just once when the new configuration is introduced.

There are only two options with respect to testing a 4/1 configuration. Increase the level of testing for each flight or reduce the number of tests of the 4/1 configuration (in comparison to needs for testing a 5/0 configuration). An unknown at this point is the difference in testing requirements between the two configurations. JSC personnel do not feel comfortable in estimating this difference without performing a detailed testing plan. However, 10 - 15 percent would probably not be too poor an estimate. As flight simulation tests are very expensive, this difference represents a substantial amount of money. Equally important, it represents a longer turnaround between flights and would reduce the frequency of Shuttle flights (there is only one Shuttle Avionics Integration Laboratory (SAIL) facility and it is already in operation two shifts per day).

From the history of software and hardware failures detected during flight simulation tests, it would appear that a 10-percent reduction in testing could possibly result in missing the detection of a software failure sometime within 10-20 flights. Thus, NASA should pay the extra testing costs and not reduce testing if a 4/1 configuration is chosen. It would also be important that JSC personnel be protected from undue pressure to reduce or limit testing costs in the face of increased testing needs.

Operational Procedures: The second area of concern is the fact that the reconfiguration management in event of a BFS GPS failure is potentially more complex with a 4/1 configuration than for a 5/0 configuration. Again, the exact nature of the differences cannot be determined until additional design decisions are made in the future. Also, the opinions of NASA personnel about the nature of the changes is varied. It is possible that in the event of a BFS computer failure in a 4/1 configuration, one would be faced with either having the

astronauts manually physically rearrange the computers in the system or fly the remainder of the mission without a backup computer. Either choice introduces additional risk.

It is also important to recognize that there is some increase in the level of complexity that the human astronauts must manage and that there has already been a near-disaster due to pilot error. It was mentioned above that during the STS-9 flight, two of the computers failed. One was re-started and placed back in service (but in a reconfigured system). When the Shuttle touched down, that computer failed again. When the pilot switched it out, he forgot about the reconfiguration and switched out a good string of one of the good computers. Had such an error occurred before touchdown, a major disaster would have been likely. This error occurred because of the complexity of the system operation. Increasing the complexity of in-flight operation does, therefore, increase the risk involved.

Ultimate Configuration: There are also considerations that arise with respect to whether or not a 5/0 configuration is adopted ultimately. If a 5/0 configuration is not adopted, the Shuttle will be flying for a long time with very obsolete hardware. This obsolete hardware is also aging and will eventually become unusable, at which point a 5/0 configuration seems inevitable (unless yet another generation of new hardware is added).

If a transition to a 5/0 configuration is ultimately made, there will be an additional round of modification, testing, and training involved and, hence, additional expense incurred.

Reliability of New and Old GPCs: It seems clear that, on paper, the new GPC is more reliable than the original but it does not have the flight testing of the original. All of the problems found in the original GPC have been corrected in both the current versions of the original GPC and the new GPC. If an original GPC

is used, it will be a processor that has been in use for several years, not a new production copy of the original design. This has potential for both positive and negative effects. Through its use any initial manufacturing defects have been eliminated. However, as it has been in use for several years, one must question the effects of aging.

Findings

The principal factors between a 4/1 and a 5/0 configuration are:

1. The additional safety provided by dissimilar hardware (remember that there already is dissimilar software);

2. Human factor contributions to risk - part of the safety provided by the computer redundancy is achieved through astronaut training and in flight operations and maintenance procedures performed by the astronauts. There would be some differences in the training and in these procedures between a 4/1 and a 5/0, and correspondingly a difference in the risk introduced by human factors. This risk difference may well be greater than that in item 1 above;

3. The impact of the flight schedule on the software testing that will be possible, or stated conversely, the impact of the software testing (which is larger for the 5/0 configuration) on the flight schedule, and;

4. The additional costs required for a 5/0 decision.

It is not possible to quantify the first of these. Though there have been a few claims regarding the second, there has not yet been a careful study of this factor. The third has also not been studied in detail, but 10-15% is a reasonable estimate. The

fourth has also not been studied.

The second item has strong safety implications beyond the decision between a 4/1 or a 5/0 configuration. It is clear that some current operational and/or in flight maintenance procedures performed for the purpose of improving computer reliability may require the astronauts to do things in a different manner than that in which they were trained. This results in a significant additional risk, and has already resulted in a near disaster.

Recommendations

1. In order to provide greater confidence in the new GPC, it is recommended that the new GPC be flown on several flights as the backup computer. Since several flights are scheduled with the old GPC's before the changeover, this should be possible.

2. NASA should conduct a study of the human factors aspect of risk associated with in flight operations and maintenance procedures, particularly changes in procedures resulting from response to some failure. Included in this should be a preliminary design of the 4/1 procedures and training and an assessment of their impact.

Software Development Procedures

The software development procedures used are critical to the reliability and cost of the on-board computer system. As it is not yet possible technically to automatically guarantee the correctness of real-time embedded programs of the size and complexity of those running the Shuttle, extensive testing is essential. Techniques and languages have been developed, however, that ease the problem somewhat, reducing the cost and amount of manual testing required. The review of these activities for the Shuttle has just begun and has not reached a stage where useful comment can be made. This review will be a

major activity of the Panel during the coming year. Among the concerns are the following:

1. The methods of determining and validating the 8,000 I-LOADS that must be defined for each Shuttle flight. These constants define the mission to be flown and are as important as the software and computers to the success of a mission.

2. Implications of proposed flight schedules on flight software testing on the SAIL facility. In particular, there are concerns that the increased flight schedules will force reduced per flight testing.

3. The methods by which software tests are generated. The quality of the resulting software is highly dependent upon these procedures.

4. The methods by which compiler upgrades are tested. The compilers translate the program written for the Shuttle into the code executed by the computers.

5. More detail on the redundancy management among the computers, in particular, timing and comparison methods.

6. General hardware and software support system upgrade policies. It is not clear that NASA has general procedures. In the aftermath of the GPC upgrade, it would be a good idea to examine this issue and encourage NASA to develop suitable procedures.

In addition to these technical concerns, there are several concerns about personnel matters:

1. The salary structure for technical persons within NASA is of concern. It appears that in order to progress in

terms of salary, people must move into management ranks, making it difficult to keep experienced, highly qualified people in the technical ranks. Moreover, it appears that the salaries of NASA technical people are substantially below corresponding industry salaries.

2. Much of the knowledge of Shuttle computer development and operation resides in the corporate memories of the employees who have worked on the system. The age distribution of the employees working on the computer system is of concern. There have been initial inputs that the current staff is heavily skewed toward the older age groups and that there is a dearth of employees in the mid-age group.

3. Some concern has been expressed about pressure from above to state that adequate tests can be performed within budget, whether or not they can be; it is also implied that if individuals do not conform, someone else will be found who will.

F. External Tank

At this time the External Tank is the Shuttle element that has been least affected by the activities undertaken in the aftermath of the Challenger accident. This is not to imply, however, that there have not been activities to ensure continued confidence in the External Tank. As with other elements of the Shuttle, a review and assessment of all the requirements for the External Tank is being made. This review includes design, test, integration, and FMEA/CIL hazards analysis. Thus far, no significant issues have surfaced although the External Tank Tumble System was the first subsystem to go before the Level II Program Review and Control Board for a waiver subsequent to the re-visit of the FMEA/CIL process.

G. Orbiter Landing Gear System

The Orbiter landing gear has been a subject of concern to the Panel and has been discussed in its reports since 1981. The Presidential Commission commented on this system and on other aspects of the landing phase in the section of its report entitled "Landing: Another Critical Phase." In this section the concerns discussed by the Panel were highlighted. NASA has responded to Recommendation VI of the Commission's report; the response meets the objectives of the Panel's earlier recommendations. The actions undertaken comprise test, operational, and redesign activities. The significant elements thereof are summarized below:

1. Operational:

a. Shuttle landings will be planned for Edwards Air Force Base until satisfactory structural safety margins have been demonstrated.

b. Gear load reduction by means of appropriate positioning of Orbiter elevons during the period from nose-wheel touchdown through high-speed roll-out will be implemented.

c. Planning will include the determination of optimum Transatlantic Abort sites including any needed upgrade thereof.

d. A runway overrun barrier is to be used at Dakar, Senegal.

e. Improved wind measuring equipment will be installed at both launch and landing sites.

2. Test:

a. Prior to first reflight, a heavyweight brake dynamometer facility will be assembled and used to verify braking capability.

b. High-energy "wear-ins" or "green-runs" will be conducted on brake assemblies.

c. Tests will be conducted to assess the characteristics and adequacy of the anti-skid system.

d. Tests will be conducted to determine braking capacity taking into account the maximum brake pressure capability and response time of the crew under the known post-flight physiological condition and capability of crew members.

e. Tests will be conducted to determine the feasibility and consequences of a "roll-on-rim" capability.

f. Tests to determine the effects of fifteen (15) knot crosswinds (completed).

3. Design:

A number of changes to the brake system will be designed and implemented. Among these are the following:

a. Thickened brake stators.

b. Modifications to balance brake system hydraulic pressures to eliminate the apparent 60/40 energy distribution between inboard and outboard brakes.

c. A six-orifice brake hydraulic system to alleviate hydraulic chatter that has been observed.

d. Stiffened axles to alleviate relative motion between

stator and rotors to increase effective rubbing area contact.

e. The development and installation of a tire pressure monitoring system.

f. Develop tire improvements. Development tests are to be conducted at Langley Research Center and at Wright-Patterson Air Force Base.

Additional areas are being investigated as part of the effort to improve the Orbiter braking system. These areas have not, however, been designated as mandatory for first reflight. They include items such as use of an Orbiter drag chute, up grading of nosewheel steering system, and wheel spin-up devices. Also, landing and roll-out simulations are to be conducted at the Ames Research Center flight simulators. The Panel will continue to monitor progress in these areas.

## IV. Space Shuttle Operations

### A. Launch Processing

The Panel has continued to review and assess the multitude of activities that comprise the preparation of the Shuttle for flight and the launch of a mission. Emphasis was placed this year on determining the effects of actions being taken to recover from the Challenger accident and the identification of areas that, in the Panel's opinion, might require added management attention and/or might affect the ability to achieve a safe first reflight on schedule.

In the course of its reviews, the Panel drew information from a variety of sources but concentrated its efforts at the Kennedy Space Center (KSC). As part of the review process, Panel members held discussions with more than 40 "hands-on" technicians, quality control inspectors, and schedulers. Detailed discussions were conducted with senior and mid-level managers from KSC and from the Shuttle Processing Contractor (SPC).

Among the subjects examined were the status of facilities and flight hardware; the organization of both the KSC and the SPC and changes that occurred, the effectiveness of internal and external communications of these organizations; the status of personnel training, morale, and motivation especially as affected by the stand-down from flights and by personnel reductions during this period; the logistics and safety, reliability, maintainability, and quality assurance activities; the results of the recent activities of the SPC Risk Review Board and Safety Advisory Board (these topics are covered in another section of this report); and finally, the response to Presidential Commission recommendations.

Status of Facilities: There is much activity in process to

bring the facilities at KSC to a state of readiness to support the program when flights are resumed. Among the major facilities, the following are of note:

1. Pad "B" is almost complete with all modifications considered necessary prior to the first re-flight. The latter include items such as rain protection system, ET vent, and debris plate changes.

2. Pad "A" modification projects are running behind those of pad "B". Because of the availability of pad "B" and a limitation of resources, there is a slower construction rate in effect for pad "A". Current plans indicate that construction work on this pad will be completed about December 1987.

3. Mobile Launch Platform Number 3 is in the activation process and will be placed in a "minimum maintenance mode" from February 1987 through September 1988.

4. The Orbiter Modification and Refurbishment Facility now has an operational readiness date of April 1989.

5. The Orbiter Thermal Protection System (TPS tiles) Facility has an operational readiness date of April 1987.

6. The contract for the Orbiter Processing Facility Annex is scheduled to be let in early 1987.

7. The Payload Hazardous-Servicing Facility is in work.

Operations: NASA has selected McDonnell Douglas Astronautics Co. to perform payload ground operations at KSC, Vandenberg AFB, and at Shuttle landing sites. It is anticipated that work under the contract can begin in early 1987.

The issue of weather forecasting has been under review for some time as it affects operations at KSC. The need for more accurate and timely weather data, particularly winds aloft and rain, has been apparent and became more apparent as the pace of operations increased. From this review has come a plan that includes support from the National Research Council. Among the items being pursued is a development activity that will examine the feasibility of using a specially instrumented aircraft to determine wind velocity and direction in near real-time as it flies a trajectory that approximates that of the planned Shuttle ascent. The technique in use for this purpose at present yields data that can be as much as 3 hours old. Under these circumstances it is necessary to make allowances for uncertainty in the persistence of the wind conditions in predicting the structural loads that will be experienced by the Shuttle during ascent. Obviously, reducing the allowances for such effects will improve the assessment of loads and permit more informed control of risk.

In response to concerns raised by the Presidential Commission, the Associate Administrator for Space Flight established a review team to examine and assess the implementation of the Shuttle Processing Contract at KSC. The team was to give particular attention to the relationship between the SPC contractor and the several flight hardware contractors. This team has begun its activity and the Panel plans to meet with this group to exchange views.

In response to a request from the USAF, NASA is evaluating potential use of Vandenberg AFB Shuttle facilities during the period of "caretaker" status, now estimated to extend to 1992 or later.

General: On the basis of the discussions described at the beginning of this section, the following observations are noteworthy:

1. The magnitude of the documentation required at KSC for a typical mission illustrates the complexity of the launch preparation and launch processes. There are some 3,000 separate documents required comprising some 200,000 pages. When the number of copies required are factored into the consideration, some 15 million pages of documentation are distributed for each launch! If a launch is "scrubbed", some 2-3 percent of the pages (i.e., 300 to 450 thousand) pages must be reissued.

2. Facilitating internal NASA communications continues to be a key ingredient for KSC to meet its goals. This is recognized by all those involved and as the operations organization evolves under the changing STS organization, senior management attention must continue to be focused on this area to be sure that the communications system does not lose its efficacy during the transitional period.

3. There is a substantial amount of unplanned and previously deferred work at KSC. This is particularly true for the Orbiters. This work must be carefully scheduled and accomplished.

4. It was observed that, with lay-offs completed, the morale of the employees, particularly those of the SPC, has improved. This could be a transient phenomenon if any further personnel reductions are not handled adroitly. Frequent impromptu visits by senior managers to the work sites are an effective means for maintaining morale and motivation among the "hands-on" personnel. This is also true when the tempo of activity increases in preparation for the resumption of flight.

5. Workers often expressed the opinion that training should employ real or equivalent hardware and situations so that

the trainee can attain proper understanding of the hardware, software, and procedures. It was also suggested that competent supervisors and/or engineers should give the technical training courses rather than a training staff considered to be unfamiliar with the "real world."

6. The "hands-on" personnel exhibited respect for and reported satisfactory relations with most engineers. There was, however, concern expressed about the lack of experience and/or ability of many of the newly hired engineers.

7. The concerns about the use of "shop aids" that had been expressed by the Panel have been addressed most effectively and thoroughly. All the organizations involved--KSC, MSFC, JSC, and their contractors--are to be congratulated.

There are no specific findings or recommendations to be made in this area, other than these related to Shuttle management set forth in Section II and the Executive Summary. Launch processing is a complex activity and requires constant attention and discipline, along with adequate budgets and schedules, to be effective and safe. The Panel will continue to monitor activities in this area during the next year.

B. Logistics

The subject of logistics has been thoroughly reexamined by NASA since the Challenger accident. The concerns expressed by the Panel in previous annual reports have been fully borne out by this review. One positive result has been the safeguarding of funds designated for logistics--they can no longer be "transferred" or "re-programmed" to satisfy needs in other areas. There remain important issues and problems that must be addressed

forcefully and solved so that NASA can believe, with assurance, that it has established an effective logistics system for the long term. These issues/problems lead to the following recommendations:

1. Complete the procurement process for necessary spares.

2. Establish procedures for the control of cannibalization with the ultimate objective of eliminating the practice.

3. Establish control of the pipeline for the repair of Line Replaceable Units (LRUs), in particular, as well as for other components. This will probably include the need for a repair depot on-site at KSC. Although it will still be necessary to return certain sensitive units to the manufacturer for repair, the number of such units should be kept to a minimum.

4. Determine, as soon as feasible, the impact of the "Maintenance Safeguards" program. If there is a financial effect (i.e., increased spares requirements) necessary budget modifications should be made promptly.

5. Ascertain the effect of the planned maintenance program on logistics. Make necessary adjustments to spares required. If the maintenance program planning is not yet complete, do so promptly in order that the effect on spares requirements may be known and incorporated into the recovery plan.

6. Determine the effects, if any, of the results of the ongoing Shuttle Design Review program (if any) and factor them into logistics planning.

7. Re-examine and assess the logistics targets to ensure

that they are compatible with realistic flight rates.

8. Establish a program to determine which components, devices, or parts are no longer available or may become so as a consequence of the supplier going out of business or ceasing their manufacture. Establish an activity to obtain equivalent hardware.

9. Reduce pipeline turnaround times for all critical LRUs.

C. Shuttle Flight Simulators

The Shuttle flight simulator program requires an additional airplane because the current three airplanes are aging and will soon require major modification. The restart this year of the astronaut mission related training program will require the fourth airplane in order to maintain the proposed flight schedule. Although this is approved, it appears to be suffering from lack of top management attention.

Recommendation:

NASA Headquarters should ensure that this program is continued and completed in a timely fashion so that astronaut training will not be delayed or restricted.

## V. SAFETY, RELIABILITY AND QUALITY ASSURANCE

### A. The NASA System Safety Program

Following the Apollo 204 tragedy, NASA spent several years putting in place a basically new type of safety program. An organization was set up at Headquarters and the methodologies were developed for an overall safety program. These methods were incorporated into the various volumes of the NASA document NHB 1700.1 "NASA Safety Manual." Other documents describe "Reliability Program Provisions," NHB 5300.4(1A), and "Quality Program Provisions," NHB 5300.4(1B).

At the core of NASA's safety program was the idea of "risk management" through the control of "hazards." Residual hazards that could not be designed away would be controlled at least to the level consistent with program objectives and cost constraints. The definition and analysis of hazards associated with a system and its operation was to be performed by "System Safety Function." The level of hazard control was not always expected to be perfect, and a "residual risk analysis" would be performed to provide a "retention rationale" for continuing to operate.

In parallel with the "Systems Safety" activity was a "Reliability" activity. This function was basically concerned with establishing a data base for selection of components which would meet allocated failure probability requirements, performing "failure mode and effects analysis," establishing redundancy criteria and configuration definitions, maintainability criteria and life limits, and the preparation of "critical items lists," containing items with single-point failure modes which could cause catastrophic results.

In principle, the failure modes and effects analysis should be both a design tool to provide an impetus for design change and

an evaluation tool of the final configuration to define the necessary control points on the hardware.

The identified "critical items" would require a supporting "risk assessment and retention rationale" in order to be included in the overall system configuration. The hazard analyses being performed by the system safety function and the failure mode analysis and critical item identification performed by the reliability function came together in the generation of Safety Analysis Reports (SARs) and subsequent retention rationale for the critical items.

A third element in the overall safety program was "Quality Assurance." This function, as defined by NASA, would be responsible for ensuring 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 included supervision of personnel certification and establishment of non-destructive testing methods to detect flaws and non-conforming materials.

At the beginning of the Shuttle program, the basic system safety policies and methods to be used were established by NASA Headquarters and used many of the approaches evolved during the Apollo program. The responsibility to implement these requirements was tiered down to various program levels and centers by management instructions and other requirements documents. During the earlier development phases of the STS program, NASA Headquarters retained a daily strong role in directing the overall safety program. However, by the time of the Challenger loss, the Headquarters organization was only minimally staffed, and had basically only a limited review and audit function. They were essentially a Headquarters Level 1 staff organization with no explicit responsibility and corresponding authority for system safety engineering throughout NASA. Headquarters field representatives at the Centers began to

report directly to the program managers, and were simply reviewing data and specific problem areas rather than leading a comprehensive safety engineering activity. Annual audits by Headquarters declined to biannual and became merely surveys of limited scope with minimal staffing.

The implications of this relatively weakened safety organization was highlighted in the President's Commission Report when they said in Chapter VII that "the Commission was surprised to realize after many hours of testimony that NASA's safety staff was never mentioned."

Discussion of the NASA Safety Program

The Panel recognizes, as does NASA, that modern hardware systems such as aircraft or weapons or the STS are not only incredibly complex, but usually demand high performance and, therefore, are subject to significant risk. The objective of a System Safety Program in any enterprise or organization should be to manage such risk to an acceptable level (not zero) throughout the operational life of the system. In our view, the elements of such a Total System Safety Program are comprised of the following:

1. System Safety Engineering
2. Program Quality Assurance
3. Operational Safety Doctrines

In some organizations the first two elements are sometimes combined into a function called Product Assurance and is many times organized and thought of as the "Quality Assurance and Reliability Function." Within the Space Shuttle Program they were grouped in 1979 (NHB 5300.4(1D-2)) into what is even now referred to as Safety, Reliability, Maintainability and Quality Assurance (SRM and QA). Experience teaches, however, that under this "ility" structure, the system safety function loses its

"engineering" role. Further, as operated in NASA, it does not have the authority to ensure that safety is designed into the system, does not control the system safety validation, and eventually becomes an analysis, record-keeping and audit function populated with personnel having that type of background.

However, beyond the disturbing decline in safety engineering stature throughout NASA, we believe there are also issues with the basic methodology used to ensure that risks are adequately projected (quantitatively) and then controlled to the levels accepted.

The Presidential Commission recommended that NASA should review all Criticality 1, 1R, 2, and 2R items and Space Transportation System hazard analyses. NASA responded during 1986 by performing a massive rework of all Shuttle program failure modes and effects analyses, an update of the resulting critical items lists, and a review of all hazard analyses all of which continues today. Although this may have value in identifying any new critical failure modes that may have been missed earlier, or subsequently introduced through changes, the crucial problem with the safety methodology is not really the failure mode nor hazard identification process. The procedures used do indeed result in definition of the critical modes of failure and their resultant hazards, and also the hazards which result from external influences beyond the system hardware and software. The crucial issue with the process is the "retention rationale" used to accept the hazards and which justify a waiver for using Critical 1 and 1R items. In many instances the stated rationale is really only qualitative "rationalization."

Criteria for quantitative risk assessment and explicit definition of the operating constraints to which the waiver is subject are not explicitly required by NASA's safety program guidelines. Although the Panel is quite aware of the pro's and con's of trying to establish "likelihood" or "probability" of

failure, we believe a more realistic quantitative assessment of the critical hazards is crucial to overall risk management. There are many analytical tools and test methods that can provide data for such assessments. Among the most important inputs are the validation of critical design criteria and the demonstration of actual margins to failure modes.

The Panel believes that NASA could achieve a significantly better level of Operational Risk Control by recognizing Safety Engineering as an engineering design and hardware/software validation function; that Program Quality Assurance is a "total configuration control" function; and that Operations Safety Engineering is an "operational doctrine and control function." Within such an overall framework, the System Safety Engineering function should be carried out within clearly established policies and guidelines by means of specific organizational units directly responsible to teh NASA Center Directors and operating under policies established by the new Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance. This new Headquarters office must have more than the loose oversite role in overall safety exercised by the Chief Engineer's Office over the past few years. The Associate Administrator should be made responsible for NASA system safety engineering in the broadest definition of that function (see below) and given the authority necessary to impose safety methodology, policy, and approval authority for system implementation. NASA safety engineering personnel should be part of the NASA Headquarters organization, although they would be matrixed into the various programs and projects. Their professional stature, career paths, and rewards should be a part of a respected Safety Engineering organization.

The System Safety Engineering function skewers through the overall hardware and software engineering activities. Among other things it should embody the following elements:

1. Overall system safety analysis

2. Hazard analyses and relative risk assessments

3. Failure modes and effects assessments and critical item definition

4. Critical components and subsystems reliability analysis and redundancy criteria

5. Criteria for design safety factors and operating margins

6. Component validation and systems certification test program requirements and implementation criteria

7. Specification of all environmental constraints at every level to ensure control of the validated margins on each subsystem

8. Evaluation of all flight data and modification of operating constraints as required to stay within validated margin regimes

The reason the Panel recommends that Safety Engineering be responsible for establishing safety factor and operating margins criteria and for defining the component and system certification programs is that these areas have the highest leverage on overall risk assessment and control. To be made responsible for system safety without authority over all of these critical functions that control the real risks is not viable.

Mission Operations Safety Engineering should also be the responsibility of the Systems Safety Engineering Organization. The function of Operations Safety Engineering is to ensure conformance with the policies and constraints under which the mission operations of the system will be carried out so as to

sustain the certified configuration. These policies and constraints should encompass launch commit criteria, flight validation policies, and environmental constraints. The overall NASA policies in this area should be the responsibility of the new Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance.

The Safety Engineering Organization should not be responsible for NASA Occupational Safety which should be a totally separate function under a Health and Safety Organization. It is most important that the Safety Engineering functions in NASA be perceived and operated as a true engineering discipline. The engineers should have significant professional training in safety engineering methodology and be incorporated into the earliest phases of the planning and design phases of every major hardware system program.

The third element of overall program risk management is Quality Assurance. Quality Assurance should be viewed as a configuration control function. As such it provides the certified documentation that the hardware and software have been produced to the exact designs which delineate the validated and qualified components and integrated systems. The "configuration" includes all aspects of the hardware and software including the applicable environments which in any way influence the properties of materials or stress margins or temporal behavior of components and systems. This function should be performed by a separate Quality Assurance organization and should not be a part of the responsibility of Safety Engineering (although there is certainly an interaction). The Quality organization should be the direct line responsibility of each NASA Center (and, of course, each Contractor) with the Director of Quality Assurance reporting to a top level of management to retain its independence and full integrity. Its purpose is not to engineer but to control and assure. As part of this function it does control the entire set of final released engineering documents describing the complete

configuration of the system.

In the fall of 1986, responsibility for policy and oversight of this function was also included in the new Associate Administrator's Office. This is important because overall risk management and total Systems Safety is dependent on the Quality Assurance function throughout NASA.

Findings:

At the time of the Challenger loss, the safety function at NASA Headquarters had significantly declined in both function and staffing levels from its early role in the STS program. The Panel's perception from many briefings, documents, and discussions was that it had become basically a reviewing and auditing activity with little explicit authority for establishing and implementing System Safety Engineering policy throughout NASA.

The Panel's investigations into NASA's safety engineering methodology led us to believe that even had the activities been fully staffed, there still remained questions about how effective the safety program could really be. The safety engineering function has been basically lumped into a Safety, Reliability and Quality Assurance staff-oriented organization. At the present time, our understanding of the new office of safety, reliability, maintainability and quality assurance, is that it is still basically a staff function with responsibiity to define roles, requirements, and organizational structures in safety, reliability, maintainability and quality assurance. Three fundamental weaknesses appeared evident. First, there was a lack of in-line responsibility and authority in a Headquarters organization for establishing and directing the safety engineering function. Second, the elements of the safety functions that were being done at various locations did not include responsibility for defining and controlling the

validation and certification programs. Thus, there was no way that the safety organizations in NASA could take responsibility for assuring that failure mode margins were acceptably demonstrated nor assure that the hazard analyses on which the risk assessments were based were valid. Third, there was a conscious lack of quantitative approaches to determine failure-mode probabilities for the purpose of defining acceptable margins, nor for the relative likelihood of resulting system interactive hazards.

Recommendations:

The Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance should have full responsibility to establish a total Systems Safety Engineering program throughout NASA and be given the authority to assure its full implementation. A Systems Safety Engineering organization reporting to the Associate Administrator should generate the overall safety program policies to be followed. It would also define the critical safety design criteria to be used and the testing program methodology necessary to assure that those criteria have been properly validated. This Headquarters organization would also establish requirements and methods for performing overall system integrated hazards analysis and for the generation of quantitative risk assessments tied to controllability of failure mode margins and test and flight results.

Reliability, Configuration Maintainability and Operations Safty Engineering should be integral parts of this Systems Safty Engineering organization and it would provide policy direction for these functions throughout NASA. The definitions of policies and operating instructions for the Quality Assurance functions which are a vital part of risk management should also be the responsibility of the Associate Administrator.

The policies and implementation directives should be implemented by System Safety Organizations reporting to the Director's office at each NASA Center. As appropriate, personnel from these organizations could be matrixed into the various programs. A significant part of NASA funds to be spent in safety areas should be allocated directly to the Systems Safety Organizations. This would provide assurance that necessary safety engineering activities can be controlled independently of the funding tradeoff pressures which always exist within the programs.

B. Non-Destructive Evaluation/Quality Assurance

Special attention is being given to non-destructive evaluation (NDE) test methods to assure quality (conformance to the design and build methods) for critical items, e.g., the internal components associated with the various joints in the solid rocket motor. In support of accomplishing this a meeting of national experts was held at the NASA Langley Research Center (LaRC), November 20-21, 1986, to discuss techniques for non-destructive evaluation (NDE) for qualifying critical Shuttle components. LaRC's expertise lies in detection sensors, signal processing and enhancement and data interpretation techniques.

The measurement technologies which Langley Research Center believes are candidates for assessing many of the questions of Solid Rocket Motor integrity are related to acoustic and thermal propagation. Both of these appear capable of detecting the various bond line problems that have been identified as critical failures modes. X-ray techniques which may play an important role will take a number of years to be of value. The thermal methods seem, at this time, to be the most practical in that they can determine properties over large surfaces efficiently and effectively. For example, it has been shown by a major contractor that hot water can be used to heat the rocket motor case to "see" into the insulation with infrared imagers. LaRC

tests have shown that one can determine quantitative physical properties of materials with a thermal NDE system consisting of scanning lasers, IR detectors, and computer controls and analysis models. However, the interpretation of the thermal data for the complexities of the solid rocket motor requires further lab testing. Ultrasonic energy is an ideal proble for finding debonds. However, the rocket motor geometry is more difficult to test since it consists of a steel case which is an acoustic resonator with insulation which is a laminated acoustic absorber. Recent tests by LaRC on a delamination problem of the X-29 R&D aircraft show that significant improvements in resolution can be achieved by methods which have the potential to remove the steel case from the signal and concentrate on the weak insulation energy.

The Panel recommends that NASA should emphasize development of NDE techniques for assistance in qualifying critical STS elements.

## C. Reliability and Probabilistic Risk Assessment

There is a distinction between "reliability" which has a generally accepted definition as the probability a device will operate for a specified period under specified conditions, and "reliability engineering" which is a much broader and more appropriate term to describe a part of the design process. Reliability engineering is that portion of the design process which concerns itself with assuring that the hardware will perform as intended. It utilizes such analytical tools as the Failure Modes and Effects Analyses and the Critical Items List to focus designers' and management's attention on the relatively few failures which can have catastrophic results so that they can be eliminated from the design or their effects can be mitigated. There is also the responsibility for assuring that a vigorous process of recurrence control is applied to design related failures. It assures that proven or tested parts and materials

are selected and emphasizes design techniques such as derating and redundancy. Reliability Engineering sometimes utilizes statistical tools to quantify probabilities. The concept of probability when one is dealing with extremely low probabilities is best described as a measure of the odds of a fair bet on whether or not the event will occur. These odds are usually derived from a combination of expert opinion and of operating experience, and change with experiences. As stated by Dr. Harold W. Lewis, in his paper "Probabilistic Risk Assessment Merits and Limitations":

> "It also serves as a systematic means for the quantification of the performance of a plant under upset conditions, and thereby is a means for the identification of weak points in design or operation . . . the major need . . . is a systematic purging of the conservative influence on the conduct of probability risk assessment, so that the results (including the uncertainties) are given generally understood meaning."

## VI. SPACE STATION PROGRAM

### A. Background

The Challenger accident has forced reconsideration of important space policy issues including the proposed Space Station. Whereas NASA, after many months of intensive Phase B definition studies, had established what it believed to be a "baseline configuration" now finds this to be wanting in several respects. The extensive extravehicular activity planned for assembly and maintenance is now considered beyond that to be feasible or safe. Also the Shuttle performance (payload pounds to orbit) has deteriorated somewhat and the flight rates envisioned are now considered unreasonable. The accident also raises concerns about the escape and rescue philosophy that dominated the early concepts. All of this led to the formation within NASA of task forces charged to review the design and operational concepts, including Center assignments and management responsibilities.

The Panel offers the following observations:

1. The Panel endorses the initiative to simplify the Space Station design and reduce the extent of manned assembly in orbit.

2. The Panel suggests that expendable launch vehicles (ELVs) of greater performance than the Shuttle be included in the launch stable inasmuch as such vehicles may emerge from other national programs such as Strategic Defense Initiative.

3. The Panel recognizes the problems associated with the "safe haven" and "life boat" concepts and suggests that both options may be required to satisfy ultimate safety requirements.

4. A concern has been registered that the computer systems being considered for the Space Station may not be taking into

consideration evolutionary changes that will inevitably evolve in the industry in the next two decades. The Panel suggests the system be designed to allow for the replacement of components as new technology develops. A 32-bit architecture should be mandatory as well as a standard bus.

We appreciate that many of the systems being explored for the space station are in a state of flux and that some of the concerns expressed here may already be under scrutiny. It is intended that many of these areas will be reviewed by the ASAP in the future.

B. Management

Reorganizational concepts emphasize that overall program guidance will be centered at NASA Headquarters, Washington, DC, under the Space Station Office directed by the Associate Administrator for Space Station. Day-to-day direction and control of the program will be conducted by the Program Director who heads the Space Station Program Office (SSPO) located in Washington, DC. Detailed performance of the development activities are assigned to NASA field centers. Assignments for specific areas are as follows:

Electric Power System.....Lewis Research Center
Data Management .....Johnson Space Center
Thermal Control
*Internal.....Marshall Space Flight Center
*External.....Johnson Space Center
*(These refer to pressurized and unpressurized areas)
Communication.....Johnson Space Center
Internal Audio and Video.....Marshall Space Flight Center
Guidance, Navigation and Control.....Johnson Space Center
Environmental Control/Support..Marshall Space Flight Center
EVA Systems.....Johnson Space Center
Man Systems.....Marshall Space Flight Center

User Servicing.....Goddard Space Flight Center
Assembly and External Systems
Maintenance.....Johnson Space Center
Mechanisms/Gimbals.....N/A

An Architectural Control Document (ACD) responsibility is assigned to Johnson Space Center. This responsibiity encompasses all functions and components of the system--inside and outside--with respect to the standard responsibilities of being the ACD agent. Marshall Space Flight Center has the design and engineering responsibility for assigned systems components consistent with the ACD documentation. JSC retains end-to-end system analysis and verification responsibility. The foregoing assignments to the various Centers impose special Space Station management requirements on the Headquarters Space Station office both as they regard program content and cost.

C. Technical and Resource Risks

From the point of view of Space Station safety there are three general categories of Space Station threats: hardware/ software, human performance, and logistics/resupply. In brief it would appear that these are some of the risks:

1. Human performance errors should be a major concern of Space Station design and operation.

2. The docking, electrical, flight control, and instrument systems have great potential for adversely affecting Space Station operations.

3. A major logistics/resupply threat is the unreliability of launch vehicles.

The baseline Space Station program associated with the "build-to-cost" concept is a resource risk. The difference

between the stated $8 billion cost and the resources needed to achieve the current requirements (in the request for proposal due out in early 1987) is sizeable. These technical and resource risks result from such things as the following:

1. Compatibility between the current assembly scenario for the Space Station baseline configuration and the transportation system this Nation will have in the early to mid 1990s.

2. Extensive Shuttle-based and time-constrained extravehicular activity required for assembly and maintenance of the Space Station baseline configuration.

3. Adequacy of safety margin provided by the "safe haven" and/or "life boat" concepts currently considered for the Space Station configuration.

4. Adequacy of the proposed assembly scenario for the Space Station baseline configuration to support early scientific utilization.

## D. Space Station Computer Systems

The Space Station designs developed over the next 18 months will impact the Station's utilization and safety for probably two decades. It is thus particularly important to ensure that the utmost care and planning go into the design. It is, therefore, appropriate for the Panel to investigate the planning. This preliminary report is, therefore, more a statement of principles than a detailed set of findings. The examination of this subject will continue during 1987.

### Design Evolution

Almost nothing changes as rapidly as the state of the art of

computer hardware systems. We can predict with great certainty that any of today's computer systems chosen as the basis for the Space Station will be out of date before the first launch of the Station's components, and that three or four generations of computers will pass before the Station becomes obsolete. The same will be true of other components as well, of course, but to a lesser extent. It is thus essential that the Station be designed for evolution so that components can be replaced and extended as new technology permits. The costs of not being able to accommodate new technologies effectively can be expected to be very high; much higher than the savings that might be realized initially by cutting corners.

There are two things that can and should be done in planning for evolution. First, technology forecasts can give a hint of expected technology developments. One can then develop a set of technology vectors that point toward forthcoming technologies. The Station designs should not only fulfill immediate objectives, but take these technology vectors into account. More specifically, the Station designs should explicitly identify the technology vectors which they endeavor to take into account. Further, the extent to which the designs cover the forecasted technology vectors should be one of the evaluation criteria for proposed designs.

Technology forecasts can, however, predict neither the unusual breakthroughs that occasionally occur nor the applications that might arise from such breakthroughs. To try to minimize the inability of the Station to accommodate unexpected breakthroughs, one can perform a limitations analysis on the design decisions that are made to indicate the directions in which these decisions will impede future evolution. The designs accepted should be chosen to minimize the limitations they impose on future evolution.

Computer system areas in which these principles should be

observed for the Space Station include the following:

1. The implementation language chosen. (This should be a small number, probably no greater than two.)

2. The networking protocols chosen.

3. The communication media chosen.

4. The instruction set architectures chosen. (There may justifiably be two or three needed.)

5. The bus structures chosen.

Of particular immediate concern is the selection of the instruction-set architecture, which will be made in the near future. There have been some indications that a 16 bit architecture or an architecture that will be available from only a single vendor might be chosen. A decision for either of these is cause for considerable concern. Long before the Station is placed in orbit, 32-bit architectures will be the standard of the industry. Also, reliance on a single vendor has many well-known disadvantages. The requirements developed by NASA for the computer structures for the Space Station should take these concerns into account.

Status and Areas Needing Study

The implementation language chosen can buffer many changes in the underlying hardware as programs can be recompiled to operate with new hardware as it is developed. NASA's decision to adopt Ada as its principal implementation language is a very good decision. Ada is basically a good language; incorporating many modern software engineering concepts and having excellent extensibility capabilities. It is just now maturing, and will be a stable mature language long before the Station is ready for

launch. Due to DOD's emphasis on standardization, compilers for any architecture the Station is likely to adopt will be available and the porting of code to new processors will be straightforward. Moreover, its life time will exceed that of the Station.

There has not been time to study the other areas mentioned more than superficially, nonetheless there is concern from the preliminary information obtained that unnecessarily limiting decisions might be made. These areas will be investigated further in the coming year.

Automation and Robotics in the Space Station

The observations and comments are made above with respect to the computing resources of the Station are equally applicable to automation and robotics capabilities. This is another area which needs attention during the coming year.

Findings:

1. The design choices for the Station's computer systems that will be made over the next 18 months will significantly affect the utilization and safety of the Station.

2. There are indications that a 16-bit architecture might be chosen for the Space Station computer system.

3. Technology forecasts and limitations analysis can aid in design decisions that will permit the evolution of the station computer capability as technology advances.

Recommendations:

The Station's computer systems should be designed so as to

permit evolution of capability as technology advances. Specifically, a 32-bit architecture and industry standard bus should be selected.

The requirements and specifications developed by NASA for the computer structure for the station should recognize the future standardization of the industry of the 32-bit architecture and the inadvisability of locking into a single-source architecture.

E. Life Sciences

Specifically those Life Science projects needed to assure success of long duration human residence in space must be scheduled and funded in a timely fashion to support future long duration missions. The Life Sciences Advisory Committee (LSAC) is pondering the best way to gain knowledge on the proper path to follow in gaining what it perceives as its objectives for the Space Station. Life Sciences probably needs to establish a more effective mechanism within NASA so that it can compete for available funds.

F. Lessons Learned

This is to reiterate the same theme noted in our last year's annual report: "Since there are many similarities between the STS and Space Station programs, looking into the "lessons learned" relating to the early days of the Shuttle might better define Space Station actions to preclude missteps. This understanding of possible pitfalls for the Space Station program might include insight as to what not to do, thereby preventing inefficient use of resources (money, people, schedule)."

In support of this, the the Panel Staff Director, using data collected through Panel factfinding, prepared and issued a panel document "Lessons Learned--An Experience Data Base for Space Design, Test and Flight Operations." The following taken from

the report's preface is the story:

> "This document summarizes specific and generic lessons that have been "learned" as a result of the factfinding 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.

## VII. NASA AERONAUTICS

The NASA emphasis on aeronautical flight activities has increased significantly with the award of major contracts for development of the National Aero-Space Plane (NASP); the roll-out of the X-Wing vehicle; the accelerated flight envelope extension and the addition of the high angle-of-attack investigation to the X-29 aircraft program; testing of the gearless ducted fan engine and the advanced prop fan program; plans to flight test a variable-sweep oblique wing mounted on an F-8 Crusader; and the joined-wing flight test program. The Panel attention was directed primarily to the X-Wing since it has entered the Flight Readiness Review phase with the first flight scheduled for sometime in 1987. The X-29A technology demonstration flight program was reviewed periodically with particular attention paid to the next phases of the flight program. The NASP program is aimed at a manned flight demonstration and is ambitious in both a technical and financial sense and therefore is also being reviewed for general familiarization of the program plans for safety and for early identification of safety issues.

Other NASA safety-related aircraft activities that were reviewed during the year were the NASA/FAA airborne wind shear program, the Takeoff Performance and Monitoring System effort, the Heavy Rain Effects on Aircraft Performance program, and problems associated with certification of General Aviation Aircraft that use laminar flow airfoils.

### A. Flight Operations Management

The appointment of a new Director, Aircraft Management at Headquarters places the flight management staff in a better position to be recognized as a major player in assuring continued flight safety within NASA's administrative organization. In order to ensure that flight safety remains a paramount objective of NASA, flight operations requires continued representation at

the highest management level to assure that efforts to maintain and improve operational safety receive appropriate attention. A similar type of situation exists regarding flight operations offices at the various centers except for the Ames/Dryden Flight Research Facility.

Recommendations:

The Panel recommends that NASA assure that the Headquarters Flight Operations Management Office and those at the Centers have proper recognition and ready access to their senior management.

## B. The Rotor Systems Research Aircraft//X-Wing Flight Test Program (RSRA/X-Wing)

The objective of the RSRA/X-Wing program is the successful demonstration of the capability to design a rotor system that can be flown and controlled in either a fixed wing or a rotory wing mode; and that can be converted from one mode to the other without loss of lift or control during the conversion. The selection of the RSRA vehicle was based on safety considerations--the vehicle can be flown as a fixed wing airplane (a separate conventional wing) independent of the rotory system. Since the rotory wing incorporates a circulation control system and depends upon exacting modulation of blowing through slots in the blades, it absolutely requires a digital automatic (fly-by-wire) flight control system. The conventional fixed wing utilizes a standard manual control system; however, there are interconnects between the two systems which add to the complexity of the overall system.

Of primary concern is the raising of the vertical center-of-gravity of the vehicle by some 18 inches as compared with the standard RSRA vehicle. This situation is having a pronounced effect on the structuring of the flight test program and the planning of the Flight Readiness Review activities. The current

plan is to build up to the first rotor-on (stopped) flight with four flights beginning at 28,000 pounds with the rotor and associated equipment off; then increasing the vertical position of the center of gravity and aircraft weight up to the rotor-on gross weight and center of gravity position. Control of the vehicle will be maintained using the mechanical system.

1. Flight Readiness Review: The flight readiness review (FRR) of the RSRA/X-Wing has been structured to include five preliminary reviews and a final meeting of the committee just prior to the first flight. The X-Wing flight test program is to be conducted in two phases. The first phase includes testing of five aircraft configurations with a buildup in weight and vertical C.G. position. The first flight will be of a configuration that very closely duplicates the fixed wing flight of the original RSRA aircraft and will be without rotor, hub, compressor, standpipe or standpipe support structure. The next two flights will add the compressor and rotor support structure and the final two configurations will be with the hub and two blades followed by the final Phase I test of four-bladed configuration (all fixed unloaded rotor). The full up loaded rotor testing will begin in Phase II. The six scheduled flight readiness reviews are:

1. Vehicle dynamics and flight control.
2. Unique X-Wing structure, power train, and other systems.
3. Handling qualities.
4. System safety, reliability and quality assurance, emerging escape system, flight test plans, and project pilots report.
5. A wrap-up session for assessment of actions taken since the previous reviews on the respective subjects.
6. A final review of all requests for actions generated from all previous sessions.

The Flight Readiness Review Board (FRRB) is structured in a

way that will assure complete and adequate coverage of the X-Wing design activity. Included should be an evaluation and assessment of all data from the various X-Wing test and simulation activities.

The first session of the Flight Readiness Review Board was held on July 28-30, 1986, and included an assessment of the flight controls and vehicle dynamics.

There were a number of action items that the Panel believes to be critical--ones that should be monitored closely. These include the following:

1. Adequate correlation of dynamic analysis with the stopped rotor wind tunnel tests is not clear. Also, the plan for showing a wind tunnel/analytic correlation should be improved.

2. The structural divergence prediction from the tunnel tests were not conclusive--some differences in the data are not accounted for.

3. The flutter and divergence analyses results performed by Northrop need further refinement. It is difficult to address the meaning of the results of the flutter analysis.

4 Various aerodynamic models for downwash interference are being used. Results from the powered model tests are not in agreement with predicted analytical model results.

5. Current Northrop controls/dynamic analysis is conducted for 200 kt/2.50 angle of attack. The analytical method may not cover 140 kts - 250 kts of the flight envelope.

6. Better definition of the telemetering requirements with

emphasis on software requirements for automatic monitoring is needed.

There is a need for a well thought-out written plan that describes the expansion of the flight envelope in a methodical manner to ensure avoidance of flutter divergence and tail buffet. The flight data should be correlated with the analytical and wind tunnel test data at each point as the envelope expansion proceeds.

2. Propulsion System Test Bed (PSTB) and Other Simulation: The PSTB is an "iron bird" representation of the X-Wing Rotor system, the Allison T-51 engines, transmission, compressor and pneumatic system, and the rotory wing flight control system. The mechanical architecture is identical to the aircraft and therefore serves the purpose of gaining operating experience during the period that the aircraft is being fabricated. Design problems may be discovered in time to formulate modifications prior to the completion and ground testing of the aircraft. The PSTB is scheduled for 50 hours of testing of operational adequacy and another 30 hours of endurance testing for a total of 80 hours. The aircraft will be subjected to 25 hours of tie-down testing which, in addition to the PSTB hours, should be sufficient to ensure the absence of weak points in the design. The aircraft is only programmed for 40 hours of flight time; the successful completion of 80 hours of PSTB testing will provide a great deal of confidence in the mechanical design of the system. The PSTB testing is programmed to lead flight testing by no less than 2 to 1 in total numbers of operating hours.

Another important aspect of the PSTB is the verification of the adequacy of the rotor wing control system. The digital automatic flight control system of the X-Wing is a most complex design and the ability to test the algorithms with the actual rotor dynamic response is a valuable asset to the program that is needed to verify the veracity of the computer simulation. The

Vehicle Management System Laboratory (VMSL) including the systems Integration Test Stand (SITS) and the Vehicle Motion Simulation (VMS) are being utilized to develop the flight control system software which will be incorporated in the PSTB before the rotary wing flight test begins.

There have been a number of problems that have been discovered this year during the PSTB testing. The gap at the middle seal between the rotating inner cylinder and the stationary middle cylinder closed causing metal-to-metal contact which could have caused failure of the hub if it had happened on the flight vehicle. The seal design had to be modified to correct the situation. Another problem was the failure of the flexible duct in the pneumatic system caused by a faulty clamp. Excessive overboard venting of the air/oil from the compressor gearbox has been observed, as well as excessive heating of the compressor. The most serious problem was a gearbox failure which occurred in the throughshaft to the compressor gearbox bearing assembly.

Finding:

It is apparent that due to the unique equipment and designs of the heavy mechanical equipment of the X-Wing, oil starvation, or vibration problems can add to fatigue failures. The PSTB has already proven invaluable detecting flaws that otherwise may not have been identified before the flight program.

Recommendation:

Additional running time be allocated to the PSTB.

3. Powered Wind Tunnel Model Testing: An important element of the X-Wing program is the wind tunnel testing of a 1/5 scale powered model. The results of the tunnel test are used in the simulation programs for predicting the stability characteristics

of the vehicle and also for the prediction of the flight loads needed to verify the structural integrity of the rotor system. The tunnel results for the fixed rotor have not agreed well with the analytically predicted values. The Panel will continue to monitor this situation during the remainder of the FRR phase.

4. X-Wing Safety: The Panel found the safety effort for the program has been increased substantially over the last year. In addition to the hazard analysis, a top-down event model has been generated to provide an analytic and systematic safety analysis. Of particular concern to the Panel is the emergency escape system which includes a blade severance device.

The Panel recommends that NASA should complete fault and failure analysis to provide an adequate level of confidence for its use.

C. X-29 Flight Test Program

1. Current Status: The X-29 aircraft has completed over a hundred flights since the flight test began on December 14, 1984. The program has been remarkable when measured by the absence of safety or other significant flight problems. This excellent record is particularly impressive when one considers the advanced technologies that are integrated into the design and are being tested for the first time. They include the following:

a. An aeroelasticly tailored forward swept wing
b. Close-coupled canards
c. A thin supercritical wing airfoil
d. Discrete variable camber
e. A three-surface pitch control
f. A high degree of static instability
g. An advanced fly-by-wire flight control system

This Panel believes that Defense Advanced Research Projects

Agency (DARPA), the Air Force program office, the NASA flight test team, and the Grumman Aerospace Corporation should be commended for this well conceived and executed effort.

With so many new technologies involved, the first phase of the flight test program has been engaged in a meticulous expanding of the flight envelope. Fundamental to the program in examining the various technologies is the demonstration of their combined relationships at all flight regimes normally experienced by fighter type aircraft--subsonic, transonic, supersonic, and at a wide range of altitudes.

2. Flight Test Methods: Of particular concern during testing of the aircraft is its high level of longitudinal instability. Control of this extreme instability made special demands on the X-29 flight control system design. For example, extensive lead compensation, high canard surface displacement, and rate capability were required. In addition, traditional flight control system stability margins had to be relaxed. These margins were reduced to 3 db high-frequency gain margin and 22.5 degree phase margin, which are half of the typical design values. This compromise could only be accepted in the presence of real-time monitoring and on-line analysis of the flight test data.

In this connection, since the consequences of pitch control surface limiting or extended periods of surface rate limiting in the X-29 can be disastrous (the time to double attitude pitch angle is .15 second), flight testing of the aircraft requires special approaches and methods. The flight control considerations related to the extreme instability, wing structural divergence, and aerolastic effects dictated a cautious incremental approach to envelope expansion with thorough analysis of all of the data.

Both traditional and specialized flight test approaches are

used on the X-29 program to monitor overall aircraft and control system stability during envelope expansion. A key element of the approach is an accurate, hardware-in-the-loop simulation of the X-29. The extraction of accurate longitudinal stability derivatives with three active control surfaces and the extreme pitch instability is very difficult. Because of these difficulties and the fact that the flight control system clearly dominates the X-29 responses, direct monitoring of the health of the flight control system as a flight safety issue has taken precedence over all other aspects of monitoring.

In general, the agreement between the flight data and the predicted data has been quite good. In fact, the quality of the real-time frequency response data has been good enough that monitoring of stability margins has become the primary flight safety tool during envelope expansion. A principal advantage to this method is that the effects of any nonlinearities, for example, rate limits, hysteresis, or transport delay, are immediately reflected in the measured control system stability margins.

3. Handling Quality/Safety Relationships: As a direct result of precautions taken in the design of the flight control system to ensure flight safety, the handling qualities of the aircraft have been somewhat degraded. The X-29 has half the natural frequency of the F-18 feel system and can fairly be labelled "slow." If the time delay measurements are related to stick position, not stick force, which eliminates the feel system, then the correlation with the military specification boundaries and the pilot ratings is more reasonable. The X-29 appears to have significant time delays but, certainly in the roll axis, does not exhibit the flying qualities problems expected with these delay levels. No pilot induced oscillation (PIO) tendency has been observed in the roll axis during precision formation tasks, for example. The X-29 results bring into the question the present MIL-8785C requirements on time

delay and the more general questions of whether stick force or position is the important parameter for precision tasks. The X-29 example also gives some indication that "slow" feel systems may indeed be a beneficial element with which the control system designer can smooth out high gain system deficiencies without paying the penalty of increased time delay.

In summary, the X-29 results raise several fundamental flying qualities issues which are potentially important to the design of future flight control systems. As a result of the X-29 experience, a spin-off flying qualities experiment is now underway using the Air Force variable stability NT-33 aircraft to help resolve these issues.

4. Langley Support for X-29 High Angle of Attack Maneuverability Program: The second X-29, by current plan, is to be used for exploration of fighter maneuverability at very high angles of attack. NASA Langley, coordinating its work with engineers of the Dryden Flight Research Facility, is supporting this program with free-flight model studies. The first X-29, now flying at Dryden, has been arbitrarily restricted to a maximum angle of attack of 20 degrees.

Throughout the Langley program a continuing effort will be made to improve control laws of the digital avionics to enhance system capability, suitability, and safety.

The Panel believes this research will further the achievement of flight safety during both high angle-of-attack operations and recovery in the case of accidental spins.

## D. National Aero-Space Plane (NASP) Safety Considerations

The National Aero-Space Plane (NASP) program has completed its conceptual phase (Phase I) and is currently directed towards a future flight demonstration. The schedule for development of

the manned hypersonic research vehicle is divided into two phases. Phase II (in progress) is primarily directed at a propulsion system development, technology advancement (aerodynamic codes, materials, structures, etc.) and vehicle configuration analysis studies. The Phase III (to follow in 1989) is slated for fabrication and flight testing of the vehicle for flight at speeds up to Mach 25.

One important key to this program is the ability to predict internal and external flow fields. A major technical issue is the establishment of an adequate data base and overall validation of the design of the experimental manned transatmospheric research vehicle since the full-scale vehicle cannot be groundtested through the full-range of its operational flight speeds, Mach numbers, and altitudes. A thorough evaluation of existing ground research facilities, their modernization and upgrading needs, the need for new ground facilities, as well as possible flight research facility options must be established and the corresponding budget requirements defined. This facility evaluation is necessary in order to ensure the ability to verify analytically determined design parameters associated with uncertainties such as the interaction between vehicle and engine flow fields, inlet region effects of forebody crossflow and viscous influences, inlet spillage flow effects with angle of attack variations, dynamic interactions between the engine operation and the vehicle motion, flight control dynamic responses to nozzle lift/thrust and pitching moment variation, etc. The ability to determine the characteristics and parameters of a complex flow field accurately has been greatly improved through the use of high-speed computer simulation that uses numerical solution methods. Traditionally, analytical methods have been used in the initial design of air vehicle and propulsion systems but the final design has always required and has been the result of extensive wind tunnel and flight tests. With the development of advanced computational capability, significantly less hardware testing will be required; however,

the computational tools are far from perfect and the code development must be accompanied by a vigorous and systematic program to provide comprehensive experimental verification and correlation of analytical predictions. Confidence in the codes can only be gained by a carefully structured verification program expanded to cover the full range of configurations and aerodynamic/thermodynamic phenomena to which the computational procedures are applied. It is important to realize that experimental verification is a vital element of the overall computational aerodynamics program, and it must receive at least equal emphasis to the development of the codes and computer facilities themselves. To do otherwise will result in less than desirable return on investment and could, if experimental verification is slighted, waste a portion of a vital national resource and increase the likelihood of a flight mishap.

The use of large quantities of liquid hydrogen over relative long flight durations at high mach numbers where extreme heating on the exterior of the vehicle and low cryogentic temperatures of the interior will pose a set of unique structural challenges and basic safety questions and concerns which will undoubtedly provide ammunition for vigorous debate at and before the Flight Safety Board grants approval for the first high mach number manned flight.

## E. NASA Safety-Related Aircraft Programs

There are several NASA activities that are directly related to flight safety that have been reviewed by the Panel during the year. The Panel supports the continued research activities as noted below.

1. Takeoff Performance and Monitoring System: In response to the Airliness Pilots Association (ALPA) and SAE S-7, a takeoff performance monitoring system (TOPMS) has now been implemented for both pilot and copilot positions in the Langley fixed-base

simulation for the Transport Systems Research Vehicle (TSRV) (a Boeing 737). The display is now being evaluated and developed using Langley research pilots, and it looks very promising. ALPA and industry transport pilots will soon be invited to evaluate it. The next step will be to implement the display in the research cockpit of the actual B-737 airplane. The purpose of TOPMS is to provide guidance to the pilot for takeoffs and aborts including cues for helping make the critical decision. The TSRV simulation is to qualitatively evaluate the system and is utilized to solicit pilot suggestions for improvements.

2. NASA/FAA Airborne Wind Shear 5-Year Program: The seriousness of the microburst wind shear problem is now recognized as a highly significant aviation hazard, although encounters are infrequent. It has been the causal factor in 27 U.S. accidents since 1964, resulting in more than 50% of U.S. accident fatalities during the 1975-1985 time period. The object of the NASA/FAA program is to develop and demonstrate technology for low altitude wind shear risk reduction through airborne detection, warning, avoidance and/or survivability. The basic requirement is to provide an airborne capability that promotes flight crew awareness of the presence of wind shear or microburst phenomena with enough time to avoid the affected area of escape from the encounter. The program has three primary elements: (1) the characterization of the hazard, including the modeling of the wind shear physics and its impact on flight characteristics; (2) the development of optimum sensor technology, which includes the use of doppler radar, lidar, and the fusion of the two; and (3) the flight management system requirements, displays for the pilot, procedures and other techniques that can aid the pilot in recognizing the presence and severity of shear in time for appropriate action.

3. Heavy Rain Effects on Aircraft Performance: Heavy rain associated with downbursts has been found to cause a significant loss in maximum lift (premature stall), particularly for high

lift (flaps extended) configurations. Wind tunnel tests of a high lift configuration with an NACA 64-210 airfoil have shown significant lift and drag changes with rainfall rate at relatively low Reynolds number. Tests with a larger model will be performed on the Langley outdoor landing loads track near full-scale conditions.

4. Certification of General Aviation Aircraft Using Laminar Flow Airfoils: With the advent of very smooth and stiff composite materials for aircraft construction there has, appropriately, been an increased application of laminar flow airfoils to minimize drag, particularly to general aviation aircraft. These airfoils are shaped to have, in cruise, a falling (favorable) pressure gradient from the leading edge as far aft as possible over the top, or suction side, of the lifting surface. This tends to keep the boundary layer from slowing due to friction and becoming turbulent or separating from the surface. These airfoils have generally been considered highly sensitive to surface irregularities and contamination, resulting in adverse changes in lift and drag.

Surprisingly, recent flight investigations have shown extensive laminar flow over the wings of several general aviation aircraft using these airfoils, even with small-scale contamination (bugs, dirt, light rain, etc.), or disturbances such as caused by the propeller slipstream. Propellers with such sections also have shown sizeable areas of laminar flow. However, heavy rain, large bugs or deposits of mud, de-icer boots, leading edge or surface damage, severe turbulence, or hard maneuvers may cause breakdown of the laminar flow into turbulent flow, thus increasing drag. Of greater concern, however, is that laminar breakdown may lead to premature stall (perhaps asymmetrically), reduced lift curve slope of wing and tail surfaces (leading to reduced stability), and a reduced control effectiveness. These effects could occur abruptly and unexpectedly.

Because of these potential uncertainties, the FAA will review the current Part 23 Airworthiness Standards and the certification flight test requirements. One test technique is to apply "trip strips" at the leading edge of lifting surfaces to induce and ensure non-laminar boundary layer conditions to establish baseline characteristics. These "trips" could be applied in various locations on the aircraft to examine likely situations. The aircraft involved would probably be required to meet the minimum standards for Part 23 aircraft in the worst case.

FAA and NASA plan a joint flight investigation with a single engine general aviation aircraft having laminar flow airfoil sections on wing and tail surfaces as well as on the propeller. Flight test requirements and additions to the Standards are expected to result, but results will not be immediate. In the meantime, special consideration will have to be given each case.

## IX. APPENDICES

This section includes an overview of the Panel membership, activities during Calendar Year 1986, proposed activities for 1987, and the detailed NASA response to the Panel's annual report, dated January 1986, along with a current status of last year's open actions. This information is provided under the following three sections:

A. Panel Membership/Consultants/Staff
B. Panel Activities During Calendar Year 1986
C. Panel Proposed Activities Calendar Year 1987
D. NASA's Response to Panel's Annual Report

### A. Panel Membership/Consultants/Staff

The Panel membership has had significant changes during this past year. The current membership is listed below.

Mr. Joseph F. Sutter, former Executive Vice President of the Boeing Commercial Airplane Company, now an aerospace consultant, was selected to succeed Mr. John C. Brizendine as the new Chairperson of the Aerospace Safety Advisory Panel.

Mr. Norman R. Parmet was selected as the Panel's Deputy Chairperson.

Dr. Richard A. Volz, Professor/Director Robotics Research and Systems Division, University of Michigan, was selected to succeed Dr. Richard H. Battin covering the computer hardware and software disciplines.

Dr. Charles M. Overbey, Director of the Human Performance Division, National Transportation Safety Board, was selected as a consultant to the Panel to cover human factors associated with ground and flight operations.

Panel membership is set by statute at no more than nine members with the number of consultants commensurate with required activities. None of the current Panel members are NASA personnel. In addition, the new NASA Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance, George A. Rodney, is the ex-officio member of the Panel.

## CHAIRMAN

Joseph F. Sutter
Aerospace Consultant
Retired Executive Vice President
Boeing Commercial Airplane Company

Harold M. Agnew
Consultant
Retired President of
General Atomic

Charles J. Donlan
Consultant, Institute
for Defense Analysis

Gerard W. Elverum, Jr.
Vice President/General Mgr.
Applied Technology Group
TRW Space Technology Group

John F. McDonald
Aeronautical Consultant
Retired Vice President,
Maintenance and Engineering
TigerAir, Inc.

Norman R. Parmet
Aeronautical Consultant
Retired Vice President,
Engineering and Quality
Assurance, TWA

John G. Stewart
Assistant General Manager
Tennessee Valley Authority

Melvin Stone
Aeronautical Consultant
Retired Director, Structural
Mechanics, Douglas Aircraft

Richard A. Volz
Professor and Director
Robot Systems Division
University of Michigan

## Panel Consultants

Herbert E. Grier
Consultant
Retired Senior Vice
President, EG&G, Inc.

Seymour C. Himmel
Consultant
Retired Associate Director,
NASA Lewis Research Center

Norris J. Krone
Executive Director
University of Maryland
Research Foundation

Charles M. Overbey
Human Performance Division
National Transportation
Safety Board

John P. Reeder
Former Chief, Research
Aircraft Flight Division
NASA Langley Research Center

## Ex-Officio Member

George A. Rodney
NASA
Associate Administrator for
Safety, Reliability, Maintainability
and Quality Assurance

## Staff

Gilbert L. Roth
NASA
Staff Director

Susan C. Esmacher
NASA
Staff Assistant

B. PANEL ACTIVITIES FOR CALENDAR YEAR 1986

| DATE | SITE | SUBJECT |
|---|---|---|
| 2/3-4-5 | Ames Research Center | Life Sciences Advisory Committee Meeting |
| 2/11 | HQ | Statutory Annual ASAP meeting with Administrator |
| 2/21 | Langley Research Center | X-29A Aircraft |
| 3/11 | Langley Research Center Control | Shuttle Landing Gear and Tires, Structures, Stability and |
| 3/10-13 | Sikorsky Pratt & Whitney West Palm Beach | X-Wing Propulsion Test Program and Safety |
| 3/18 | MSFC | STS Element Status |
| 4/1-3 | JSC | Space Shuttle, Space Station, Aircraft Operations |
| 4/10 | Lewis Research Center | Centaur management and technical status |
| 4/22 | Lewis Research Center | Centaur program discussion with staff from House HUD-Independent Agencies subcommittee |
| 4/29-30 | PAFB, FL | Intercenter Aircraft Operations Panel |
| 4/30-5/1 | HQ | STS, Space Station Logistics |
| 5/8 | U.S. Senate | Senate Testimony regarding ASAP Annual report and "where do we go from here." |
| 5/15-16 | HQ | Life Sciences Advisory Committee Meeting |
| 5/15 | U.S. House accident | Testimony concerning 51L |
| 5/20 | Rocketdyne Canoga Park, CA | SSME status and activities for first flight |

| | | |
|---|---|---|
| 5/21 | Vandenberg Air Force Base, CA | H2 exhaust duct problem, activities leading to first mission, SPC operations. |
| 5/21 | U.S. House | Quality Assurance Hearing |
| 5/21 | Langley Research Center | National Aerospace Plane |
| 5/21-22 | Sikorsky, CT | X-Wing Discussions on Flight Simulators and Rotor Blades |
| 6/17-19 | MSFC | SRM Redesign, SSME status |
| 6/19-20 | JSC | Space Station Engineering and Operations Safety Review |
| 7/1 | Vandenberg Air Force Base, CA | Hydrogen Exhaust Problem |
| 7/24 | HQ | Systems Safety |
| 7/24 | JSC | Space Station Engineering and Operation Safety Review |
| 7/24 | Lewis Research Center | National Aerospace Plane (propulsion system) |
| 7/29-30 | Sikorsky, CT | X-Wing RSRA Flight Readiness Review |
| 8/7-8 | HQ | Life Sciences Advisory Committee Meeting |
| 8/12-13 | Sikorsky, CT | X-Wing RSRA Flight Readiness Review |
| 8/19 | Sikorsky, CT | X-Wing Safety program |
| 8/20 | HQ | Probabilistic Risk Assessment Approach |
| 8/25 | HQ | ASAP Activities |
| 8/26-27 | KSC | NASA/SPC Launch Processing Operations |
| 9/23-25 | Denver, CO Martin-Marietta | FMEA/CIL, Space Station Safety |
| 9/23 | MSFC | Probabilistic Risk Assessment |