JOURNAL OF SPACECRAFT AND ROCKETS
Vol. 36, No. 5, September–October 1999

Liquid Propulsion Launch Vehicle Reliability in Closed Form

Zhaofeng Huang*
The Boeing Company, Canoga Park, California 91309
and
Theodore F. Weber Jr.†
The Boeing Company, Downey, California 90241

The derivations of two closed-form formulas for calculating liquid propulsion launch vehicle system reliability are presented, and the formulas with application examples are illustrated. These formulas overcome the inadequacy of some existing formulas and inefficiency of Monte Carlo simulation and serve as an efficient analytical tool for accurate system reliability evaluation under a given set of input parameter conditions. Therefore, they greatly help system-level trade studies and optimization.

Nomenclature

C_f = catastrophic fraction; portion of a single engine failure probability that will result in catastrophic failure consequence of the vehicle
$F(t)$ = failure decay function, where t is instantaneous time during a mission
N_c = number of clusters (or boosters) to which N_{te} engines are allocated
N_e = number of engines in each cluster, N_{te}/N_c
N_{te} = number of total liquid propulsion engines on vehicle
R_d = reliability of single engine at a powered-up thrust level
R_e = reliability of single engine at nominal thrust level
R_s = vehicle system reliability
T_h = engine hold-down check-up time during engine start phase for engine readiness check, s
T_t = total engine burn time for a mission that includes engine hold-down time T_h, s

Introduction

RELIABILITY is one of several key parameters considered during a propulsion system design and tradeoff study. Accurate and efficient reliability evaluation therefore becomes essentially important. A space launch vehicle is often powered by multiple liquid-propulsion rocket engines. Such a system is usually capable of accommodating engine out capability, which, when one or more of the engines fail during a mission in a self-contained manner, allows the remaining engines to continue operating and to accomplish the mission. There have been some existing techniques and solutions for reliability calculation of such system. However, they are either approximate or too time consuming to obtain an answer.

Problem Background

Simplified Scenario and Analytical Solution

Assume a launch vehicle is powered by three liquid rocket engines. The reliability of single engine at nominal power level, R_e, is 0.999. However, when an engine fails, it can fail in a self-contained manner and shutdown in a benign nature, which we call safe shutdown. It can also fail catastrophically and destroy the vehicle instantly. The portion of catastrophic failures among all engine failures is the catastrophic fraction C_f. For example, a C_f of 10% of single-engine reliability 0.999 represents a probability of catastrophic failures of $(1 - 0.999) \times 10\% = 0.0001$. Correspondingly, the probability of engine safe shutdown is calculated to be $(1 - 0.999) \times 90\% = 0.0009$. The vehicle propulsion system is designed to accommodate one engine out capability, which means when one of the three engines experiences safe shutdown, the remaining two engines will continue to operate to accomplish the mission. Therefore, this three-engine system reliability R_s is defined as the probability that none of these three engines fails catastrophically and no more than one engine requires safe shutdown during the mission. Given the single-engine reliability $R_e = 0.999$ and catastrophic fraction $C_f = 10\%$, we conventionally use the following formula to calculate R_s:

$$R_s = R_e^3 + 3(1 - R_e)(1 - C_f)[1 - (1 - R_e)C_f]R_e^2$$

This formula is derived using binomial theory.[1] The first term is simply the probability of three successes out of three trials. The portion $(1 - R_e)(1 - C_f)[1 - (1 - R_e)C_f]$ in the second term is the probability that an engine experiences safe shutdown but not catastrophic failure. Therefore the second term represents the probability that any one of the three engines safely shuts down but does not suffer catastrophic failure and the other two engines operate successfully without either catastrophic failure or safe shutdown. The general form of the formula, derived according to the binomial theory, is given by the following equation for an N_{te}-engine system with one engine out capability:

$$R_s = R_e^{N_{te}} + N_{te}(1 - R_e)(1 - C_f)[1 - (1 - R_e)C_f]R_e^{N_{te}-1} \quad (1)$$

Some issues are associated with this formula. First, when one of the three engines safely shuts down, that engine is no longer capable of experiencing any catastrophic failure or safe shutdown afterward. Therefore, this formula may underestimate the system reliability. Second, the single-engine reliability R_e is usually not constant as is assumed in the formula. During a mission, when one engine shuts down, the other two engines have to be powered up to generate a thrust equivalent to the three-engine system during the remaining mission period. The increased power level usually increases stress level, therefore degrading single-engine reliability from R_e to R_d ($R_d < R_e$). Considering all of these facts and scenarios, the system reliability calculation becomes more complicated than what Eq. (1) can handle. Some shared-load, time-dependent reliability model described in Ref. 2 needs to be developed to solve our problem.

Computer Simulation as a Solution

Monte Carlo computer simulation provides a powerful tool for this kind of analysis. The basic idea of the simulation is to discretize the mission duration to small time intervals, such as 5 s. Then one can allocate the given single-engine failure probability to each 5-s time interval. The computer simulation then checks the failure condition of each engine during that time. If any engine experiences a catastrophic failure, the mission fails. If any one of the engines safely shuts down at a certain time during the mission, the remaining engines are powered up with a degraded reliability. Simulation

Received 3 September 1998; revision received 17 November 1998; accepted for publication 17 November 1998.

*Reliability and Statistical Specialist, Rocketdyne Propulsion and Power, Mail Stop AC73, 6633 Canoga Avenue. Member AIAA.

†Associate Technical Fellow, Reusable Space Systems, P.O. Box 7009.

continues to check the engine condition and mission failure encounters if the second engine requires shutdown or any remaining engines fail catastrophically. Although we often enjoy the powerfulness and straightforwardness of Monte Carlo simulation, we realize that it has some limitations, such as difficulty of rare-event simulation, significant computer run time, and random number inaccuracy. Some closed-form formulas are presented as an alternative.

Main Result: Closed-Form Formulas as Solution

Assume that the vehicle system is powered by N_{te} liquid rocket engines. These N_{te} engines are physically allocated to N_c clusters (or boosters). Depending on the vehicle operating requirement and other tradeoff considerations, the following two vehicle engine out capability scenarios are defined:

1) The vehicle system allows one engine to safely shut down during main stage from each N_c cluster, allowing a total N_c engines out. Therefore, this scenario defines a vehicle catastrophic failure as the event that any of N_{te} engines experiences a catastrophic failure or more than one engine from the same cluster requires safe shut down during main stage.

2) The entire vehicle system allows only one engine to safely shut down during main stage among all N_{te} engines. Therefore, this scenario defines a vehicle catastrophic failure as the event that any of N_{te} engines experiences a catastrophic failure or more than one engine among all N_{te} engines requires safe shutdown during main stage.

The following are the two theorems presented for system reliability calculation for the preceding two scenarios, respectively. In both cases, the system reliability R_s is defined as 1 minus the probability that a vehicle catastrophic failure occurs. The function $F(t)$ is an accommodation because the failure rate during a mission may not be constant. For example, an engine may be more likely to fail during the first 10 s of a mission than the last 10 s. We normalize the engine failure probability of a mission to 1. Therefore, $F(t)$ satisfies $F(0) = 0$ (the engine has not started, thus no chance to fail) and $F(T_t) = 1$ (the engine consumes all predefined failure probability during a mission).

Theorem 1: Assume that a launch vehicle allows one engine to safely shut down during main stage for each cluster (scenario 1). For given N_{te}, N_c, N_e, R_e, R_d, C_f, T_h, T_t, and $F(t)$, the vehicle system reliability R_s is computed by

$$R_s = R_1^{N_c}(R_2 + R_3)^{N_c} \tag{2}$$

where R_1 is the probability that all engines in one cluster experience no catastrophic failure during engine hold-down, check-up period:

$$R_1 = [1 - (1 - R_e)C_f F(T_h)]^{N_e} \tag{3}$$

R_2 is the probability that all engines in one cluster operate successfully during main stage without either catastrophic failure or safe shutdown:

$$R_2 = [1 - (1 - R_e)(F(T_t) - F(T_h))]^{N_e} \tag{4}$$

and R_3 is the probability that only one engine safely shuts down during main stage and the rest of the $N_e - 1$ engines in the same cluster operate successfully without either catastrophic failure or safe shutdown:

$$\begin{aligned} R_3 = {} & N_e(1 - C_f)c^{N_e+1}c_1^{N_e-1} \\ & \times \left[\mathrm{Beta}(N_e+1, N_e)\left\{\mathrm{Beta}\left(N_e+1, N_e, \frac{1}{c}\right)\right.\right. \\ & \left.\left. - \mathrm{Beta}\left(N_e+1, N_e, \frac{1-(1-R_e)(1-F(T_h))}{c}\right)\right\}\right] \end{aligned} \tag{5}$$

where

$$c_1 = R_d + \frac{1 - R_d}{1 - R_e} + (1 - R_d)F(T_h)$$

$$c = c_1\frac{1 - R_e}{1 - R_d}$$

The beta function value is

$$\mathrm{Beta}(A, B) = \int_0^1 t^{A-1}(1-t)^{B-1}\,\mathrm{d}t$$

The incomplete beta function value is

$$\mathrm{Beta}(A, B, x) = \frac{\int_0^x t^{A-1}(1-t)^{B-1}\,\mathrm{d}t}{\int_0^1 t^{A-1}(1-t)^{B-1}\,\mathrm{d}t}$$

Theorem 2: Assume that a launch vehicle allows one engine to safely shut down during main stage for the entire vehicle (scenario 2). For given N_{te}, N_c, N_e, R_e, R_d, C_f, T_h, T_t, and $F(t)$, the vehicle system reliability R_s is

$$R_s = R_1^{N_c}\left(R_2^{N_c} + N_c R_2^{N_c-1}R_3\right) \tag{6}$$

Here R_1, R_2, and R_3 are defined and computed as in Theorem 1.

A computer program has been written to calculate R_s for both scenarios 1 and 2.

Illustrative Examples

Example 1: Assume that a launch vehicle requires eight liquid propulsion engines, $N_{te} = 8$. These eight engines are allocated to two boosters, $N_c = 2$ and $N_e = 4$. The mission duration is 160 s, $T_t = 160$, and the engine start hold-down, check-up period is 6 s, $T_h = 6$. The engine reliability is predetermined to be 0.999 at nominal power level, $R_e = 0.999$, and degraded to 0.99 when powered up to accommodate engine out condition, $R_d = 0.99$. The catastrophic fraction of the engine reliability is 10%, $C_f = 0.10$. Failure decay function is represented by $F(t) = (t/160)^{1/2}$. We are calculating the system reliability R_s for scenario 1, which allows one engine to safely shut down during main stage for each of the two boosters (two engine out condition). Equation (2) gives $R_s = 0.9991289$.

Example 2: The same data used in example 1 apply to scenario 2. Now only one engine to safely shut down is allowed for the entire vehicle consisting of the two boosters. Equation (6) gives $R_s = 0.9991207$, which is slightly lower than the answer for example 1.

Example 3: This example presents a sensitivity result of our newly derived formula, contrasted with the result of Eq. (1), which is based on the assumption of constant reliability. Assume that a launch vehicle requires eight liquid propulsion engines, $N_{te} = 8$. These eight engines are allocated to two boosters, $N_c = 2$ and $N_e = 4$. The mission duration is 160 s, $T_t = 160$, without engine hold-down, check-up period, $T_h = 0$. The catastrophic fraction of the engine reliability is 10%, $C_f = 0.10$. Failure decay function is given by $F(t) = (t/160)^{1/2}$. The vehicle engine out scenario is to allow only one engine to safely shut down during main stage (scenario 2). Nominal power-level reliability R_e is 0.999. First, let us assume reliability is constant without degradation at a higher power level. Equation (1) gives $R_s = 0.999177$, or mean missions between failures is equal to $1/(1 - 0.999177) = 1215$. Now we let the higher power-level reliability R_d vary from 0.999 to 0.90 and use our newly derived Eq. (6) to compute R_s according to the value of R_d. Figure 1 plots R_s in

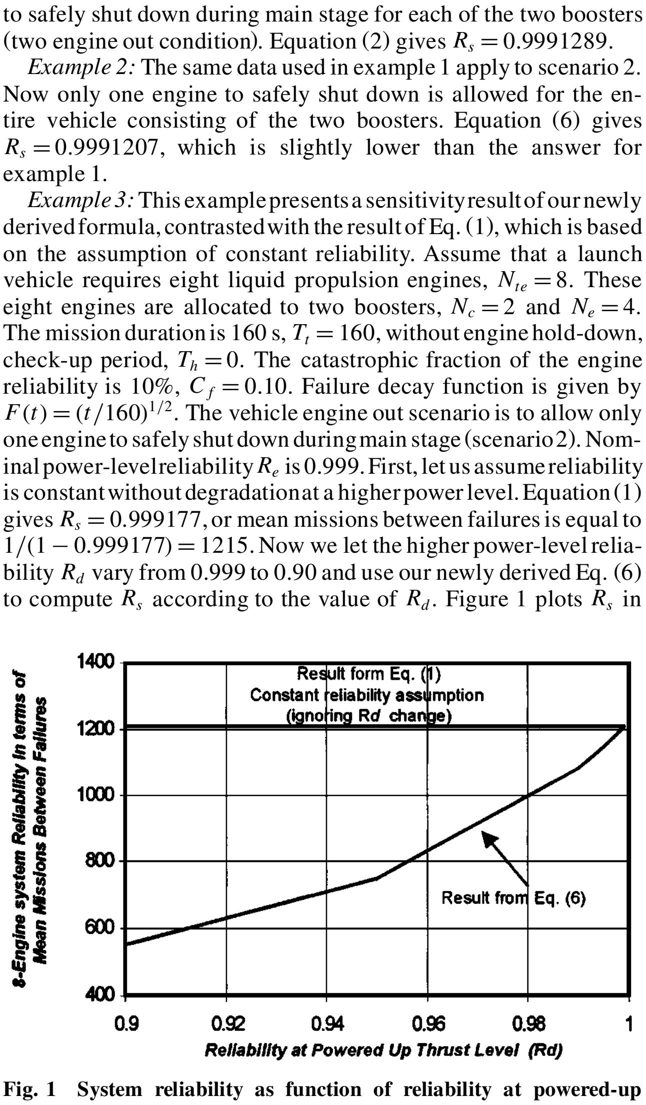

Fig. 1 System reliability as function of reliability at powered-up thrust level.

terms of mean missions between failures against R_d. It shows that the system reliability R_s is quite sensitive to the degradation of R_d, but Eq. (1) does not enable us to capture that.

Conclusion

Two closed-form formulas for calculating liquid propulsion launch vehicle system reliability were presented, and some application examples were illustrated. The result indicates that these formulas are very efficient and can be used as a powerful tool to assist a liquid propulsion launch vehicle system tradeoff study.

Appendix: Proofs of Theorems

Proof of Theorem 1

R_1 is defined as the probability that all engines in one cluster operate successfully without catastrophic failure during the engine hold-down, check-up period. If any engine safely shuts down because of some anomaly during that period, the mission will stop without catastrophic consequence. Therefore, we are concerned only with catastrophic failure during that period. The catastrophic failure probability for a single engine during that period is $(1 - R_e)$ $C_f F(T_h)$. Thus, the probability that all N_e engines operate successfully without catastrophic failure is $[1 - (1 - R_e)C_f F(T_h)]^{N_e}$. R_2 is defined as the probability that all engines in one cluster operate successfully without either catastrophic failure or safe shutdown during main stage. Single-engine failure probability during main stage is computed by $(1 - R_e)(F(T_t) - F(T_h))$. Therefore, we obtain $[1 - (1 - R_e)(F(T_t) - F(T_h))]^{N_e}$ as the probability that all engines in the same cluster operate successfully without either catastrophic failure or safe shutdown during main stage. Proof of R_3 is lengthy. R_3 is defined as the probability that only one engine safely shuts down during main stage and the rest of the $N_e - 1$ engines in the same cluster operate successfully without either catastrophic failure or safe shutdown. Because after one of the N_e engines in the cluster safely shuts down, that engine will not experience any catastrophic failure or safe shutdown afterward during the mission. However, the rest of the $N_e - 1$ engines have to be powered up to produce equivalent total thrust to accomplish the mission. The reliability of a powered-up engine is degraded to R_d, which is generally less than R_e, because of increased stress level. Let us study the scenario of only one engine safely shutting down among all N_e engines in the same cluster during the main stage time period from T_h to T_t. Assume that the engine shuts down at time t within (T_h, T_t). That engine must survive the time period from T_h to t along with the rest of the engines in that cluster. Therefore, we have P_{31} as the probability (all engines operate successfully up to time t, and one of the N_e engines safely shuts down at time t)

$$P_{31} = N_e[1 - (1 - R_e)(F(t) - F(T_h))]^{N_e} \times [(1 - R_e)(1 - C_f)]\,\mathrm{d}F(t) \tag{A1}$$

After one of the N_e engines safely shuts down, the other $N_e - 1$ engines are powered up, and the failure probability for the single engine during the remaining period from t to T_t is $(1 - R_d)(F(T_t) - F(t))$. Therefore, we have P_{32} as the probability (the rest of the $N_e - 1$ engines operate successfully during the remaining time)

$$P_{32} = [1 - (1 - R_d)(F(T_t) - F(t))]^{Ne-1} \equiv [1 - (1 - R_d)(1 - F(t))]^{N_e - 1} \tag{A2}$$

Note that $F(T_t) = 1$ by definition.

Now the probability that only one engine safely shuts down during main stage and the rest of the $N_e - 1$ engines in the same cluster operate successfully without either catastrophic failure or safe shutdown can be summed up using an integral. Therefore, we have

$$R_3 = \int_{T_h}^{T_t} P_{31}P_{32} = \int_{T_h}^{T_t} N_e[1 - (1 - R_e)(F(t) - F(T_h))]^{N_e} \times [1 - (1 - R_d)(1 - F(t))]^{N_e - 1}(1 - R_e)(1 - C_f)\,\mathrm{d}F(t)$$

Through a series of lengthy substitution, simplification, and manipulation of equations, we proved Eq. (5). Now the probability that no more than one engine safely shuts down during main stage and no catastrophic failure occurs for all N_e engines in the same cluster during the entire mission is given by $R_1(R_2 + R_3)$. Therefore, for scenario 1, which allows one engine to safely shut down during main stage in each of N_c clusters, the vehicle system reliability is

$$R_s = R_1^{N_c}(R_2 + R_3)^{N_c}$$

Proof of Theorem 2

R_1, R_2, and R_3 are all defined and calculated the same as in Theorem 1. However, in this theorem, we have the scenario that the entire vehicle only allows one engine to safely shut down during main stage. During the engine-start, hold-down, check-up period, the system still cannot allow any catastrophic failures. Therefore, we have $R_s =$ probability (no catastrophic failure occurs for all N_{te} engines during hold down period) × [probability (all engines operate successfully during main stage) + probability (only one cluster requires one engine to safely shut down and other $N_c - 1$ clusters operate successfully without either catastrophic failure or safe shut down during main stage)]:

$$R_s = R_1^{N_c}\left(R_2^{N_c} + N_c R_2^{N_c - 1} R_3\right)$$

References

[1] Lloyd, D. K., and Lipow, M., *Reliability: Management, Methods, and Mathematics*, 2nd ed., American Society for Quality Control, Milwaukee, WI, 1989, pp. 113–115.

[2] Kapur, K. C., and Lamberson, L. R., *Reliability in Engineering Design*, 1st ed., Wiley, New York, 1977, pp. 222–224.

J. A. Martin
Associate Editor