N64-H555*
NASA, Washington, D.C.

In Sandia Corp. Aerospace Nucl. Safety Jan. 1964 p 33-37
(See N64-H551 06-01)

THE NASA AEROSPACE NUCLEAR SAFETY PHILOSOPHY

H. B. Finger, ~~Manager~~
Space Nuclear Propulsion Office, AEC-NASA
Director, Office of Nuclear Systems, NASA

I seldom have the opportunity to philosophize. I talk about the programs that we are running, principally the nuclear rocket program. My talk today, however, will not cover the nuclear rocket program at all. I have been asked to talk about NASA's philosophy of safety; since I don't really know what that is, I'll give you my own philosophy. Certainly for my programs it represents the project philosophy. Where I can, I'll include NASA examples.

The philosophy of nuclear safety in aerospace systems is, to me, just like the philosophy used in the development of any space system in which human life may be involved, whether it be human life in the vehicle itself or the effects that may be felt on the ground. The main point must be that the system will be as reliable as possible; its operation must be assured. We would like 100 percent reliability.

I think the main effort must be in ensuring that the system will work as designed. In addition, we believe that even when we do everything possible to make it work as we intend, we assume that something will go wrong and design appropriate countermeasures. I think we can develop a system that really is reliable, one with a negligible probability of abort and damage. I will later indicate some examples to show that such systems do exist in the space program, as established by the record of space flights.

I also believe we can develop reliable countermeasures. My real worry, however, is that countermeasures may make the basic system unreliable and may make it almost impossible to operate the system satisfactorily. This is where the judgment that Mr. DiLuzio talked about enters. I have seen many countermeasure gadgets that we could add to nuclear rockets and nuclear electric power systems which would, I am afraid, make it impossible for the basic system to operate successfully. At some point, tradeoffs must be made to optimize overall safety. I believe it has to come at the beginning of the development program and be integrated throughout the program.

Everything I have talked about so far--development of the system and development of the countermeasures--is, to my way of thinking, a project responsibility. It is up to the people who are developing the system to handle these responsibilities. Only the project people can make the design decisions and tradeoffs to ensure overall safety and reliability. Over and above this, we get what is usually referred to as an independent review. As Mr. DiLuzio pointed out, it is frequently difficult to get such a review, but we try. This independent review hardly ever does, or should, dig into the development program of the system to determine whether the system will operate successfully. What it looks at are the countermeasures, which, of course, we hope are never used. Thus, it looks at only a small part of the overall problem. My concern is that a review may be so independent that its only purpose is to say, "No, there is something you haven't looked at, and until you look at it we won't let you fly." I think the project has a responsibility to be as objective as it can, to point out every trouble, to force itself to be aware of the problems it may run into, and to explain these and discuss them with anybody who wants to know about them so that it may objectively make a responsible decision on the safe operation of the system. I am frankly concerned, however, that both the countermeasures and a too-independent review may reduce the likelihood of successful operation and application of nuclear systems in space.

AS]

I'd like now to discuss how we go about getting a system to operate successfully. We have, I think, several examples of the kind of reliability we want. Though few in number and statistically a poor sample, the four successful flights by the Marshall Space Flight Center of the Saturn I first stage indicate that a reliable system can be developed. To do so, it requires a thorough enough understanding of the system so that if anything troublesome shows up in the development program, it can be located and corrected. Then again, we try to put enough margin into the system to make the operation reliable.

We have had 19 consecutive successful Thor-Delta flights out of a total of 20 tries. It is clear once again that it is possible to develop successful systems.

The Mercury program is probably the best example of all. There were no mission failures. Human life was involved. The main emphasis was on ensuring that each flight would be successful, whether it was manned, unmanned, or flew a monkey. In addition, countermeasures were always available so that in the event anything happened the astronaut would get out safely. Happily, the abort countermeasures never had to be used--and that really is our goal, it seems to me in nuclear aerospace systems.

Another example appears in the successful space flights of the Goddard Space Flight Center, which has had 30 successful flights out of 31 attempts. Thus, it is clear that methods exist for obtaining reliability.

The problem with nuclear systems, however, is that these systems will fly with hardware which has never been tested before--a rather unique situation. In almost every other case, ground tests are made of the hardware flown. In general, the philosophy is to test the hardware to be flown. This philosophy cannot be followed with nuclear systems and, hence, it will have to be ensured that, throughout the development program, each unit is exactly like the next and any damage appearing in one is understood well enough to avoid similar damage in later units.

The burden, then, is on the process of developing such reliability, and I'll spend most of my time talking about this area of work.

In order to achieve high reliability, we must have a good design, the test equipment and hardware must be built as designed, and a thorough development test program must be conducted including extensive testing under simulated space flight environmental conditions. First, we obviously must start with a good design. The entire system must be designed with as much margin as we can build into it and with redundancy for critical or uncertain operations and components. The problem is that we don't necessarily know how the system will operate under all conditions. Therefore, we don't really know where the margin must be added and how much is required to ensure reliability, especially when we are in an early part of the program and are developing a new technology.

Secondly, and I think this is where we get into many of our problems, we must be sure that the hardware is built as designed. I know all of you who are responsible for building systems or hardware are shocked at what frequently happens in procurement and fabrication. Although we monitor and direct vendors and contractors and succeed in catching some errors and deviations, some get through because we lack sufficient manpower and because we are not necessarily, in all areas, better than the many competent industrial people participating on our programs. Many examples can be cited. For instance, a raw material delivered to us is certified to have a certain heat treatment; when checked for certain properties after fabrication, we find that it isn't the material we were supposed to have had to do the job. Obviously, the vendor of the raw material must have his quality control techniques reviewed. Such problems take us back to the supplier of the raw material--all the way through every one of the vendors, fabricators, and inspectors and through every step along the way if we are to ensure that the hardware delivered is, in fact, as designed.

There is frequently a feeling that quality assurance need not start in an early research and development phase of a program. I don't agree. I think the

fault in this concept is that as we establish a design, every result must be able to be correlated with certain reasoning and certain things which happen in the system. There may be anomalies in the results from different systems, and we must be able to track back to ascertain that the piece of hardware we started with is everywhere the same. In addition, it must be recognized that every bit of data must contribute to the setting of specifications, to establishing quality control procedures, and to proving out the design, especially when comparatively few systems are to be built. I think it is a real problem. It requires that we start quality assurance efforts very early in research and development.

In addition, we must not fail to recognize that our quality assurance techniques themselves require research. There are many areas of inspection and quality control that are not yet established. We don't always know how to measure the inclusions in a weld. We don't always know how to ensure the physical properties which we want over the full range of conditions required. Where there are thick sections, X-rays may not always be satisfactory; means must then be found both for inspecting such sections and tracing them through the fabrication process in order to ensure that we have in fact, even with prototypes, a way of building hardware as designed. All this work, it seems to me, must start in the research and development phase of the program.

It is, in addition, necessary that a comprehensive analysis and development test program on all system components and subsystems be conducted in a program leading to full system tests so that all the phenomena encountered are thoroughly understood. This development work must include full system tests on the ground under simulated space flight conditions. Some feel that it is too difficult to test nuclear systems under simulated space conditions and that because of the cost this step should be skipped. Thus the system goes from component and system tests under nonsimulated conditions directly to flight. I don't believe, however, that the full system simulated environmental tests can be skipped. Such tests are made on every other system; why not on nuclear systems? Nuclear systems are not simple; they are not easier to develop than other systems; they involve as much or more test work. There must be a clear, comprehensive test program that includes every step able to provide assurance that the end item will operate as intended.

I don't believe there are any short cuts in these developments. We cannot plan on any luck. We must build success into the system during development, and we must build it in by including every facility, every piece of test equipment, and every test that will help to ensure successful operations. The development time will not be longer with such a program; the time will be shorter in terms of delivering the thing we want. Nor will the cost be any greater with such a program. Rather, it will lead to success that would not be assured by any short-cut approach.

In the hearings before the House Appropriations Committee just a few weeks ago, a rather interesting question was asked by Congressman Thomas, Chairman of the Independent Offices Subcommittee, with which NASA works. This question was asked of Dr. Robert Gilruth, Director of the Manned Spacecraft Center: "To what do you attribute your main success, Doctor? I think the outstanding thing in my lifetime has been the Mercury program that you gentlemen put on so successfully. You did not lose even a monkey, much less a human being." Dr. Gilruth replied, "I think it is the great care on the part of the government personnel and skill on the contractors', which, in this case, were McDonnell Aircraft for the spacecraft and General Dynamics for the booster--the great care, checkout, and testing and retesting, going as far as we possibly could in assuring it would work when we tried it. Even when you do all this you cannot always guarantee success." Later in the discussion, Mr. James E. Webb, the NASA Administrator, added, "You see, one of the things that is so essential in these matters is never to proceed, when something shows up that you do not understand, until you really understand it and know what the cause of any particular phenomenon or difficulty is. I think Dr. Gilruth, perhaps more than any other person, has been the driving force to make absolutely sure that nothing unknown will be permitted, that you must really identify the cause of some occurrence before you proceed to the next step."

This, I think, is the NASA philosophy. It does lead to successful systems as indicated by the Mercury program and the several others I mentioned. Hopefully, the same philosophy will be used in nuclear programs. Even though it may appear to delay the programs at first, it will actually give successful completion in the shortest possible time, and, I am convinced, at the least cost.

Incidentally, in the Mercury program and later in these House Appropriation Subcommittee hearings, Dr. Gilruth made the point that in order to ensure the required booster reliability, the Atlas boosters delivered for the Mercury program were different from military boosters. The parts were carefully tracked through fabrication and assembly; more severe requirements were put on the parts than on those for military use, and the cost of the system went up by about 30 percent, I believe he said. But the point is that the program ran successfully, and every mission was a successful one. Let me give you an example of the requirement to explain every detected flaw. On Cooper's flight, there was an inverter and 0.05-g signal problem. Months after the flight, tests were still being run to figure out what went wrong in the electrical system, even though it was known that no Mercury flights were to follow. Detailed explanations must be available for everything that happens in a test or a flight. I believe this applies as well to ground testing. I agree also with Dr. Gilruth that no matter how hard you try, there may still be difficulties that you won't find. You do your full system tests on the ground and your flight tests as part of the development program to find these troubles. When you fly an operational system, you should have worked all of those bugs out.

I will only mention a few other areas which, I think from a systems approach, must be developed at an early time. These include all aspects of ground checkout at the launch site. A means must be developed to check the vehicle out and ensure that every system is working properly. The range safety system must also be checked out to be sure that the sensors and the transmitted data it will have to read will, indeed, give the kind of information that is needed. This is a very large and important overall system development problem.

All these things I have talked about are project responsibilities. No independent safety committee looks deeply into this part of the program. The project establishes the way it wants to work and the way the system is to be developed. The success of the program depends upon the serious attitude of the people who are responsible for the development of the system. Beyond this, however, because we can't always be assured that every piece will work as intended on a flight, we apply countermeasures. In nuclear systems, the particular hardware will not have been tested before. We, therefore, try to postulate anything that can happen anywhere along the operating cycle--in the shipping of the reactor to the Cape, the assembly of the reactor with the rest of the system, its installation on the vehicle, the initial boost phase, along the trajectory, and after operation. Everything must be considered. We then postulate every possible accident that could occur, and we try to devise a countermeasure for each one. Hopefully it is a passive countermeasure, but we can't always do that. Sometimes we need active countermeasures. We must then go off on a new development program to develop the countermeasures, following the same philosophy as on the basic system itself.

As I have said, I am concerned that some of the things we talk about as active countermeasures in these nuclear systems will have some effect on our ability to successfully operate the basic system. We haven't yet reached the point of making all the necessary tradeoffs, but they will have to be made. Some judgments must be made, and some risks must be accepted as long as we can show that the probability of an incident is small.

Now, this is the one area, to my mind, that needs some safety review. It should not be a project review, but it should not be a review whose entire purpose is to say, "No, don't fly." It has to be a review that is constructive. It must look at the problems associated with the entire system and at its reliability, especially its countermeasure reliability. It will not follow the same ground rules as the ACRS review of ground reactor systems. I believe the ACRS has established an enviable record in ensuring the safety of ground systems, but we are talking now about a different kind of environmental situation where different technologies are required.

How does one obtain a single review when there are so many different groups involved? NASA is responsible for the mission, the AEC and NASA for developing the systems, and the Air Force for the range and the launch area (if launch is from the old Cape Canaveral area; NASA is responsible if it is from the new Merritt Island launch area). A coordinated review is, therefore, extremely important. Each agency has some review function, but, if we went through all of them one by one, we might never fly. There must be some pulling together of all these groups to review the safety of the system. From a technical point of view, several agencies were involved in the review of SNAP-9A system safety and potential hazards. The Division of Reactor Development and the Division of Licensing and Regulation in the AEC drew on experts from the different agencies in their particular fields of competence. Sandia was deeply involved in this program of testing as well as Cornell Aeronautical Laboratories and various other groups. I think it was a very constructive exercise. But the fact is, even after going through all this review, we couldn't have at the launch site a whole committee trying to make decisions. One man will have to be delegated to speak for the project and make the very final judgments within a broad framework of specifications that the review committee presents. One man must have the authority to make the decision, and he will have to be responsible. He will have to be a very competent man with a real understanding of the responsibility that he will take on.

In summary, I would like to say that I believe that nuclear systems can be developed to be reliable. In some ways, they are simpler than the systems we are working with now--simpler than the chemical combustion rocket systems, the solar cell systems, etc. I believe we can apply countermeasures, but these will have to be applied with judgment to ensure maximum reliability and overall safety. I believe also we will need some kind of an integrated interagency safety review. This is the basis upon which we will establish a nuclear space capability for the country that will permit us to explore in areas that we would not otherwise be able to approach.