PAPER TO BE GIVEN TO THE NORTH EAST CHAPTER, MISSISSIPPI SOCIETY OF PROFESSIONAL ENGINEERS, IN TUPELO, MISSISSIPPI, MAY 11, 1967, BY

JOHN D. BEAL, JR.,
QUALITY AND RELIABILITY ASSURANCE LABORATORY, MSFC

History of MSFC Reliability Philosophy

Tonight I will discuss the History of MSFC Reliability Philosophy which began with the Redstone Missile. There it was necessary to establish specialized groups, such as design, manufacturing, checkout, and launch. There was one small group assigned to take care of checkout. This group took the documentation as it came from the drawing board, checked it out thoroughly, and generated procedures necessary to perform a good checkout. After the group had everything as well prepared as they thought it could be done, the vehicle was moved into the bay area for the checkout where the group ran into many difficulties. There were workmanship, parts, and component problems, and there also were problems with the subsystems and the systems. After this experience it was clear that a much more thorough preparation was mandatory. This resulted in the systematic buildup of the receiving inspection so that all components going into assembly were inspected before they were released. This led to the systematic buildup of inprocess inspection including checking those points where inspection at a later time was impossible. Also developed at that time were the step-by-step procedures which were necessary for the engineer to familiarize himself with the problems. They were excellent guidelines for performing the tests

and could also be used collectively as a training document for people entering the profession. We developed at that time what is now called pyramidal testing. Here we tested first the parts, then the components, then the subsystems, the systems, and eventually performed a simulated flight test. With these steps taken and implemented, the situation had improved. Closer contact was established with the designer. Feedback to the vendor and manufacturer was built up and we said that we had made progress.

It was about 1958 when we had an unhappy experience. We had received a shipment of valves from a manufacturer, who had established a pretty good reputation, but all failed our acceptance tests. We investigated the matter and found out that the manufacturer had not received the proper technical requirements from the purchasing office. We found furthermore that contracts often did not contain sufficient quality control provisions to allow the government to properly monitor and assess the performance of the contractor. This explained to us why we still had difficulties in getting acceptable hardware. This hole was plugged by introducing a procurement review which made sure that the requirements as they existed were made known to the contractor. It was comparatively easy to discover the problem but it was much more difficult to correct it. Although we started in 1958, it took some years before we had it contractual and under control.

At that time we came to the conclusion that we must write a document which covered the subject more completely than we had

After we had laid out the pattern in the prescribed way for the quality assurance area, we realized that the next step would be to set the frame work for a reliability effort based on the same fundamental principle: i.e.; the marriage of theoretical analysis and hardware effort. NASA document NPC 250-1 made an attempt to spell this out. This step was not an easy one to sell, since the theoretical approach emphasizing the importance of apportioning of numbers and prediction prevailed at that time. We did not say that we did not need or appreciate this effort, but that we just wanted to put it into proper perspective, using it as a tool which would enable us to zero in on the problem areas, the resolution of which would require utilization of many kinds of engineering disciplines.

Based on this background information, we have now a reliability effort, the main elements of which I would like to discuss with you.

At the outset of a project, we ask for a Reliability Program Plan which is finalized at the time a contract is let. This Plan must show that there is a clearly identified group which will be responsible for the management of the reliability program and that the head of this group has unimpeded access to top management, and has the necessary authority for proper discharge of his responsibilities. These responsibilities include planning, funding, staffing, directing, and monitoring the reliability effort to assure that the goals are achieved at minimum cost and within schedule.

Formal reviews of the reliability program or elements thereof, by the contractor himself and by MSFC, to assess progress and effectiveness,

are another essential requirement. These reviews are scheduled at major milestones in the program and on other occasions as required.

Since we consider our primary goal to be the achievement of reliability, the effort must start with the design. In the design area, we have one ground rule to which we adhere as closely as possible, and it is: "Use design features and components which are already flight proven. Introduce new features and new designs only when you have a very sound reason for doing so." We also give considerable attention to redundancy, but as you know actual application of redundancy is limited, since in the missile and vehicle field you must be weight conscious. Redundancy can be and is being applied comparatively easily in areas where miniaturization and microelectronic circuits can play a part, such as in computers, amplifiers, and emergency detection systems. In other areas for example, the philosophy of redundancy can be applied only indirectly. The eight engines operating the Saturn I and the advanced Saturn I have the so-called engine-out capability provided, which means that if one engine fails, the lost thrust is made up by increased burning time of the other seven engines.

Prior to procurement and manufacture, we need to assure that complete design specifications are provided for each hardware element, subsystem, system, and end product. These specifications include performance and functional tolerances, design and process requirements, mission profile, reliability goals, tests for measurement of compliance, a plan for statistical analysis of data, and inspection and acceptance requirements. The specifications should leave no doubt in the

contractor's mind what the requirements are and what use is intended for the end product. It should contain no "how-to-do" information since there are usually several approaches possible. The customer should not be restricted to approaches previously taken except to assure himself that the stated requirements can be met.

This complete information is not only to be given by us to the prime contractor, but we expect the prime contractor to pass it on to his subcontractors and vendors in such a way that everyone contributing anything to a space vehicle knows what he is supposed to do and how essential a part his products play in the space vehicle program. To emphasize the importance of this endeavor, not only is the procurement documentation verified, but a special program--the manned flight awareness program--has been initiated and is being carried out. This program must ascertain that all participating companies and employees receive the message concerning the importance of their performance for the success of the space effort.

A failure mode, effect and criticality analysis is considered to be one of the cornerstones of any reliability effort. This consists of a continuous formally documented analysis of all structural and functional design in order to discover inherent potential failure areas, specifying the effect of a failure on the mission. Such failure mode, effect and criticality analyses provide the bases for engineering management action concerning improvements in design and in specifications, and for tests for design verification. It is also a prerequisite for reliability prediction and assessment through mathematical

techniques. Just to again point out the importance of combining theoretical analysis with practical engineering judgement of the hardware, I would like to mention that we were asked by NASA Headquarters in 1966 to furnish for each Flight Readiness Review of a Saturn vehicle a list of the 10 most critical items of each stage. After we had listed them in the order of their criticality numbers based on the failure mode, effect and criticality analysis, we looked them over and found that many of them had not given us any trouble while other components not on that list had given us headaches over and over again. This analysis indicated that we had to develop a second list based on actual failure history of components and, then, to blend the two lists properly together to arrive at a realistic assessment and to orient additional design and test effort into areas where improvements were badly needed. With this approach, criticality ranking was utilized as the basis for applying priority effort.

The reliability apportionment, prediction and estimation are related to the failure mode, effect and criticality analysis and allows us to construct a mathematical model, first to allocate qualitative reliability predictions, and second to assess reliability achievement based on test data. The models which are updated continuously afford designers and management clear visibility of progress, and point out problem areas which require attention.

The value of design reviews is recognized almost everywhere today. They are organized and well-documented evaluations by management of the engineering progress at scheduled program points, with participation of all required disciplines. Technical as well as management problems are identified and defined. Action items are formulated for resolution and followup. It came as a surprise that we met, in some places, considerable resistance against the introduction of a formalized approach for design reviews, but these reviews have proven to be very worthwhile and effective by bringing unbiased talent from all disciplines into the loop at a fairly early date in the development cycle.

Failure reporting and corrective action is another feature in which we are strong believers. We have built up a strictly controlled system for reporting, analysis, correction and followup of all human errors and hardware failures through the several project phases, including launch countdown and flight. We have set up the machinery and have it working well, but were still not satisfied with the response on our requests for failure analysis in the laboratory or plant which originated failed components, subsystems, or systems. Therefore, we have increased the failure analysis effort in our own Quality and Reliability Assurance Laboratory in order to permit people who are unbiased to perform more failure analysis work on their own.

A very essential part of a reliability program is an adequate amount of testing. I think I should say a few words about this effort. Even if testing activities are not always a part of a reliability organization, test plans must be influenced by reliability engineers and test results must be evaluated and utilized by them, regardless of

who actually performs the tests. This is most important in the area of launch vehicles, where there is no appreciable production volume. For this purpose, we must try to eliminate all modes of failures, or to circumvent them by application of redundancy or other techniques in order to reduce the possibility of occurrence to an acceptable level. This requires various types of testing, the results of which are investigated continuously by reliability engineers who recommend elimination of weak spots by whatever means necessary.

The three principal types of testing, even if they are called by other names occasionally, are:

a. Development tests, which provide for the necessary understanding of principles and operating characteristics involved;

b. Qualification tests, which provide an objective measure of the success of design work; and

c. Reliability tests which provide statistical evidence concerning reliability, and the limits to which the design can be taken.

Since reliability tests are often cancelled because of funding limitations, the emphasis must be placed on development and qualification tests, and the reliability engineer must be sure that all tests are carefully planned and properly instrumented. During the development tests, testing should be performed over a range of operating and environmental conditions above and below the nominal to enhance the fundamental characteristics of the device, to disclose unsuspected modes of failures, and to gain confidence that adequate safety margins exist.

Based on the results of the development and qualification tests, we are required, in the majority of the cases, to make our statement as to the flight readiness of the device. This we can do only if we know that the concept of total quality and reliability assurance in the manufacturing plants has been followed. This means that good quality and reliability programs, including quality control and corrective action, configuration control, and procedural discipline, have been followed. At this point it becomes evident that efforts in reliability and quality assurance must go on simultaneously. They cannot be really treated as independent disciplines, but must supplement each other strongly and completely.

Now, after having given what are considered the most essential points in the MSFC concept of reliability, I would not close the subject without mentioning another very important ingredient, the human being. Have you ever given thought about what qualifications you expect in a man or woman who devotes his time to the unglamorous field of reliability and quality assurance? In this person you need a combination of features which is not easily available on the market. People must be professionally competent. They must be willing to fight an uphill battle as long as they carry the quality or reliability badge. They must have a tremendous stamina against frustration, otherwise they cannot survive. They must be self-motivating, since no force from the outside can continuously supply enough motivation to overcome the daily adverse conditions. They must be able to deal with people. They must be objective and persuasive. They must have a desire to

work hard, and a pride of accomplishment. They are, indeed, extremely important assets, and effort should be expended to keep them on the job as long as possible, so that they can transfer experience from one project into the other and thus help to develop and improve proper methods of implementation over extended periods.

I would like to sum up, as follows: Success requires a realistic concept implemented by extraordinary people who know the importance of theoretical analysis and paperwork and have a thorough understanding of the hardware and never forget that paperwork and hardware must go together.