XI.15

RELIABILITY PREDICTION IN DESIGN DECISION

By

JOHN R. LEVINSON
Propulsion and Vehicle Engineering Division
George C. Marshall Space Flight Center
Huntsville, Alabama

A paper presented at the 10th National Symposium on Reliability and Quality Control, January 7-9, 1964, Washington, D. C.

RELIABILITY PREDICTION IN DESIGN DECISION

by

John R. Levinson

Propulsion and Vehicle Engineering Laboratory

George C. Marshall Space Flight Center

Huntsville, Alabama

Summary

Developing large, complex liquid-fuel rockets such as the Saturn I and Saturn V space vehicles requires intensive coordination to resolve design problems that affect many design and manufacturing groups at MSFC. Many problems which arise within the design laboratories require study and analysis by other branches and laboratories or the stage contractors. A method which has proved effective at MSFC is to discuss the problems, the proposed solutions, and the impact of the proposed solutions upon a particular engineering discipline or stage subsystem at weekly or special meetings. Representatives from design and other groups describe the problem and make their recommendation for the solution. Each group, including reliability, is expected to present the results of their study and analysis. This paper presents some case histories in which reliability prediction has played an important role.

The Design Review

These weekly meetings, which take the form of preliminary design reviews, are attended by representatives of the reliability, design, manufacturing, quality assurance, testing, and other departments. During each meeting, the factors which could affect the vehicle design are thoroughly discussed, the merits of the original and alternate approaches weighed, and a decision made on the design approach to be followed. In addition to reliability, other design trade-offs include payload, safety, checkout, maintainability, manufacturing, and quality control. The relative importance of each factor in relation to the other factors is also considered.

At these weekly meetings, a representative of a design group will make a presentation of the problem, describing the primary solution, and any feasible alternate solutions. The problem description will usually include:

1. Environmental conditions
2. System performance parameters and characteristics
3. Component complexity
4. Design criteria which must be met
5. Test results
6. Design or performance penalties associated with each solution
7. Trade-off factors

Based on the design groups evaluation of the above factors, a recommendation is made for a solution to the problem. Representatives of other groups are then called upon to present their evaluation of the problem, its trade-off factors and make their recommendations. That is, someone from quality will present the quality viewpoint and recommendation, someone from manufacturing will present the manufacturing viewpoint, someone from reliability will present the reliability viewpoint, etc.

As much as possible, coordination of possible solutions to the problems is performed outside of the meetings, leaving the attendees at the meetings free to discuss major problems which have not been resolved at a lower level. At the meetings it is the responsibility of the representative of each organization to clearly state his position on the problem. Because much of the coordination is carried out prior to the meetings, each organization is prepared to offer the impact of each possible solution on their area of interest. It is the responsibility

of each designer to inform all other interested groups of the possible solutions. A design information packet is usually prepared a week or more before the due date and distributed to each interested person. Revisions and deletions of the design data are coordinated on a daily basis.

The Reliability Contribution

Reliability plays an important part in the design decision. The reliability group is responsible for analyzing the primary and alternate design configurations, determining the configuration of optimum reliability, calculating the necessary trade-off factors, and recommending a course of action. Each possible solution necessitates development of a suitable mathematical model, determination of critical failure modes, generation of failure rate data when none exists, and a prediction of the inherent reliability of the system.

The reliability group is responsible for recommending other solutions when their analysis has shown that the design contains undesirable (catastrophic) failure modes, or that a complex design limits the inherent reliability. By showing how the inherent reliability can be improved, a performance penalty can often be reduced considerably while maintaining the system reliability at its present level. Performance penalties must sometimes be insurred to attain the required system reliability goals. The reliability predictions have also been used to point out possible areas of intensive testing to eliminate failure modes, determine test priorities, and show how costs can be reduced by alleviating excessive reliability requirements.

Case Histories

The 4 appendices to this report tell of actual cases in which reliability has had an important, direct affect on design decisions. As noted above, the reliability predictions have shown how performance can be improved while maintaining reliability (Appendix I & III), how redundancy has improved reliability (Appendix IV), and how reliability prediction helped show how system reliability could be improved and a potentially dangerous failure mode could be avoided (Appendix II).

In addition to these cases which have been officially documented as part of the minutes of themeetings, other designs are analyzed and reliability predictions made without a formal report.

APPENDIX I

SATURN I ENGINE-OUT CAPABILITY

System Description

The first stage of the Saturn I space vehicle, the S-I stage, is powered by a cluster of eight H-1 engines. The basic engine had already demonstrated a high reliability for booster flights in single engine static firings. Since problems and dangers might result when the engines were clustered, all feasible means and methods were necessary to ensure a high reliability of the clustered propulsion system. Redundancy is one method of increasing reliability. Therefore, in the early design phases of the booster, it was decided that the S-I Stage should incorporate an "engine-out capability"

S-I engine-out is analogous to the engine-out capability of a modern aircraft; alternate routes and destinations are possible even when an engine malfunctions during flight and must be shut off. In a similar manner, any single engine of the S-I stage may be shut off in flight, changing a possible mission failure into a simple non-catastrophic reduction in thrust. Engine failures would be detected by a simple sensor and, through automatic relay switches, the malfunctioning engine would be shut off, and the flight continued on the remaining seven engines.

Problem Description

In the present form of the engine-out capability, each engine utilizes a single sensor, with associated switching and logic circuits, to warn of impending or actual engine malfunction. Automatically, an engine which malfunctions (or which the sensor detects has malfunctioned) is shut off, preventing a catastrophic engine and booster failure. The thrust loss affects other systems directly and indirectly. Some of the factors which must be balanced against the reliability gain of the propulsion system using engine-out capability are:

1. The guidance scheme must allow for the thrust loss and longer burning time.
2. The control system, which gimbals the four outer engines to control the vehicle, must possibly now work with only three.
3. The structure must absorb larger loads due to greater angles of attack
4. The propellant distribution system must reduce residuals to a minimum, by redirecting propellants to the engines which are burning.

5. Trajectory shape and payload are affected by the time of engine out.

Method of Analysis

Early studies showed a significant increase in propulsion system reliability due to the engine-out capability. The mathematical model shown below describes system success if no more than one engine of the 8 fails to perform within the required limits:

$$P_s = (P_e)^8 + 8(P_e)^7 (1 - P_e)$$

Where P_s = probability of propulsion system success

P_e = probability of single engine success

Note that this simple model is based on the first two terms of the binomial expansion $(S + F)^8 = 1$.

It was soon discovered that the above model did not accurately describe the actual conditions. It lacked terms which

1. Described sensor system reliability
2. Discriminated between catastrophic and non-catastrophic engine failure modes
3. Included the possibility of damage to other engines by catastrophic failure of an engine
4. Discriminated between non-catastrophic failure modes which are sensed and those which cannot be sensed.

A later but still incomplete model used to describe the system was as follows:

$$P_s = (P_c)^8 \Big[(P_e)^8 \left[R_s{}^8 + 8R_s{}^7 (1 - R_s) \right] + 8P_e{}^7 (1 - P_e) (R_s)^8 \Big]$$

Where R_s = the probability of sensor system success

P_c = the probability of catastrophic failure not occurring

P_e = the probability of non-catastrophic failure not occurring

As the mathematical model was developed, an assessment of the H-1 single engine reliability was in progress. Single engine static firing tests were used in this assessment. Reliability estimates were based on the standard assessment techniques of binomial and exponential distributions (MTBF). (A reliability estimate was available from the engine manufacturer, but, based upon a standard demonstration procedure, it was not suitable for use in the mathematical model).

Possible Solutions

As the vehicle was developed, it became necessary to finalize the design of other systems which were directly affected by the use of the engine-out capability (e.g., navigation and control systems). Thus, there were three choices regarding engine-out capability which could be made:

1. A single-engine-out capability throughout flight
2. A single-engine-out capability beginning at a certain flight time
3. No engine-out capability

FIGURE I - 1

SATURN I ENGINE-OUT CAPABILITY ANALYSIS

Engine-out Condition	Propulsion System Reliability Gain	Performance Penalty
1. From liftoff	Highest	Greatest Loss
2. At a given time during flight	Some*	Some Loss*
3. None	None	None

*Reliability gain and performance loss depend on the flight time for which engine-out capability is designed to be invoked.

Problem Analysis

As stated previously, early studies showed a large increase in propulsion system reliability due to the engine-out capability. With a higher estimate of single engine reliability due to development progress, the more complex

mathematical model showed an almost negligible gain in propulsion system reliability by using the single engine-out capability throughout booster flight. A performance penalty is associated with the use of the engine-out capability throughout booster flight. The later in flight that the engine-out capability was invoked, the smaller the performance penalty. The no engine-out capability showed no performance penalty.

Recommended Solution and Results

Since the reliability analysis showed little gain in reliability, it was recommended that the S-I engine-out capability be dropped as a controlling design consideration for the entire booster flight. However, the engine-out capability was retained for the following reasons:

1. The possible need to have a very high reliability booster at a later date. For this scheme the engine-out capability would be available throughout flight, with the performance penalty.

2. The needs for crew abort. By continuing the flight for a short time, even with reduced thrust and control, more favorable abort conditions might be obtained.

3. System complexity was unchanged by the engine-out capability when "locked out" until a given time.

The solution which was reached was a compromise. The performance penalty was minimized by allowing the engine-out capability to be effective only after a certain time of booster flight.

For this case the reliability analysis showed that a large performance penalty was being incurred for only a small gain in reliability. It also prevented a possible loss in the reliability of other systems due to the complexity necessary to accommodate the engine-out capability throughout flight.

APPENDIX II

SATURN V VEHICLE

UMBILICAL DISCONNECT

System Description

The Saturn V vehicle consists of 3 separate stages, an Instrument Unit and the manned payload. Each stage and the payload requires connections to the ground for

1. Transmitting the vehicle functions and status to the blockhouse
2. Supplying electrical, pneumatic and hydraulic power to the vehicle before lift-off
3. Filling, topping and draining propellants.
4. Providing access to the intertank and interstage areas for service or maintenance.

After engine ignition, the 5 booster stage engines are monitored for proper performance while the entire vehicle is held down. Once all systems, including the engines, check "go", the vehicle is ready for release. At this time all umbilical arms, propellant lines, and access arms must be rapidly disconnected and swung away from the vehicle to prevent collision between an arm and the vehicle.

Problem Description

Because a disconnect failure at lift-off could cause a serious vehicle flight malfunction, it was necessary to decide on an optimum disconnect method. The disconnect scheme is complicated by the holddown period. The operation of the first stage is being monitored during the holddown period. Any indication of malfunction from any of the critical parameters being monitored will cause immediate cut-off of the engines. Thus, one design criteria is that all umbilical arms be disconnected at lift-off so that the vehicle can be returned to ground control in the event of an aborted launch. Maximizing the probability of successful lift-off requires that all umbilicals be disconnected and retracted prior to lift-off; in this way the retraction could be confirmed.

FIGURE II-1 COMPARISON OF UMBILICALS DISCONNECTED AT LIFTOFF

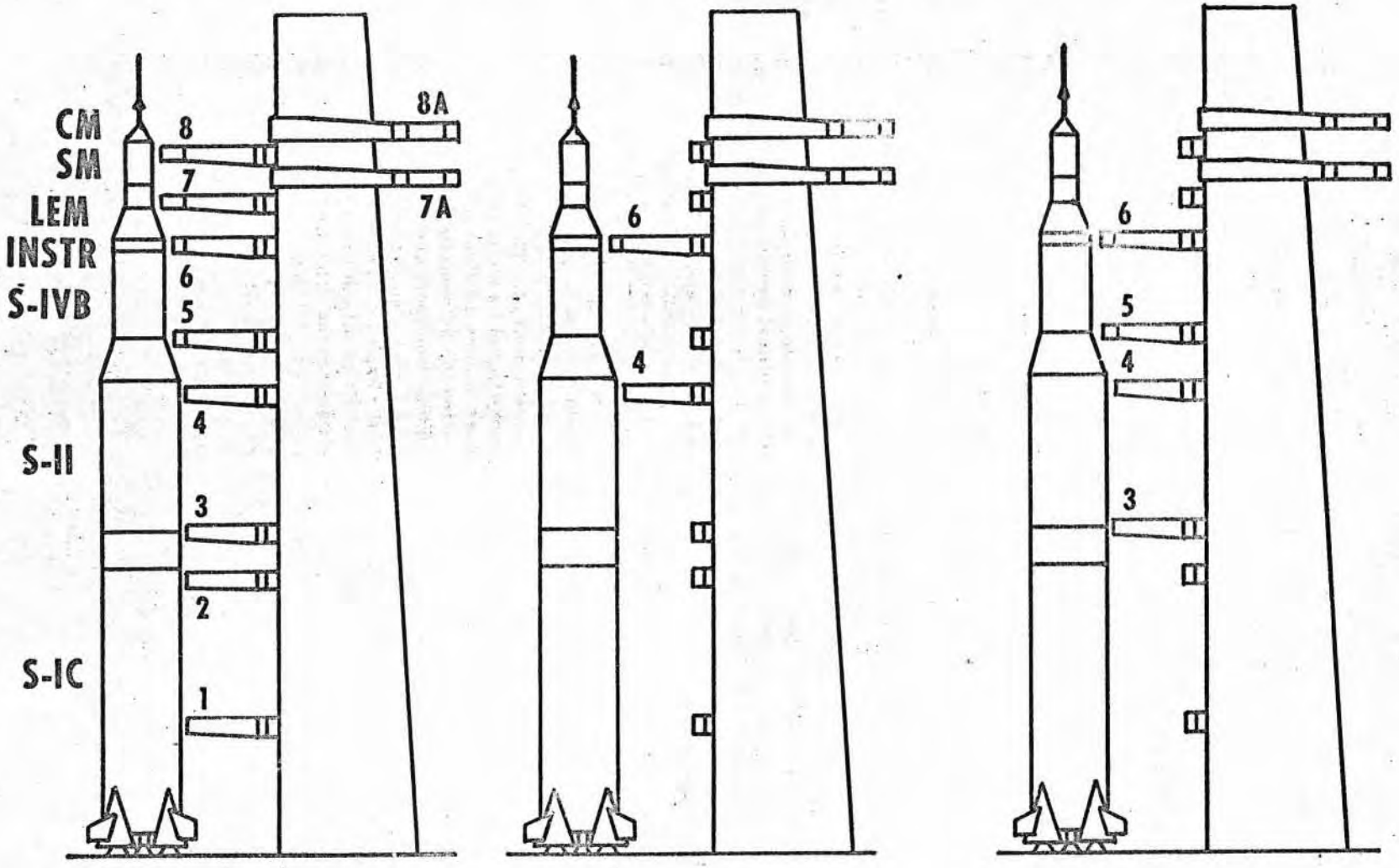

FIGURE II-1A
UMBILICAL DISCONNECT
METHOD 1

FIGURE II-1B
UMBILICAL DISCONNECT
METHOD 2

FIGURE II-1C
UMBILICAL DISCONNECT
METHOD 3

FIGURE II-1 COMPARISON OF UMBILICALS DISCONNECTED AT LIFTOFF

Method of Analysis

For this analysis the reliability prediction was not based on a detailed analysis of the arm disconnect and retract mechanisms. Since the complexity of all arms would be about equal, it was only necessary to make a relative comparison of the 3 proposed disconnect schemes and not an absolute prediction. A reasonable reliability value of 0.99 was assumed for the successful disconnection and retraction of each arm, based on previous umbilical history. The reliability prediction was also necessary to compare the modes of failure of each of the proposed schemes. While differences might exist between the arms, assuming a single arm reliability greatly simplified the analysis. The operation of each arm is mutually independent so that the product rule can be used to calculate the reliability of successful disconnect and retract.

For this solution it was necessary to maximize the number of vehicles which successfully pass lift-off, while minimizing the number of aborted launches due to umbilical malfunction. The transfer of vehicle control to the ground and de-tanking of propellants in the event of an aborted launch are also important factors.

Possible Solutions

The following solutions were proposed:

1. Disconnect all umbilical arms and propellant couplings at lift-off (See Figure II-1A).
2. Reroute critical functions so that only one umbilical per stage is disconnected at lift-off. (See Figure II-1B)
3. A compromise of the above.

Problem Analysis

Booster stage propellant lines are lift-off disconnects, using a simple ball-seal, spring loaded mechanism. Critical propulsion system electrical and pneumatic lines are routed through tail plug disconnects which pull out at first vehicle motion. See Figure II-1.

When the umbilical arms and propellant couplings are disconnected at lift-off, there is no need to reconnect them if there should be an aborted launch. The transfer of vehicle control to the ground is also not a problem should an abort be necessary. But to disconnect 8 umbilicals at liftoff (including 2 cryogenic propellant couplings per stage) posed severe design and reliability penalties. See Figure II-1A. Complex redundant swing arm retraction mechanisms would be necessary. The probability of successful cryogenic propellant coupling disconnect was low. Because the disconnection occurred at lift-off, there was no way to confirm that the retraction of the swing arm had begun.

The second proposal, to disconnect all possible umbilicals and propellant couplings before lift-off, showed the highest predicted probability of successful lift-off. See Figure II-1B. Only 2 umbilicals would be required to disconnect at vehicle release, one for each upper stage, arms 4 and 6. The requirement to have only one disconnect per stage imposed a severe weight penalty on each stage. Hydraulic and pneumatic tubing, ducts, electrical cables, etc., must be rerouted to the single umbilical. This proposal also creates a potentially dangerous situation in the event of a vehicle abort during holddown. Should a launch abort be necessary during the holddown period, the upper stage propellant lines must be reconnected, a difficult accomplishment with a swaying vehicle as a target. The reliability analysis also pointed out that, though the probability of successful lift-off was higher than the first case, the probability of the vehicle successfully passing from ignition through lift-off is unchanged from the first proposal to the second. In this proposal the umbilicals are disconnected before lift-off so that now any failure to disconnect causes an aborted launch rather than a flight failure.

The third proposal was a compromise between proposals one and two. In this disconnect scheme, all vehicle electrical and pneumatic lines which would be required for vehicle safing are routed to 4 umbilicals which are disconnected at lift-off. Arms 3, 4, 5 and 6, See Figure II-1C. The propellant fill and drain lines (attached to umbilical arms 3 and 5) are disconnected before engine ignition, but not retracted. The remaining 4 umbilicals (arms 1, 2, 7 and 8) are disconnected and retracted prior to engine ignition, eliminating an aborted launch due to disconnect malfunction during the critical holddown period. There was some weight and payload penalty incurred by the use of this scheme, but it was not as great as proposal 2. It also required that the propellant couplings be reconnectable in the event of an abort caused by vehicle malfunction during holddown, but reconnection only has a higher probability of success than "chasing" the vehicle, aligning arms and couplings to the vehicle and then reconnection. (As in method 2)

Note that by this method one-half of possible disconnect malfunctions were moved to the less critical time before ignition.

Recommended Solution and Results

The reliability group recommended that the umbilical disconnect method 3 (See Figure II-2) be adopted. This recommendation was based on

1. An increase in the probability of successful vehicle liftoff from 0.83 to 0.86.
2. A 50% reduction in the percent of vehicles lost due to disconnect failure
3. An acceptable performance penalty for the gain in reliability

The recommendation was adopted and implemented.

FIGURE II-2

RELIABILITY ANALYSIS OF UMBILICAL DISCONNECT PROPOSALS

Event	Cumulative Probability of Success		
	Disconnect Method 1	Disconnect Method 2	Disconnect Method 3
Ignition	1.00	1.00	1.00
All Engines OK	0.90	0.90	0.90
All Systems Go	0.90*	0.85*	0.90*
Lift-off	0.83	0.83	0.86
Percent vehicles lost due to disconnect failure	8	2	4
Percent aborted launches	10**	15***	10**

*Using fictitious reliability of .99 for each umbilical arm.
**Due to vehicle malfunction only.
***10% due to vehicle malfunction, 5% due to disconnect malfunction.

APPENDIX III

S-IC AND S-II STAGE SEPARATION

The function of the S-IC booster (the first stage of the Saturn V) is to place the upper stages of the vehicle in space, at a certain velocity, with a given attitude, at the required time. Once the booster has accomplished its task it is necessary to separate the spent stage from the upper stages, allowing them to continue. The lower stage should be separated and the engines of the next stage ignited as soon as possible after cutoff of the lower stage to minimize trajectory perturbations and performance penalties. But sufficient time must be allowed for thrust decay and damping of torques which might be present from lower stages operation.

stage retro motor firing and S-II stage ullage motor firing. The upper stages then coast out of the interstage under the momentum applied by the retro and ullage motors. The S-II stage engines are ignited a short time after the stages have separated.

Analytical studies showed that the single plane separation method was satisfactory; separation clearance, S-II stage control after separation, and vehicle hardware requirement met the required design criteria.

However, the quest for greater payload capability caused investigations into other separation methods. These studies showed that a significant gain in payload was possible with a dual plane separation scheme because of the different separation sequence. Several different methods of dual plan separation were investigated to determine a method of minimum degradation to reliability and maximum payload capability.

TABLE III-1

DUAL PLANE SEPARATION COMPARISON

Separation Method	Engine Condition at Interstage expulsion	Interstage Expulsion Method	Clearance Margin	Separation Plane (Stations)	Predicted System Reliability	Payload Difference
Single Plane	Not applicable	Not applicable	Adequate	196	.9967	-------
Dual Plane "A"	Operating	4-300 lb retro motors, rails and engine impingement	Not applicable	-16/196	.9958	-2200 lb*
Dual Plane "B"	Not Operating	8-2000 lb retro motors and rails	Adequate	-16/196	.9948	-100 **
Dual Plane "C"	Operating	Engine Impingement	Adequate	-16/196	.9961	+1000***
Dual Plan "D"	Operating	Engine Impingement	Adequate	85/196	.9958	+800****

*Payload difference due primarily to added guide rails and structure beefup
**Guiderai's weight overbalances other weight losses
***The retro motor, ullage motor and mounting structure weight is reduced
****Change in separation plane increases ullage motor weight

Problem Description

As originally conceived, the separation of the S-IC stage from the S-II (second stage) would take place as a single event along a single plane (Station 196). The scheme is a "coast-out-of-the-hole" scheme in which the stages are physically separated, followed by lower

Method of Analysis

For each of 4 different dual plane separation methods, reliability predictions were based on the detailed analysis of the subsystems. For each separation method, reliability block diagrams were completed and subsystem components assigned a reliability value. Failure effect analysis pin-pointed catastrophic and critical failure modes and the probability of their occurrence.

Possible Solutions

The possible solutions are shown in Table III-1.

Recommended Solution and Results

While the single plane separation system showed the highest separation reliability, the desire for greater payload capability caused a change to the dual plane separation system 'C'. Note that the reliability of this system is the highest of all dual plane methods and shows a significant payload increase. Note though that this is lower than the single plane separation system reliability.

APPENDIX IV

S-IC AND S-II RETRO AND ULLAGE MOTOR-OUT CAPABILITY

System Description

After completion of the powered flight of the S-IC (first stage of the Saturn V), it is necessary to separate this stage from the S-II stage. To help insure a clean separation of the stages, solid propellant rockets are mounted on the booster to reduce its velocity relative to the upper stages. The retro motors also cancel the residual thrust of the engines after cutoff. This prevents possible collision between the two stages. In addition to the retro motors, solid propellant ullage motors are used on the S-II stage to provide a slight accelerating force to settle propellants and prevent engine turbopump cavitation at engine start.

Problem Description

The addition of retro and ullage motors to the vehicle is necessary to insure successful separation of the stages and successful engine start. It reduces the probability of vehicle success by increasing system complexity. There are 8 retro motors on the S-IC stage, mounted in pairs within the engine fairings at the rear of the stage. An additional 8 ullage motors are mounted, also in pairs, on the S-IC/S-II interstage and remain attached to the interstage at stage separation.

Method of Analysis

The operation of each retro motor is mutually independent. The probability of retro motor success can be expressed as the following series relationship:

$$R_{system} = (R_{retro})^8$$

Similarily, the probability of ullage motor success can be expressed as

$$R_{system} = (R_{ullage})^8$$

Note that even with a predicted retro motor reliability as high as 0.995, the system reliability is reduced to 0.96. The effect on vehicle reliability of two systems with such low reliabilities could not be tolerated, obviously. Some means were necessary to increase the reliability of the retro and ullage motor systems. The use of redundancy by utilizing a motor-out capability was one method investigated. This increases the system reliability from 0.96 to 0.9986, a significant increase. Other methods of increasing reliability which were investigated included raising the inherent motor reliability. The probability of retro or ullage motor success with a motor-out capability is determined by

$$R_{system} = R^8 + 8R^7 (1 - R)$$

Separation criteria and tolerances are set so that successful separation takes place even though one retro motor and one ullage motor fail. Nominal design conditions for the retro and ullage motors are shown in Figure IV-1. A search of available records of solid propellant motor firings for reliability and design information revealed that no solid propellant motor had been built or fired in the thrust range and burning time of the retro motor. This caused somewhat severe design and reliability penalties, since an entirely new motor must be developed for this particular application. The lower thrust level and longer burning time of the ullage motor indicated that there would be no severe design or reliability problems.

FIGURE IV-1

RETRO AND ULLAGE MOTOR DESIGN CONDITIONS

	Thrust	Burning Time
Retro Motor (Each)	100,000 lb.	0.5 seconds
Ullage Motor (Each)	22,000 lb.	4.0 seconds

Results of all available solid propellant motor firings were assessed to determine a reliability which could be used as a base for predicting the reliability of the retro and ullage motors. The data was also analyzed to determine the frequency of undesirable failure modes, such as chamber burnthrough or detonation.

Possible Solutions

The possible solutions were:

1. Keep the thrust and burning time as shown, but do not use a motor-out capability.
2. Keep the thrust and burning time as shown, and use a motor-out capability.
3. Increase the inherent reliability by a Quality Control and Failure Recurrence Prevention Program.
4. Increase the inherent reliability by changing the thrust level (hence burning time) to ease the motor development problems or to use an "off-the-shelf" motor.

reliability was feasible, with an increase in motor development time and cost. A decrease in failure rate of an order of magnitude was necessary to compete with the motor-out conditions.

Changing motor thrust a small amount (total impulse must remain constant) to ease development problems would not solve these problems. The same problems would exist at the lower thrust level. Reducing the thrust sufficiently to use an "off-the-shelf" motor caused a weight penalty by the change in coast time. It also reduced the performance margin reserved for growth of thrust decay impulse of the booster engines, which could lead to possible collision between stages. The results of the analysis are shown in Figure IV-2.

It was decided that the loss in payload was a small price to pay for the large increase in system reliability. Therefore, operation

FIGURE IV-2

MOTOR-OUT ANALYSIS

Motor Operating Condition	R_{motor}	R_{system}	Payload Penalty	Estimated Relative Cost
(1) No motor-out	0.995	0.96	----	1.0
(2) Motor-out	0.995	0.9986	-90	1.0
(3) No motor-out	0.9995	0.996	----	1.5
(4) Motor-out	0.9995	0.99998	-90	1.5
(5) No motor-out	0.9995	0.996	----	0.75
(6) Motor-out	0.9995	0.99998	-200	0.75

Problem Analysis

As mentioned previously, a severe reliability penalty is incurred by not using a motor-out capability, eliminating solution (1) above from further consideration. Using the thrust and burning time shown in Figure IV-1 with a motor-out capability increases system reliability at a small cost in payload. See Figure IV-2. Asking for an increase in inherent motor

condition (2) above was chosen for the design of the retro and ullage motors. In this example, the reliability prediction showed that a large increase in reliability could be possible with only a small weight penalty.