RELIABILITY ACHIEVEMENT IN HIGH TECHNOLOGY SPACE SYSTEMS

Dean L. Lindstrom, Hughes Aircraft Company, Space
and Communications Group, El Segundo, Calif.

ABSTRACT

Long Life space systems developed from the early 1960's to the present day have demonstrated the achievement of long life and high reliability in a high technology space environment. With electronic parts improvements, decreasing failure rates are leading to greater emphasis on the elimination of design errors. The achievement of reliability is dependent on three primary factors: technical capability, good judgement, and discipline.

INTRODUCTION

My discussion will center primarily on the achievement of reliability on long life, high reliability spacecraft. These utilize a combination of proven technology and new technology. The lives of these spacecraft, for the most part, have been longer than anticipated. When we started the Intelsat IV program, for example, noone had any experience to indicate that a battery would last for the seven years required.

Several of these spacecraft have introduced new technology without compromising life or reliability. One recent development is the Compact Hydrogen Maser frequency standard for Navigational Satellites, delivered this year to NRL. It is still not space proven, but initial clock comparison data indicated performance unsurpassed for a device of its size.

DISCUSSION

Figure one (1) shows the Hughes family of satellites. This family started with the launch of Syncom (lower right corner) in 1963. This was the world's first synchronous communication satellite. It operated successfully until operation finally was discontinued in 1969. The newest member of this family in the upper left hand corner is the Leasat. This satellite, to be launched in the 1980s is our first spacecraft design optimized for a shuttle launch. Some other spacecraft are worthy of note. The ATS, launched in 1965 for Goddard Space Flight Center, is still providing useful data. The TACSAT, launched for the air force in 1969, was the first gyrostat or dual

DISCUSSION - Continued

spin-stabilized spacecraft. On the left hand side in Intelsat IV, which was the first large International Communication Satellite. It is capable of handling 9,000 simultaneous two-way telephone conversations. The OSO, orbiting solar observatory, with the design life of 3 years, was turned off after 4 years of successful operation.

Two spacecraft shown in this figure are shown more closely in Figure 2. Pioneer Venus Orbiter and Multiprobe spacecraft represented some very difficult technological challenges. 33 different scientific instruments for taking atmospheric measurements in Venus were integrated into these two spacecraft. For the probes that went to the surface of Venus, this meant withstanding the high temperature and acid of the Venus atmosphere plus the extremely high pressure encountered at the Venus surface.

The next two figures (Figures 3 and 4) show the operational performance of this family of satellites. Together they have accumulated over 200 spacecraft years of successful operation. More than 15 billion electronic parts hours have been accumulated with less than 30 failures attributable to electronic parts. None of these part failures has had a significant impact on spacecraft operation.

These spacecraft have demonstrated several significant things relative to reliability. First, they have demonstrated that long life in the vicinity of 7 to 10 years is achievable with complex space systems. ATS has demonstrated that, under the right conditions, a life of 15 years or more is possible. Second, they have demonstrated that the reliability of electronic parts can be extremely high and a negligible factor in overall system reliability. They have demonstrated another fact that is not apparent from these charts. When you take any element or item for granted, it will be the element that comes up and bites you. The only significant problems we have had on orbiting satellites is with travelling wave tubes. Due to oversights in the modification of existing designs, we had early life failures of travelling wave tubes on several spacecraft. Because of redundancy within the satellites, the effect of the shorter tube life was minimized. The problems have been corrected and we expect to get longer life on our tubes in the future. The second illustration is a non Hughes satellite, but it was one that caused a major investigation. The SEASAT had an early failure of slip ring power transfer assembly. In this case an existing proven design was used for a different application. The difference in the application was not recognized initially and eventually led to the failure of the satellite.

DISCUSSION - Continued

What are the keys to achieving high reliability in a high technology environment?

- Understand the Design
- Design with conservatism
- Control Parts, Materials and Processes
- Test and Analyze

Understand the Design

Generally, there is a hesitancy on the part of the design engineer to document his design and document what he understands about the design. I have two concerns about this. One is, since the full understanding of the design is in his head, what happens if someone else attempts to supply that design? And second, does he really understand the design or does he just think he does? The process of setting down on paper how the design works and interacts with other hardware systems generally leads to better understanding by the designer himself. I can refer to a recent example, where a very competent design engineer was requested to perform a hazard analysis. After the explanation by the safety engineer, the design engineer spent a day and a half fully documenting how his design works. He later acknowledged that now not only were other people able to understand how this design worked but he now understands it better himself.

Failure modes and effects analysis is an important tool in both documenting the design and identifying what can happen to cause the system to fail. Unfortunately failure modes analyses are often conducted after the design process is complete. This results in mechanically accomplishing the task to satisfy some contractual requirement. With the great reduction in part failures, design error or oversight becomes one of the principal causes of failures occurring during ground test and system operations. Therefore, it is important to identify and eliminate all failure modes as early as possible in the design process. Failure modes and effects analysis can be divided into the four areas listed below.

Functional - The functional FMEA should be initiated early. It shows the interaction of all functions of the item and the role of the individual hardware elements in the overall item operation.

Design - The design FMEA considers all hardware elements, their inputs and outputs, down to the level necessary to determine the item's failure mode and the potential of failure.

DISCUSSION - Continued

Understand the Design - Continued

Interfaces - Commonly overlooked in an FMEA is the assessment of all the interfaces and interconnections. I know of one case where the conventional failure modes and effect analysis was performed on some complex hardware. By standard considerations, it was a good FMEA. However, after some problems during system operations a reliability engineer was assigned to reassess the failure modes in that hardware. He found over 100 single point failures in that system design. In order to accomplish this analysis he had to reconstruct the interconnects and the interfaces of all the elements in that system.

Product Design - This is a new concept now being introduced in some programs. It is one which I feel will be one of the most constructive. Great attention is often paid to circuit design and system design, but product design, which can greatly affect the manufacturability and, ultimately, the reliability of hardware is often overlooked. How many of you have had a product design review?

Another element in understanding the design is testing - test to determine design limitations, safety factors, and failure modes that may have been overlooked in the failure modes and effect analysis. Development tests and qualification tests generally are aimed at proving the design capability of the hardware. While this is valuable, I maintain that testing that uncovers no failures is wasted testing. Sometime during the development process, tests should be conducted on the hardware to accelerate the failures. Failures can be accelerated through the application of environmental or performance stresses. You cannot fully understand your design until you know how it operates under extremes of temperature, thermal cycling, vibration, or performance. If a system is designed to operate for several years, it is not possible to fully evaluate that system within normal time constraints without accelerated testing. This testing must also consider the interfaces. Until all the interfaces have been tested with the adjoining equipment, a full understanding of that unit is not possible.

One other area that I think is very important in understanding the design and helping to stay out of trouble is to modularize the functions and the hardware. By this I mean divide the functions and hardware into workable independent or semi-independent elements. Design decisions are difficult under the most straightforward of circumstances. If the hardware functions are so interrelated that each decision affects all elements then you can count on overlooking some element that later causes problems.

DISCUSSION - Continued

Design with Conservatism

One of the keys to the success of our space systems has been the conservative design. From early systems, parts derating has been an important factor in achieving high reliability. The thermal environment is extremely important. We generally try to derate our parts to about 20% stress at 25^{o} centigrade. If the temperature goes up the stress goes down. At the most, parts should not be operated over 50% of their rated values to achieve high reliability.

What have you learned from your past experience? Utilize the past experience and past problems to develop design guidelines. We have developed design guidelines aimed at preventing problems that previously have occurred or similar problems that might occur. Design check lists provide a good tool for implementation of design guidelines and for design review.

Design with Safety Factors. This is a significant factor in achievement of overall reliability. And finally, there is redundancy. I consider redundancy as a crutch to protect from what you do not know. It also protects from errors that may be introduced during the manufacturing process.

Parts, Materials and Processes Control

We establish a Parts, Materials and Processes Control Board (PMPCB) at the beginning of each program. The objective is not to prevent the introduction to the new parts and materials; rather it is to manage the introduction of new parts and materials, and to assure that proven parts and materials are used wherever possible.

Control of electronic parts through the manufacturing process, test, application, and installation in hardware is extremely important. As I said before, we have very few parts problems in Space. The driving force for the controls we place on electronic parts has been the failures on the ground. While high reliability parts may cost more initially, the savings in parts replacement, equipment repair, and test time usually more than compensate for the higher cost for the parts. Control on the materials is just as important. They should be properly specified, controlled, and analyzed so that all the materials characteristics are understood.

Probably the best term to describe the control of manufacturing process is "tender loving care". Introduction of new process specifications also is approved by the PMPCB. The associated quality controls

Parts, Materials and Processes Control - Continued

are tighter for high reliability products. Documentation is extremely important, so that when a problem does occur, you can trace its source and correct the cause.

Test and Analysis

I previously discussed the importance of the proper development and qualification testing. A technique that has been found to be very effective in producing a high reliability product, and at the same time reducing manufacturing cost, is environmental stress screening. This usually consists of thermal cycling, vibration, vacuum testing, shock, or some combination thereof, applied at various hardware levels. It may be applied as low as the card or module, or as high as the system. It is most frequently applied at the black box level. The objective of this testing is to stress the hardware sufficiently to uncover workmanship or parts defects. At the same time, it is also a good tool for finding design weaknesses. In one case, we applied thermal cycling to a spacecraft after it had completed all the acceptance tests and was ready for launch. In the process, a number of failures were uncovered, at least six of which would have caused significant spacecraft degradation during operation.

Generally tests should be conducted under conditions more severe than operational conditions. Concern is often expressed that this may cause wearout or early failures of your systems. Performed with discretion, I know of no failures in Space on Hughes systems that have been caused by over-testing. I do know of failures that have occurred because of oversight. One important aspect of testing is to test all modes of operations. This is not always possible during system testing, therefore some of that testing must take place at lower levels.

I think one of the keys to achievement of High Reliability Spacecraft has been the fact that every failure is treated as a critical failure. All failures should be reported, should be fully analyzed, and corrective action should be identified and instituted wherever possible. It sometimes takes time and costs money, but it will surely result in a more reliable system. Do not overlook the analysis of all test data. Numerous cases have occurred where failures occur in operation and subsequent analysis of test data showed that the symptoms of the failure had occurred but had been overlooked.

CONCLUSIONS

There are no simple answers for achieving high reliability in a high technology environment. Specific techniques that are applicable to one contractor, one system or one hardware element are not necessarily the same techniques that are applicable to another.

Failure-free hardware can be produced. The elements required to achieve failure-free hardware are:

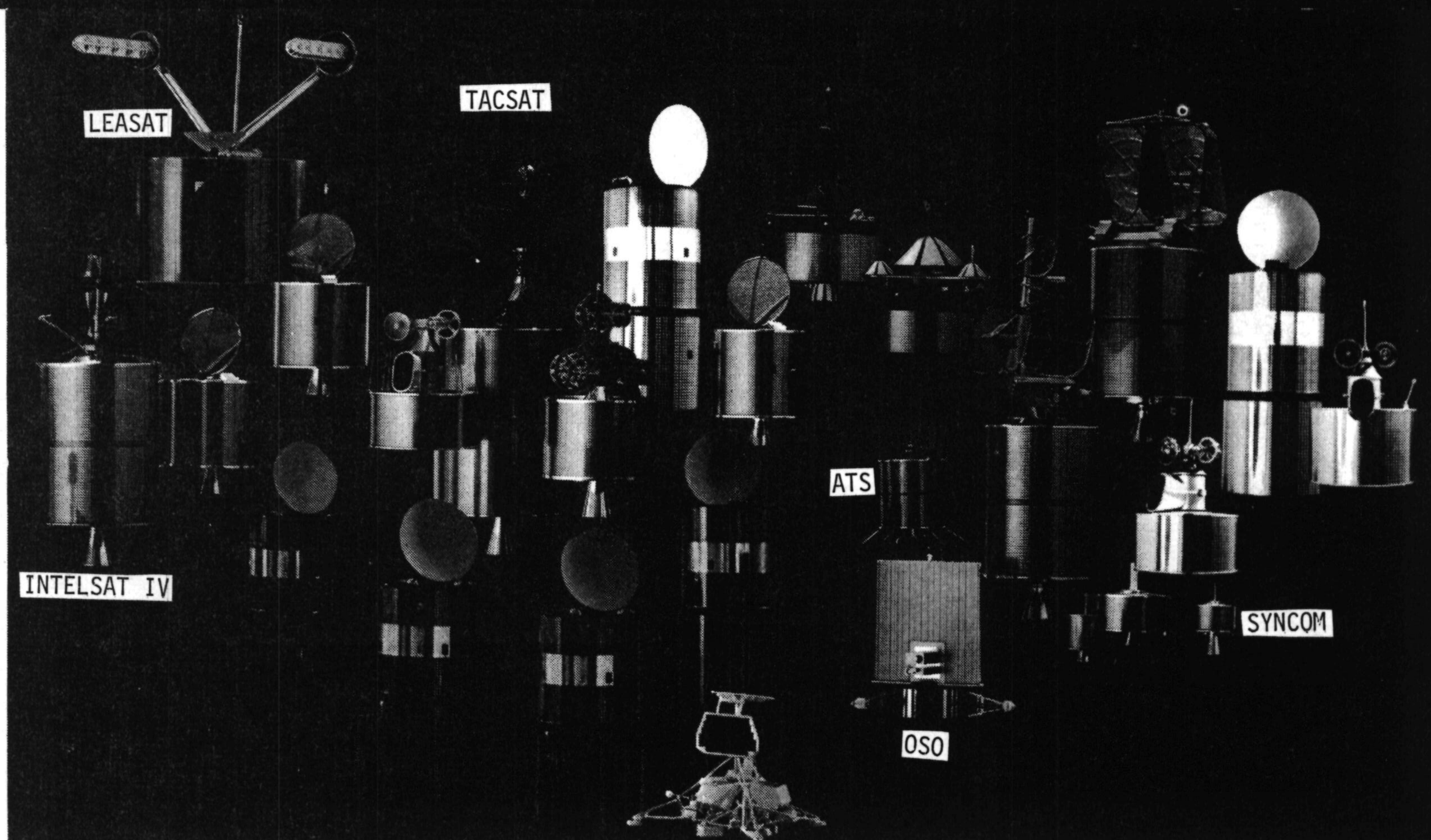
> Technical expertise to design, analyze, and fully understand the design.
>
> Use of high reliability parts and materials control of, and tender loving care in, the manufacturing processes.
>
> Testing to understand the system and weed out defects.

Proper application of the above requires sound judgement in decision making and the discipline necessary to follow proven practices.

HUGHES FAMILY OF SATELLITES

HUGHES

FIGURE 1.

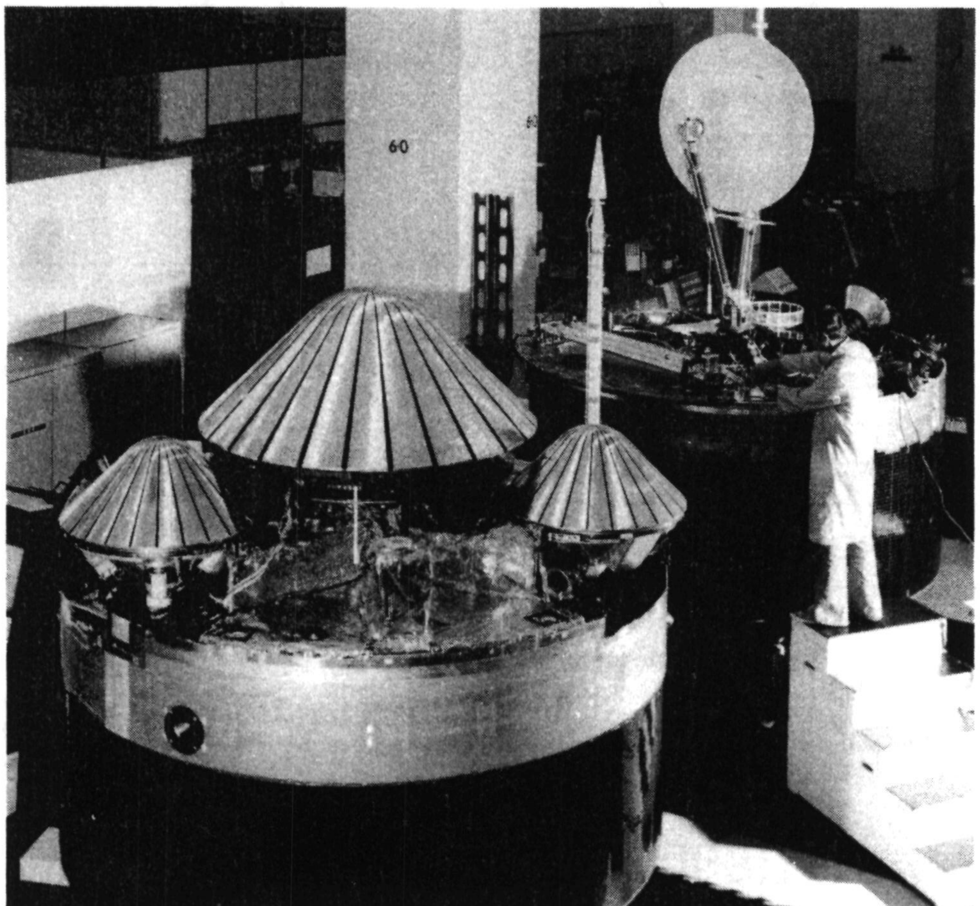


06100-86

PIONEER VENUS

HUGHES

FIGURE 2.



86100-49

ORBITER

- 522 KG (1218 LB) AT LAUNCH
- S BAND
- 193 W
- LAUNCHED: 20 MAY 1978

MULTIPROBE

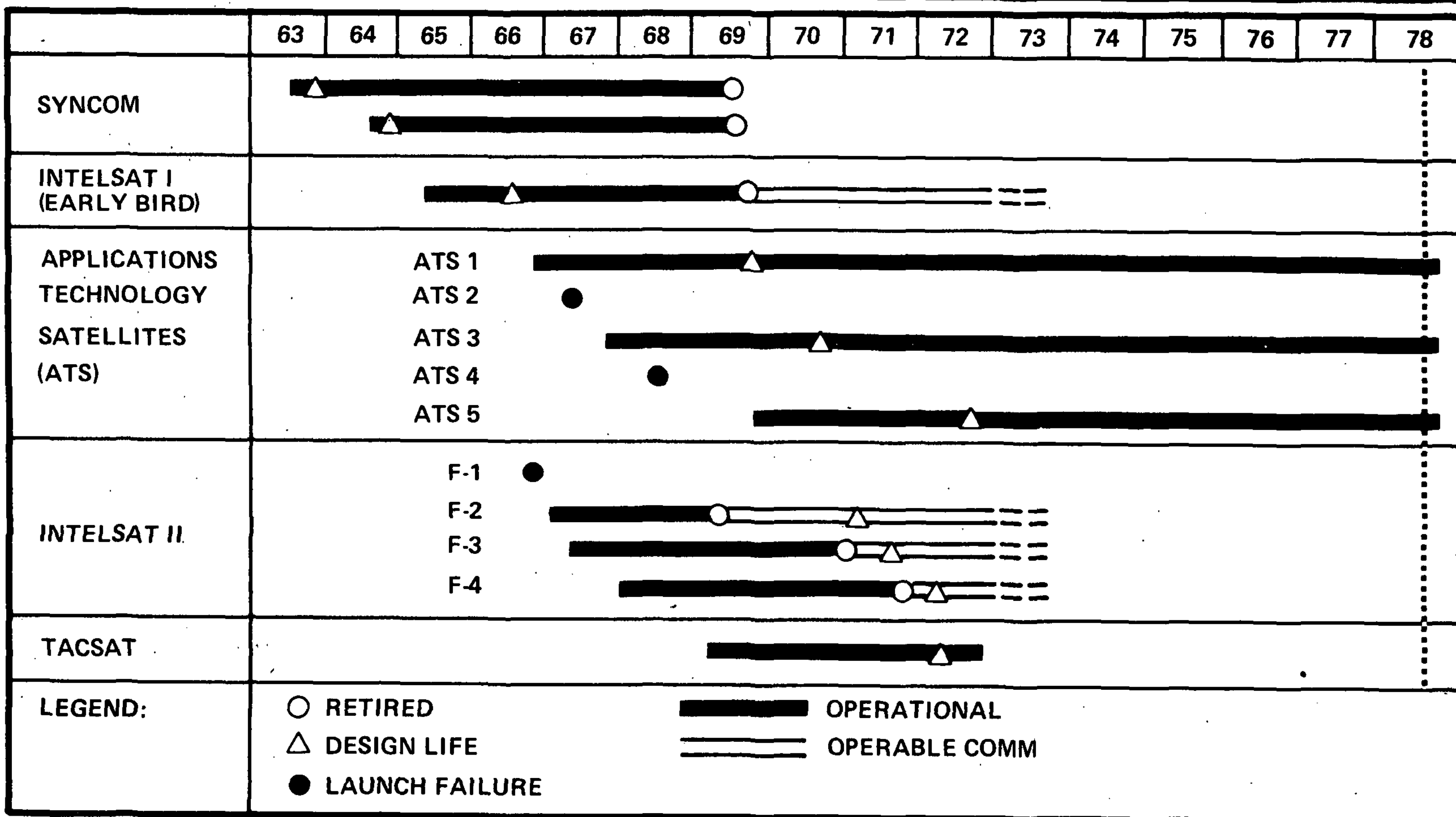
- 920 KG (2024 LB)
- 170 W
- LAUNCHED: 8 AUG 1978
- ENCOUNTER: 9 DEC 1978

77-61233

EARLY HUGHES SATELLITE ORBITAL PERFORMANCE

HUGHES

FIGURE 3.

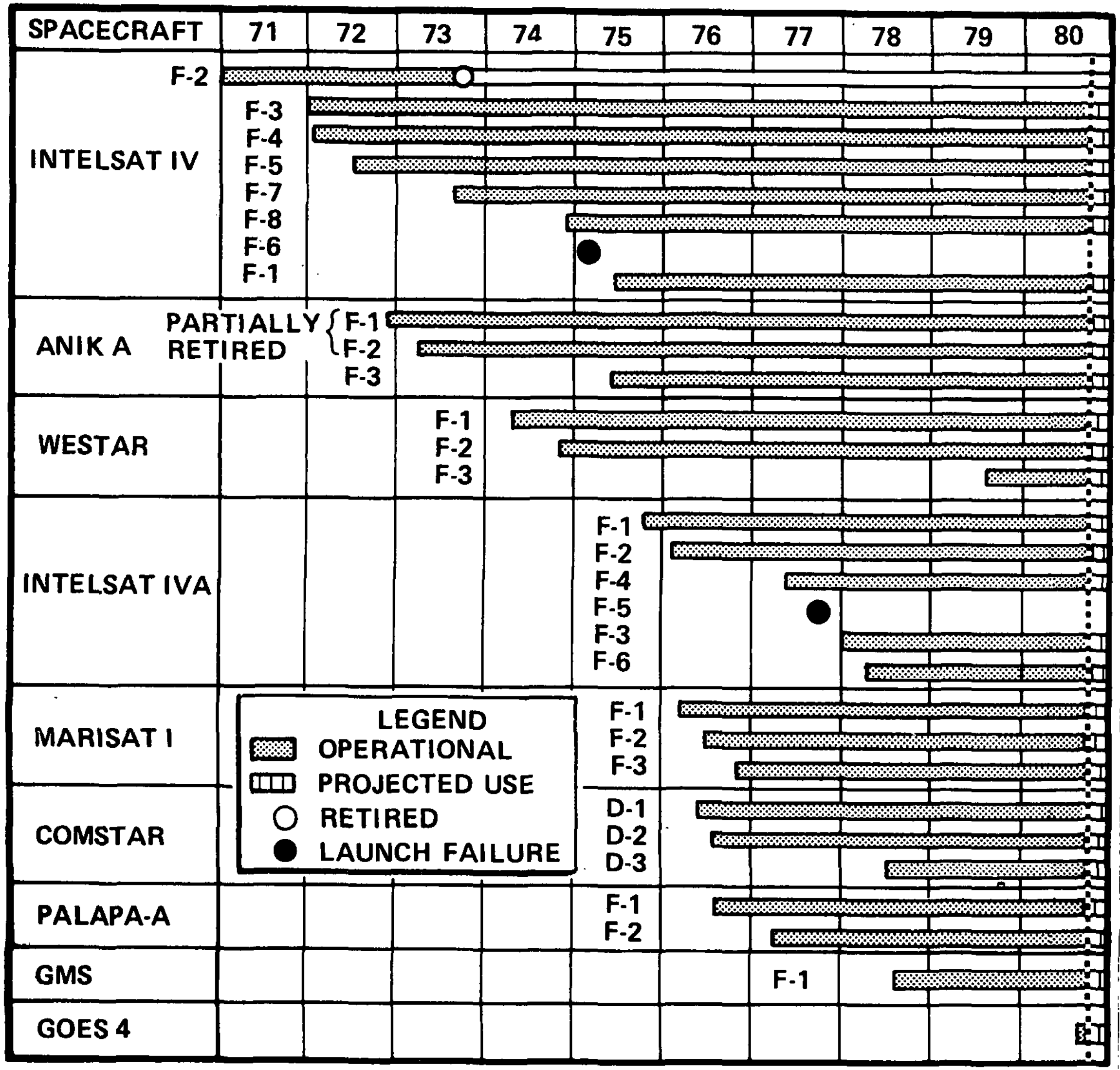


86100-7

HUGHES

FIGURE 4.

MODERN HUGHES SATELLITE PERFORMANCE



AS OF NOVEMBER 1980 HUGHES HAD OVER 200 ORBIT YEARS EXPERIENCE

06100-8