N72-25978

LUNAR MODULE PROGRAM SYSTEM SAFETY

by

Mr. William E. Scarborough
LM Safety Manager
Grumman Aerospace Engineering Corp.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

During the development of the Apollo Program spacecraft, the complexity of the vehicle systems and the pressures of mounting costs and time schedules established a requirement for company and NASA management visibility to support intelligent decisions with respect to risk management. These considerations, with the added emphasis of the Command Module fire at Cape Kennedy in early 1967, led NASA to establish the Office of Manned Space Flight Safety and to implement formal safety programs at all NASA Centers and at major contractor facilities.

LM SAFETY

Gruman, as a major contractor, was authorized to establish a formal LM System Safety program covering the main production facility at Bethpage and field site operations at Houston, Cape Kennedy and White Sands. The Gruman safety effort prior to implementation of this LM System Safety program was limited to a test operations group working with the spacecraft assembly and test organization and an analytical safety effort within the LM engineering organization. This early effort, coordinated with Reliability and the engineering subsystems groups, had identified crew hazards in the spacecraft and had implemented hardware fixes or compensating operating procedures for the flight crew data file. The implementation of a formal program based on an approved System Safety Plan provided a consistent and systematic effort, increasing the probability of detection of potentially hazardous conditions by in-depth design review by the safety group.

OBJECTIVE AND SCOPE

The objective of the program was and is the elimination or reduction of risk to personnel, material, and facilities resulting from failures or malfunctions in hardware or procedures.

The scope of this wide-ranging program was an integrated engineering, test operations and industrial safety effort in direct support of LM design, production and test activity in the Bethpage area. Indirect support and liaison was provided to the Gruman field sites and NASA offices. Safety support included analysis of design and proposed design changes for flight hardware, ground support equipment and facilities; the exchange of information on hazard assessments and accident experience, and review and analysis of discrepencies and anomalies reported during ground test and flight operations.

REFERENCES

The NASA Safety Manual (NHB 1700.1) and the System Safety Requirements for Manned Space Flight (OMSF SPD NO 1A) are the primary NASA source documents for the LM System Safety Program.

Other documents utilized in the development and implementation of the Program include applicable Grumman Corporation Procedures and Federal, State and local statutory requirements, and the USAF Systems Command System Safety Design Handbook DH 1-6.

ORGANIZATION

The organizational structure adopted provided for a Manager on the staff of the LM Program Director heading a Safety group with two branches, System Safety and Test Operations Safety. The System Safety branch supports LM Engineering and provides liaison service to the field sites and to cognizant NASA offices. The Test Operations branch supports production and test operations and provides industrial safety service to all LM Program personnel and facilities.

LM Safety provides support on a day-to-day basis to all Program groups and, in turn, receives support from Engineering, Reliability, Q.C. and the Sub-Contract managers. This closely coordinated effort assures maximum utilization of all available documentation and avoids duplication.

SAFETY FUNCTIONS

There are four major functions of System Safety on the LM Program - Analysis, Review, Surveillance and Test/Mission Support. Each of the functions includes a number of detailed tasks - some basic to any system safety effort and some peculiar to the LM program.

• Analysis

The analysis function includes a hazard assessment of each spacecraft subsystem,

performed on a functional basis for each mission phase. The FMEAs (Failure Mode and Effect Analyses) from Reliability, the Mission Time Lines, and the documentation from other subsystem groups are utilized for a detailed study which considers both ground and flight crew operations as well as hardware failures in identifying hazards. The study effort classifies hazards as crew safety or mission success and confirms compensating provisions or backout procedures. Uncompensated hazards are reported to the cognizant engineering group and are tracked to final closeout by hardware or procedural changes.

This technique is also applied to proposed design changes, which are analyzed for personnel or hardware hazards and are followed-up through the approval cycle to installation and retest or rejection.

An example of the hazard assessment effort is the analysis which was completed for LM-5, the vehicle which flew on Apollo 11 and made the first lunar landing. The functional analysis of each subsystem was performed for the mission phases during which the spacecraft was active. The subsystem functions were evaluated for their effect on the flight crew, vehicle, and mission; the adequacy of contingency procedures, and other compensating provisions. The comparison of mission phase per sub-system function was related to methods of detection, time criticality, and availability of corrective or backout procedures. Uncompensated hazards were identified and evaluated and a rationale for their acceptance or rejection provided. This analysis revealed no crew safety hazards requiring hardware changes. All hazards identified were of the "acceptable risk" category based on the compensating provisions available in the vehicle. Procedural changes were recommended, however, to enhance mission success. These included an independent exercise of the redundant explosive device systems and constraints on attitude changes during the period while the lunar and command modules were "soft" docked on the capture latches. The capture latches are the devices on the Command Module probe which initially engage and lock-on to the LM drogue mounted in the top deck tunnel area. "Hard" docking is the subsequent action of retracting the probe and engaging the twelve docking latches.

This major analytical effort has since been utilized as a base-line study for the program, with each of the follow-up spacecraft reviewed emphasizing the hardware and mission changes incorporated since LM5. Analysis of these later vehicles missions has identified additional hazards which have been compensated by hardware changes or procedural workarounds incorporated in the crew check lists and mission rules.

- Review

The Review function includes those tasks involved on a continuing basis with the review of test and working documents and the operations they control.

Operational checkout Procedures (OCP) which are utilized for subsystem and system checkout are reviewed. Particular attention is devoted to revised procedures and to changes proposed during operations. The hardware setups utilized for tests are included, with emphasis on safety provisions such as relief valves, hose restraints, proper bonding and grounding and the like. Hazardous sequences in these operations are identified and marked and special control exercised while they are in-work. Real-time deviations to procedures are reviewed, with a safety concurrence and sign-off required for those designated hazardous.

An early and highly satisfactory Review effort was the Operational Readiness Inspection (ORI) conducted on the LM Internal Environment Simulator (IES). This altitude chamber facility was designed to provide checkout and verification of the LM life support system and involved manned runs in 100% oxygen environments. The ORI was conducted in accordance with NASA directive MSCI 8825.2, which establishes criteria for manned operations in oxygen-rich environments. GAC believes that the ORI conducted under 8825.2 is an extremely valuable safety tool for any facility requiring man-rating. Effective program cost control will tailor the ORI, the Board size, and the scope of activity to the hazardous nature of the facility being inspected.

Prior to the LTA-8 LM test vehicle operations in the MSC Houston altitude chamber, a review of the OCPs to be utilized during the tests was conducted by a special team of subsystem engineers, coordinated by LM System

Safety engineers. These tests, the first manned LM operations in a simulated space environment, were identified as extremely hazardous and a thorough analysis of every phase of the operation was conducted. The Safety Review team identified numerous procedural problems, all of which were corrected by changes to the documents prior to the chamber runs.

A similar review of the test documents to be utilized during the checkout of LM-1, the unmanned first flight spacecraft, was conducted at Cape Kennedy by the LM Hazard Review team. This review, chaired and coordinated by LM System Safety program personnel, covered thirty-seven documents and identified and documented fifty-three hazards. In three cases, hardware fixes were required and change requests were initiated. The remainder of the hazards were satisfied by procedural changes incorporated in the test documents.

For the first manned flight, LM-3 in earth orbit, the team reviewed the documents to be utilized for the preflight spacecraft checkout and altitude chamber runs at KSC. This team also identified more than fifty hazards requiring changes to the procedures, all of which were incorporated in the test documents. More important than these statistics, however, was the heightened interest stimulated in hardware, test set-up and procedural changes when the Safety Review was scheduled and imminent.

With each of these safety reviews, confidence in the spacecraft and the test procedures increased and on completion of the LM-3 assessment, formal reviews were terminated. However, procedural changes proposed during any test or operation are still reviewed and approved by Safety prior to their incorporation in the documents.

An additional Review task is the investigation and reporting of accidents which occur during production or test operations. On the LM Program, an accident is defined as any unplanned event which results in injury or damage to program material or facilities. All accidents are thoroughly investigated and reports submitted to cognizant management and NASA offices. Recommended corrective actions are tracked to close-out, with periodic status reports to responsible groups.

Experience on the Program to date shows a steadily declining accident rate, with 3.9 accidents per million manhours in 1969 and a low of 2.2 in 1970. During a one year period, from May '69 through May '70 more than 8,000,000 man hours were worked without a disabling injury. Analysis of the accident record indicates that the majority of the accidents are caused by carelessness and failure to follow procedures. Some typical examples include the following:

1. A facility technician installing a workstand on a concrete floor was setting studs with an explosive-actuated gun. To expedite the job, he attempted to drive a stud through a pre-drilled hole in a flange of the stand instead of using a clip held by an additional stud. Missing the hole, the stud ricochetted off the flange and floor and struck the man on the jaw, where it lodged and was subsequently removed surgically.
2. During installation of replacement components in the spacecraft heat transport (cooling) system a technique involving freezing the system fluid in the coolant lines with liquid nitrogen coils was being utilized. (This process permits cutting lines without draining the system or introducing air into the lines). An inadequate temperature gage and inattention by the man monitoring the temperature allowed the plug to thaw and pop out. Attempting to stop the flow of glycol, the technician held his thumb over the open line, suffering second degree cryogenic burns from the escaping fluid. In addition to the injury, extensive cleaning was required to remove the spilled glycol from wire bundles and spacecraft structure.
3. At the start of the transfer of approximately 2500 gallons of waste alcohol from a facility storage tank to a tank truck the 3" pickup hose ruptured, spraying approximately 100 gallons of alcohol over the truck and the surrounding area before the transfer pump was stopped. There were no injuries and no other damage although the incident was potentially catastrophic considering amount of alcohol involved and the ignition sources present in the area. Prompt action by the Safety Engineer and the Fire Guard covering the operation minimized

the spill and dissipated the free liquid. Cause of the accident was an unqualified driver-operator on the tanker who did not operate the pick-up pump and valves in proper sequence.

Also included in the Review function is the tracking of close-out action on safety-significant failures which occur during test or flight operations. While the primary responsibility for failure close-out action rests with the Reliability group, Safety is concerned with failures involving hazards to ground or flight crew personnel and makes full use of the Reliability documentation which is available. Identification of those failures for which Safety has a responsibility is based on criteria established by the Safety group in accordance with hazard classifications developed by NASA. Action in tracking these failures consists of coordinating with the responsible engineering subsystems groups and continuing the follow-up to final close-out.

LM Safety also reviews all ground support equipment failures, assessing hazards to personnel or hardware and coordinates with the GSE group on close-out action. For common-use GSE, which is shared with other contractors, an information exchange procedure has been established to assure timely corrective action on all hardware at all sites.

We have found that the daily Program Status meetings attended by the Program Director and Engineering subsystems managers, provides maximum visibility on developing problem areas and the opportunity to initiate immediate corrective action. This activity is a major day-to-day function of the system safety group.

- Surveillance

The surveillance function is primarily the activity of the Test Operations Safety group. All manufacturing and test facilities are monitored for compliance with safety requirements and for adherence to current Corporate Procedures and legal requirements of local and Federal safety statutes. Identified hazards are corrected immediately or the work area is tagged out-of-service. This coverage is provided by Safety on a full-time basis for all scheduled operations, 24 hours per day seven days per week.

- Test and Mission Support

Safety support of test operations includes participation in Test Readiness Reviews and Pre-test Briefings. Safety requirements and emergency procedures are reviewed with the test team and qualification of test team members confirmed with the Test Conductor.

Frequent surveys of test facilities are conducted to assure adherence to established safety requirements. Special attention is devoted to hoisting and lifting equipment, pressure hose restraints, proof testing of equipment, and installation of safeguards such as kick plates, guard rails, safety nets etc.

Test team training and certification (as required) are monitored and frequent drills in emergency shut down or back-out procedures are conducted. Authority for safety approval of deviations to hazardous test procedures is delegated to the safety engineer on duty. The Safety Manager is the only Authority for waivers - which are granted for one-time exceptions to established safety requirements or rules. In all such cases, additional specific safety requirements are imposed.

During hazardous test sequences or operations, a safety engineer is required to be present at the test site at all times. His support of the activity includes real-time approval of procedural deviations, equipment changes, and maintenance of a safety test environment throughout the facility.

For the Apollo Missions, LM System Safety engineers are assigned to the Mission Support Team and provide full coverage of all LM active mission phases in the Bethpage mission support room. Activity in this role includes participation in the mission simulation training runs, flight crew debriefings, and follow-up on flight anomalies and discrepencies.

SUBCONTRACT SAFETY

For the task of reviewing the safety of the Program sub-contractors, the LM Safety team monitors the formal review activity of the Reliability, Quality Assurance, and Sub-system Engineering groups which have primary responsibility. Reports are reviewed regularly and the safety group participates when required for on-site reviews. Documentation and advisory service are supplied to the regular inspection teams and to the resident personnel in

the plants. LM Safety provides personnel and participates on-call for investigations of accidents or when plant conditions involving safety are being reviewed. Recommendations resulting from investigations or reviews are made to Program Management, with follow-up to assure implementation of approved changes. This coordinated effort with QA group has been demonstrated to be a satisfactory, cost-effective method of monitoring a vast network of subcontractors.

FIELD SITE SUPPORT

An essential element of the LM safety effort is support of the Grumman field sites at MSC Houston and White Sands, with the Bethpage Program office providing policy direction and liaison between sites. The Houston operation is primarily manufacturing and test in support of Grumman activity at NASA.MSC. At White Sands, the company provides engineering and material support for the engine firing and propulsion system tests conducted in the test cells.

At KSC, the company maintains a safety group which provides all required functions for the local activity. Liaison and coordination for this group is also provided by the LM Safety organization at Bethpage, particularly in the area of spacecraft technical support and in the exchange of operational experience and information.

REPORTS

Management visibility, both for NASA and Gruman, is provided by regular and special reports of significant events and safety accomplishments on the Program. A monthly status report is provided to the MSC Safety office with other special reports as required.

An accident reporting system has been established to provide the background material for positive preventive action. All occurrences are recorded, utilizing a simple, one page form, and are followed-up until final close-out action is complete. Reports and periodic summaries are distributed to Program, Corporate, and NASA offices to assure maximum benefit to other groups with similar problems.

MEETINGS

Accident experience and preventive actions were also shared with other contractors and the NASA Centers by means of the STEMs (Safety Technical Exchange Meetings) sponsored by the NASA. These valuable meetings were scheduled periodically at the Centers or at Contractors' plants and provided a useful forum for the exchange of information.

Currently, the LM Safety group participates in regular Safety Concern meetings via telcons with the MSC Safety office. This coordinated approach avoids duplication and assures maximum effort on follow-up and close-out of identified hazards.

CONCLUSION

The application of System Safety principles to the LM Program has been eminently successful by any standard. In the face of the pressures of tight schedules and shrinking budgets, LM manufacturing and test operations have been on-time, with a continually declining accident rate. The LM spacecraft performance on the Apollo missions to date - from the first lunar landing by Armstrong and Aldrin in LM 5 to the latest by Shepard and Mitchell in LM 8 - has met or exceeded all mission objectives. The success of the total effort to put man on the moon marks Apollo as probably the most significant program of our age. As a small part of that total effort, LM Systems Safety made a contribution which will continue, maintaining or improving the standards established for the Program until the final Apollo mission is flown.