67-WA/MGT-2

an ASME publication

12-17 Nov 1967

Fulfilling the Aerospace Engineer's Responsibility for Product Reliability[1]

R. B. WILSON

Chief, Reliability Verification Section, Reliability Engineering Branch, Saturn Mechanics and Reliability, Douglas Aircraft Company, Huntington Beach, Calif.

J. HILMAN

Branch Manager, Mechanical Reliability and Maintainability, Systems Safety and Effectiveness Directorate, Douglas Aircraft Company, Huntington Beach, Calif.

The aerospace engineer has responsibilities for product reliability to his management, to the immediate customer, and to us, the taxpayers, who are the ultimate customers for large, internationally prominent aerospace programs. His responsibility is to provide the best possible product, concomitant with his responsibilities to cost and schedule limitations. A variety of program management techniques is exercised at the authors' company to fulfill these responsibilities, and to evaluate the engineer's performance of these responsibilities. Several of these techniques, which are described here, are the Vehicle Flight Readiness Review, the Formal Design Review, System Analyses, the Management Failure Review, and the Quality Maintenance Program. These techniques have enabled the engineer and his managment to fulfill their responsibilities on the Saturn S-IVB Program.

[1]The management techniques described in the paper support the Saturn S-IVB Program which is being conducted for the National Aeronautics and Space Administration, Marshall Space Flight Center.

Contributed by the Management Division for presentation at the Winter Annual Meeting and Energy Systems Exposition, Pittsburgh, Pa., November 12-17, 1967, of The American Society of Mechanical Engineers. Manuscript received at ASME Headquarters, June 28, 1967.

Copies will be available until September 1, 1968.

THE AMERICAN SOCIETY OF MECHANICAL ENGINEERS, UNITED ENGINEERING CENTER, 345 EAST 47th STREET, NEW YORK, N.Y. 10017

Fulfilling the Aerospace Engineer's Responsibility for Product Reliability

R. B. WILSON J. HILMAN

INTRODUCTION

The aerospace engineer has responsibilities for product reliability to himself, to his management, to the immediate customer, and to us, the taxpayers, who are the ultimate customers of the large, internationally prominent aerospace programs. This is true whether he is in industry (as prime or subcontractor), in the government, or in an advisory (consultant) agency. This paper discusses the engineer's dilemmas, and describes techniques by which it can be determined how well the engineer is fulfilling his responsibilities.

Although this paper is presented from the point of view of a major industrial contractor to the government, and will draw examples from experience on the S-IVB Stage Program (for Saturn Launch Vehicle), many of the techniques and concepts described here can be utilized by other industrial, governmental, or consultant organizations.

ENGINEERING RELIABILITY DILEMMAS

Before discussing techniques for fulfilling the aerospace engineer's responsibilities, it is first appropriate to identify the concurrent difficulties.

The engineer's basic responsibility is to provide the best possible product, concomitant with his responsibilities to cost and schedule limitations. It must be recognized that the engineer is in the position of having to tradeoff continually between the requirements of performance, cost, and schedule, while primarily motivated to attain that for which he is technically trained, that is, outstanding performance. The only acceptable compromise with these three mutually contradictory requirements is to provide a product that meets contractual performance, cost, and schedule requirements. To fulfill this responsibility, the engineer needs a contractually defined measure of his technical performance, including product reliability, and a means to measure his accomplishment against this goal.

While it is not too difficult to specify performance requirements by means of measurable parameters, this cannot easily be done for the characteristic of product reliability. The only true measure of product reliability is the satisfactory operation of a specified number of units under a specified set of operating conditions for a specified period of time. Where a high degree of reliability is required, it is necessary to operate a large number of items, and it may be necessary to operate them for a long period of time. For small, inexpensive devices with relatively short operating life, such as light bulbs, fuses, and vacuum tubes, a high degree of confidence can be obtained for a high level of reliability at a reasonable cost. For space vehicles, this approach is not practical. The reliability of the end product, such as a space vehicle, must be assured to the extent possible, prior to its final assembly, and obviously cannot utilize a large number of end items in a test to examine the reliability characteristic. Where the number of space vehicles is comparatively small, as is usually the case, it is not even feasible to test a large number of components to obtain a reasonable assurance of high reliability, with any degree of confidence. Other traditional tools of Reliability Engineering/ Systems Effectiveness Engineering, such as combining engineering judgment with statistical test results from supposedly similar items, are susceptible to infinite permutations of subjective and usually optimistic judgment. Consequently, in order to fulfill his responsibilities, the engineer must exercise systematic program management techniques in advance of the operational use of the hardware and, ideally, prior to completion of production of the hardware.

For the Saturn S-IVB Program, management techniques of a nonnumerical nature have been utilized, as well as the familiar reliability statistical methods. While these management techniques cannot demonstrate statistical compliance with a numerical goal, they do provide engineering confidence and management visibility into the effectiveness of design decisions. These techniques succeed in bringing to management attention the trade-offs which must be made between performance, cost, and schedule. Trade-off decisions can then be made by the appropriate level of engineering management. This assures that the inherent design is free from "nonresponsible" decisions based on limited information, human error,

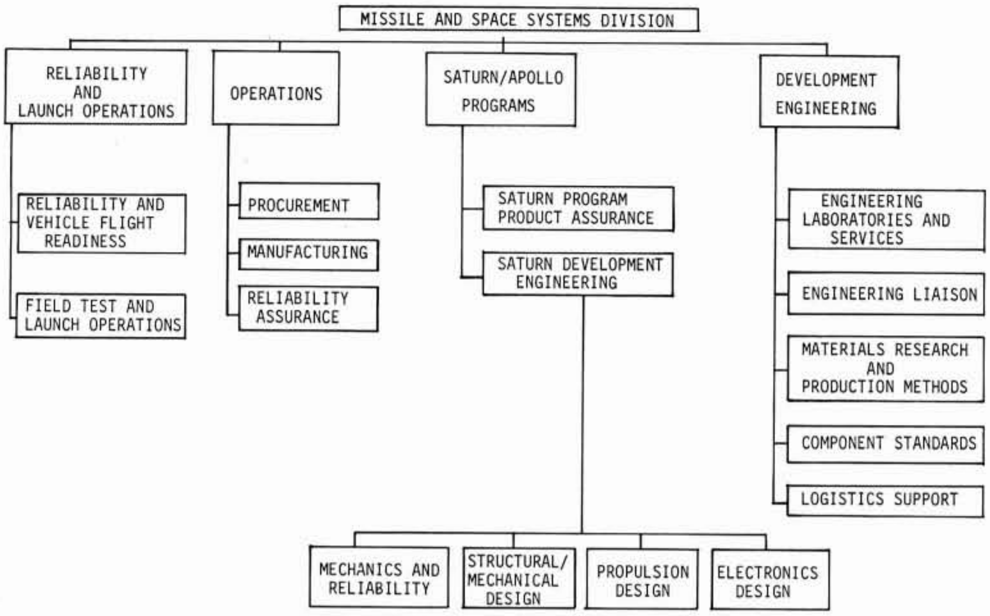

Fig.1 Douglas Missile and Space Systems Division organization illustrating reliability program functions

oversights, undesirable interface characteristics, and overly subjective decisions.

In addition to fulfilling contract requirements, the engineer has a responsibility to utilize his technical judgment and advise the customer, through his management, where contract requirements should be changed to obtain realistic reliability requirements. This activity is performed by the standard procedures of contract letters, engineering change proposals, and working-group meetings. However, the management procedures described in this paper provide added visibility to identify reliability and other design problems, and to substantiate the need for changing program requirements. These program management techniques, which are used on the Saturn S-IVB Stage Program, satisfy much of the need for providing a measure of how well the designer and his management have met their conflicting responsibilities to the contractually specified goals at the time the assurance is necessary.

ORGANIZATION

Program management techniques, which draw upon many functional departments, require an organization chart to illustrate the interrelationships. Fig.1 is the Douglas Aircraft Company, Missile and Space Systems Division (MSSD) organization, and shows the relationship of Saturn/Apollo Programs (which handle the S-IVB Stage Project) to the whole.

MSSD utilizes a balanced organization consisting of program management elements and functional departments in performing the Saturn S-IVB Program tasks. Program management organizations have the responsibility to plan, authorize, direct, and monitor the Division's efforts to achieve program objectives. Functional departments are responsible for accomplishing the work which has been authorized.

There are some features of this organization chart that are worthy of note. The Reliability and Launch Operations office is responsible for review of the reliability of all Division products, and for all field test and launch operations. This is a staff office reporting directly to the Division General Manager. The former responsibility is exercised through a suboffice for Reliability and Vehicle Flight Readiness. This activity supports the Division goal that all field test and launch operations on aerospace hardware be accomplished successfully.

Also reporting to the Division General Manager are Operations and Saturn/Apollo Programs. The head of Operations has the responsibility for Procurement, Manufacturing, and Reliability Assurance for all the Division's Products. Quality Control is exercised by the head of Reliability Assurance, with one of his specific responsibilities Reliability Assurance for Saturn/Apollo Programs. The head of Saturn/Apollo Programs has Saturn Development Engineering and Saturn Program Product Assurance reporting to him.

The authors of this paper are within Saturn Development Engineering, reporting through Mechanics and Reliability. Mechanics and Reliability functions are analytical, as contrasted to the Design Technologies that are also part of Saturn Development Engineering, who create the drawings and specifications.

Saturn Program Product Assurance has the responsibility for providing program direction to apply the disciplines of reliability, system safety, quality control, and configuration management to Saturn products. Performance of the many "doing" functions is continually monitored and audited to assure accomplishment commensurate with contractual requirements.

Also reporting to the Division General Manager is a central Development Engineering function which serves all of the Division programs. Development Engineering has the responsibility for Engineering Laboratories and Services, Engineering Liaison, Materials Research and Production Methods, Component Standards, and Logistics Support. Engineering Laboratories and Services operates and maintains all the Division component test facilities, exclusive of production acceptance testing. Engineering Liaison represents project Design in the field for both procurement and test. Component Standards provides Approved Parts Lists for use by the respective projects. With this background, it is now possible to describe the program management techniques that are employed by the S-IVB organization to enable the engineer and his management to fulfill their responsibilities.

VEHICLE FLIGHT READINESS REVIEW

The Vehicle Flight Readiness Review is a high-level management review of the status or resolution of design, fabrication, and operational problems as evidenced by Test History, Formal Design Reviews, and Configuration Verification results. This review technique is exercised on the completed product, prior to major milestones, when system and personnel safety, as well as contract performance, is at stake. For each Saturn S-IVB Stage, these reviews are held prior to factory checkout, prior to acceptance test firing, and again prior to launch. This review function is chaired by an engineer who reports to the head of Reliability and Launch Operations. This office is independent of the program organization responsible for developing, fabricating, and testing the S-IVB Stage. Its sole concern is the flight worthiness of the stage. This review function serves as an internal (to MSSD) audit which is at least as stringent as any which the customer might institute. The review is conducted through the use of a committee whose members are on loan to the chairman from the S-IVB Stage Program. The committee consists of engineering management personnel representing the several program design technologies, and the Reliability Assurance Organization associated with the program.

The committee considers the status of:

1 Component qualification testing, as it affects the readiness of the stage to meet the milestone under consideration.

2 Formal Design Review action items.

3 Failure history of each flight critical item installed on the stage. This includes failures before and after installation on the stage, and failures of similar items during any test function. The results of all failure analyses, and the corrective action therefore, are also reviewed for adequacy.

4 Configuration of the stage, as compared to the required configuration expressed by engineering documentation.

The committee action includes a "walk-around inspection" by the committee (or a subcommittee which includes the chairman). The Vehicle Flight Readiness Review also assures that any temporary deficiencies have an adequate, planned corrective action, and that this corrective action is adequately documented to assure that the deficiency will be corrected on schedule. These scheduled corrective actions are then reviewed at subsequent milestones to assure satisfactory completion.

If, after a thorough airing, any of the problems under consideration is still a cause for concern on the part of the committee, or its chairman, as to the readiness of the stage for its intended exercise, the committee is mandated first to bring about corrective action and, ultimately, if concern still exists, to present the facts through its chairman to the head of Reliability and Launch Operations, with a recommendation against the exercise. This office has the authority to prevent a stage from going into acceptance firing or into flight.

The function of this committee has a salutary effect on project performance. It does serve as a means of demonstrating that engineers are fulfilling their responsibilities. Each design engineer must answer for his design decisions in depth, and without hedging.

FORMAL DESIGN REVIEW

One of the sources of information to the Vehicle Flight Readiness Review Committee is the Formal Design Review. These formal, documented reviews are in addition to the many informal documented and undocumented design reviews which are part of the design process. Ideally, they are held after sufficient design has been completed, but before the design has been released for production. The participation is broadened to include all departments which may affect or be affected by the design under review. Participation is mandatory, and requires specific supervisory levels of attendance. These reviews may consider a single component, a family of components, or a complete system. Formal presentations are made by the Design Engineer, Reliability Engineer, and the Quality Engineer. Other presentations may be required of such organizations as Component Standards, Material Research and Production Methods, Test Engineering, Production Engineering, and Logistics Support. All questions raised at the meeting must be answered, either at the meeting or by documented action items.

Typical characteristics which are reviewed include performance requirements, environmental requirements, material compatibility, test-and-failure history of similar devices, redundancy, service life, maintainability, and human-engineering features. Each participant is required to submit a completed checklist prior to the meeting. The discussions are tape-recorded. The proceedings of the Formal Design Review meetings are recorded in the form of preliminary minutes which also contain action item assignments and due dates for completion. There is then a final set of minutes when all open action items are closed and the design has been accepted by all participants. A final set of minutes can also result in the design being rejected and a new meeting scheduled for the new design which is then recommended.

There is also an opportunity for "minority reports" to be filed by dissenting individuals or organizations, if the management or customer decision has overruled a specific recommendation. The action items (open and closed items) and minority reports are presented to MSSD management (especially through the Vehicle Flight Readiness Review) and to the customer. These reviews also provide insight to the design engineer into circumstances or conditions he may have overlooked or been incorrectly informed about during the design. Indeed, many improvements have resulted from the process of the design engineer simply preparing for a design review.

SYSTEM ANALYSES

There are many types of system analyses performed to obtain performance characteristics, marginal operating conditions, weight characteristics, cost, and so on. The particular analyses considered here are for the purpose of identifying system and mission interdependency relationships. The result of these analyses is the Reliability Engineering Model (REM). This REM provides identification of all functional components, describes their function in relation to the performance of a specific mission assignment, and states the effect on mission success for each possible failure mode. This REM is then used to identify the Flight Critical Items (FCI)[2] and their critical modes of failure.

The REM is widely used by personnel involved in Component Test, System Test, Design, Reliability Assurance, Logistics, Program Management, Purchasing, and Systems Integration as a handy reference document with simplified schematics, functional explanations, and criticality interpretations. The most widely used derivative is the FCI list, which is used as the basis for providing specific priority attention to problems and as a list of audit items to check any facet of program activity.

Since the degree of criticality of these items is a function of the probability of failure occurrence, as well as effect on mission success, the highest criticality items are often the ones experiencing the greatest difficulty in achieving maturity of design. This is usually because they are pressing the limits of performance and also the limits of the state of the art. Thus, these items are excellent candidates for review of procurement/manufacturing problems, adequacy of traceability procedures, adequacy of design (via Formal Design Review), adequacy of qualification testing, verification of configuration management procedures, drawing release procedures, failure reporting, and corrective action effectiveness, and so on. This list of approximately 100 items for the S-IVB Stage provides an excellent means of checking adequacy of all operating procedures and activities for the program and, at the same time, provides extra assurance that these key items will receive the added management and line personnel attention which they deserve. This list and the REM also serve to alert the cognizant design engineers that their items must have safety margins which have been more thoroughly assured, and advise them of what specific characteristics are most crucial to mission success.

MANAGEMENT FAILURE REVIEW

A standard procedure in most companies for determining disposition of "failed or rejected" hardware is a Material Review Board. At Douglas, an additional procedure is used which is aimed primarily at prevention of similar failures (corrective action) rather than merely conservation

[2] Flight Critical Items are those items whose single independent failure could result in a loss of primary mission.

of material under review. This can be seen in the following system description.

All development and qualification testing is conducted under the supervision of Engineering, with Reliability Assurance representatives in attendance. Likewise, all vehicle checkout is conducted under the supervision of engineering personnel, with Reliability Assurance representatives in attendance. Production Acceptance Testing is monitored by Reliability Assurance. Reliability Assurance personnel document discrepancies, malfunctions and/or failures on Failure and Rejection Report (FARRs). After the FARR is written, Engineering determines disposition, after a suitable investigation of the cause of the discrepancy. The depth of investigation and the degree of documentation of the investigation depend upon:

1 The kind of discrepancy: If the discrepancy is a functional failure, as contrasted, for example, to a mismarked component or a documentation problem which would be nonfunctional, there is a more detailed investigation to determine if the discrepancy was due to mishandling, incorrect testing, or design deficiency. There would also be a search of past history of similar failures.

2 The kind of component: If the component is one whose failure would jeopardize achievement of the mission (Flight Critical Item), it is accorded special attention, and Reliability Engineering is required to conduct an independent investigation of the cause of failure.

If the cause of the discrepancy is not apparent, and the discrepancy is functional, then a procedure called "Supplemental Failure Analysis" (SFA) is required. It is necessary to document the rationale for either a decision to have an SFA or a decision not to have an SFA. The decision not to have an SFA must be unanimous after review by Reliability Assurance, Reliability Engineering, Design Engineering, Program Management, and Engineering Liaison.

When the cause of the discrepancy is known, or the nature of the discrepancy or the nature of the component is such that the expense of an SFA is not warranted, disposition is recommended to Material Review Control Center (MRCC). This disposition may include "acceptable as is," scrap, salvage, rework, and so on. It is then the responsibility of Reliability Assurance to assure that adequate corrective action has been accomplished and is documented on the FARR. The corrective action may be performed by Manufacturing, Tooling, Manufacturing Engineering, Reliability Assurance, Design Engineering, or the supplier, or by several of these groups working together. The FARR is then submitted to the customer for approval that adequate corrective action has been performed.

When the SFA is required, the conduct of the SFA is systematic and orderly, with participation of all cognizant MSSD Engineering Departments and Reliability Assurance representatives. If the component is purchased from a supplier, his Engineering and Reliability/Quality people are also involved. The analysis takes place in an appropriately equipped laboratory, according to a deliberate plan that optimizes the likelihood of pinpointing the exact cause of failure. The laboratory examination and teardown is supplemented by Metrological, Metallurgical, Chemical, and Strength Testing Facilities, as needed, to evaluate the physical evidence. The analysis is carried to the depth necessary to isolate the cause of failure, and may include a micrometallurgical analysis of materials or mass-spectrographic analysis of contamination. The findings are documented, reviewed, and evaluated by Engineering and Reliability Assurance to assure appropriate corrective action.

Supplemental Failure Analysis is carried out under the direction of the cognizant design engineer. However, the review and evaluation of the stated cause and corrective action are performed by the Failure Analysis Committee. This committee is chaired by Liaison Engineering and includes managerial personnel from Reliability Engineering, Reliability Assurance and Product Assurance, as well as the cognizant Design Section. Other delegates to the committee are managerial personnel from the appropriate support organizations, such as Component Standards and Material Research and Production Methods (MR&PM). This committee monitors the scheduling of the analysis and receives the findings. It evaluates the corrective action decided upon. The case is not considered closed until the corrective action has been authorized by Project Management and is accepted as adequate by all members of the SFA committee. At the same time, Project Management maintains pressure to complete the analysis and implement corrective action expeditiously, and in accordance with the schedule. Responsibility is at a level where it belongs! An effective, closed-loop, corrective-action system is assured to provide for the engineer another technique through which he fulfills his responsibility for product reliability.

QUALITY MAINTENANCE PROGRAM

The Douglas S-IVB Stage project Quality Maintenance Program has two goals: "To maintain existing performance and to improve reliability confidence levels." This is brought about by a rigorous program that builds upon the performance and reliability confidence achieved through the hardware development phase of the project. The program includes:

- Hardware Audit
- First Article Reliability Review
- Periodic Requalification Testing
- Production Acceptance Testing
- Reliability Critical Items Inspection

The Hardware Audit consists of a random, in-depth audit of the manufacturing operations, inspection operations, documentation, and in-process handling techniques to determine the consistency of these operations and their ability to provide uniform hardware. This is applied to both supplier activities and in-house activities. The audit is conducted against a checklist that has been prepared by MSSD Reliability Assurance, with assistance from the cognizant Design and Reliability Engineering personnel and supplier personnel. As part of this audit, a selected hardware review is made, consisting of detail part physical measurements. Functional and/or production acceptance testing is also reviewed. Emphasis is placed upon performing the audit at the lowest level of assembly possible. The hardware audit is performed by MSSD Reliability Assurance personnel and recurs at approximately 6-month intervals on a list of selected critical items.

First Article Reliability Review consists of an examination and appraisal of the detail design concept, physical hardware assembly, hardware maintainability evaluation, and the evaluation of manufacturing techniques and documentation quality and content. Production disassembly (teardown) is performed. Physical, microscopic, and chemical analyses are performed as required. Reliability Engineering, jointly with Design and Reliability Assurance, prepares the review plan. All of these groups participate in the review and preparation of the report. The review performed on a unit, representative of the first deliverable production unit, provides evaluation of those controls necessary to assure consistent follow-on delivery of a like product. When performed on units other than the first production item, this review serves as an audit of those production and inspection disciplines required to achieve the desired results.

The First Article Reliability Review is a comprehensive Hardware Audit, carried out under Reliability Engineering direction. The reviews have resulted in recommended action items. Typical action items that have resulted from these reviews have included changes to existing manufacturing methods; i.e., potting and crimping procedures, recommended thread lubricants, drawing corrections, etc.

Requalification Testing is just what the name implies. It consists of randomly sampling production items, and subjecting such items to specific critical tests of the original qualification program. This activity is under the cognizance of Design Engineering, with Reliability Engineering and Reliability Assurance assistance.

Production Acceptance Testing is application of stressful environments, such as temperature or vibration, within design limits, to certain production items on a 100-percent basis, plus the measurement of functional characteristics. The environment(s) to which any particular item is subjected is selected to uncover workmanship defects and/or initial critical failure modes. The stress duration is long enough to uncover incipient failures, but not so long as to jeopardize the useful life of the item. These tests are under the cognizance of Reliability Assurance.

Reliability Critical Items are selected for application of a carefully designed Quality-Control inspection plan to inhibit the occurrence of critical failure modes. The modes of failure that are critical are identified by Reliability Engineering through their conduct of System Failure Effects Analyses, and concurred in by Design Engineering. Reliability Assurance determines the significant physical characteristics related to those critical failure modes, subject to the approval of Reliability Engineering. One hundred percent inspection and control of those significant characteristics, encompassing all phases of manufacturing and acceptance testing, is instituted. For example, the critical leakage of a butterfly valve (that is, a function of the angular position of the stem at "closed position") is controlled by control of the physical dimensioning of the closure stops. All production documentation -- Assembly Outlines, Fabrication Orders, Inspection Operation Sheets, Production Acceptance Test Documents, and so on -- are especially annotated for these significant physical characteristics, to ensure their verification for proper value.

Each of these procedures provides checkpoints at which time the aerospace engineer can obtain additional evidence of the degree to which he has fulfilled his responsibility for designing and maintaining product reliability.

CONCLUSION

As a result of the difficulties in estimating accomplishment of numerical goals for product reliability, the engineer will always be in a position where it can be simultaneously proclaimed that he has "not met his customer's expectations" and has also "overdesigned a gold plated product." The essentially nonnumerical techniques described in this paper (Vehicle Flight Readiness Review, Formal Design Review, System Analyses, Management Failure Review, and Quality Maintenance Program) assure that the engineer has melded his conflicting responsibilities and fulfilled his responsibility for product reliability.

In addition to utilizing the foregoing techniques to meet the contractual product reliability goals, the engineer must try to persuade the customer, through his management, to want what, in the engineer's professional opinion, would best suit the customer's needs. After agreement is reached with the customer on what will be provided under the contractual performance, cost, and schedule requirements, the engineer must meet these requirements. Utilization of the techniques discussed in this paper will help assure that this responsibility is met.

It should be noted that the techniques described here represent only a selected few of the many management and specialty techniques used at Douglas Aircraft Company on the S-IVB Program. These particular techniques have been selected because they demonstrate: the broad participation employed from many departments; how MSSD provides assurance that potential design problems have been eliminated and product reliability goals have been met; and how the aerospace engineer and his management know that they have fulfilled their responsibility for product reliability.