PRESENTATION 4.4.1

LESSONS LEARNED AND THEIR APPLICATION TO PROGRAM DEVELOPMENT AND CULTURAL ISSUES

BY

GILBERT L. ROTH
STAFF DIRECTOR
AEROSPACE SAFETY ADVISORY PANEL
NASA HEADQUARTERS

SPACE TRANSPORTATION PROPULSION TECHNOLOGY SYMPOSIUM

PENNSYLVANIA STATE UNIVERSITY

JUNE 27, 1990

LESSONS LEARNED
AND THEIR APPLICATION TO
PROGRAM DEVELOPMENT AND CULTURAL ISSUES

"POINT ONE"

The knowledge we use today is contained in an untold number of technical and managerial handbooks. This knowledge is derived from the known strengths and weaknesses experienced during the execution of programs and projects that are being used today. Tomorrow's handbooks will define many additional lessons that designers, test operators, management, and operational personnel will apply on such programs as the National AeroSpace Plane (NASP), the Space Station Freedom (SSF), and future launch vehicles. Before placing specific lessons learned and cultural issues before you, I believe a few introductory remarks are appropriate so that we all start off from a common reference point. Let us begin with a few well-known and generally accepted concepts: (Not everyone will agree or be happy with these!)

- The greatest lesson we seem to learn is that we seldom learn from lessons learned! What this indicates is our inability to present them in an appropriate way or .....

- The "Over and Under 40 Syndrome." That is, if you are under 40, it is difficult to believe that those over 40 have been through what "YOU" are going through; whereas those over 40 find it difficult to believe that everyone else may not already know of their weaknesses and more importantly of their successes! Lessons learned are in effect the history, the evolution of technical, scientific, and managerial advancement.

- The genesis of a useful safety tool is often a tragedy. In the aftermath of the Apollo Command Module Spacecraft fire of January 1967, the Congress of the United States, along with NASA, took a number of steps to resolve the many issues raised by that accident. One such step was the creation of the Aerospace Safety Advisory Panel (ASAP) by Congress. The Panel is charged with reviewing and assessing all NASA programs and projects with an emphasis on safety, reliability, and quality assurance. An excellent explanation of this was given by Alan Lovelace Acting NASA Administrator in May 1978:

  "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 the manufacturing practices, organizational structure, 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."

It is easy to see that the genesis of many of the design, test, operational, and management tools are derived from near-misses as well as tragedies.

"POINT TWO"

Although it may be somewhat difficult to separate program development and cultural issues, it is worthwhile to at least think of them separately in the beginning to understand their synergism in the end. First, let us consider cultural issues as they affect the thinking and actions of technical management and engineering.

Just as the American public was awed by the early flights made by the Wright Brothers in the first decade of the 20th century, they exhibited the same degree of amazement at the Russian's launching and orbiting the first Sputnik in October 1957. With the passage of time, the public takes for granted the continuation of these truly fantastic steps in the aerospace sciences and their implementation and application to our daily lives. Transmission of live real-time TV pictures are accepted; and if you ask one thousand viewers how it is accomplished, the answer is "I really am not sure, but it is there!" Airline transportation is accepted in the same way, and few people can remember taking a prop-driven plane from New York to Los Angeles or to London and all that it entailed. Now apply this to current and projected aerospace programs where the public expects...actually demands...that complex, beyond the state-of-the-art activities be conducted without mistakes, on-time at low cost, and provide useable and profitable spin-offs to earth-bound activities. What does this lead to?

- Horror when the Challenger accident occurred and a sweeping indictment against management and technical capability;
- How can we spend billions to put men and experiments in space when people are hungry and homeless here on earth?
- Additional oversight by outside agencies, including the Congress. What about Senator Gore's reasonable statement that "only through an annual authorization can Congress play a continuous oversight role effectively."
- The continuing argument over the appropriate mix of manned versus unmanned, reusable Shuttle versus Expendable Launch Vehicles, and government versus civilian space roles.

All of these affect the environment within which the current and future aeronautical and space ventures will have to operate. These affect resource availability to conduct every facet of the program and leads to another problem that has become a part of our lives.

Environmental concerns are no longer taken lightly. The impact of propulsion system effluents are emerging as a major determinant in the selection of propellants. Solid rocket motors are now viewed with some apprehension because of the acids and chlorine derivatives that are discharged from launch point to stratospheric altitudes as well as the other particulates. Cleaner burning propellants and oxidizers are being developed, and the use of hybrid rockets as well as more extensive use of liquid rockets are in the offering. Even the burning of waste propellants is now a controlled activity. The use of hydrazines and other sophisticated but toxic propulsion systems require additional care and feeding. In the coming years, the "environmental movement" will be

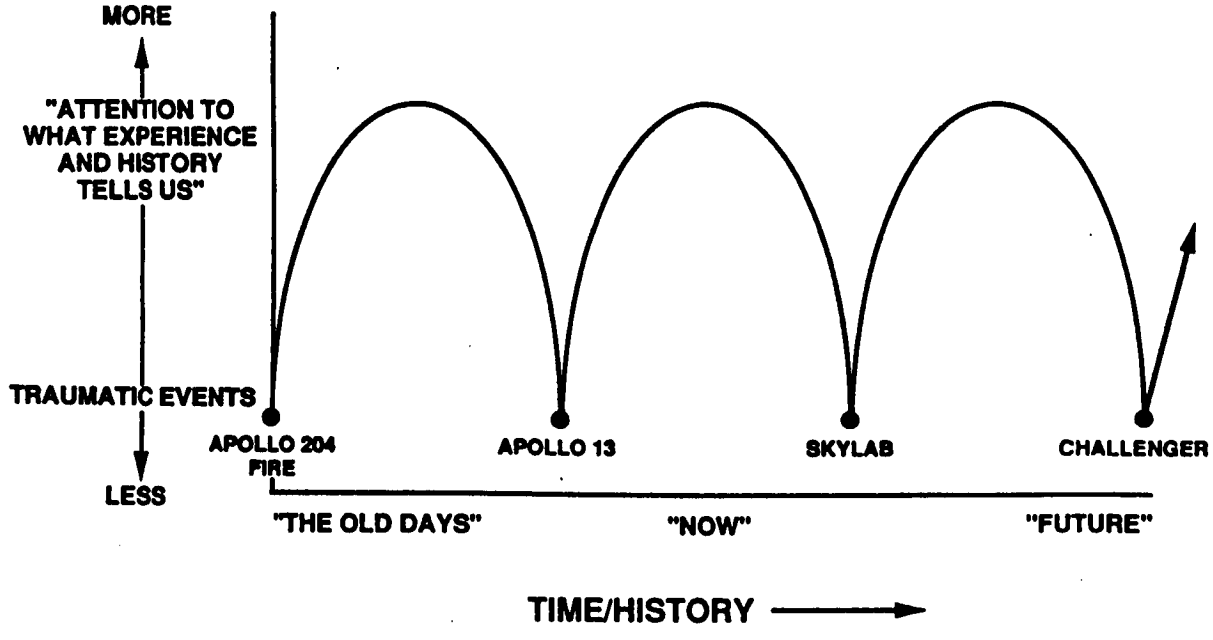
having an ever greater impact. The public's view of the world and man's affecting it is not confined to the United States, but is a world-wide concern.

In a totally different arena, look at the difference between the early spacecraft put into orbit by the United States and the USSR. The Apollo-Soyuz combined Russian-American missions conducted in the period July 15-24, 1975, showed some distinct differences:

- The androgynous USSR docking system versus the Apollo probe and drogue system;
- The use of solar panels rather than fuel cells;
- The use of 14.7-psia atmosphere versus 5-psia oxygen rich, and so on.

In effect, our spacecraft were somewhat more sophisticated and even, to a degree, chrome plated. Today, the Russian and American space vehicles are tending toward a more center-of-the-road in "chrome-plating." None-the-less, both of them do the job. In today's fiscal environment, any so-called excess in chrome-plating is not acceptable.

CULTURAL HISTORY SHOWS - - -



"POINT THREE"

Some typical lessons learned that deal with the four areas of interest:

- Requirements
- Technology/Performance/Operations
- Reliability/Safety
- Procurement/Contracting

are given here. They are, of course, only representative of so many others that each and everyone involved in aerospace design, development, test, and operations has perhaps experienced.

Requirements

Requirements come in many forms; for our purposes we will use a broad brush and look at technical specifications as well as technical management requirements at the start of a program. The reason? A lesson learned is: The future of a program is determined to a great extent by how it is started.

1. Initial system definition either was not accomplished by an orderly analysis process or effort, and was incomplete and inadequate. There were no continuing requirements to perform system analysis on selective basis during the acquisition phase. Critical evaluations should be made by the government and contractors in the early design stages concerning the specification requirements. They should be evaluated from both viewpoints--too tight, too loose. ("A Summary of Lessons Learned from Air Force Management Surveys," 1 June 1963).

2. Technical and management requirements must take into account the "Resource Conservation and Recovery Act" (RCRA was established in 1976 with amendments added in the 1980s). The development of advanced weapons systems and new aerospace technologies will be accompanied by new fuels, hybrid structural materials, and other unique chemicals as well as new processes, many of which have the potential for creating unacceptable health hazards. This continuous influx of new and exotic materials from the research, development, and acquisition pipeline brings attention to the first point in the process at which decisions need to be made to procure or not procure a specific material. (JANNAF Safety and Environmental Protection Subcommittee Workshop, 3 April 1989).

3. From a "Report to the Committee on Science and Technology, House of Representatives On Centaur Cost, Schedule and Performance Review," 1986:

The most significant reason for the problems experienced in the Centaur/Shuttle integration process was that, while we have two centers with considerable space flight experience, the prime center responsible for development of the Centaur had previously been involved in unmanned vehicle systems and now was responsible for providing complex vehicle systems that would fly within a manned vehicle. Significant

philosophical differences exist between a manned and unmanned vehicle regarding safety requirements and issues. The level of fault tolerance, fault isolation and system design, including increased redundancy, are considerably greater for manned missions.

More critically, the planning and design requirements associated with the Shuttle off-nominal and abort modes were not properly assessed at the start of the program. Program requirements that should have been designed into the vehicle system to prevent loss of life or loss of an Orbiter were developed after the flight hardware design was well under way.

Lessons Learned included:

For future systems, the safety process must be understood and considered in the basic design effort of the specific flight hardware commensurate with the philosophy that exists for our manned flight programs. Responsibility of the prime hardware contractor for safety should also be emphasized. Some of the other lessons learned items mentioned in this report are also a significant contributor to the safety process problem, i.e., getting all organizations involved in the program design process very early so that their requirements can be incorporated in the most effective manner. More manpower and resources should be allotted to complex, first-time payloads, posing unique safety hazards to the NSTS and crew early enough to support major program milestones such as a critical design review and phase II safety review.

Technology/Performance/Operations

Although propulsion systems and their components are but one of a number of independent yet integrated, members of a complete aerospace flight vehicle, propulsion systems are more often the focus of concern because:

- They are active,
- They have potential for fire, detonation, toxicity, and corrosion;
- They are often life limited and temperature sensitive; and
- They provide and are a major contributor to ascent capability, attitude control, and trajectory modification.

Typical propulsion interests are centered upon such items as:

- Solid Rockets - Propellant integrity, ignitor reliability, nozzle durability, safe handling, reuse, safe/arm systems, case insulation, ballistics.
- Liquid Rockets - Turbomachinery design and certification, red-lines for test and flight, leakage, sensors, reuse, engine controllers.
- Hybrids - all of the above

- Auxiliary Power Units - Reliability, maintainability, speed control, heat dissipation, restart, leakage.

Typical lessons learned are as follows:

1. A simple design change that lost an engine

Figure 1 shows a "straight forward" design change made to the SSME High Pressure Fuel Turbopump that was the cause of SSME Engine #2013 to fail and caused the loss of the engine. This occurred April 7, 1982. It is only a small part of the whole pump assembly, but the change to the "Kaiser Hat" nut assembly configuration was pinpointed as the cause of the failure.

2. Figure 2 shows the culprit in the April 1980, spacesuit backpack fire. Ignition took place in a V-shaped passage that served to restrict the flow of oxygen between a shut-off valve and a chamber in the backpack's high pressure regulator module. The failure resulted in autoignition of the metal at the end of the drilled passage due to compression and/or shock heating of the high pressure gaseous oxygen.

3. Figure 3 indicates the erosion concerns on the solid rocket motor composite nozzle in the early days of Shuttle missions. The degree of char or erosion was ascertained to be greatly dependent upon composite ply angle, nozzle manufacturing process temperature-time-pressure parameters, material controls for volatiles, and ash. The current nozzle has predictable final characteristics and is performing as specified.

4. To meet the needs of designers, the NASA Chief Engineer's office initiated a series of "Experienced Bulletins" providing design and operational lessons learned. An example of this, shown in Figure 4, deals with a rocket motor case problem occurring on a scout launch vehicle.

5. The point of view that the SEASAT spacecraft Agena "bus" (launched in 1978) used flight proven equipment that was also standard on other spacecraft and did not need tender loving care had far reaching consequences. The SEASAT Failure Review Board noted: "It became program policy to minimize testing and documentation, to qualify components by similarity wherever possible, and to minimize the penetration into the Agena spacecraft or "bus" by the government. It led to a concentration by project management on the sensors (experiments), sensor integration, and the data management system to the near exclusion of the "bus" subsystems. Important component failures were not reported to project management, a test was waived without proper approval, and compliance with specifications was weak." The component that failed--the slip ring assembly--was never mentioned in the briefing charts. The power subsystem design had the adjacent brush assemblies of opposite electrical polarity. This wiring arrangement, together with the congested nature of the design itself, made the slip ring assembly actually unique and very prone to shorting--which it did.

6. Just a very brief word on ground facilities. The KSC "uninterruptable power supply" system has been interrupted several times during the past 10 years. There would appear to be some difference between system names and system performance.

Reliability/Safety

In a memo from the astronaut senior member discussing the proper perspective to put on corrections to eliminate or reduce possible failure modes we have this:

> "...for every failure mode someone can envision, someone else must provide a solution. These solutions come in the form of hardware and software changes, complication of ground and flight procedures, new or modified facilities, manufacturing and inspection requirements. The proven costs of such solutions are money, schedule delays, and additional unknowns. I believe that many of our solutions to problems create more serious problems through added complication, dilution of effort, and increased time compression on already over-stressed work loads. There is an infinite supply of possible failures to support these hypotheses, as evidenced by continual and sometimes increasing hardware and software change board traffic. Unless management and program personnel develop a sense of proportion, we will forever be trying to chase things to the last decimal point, frittering away limited resources on insignificant issues."

It is for this reason that the Aerospace Safety Advisory Panel is strongly supportive of the framework for risk assessment described in NASA's Management Instruction NMI 8070.4, "Risk Management Policy for Manned Flight Programs." I might add that much of this NMI would certainly apply to unmanned space flight programs and certain aeronautical R&D programs as well. The qualitative prioritization of mishaps, which are only identified by Fault Tree Analysis (FTAs) and Event Tree Analysis (ETAs), is a good first step in focusing on what could possibly be the most significant possible risks. However, where the risk level may be significant, a more quantitative risk assessment methodology may be required such as that used to determine the possibility and severity of failures during missions using nuclear power devices such as RTGs (radioisotope thermoelectric generators/Galileo and Ulysses missions). This has many other names such as Probabilistic Risk Assessment (PRA) and others. If used judiciously it can show relative values of risks (not absolute) and support effective use of program and project resources.

Some other points that can be made include the following:

1. There is obviously a close tie between requirements and safety/reliability. The safety process, including system safety, must be a part of the original program requirements so that the old saw of "Reliability should be designed into the hardware and software, not tried to be inspected into it." This also applies to safety and, to some degree, the quality control aspects of design and manufacturing. To use a current term that is receiving a great deal of attention, this means Total Quality Management (TQM), or any of another half-dozen terms meaning the same thing.

2. There is danger in placing undue reliance upon an elaborate structure of review and oversight groups in that it can become a justification for sometimes not doing the job correctly in the first place. This stems from the "Not To Worry" attitude in which the manager and the engineers say to themselves: "The reliability and quality assurance guys down the line will catch any problems, so why worry!"

3. Although this is placed under safety and reliability, it really applies across the board to everyone connected with an aerospace program...engineers, technicians, middle and higher management. The following conversation might have occurred in any company or at any government agency:

Engineer: "Why don't I get any respect from my managers?"

Supervisor: "Partly because of the way you dress. They often rely solely on shallow, initial first impressions! It's true! Most managers and executives rarely take the effort to delve beneath surface features."

Engineer: "But that's absurd. It is like saying they read reports just by glancing at the title page!"

Supervisor: "Hey, I've got some bad news about that as well....."

4. Safety also encompasses communications and the fostering of interplay between various groups and individuals working on a program. Noncommunications can certainly result in failures. The Skylab launched on May 14, 1973, had suffered a complete loss of the meteoroid shield around the orbital workshop. This was followed by the loss of one of the two solar array systems on the workshop and a failure of the interstage adapter to separate from the S-II stage of the Saturn V vehicle. The investigation identified the most probable cause of this flight anomaly to be the breakup and loss of the meteoroid shield due to aerodynamic loads that were not accounted for in its design. The Skylab report noted: The venting analysis for the auxiliary tunnel was predicated on a completely sealed aft end; the openings in the tunnel thus resulted from a failure of communications among aerodynamics, structural design, and manufacturing personnel. The failure to recognize the design deficiencies of the meteoroid shield through six years of analysis, design, and test was due, in part, to a presumption that the shield would be "tight to the tank" and "structurally integral with the S-IVB tank" as set forth in the design criteria. In practice, the meteoroid shield, as a large, flexible, limp system that proved difficult to rig to the tank and to obtain the close fit that was presumed by the design. These design deficiencies of the meteoroid shield as well as the failure to communicate within the project the critical nature of its proper venting, must therefore be attributed to an absence of sound engineering judgement and alert engineering leadership concerning this particular system over a considerable period of time."

Procurement/Contracting

In its 1963 report, the Air Force singled out the following as Program and Contract Functions that needed attention:

1. Decentralized Program Management Lacked Essential Controls

In contractor organizations that were structured according to functional line department conventions, top management did not take action to ensure that internal policies, procedures, authority, and responsibilities were clearly defined for integrated

program control. To alleviate the concerns, it was recommended that clear-cut management interfaces be established between the government and their contractors with well-defined reporting procedures.

2. Late Definitization of Letter Contracts

Delays in definitizing letter contracts result in creation of work forces without positive direction, handicap progress evaluation, stimulation of continued program redirection, and expenditure of funds on tasks that do not contribute fully to the achievement of program objectives. Two points were made here: (1) program definition activities should keep two or more competitors active until definitive contract is singed with one; and (2) emphasize alternatives to letter contracts and definization milestones when letter contracts are unavoidable.

3. Make-Or-Buy Policies Not Enforced

Make-or-buy decisions were not made or evaluated in accordance with government policy or intent, thereby permitting poor utilization of industrial resources, contributing to late deliveries, poor performance, and increased costs. The action recommended was to have more fixed-price and incentive contracts that obviate government concern with contractor's make-or-buy decisions (unless use of a government-owned facility is involved).

In NASA's report to Congress on Centaur cost, schedule, and performance the following was stated regarding a "Procurement System:"

1. NASA has established a unique system for Headquarters review of selected major procurements above specified dollar thresholds. This "Master Buy Plan System" provides visibility into major procurements and allows Headquarters' review of key procurement documents to endure the quality of individual procurements as well as to identify trends that may require adjustments to the procurement system.

2. Regular and special procurement management surveys determine compliance with applicable policies et al. Included is a system for regular follow-up to ensure timely accomplishment of the recommendations included in the survey reports.

3. NASA has in place a procurement data system that provides integrated statistical reporting and trend analysis to manage effectively the NASA procurement system.

4. NASA has a procurement career development program that develops and monitors the training and skills of the procurement work force.

There are many others, but this appears as a typical list.

"SUMMARY"

This is obviously a brief, very brief, look into the lessons learned world. The purpose was to stir up your thinking, not with regard to the specific items noted here, but how to implement those lessons you have learned and will be learning to the next generation of aerospace programs. As we all know, what good is an education if we don't put it to some constructive use, and that applies to lessons learned.

FIGURE 1

HPFTP THERMAL SHIELD NUT

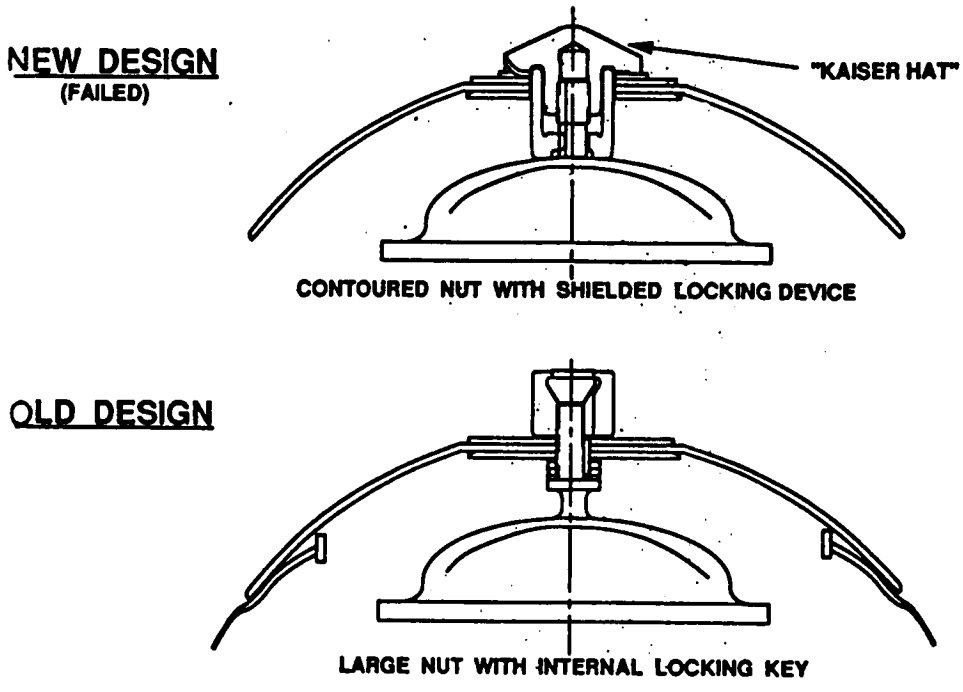


FIGURE 2A

NOMINAL INTERSECTION

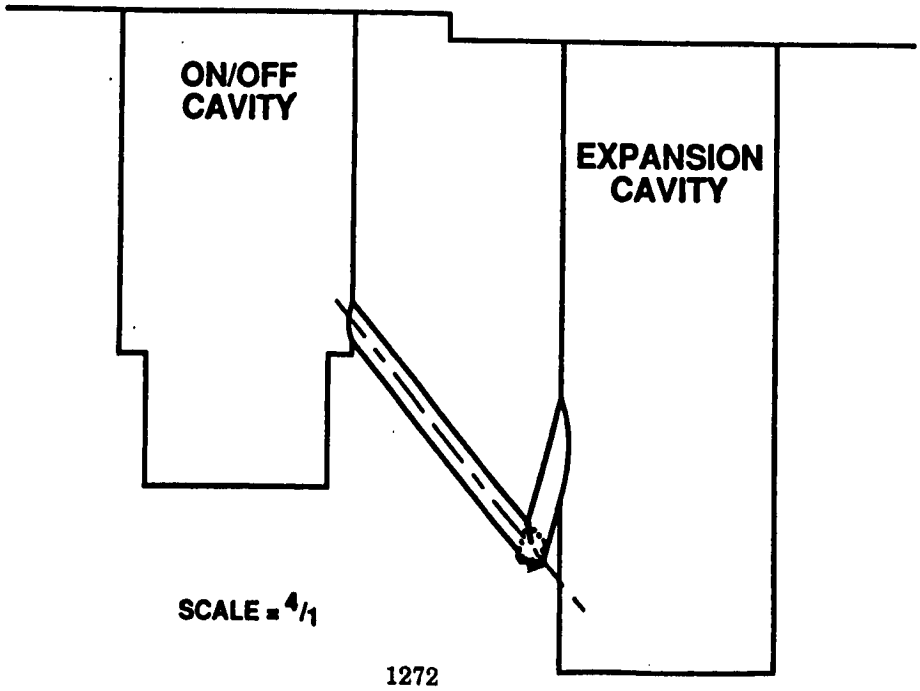


FIGURE 28

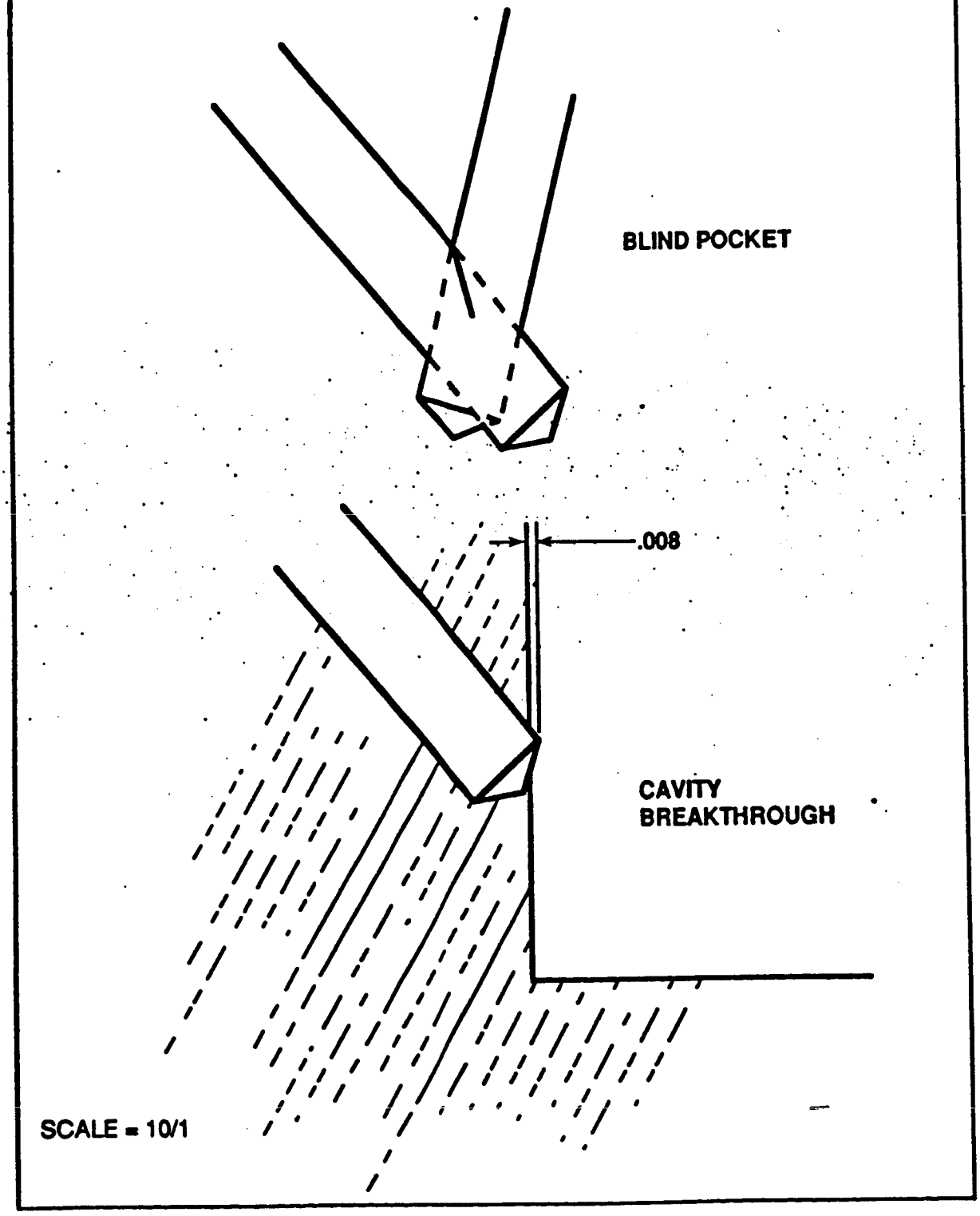


FIGURE 3A

NOZZLE ASSEMBLY

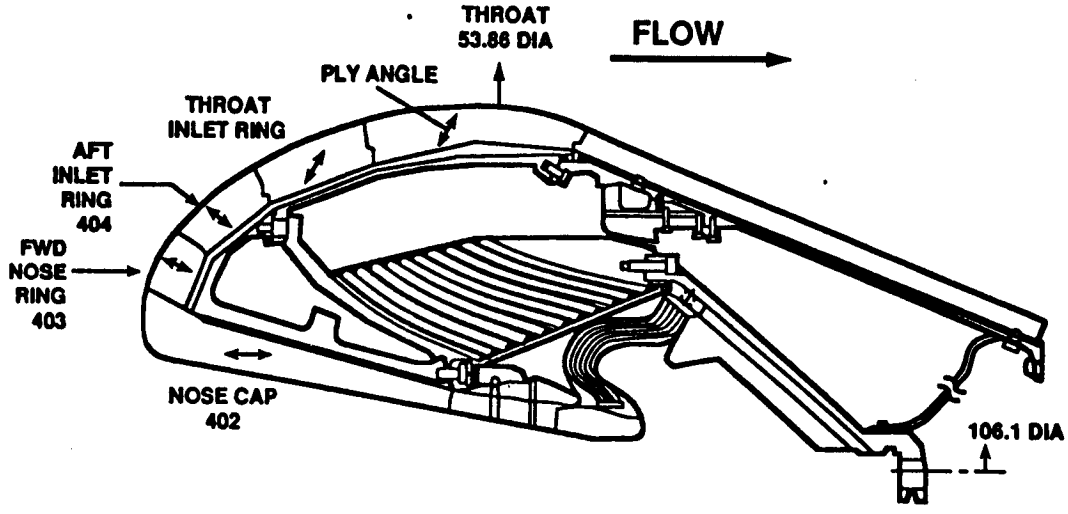


FIGURE 3B

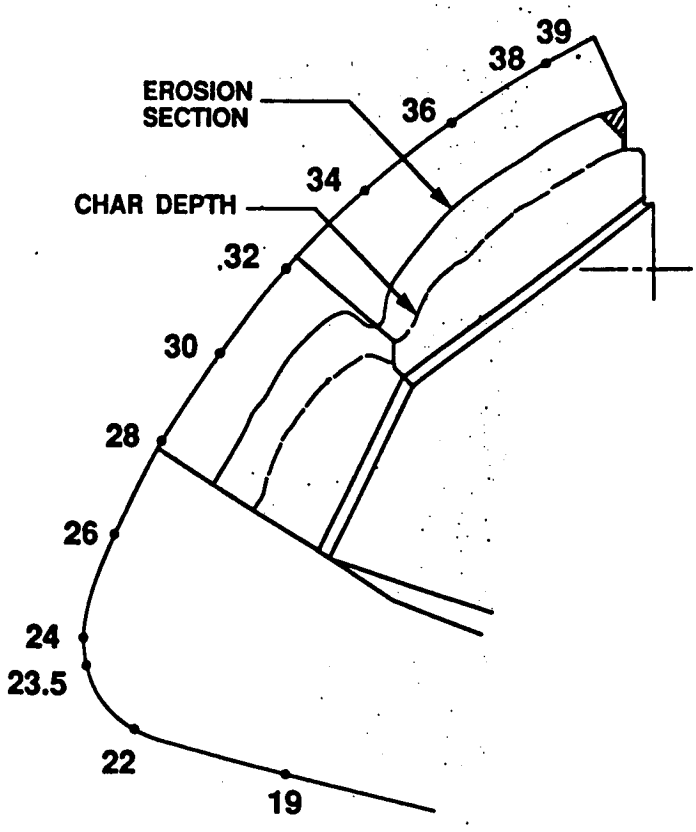
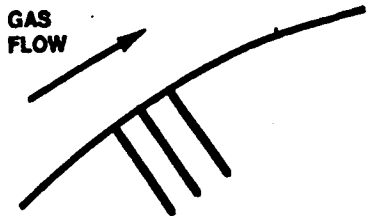


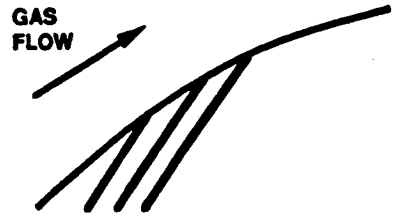
FIGURE 3C

PLY ANGLE EFFECTS



PLY PERPENDICULAR
TO NOZZLE WALL

- CONDUCTION DOWN CARBON FIBERS GETS HEAT IN DEPTH MORE QUICKLY
- THERMAL EXPANSION RETARDS OPENING BETWEEN PLIES



PLY AT ANGLE
TO NOZZLE WALL

- CARBON FIBERS REQUIRE CONDUCTING HEAT ALONG LONGER LENGTH TO REACH IN-DEPTH REGIONS
- PLIES CAN OPEN IF HIGH PRESSURES ARE GENERATED IN DEPTH

FIGURE 4

NASA
National Aeronautics and Space Administration

OFFICE OF THE CHIEF ENGINEER
Experience Bulletin No. 42 JUNE 1, 1982

ROCKET MOTOR CASE PROBLEM

INCIDENT

A Kevlar Motor Case, used on the Scout launch vehicle, was delivered to the contractor's machine shop to have aluminum skirt rings installed on the case. When a machinist attempted to remove the forward drill jig, it fell off causing the motor case to drop approximately 5 inches. The unit subsequently failed proof testing.

PROBABLE CAUSES AND CONTRIBUTING FACTORS

Visual and radiographic evaluation of the case for drop impact damage did not reveal any evidence that the structural integrity of the case had been compromised. It was decided to conditionally accept the case pending the results of hydroproof testing using strain gages and deflectometers. The results of the hydrotest were more startling than expected. Not only did the case catastrophically fail at 5% over the mean effective operating pressure of 1000 psi, but it showed positive signs of failure beginning to occur at 100 psi.

Post test visual inspection and strain gag data indicated that failure originated in one of the two drop-impact areas on the aft dome. Visual examination revealed two crack-like indications on the aft dome and evidence of interlaminar separations emanating from the ends of the crack-like indications. A 10X visual examination showed the indications to be ridges of Kevlar fibers rather than cracks, and there were no broken fibers. It is postulated that compressive loads induced in the outer layers of Kevlar by the deflection of the aft dome caused local buckling and resin crazing in the area of maximum deflection.

LESSONS TO BE LEARNED

Kevlar rocket motor cases may fail catastrophically well below anticipated operating pressures after apparent superficial damage is sustained. This finding was corroborated by other similar "drop" incidents. Two kinds of damage can occur from rough handling: (1) the case can sustain broken fibers; and/or, (2) there can be interlaminar shear failure between Kevlar winding layers. Interlaminar failures/defects are more critical in the domes than in cylindrical sections of the case. It is imperative that operating crews be warned to exercise extreme caution in handling Kevlar motor cases in order to prevent catastrophic failures due to drop damage. If Kevlar cases are damaged, even if only superficially, it is recommended that they be re-proof tested prior to use.