atlas/Centaur programs' direction in the year or two prior to the firm commitment to start the Shuttle/Centaur Program caused a severe startup impact on the contractor and NASA. There was an attitude of uncertainty that prevailed across prime and secondary contractors as well as within NASA. The Atlas/Centaur, which was scheduled to be phased out, was extended for several years. The Centaur was initiated, stopped, and then restarted. During this time a great many of the key personnel from the factory floor up through management were moved to other programs, laid off or retired. Added to this was the challenge set by a given planetary launch schedule.

Lessons Learned:

For programs that have development activities and long lead time procurement requirements in addition to significant interfaces with the Orbiter and ground facilities, firm program goals must be established and maintained, but the associated schedule must be realistic.

Recommendation:

It is imperative that all team members, both contractor and government, develop and maintain stable and realistic plans if the mission objectives are to be met within reasonable resource expenditures.

3. Concurrent Development

Findings:

A factor that complicated Centaur development was the number of interdependent development activities conducted in parallel. These included the Orbiter modifications for both the Centaur G and G-Prime configurations plus the changing induced structural loads resulting from a better understanding of the flight data from Shuttle mission. For example, Centaur/Orbiter interface line load changes caused a major redesign of the Centaur Integrated Support Structure lines and valves; Ascent flight loads have impacted the Orbiter/Ciss/Centaur trunnion mounts; the

hydrogen dump and vent lines affect the thermal environment of the Orbiter Tail surface affecting its location and thermal stress on tail structure. In addition, the degree of commonality of the Centaur G and G-Prime designs was overestimated relative to their integration to the Orbiter and the basic spacecraft requirements. Establishing a generic Centaur design that is compatible with multiple spacecraft also took more effort that anticipated.

Lessons Learned:

In programs where there are multiple complex development interfaces such as Centaur, development issues on one side of the interface are likely to affect the other side. The degree of the impact is not easily estimated at the start of the program nor, for that matter, even in latter stages of development.

Recommendation:

Sufficient resources and manpower, as well as contingency reserve time, should be set aside to handle these types of activities. Adequate involvement early in the program by management on both sides of all interfaces is mandatory.

4. Integration Process

Findings:

When the Centaur Program was originally approved, the Centaur Upper Stage was considered a Level III element of the Space Transportation System. This meant that the Centaur would follow the same integration process that was used for the other STS elements. A separate office at JSC would provide the direction and guidance for Centaur as had been performed for the other Shuttle elements. During early development of the Centaur, the roles and responsibilities between JSC and LeRC evolved more closely aligned to the JSC payload integration approach as opposed to the Shuttle element approach. At that time, it appeared that both centers preferred this method of integration. In April 1983, the process of integrating the Centaur as a payload was formally adopted and agreed to by both centers. This approach to integrate Centaur as a payload has resulted in attempting to achieve integration as an "end item" as is customary for payloads rather than the usual interplay and trade-off approach that is employed when a total systems engineering and integration effort is conducted between elements. In addition, the LeRC based their integration estimates on their experience of integrating spacecrafts on unmanned vehicles. Integration into the manned Shuttle system proved to be an order of magnitude greater than their Atlas and Titan/Centaur experience indicated.

Lesson Learned:

Integration of a government-funded system as complex and sophisticated as a Centaur Upper Stage should be treated as an integral part of the Shuttle and not simply as "another payload." The proper degree of systems engineering and integration trade-off on both sides of the interface is required. The payload approach was established to handle the large number of payloads to be manifested with the Centaur. Safety of the Space Shuttle was compromised.

Recommendation:

The payload approach should be reserved for simpler payloads or upper stages that can basically use a standardized payload launch processing procedure and in-flight operations. Safety of flight dictates that a payload requiring major modifications to the Orbiter can not be "another payload."

5. Safety Process

Significant philosophical differences exist between a manned and unmanned vehicle regarding safety issues. A significant difference exists in the technical and administrative experience of dealing with a manned versus an unmanned space vehicle. The level of fault tolerance, fault isolation and system design for reliability are considerably greater for manned missions. The major reason then for the problems which surfaced during the design and development of the Shuttle/Centaur upper stages is that while these two centers both have considerable flight experience, the prime center responsible for development of the Centaur had previously been involved in unmanned vehicle systems and did not fully understand the complexities of mating with a manned system.

In addition, the planning and design requirements associated with the Shuttle off-nominal and abort modes were not properly assessed at the start of the program.

Lessons Learned:

Program requirements should be defined and designed into the vehicle system from the beginning, not after the flight hardware design is well underway. The safety process is a continuum and requires the proper managerial mentality and philosophy. The findings noted above are also, to a great extent, the lessons learned.

Recommendations:

For future vehicle systems, including complex payloads, the safety process must be understood and considered in the basic design effort of the specific flight hardware commensurate with the philosolphy that exists for the manned flight programs. Most of the "Lessons Learned" items mentioned above are significant contributors to achieving the required level of safety, i.e.,

getting all organizations involved in the design process very early and fully, so that safety requirements can be incorporated in the most efficient manner.

6. Acquiring Space Qualified Electronic Piece Parts

Findings:

One of the top level specifications for the Centaur program called for stringent screening of electronic piece parts. Although an electronic piece parts screening requirement has existed for many years on the Atlas/Centaur program, the Shuttle/Centaur requirement was more stringent because of the manned involvement. In meeting such a requirement, the experience of the aerospace industry is that electronic device manufacturers are unwilling or unable to perform the testing required by the tight screening requirements in a timely and cost effective manner because of the small numbers procured and the slow rate of use compared to something like the automotive industry. This practice forced the Shuttle/Centaur associate contractors to procure "unscreened" parts from the manufacturers and "high grade" the parts through their own screening process. A large rejection fallout from this process had then been experienced.

Lessons Learned:

o Identify the specific piece parts required, purchase sufficient quantities for screening and initiate the procurement action as early as possible after the program has been approved.

o Since electronic piece parts are a problem for all government programs, it may be cost effective to identify and purchase often used parts in large quantities qualified to the needed high grade specifications.

Recommendations:

In addition to following the lessons learned as noted above; these high-use, high-grade parts could be stored in a depot from which government users could obtain the parts which would be faster and less costly overall.

7. Weight and Performance

Findings:

When the Centaur G-Prime Program was started, approximately four years prior to launch (at that time), the Shuttle program performance and spacecraft (Galileo and Ulysses) weights were provided, which resulted in a Centaur performance margin of about 200 pounds. By any standard, such a reserve margin was not only very low but in fact unacceptable. This would be true for a mature, ready to launch system let alone one just starting

development. As time went on the expected occurred, the weight of the flight systems increased and the performance available eroded. To maintain even a slim performance margin for the combine Shuttle/Centaur system weight reduction and design change programs were initiated at great cost of resources.

Lessons Learned:

o Sufficient performance reserves must be established at the outset of any program where such are critical . . . most space programs.

o Because of the interdependence of the Shuttle program and the Centaur program (both G and G-Prime) they should have been treated as an integrated and coordinated whole. The complete stack approach could then be used to make the appropriate engineering systems analyses for the benefit of the mission as a whole as opposed to forcing the Centaur to make costly weight reduction changes when simpler and less costly total trade-offs might have been made. The impacts on safety of such an operation resulted in the final nail in the Shuttle/Centaur coffin.

Recommendations:

Here again the lessons learned are within themselves the recommendations for future programs. These are not new problems but they seem to be relearned for each new program as as result of external forces over which the program management has little control.

III. SUMMARY

It has been customary to collect and publish a document or documents containing significant lessons learned during the course of each of NASA's major programs and particularly its manned space flight programs. In the past this has been done at the conclusion of the program and as a result much of the "good" that can come from such lessons are lost on either on-going programs or those just starting up . . . time is of the essence. In the case of the Space Transportation System with its broad scope and large variation in vehicle elements, the lessons learned can be used on the Space Transportation System since it will be on-going for many years, and the Space Station which is now undergoing reevaluation.

Design excellence and manufacturing quality are the result of engineers and managers using the experience bank built up over the years on aerospace programs. These lessons learned are in support of that thesis.

The Space Transportation System as viewed by the Aerospace Safety Advisory Panel was specified and designed with appropriate attention to cost, safety and performance (flight and ground). However, as noted by the President of the Flight Safety

Foundation in a recent article "Contrary to what many of us wish were otherwise, there is a correlation between economics and achieved safety levels. It cannot be quantitatively defined in most cases, but, qualitatively, the relationship is abundantly demonstrated. We live in an economic world, and it is up to us to be clever enough to wrest the highest levels of safety from the many economic constraints that hamper its full achievement."

The Space Station in particular is in a position to learn from lessons from specification of requirements to operations.

Finally, when dealing with risk, one is dealing with uncertainties, with things one hopes will not happen--things it would be pleasant to forget. With experience one learns, however, that it is not wise to forget them.