

AEROSPACE RECOMMENDED PRACTICE

Submitted for recognition as an American National Standard

SAE ARP4900

Issued 1996-04

Superseding ARD50009

LIQUID ROCKET ENGINE RELIABILITY CERTIFICATION

TABLE OF CONTENTS

1.	SCOPE	4
2.	REFERENCES	6
2.1	Applicable Documents	6
2.1.1	U.S. Government Publications	6
2.1.2	FAR Publications	7
2.1.3	Other Publications	7
3.	INTRODUCTION	10
3.1	The Need for a New Approach	10
3.2	Current Certification Processes	13
3.2.1	Rocket Engine Certification Process	14
3.2.2	Jet Engine Certification Process	18
3.3	Deterministic Design Methodology	20
3.4	Introduction to the Recommended Approach	21
4.	DESIGN CERTIFICATION METHODOLOGY	24
4.1	Introduction	24
4.1.1	Overview	26
4.1.2	General Approach	27
4.1.3	Benefits	30
4.2	Design for Reliability Approach	31
4.2.1	Conceptual Design	33
4.2.2	Preliminary Design	33
4.2.3	Detailed Design	35
4.2.4	Design Feedback	39

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be reaffirmed, revised, or cancelled. SAE invites your written comments and suggestions.

Copyright 1996 Society of Automotive Engineers, Inc.
All rights reserved.



Documents
Printed in U.S.A.
Document Sharing Hub

SAE ARP4900

TABLE OF CONTENTS (Continued)

4.3	Reliability Design Tools	40
4.3.1	Reliability Allocation.....	40
4.3.2	Fault Tree Analysis.....	42
4.3.3	Failure Modes and Effects Analysis (FMEA).....	42
4.3.4	Screening for Probabilistic Design Assessment	46
5.	RELIABILITY CERTIFICATION TEST PROGRAM	47
5.1	Introduction	47
5.2	New Requirements.....	48
5.3	Test Program	49
5.3.1	Operability/Functionality	51
5.3.2	Durability	52
5.3.3	Performance.....	53
5.3.4	Design Verification/Substantiation (DVS)	53
5.3.5	Margin Testing	54
5.3.6	Reliability Testing	56
6.	AGGREGATION OF TEST RESULTS	59
6.1	Individual Component Tests	59
6.2	Integrating the Results for Multiple Components	60
6.3	Procedure for Weighing Tests That Are Not Full Duration Firings	63
6.4	Test Data Base	65
7.	PROBABILISTIC METHODOLOGY	66
7.1	Probabilistic Assessment of Reliability.....	66
7.1.1	Information Used in Probabilistic Design Reliability Assessment.....	66
7.1.2	Probabilistic Design Reliability Assessment Approach and Structure	67
7.1.3	Failure Mode Model Types	70
7.2	Probabilistic Life Modeling.....	70
7.2.1	Approach.....	70
7.2.2	Statistical Characterization of Life Drivers	75
7.2.3	Engineering Modeling.....	78
7.2.4	Life Driver Transformation.....	81
7.2.5	Materials Modeling	84
7.2.6	Bayesian Statistical Analysis	84
7.2.7	Application Example	88
7.2.8	Fracture Mechanics/Nondestructive Evaluation	103
7.2.9	Simplified Probabilistic Life Modeling.....	106
7.3	Event Consequent Modeling	107
7.3.1	Introduction	107
7.3.2	The Event Consequent Modeling Approach	108
7.3.3	Simplified Event Consequent Models	109

SAE ARP4900

TABLE OF CONTENTS (Continued)

7.4	Computational Methods for Probabilistic Life Modeling and Their Applicability	115
7.4.1	Introduction	115
7.4.2	Direct Integration.....	115
7.4.3	Numerical Integration	116
7.4.4	Direct Monte Carlo Simulation	116
7.4.5	Efficient Monte Carlo Simulation.....	117
7.4.6	Propagation of Errors	119
7.4.7	g-Function Methods.....	120
7.5	Mission Risk	124
7.5.1	Introduction	124
7.5.2	System Definition as a Function of Components	124
7.5.3	Interactions of Components	125
7.5.4	Computational Methods and Models	125

1. SCOPE:

Current design and development practices leading to formal liquid rocket engine qualification (USAF) or certification (NASA) will not achieve the specific reliability objectives of future programs. New rocket engine programs are dictating quantified requirements for high reliability in parallel with a cost-constrained procurement environment. These specified reliability levels cannot be validated with the necessary confidence in a timely or cost-effective manner by present methods. Therefore, a new improved process is needed and has been developed. This new reliability certification methodology will be discussed in detail in the five sections that comprise this document. Primary purposes of this report are to:

- a. Define and illustrate this process
- b. Point out its strengths and weaknesses
- c. Provide guidelines for its application on programs which have specified reliability requirements

Increased emphasis on rocket engine reliability and cost has prompted the Liquid Rocket Certification Subcommittee (Society of Automotive Engineers for Reliability, Maintainability, and Supportability) to thoroughly examine current methodologies to qualify or certify liquid rocket engine systems. For example, new liquid rocket engine programs, such as the joint NASA/Air Force effort for the National Launch System (NLS) or the Air Force XLR-132 storable propellant upper stage engine, include documented requirements for high levels of reliability. These new requirements exceed those historically demonstrated over the operational life of most current rocket propulsion systems. Certification of reliability was not required for past liquid rocket engines developed for the Air Force or NASA. The importance of demonstrated reliability was low, relative to such requirements as performance, schedule, and cost. Engines were formally qualified or certified by test programs aimed primarily at demonstrating design maturity and operational readiness in terms of performance and durability. In general, relatively little propulsion system testing, as distinguished from engine system testing, was implemented on past flight hardware for launch vehicles.

Reliability estimates prior to the first flight of a new engine historically have been based largely upon results from qualification or certification tests which formally declared the engine ready to fly. Many changes typically were made during the engine development period, until the engine was considered mature enough to qualify or certify. The process, therefore, precluded the gathering of test results applicable to reliability assessment during this development phase of a program. As a consequence, predicted reliability levels, at high confidence, prior to the first flight of a new engine have been consistently low. This was due to the small number of engines tested, especially identical units, and the limited number and type of tests performed on each engine during a typical qualification or certification test program. Reliability levels for current operational rocket engines are based upon a combination of ground test experience supplemented by the accumulation of data derived from actual flights. This process typically takes years and hundreds to perhaps thousands of tests to develop a satisfactory level of reliability and confidence for a particular engine system.

1. (Continued):

The Liquid Rocket Certification Subcommittee advocates a new approach to rocket engine reliability certification as a result of reviewing current methods to qualify or certify engines. It is felt that this new approach is an improvement over current qualification/certification methods. The recommended new approach, described in the following sections of this report, involves a judicious combination of analysis and test efforts that begin at an early stage of the design prior to formal certification. This methodology quantifies reliability estimates by focusing upon early identified weak links in the design and system reliability drivers. The recommended approach includes development tests that assist in establishing the necessary information base for probabilistic analyses and engine system certification testing to demonstrate structural, thermal, and dynamic capabilities, as well as the more typical performance and life requirements.

The new approach begins with a traditional deterministic preliminary design of the engine. A failure modes and effects analysis and a fault tree analysis are then conducted. At this point, the improved approach departs from typical methodology by screening engine components for criticality. A critical component has one or more critical failure modes. This screening is based upon the accumulated knowledge which impacts the design at this point. Critical components typically are complex in geometry, difficult to analyze, susceptible to catastrophic failure, and sensitive to such things as environments, loads, or material properties. Experience has shown that a majority (about 80 to 90%) of the components of a rocket engine can be classified as noncritical, and their reliability is essentially unity. Therefore, a conventional deterministic design approach is satisfactory for these components. However, probabilistic analysis may be desirable for these noncritical components to realize other benefits such as weight savings. The remaining engine components have a higher probability of failure as well as being engine system critical and require the more intensive probabilistic analysis. A probabilistic analysis recognizes dimensional tolerances, variability in material properties, inadequacies in modeling techniques, load distributions, manufacturing variabilities, and so forth, involved in each critical failure mode.

Components that utilize the more intensive probabilistic analysis techniques will yield quantified reliability estimates, while those designed deterministically are assessed only for serviceability. The process is iterative and continuous in nature, whether the component follows the deterministic or probabilistic path, and utilizes the best information available at the time of the analysis. Data deficiencies identified by the probabilistic analysis approach provide guidance for establishing a cost-effective test program during the development phase of the engine program.

The final step in the recommended new approach is a formal, hot firing, test of the engine system which simulates, to the maximum extent possible, the complete propulsion system. Tests will be conducted to engine operational limits to validate structural, thermal, and dynamic margins. A careful review of earlier rocket engine certification and re-certification test programs revealed a number of weaknesses in these formal programs. For example, tests were implemented on a very limited number of like engines. Similarly, most tests were conducted at nominal engine operating conditions with little or no testing at or near anticipated flight operational boundaries. Few attempts were made to demonstrate structural, dynamic, or thermal margins. Duration typically was

1. (Continued):

stressed by multiple full-term firings as suggested in MIL-R-5149 (1969). However, margins in duration frequently were compromised by engine rework. Early test programs failed to provide adequate reliability data because of the many shortcomings indicated above. Sections 5 and 6 of this report will be devoted to reliability validation for the application of this new approach on programs that have specified requirements for engine reliability.

In summary, an examination of weaknesses in past programs to qualify or certify liquid rocket engines, combined with recent strong emphasis on high engine reliability, has led to this recommendation of a new improved approach for the entire process. It is hoped that this new approach will be adopted by and satisfy the future needs of the military, NASA, and commercial users of liquid rocket engines because of the many advantages that will accrue from this approach. For example, it elevates reliability to a status typical of performance, schedule, and cost. It provides early identification of weak components and mitigates nonbeneficial conservatism due to compounding of margins and factors of safety on some components. The approach also guides cost-effective test programs to validate analytic models, confirm environmental predictions, and define system interactions. It provides continuous quantified estimates of component and engine reliability and validates the required level of reliability prior to commitment to flight. It demonstrates structural, thermal, and dynamic capability to operational limits. Finally, the new approach reduces total costs of development, certification, and flight, at some affordable increase to the initial design costs.

2. REFERENCES:

2.1 Applicable Documents:

The following publications form a part of this specification to the extent specified herein.

2.1.1 U.S. Government Publications: Available from DODSSP, Subscription Services Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

MIL-HDBK-338 (1984)	Electronic Reliability Design Handbook
MIL-R-5149A (1954)	Rocket Engine, Liquid Propellant, General Specification for
MIL-R-5149B (1969)	Rocket Engine, Liquid Propellant, General Specification for
MIL-STD-785B Notice 2 (1988)	Reliability Program for Systems and Equipment Development and Production
MIL-STD-882B Notice 1 (1987)	System Safety Program Requirements
MIL-STD-1629A Notice 2 (1984)	Procedures for Performing a Failure Mode Effects and Criticality Analysis
MIL-STD-1783 (1984)	Engine Structural Integrity Program (ENSIP)

SAE ARP4900

2.1.2 FAR Publications: Available from FAA, 800 Independence Avenue, SW, Washington, DC 20591.

Federal Aviation Regulation (1974), Part 33, Section 33.14, Amendment 33-6

2.1.3 Other Publications:

Abernethy, R. B., et al, (1983), Weibull Analysis Handbook, AFWAL-TR-83-2079, Pratt & Whitney, West Palm Beach, FL

Anderson, T. W. and Darling, D. A. (1954), "A Test of Goodness-of-Fit," Journal of the American Statistical Association, 49, pp. 765-69

Anderson, V. L. and McLean, R. A. (1974), Design of Experiments - A Realistic Approach, New York: Marcel Dekker, Inc.

Bjerager, P. (1989), "Methods for Structural Reliability Computations," Lecture Notes for the course "Structural Reliability: Methods and Applications," University of California, Berkeley, April 27-29

Box, G. E. P., Hunter, W. G., and Hunter, J. S. (1978), Statistics for Experimenters, New York: John Wiley & Sons, pp. 563-70

Brussat, T. R. (1974), "Rapid Calculation of Fatigue Crack Growth by Integration," Fracture Toughness and Slow Stable Cracking, ASTM STP 559, American Society of Testing of Materials, pp. 298-311

Conte, S. and deBoor, C. (1980), Elementary Numerical Analysis: An Algorithmic Approach, New York: McGraw-Hill Book Co.

Cox, N. D. (1979), "Tolerance Analysis by Computer," Journal of Quality Technology, Vol. 11, No. 2, pp. 80-87

D'Agostino, R. B. and Stephens, M. A. (1986), Goodness-of-Fit Techniques, New York: Marcel Dekker, Inc.

Feynman, R. P. (1986), "Personal Observations on Reliability of Shuttle," Report of the Presidential Commission on the Space Shuttle Challenger Accident, Appendix F

Fox, E. P. (1990), "SSME Alternate Turbopump Development Program - Probabilistic Failure Methodology Interim Report," FR-20904-02, Pratt & Whitney, West Palm Beach, August 1990

Fox, E. P. (1991), "SSME Alternate Turbopump Development Program - Probabilistic Failure Methodology Final Report," FR-20904-09, Pratt & Whitney, West Palm Beach, August 1991

Fox, E. P. and Safie, F. (1992), "Statistical Characterization of Life Driver Distributions for a Probabilistic Life Analysis," AIAA/SAE/ASME 28th Joint Propulsion Conference, AIAA-92-3414, July, 1992

2.1.3 (Continued):

Fuchs, F. O. and Stephens, R. I. (1980), Metal Fatigue in Engineering, John Wiley & Sons

Guttman, et al. (1988), "Confidence Limits for Stress-Strength Models with Explanatory Variables," Technometrics, Vol. 30, pp. 161-68

Hastings, N. A. J. and Peacock, J. B. (1974), Statistical Distributions, New York: John Wiley & Sons

Haugen, E. B. (1980), Probabilistic Mechanical Design, New York: John Wiley & Sons, pp. 356-97

Hogg, R. B. and Klugman, S. A. (1983), "On the Estimation of Long Tailed Skewed Distributions with Actuarial Application," Journal of Econometrics, 23, pp. 94-95

Hulting, F. L. and Robinson, J. A. (1990), "A Bayesian Approach to System Reliability," General Motors Research Publication, GMR-7110

Khuri, A. and Cornell, J. (1987), Response Surfaces: Designs and Analyses, New York: Marcel Dekker, Inc.

Law, A. M. and Kelton, W. D. (1982), Simulation Modeling and Analysis, New York: McGraw-Hill Book Company, pp. 219-278

Lloyd, D. K. and Lipow, M. (1977), Reliability: Management, Methods, and Mathematics, Redondo Beach, California

Madsen, H. O., Krenk, S., and Lind, N. C. (1986), Methods of Structural Safety, Prentice-Hall Inc., Englewood Cliffs, NJ

Mann, et al. (1974), Methods for Statistical Analysis of Reliability and Life Data, McGraw-Hill Book Co., New York

Martz, H. F. and Waller, R. A. (1982), Bayesian Reliability Analysis, New York: John Wiley & Sons

Martz, H. F. and Waller, R. A. (1990), "Bayesian Reliability Analysis of Complex Series/Parallel Systems of Binomial Subsystems and Components, Technometrics, Vol. 32, November 1990, pp. 407-416

Martz, H. F., Waller, R. A., and Fickas, E. T. (1988), "Bayesian Reliability Analysis of Series Systems of Binomial Subsystems and Components," Technometrics, Vol. 30, May 1988, pp. 143-54

Mischke, C. R. (1989), "Stochastic Methods in Mechanical Design: Part 3: A Methodology," Proceedings of the Eighth Biannual Conference on Failure Prevention and Reliability, Design Engineering of ASME, Montreal, Canada, Sept. 17-20

2.1.3 (Continued):

Moore, N. et al. (1986), A Review of Certification Practices Potentially Applicable to Man-Rated Reusable Rocket Engines - Certification Process Assessment Task, JPL D-7969, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, February, 1986

Moore, N. et al. (1992), An Improved Approach for Flight Readiness Certification - Methodology for Failure Risk Assessment and Fatigue Failure Mode Case Study Examples, JPL D-9592, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA

Moore, N., Ebbeler, D., and Creager, M. (1990-1), "A Methodology for Probabilistic Prediction of Structural Failures of Launch Vehicle Propulsion Systems," Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference, April 1990, Part 2, pp. 1092-1104

Moore, N., Ebbeler, D., and Creager, M. (1990-2), "An Improved Approach for Flight Readiness Assessment - Methodology Summary," JPL Publication 90-46, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, October 1990

Neter, J., Wasserman, W., and Kutner, M. H. (1985), Applied Linear Statistical Models, Homewood, Illinois: Richard D. Irwin, Inc.

Newlin, L. et al. (1990), "Probabilistic Low Cycle Fatigue Failure Analysis Applicable to Liquid Propellant Rocket Engines," Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference, April 1990

"Post Challenger Evaluation of Space Shuttle Risk Assessment and Management," (1988), Committee on Shuttle Criticality Review and Hazards Analysis Audit, National Research Council, Washington, DC

Roberts, N. H. et al. (1981), Fault Tree Handbook, NUREG-0492, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC

Ross, P. J. (1988), Taguchi Techniques for Quality Engineering, New York: McGraw-Hill Book Company

Safie, F. and Fox, E. P. (1991), "A Probabilistic Design Analysis Approach for Launch Systems," AIAA/SAE/ASME 27th Joint Propulsion Conference, AIAA-91-3372, June 1991

Singpurwalla, N. D. (1988), An Interactive PC-Based Procedure for Reliability Assessment Incorporating Expert Opinion and Survival Data," Journal of the American Statistical Association, March 1988, pp. 47-50

2.1.3 (Continued):

Sutharshana, S. et al. (1991), "A Probabilistic Fracture Mechanics Approach for Structural Reliability Assessment of Space Flight Systems," Advances in Fatigue Lifetime Prediction Techniques, Special Technical Publication 1122, American Society for Testing and Materials

Sutharshana, S. et al. (1990), "Probabilistic High Cycle Fatigue Failure Analysis Applicable to Liquid Propellant Rocket Engines," Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference, April 1990

USAF R&M 2000 Process (1988), Headquarters, United States Air Force, Office of the Special Assistant for R&M, Washington, DC

Wu, Y. (1987), "Demonstration of a New, Fast Probability Integration Method for Reliability Analysis," Journal of Engineering for Industry, Vol. 109, Feb. 1987, pp. 24-28

Wu, Y. and Burnside, O. H. (1988), "Validation of the NESSUS Probabilistic Finite Element Analysis Computer Program," AIAA/ASME/ASCE/AHS 29th Structures, Structural Dynamics, and Materials Conference, AIAA-88-2372, April 1988

3. INTRODUCTION:

3.1 The Need for a New Approach:

The Liquid Rocket Certification Subcommittee of the Reliability, Maintainability, and Supportability Committee of SAE is advocating an alternate approach to the current methodology employed to qualify (U.S. Air Force) or certify (NASA) liquid rocket engine systems. In the remainder of this document, the NASA term "certify" will be used interchangeably with the Air Force designation "qualify." The recommended new approach is needed to achieve specific objectives of new engine programs which, for example, stipulate quantified requirements for high levels of reliability that cannot be validated with the necessary confidence in a timely or cost-effective manner by present methods.

The recommended approach results from a thorough examination of current methodology which, in turn, was prompted by increased NASA and Air Force emphasis on improved rocket engine reliability and reduced costs. Government initiatives, such as the Department of Defense Total Quality Management Master Plan and the U.S. Air Force "R&M 2000" Process, provide strong support for increased reliability and lower costs. For example, the "R&M 2000" (1988) initiative mandates that reliability be considered equal to performance, schedule, and cost.

3.1 (Continued):

The development of liquid rocket engine systems currently is conducted through an evolutionary or "test-fail-fix" process which is continued until the system is considered mature enough to fly. The engine is then declared ready for flight through a formal process known as "certification." The specific process is defined by the responsible agency or program, sometimes utilizing general military specifications and standards as guidelines.

The current certification process provides little quantitative information as to the reliability of a particular engine design. Actual reliability estimates for current engines are based on system ground tests of the flight design along with the accumulation of actual flight tests. However, due to configuration changes made during the evolutionary development phase of a program, few, if any, applicable results are available for reliability assessment from development system testing. As a consequence, reliability estimates prior to engine first flight must be based on the limited ground test experience gained primarily in the certification test series.

The certification test series typically has demonstration of design maturity and/or operational readiness as its prime objective. Therefore, it includes too few tests to adequately demonstrate reliability. Confidence to fly an engine is gained through the use of historically based factors of safety in the design, accepted design practices, component testing, subsystem testing, and system level development testing as well as the final certification test series. However, the reliability of the engine system as the result of this process cannot be quantitatively assessed from the certification test program because of a very limited number of tests on like engines.

A review of earlier rocket engine certification programs revealed other important weaknesses. For example, most of the past tests were conducted at or near nominal operating conditions with little or no testing at or near the actual flight operational boundaries of the engine. Few attempts were made in the past to demonstrate structural, thermal, or dynamic margins. On the other hand, margin in durability was emphasized by multiple full-duration firings as suggested by military specification MIL-R-5149 (1969). Unfortunately, durability margin frequently was compromised in past certification test programs by allowing considerable engine rework. Finally, relatively little propulsion system testing, as distinguished from engine system testing, was completed on past flight hardware for previous launch vehicles.

Specifications for previous liquid rocket engine systems did not normally include a required value for reliability. However, engine programs currently being considered for future vehicle applications are defining a quantified engine system reliability requirement. Examples include the NASA/Air Force National Launch System (NLS) engine and the Air Force XLR-132 storable, upper stage engine. It has long been recognized that demonstration of reliability by standard pass/fail statistical methods, utilizing only ground test and flight experience, is impractical, if not impossible from a cost and schedule viewpoint. The basic challenge is to provide a flightworthy engine system with demonstrated reliability within reasonable budget and schedule constraints.

3.1 (Continued):

The Liquid Rocket Certification Subcommittee has defined an approach to meet this challenge. The recommended new approach involves a judicious combination of analysis and testing. This combination utilizes methodologies and concepts such as failure modes and effects analyses, probabilistic design and analysis techniques, incorporation of test history through Bayesian statistics, design of experiments, and so forth. Application of these techniques begins at the early stages of the engine design process and is systematically applied to the engine critical components throughout the design and development phases of the program. By applying this certification design approach, the following advantages accrue:

- a. Early identification of weak links during the design phase rather than during test, therefore, avoiding some failures.
- b. Cost-effective testing arranged to validate analytical models, establish operating environments, define system interactions, and demonstrate margins.
- c. Application of design and test information to continuous determination of quantitative reliability.
- d. Mitigation of nonbeneficial design conservatism due to compounding of margins and factors of safety.

The new approach will develop the necessary information in an organized, timely manner to allow a more rapid growth of reliability prior to the initial flight of an engine system when compared to the current approach. An example is illustrated in Figure 1. Accelerated reliability growth may also be accompanied by reduced time in the development and demonstration phases for the engine program.

The purpose of this document is to provide the using agency/engine manufacturer team guidelines with which to select or define a program specific and cost-effective engine development certification process. This process will provide quantitative information about the reliability of the flight design throughout the life of the program. The generic certification process described in this document will serve as the basis of a vehicle specific, tailored engine program based on:

- a. Knowledge from design analysis
- b. Component and system development experience
- c. Engine certification tests
- d. Development flight experience

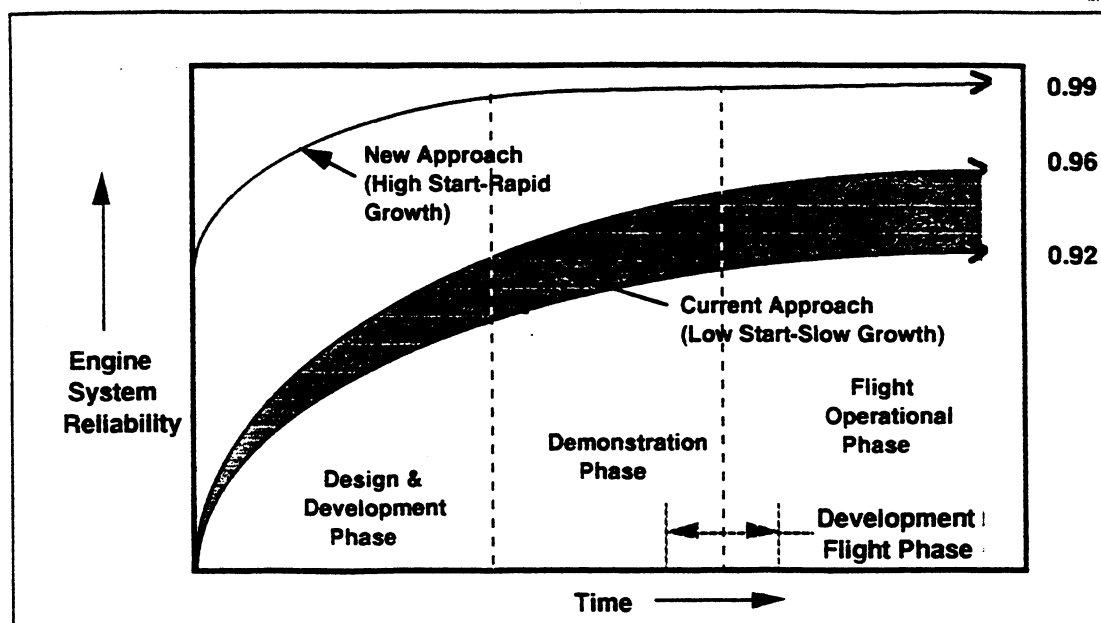


FIGURE 1 - Engine Certification Process

3.1 (Continued):

The primary purposes of this new methodology is to improve the cost-effectiveness of the process and to achieve the desired engine reliability. This is accomplished by providing a continuous quantitative reliability assessment of the engine system and by early identification of areas of weakness in the design and test phases of the program. The certification approach defined by this document will provide a tool for design decisions, hardware provisioning, optimized test planning, and flight-readiness schedule forecasting.

The methodology for the certification process described in this document specifically addresses liquid rocket engine systems. However, this technique should be applicable to other complex systems for which a high degree of confidence in the reliable operation of the system must be established. This is especially true when the engine program must be conducted with a limited number of tests and for which system failure has catastrophic consequences. The definition of a "limited number of tests" is an engine test program with less than approximately 1000 tests during the entire development and certification program.

3.2 Current Certification Processes:

This section provides an overview of the processes currently used to certify liquid rocket engine systems. The requirements imposed on previous programs are presented to provide a historical perspective for selected military and NASA rocket engines. An overview of the process used to certify high performance jet engines also is included to highlight similarities and differences between current rocket engine and jet engine certification approaches.

3.2.1 Rocket Engine Certification Process: The current process for design, development, certification, production, and operational use is depicted in Figure 2 (see Moore et al. (1986)). As indicated earlier, due to the evolutionary or “test-fail-fix” type of maturing for the engine system, it has been typical that only the formal testing of the flight configuration, shown in the dashed box, is usable for reliability quantification. The number of tests in the certification series is typically small (of the order of 20 tests on one or more units). For the first flight usage, this limited testing yields a demonstrated engine system reliability of only 89%, at 90% confidence.

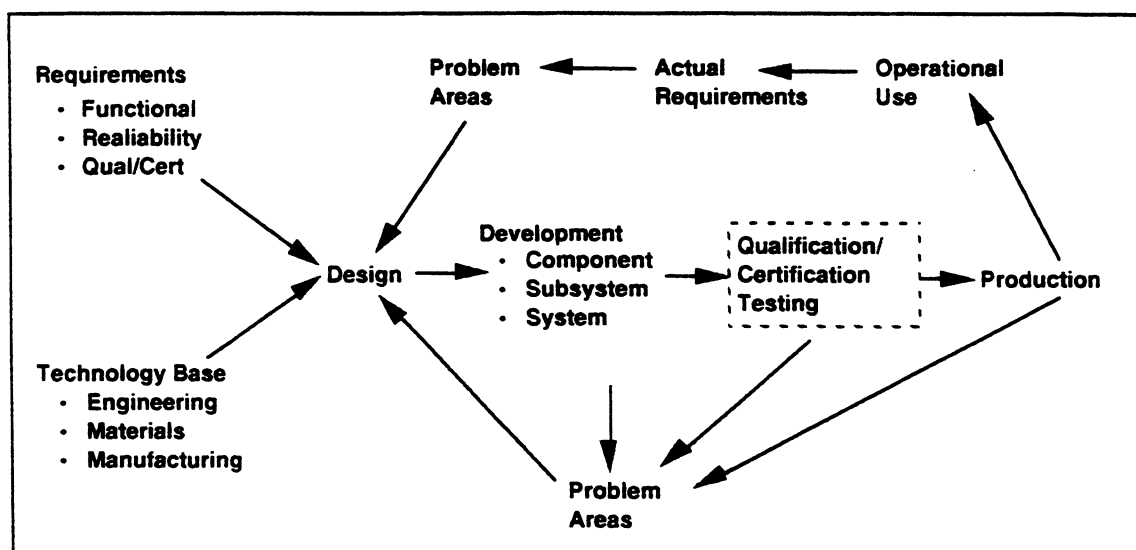


FIGURE 2 - Typical Rocket Engine Certification Process

As shown in Figure 2, the design methodology provides the mechanism for translating both the requirements and technology base into a system design from which hardware can be produced. The technology base encompasses such things as the materials available for use, understanding of materials behavior, engineering methodology, manufacturing techniques, and so forth. Iteration of the design and developmental testing phases at the component, subsystem, and system levels provide the means by which the production configuration evolves. The engine level development testing identifies problems not detectable in component and subsystem level testing (e.g., environmental conditions and dynamic effects caused by the interaction of components in the system). System level certification testing validates the flight configuration for production and operational readiness based upon demonstration of satisfactory design maturity and functional performance. However, explicit demonstration or quantification of reliability at a given confidence for the engine is not provided.

3.2.1 (Continued):

Completion of certification testing and validation testing for first flight, is often preceded by commencement of flight hardware production due to schedule requirements. Similarly, development flights can begin prior to full certification by limiting the use of specific hardware within the engine system that has not demonstrated performance or life requirements during development or certification testing. These development flights provide additional data for design validation.

Ground test engines are used to lead the fleet by some factor to uncover design problems resulting from use and aging before they become flight problems (the fleet-lead factor is two for SSME; i.e., flight units can be utilized up to one-half the duration demonstrated by the ground test fleet leader). Problem areas identified by fleet leader data or actual flight experience may result in limiting the life of the involved items until design changes can be implemented through the process shown in Figure 2.

- 3.2.1.1 Component and Subsystem Testing: Following completion of the initial engine design phase, component and subsystem testing are conducted to verify component designs. The number of tests has been determined historically by experience factors and programmatic/requirements such as hardware and facility availability and schedule constraints. Component and subsystem testing occurs prior to engine system testing. For example, all major Space Shuttle Main Engine (SSME) components were subjected to structural tests. Rotating parts were spin tested. The main combustion chamber and ducting were fatigue testing, and some components were subjected to dynamic and proof pressure tests. Of the components tested, about 6% failed the test criteria and were redesigned. Similarly, all SSME subsystems were subjected to limited development testing to verify operational capability. These include the igniters, preburners, main injector, turbopumps, and software subsystems.

Component testing of the RL-10 involved the testing of turbopumps, valves, controllers, and injectors during the first two years of development. Structural, fatigue, and proof-pressure tests were conducted. Subsystem testing of the RL-10 was limited to operational verification and characterization of the fuel turbopumps in the early 1960s.

Component testing of Titan engines included testing of the thrust chamber, gas generator, turbopumps, and start cartridges for structural and operational integrity. Dynamic and proof-pressure tests also were performed. Titan subsystem testing included testing of the gas generator/turbopump combination and the thrust chamber (injector and chamber) during engine development to verify operational capability.

- 3.2.1.2 **System-Level Development Testing:** Engine system level development tests demonstrate system operating capability, system tolerance to off-nominal conditions, and define engine environmental conditions. Operating parameters which are characterized include performance, controllability, repeatability, and durability. Engines are tested at off-nominal conditions within the operating envelope including propellant inlet conditions, propellant mixture ratios, and vehicle-induced anomalies such as abnormal voltages. Testing verifies required engine environments, such as vibration levels, temperatures, and pressures.

During system level development testing, the SSME was subjected to system level durability, thermal, operational, and margin testing. The engine used in the majority of SSME system-level development tests was essentially the same configuration as the flight engine.

Early Titan engine, system-level development tests demonstrated operating capability and margins on thrust, engine frame structural loads, turbopump speeds, mixture ratio, inlet conditions, and chamber pressure. Tests included vibration, thermal cycling, and durability. In addition, engine storage capability in a fueled, operationally ready mode was evaluated to satisfy Titan weapon system requirements.

For the most recent version of the RL-10 Centaur engine, approximately 400 development tests were run prior to start of the qualification cycle. As with the Titan engines, RL-10 margins were demonstrated during system-level development testing over a range of thrust, mixture ratio, and inlet conditions. Types of tests include dynamic, durability, thermal, and operational verification tests.

- 3.2.1.3 **Certification/Qualification Testing:** Rocket engine systems are certified primarily by engine system level tests. Nominal performance, selected margins, and design life of rocket engines are demonstrated as part of the certification ground test program and later verified during flight. Since the design life of rocket engines is relatively short, the entire design life was simulated historically at nominal conditions during the test program for expendable engines. Certification testing to demonstrate life for reusable rocket engines is performed for only a portion of design life prior to first flight. Certification testing is then extended past initial certification life by a ground test certification-life extension program.
- 3.2.1.4 **NASA Certification Test Requirements:** NASA certification requirements for reusable engines are typified by the SSME program. The SSME flight configurations include the first manned orbital flight (FMOF) configuration, the full power level (FPL) configuration, and the Phase II configuration. FMOF engines were used on the first five flights of the space shuttle. FPL engines were used on shuttle flights prior to the STS-51L Challenger flight configuration and Phase II for post-Challenger flights. Each configuration was certified for flight using a plan approved by the Space Shuttle Program.

3.2.1.4 (Continued):

The basic philosophy for certification of the SSME is the "2x" rule: two samples (engines) are demonstrated for twice the intended flight use. SSME certification for the Phase II configuration requires specified hardware changes to demonstrate, on two samples, the time and starts equivalent to ten missions in order to fly for five missions. Following initial certification for five flights, the configuration can be certified for more missions by additional testing of the two samples (for twice the proposed usage). This requirement is consistent with the philosophy used to certify both the initial FMOF (STS-1/5) and the Phase I (STS-6/51L) configurations. Testing includes evaluation of the configuration over the specification range of inlet conditions, power levels, and throttling. Each sample is required to demonstrate at least one overstress test at 2% above the maximum commanded operating level. Failure of the engine during a certification cycle will cause the cycle to be restarted. Hardware changes are permitted during certification, if appropriate life limits are established for those components that are changed.

F-1 and J-2 flight certification basically demonstrated design life. Requalification of J-2 from 225K to 230K lbf thrust required 31 tests on two samples. Qualification of F-1 required 20 tests on one engine system. Hardware changes were allowed during qualification.

- 3.2.1.5 Military Qualification Test Requirements: The primary current military specification developed exclusively for liquid rocket engines is MIL-R-5149B (1969) with Amendment 1 of March 1969 and entitled, "Military Specification - Rocket Engine, Liquid Propellant General Specification For." The "A" version of this document was released initially in February 1954, updated to the "B" version in November 1966, and Amendment 1 was added in March 1969. The latest version of this document, therefore, is over 20 years old.

MIL-R-5149B covers standard requirements for liquid propellant rocket engines and emphasizes the preparation of engine model specifications for particular applications. The document served as a guideline for qualification test specifications for liquid propellant rocket engines. For example, it recommends a sequential series of key tests and suggests other tests which can be interspersed between the key ordered set. The total firing duration of all tests must accumulate the equivalent of 12 mission firings for reusable engines. However, the tests may be divided among more than one engine, provided at least one of the engines demonstrates the required operating life. Consequently, the mandatory requirements for past engine tests can be found in the qualification test applications for specific rocket engine programs.

Two Rocketdyne Atlas MA-3 booster engines completed qualification testing to military guidelines in 1960. However, posttest engine modifications were required, and a reverification test series was then completed on a third unit in 1961. The pair of initial engines completed 12 full-duration firings and 23 safety limit tests. A total of 1866 seconds and 19 starts were accumulated on one engine and 2033 seconds and 20 starts on the other engine. The reverification test series included six additional full duration firings.

3.2.1.5 (Continued):

Both the Aerojet Titan LR-87 and LR-91 were qualified to the military guidelines with each configuration qualified using a single engine. The LR-87 qualification program was interrupted, then restarted due to a gearbox failure. After gearbox redesign, 12 full-duration tests were performed. A total of 3579 seconds was accumulated on the LR-87 engine in 46 test firings during the qualification series. Eleven full-duration tests were part of a total of 39 tests and 2933 seconds performed on a single LR-91 engine during qualification. Repairs and replacement of parts on both LR-87 and LR-91 were necessary during the qualification test series.

Requalification of the Pratt & Whitney - Centaur RL-10 from the 3-3A to the 3-3B configuration (thrust reduced from 16.5K to 15K lb; mixture ratio increased from 5.0 to 6.0) required a minimum of 20 tests and 4500 seconds time, representing 10x starts and approximately 7x current mission durations. Three engines each completed the requirement. No hardware changes were permitted during the testing. Maximum and minimum flight performance requirements were demonstrated as part of the test series.

- 3.2.2 Jet Engine Certification Process: Typical practice in the gas turbine engine industry is to incorporate certification into an advanced system development program because the information available for certification depends on the structure of the development program. In both military and commercial sectors, system certification may be based on either analysis or testing or both at the component and systems levels. Often the components and subsystems are certified to different service lives and/or inspection intervals which mandates that field maintenance and inspection programs be considered in certification.

Figure 3, which is similar to Figure 2, illustrates a systems development practice that is typical of both military and commercial programs in the gas turbine industry. The systems development process as shown is not specifically required by either military agencies or the Federal Aviation Administration. Individual elements of the process may be required by regulations or military specifications. For example, the Air Force Propulsion Power System Integrity Program (PPSIP) and MIL-STD-1783 (1984) both require specific elements in the system development process.

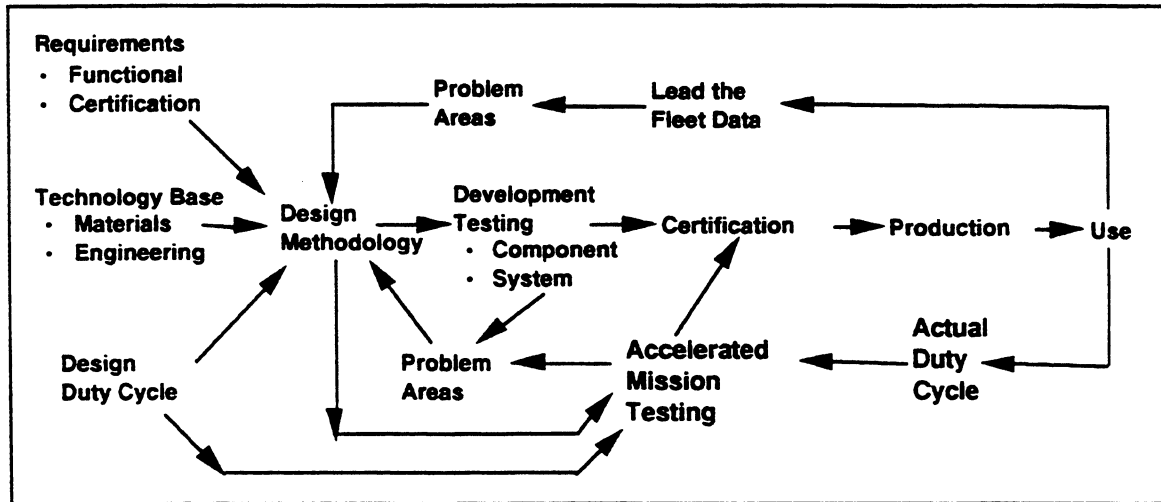


FIGURE 3 - Typical Engine Certification Process

3.2.2 (Continued):

As shown by the information exchange depicted in Figure 3, the design methodology provides the mechanism for translating the requirements and the duty cycle into a system design from which hardware can be produced. The iterative loop between design methodology and development testing at the component, subsystem, and system levels is the means by which the production prototype system configuration is established. The certification shown in Figure 3 is structured to utilize information from multiple sources acquired throughout the systems development program. Thus, this approach to certification incorporates information from engineering analysis, characterization of materials behavior, component testing, and system level testing.

System level testing may be carried out more effectively by increasing the information return on test time through Accelerated Mission Testing (AMT). AMT consists of replicating the damage-inducing portions of the duty cycle during system level testing, while omitting the nondamaging portions of the duty cycle from the tests. As suggested in Figure 3, AMT requires that the damaging portions of the duty cycle be identified by means of the analytical capability for failure mode identification that is embodied in the design methodology. Problem areas that are identified by AMT are corrected through design changes.

The AMT concept concentrates the thermal cycle damage that is seen in a typical jet engine mission into a shorter length of time by eliminating the more "benign" cruise-and-loiter time portions of the duty cycle. The U.S. Air Force and U.S. Navy requirements for certification/qualification have changed over the last 15 years to make use of this AMT concept and, hence, more realistically simulate the actual engine reliability in the field.

3.2.2 (Continued):

Formerly, each jet engine consisted of one 50 h test. This test typically was set up to demonstrate three to four points in the flight envelope (e.g., Mach 1.2 at sea level, Mach 2.3 at 40 000 ft, and Mach 1.7 at 20 000 ft). This test did not consider cyclic durability or reliability over the projected engine life. The Air Force and Navy, therefore, have evolved their jet engine qualification programs to simulate the projected time between inspections on three to four AMT engines. For example, on the Pratt & Whitney F100-PW-200 engine (which powers the newer F15 and F16 fighter aircraft), three AMT engines were run to 4000 cycles each. In this case, the 4000 cycles represented the time to the first scheduled inspection (about 9 years).

After an engine system is put into use, a very limited number of engines, designated as “fleet leaders,” accrue service time at a much higher rate than the average engine system. The fleet leaders are intended to reveal failure modes that are missed by the AMT and by the failure predictions of the design methodology. While an engine system is in use, the service life or inspection interval for which a system component is certified may be extended. Components that have accumulated substantial operating time may be removed from service for analysis and testing to estimate their remaining life. This information can serve as the basis for extending previously established service life limits or inspection intervals.

3.3 Deterministic Design Methodology:

The predominant approach to the design of rocket engines has been deterministic in nature. Similarly, present rocket engine certification practices rely on a judgmental evaluation of testing at the component, subsystem, and engine system levels in conjunction with engineering analyses of individual components. In current practice, the suitability of individual components for flight service is assessed, in part, by a design verification process. In concept, this process could consist of:

- a. Analysis only
- b. Testing only
- c. Combination of analysis and testing

Components assessed by analysis only are not critical in that component failure does not cause engine failure. These components are conservatively designed with margins sufficient to cover uncertainties regarding loads, environment, and engineering modeling of failure phenomena. The failure modes of such components must be known and adequately characterized by an engineering failure model. In situations where analyses are more uncertain and margins cannot be assessed with confidence, the second approach, testing only, could be considered. However, it is rarely feasible to carry out a test program to acquire enough failure data to statistically characterize the probability of occurrence of rare event failure modes.

3.3 (Continued):

The suitability of components that are critical in the sense that their failure results in engine system failure and whose margins are difficult to establish is typically assessed by a combination of analysis and testing. However, no consistent approach for design verification by means of analysis, testing, or a combination of the two is used for components in a particular development. Typically, procedures for carrying out design verification are formulated for individual components according to the criteria of "reasonable and sufficient". No statistically valid procedures are employed to establish a credible quantitative estimate of component reliability. Such quantitative reliability estimates are not available from these conventional approaches for design verification because the analyses are deterministic in nature, and testing programs are too limited for meaningful use of statistical methods. This is a result of avoiding a failure because of its expense. Deterministic analyses assume the use of conservative methods and materials characteristics in conjunction with worst-case operating conditions. Although conservatism may be imposed in the analysis, there is no quantification of how conservative the results could be. Typically, a single-point analysis is performed and no sensitivity analysis is conducted to determine a component's capability to survive off-nominal operating conditions. It is not known whether the deterministic analysis is consistently conservative and to what extent the analysis represents the worst-case conditions. This prompts the question, "What is reasonable and sufficient?" Shortcomings of the exclusive use of deterministic design methodology, especially in regard to reliability certification, have been considered. The recommended new approach to liquid rocket engine certification is introduced in the following text and is discussed in depth in Section 4 through 6 of this document.

3.4 Introduction to the Recommended Approach:

A simple block diagram of the recommended approach for liquid rocket engine reliability certification is shown in Figure 4. The process begins with a traditional, deterministic preliminary design of the engine. This early design is subjected to a "bottom-up" failure modes and effects analysis (FMEA) to identify failure modes to be considered in the design of engine components and subsystems. Similarly, a "top-down" fault tree analysis (FTA) of the engine system or subsystems is conducted to identify failure modes or conditions which could contribute to a "major" failure event, such as, unexpected component interactions.

The next step in the new approach is the screening of engine components for criticality using the previously developed information. That is, the preliminary design analysis, the FMEA, and the FTA. Experience to date has shown that relatively new (10 to 20%) components of a rocket engine may be classified as critical. Critical components may be categorized through several characteristics:

- a. Complex in design geometry
- b. Difficult to analyze
- c. Susceptible to catastrophic types of failure

SAE ARP4900

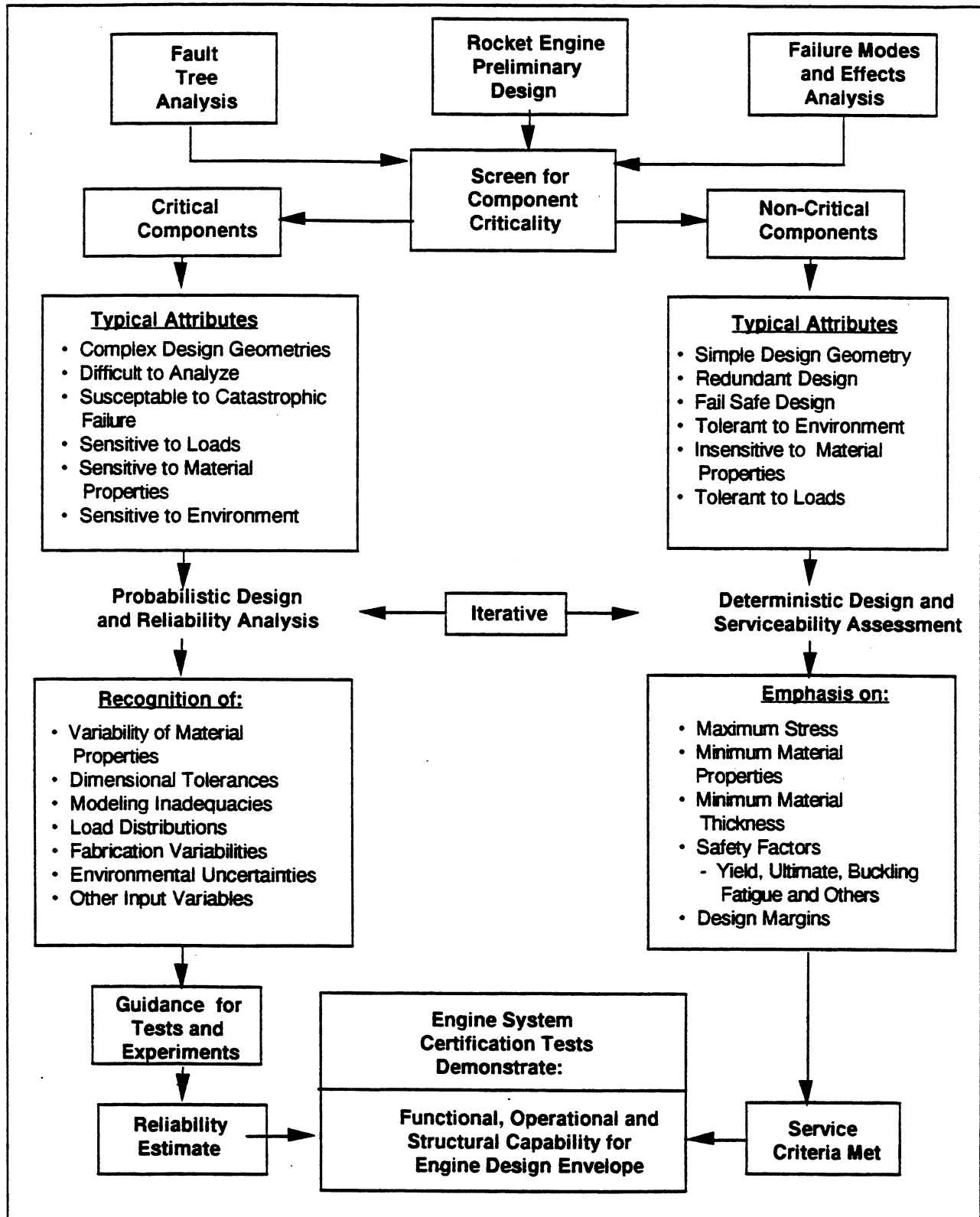


FIGURE 4 - New Approach to Engine Certification

3.4 (Continued):

Finally, critical components may be sensitive to such things as their operating environments, the properties of the materials from which they are fabricated, or variations of loads that they must withstand.

The remaining components can be classified as noncritical, and their reliability assessment is unity (effectively), if they are correctly designed. Noncritical components often have simple design geometries, may be redundant in nature, and may be fail/safe in design concept. Also these components tend to be tolerant of their operating environment, insensitive to materials property variations, and passive to variations in operating loads. The increased effort and cost of the more extensive probabilistic analysis is not warranted.

The component design process is iterative in nature and requires considerable judgment, whether the component follows the probabilistic or the deterministic path in Figure 4. The methodology for those on the probabilistic path will formally quantify variability in material properties, dimensional tolerances, inadequacies in analytical models, distributions in loads, uncertainties in environments, variabilities in fabrication processes, and so forth. Probabilistic methodology encompasses the concept of simultaneous engineering by concurrently considering such areas as design, reliability, manufacturing, and so forth. It also provides guidance for tests and experiments to effectively invest program funds to develop appropriate data base material. Initially, the probabilistic approach may be somewhat more costly but should result in long-term savings because analysis and testing are focused on critical areas.

Methodology for those components on the deterministic path in Figure 4 follows traditional design procedures which emphasize single values such as maximum stress, minimum material properties, minimum wall thicknesses, and so forth. Safety factors on material strengths, such as yield, ultimate, buckling, etc., are used to compensate for the lack of precise knowledge on the single values. Similarly, design margins are used in deterministic analysis because exact loads and stresses are not known. Only a serviceability assessment, rather than a reliability estimate, can be made based upon analysis and tests which support a deterministic design. The engine structural reliability estimate will be primarily based on using component reliabilities predicted by probabilistic methods.

The next step in the recommended new approach is engine system, hot firing, certification testing. This should simulate, to the maximum extent possible, the entire propulsion system. The primary goals of the tests include a validation of structural, thermal, and dynamic capabilities of the rocket engine to at least the limits required by the operational envelope.

3.4 (Continued):

The final step in the certification process is the aggregation of the individual failure rates within a component, calculation of the component reliability, and comparison of its calculated reliability to its reliability allocation. This bottom-up reliability assessment must be greater than the predefined reliability allocations for each component. This does not mean that no failures will occur during testing, but there will be fewer failures than in prior programs.

The intent of this document is to provide an indication of the future reliability challenge, and to define a recommended engine certification process to meet this challenge. The user-level detail of this certification process is explained in subsequent sections. These features include:

- a. Priority on reliability equal to performance or cost.
- b. Utilization of failure modes and effects and fault tree analyses for early identification of design weak links and critical failure modes or parts.
- c. Early (design phase) quantification of reliability, based on estimates allowing early corrective action.
- d. More sophisticated analysis (i.e., probabilistic techniques) to supplement conventional (deterministic or margin) analyses on critical parts or failure modes.
- e. Guidance to focused, cost-effective testing.
- f. Continuous feedback of results (design analysis and test data) allowing continuous assessment of reliability, refinement of analytical models or identification of design improvements.
- g. A mechanism to encourage the TQM principle of concurrent engineering and track progress toward the principles on continuous improvement.

4. DESIGN CERTIFICATION METHODOLOGY:

4.1 Introduction:

New launch vehicles being developed for flight in the year 2000 and beyond are requiring demonstrated propulsion system reliabilities of $\geq 99.0\%$. However, the reliability of prior launch vehicles has only demonstrated flight reliabilities of $\sim 96\%$. Examination of the flight failure histories indicate that many of these failures have been associated with the propulsion system. A further review reveals that these failure rates are consistent for several classes of vehicles (Atlas, Delta, Thor, and Titan). Flight histories for the foreign vehicles show a similar trend. The French Ariane and the Russian Proton have flight failure rates close to 5% (or $\sim 95\%$ reliability). Based on these statistics, vehicles designed and developed by the current process can expect to achieve flight reliabilities of no greater than 96% flight success. This means that current vehicles will experience one failure every 25 launches on average. The occurrence of the propulsion

4.1 (Continued):

failure on the Space Shuttle-mission 51L clearly established this same failure rate, one in twenty-five launches. Since most propulsion systems have been designed in a similar manner over the last 30 years and propulsion system failure rates between most vehicles are similar, then the design, development, and demonstration/qualification process of these propulsion systems must be suspect. Design practices, in the rocket propulsion community, for establishing the expected mission reliability, typically have been based on qualitative assessments and/or deterministic methods. Quantified reliability assessments have been based on limited test experience and deterministic engineering analysis. These methods are extremely limited in quantifying the system reliability and can lead to erroneous reliability assessments. Shortcomings of these approaches are given in Feynman (1986) and in a National Research Council Audit (1988). These references indicate a need for improved approaches for characterizing and managing failure risk. If we wish to improve flight reliabilities for future vehicles, the design/development philosophy and approach must change in order to attain higher vehicle reliabilities.

Currently, the design process for determining mission reliability is referred to as flight certification. Flight certification is a process during which design confidence is established through a combination of engine analysis and testing. Design analysis is verified through a series of formal design reviews whereas the engine testing is evaluated through a formal group of flight profile tests. These certification tests are conducted at two levels, the single engine test level and the engine cluster level. This testing assures that the flight configuration engine can perform over a specified range of operational and environmental conditions without failure or a major engine anomaly for a defined period of time. The certification of launch vehicle propulsion systems consists of a limited amount of engine testing of flight configuration systems, due to funding limitations. For example, certification of the Space Shuttle Main Engine (SSME) has consisted of testing two flight configuration engines, each under simulated mission conditions, for twice the operating time or number of missions. This practice is commonly referred to as the "2X rule". For example, under this rule, certification for a five mission increment would consist of testing two engines each for ten missions with inspections and/or maintenance, including scheduled component replacement, carried out according to procedures prescribed for flight engines. Certification is accomplished if the testing is completed with no failure or anomalous events.

Much of the engine flight operating confidence is determined during flight certification reviews and engine testing. These practices are similar to past aircraft practices, in both the commercial and military sectors, as exemplified by the now obsolete FAR 33.14-6 (1974). Sufficient flight certification testing, extensive enough to establish high design confidence and high engine operating reliability, is prohibitively costly. Therefore, engine design confidence and reliability must be improved during the design process. Additionally, where the design process cannot fully establish design confidence, a structured test program can be defined to validate or obtain the design data to improve the design confidence and overall engine reliability.

4.1.1 Overview: The method by which new rocket propulsions systems are designed, analyzed, and tested must change. This change in the design process is caused by new demands for increased engine reliability at the lowest possible cost. High reliability at low cost seems like an anachronism, but new Air Force guidelines (RM2000) and the DOD "Total Quality Management Initiative" are dictating that contractors elevate reliability to equal status with performance and cost. These guidelines/initiatives are also carrying incentives/penalties, if program cost, performance, and reliability goals are not met, such as:

- a. Program incentives for achieving cost/performance goals or penalties of nonpayment if goals are not achieved
- b. Source selection participation
- c. Performance-based progress payments
- d. Warranties to ensure performance over time

More recently, the National Launch System (NLS) and the National Aerospace Plane (NASP) programs are specifying quantitative reliabilities at the engine level for new launch vehicle propulsion systems. These new government guidelines and contract specific engine reliability requirements are dictating new approaches to design, analysis, and testing.

Traditional design analysis approaches are deterministic and not capable of quantitatively predicting hardware reliability. Most engine design/development programs rely on the component and engine level test programs to establish engine reliability. This forces the engine program to wait 2 to 3 years before component reliabilities can be demonstrated and 4 to 5 years before an engine system reliability can begin to be demonstrated. A "test for reliability" process was required on prior engine development programs, since the "design for reliability" approach was not available to assess hardware reliability during the design phase. As a result, alternative design configurations could not be quantitatively assessed for risk during the design phase, and engine reliability demonstrations come too late in the program to modify effectively the baseline design (unless a catastrophic failure mode was uncovered).

Since design reliabilities for most components are never determined, these component reliabilities usually remained unknown, and one never knows how robust a particular design is or how close to failure it may be during the test program. However, many hardware failures can be circumvented by analytically determined design margins during the design process. Fewer hardware failures result in a shorter engine development program with attendant lower program costs. The objective is to determine hardware reliability during the design process and to assure that system reliability is being achieved efficiently and effectively.

The NLS program demands a highly reliable/low cost engine system, whereas, the National Aerospace Plane (NASP) demands high performance/high reliability. Both programs dictate a "design for reliability" approach to assure a robust engine design. Based on the need for a

4.1.1 (Continued):

“design for reliability” approach, traditional design/analysis methods must be modified or supplemented to achieve program goals. An approach is presented below, which allows the Simultaneous Engineering Team to quantitatively estimate the design reliability in the early stages of the design process. This method will also allow conscious design trades to be made, based on reliability, cost, and performance issues. This approach is generic enough in nature that it can be applied to any engineering project and not just rocket engine propulsion systems.

- 4.1.2 General Approach: During the design and development of launch vehicle propulsion systems, engines have a significant number of failure modes. In order to assess the probability of failure for each failure mode, data for important governing design parameters may not be well known (e.g., knowledge of dynamic environments or local operating conditions may be highly uncertain, or the accuracy of engineering models used to characterize the failure phenomena may be in question). Deterministic analysis approaches alone cannot quantitatively account for the sensitivity of reliability with respect to these unknowns. In addition, cases where performance, weight, and cost requirements force the use of new design approaches, advanced materials, and more severe operating conditions, no suitable experience base exists to “calibrate” deterministic analyses to either characterize or predict failure. Deterministic analyses under these conditions (limited information and uncertain knowledge) have serious shortcomings and can result in erroneous design decisions or misinterpretation of the analysis. Therefore, a formal procedure for quantitatively accounting for design risk is required.

Two fundamental sources of information are available during the design and development of an engine: engineering analyses and operating experience. Engineering analyses characterize the conditions under which specific failure modes may be expected to occur, for example, engine operating conditions and accumulated time in service. Operating experience may consist of development testing, certification testing, and flight operation. When operating experience for flight configuration hardware consists of a relatively limited amount of testing without failures, which is the case for most launch vehicle propulsion systems, it is a weak information source for failure risk assessment. This requires engineering analysis for an accurate assessment of the engine design.

The design process must assess all potential failures modes through a combination of deterministic and probabilistic analyses. All hardware designs should be evaluated deterministically for two reasons:

- a. Most hardware designs are sufficiently insensitive to the environment that a probabilistic analysis is not warranted. A rigorous deterministic analysis with consideration of design sensitivities is adequate.

4.1.2 (Continued):

- b. The deterministic approach is the current technique for evaluating hardware designs. A change to a reliability assessment approach must be gradual for design continuity and should only be substituted as confidence is warranted.

Probabilistic analyses should be conducted on “critical components” (e.g., turbine blades, bearings, injector posts, or critical weld joints, etc.). Probabilistic analysis would be limited to this type component, since it is these components that historically account for most engine failures. Other components that should be considered would be identified as a result of uncertainty of design values, low design margins, or inadequate analysis modeling tools. This process of design analysis continues in an iterative manner until the engine reliability goals are met. In contrast to deterministic analysis, probabilistic analysis considers distributions of input variables rather than worst case values, which yields a distribution on failure occurrence. It also permits design sensitivity analyses to be conducted. The output of this analysis process is the probability of failure for a particular failure mode. Failure modes can be aggregated to obtain the failure rate for a major component or the entire engine system. Figure 5 describes the design flow process.

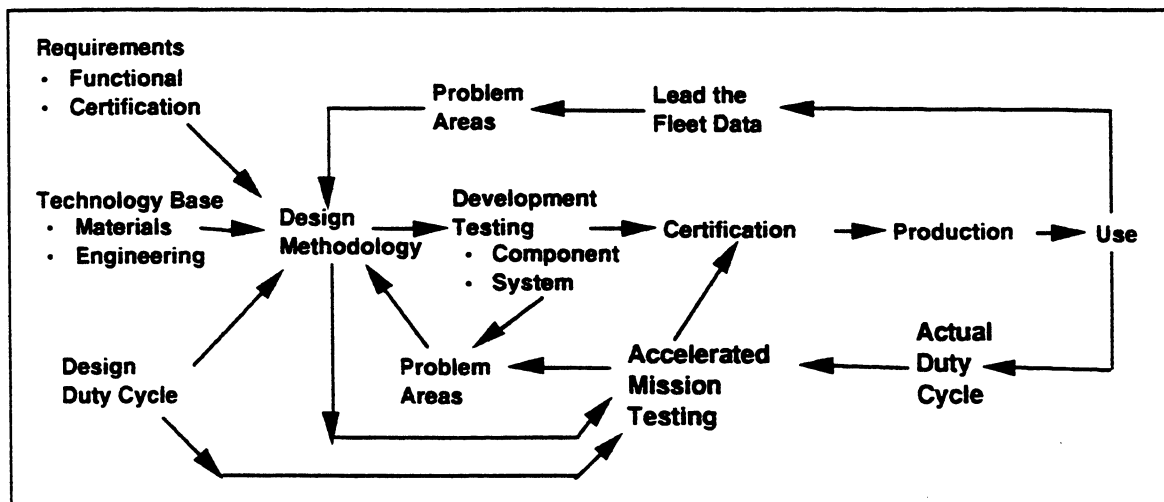


FIGURE 5 - Design Flow Process

The probabilistic analysis sensitivity evaluation referred to above, can identify and assess the magnitude of design weaknesses and/or data limitations (effect of input variables to the analysis result). The magnitude of the data deficiencies are defined by the importance of one input variable's effect on the analysis result. Assessment of all input variables (in this same manner) will dictate the priority of each input variables effect on the analysis result. Input variables which significantly affect the analytical result may require additional data and can assist in developing a structured test program to acquire these data. This structured test program may affect the materials selected and/or tested, manufacturing machining data

4.1.2 (Continued):

(final geometry/tolerances and surface finish effects), or the instrumentation and tests to be conducted on the hardware. Conducting such a structured test program will mitigate design, development, and production risk and will assist in developing a robust or damage tolerant design.

Once the engine has been designed and analyzed by an iterative process, the focus would be toward development testing of the hardware. This test program would verify or anchor design assumptions/analysis, obtain necessary data dictated by the analysis process, update estimated environments, or augment the design reliability based on test history. Test data can be incorporated into the failure risk assessment for specific failure modes via a Bayesian statistical framework. Figure 6 illustrates the process. Engineering analyses provide information to establish the "prior" failure risk estimate, which can be modified to reflect available success/failure test data using a Bayesian statistical analysis. Engineering analyses are based on available knowledge of governing parameters that may be derived in part from measurements taken during operation and in part by experience and/or relevant analysis. The failure risk estimate resulting from the combination of the prior risk estimate and the success/failure data is that warranted by the available information (see Moore et al. (1990-1991), Martz and Waller (1982), and Moore et al. (1990-1992).

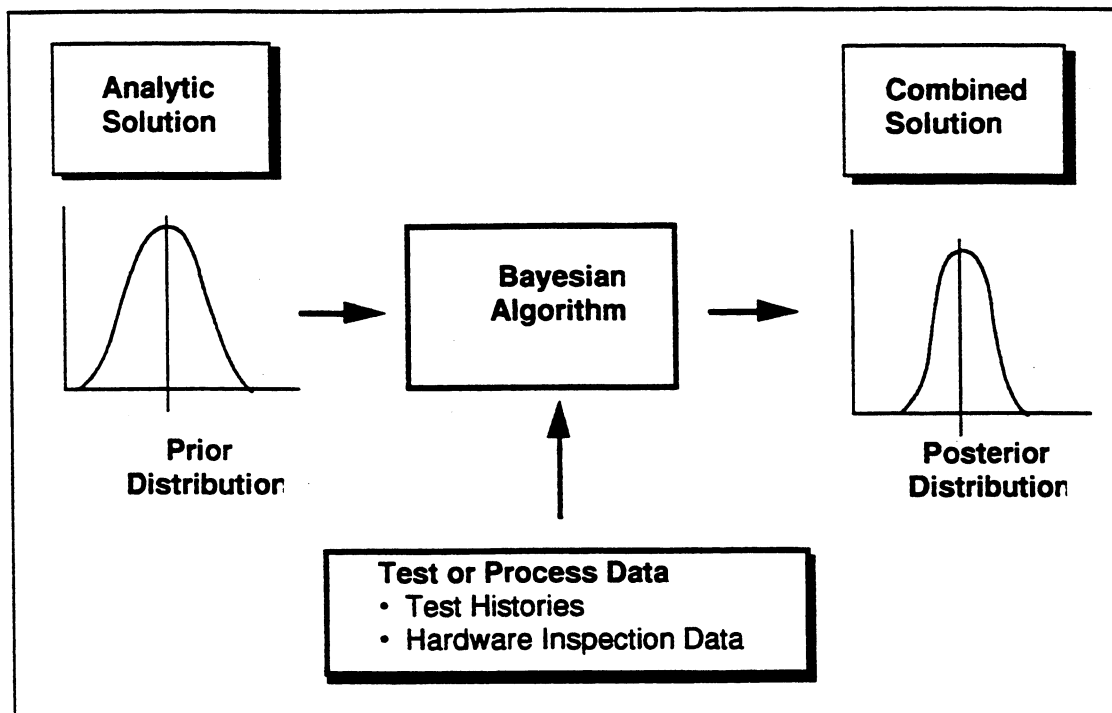


FIGURE 6 - Bayesian Algorithm Incorporates New Information

4.1.2 (Continued):

As additional information regarding governing parameters becomes available, it can be incorporated into the engineering analysis using the same Bayesian statistical algorithm, which will update the failure risk estimate. Since the available success/failure data is a weak information source, the failure risk estimate will be predominantly based on the prior failure risk estimate of Figure 6. During several case studies of liquid propellant rocket engines failure modes, it was found that incomplete knowledge of certain design analysis parameters was a major source of uncertainty regarding the probability of occurrence of specific failure modes (see Newlin et al. (1990) and Sutharshana et al. (1990)).

4.1.3 Benefits: There are several benefits derived from using a “design for reliability” approach:

- a. A quantitative assessment of the hardware reliability can be made during the design phase.
- b. The uncertainty of each design variable is explicitly considered in the analysis process which considers the sensitivity of the design.
- c. The most significant design variables are ranked in order of their effect on reliability.
- d. Design trades can be assessed for reliability impact.
- e. Gaps in the design data base are identified - program resources can be utilized effectively to obtain necessary data.
- f. Communication between disciplines is facilitated thus aiding the concurrent engineering process.

Application of this certification methodology to assess mission failure risk during design, development, and operational phases will reveal weaknesses through unacceptably high failure probabilities for specific designs. Specific corrective actions can be taken to reduce high risk designs as shown in Figure 7. Since this methodology produces a risk assessment of the design that is commensurate with the available information, designs which produce unacceptably high risks can be improved by:

- a. Acquiring additional information to reduce the design parameter uncertainty (e.g., additional characterization of loads and/or environments)
- b. Changing the design
- c. Improvements in manufacturing processes to decrease variability
- d. Validation of analytical models
- e. Improved characterization of materials

4.1.3 (Continued):

The additional testing indicated provides a broad range of options for corrective action of a specific design deficiency.

Design Guidelines • Reduced stress concentrations • Flexible tolerancing • Standard machining callouts • No platings for H₂ embrittlement • No sharp design transitions • Make part inspectable	Development Guidelines • Material testing/data • Comprehensive component testing • Structured system test program • Highly instrumented system tests • Statistical process control • Design feedback
Fabrication • Influence design up-front • Target Tolerancing • On-machine inspections • Statistical process control • Design feedback	Operations Guidelines • Influence design up-front • Maintenance lessons learned • Failure history (operations or test) • System simplification/streamlining • System reliability checkouts • Pre-launch checkouts

FIGURE 7 - Design Risk Reduction Concepts to Infuse High Reliability

Any overall additional cost of the probabilistic analysis will be defrayed based on early failure mode identification and mitigation or reduction of failures during engine development or flight operation. This rigorous approach to design and development forces the design to be more robust or damage tolerant, which results in the hardware being more forgiving. It is anticipated that several potential failure modes will be eliminated during the development program resulting in major cost program savings.

4.2 Design for Reliability Approach:

The approach to certification outlined and depicted in Figure 8, not only controls the overall design process, but takes full advantage of present day design/analysis tools and engineering/reliability methodologies. This approach, which starts during the conceptual design process, continues throughout the design phase, the engine demonstration phase, and flight development phases of the program. It is important to realize that product reliability must be designed-in to achieve the desired end result. Therefore, a quantitative reliability assessment during the design phase is imperative. This process starts as early as possible and continues throughout the program, as required. For reference, the NLS engine program has selected a design reliability goal of 0.999 (design-to-reliability goal) for the engine system and has a demonstrated reliability goal of 0.99 at 90% confidence.

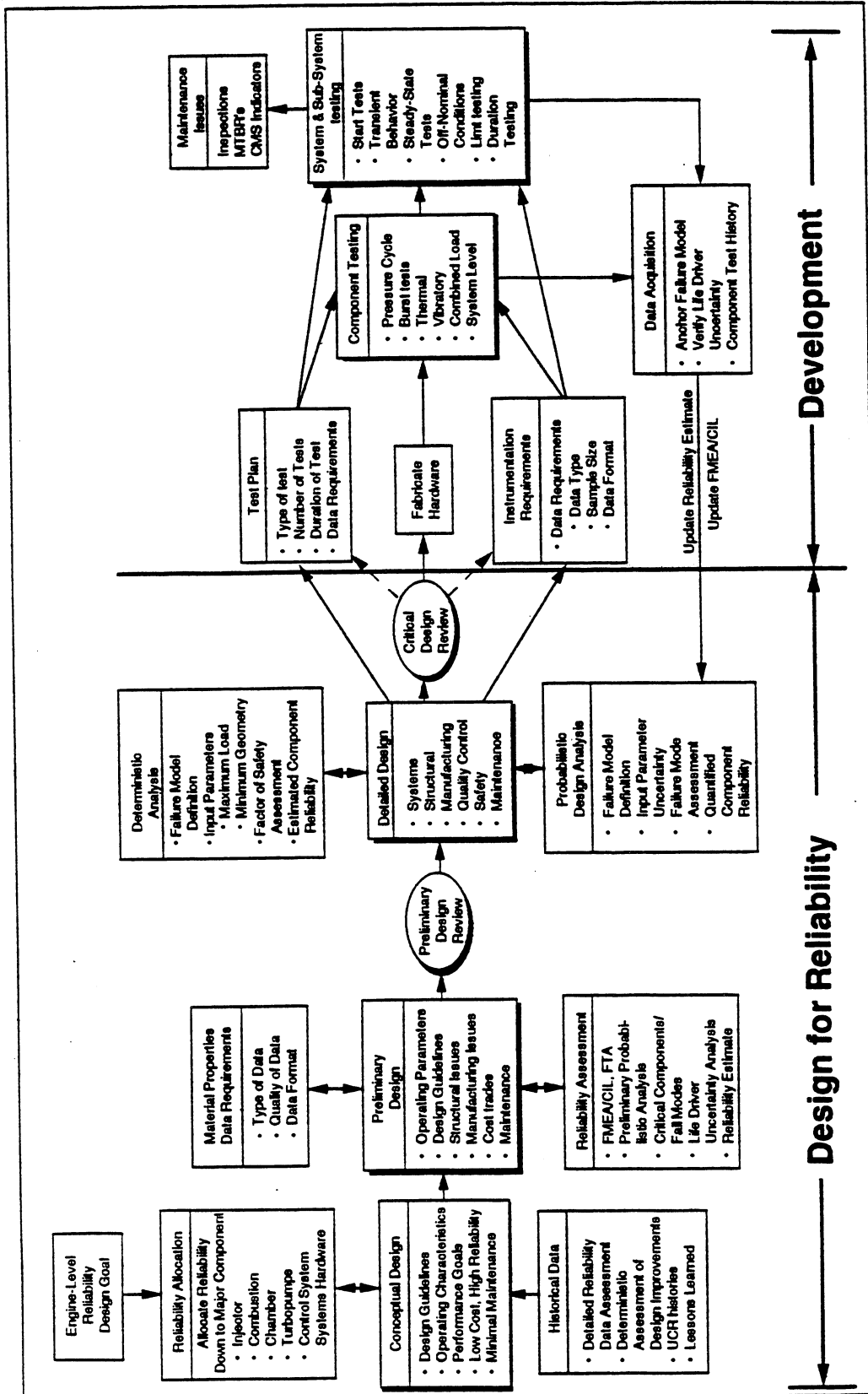


FIGURE 8 - Design for Reliability Flow Process

4.2 (Continued):

An overview is presented, which shows the project phase relationships to the “design for reliability” approach and their order of execution. This overview is followed by a more detailed discussion of the unique features on the design process. Specific design references will be identified.

- 4.2.1 Conceptual Design: During the conceptual design phase, designers establish a clear definition of product requirements and essential engine operating conditions leading to a responsive design concept. At this point, a preliminary reliability assessment must be performed to define system level design reliability goals and major component reliability allocations. Initially, an engine level reliability must be selected, which is dependent on what the program is willing to accept.

It should be noted that the reliability allocations are based on design-to goals and these reliability allocations cannot be demonstrated by test, due to prohibitively high test program costs. Design-to reliability goals are selected to ensure meeting the demonstration reliability goals during the engine certification program (usually six years after starting the design). This design-to engine level reliability is then allocated down to the major elements such as turbopumps, combustion chamber, nozzle, ducts, valves, etc. Figure 9 graphically describes the process. Reliability allocations are usually based on historical data from past engine programs or similar commercial engine systems. Once these reliability allocations have been defined, they become target values for designing new components using a bottom-up reliability assessment.

During the conceptual design phase, competing designs are evaluated to identify a configuration which is balanced between reliability, cost, and performance. Initially, a deterministic design approach is used to evaluate each design concept. These conceptual designs are evaluated qualitatively in nature, based on program requirements, design goals, and incorporation of “lessons learned”. Most designs are selected based on a qualitative figure of merit, engineering judgement, and minimum risk to the program, while still meeting or exceeding the program goals/requirements. A more quantitative design assessment can be performed using simplified probabilistic analyses techniques based on experience with previous programs. This approach would allow a more rational criteria for the conceptual design down-select. Once the down-select process narrows the design options to one or two concepts, then the more formal probabilistic modeling to assess reliability begins (on critical parts).

- 4.2.2 Preliminary Design: The preliminary design process involves several tasks, which include sizing of the hardware, assessing the system integration issues, defining potential failure modes, and estimating the hardware reliability (bottom-up design appraisal). These tasks are:
- a. Establish preliminary design configuration
 - (1) Complete top assembly layouts
 - (2) Define the preliminary parts list

COMPONENT RELIABILITY ALLOCATION

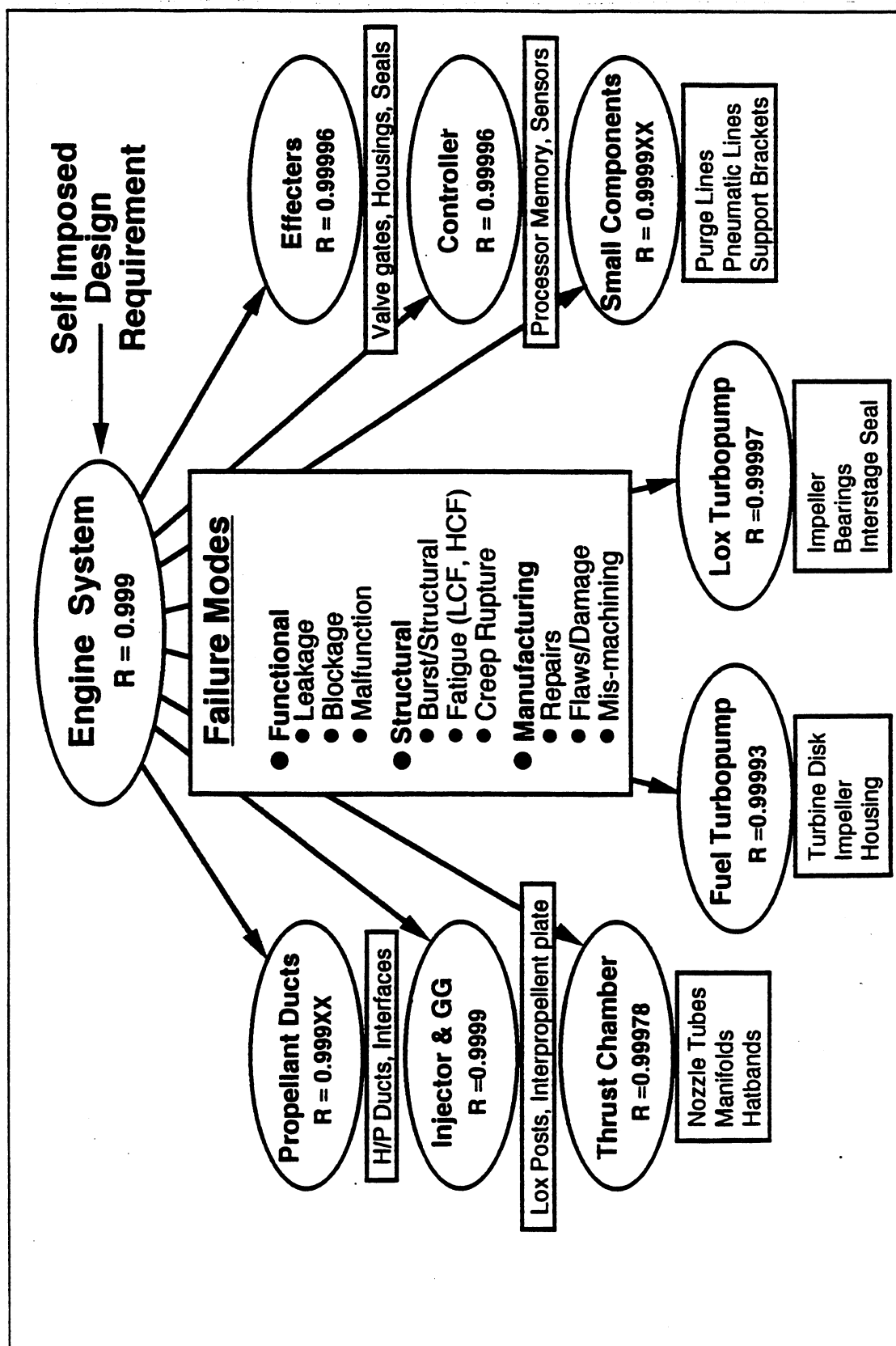


FIGURE 9 - Initial Top Down Approach

4.2.2 (Continued):

- b. Conduct a deterministic analysis of the preliminary design
 - (1) Hardware sizing
 - (2) Identification of weak links
 - (3) Quantification of design parameter uncertainty
 - (4) Material property definition/characterization
- c. Perform failure modes and effects analysis (FMEA and fault tree analyses - FTA)
 - (1) Identify all functional failures
 - (2) Define potential structural failures
 - (3) Assess the synergistic effects between failure modes
 - (4) Develop a manufacturing process diagram for critical processes
 - (5) Identify potential process failure modes
 - (6) Define potential engine level/system failure modes
 - (7) Establish failure mode criticality
- d. Conduct a critical hardware screening assessment
- e. Perform a preliminary reliability assessment
 - (1) Evaluate the “driver” variability/uncertainty
 - (2) Estimate hardware reliability using simple analysis methods

This information must be summarized for each component or critical part. Once the design data are available, critical engine components must be identified that require more detailed analysis. These components can be identified by use of a screening technique. A screening technique, illustrated in Figure 10, evaluates all components based on several criteria related to design, analytical, and failure consequence issues. Components identified by this screening technique are defined as “critical hardware” and require a probabilistic analysis. The number of critical hardware items is a small percentage of the engine hardware and will be a function of hardware complexity, severity of operating conditions, low structural margins, and hardware failure consequences. Simplified probabilistic analyses can be accomplished for these components to provide a limited assessment of this hardware. This simplified analysis furnishes the first assessment of hardware design margin (level of robustness).

- 4.2.3 Detailed Design: The detailed design analysis formally assesses the baseline design. As mentioned earlier, all components must be analyzed deterministically and only the “critical hardware” will receive a probabilistic assessment. The traditional deterministic approach assesses components based on maximum predicted engine operating loads, worst case component geometries, and minimum material properties. This methodology is well established and no further discussion is warranted. The main difficulty with the deterministic method is that component factor of safety (margin of safety) does not allow component or system reliabilities

CRITICAL COMPONENT SCREENING

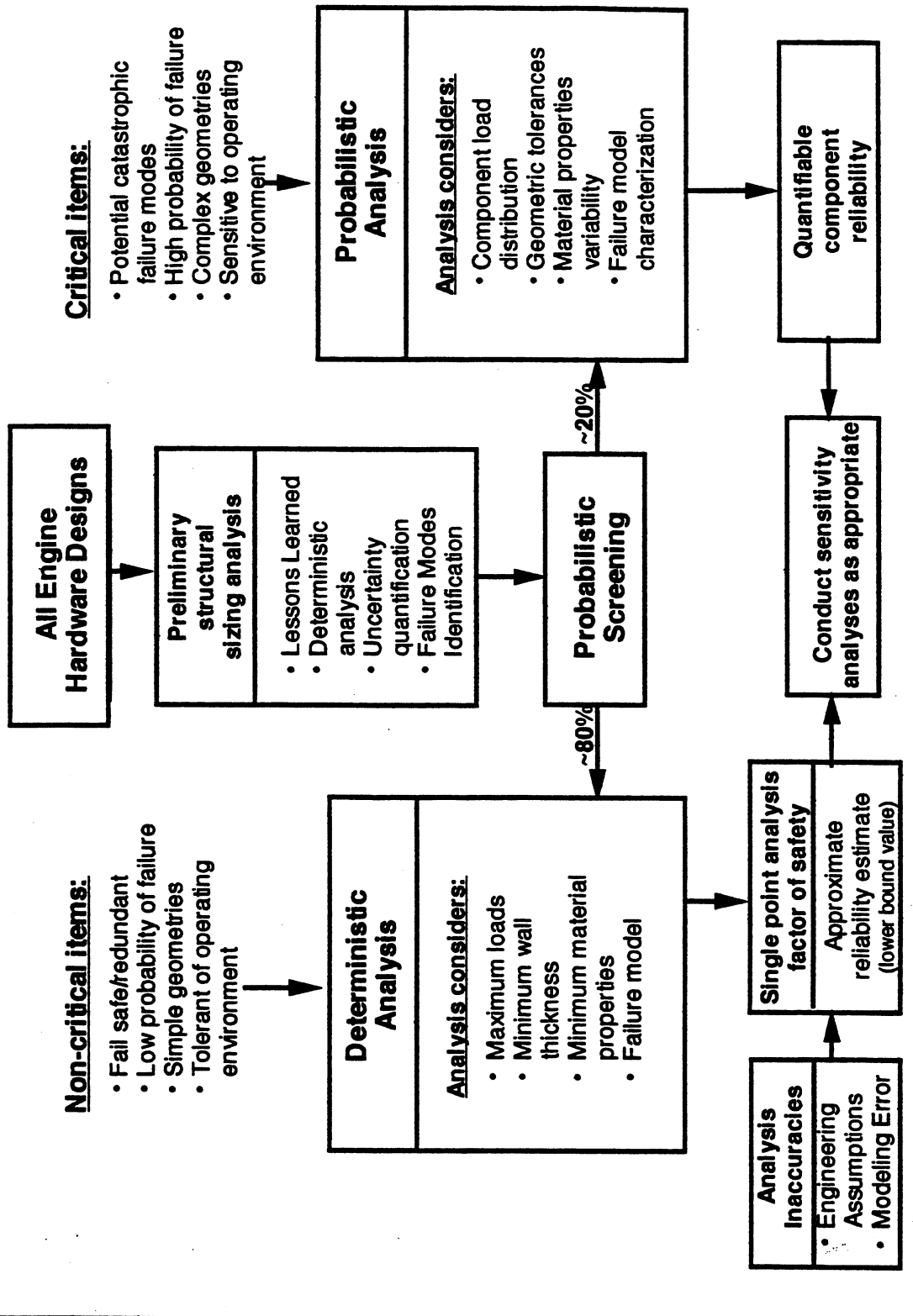


FIGURE 10 - Critical Failure Modes Screening Technique

4.2.3 (Continued):

to be estimated. Additional analyses are required to estimate component reliability. Two methods are available that can predict component reliability:

- a. Simplified probabilistic analysis
- b. Detailed probabilistic analysis

Simplified analysis techniques are fast, but not highly accurate. These techniques permit a rapid assessment of the design, but not an in-depth one. Several techniques exist for conducting a simplified probabilistic analysis and are described in Section 7. These analysis techniques are generally used in the preliminary or detailed design phases. In the preliminary design phase, rapid analysis techniques permit a quick assessment between competing designs. In the detailed design phase, this technique can assess a failure mode that was not identified as "critical" but still requires further study due to its critical failure consequence.

Detailed probabilistic analysis techniques are more complex than the simplified analysis, but results are highly accurate. These techniques permit a detailed assessment of the design and are usually conducted in the detailed design phase. All critical components identified by the screening process must undergo a probabilistic analysis and a detailed sensitivity analysis. Output from this assessment will affect the fabrication process and/or the material, component, and engine level test programs. This technique is also described in Section 7.

Once the reliability is computed for each failure mode, the reliability estimates are combined based on failure mode relationships, such as dependent or independent failure modes. Most failure modes can occur independently of each other in most situations, but synergistic relationships between failure modes are not uncommon. An initial approach would be to assume that all failure modes are independent and in series, unless a definite relationship exists that can be modeled. This technique for combining failure mode reliabilities is continued until a bottoms-up reliability assessment has been computed for the major component. At this point, the major component reliability estimate is compared to its predetermined reliability allocation. If the reliability estimate is greater than the allocation, then the design is adequate; if not then a reassessment is required. Figure 11 describes this process. This reassessment may involve one or more of the following actions:

- a. Redesign of the hardware to eliminate or minimize failure mode
- b. A more rigorous analysis of the hardware
- c. Better definition of the component environment which may dictate a specific test program or instrumentation
- d. Acquisition of data, such as material properties test data or engine operating environments which may not be well defined

ASSESSMENT OF RELIABILITY COMPLIANCE WITH ALLOCATION

Component	Allocation	Estimate	
		Simplified	Probabilistic
Fuel Turbopump Pump Assy Main Housing Pump Inlet Hsg Inducer Impeller Tie Bolt Seals	0.999722		
	↑ 0.999930		
	↑ 0.999997		0.999997
	0.999997	0.999999	
	0.999994		0.9999975
	0.999991		0.9999984
	0.999991	1.0	
Turbine Assy Inlet Manifold Turbine Nozzle Turbine Wheel Turbine Disk 1st Stg Blades 2nd Stg Blades Bearings	0.999994		
	↑ 0.999994		
	0.999994	0.999999	0.999996
	0.999932		
	↑ 0.999994		0.999996
	0.999968		0.999970
	0.999971		0.999983
	0.99995		0.999998
			0.999999

FIGURE 11 - Comparison of Reliability Estimate to Allocation

4.2.3 (Continued):

e. Improvement in fabrication process or inspection capability

The probabilistic methodology provides the capability to perform sensitivity analyses which would identify analytical, design data, or process deficiencies. Sensitivity analyses identify key design and process parameters that significantly affect the design reliability and where acquisition of specific design data would be prudent. Based on these data deficiencies, necessary design data can be acquired through a structured test program. This structured test program would enable program managers to utilize effectively limited financial resources during the development and improvement test programs. Probabilistic analyses can provide a key to defining a comprehensive test program for either material, component, or engine level test programs. Analytical or design data deficiencies, such as design variable uncertainty (poor loads or material definition) or ill-adapted analytical models (usually associated with nonlinear component behavior), are identified by the "design for reliability" method. The magnitude of the uncertainty and its associated effect upon the failure model/reliability assessment will dictate where additional data are required. The test program can be restructured or instrumentation can be added to obtain the necessary data. In many cases, the test program will be conducted in the same manner, except that specific instrumentation will be added to acquire the desired data.

- 4.2.4 Design Feedback: During the life cycle of the program it is important to receive design feedback from the development and production phases of the program. The design analysis cannot stand by itself. Engineering assumptions, estimated loads/environments, material properties, and model results for critical hardware must be validated. The structured test program (sometimes referred to as the master test program) will provide these data. These data are obtained from test programs such as materials testing, piece part or component testing, and/or system level testing. These data are extremely important but not sufficient. The hardware process data must be validated. New fabrication techniques require verification and process control. This statistical data can validate geometric data including actual versus design tolerances. Additionally, surface finishes can be defined which may affect the material properties. Most importantly the manufacturing process must be reviewed to ensure that the hardware does not see a more aggressive environment during fabrication than normal engine operation. These design data must be compared to the initial input variable distributions to verify compliance. Installation and assembly procedures can also affect the capability of a part. Therefore, for "critical components", the specific failure modes should be assessed for process variations that could significantly affect the component reliability.

It must be noted that many of the flight failures that occurred on the prior vehicles can be attributed to a process or procedural change. It is for this reason that process failures must be considered and assessed. A process FMEA can provide significant insight into the criticality of the process on the part.