DEVELOPMENT EFFORT TO ACHIEVE RELIABILITY

by

G. M. Clark
and
K. B. Haigler

Rocketdyne
A Division of North American Aviation, Inc.
Canoga Park, California

Presented at the
6th Annual West Coast Reliability Symposium
University of California at Los Angeles, Los Angeles
California

20 February 1965

DEVELOPMENT EFFORT TO ACHIEVE RELIABILITY

by

G. M. Clark

and

K. B. Haigler

Rocketdyne

A Division of North American Aviation, Inc.
Canoga Park, California

INTRODUCTION

The development of a large liquid rocket engine can represent the expenditure of several hundred million dollars of effort. Before 30 percent of the contracted development funds have been expended, however, the engine will probably have operated for the mission duration. The capability to operate at least one successful test early in a development program is evidence of achieving a minimal reliability level, but the major objective of the development program is producing a design which performs reliably. A rocket engine reliability prediction must view reliability as a dynamic concept, constantly being altered by development effort.

Since achieving reliability consumes the majority of the engine development expense, the concept selection phase will be actively concerned with reliability as a design and program parameter. An advance planning effort should not only select an inherently reliable design concept, but also one that is capable of being efficiently developed. Appropriate provisions for allocating development effort to assure efficient reliability growth must be incorporated in the development plans. Because these characteristics adversely affect engine weight, performance, and development cost, a qualitative evaluation does not adequately support sound decisions.

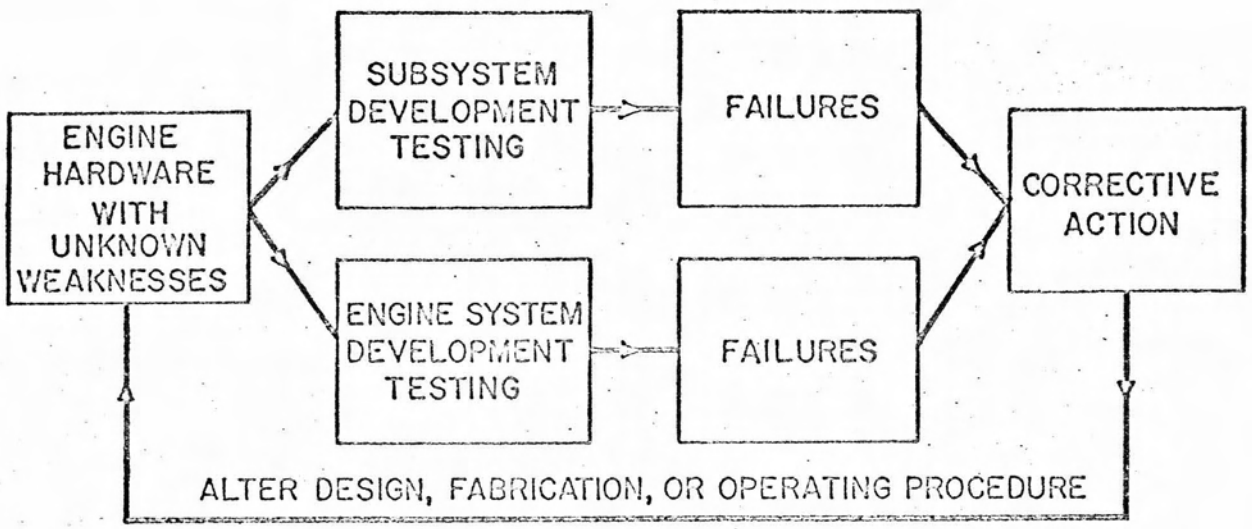
DISCUSSION

TEST-FAIL-FIX CYCLE

A continued repetition of test-fail-fix cycle conceptually describes the manner in which the development process produces a reliable design. After the hardware has been designed, it possesses a finite number of weaknesses, although the exact nature of each defect is unknown. As the hardware is tested, the weaknesses produce failures or symptoms of failures, then an attempt can be made to remove the deficiency from the hardware. An analysis is performed to isolate the actual cause from symptoms, and corrective action designed to eliminate the failure cause is generated. The upper portion of Fig. 1 illustrates the development process.

The key to this development cycle is to force the unknown defects to produce symptoms of failure, generate corrective action, and verify through aggressive testing the effectiveness of the fix. The desirability of inducing failures early in the development program is readily understood by examining the mean ratio of failures to successful corrections that have been observed in the past. Some programs have experienced average ratios of 4 for turbopump failure causes, 5 for combustion chamber causes, 10 for instability causes, and 2.5 in the remainder of the engine system. It is preferable to locate the problems during the component development phase, then the more expensive system tests can be focused on those problems which are system oriented without being hampered by the more basic development problems.

It is revealing to note the point in the mission cycle when a particular failure symptom occurs. Some failure symptoms are observed during the start and shut-down portion of the mission cycle, whereas another class of failure symptoms occurs during mainstage operation. A failure cause, which is originally a minor malfunction during the start but progressively deteriorates until the symptoms occur, would be considered a mainstage failure symptom.



CONCEPTUAL RELIABILITY GROWTH MODEL

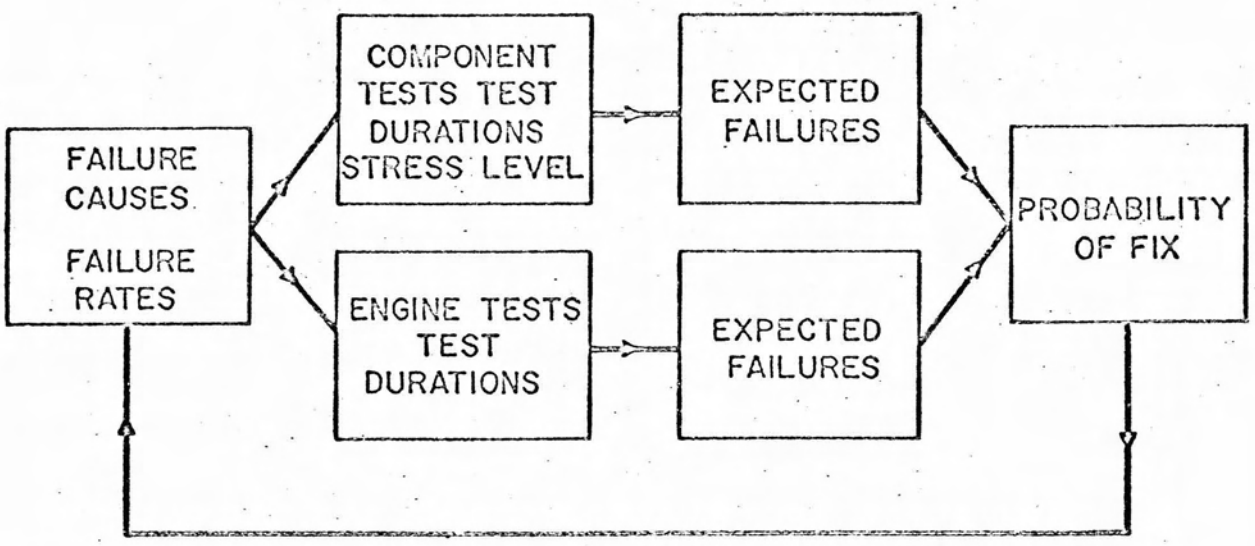


Figure 1. Development Process

Many failure symptoms require more than one successful corrective action to eliminate all the contributing causes. An example of this type of problem would be combustion instability. Instability requires the removal of many contributing causes; the problem is reduced by each design change which removes some but not all of the potential causes. Figure 2 illustrates a possible path that a symptom failure rate might follow as successive design changes are introduced.

When integrating the results of both component and engine system testing, it becomes evident that the rate of failure of a failure cause can be influenced by either the amount of hardware on test or the stress level at which the hardware is operated. For example, a combustion chamber may be operated as a component employing only a segment of the total engine combustion chamber. The geometry and environment of each tube and orifice remain equivalent to the engine while the amount of hardware is reduced. In this case, the failure rate for a combustor failure cause may vary directly with the number of design features. Also, a bomb test is designed to rate the stability of an injector through introduction of an explosive disturbance which significantly increases the probability of rough combustion.

The model of reliability development process incorporates the following features:

1. The occurrence of a failure symptom initiates corrective action which has a chance of successfully eliminating the cause or failing in the attempt.
2. The probability of some failure symptoms occurring may be affected by the intended mainstage duration.
3. The improvement in the failure probability of a symptom is described by a step function.
4. Based on the type of development testing, the failure probability of a cause can be varied by a stress factor.

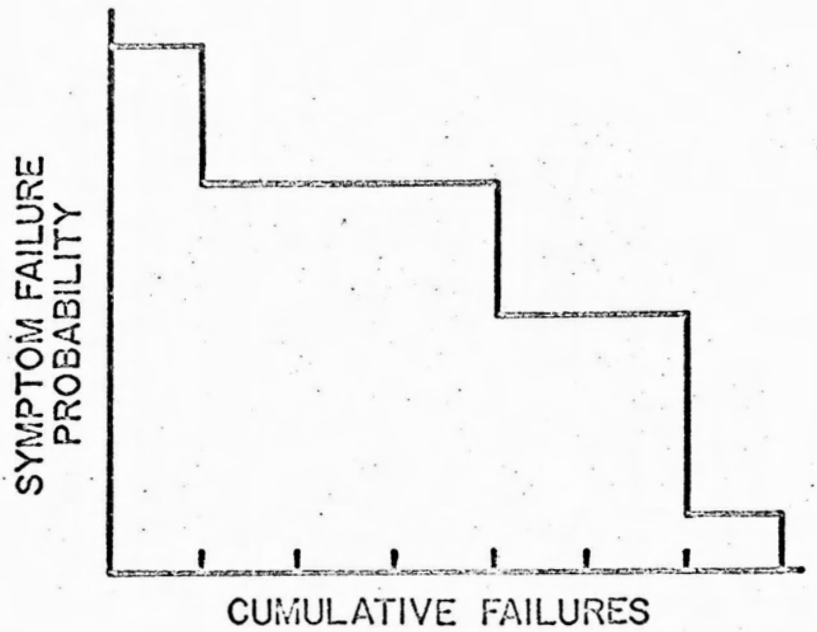


Figure 2. Possible Path of Sympton Failure Rate

MATHEMATICAL MODEL

For this application, it is assumed that the system has two classes of weakness that may cause failure: those occurring during the start-stop transient and those occurring during steady-state operation.

During the start-stop transient the probabilities of weakness causing failure are independent of intended duration. Failures that occur during this period are termed "start failures," and their probabilities of occurrence are described by the binominal distribution.

After the system has passed through the start phase, failure probabilities are dependent upon intended test duration. The probabilities of occurrence of these failures is best described by the exponential distribution, and failures that occur during this period are termed "mainstage" failures.

Definitions

Reliability - The probability of start and mainstage operation without failure for full-mission duration.

Start Reliability - The probability of no failure during the start phase.

Mainstage Reliability - The probability of no failure during mainstage for full duration, given a successful start.

Failure-Cause Unreliability - The probability of a particular weakness causing failure under nominal conditions at the beginning of the development period, given no other weaknesses exist.

Failure-Cause Reliability - One - failure-cause unreliability

Failure-Cause Probability of Occurrence - The probability a particular weakness produces a failure in a given test, if it has not been eliminated. This is not necessarily equal to the failure-cause unreliability.

START RELIABILITY

Conditions and Assumptions

1. The reliabilities of the system or failure causes prior to testing are termed "initial reliabilities."

2. The initial-start reliability of the system is equal to the product of the initial reliabilities of each failure cause. The failure causes are independent, and any number can produce a failure on the same test.

3. When a failure occurs on a test, an analysis is made. If the cause of failure is discovered, corrective action is attempted. There is a certain probability that a cause will be discovered and corrected when it occurs. If it is corrected, its probability of recurrence is zero; if not, its probability of recurrence remains unchanged.

4. If only one failure cause occurs on a test, its probability of discovery and correction is defined as "P." This P remains constant and applies to each failure resulting from that cause throughout the entire test program.

   If the failure cause occurs with one other, its probability of discovery and correction is reduced to some constant value $(P \times X)$, where $0 \leq X \leq 1$.

   If a failure cause is one of three occurring, its probability of discovery and correction is lowered to some constant value $(P \times Y)$, where $0 \leq y \leq X$.

   If four or more failure causes occur at once, none of them will be discovered and corrected.

5. After N tests there is a certain probability that a failure cause has produced one or more failures and has been corrected. This is its "probability of elimination." An expected value of the unreliability of each failure cause after a certain number of tests is found by multiplying the initial unreliability of a failure cause by the probability that it has not been eliminated. The expected reliability of the system is the product of the expected reliabilities of all failure causes.

6. Although the unreliability of a failure cause will remain constant until it is eliminated, its probability of failing alone may increase as testing increases, since other causes may have been eliminated.

7. Overstress testing may be employed in such a way that the probability of occurrence of a failure cause will be multiplied by a constant factor (called the "overstress factor") to alter its failure probability.

Definitions

M = Total number of start-failure causes present in the system

RS_o = Initial start reliability

q_i = Initial unreliability of the i^{th} start-failure cause, where $i = 1, M$

RS_j = The expected system start reliability after j tests

$E_j(q_i)$ = The expected value of the unreliability of the i^{th} start-failure cause after j tests

P_i = The probability of discovering and correcting the i^{th} start-failure cause if it occurs alone

$B_{i,j}$ = The probability of not having eliminated the i^{th} start-failure cause after j tests

φ_i = A stress factor by which the unreliability of the i^{th} start-failure cause is multiplied to alter its probability of occurrence to $\varphi_i\ q_i$, where $\varphi_i > 0$, $\varphi_i\ q_i \leq 1$. At nominal conditions $\varphi_i = 1$.

The Model

$$RS_o = \prod_{i=i}^{M} (1-q_i)$$

The actual value of the unreliability of the i^{th} start-failure cause after j tests is equal to q_i with probability $(B_{i,j})$ or equal to zero with probability $(1-B_{i,j})$

$$E_j(q_i) = q_i\ B_{i,j}$$

Given one start-failure cause in the system with unreliability (q) and the probability of discovery and correction (P), the probability that it has not been eliminated after j tests:

$$1 - \sum_{r=0}^{j-1} \left[(1-q) + q(1-P)\right]^r q \times P$$

for i start failure causes, after j tests:

$$B_{i,j} = 1 - \sum_{k=1}^{j}$$ (The probability the i^{th} cause occurs and is corrected on the k^{th} test) x (Probability it was not corrected on the previous (k-1) tests.)

To find the expected start reliability after N tests (RS_n) $B_{i,n}$ is computed for all failure causes, where i = 1, M.

$$\text{Then } RS_N \cong \prod_{i=1}^{M} (1-q_i B_{i,n})$$

Under nominal conditions, the probability the i^{th} cause occurs for the computation of $B_{i,j}$ is equal to q_i. Under overstress conditions, the probability the i^{th} cause occurs is $\varphi_i q_i$.

MAINSTAGE RELIABILITY

Conditions and Assumptions

1. The reliabilities of the system or failure causes prior to testing are termed "initial reliabilities."
2. Mainstage failure causes have constant failure rates. The initial mainstage reliability of the system is equal to exp (-1 x summation of all failure rates x full mainstage duration).
3. At the start of development, each mainstage-failure cause has a fixed failure rate. When a mainstage test is terminated because of failure, an attempt is made to find the cause and correct it. There is a certain probability that a failure cause is discovered and corrected. If a cause is corrected, its failure rate is zero. If it is not corrected, its failure rate remains unchanged. The probability of discovering and correcting a particular failure cause when it occurs remains constant throughout the development program.
4. Only one failure cause can occur on a test. As soon as one failure does occur, the test is terminated.

5. Mainstage tests may have any intended duration, and each test may have a different intended duration. Since the probabilities of failure are exponential, they will vary with the intended duration of a test.

6. If a test fails during starting transient, mainstage operation will not occur, and no mainstage failure cause will have a chance to produce a failure. If a test is successful during start, and a mainstage failure does occur, other mainstage-failure causes will no longer be exposed, since the test will be terminated.

7. After N tests, there is a certain probability that a cause has occurred, been discovered, and corrected. This is the "probability of elimination." An expected value of the failure rate of each failure cause is found by multiplying the initial failure rate by the probability that the cause has not been eliminated.

8. Although the failure rate of a failure cause is some constant (λ) until the cause is corrected and $\lambda = 0$, its probability of failure will increase with testing. As failure causes occur and are corrected, those not yet corrected will have a greater opportunity to occur. The probability that a test terminates because of another cause of failure will decrease.

9. Overstress testing may be employed in such a way that the failure rate of a mode will be multiplied by a constant factor, called the "overstress factor."

Definitions

K = Total number of mainstage-failure causes present in the system

RM_o = Initial mainstage reliability

λ_i = Initial failure rate of the i^{th} mainstage-failure cause, where $i = 1, K$

RM_j = The expected system mainstage reliability after j tests

$E_j(\lambda_i)$ = The expected value of the i^{th} cause-failure rate after j tests

α_i = The probability of discovering and correcting the i^{th} mainstage failure cause if it occurs

$v_{i,j}$ = The probability of not having eliminated the i^{th} mainstage-failure cause after j tests

θ_i = An overstress factor by which the failure rate of the i^{th} mainstage-failure cause is multiplied to increase its value to $\lambda_i \theta_i$, $\theta_i > 0$. At nominal conditions $\theta_i = 1$.

t_i = The intended mainstage running time on the j^{th} tests

t_f = Full mainstage duration

The Model

Given K mainstage failure causes, each with a failure rate (λ_i), where $i = 1, K$, the probability that a test of intended duration (t_o) is terminated by failure of the m^{th} mainstage-failure cause $(1 \leq m \leq K)$ is

$$\frac{\lambda_m}{\sum_{i=1}^{K} \lambda_i} \left[1-\exp\left(-t_o \sum_{i=1}^{K} \lambda_i\right)\right]$$

$$RM_o = \exp\left(-t_f \sum_{i=1}^{K} \lambda_i\right)$$

The actual value of the failure rate of the i^{th} mainstage-failure cause after j tests is equal to λ_i with probability $(v_{i,j})$ or equal to zero with probability $(1-v_{i,j})$ $E_j(\lambda_i) = \lambda_i v_{i,j}$. Given one mainstage-failure cause present in the system with failure rate (λ) and probability of discovery and correction (α), the probability that it has not been eliminated after j tests can be shown as follows:

$$v_j = \prod_{k=1}^{j} \{1-RS_{k-1}\left[1-\exp(-\lambda t_k)\right]\alpha\}$$

For the i^{th} mainstage-failure cause after j tests:

$$v_{i,j} = \prod_{k=1}^{j} \left[1-(\text{Probability of a start success on the } k^{th} \text{ test}) \times (\text{Probability that the } i^{th} \text{ failure cause occurs on the } k^{th} \text{ test}) \times (\text{Probability that the } i^{th} \text{ failure cause is corrected})\right].$$

To find the expected mainstage reliability after N tests, RM_N, $v_{i,N}$ is computed for all mainstage-failure causes where i=1,K.

Then $RM_N \cong \exp\left[-t_f \sum_{i=1}^{K} \lambda_i v_{i,N}\right]$ Under nominal conditions the failure rate of the i^{th} mainstage failure cause, for the computations of $v_{i,j}$, is (λ_i). Under overstress conditions, the failure rate of the i^{th} failure cause is $(_i\ \theta_i)$.

Overall Reliability

The initial overall reliability is $(R_o = RS_o \times RM_o)$. After N tests, the expected overall reliability is $(R_N \cong RS_N \times RM_N)$.

APPLICATION

Previous component and engine test experience provides a basis for estimating initial-cause failure rates for each failure symptom. The predicted-cause failure rates are derived from interpreting those encountered on historical programs in view of the variation in design parameters between the advanced and historical engines. The following design factors, however, are reflected in the estimates.

1. Design environment being within a range experienced on previous designs will reduce the number of causes, lower their failure rates, and increase the probability of fix.

2. Design environment at a level exceeding previous experience will increase the cause failure rates, introduce new failure causes with lower failure rates, and lower the probability of fix.

3. The potential effect of a malfunction also influences its classification. For example, metal to metal rubbing within an oxidizer system might be considered a failure, while the same rubbing in a fuel system might only be considered a minor malfunction.

It should be noted that a high initial frequency of occurrence per failure cause is beneficial. To illustrate the potential effects resulting from the variation in operating level, an example is presented in Table I for a single failure symptom.

TABLE I

VARIATION IN OPERATING LEVEL

Operating Level	Parameters Varied	Number of Causes	Cause Failure Probability	Probability of Fix	Expected Failure Probability (50 tests)
Nominal	--	1	0.05	0.5	0.014
Severe	Increased Cause-Failure Probability	1	0.10	0.5	0.0077
Severe	Increased Cause-Failure Probability, Reduced-Fix Probability	1	0.10	0.25	0.0282
Severe	Increased Cause-Failure Probability, Reduced-Fix Probability, Introduced Additional Cause	2	0.10 0.05	0.25 0.25	0.0553
Below Nominal	Reduced Cause-Failure Probability, Increased-Fix Probability	1	0.025	0.75	0.0097
Below Nominal	Reduced Cause-Failure Probability, Increased-Fix Probability, 25 tests operated at nominal level (Q increased from 0.025 to 0.05)	1.	0.025	0.75	0.0060

The first case at the severe operating level demonstrates the desirable effect of a high, initial failure rate presenting more opportunities to determine the failure cause. The more realistic example of high failure rate coupled with a low fix probability, however, contributes to a lower resulting reliability, while with the addition of another failure cause retards the reliability prediction to a greater extent. The first example (at a below nominal operating point) points to the potential of a high-fix probability overcoming adverse effects of a low failure rate. The potential of operating at the nominal point for 25 development tests, however, would lead to a high predicted reliability.

To assess the impact of an engine design requirement, it is necessary to translate this requirement into a meaningful operating level for each failure symptom (Table II).

TABLE II

OPERATING LEVEL FOR FAILURE SYMPTOM

Engine Design Requirement	Component Operating Levels	Expected Severity of Failure Symptoms
Thrust, Chamber Pressure, Propellant Combination, Weight ...	Temperatures, Speeds, Heat Fluxes, Flowrates, Vibration Level, loads	Number of Failure Causes, Failure Rates, Probability of Fix

Subsystem
Failure Symptoms
Significant Operating Characteristics
Associated Engine Design Requirements

Turbine
Hot gas leaks, blade or nozzle erosion, blade failures, excessive Wheel vibration level, wheel tip seal leakage
Hot gas inlet temperatures, engine system that has difficulty in controlling inlet temperatures during transient operation (fuel pump that is capable of stalling), turbine horsepower, Thrust, chamber pressure, power cycle, performance requirement, propellant combustion

Subsystem	Failure Symptoms	Significant Operating Characteristics	Associated Engine Design Requirements
Pump	Cavitation, structural failures, rubbing	Impeller tip speed, pump configuration (axial or centrifugal flow, additional boost pump), reactivity of fluid pumped, power requirement, NPSH requirement	Thrust, chamber pressure, combustion chamber cooling method, power cycle, vehicle weight, propellant combination
Dynamic Shaft Seals	Excessive leakage, fire	Seal speed, seal diameter, reactivity of fluid sealed, cooling or lubricating qualities of fluid sealed.	Thrust, chamber pressure, combustion chamber cooling method, power cycle, propellant combination
Bearing and Lubrication System	High shaft torque, bearing failure, bearing over temperature, low lubricant pressure	Bearing DN, lubricating by separate system or fluid pumped	Thrust, chamber pressure, power cycle, propellant combination
Axial Thrust Balancing Mechanism	High or low cavity pressure, bearing failure	Flowrate, shaft horsepower, type of balancing mechanism.	Thrust, chamber pressure, power cycle, propellant combination.

An analysis was performed to determine the desirable pump sizes for a large advanced booster. From design layouts, predictions were made at the amount of development testing to achieve reliability goals as a function of the equivalent engine thrust, chamber pressure, and propellant combination (Oxygen-RP1 or Oxygen-Hydrogen).

Estimates have been derived for three turbopump sizes: small, medium, and large (Fig. 3). The medium and large turbopumps deliver twice and four times, respectively, the flowrate of the small turbopump. The results show that, for equivalent turbopump reliabilities, the small turbopump requires the fewest development tests. For equivalent engine system thrusts and reliabilities, however, the largest turbopump requires the least amount of development testing (Fig. 3A and 3B).

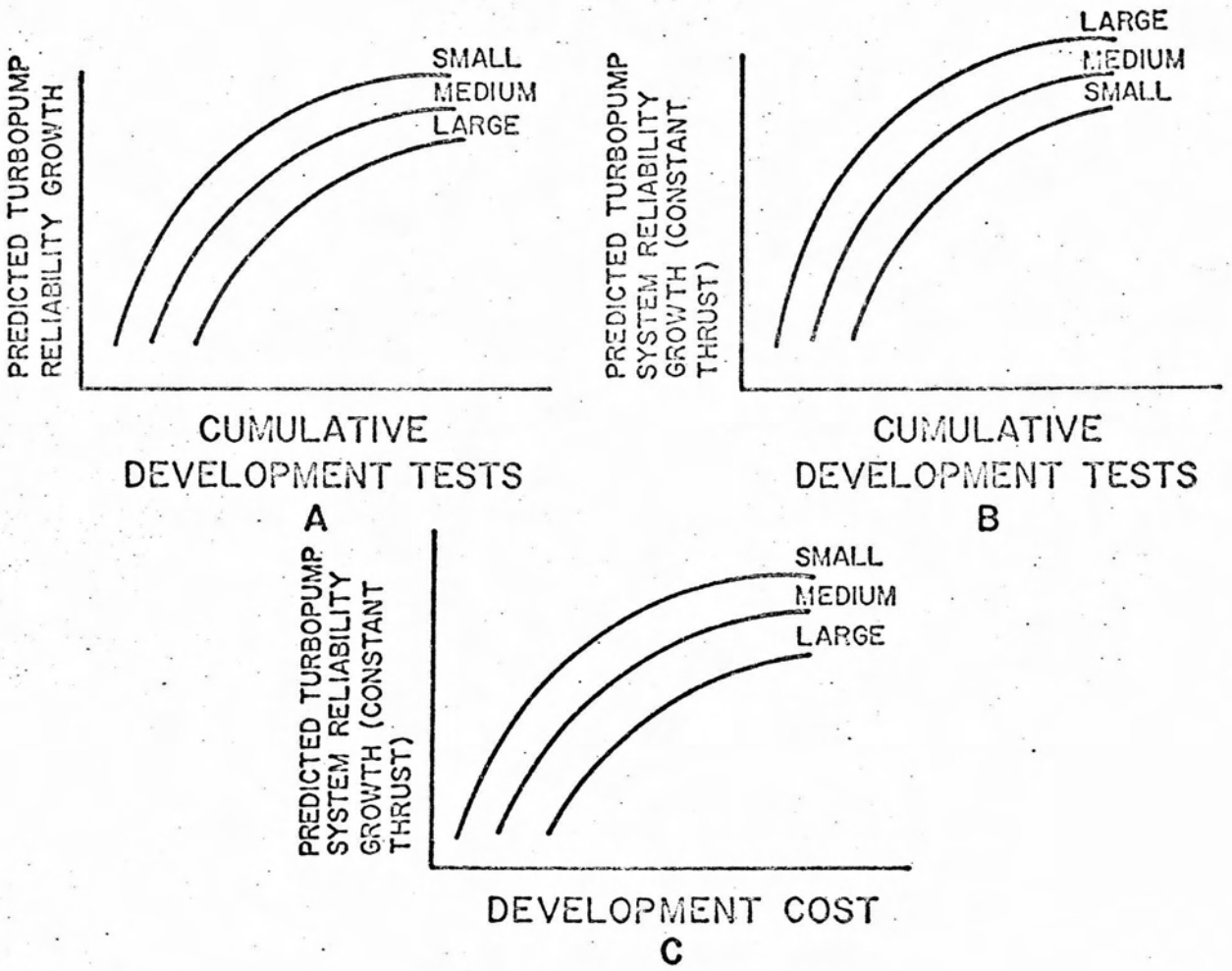


Figure 3. Development Testing and Cost for Reliability Goals

Because of the greater cost of the test-fail-fix cycle for the larger turbopump, the actual basis for comparison must be the estimated development cost to realize equivalent system reliabilities. (Fig. 3C). The results again take a reversal leaving the smallest turbopump size (implying four times the number of large turbopumps in the engine system) with the lowest development cost.

The results also indicate that higher chamber pressures and hydrogen engines will require additional turbopump development. These estimates permit a tradeoff between increased development cost and engine performance.

Rocket engine development philosophies can be placed in two categories:

1. Emphasizing component level development
2. Emphasizing engine system development.

The first concept implies that large numbers of combustor and turbopump tests be performed to correct failure modes prior to running the majority of the expensive system tests, while the second concept assumes that component testing can only approximate the engine environment. Hence, the basic development is performed through engine testing.

The problem in planning an efficient development program is to determine the appropriate amount of testing in each category. The index of effectiveness for each category of testing becomes the increase in engine reliability per test and development dollar. A reliability growth prediction can be examined and readjusted, with effort allocated to those areas indicating the greatest return (Fig. 4).

Theoretically, the optimal program can be determined through allocating effort to that category having the highest index ($\Delta R/\Delta C$) until another category becomes desirable. In actual practice, it may be impractical to carry out all possible answers. A problem has occurred when it appears more efficient to start a program with engine testing and complete it with turbopump testing. The model is applied by allowing it to indicate the test quantities, but not the schedule.

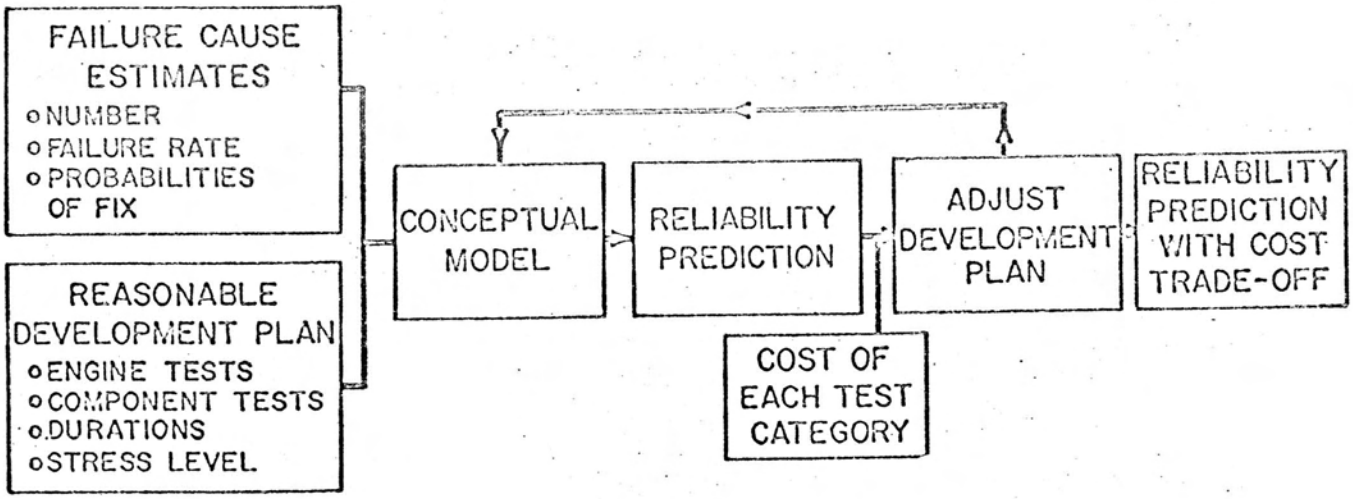


Figure 4. Cost-Reliability Tradeoff

When component testing is indicated late in the development program, the strategy of allocating the component tests earlier is the more efficient course to follow than failing to alter the amount of component testing. The instantaneous rate of reliability growth (at three points in a typical development plan) is shown in Fig. 5. During the early phase, testing the cooled and uncooled combustor appears most efficient. In the middle of the program, engine and turbopump operation yield higher expected returns than either combustor categories, and at the final program phase, the turbopump rate of growth is gaining on the module.

CONCLUSION

In essence, this approach to reliability prediction starts from initial-failure-symptom and failure-cause estimates, and utilizes previously experienced development efficiencies and development effort to predict the ultimate design reliability. Through the procedure portrayed in Fig. 6, an engineering appraisal of the design concept and the development plan is converted into quantitative estimates of the development effort to realize reliability goals. By applying this model during the advance design phase, a more efficient design concept and development plan can be selected.

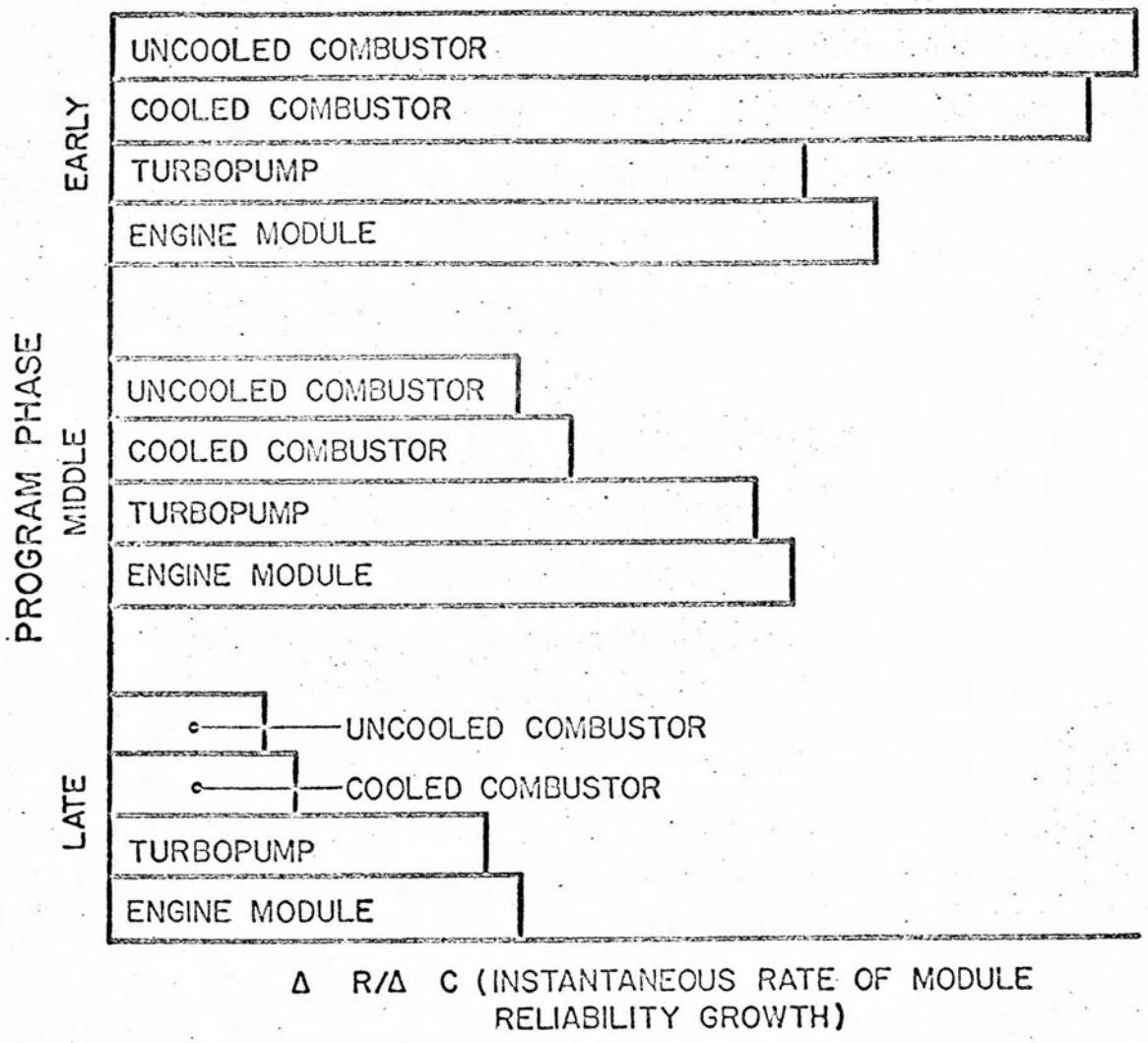


Figure 5. Allocation Index

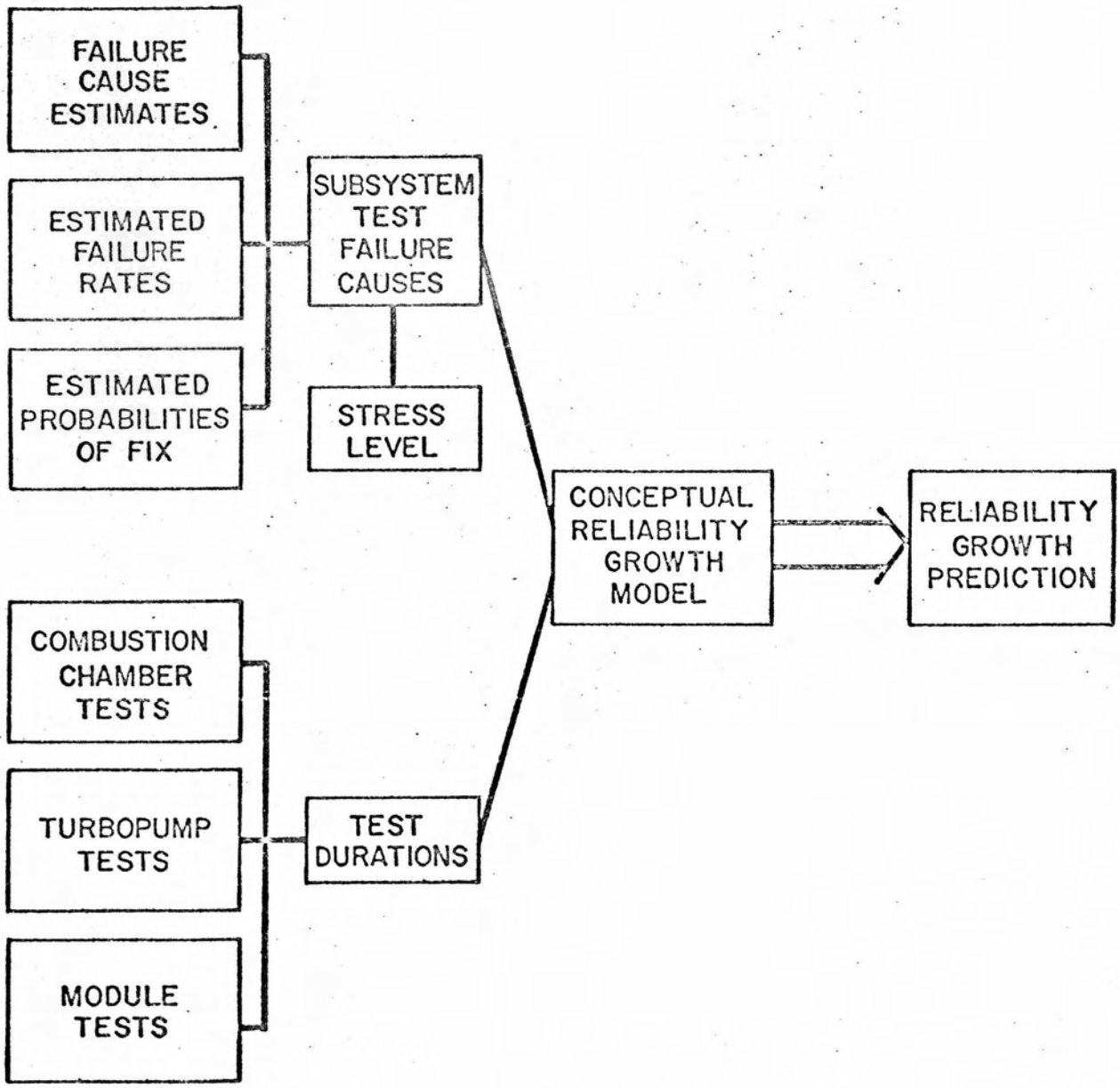


Figure 6. Reliability Prediction Procedure