Key Reliability Drivers of Liquid Propulsion Engines and A Reliability Model for Sensitivity Analysis

Zhaofeng Huang, Jeffry A. Fint and Frederick M. Kuck
The Boeing Company, Rocketdyne Propulsion & Power, Canoga Park, CA 91309

Abstract

This paper is to address the in-flight reliability of a liquid propulsion engine system for a launch vehicle. We first establish a comprehensive list of system and sub-system reliability drivers for any liquid propulsion engine system. We then build a reliability model to parametrically analyze the impact of some reliability parameters. We present sensitivity analysis results for a selected subset of the key reliability drivers using the model. Reliability drivers identified include: number of engines for the liquid propulsion stage, single engine total reliability, engine operation duration, engine thrust size, reusability, engine de-rating or up-rating, engine-out design (including engine-out switching reliability, catastrophic fraction, preventable failure fraction, unnecessary shutdown fraction), propellant specific hazards, engine start and cutoff transient hazards, engine combustion cycles, vehicle and engine interface and interaction hazards, engine health management system, engine modification, engine ground start hold down with launch commit criteria, engine altitude start (1st start), Multiple altitude restart (> 1 restart), component, subsystem and system design, manufacturing/ground operation support/pre and post flight check outs and inspection, extensiveness of the development program. We present some sensitivity analysis results for the following subset of the drivers: number of engines for the propulsion stage, single engine total reliability, engine operation duration, engine de-rating or up-rating requirements, engine-out design, catastrophic fraction, preventable failure fraction, unnecessary shutdown fraction, and engine health management system implementation (basic redlines and more advanced health management systems).

Nomenclature

R_T	=	Single engine total reliability
$R_{S,X}$	=	Engine cluster system reliability. X is a subscript to denote the system reliability formula evolvement
N	=	Number of engines in the propulsion stage
C_f	=	Catastrophic failure fraction
P_f	=	Preventable failure fraction
U_f	=	Unnecessary shutdown fraction
S_f	=	Survivable failure fraction
E_f	=	Erroneous shutdown fraction
HMS	=	Health Management System
MTBF	=	Mean Times between failures
WEO	=	With-engine-out
WOEO	=	Without-engine-out

I. Introduction

Reliability has been one of the most important launch vehicle design parameters. NASA's new space exploration activities, such as the Crew Exploration Vehicle (CEV) and the Shuttle Derived Launch Vehicle (SDLV), have given great attention to the reliability of new vehicle designs. The industry SDLV consortium team has intensively assessed reliability trades in the early stages of its conceptual configuration design and trade study activities. A liquid propulsion rocket engine, as one of the leading candidates for launch vehicle propulsion systems, is at the forefront of addressing the need to effectively improve reliability starting from the early conceptual design

phase. We start the paper by identifying a comprehensive list of reliability drivers at liquid rocket engine system and sub-system levels. We then briefly discuss each driver, the reliability implication of it, and the inter-relationships among the drivers. We would like to point out that we don't plan to elaborate details of each driver in this paper, considering each driver itself may deserve a focused discussion and a devoted technical paper. Our intention of this paper is to bring reliability awareness to all interested parties, collaboratively address reliability issues with government and industry partners, and implement design-for-reliability approaches starting from early design stages with an objective of significantly improving future launch vehicle reliability. We present a parametric reliability model and some sensitivity analysis results to illustrate the impact of some of the drivers on engine system reliability.

II. Reliability Drivers

We have listed the reliability drivers in the abstract of this paper. The list is based on launch vehicle failure history, a literature search, authors' experiences, and formal and informal communications among industry companies and customers. We will briefly discuss the drivers one-by-one in this section.

Number of liquid propellant engines for the propulsion stage -- One would think it is trivial to discuss this. Is it ? Can we answer the questions "is a propulsion system with less engines better than a system with more engines?" "How about thrust size of the engine?" "Why don't we design a stage with a single engine providing all thrust needed ?" "Is a bigger engine less reliable than a smaller engine?" The answer depends on the detailed design, application needs and physical constraints. Several factors affect the design selection. Total thrust size, total impulse, engine-out design, reliability of the engine itself, catastrophic fraction, and the unnecessary shutdown fraction are some of them. Vehicle propulsion power needs will determine the total thrust and impulse allocated to all engines. Engine-out design, reliability of the engine itself, catastrophic fraction and unnecessary shutdown fraction will decide a single engine or multiple engine propulsion system from a reliability perspective. Our quantitative reliability model presented later will parametrically address the impact of the number of engines and several other related reliability drivers.

Single engine total reliability -- Total engine reliability (R_T) is the product of the engine catastrophic reliability (R_C) and the benign shutdown reliability (R_B). Both R_C and R_B are determined not only by the inherent engine design, manufacturing and operation induced root causes but also by the effectiveness of the health management system. Health management system implementation often considers the trades between all these parameters, especially if engine-out design is pursued.

Engine operation duration -- It is intuitive that the longer the engine runs, the lower the engine reliability. However, sometimes trades need to be considered for a longer engine running duration with smaller thrust or vice versus. Now the question is how to calculate the engine reliability with different run durations for different applications for the same engine. Is a 200 second running duration application twice as reliable as a 400 second application? The parametric model we present later will introduce a time adjustment equation and show some sensitivity results.

Engine thrust size -- To certain extent, an engine design can be scaled up or down to accommodate different thrust requirements. But we have recognized that many design parameters are not linearly scaleable due to complex physical relationships. Some threshold values may also exist for certain design features such that totally different design or manufacturing methods may apply resulting in a different reliability. One example is casting versus forging because of the size limitation of a part. Another example is turbopump turbine blade design, with damping or without, driven by the size of the engine. We have noticed that the correlation of engine reliability with its thrust size has not been systematically studied. There is probably no conclusive correlation if we consider just size vs. reliability though it is often assumed that the smaller the engine, the higher the reliability.

Reusability -- If we compare a reusable engine with an expendable engine, we will see several factors leading to different design considerations. Life requirements for a reusable engine usually are more stringent. As a result, it is more challenging to address fatigue related failure modes and causes. Reusable engines also go through post flight check out and between-flights maintenance activities. Pro of this is that the post flight inspections and between-flight maintenances can reveal hardware problems that can be addressed to further improve engine reliability that is not possible for expendable engines. A con is potential adverse effect due to human and process errors that impact

next flight reliability. We have noticed there is an inclination in liquid engine industry to favor more on expendable engine designs than on reusable engines. A detailed study yet needs to be conduct to address commonality and uniqueness of reliability for reusable engines and expendable engines.

De-rating or up-rating -- De-rating is a reliability improvement method that is popularly used in electronics industry to enhance reliability. The basic approach of the de-rating is to design a component at a more severe environment than its nominal operation environment. The application of de-rating has been one of the hot topics in liquid propulsion engine design. The question is can we design an engine with 500klb thrust but just employ the engine for a 400klb thrust application for de-rating reliability benefit. The historical data has indicated that about 90% of failure modes and causes are power level related which is correlated to thrust directly. So it appears that a lower power operation will reduce the failure probability. However, other failure modes particularly in turbomachinery are sensitive to natural frequencies, and operation at a lower power level may be more detrimental. Thus any de-rating approach must be on a case by case basis for each required thrust level. Another aspect is to increase the thrust to more than the nominal engine thrust level. An example is the potential operation of the Space Shuttle Main Engines at a higher thrust (106 to 109%) in an abort scenario if one engine is shutdown to prevent catastrophic failure. *How much reliability degradation does it result in?* Engine de-rating operation is also necessary for engine-out design since when one engine fails in a contained manner (engine-out), the rest of engines may need to increase their power in order to complete the mission. Therefore all engines, under nominal mission operation, have to be de-rated to a percentage of full power level.

Engine-out design -- We have touched on the topic several times in the above discussions. Engine-out design is a unique design feature for liquid propulsion engines. It is defined as the capability to permit the surviving engines to continue to operate when one or more engines fail in a contained manner. The mission can be accomplished by elevating the power level or extending the duration of the remaining engines. The mission may also be aborted but the vehicle is saved by the continuing operation of the surviving engines at some required power level. The trade off of an engine-out design is the extra mass of the engine and propulsion system that leads to a vehicle performance penalty. Reliability impact of engine-out design will be explored in more detail in our parametric reliability model presented later.

Engine-out switching reliability -- One of the most important reliability drivers for engine-out design is engine-out switching reliability. When the engine system encounters a benign shutdown of one or more engines, the system is in a significant transient. Valves open and close, power levels go up and down, and the propellant feed system and vehicle control system try to accommodate the unexpected conditions and save the mission and the vehicle. It is also an engine and vehicle integration design issue. We see the industry hasn't accumulated much experience and it is very much a challenge to design and validate the system to accommodate all of the contingency situations reliably.

Catastrophic fraction (C_f) -- We have defined C_f as the percentage of total engine failures (summation of contained and uncontained failures) that result in an engine uncontained failure and loss of vehicle. We denote F_u as the probability of engine uncontained failures and Fc as the probability of engine contained failures. Then $C_f = F_u/(F_u+F_c)$. Lower engine C_f provides a better opportunity for engine-out design to enhance system reliability. Historical Apollo and Space Shuttle liquid engine data have indicated C_f falls into the range of 20% to 40%. Several factors that affect the C_f are inherent design characteristics of the engine, effectiveness of health management system, and vehicle tolerance on an engine failure. Our parametric reliability model will present some sensitivity results for a range of C_f values.

Preventable failure fraction (P_f) -- We define P_f as the portion of the engine failures that would be catastrophic if the health management system had not caught and shut down the engine. The root causes of P_f are due to the inherent design characteristics. This type of failures is usually slow propagation failure events. The advancement of HMS development and effectiveness of HMS implementation can potentially mitigate some used-to-be catastrophic failures to benign shutdowns.

Unnecessary shutdown fraction (U_f) -- U_f consists of two portions: erroneous engine shutdown fraction (E_f) and survivable engine shutdown fraction (S_f). An erroneous engine shutdown is defined as an engine shutdown due to engine instrumentation failures while the engine operates nominally. A survivable engine shutdown is defined as an engine malfunction the engine can tolerate but that triggers HMS to shutdown the engine. The root causes of

survivable failures are due to the inherent engine design. C_f, P_f, and U_f add up to 1. C_f, P_f, and U_f are key parameters that support an engine-out design trade study. Our parametric reliability model will address these trades in detail.

Propellant specific hazards -- Liquid propellant choices can affect reliability. Each propellant has its own design characteristics, challenges and specific hazards. Examples are hydrogen embrittlement, and material compatibility with liquid or gaseous oxygen. Design solutions that mitigate and control specific hazards of certain propellant may adversely affect reliability of the engine.

Engine start and cutoff transient hazards -- Engine start and cut off transients impose some unique design challenges. During the transient periods, valves are opening and closing, and the engine controller and health management system closely monitor and act on many engine operating parameters. Some unique hazards and failure modes can occur, such as damage due to nozzle start transient side loads, and cut off pops from main injector and pre-burner propellant backflow. There is a surmise that an engine is more likely to fail during a transient period than in a steady state. One extreme view is that all engine failures are transient driven. But another view is that as long as transient engine operation is well designed and validated through a development program, the failure rate during a transient is no different from a steady state period. Both views lead to a conclusion that transient design and corresponding failure modes and hazards have to be treated seriously and systematically.

Engine combustion cycles -- The various pump-fed rocket engine cycles, differentiated by the method used to drive the turbopumps, have an influence on the inherent reliability of the engine. Typical versions have included 1) the most popular and earliest gas generator cycle using a separate combustor for turbine gas (e.g. RS-68), 2) the "expander cycle" using heat from nozzle cooling to expand the cryogenic propellant and drive the turbine (e.g. RL-10), and 3) the staged combustion cycle using the exhaust from turbine drive gas pre-burner(s) to fuel the main combustion chamber (e.g. SSME). Cycle selection involves consideration of complexity, controllability, and operating stress, pressure and temperature, which can affect the achieved reliability as well as the ease of engine development. Simplicity, based on few components and an uncomplicated schematic does not always lead to high reliability. A specific engine cycle and its detailed designs have to be evaluated for reliability impact, and unique design and reliability challenges have to be addressed.

Vehicle and engine interface and interaction hazards -- Vehicle and engine interface design is one of the key reliability drivers. Many interface and interaction related failure modes and hazards are of concern such as contamination passing from the vehicle to the engine or vice-versa, electromagnetic interference (emi), power supply failure, and propellant feedline blockage. A multiple engine system may also have possible common cause failures that lead to multiple engine shutdowns, which can result in a catastrophe. From design-for-reliability perspective, a robust vehicle boat tail design that can tolerate a sudden engine propellant leakage and/or shrapnel due to an engine failure will greatly improve vehicle system reliability and redefine the criticality of many engine failure modes and hazards.

Engine health management system -- We refer to the engine health management system as a basic engine redline system as well as advanced sensors and algorithms that include multiple engine parameters that infer an engine anomaly condition from sensor data and take mitigation action accordingly. Basic redlines are straightforward in that they usually act on a single operating parameter anomaly, such as a turbine discharge temperature higher than a pre-predicted nominal value approaching a material property limit. The SSME basic redline system currently has four in-flight redlines with five monitoring parameters. SSME Advanced Health Management System (AHMS) Phase I effort is to implement a high pressure turbopump vibration monitor that acts on a detected turbopump abnormal synchronized vibration signature and shuts down the engine safely when the redline is exceeded. SSME AHMS Phase II, as it was originally proposed several years ago, was to introduce a linear engine model, an optical plume anomaly detection (OPAD) and advanced vibration monitor system. The AHMS II type of systems promises not only to eliminate some catastrophic failures but also to mitigate benign shutdowns to non-shutdown actions such as throttle down or propellant mixture ratio adjustment as well as to reduce unnecessary shutdowns based on smart algorithms, therefore improving total engine reliability and mission success probability. For the general reliability discussion purpose, we define HMS implementation as three levels: basic redlines, HMS level I with enhanced redlines, and HMS level with advanced sensors and algorithms inferring from multiple engine parameters. Our parametric reliability model will address the reliability impact of these three levels of HMS implementation.

Engine modification -- It is often more appealing to modify existing engines for new applications than developing a new engine. It can save cost and reduce development and certification time significantly. But it is not risk free, especially for an upgrade that demands a higher capability, such as the cases of upgrading a non-reusable engine to reusable one, fixed thrust to a variable thrust, and thrust size increase. Even without capability upgrading, modification of an existing engine encounters risks of changing original design characteristics of the engine, and introducing new failure modes, causes and hazards. All potential risks have to be carefully evaluated and addressed for an engine modification activity.

Engine ground start hold-down with launch commit criteria (LCC) -- The SSME has about 6 seconds start phase hold down during a launch event. During that period, the engine starts, valves open and the power level ramps up while the engine is still on the ground. The engine controller and health management system checks and monitors numerous engine parameters to make sure the engine runs nominally and within expected conditions compared to the pre-established launch commit criteria. If the controller and HMS detect any malfunction, the engine will shutdown and the mission will be aborted. Most ground-start engine applications have this ground hold down period. It is designed to enhance in-flight reliability in several ways: 1). making sure engine is conditioned properly to proceed into main stage operation and to be off ground; 2). verifying all in-flight instrumentations perform nominally, and 3). screening for start transient phase failure modes and hazards, possible infant mortality failures from post acceptance test or flight inspections and check-outs, and residual risks carried from the last operation. Although historical data have indicated some mission aborts due to violation of LCC's had been unnecessary due to the conservatism of the LCC, the hold down period is a significant factor for flight reliability. Without the hold down period, engine flight reliability will be reduced. This is the case for altitude start engine application we discuss next.

Altitude Start (1st start) -- A multiple stage propulsion vehicle usually requires its upper stage engines to start at altitude. There are reliability pros and cons comparing altitude start vs. ground start. Example of pros is that for hydrogen engine, altitude start will not be concerned with a fire due to a hydrogen leak because of the vacuum environment. But overall, the cons outweigh the pros, mainly because altitude start engine will not have as effective launch commit check as a ground start with hold down period. Additionally, it is not easy for development tests to simulate and address in-flight altitude start failures. Some failures that may occur during the start phase will not be protected by LCC and start redlines. Some failures that may occur during main stage but would have been detected by the start LCC's will not be prevented. Propellant conditioning may also be a challenging design issue. We have introduced an altitude start penalty factor for reliability calculation for an engine that can be used for both booster and upper stage applications.

Multiple altitude Start (> 1st start) -- Much of the discussion of 1st altitude start is applicable for an upper stage engine that is required to start a 2nd or 3rd time. A multiple start (>2) engine application is like a reusable engine application but without the between-flight check-out and maintenance. Additional risks for 2nd or 3rd start include the residual risk from the first start that could have been prevented through ground pre-flight checkout and maintenance, and engine conditioning (drying, purge, bleed, chill down, inlet condition, etc.).

Component, subsystem and system design -- Many root causes of engine failures can be attributed to component, subsystem and system design. We fully recognize the importance of design-for-reliability starting in the early phases of design activities to address failure mode elimination and cause prevention and mitigation. The subject of design-for-reliability for identified failure modes and causes will be discussed in much more detail in future articles. Our parametric reliability model will use a top level set of reliability drivers and assume some reliability parameter values to conduct sensitivity analysis. The input parameter values of the model can be varied to accommodate different design-for-reliability strategies and potential reliability improvement results.

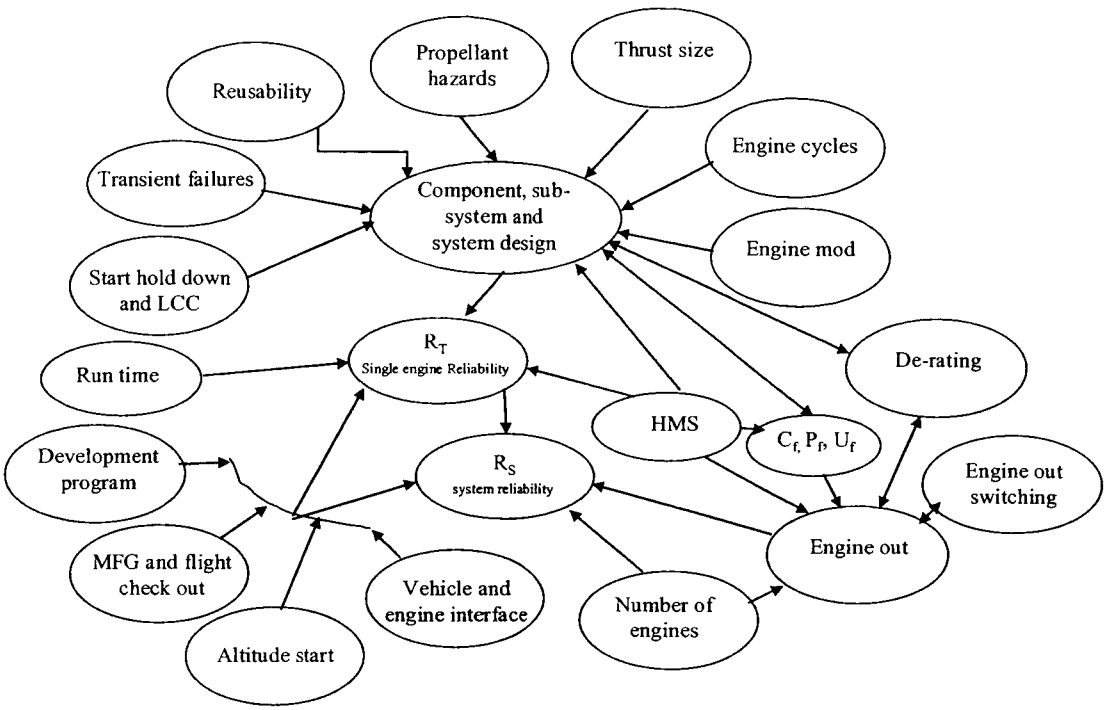
Manufacturing/ground operation support/pre and post flight check outs and inspection -- Manufacturing robustness, inspectability, pre and post flight check outs, maintenance activities all have significant effects on engine reliability. Human errors are often embedded in all these activities proportional to the opportunities of human being's involvement in the product and processes.

Extensiveness of development program – An engine development program is a key factor in the determination of flight engine reliability. Subscale, component and subsystem development and testing, lab and hot fire testing, certification programs, design verification, reliability verification and demonstration, failure analysis and corrective

actions, and redesigns are important elements of a development program to uncover issues and verify design and process fixes. Reliability growth, through a development program, and residual risk inherited from the development program, significantly impact the flight reliability.

Figure 1 presents an object oriented view of all engine reliability drivers and associations among them.

Figure 1. Engine Reliability Drivers and Their Inter-relationships



III. A Reliability Model

In this section, we will build the reliability model. Then in next section, we will derive some reliability sensitivity results using the model for some reliability parameter values.

We define an engine failure as an engine induced anomaly event that causes the engine not to meet its mission objective. We define an engine system failure for a multiple engine cluster propulsion stage as an engine anomaly that causes a mission failure. We also define the consequence of the failure in two categories: contained failures or uncontained failures. Contained failures are those that the failed engine is forced to be shutdown by health management system and the consequence of the failure is contained within the engine and no other vehicle elements are affected. We also call it as benign failures or benign shutdown. Uncontained failures are those that result in an instantaneous catastrophic failure of the engine and affect other vehicle elements in a detrimental manner. Examples of engine catastrophic failures are engine fire, explosion, massive and rapid propellant dump on other vehicle elements such as aft compartment, and engine shrapnel hitting adjacent engines or other vehicle components. By definition, a catastrophic engine failure results in loss of vehicle.

We start from a simple model then expand the model by introducing more reliability driver parameters discussed in the previous section.

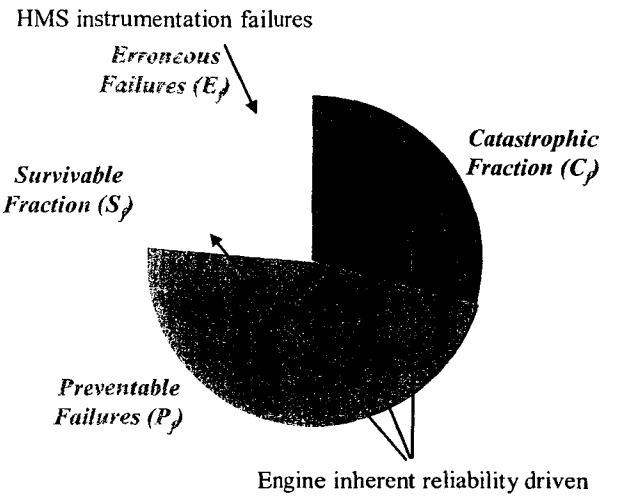
We denote R_T as single engine total reliability, N as number of engines in the cluster that powers the propulsion stage, and $R_{S,1}$ as engine cluster system reliability. We have

$$R_{S,1} = R_T^N \tag{1}$$

Equation (1) is a simple equation and needs to be evolved and be more specific for our applications. As we have discussed in Section II, the total engine reliability consists of 4 parts of the failure considerations, catastrophic fraction part, denoted as C_f; preventable failure fraction, denoted as P_f; survivable failure fraction, denoted as S_f; and erroneous failure fraction, denoted as E_f. The concept of decomposing all engine failures into these four failure fractions and addressing each of them individually according to their failure natures is one of the key and unique

reliability design features for liquid propulsion engines. These four fractions are directly relevant to an engine with health management system (HMS) in place. The four fractions add up to 100%. Root causes of C_f, P_f and S_f are due to engine hardware component failures and E_f is due to health management system errors or control system software errors. Figure 2 depicts the concept.

Figure 2. Total Engine Failure Probability



We apply Eq. (1) to an engine system with basic redlines active as the HMS implementation. After decomposing total failures into four parts, we have

$$R_{S,2} = (1 - C_f(1 - R_T))^N (1 - P_f(1 - R_T))^N (1 - S_f(1 - R_T))^N (1 - E_f(1 - R_T))^N \quad (2)$$

Considering the situation that redline system is deactivated, so we don't concern failure portions of S_f and E_f, for the reason that S_f, by failure nature, is survivable without redlines, and E_f is originated from HMS instrumentation induced erroneous shutdowns. So for the engine system without redlines active, we have

$$R_{S,3} = (1 - C_f(1 - R_T))^N (1 - P_f(1 - R_T))^N \quad (3)$$

With R_T sufficiently close to 1 (>.99), Eq.(3) can be approximated by

$$R_{S,4} = 1 - [NC_f(1 - R_T) + NP_f(1 - R_T)] \quad (4)$$

Comparing (2) with (3), one would draw a counter-intuitive conclusion that an engine system with redline system active is less reliable than the one without the redline system. Something must be missing. The missing part is engine-out design concept and its reliability implication. One of the essential reasons to implement a redline system, for multiple engine system, is to design the engine system with engine-out capability as we have described in Section II. This will improve the system reliability. Now we evolve our reliability formulas based on one engine-out capability for an engine system with N (>1) engines in the cluster. For this case, the engine system fails only when any of N engines fails catastrophically or 2 or more engines benign shutdown. Therefore, we have system reliability as follows

$$R_{S,5} = (1 - C_f(1 - R_T))^N [(1 - (1 - C_f)(1 - R_T))^N + N(1 - (1 - C_f)(1 - R_T))^{N-1}(1 - C_f)(1 - R_T))] \quad (5)$$

With R_T sufficiently close to 1 (>.99), Eq.(5) can be approximated by

$$R_{S,6} = 1 - [NC_f(1 - R_T) + \frac{N(N-1)}{2}((1 - C_f)(1 - R_T))^2 (1 - (1 - C_f)(1 - R_T))^{N-2}] \quad (6)$$

Substituting C_f with $1 - P_f - S_f - E_f$, we get

$$R_{S,7} = 1 - [NC_f(1 - R_T) + \frac{N(N-1)}{2}((P_f + S_f + E_f)(1 - R_T))^2 (1 - (P_f + S_f + E_f)(1 - R_T))^{N-2}] \quad (7)$$

Finally, we introduce HMS level I effect factor, HMS level II effect factor, engine operation run time factor, and power level de-rating factor into our model. We denote H_{1Cf} as the factor for HMS I effect on catastrophic portion of the failure, and H_{1Pf} as the factor for HMS I effect on preventable portion of the failure, and so on. We denote t_{pct}

as percentage of engine operation run time as certified run duration time and different failure rate adjustment Beta factors β_{cf}, β_{pf}, βs_f, and βe_f, for C_f, P_f, S_f and E_f portions of the failures respectively. We denote D_{Cf}, D_{Pf}, D_{Sf} and D_{Ef} as power level de-rating factors on C_f, P_f, S_f and E_f portions of the failures respectively We introduce all these factors into Eq. (4) that is applicable for without-engine-out design, and on Eq. (7) for with-engine-out design, we get

$$R_{S,8} = 1 - [NC_f H_{1Cf} H_{2Cf} t_{pct}^{B_{cf}} D_{Cf}(1 - R_T) + NP_f H_{1Pf} H_{2Pf} t_{pct}^{B_{pf}} D_{Pf}(1 - R_T)] \tag{8}$$

$$R_{S,9} = 1 - [NC_f H_{1Cf} H_{2Cf} t_{pct}^{B_{cf}} D_{Cf}(1 - R_T) +$$

$$\frac{N(N-1)}{2}((P_f H_{1Pf} H_{2Pf} t_{pct}^{B_{pf}} D_{Pf} + S_f H_{1Sf} H_{2Sf} t_{pct}^{B_{Sf}} D_{Sf} + E_f H_{1Ef} H_{2Ef} t_{pct}^{B_{Ef}} D_{Sf})(1 - R_T))^2 \tag{9}$$
$$(1 - (P_f H_{1Pf} H_{2Pf} t_{pct}^{B_{pf}} D_{Cf} + S_f H_{1Sf} H_{2Sf} t_{pct}^{B_{Sf}} D_{Sf} + E_f H_{1Ef} H_{2Ef} t_{pct}^{B_{Ef}} D_{Ef})(1 - R_T))^{N-2}]$$

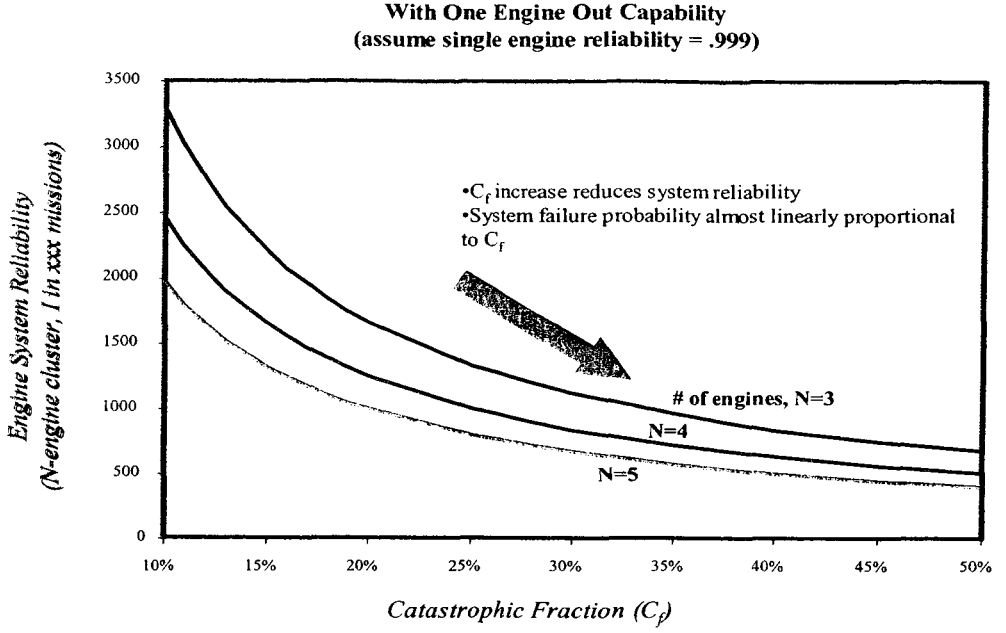
We have derived Eq.(8) and Eq.(9) as closed form formulas. These are approximations in that some higher order reliability effects are ignored, such as the case that more than two engines fail, or dynamic changing of the failure rate when engine out occurs and the rest of the engines have to power up and operate at a thrust level that exhibits a higher failure rate. Ref. 3 has discussed a dynamic changing failure rate model. Our analytical results have indicated Eq. (8) and (9) are good approximations and well suited for reliability trades study and sensitivity analysis of current space launch vehicle conceptual design and system architecture definition. The reliability model we established in this section explicitly and parametrically addresses about half of the more than 20 reliability drivers we discussed in Section II. We will continuously expand the model to include more reliability drivers as application needs arise and relevant data become available.

IV. Reliability Sensitivity Results

In this section, we will present some trades study and sensitivity analysis results for several application cases, using Eq.(8) for calculating reliability of without-engine-out design and Eq. (9) for with-engine-out design.

Case 1. Engine system reliability as function of catastrophic fraction (C_f)
In this case study, we examine the effect of C_f on the engine cluster system reliability with one engine-out design. We assume single engine total reliability R_T = .999, basic redline system, no de-rating and certified duration. So we reduce all H values (HMS effect drivers), D values (de-rating effect) and t_{pct} values (engine run time variation) to 1. Figure 3 shows some sensitivity curves. A result is obvious in that doubling the C_f will reduce the system MTBF by half. This conclusion is pretty generic even input parameter values vary within a reasonable application range.

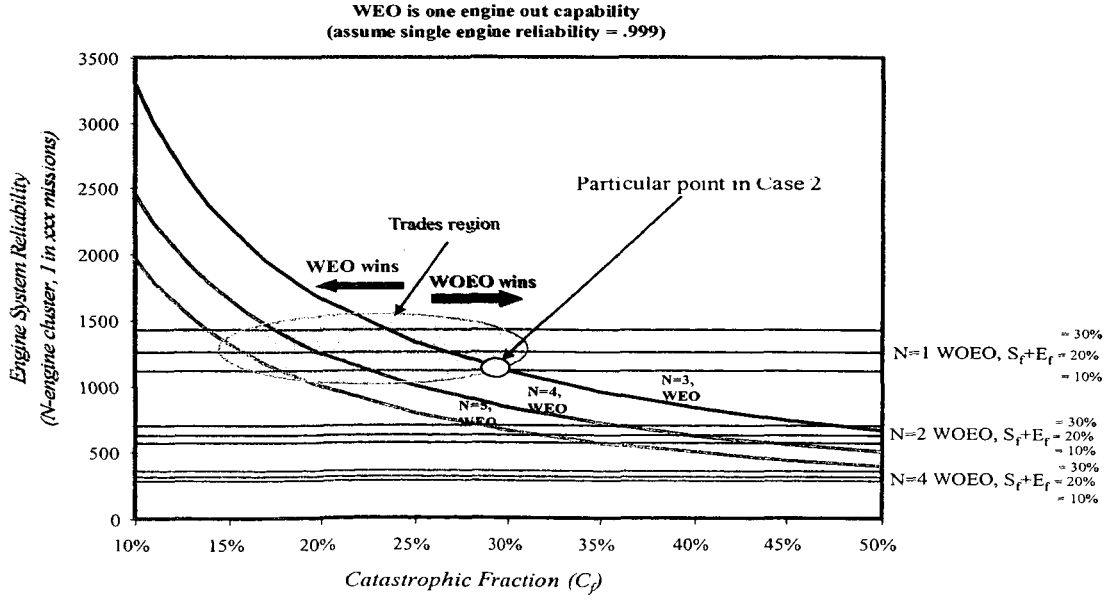
Figure 3. Engine System Reliability as Function of Catastrophic Fraction



Case 2. With-engine-out vs. Without-engine-out trades

In this case study, we examine the reliability sensitivity and trades between with-engine-out (WEO) design and without-engine-out (WOEO) design. We calculate the engine cluster system reliability for N=3, 4, and 5 of WEO and for N=1,2,4 of WOEO. Again, we assume single engine total reliability R_T = .999, basic redline system, no de-rating and certified duration like in Case 1. Figure 4 shows the sensitivity results with many trades facts. If we look at the particular curve on the graph with WEO design and N=3, and compare with the horizontal line with WOEO design and N=1 and S_f+E_f=10%, we see they intersect at about C_f=30%. This indicates as long as $C_f \leq 30\%$, the WEO design will have a better system reliability than the WOEO design. We can construct and interpret other curves from our reliability model for any particular application scenarios similarly.

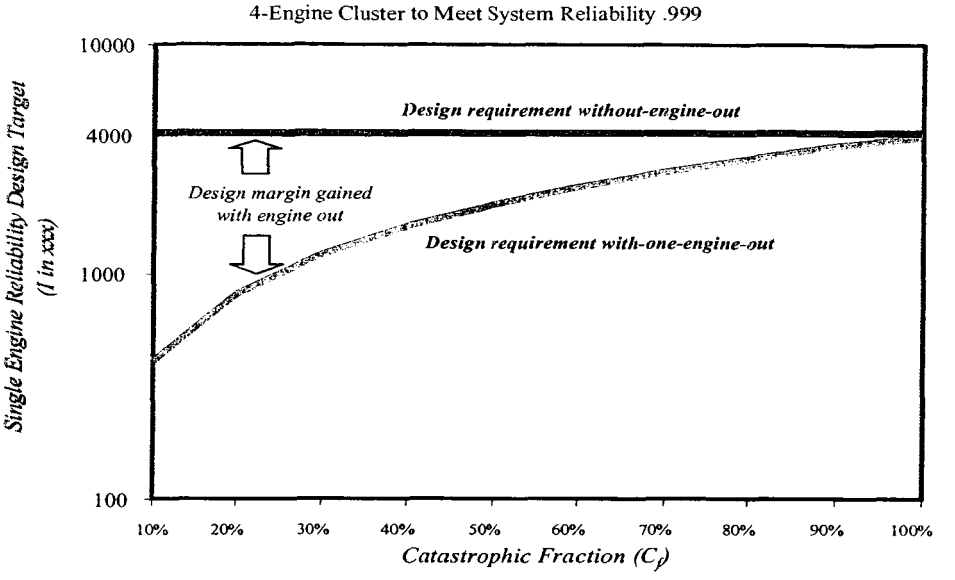
Figure 4. With-Engine-Out (WEO) and Without-Engine-Out (WOEO) Trades



Case 3. Additional design margin gained by WEO design

We continue to pursue the effect of with-engine-out design. This case study presents another view of the benefit of WEO that is an additional design margin gained through engine-out design. Figure 5 illustrates such scenario. This additional reliability margin is precious for it will help to achieve stringent reliability requirements of current space exploration launch vehicles and may possibly expand trades space among reliability and other design parameters for an optimal vehicle design.

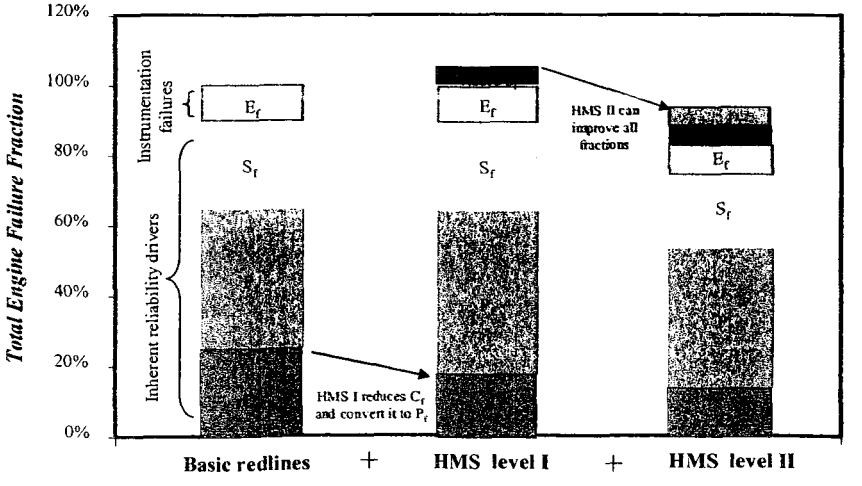
Figure 5. With-Engine-Out Design Provides Additional Design Margin



Case 4. Health Management System (HMS) effect

We have assumed a HMS basic redline system in several case studies discussed above for WEO design. We also discussed HMS implementation levels and their effects on engine reliability in Section II Reliability Drivers. Figure 6 further illustrates the HMS impact on different portions of the reliability. In summary, we can state that basic redline systems and HMS I will mitigate certain catastrophic failures to benign shutdowns but possibly increases the portion of survivable and erroneous shutdown fractions, and HMS II potentially improves all potions of reliability. We now introduce HMS effect on the scenario of Case 3. We assume HMS I mitigates 10% catastrophic failures and convert these failures to benign shutdowns, and does not change survivable and erroneous fractions. We also assume HMS II further reduces the failure probability by 5% across the board. Figure 7 shows the potential additional benefit brought by HMS.

Figure 6. HMS Impact



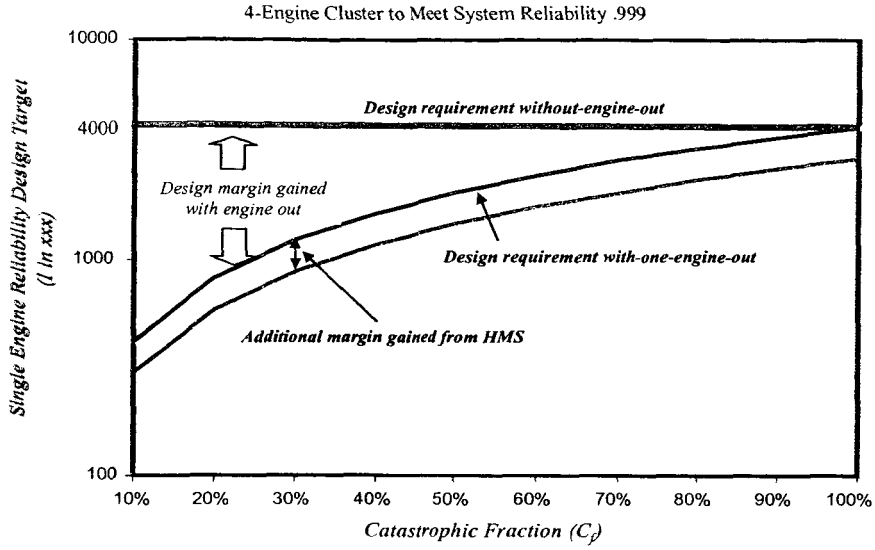
C_f - Catastrophic (uncontained) failure fractions

P_f - Fraction of failures that would have been catastrophic but prevented by HMS

S_f - Fraction of failures that would have survived but was unnecessarily shutdown by HMS

E_f - Fraction of failures that are caused by HMS instrumentation failures (erroneous shutdown)

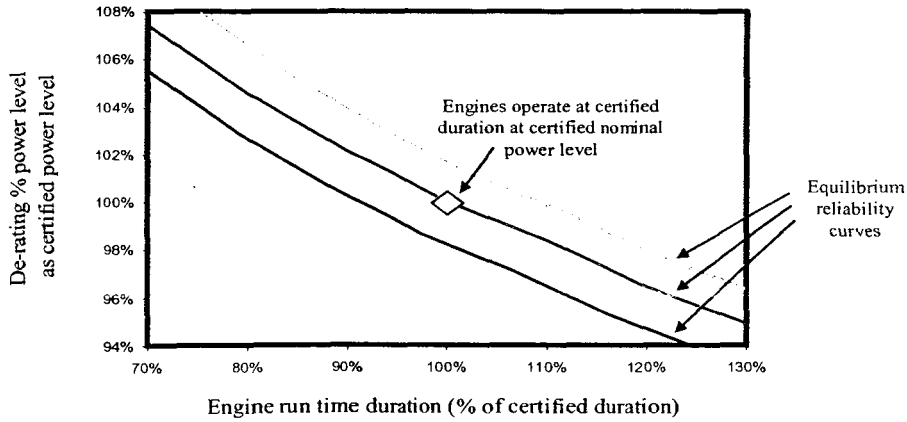
Figure 7. Additional Benefit by HMS



Case 5. De-rating effect and engine run duration adjustment

A with-engine-out design usually is accompanied by the engine power level de-rating. We have briefly discussed the de-rating concept in the Reliability Driver section. In summary, de-rating is not only beneficial to improve reliability but also a necessary design consideration to accommodate engine-out total thrust need. Liquid engine industry has examined de-rating possibility in the past and has derived various de-rating curves. An alternative design solution is to extend the remaining engine operation time at the same power level when one or more engines are out. This relates to the reliability calculation for varied engine running duration applications. We have studied relationship of failure rate vs. engine run time and established some failure rate changing functions for various launch vehicle reliability studies. Here we present an illustrative example that shows the trades between power level de-rating and run time adjustment.

Figure 8. Engine Power Level De-rating and Run time Trades



V. Summary and Conclusion

We have established a comprehensive set of liquid engine reliability drivers and developed a reliability model to address parametrically some of them. We have illustrated some application examples of the model and reliability sensitivities for some of the reliability parameters. The results shown in the examples are pretty generic though the data and scenarios are not specific to any on-going space exploration vehicle studies. We are using the reliability model to support Shuttle Derived Launch Vehicle architecture design and system trades study.

Through the discussion of the reliability drivers and sensitivity analysis examples, we recognized four fractions of engine reliability. Those are catastrophic fraction (C_f), preventable failure fraction (P_f), survivable failure fraction (S_f) and erroneous shutdown fraction (E_f). Every of these fractions has unique root causes and different

consequences on vehicle, and has to be addressed with different design-for-reliability strategy and approaches while attentions have to be paid on interaction, inter-relationships and integration of them. Assisting the system design optimization, we introduced engine out design concept, health management system implementation, de-rating, and engine run time adjustment factor. We incorporate all these parameters into our reliability model and make it a powerful tool to support our nation's new space exploration activities.

References

[1]Lloyd, D.K., and Lipow, M., *Reliability Management, Method, and Mathematics*, 2nd ed., American Society for Quality Control, Milwaukee, Wisconsin, 1989.

[2]Kapur, K.C., and Lamberson, L.R., Reliability In Engineering Design, 1st ed., John Wiley & Sons., New York, New York, 1977.

[3]Huang, Z., Weber-Jr., T., "Liquid Propulsion Launch Vehicle Reliability In Closed Form", Journal of Spacecraft and Rockets, Vol. 36, No. 5, Sep.-Oct. 1999, pp.701-703