NASA
Technical
Paper
2759

August 1987

Probabilistic Risk Analysis of Flying the Space Shuttle With and Without Fuel Turbine Discharge Temperature Redline Protection

Leonard Howell

NASA
Technical
Paper
2759

1987

Probabilistic Risk Analysis of Flying the Space Shuttle With and Without Fuel Turbine Discharge Temperature Redline Protection

Leonard Howell

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama

National Aeronautics
and Space Administration

Scientific and Technical
Information Office

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

TECHNICAL PAPER

PROBABILISTIC RISK ANALYSIS OF FLYING THE SPACE SHUTTLE WITH AND WITHOUT FUEL TURBINE DISCHARGE TEMPERATURE REDLINE PROTECTION

I. INTRODUCTION

Operation of the Space Shuttle Main Engine (SSME) in the presence of possible turbine overtemperature events and temperature sensor failures entails a measurable risk. Turbine discharge temperature sensors are employed in detecting turbine overtemperatures in the SSME. These sensors have a history of unreliability during both ground test and flight. Moreover, there have been several overtemperature events in the SSME during ground tests which are believed to have the potential to occur during launch.

Therefore, in order to make informed design and flight policy decisions concerning overtemperatures, it is important to calculate both the risk of an erroneous engine shutdown and the risk of an undetected overtemperature event as a result of sensor failures or redline protection inhibit.

This paper presents the results of a reliability study of these risks and the mathematical model that was developed to compute the desired probabilities.

A Monte Carlo computer simulation was programmed as a check on the analytical model and is also included.

II. BACKGROUND

The SSME provides measurements of turbine discharge temperatures in both the High Pressure Fuel Turbine (HPFT) and the High Pressure Oxidizer Turbine (HPOT). Two sensors (Fig. 1) in each turbine are utilized within the SSME control and monitoring system by logic to shut down the engine when the measured temperature rises above a pre-set level during launch, or does not reach a pre-set level during start. The temperature must remain in this critical region for at least 40 msec in order to trip the engine protection shutdown logic which is an event referred to as "voting to cut." This protection logic, known as redline(s), has been instrumental in protecting the SSME during its test history.

Because the failure data indicate that the hazard of sensor failures and overtemperature events in the HPFT greatly overshadows the hazard of sensor failures and overtemperature events in the HPOT, this study is restricted to the fuel turbine.

Germane to this analysis is the time required by the computer to classify a failing sensor as either being good or bad. A failing sensor whose reading is recognized as being impossible (greater than 2900 deg

Rankine) is immediately recognized as being bad by the computer and is "disqualified," a state in which it is henceforth ignored by the computer. It is noted that if both sensors are disqualified, a condition exists where the engine will continue to fire but there will be no means to detect an overtemperature event.

A failing sensor can also read an erroneous temperature which drifts into the redline region for longer than 40 msec and, thus, trips the redline logic which produces a vote to cut. During this time, this sensor is still classified as good and its reading is thus falsely interpreted as warning of an overtemperature event and, if the other sensor has already been disqualified, would result in an erroneous engine shutdown. These two sensor failure states, referred to as disqualification and vote to cut, are illustrated in Figure 2.

In the sensor Model 71 data base, 26 sensors experienced failures, 22 of which were immediately disqualified and 4 voted to cut. The 4 that voted to cut each falsely measured a temperature in the redline region long enough to cause a vote to cut. Each of these sensors' temperature reading then jumped past 2900 deg Rankine and were then disqualified.

During flight, a premature engine shutdown can cause a mission abort which is considered an unsafe condition. On the other hand, launch without protection against a turbine overtemperature event, which is symptomatic of impending catastrophe, provides no means to thwart failure. Therefore, it is imperative that these two risks be analyzed to determine whether or not they are acceptable.

III. METHODS

Estimation of these risks requires the consideration of the reliability of the temperature sensors, the reliability of the HPFT relative to overheating, and of the computer's voting logic in the presence of all possible failure scenarios of the sensors and the fuel turbine. Because the computer's voting logic considers the sequence in which failures occur, the analysis must include the chronological variable time as well.

The analysis will first develop the necessary reliability model for a single engine with two temperature sensors in the HPFT. This result will then be used to compute the reliability of the Space Shuttle's three engine configuration. Also, these risks will be computed using the Model 71 sensor and the Model 81 sensor. This will show the improvement in overall reliability as a result of replacing the Model 71 sensor by the Model 81.

Using the symbol (|) to represent the event that a sensor is disqualified, a (/) to denote the event of an erroneous vote to cut, and H to represent a fuel turbine overtemperature event, it can be seen that there are a total of 12 possible system states. These 12 cases are depicted in column 11 of Table 1; the horizontal axis denotes time in the units second and ranges from 0 to 520 sec and corresponds to the duration of a typical launch firing. Column 2 of the table gives an explanation of the state and column 3 gives the computer's decision for that state. This decision is either continue to fire (CTF) or shut down (SD). Column 4 contains comments relevant to this study, e.g., erroneous engine shutdown. Note that state S1 represents the nominal case in which no sensors fail and the fuel turbine temperature does not exceed the redline. States S6 and S9 result in erroneous engine shutdown, and states S11 and S12 result in not shutting down an engine that should be shut down.

IV. MATHEMATICAL MODEL

A. Statistical Assumptions

When constructing a model which describes the computer voting logic in the presence of sensor failures and fuel turbine overtemperature events, a level of fidelity is required which accurately models the important aspects under investigation. These include realistic probability distributions for sensor failures and overtemperature events and the computer reaction to chronologically ordered combinations of these failures in terms of continuing to fire the engine or to shut it down. This is the most important step in the modeling process and anything which falls short of this goal will be of questionable value.

It is believed that the pictorial model in Table 1 does indeed fulfill this requirement because it exactly parallels the computer voting logic in the presence of all possible combinations of sensor failures and overtemperature events. The following necessary assumptions are made about the probabilities associated with these failures which will then permit one to derive a set of equations that mathematically models the 12 states depicted in Table 1.

1) For the sensors' two failure states (disqualify and vote to cut), the probability that a particular sensor is disqualified or erroneously votes to cut in time Δt is $\lambda_1 \Delta t$ and $\lambda_2 \Delta t$, respectively, where the λ's have the dimension of failures per unit time. Specifically, the exponential time to failure model will be used which implies constant failure rates λ_1 and λ_2, i.e., no infant mortality or wearout effect. The Mean Time Between Failures (MTBF) is then given by $1/\lambda$.

2) Sensor failures and overtemperature events are statistically independent. That is, the failure of a sensor does not alter the probability that the remaining sensor fails nor does it alter the probability of a fuel turbine overtemperature event.

3) The time to failure probability distribution for a HPFT overtemperature event follows a Weibull distribution. The choice of this two-parameter distribution provides the flexibility to model the possibility that the hazard of an overtemperature is not necessarily constant, e.g., an overtemperature event might be more likely to occur at the beginning of a mission rather than the end, or vice versa. However, as shall be seen later, the risks of interest are virtually insensitive to the Weibull assumption when compared with the simpler exponential time to failure model (constant hazard).

4) A sensor that fails does not later recover and become operational again.

B. Model Construction

The "stick" figures in Table 1 which describe the 12 possible system states must now be mathematically modeled. Based on the assumptions discussed in the previous section, familiar techniques used in the study of stochastic processes are applied. The method to be employed here is referred to as the

Compound-Event Approach [1] which leads directly to multiple integral expressions for the state probabilities in terms of the system hazards. For the particular state (S12), the probability that a failing sensor votes to cut is derived, the other sensor is later disqualified, and then sometime later, there is a fuel turbine overtemperature event. This then represents one of the two state probabilities that contribute to the probability of an overtemperature event going undetected (the other state is S11).

Assume that the first event (erroneous vote to cut) occurs at some arbitrary time $t = x_1$, the remaining sensor is disqualified at time $t = x_2$, and then there is an overtemperature event at time $t = x_3$, where $x_1 < x_2 < x_3 \leq 520$ sec. This is most easily visualized by reference to Figure 3a. Construction of P12(T) is formalized in Figure 3b and the solution, obtained by first integrating with respect to x_1, then x_2, followed by an integration by parts with respect to the variable x_3 so as to remove the numerical difficulty involved when $\beta < 1$, is given in Table 2.

In a similar fashion, the other 11 state probabilities can be derived and are given in Table 2. Thus, although formulation is straightforward, computation is somewhat tedious. When the appropriate estimates of the parameters are inserted into these equations, the desired probabilities may then be computed.

C. Estimation of Parameters

Using the life data presented in References 2 and 3, the two sensor parameters and the two engine parameters which appear in the model can be estimated.

The failure rate parameter for HPFT sensor disqualification is given by the number of disqualifications that have occurred in the HPFT divided by the cumulative time on both failed and unfailed HPFT sensors.

Because the HPFT environment is believed to be significantly harsher than the HPOT environment on the sensors, only life data obtained from sensors used in the HPFT may be used to estimate these parameters. Hence, sensor failures and success time obtained from the HPOT side of the engine may not be used to estimate the failure rates for sensors which are located in the HPFT. The HPOT sensor life data may only be used to estimate the failure rates for sensors which are located in the HPOT. In this study it has been assumed that the HPOT is 100 percent reliable so that all life data from the HPOT (both sensor and overtemperature data) is not used to estimate any model parameters.

Similarly, the vote to cut failure rate is estimated by the number of erroneous votes to cut originated by failing sensors in the HPFT divided by the cumulative time on both failed and unfailed HPFT sensors. For the Model 71 sensor, $\lambda_1 = 22/265{,}256.5$ sec and $\lambda_2 = 4/264{,}256.5$ sec. For the Model 81 sensor, the failure rates are estimated to be $\lambda_1 = 2/64{,}342$ sec and $\lambda_2 = 5.65E\text{-}6$. Because there have been no erroneous votes to cut with the Model 81 sensor, the assumption is made that the ratio of votes to cut to disqualifications has remained constant in the two sensor models.

The two parameters of the Weibull distribution that were used as the time to failure model for turbine overtemperature events are estimated by the method of maximum likelihood. The estimates of these parameters, which are called a and b, are determined from the numerical solution of the two simultaneous equations in terms of a and b:

$$a - R \,/\, \left(\sum_{i=1}^{R} t_i^{\,b} + \sum_{j=1}^{S} t_j^{\,b} \right) = 0 \tag{1}$$

and

$$\frac{R}{b} + \sum_{i=1}^{R} \ln t_i - \frac{R \left(\sum_{i=1}^{R} t_i^{\,b} \ln t_i + \sum_{j=1}^{S} t_i^{\,b} \ln t_j \right)}{\sum_{i=1}^{R} t_i^{\,b} + \sum_{j=1}^{S} t_i^{\,b}} = 0 \tag{2}$$

Reference 3 provides relevant engine data spanning a period from 1980 through January 27, 1986. This data presents 682 successful engine firings with 199,654.95 sec of cumulative firing time. Figure 4 is a histogram of the duration times of the successful tests. Thus, almost 30 percent of the firings lasted about 520 sec which is largely due to the inclusion of flight data. The data further includes 28 overtemperature events, six of which are believed to have the potential to occur during flight. The others either occurred during ground test screening or a design modification was made that would eliminate recurrence [3]. Five of the six overtemperatures occurred in the HPFT. Thus, $R = 5$, $S = 682$, and t_i is the time of the ith HPFT overtemperature occurrence, $i = 1,2,\ldots,R$. Similarly, t_j is the duration of the jth engine firing that did not experience an overtemperature event, $j = 1,2,\ldots,S$. Solving the two equations in terms of a and b yield the estimates $a = 3.25\text{E-}4$ and $b = 0.566$.

Thus, the probability of no HPFT overtemperature event in a 520 sec single engine firing is 0.989 and the probability of no overtemperature event during flight (three engines) is 0.967. Note that the data set shows about 0.7 percent failures (5 overtemperatures out of 687 firings) whereas the Weibull reliability model predicts 1.1 percent. The difference can be explained by observing that 67 percent of the data was for firings of duration much less than 500 sec, meaning that one would have expected more failures in the data set had every test lasted for 520 sec. It should also be noted that assuming an exponential time to failure model for HPFT overtemperature events, the estimated reliability of a single engine firing for 520 sec would be 0.987.

D. Monte Carlo Simulation

A computer program was written which simulates the possibility of sensor failures, a HPFT overtemperature event, and the computer decision based on the programmed voting logic. The simulation is for a $T = 520$ sec period and thus represents a typical engine firing during a Space Shuttle launch.

For each simulated flight, sensor failures and a HPFT overtemperature event are simulated according to the specified probability distributions. The time ordered sequence of failures are then examined to determine which one of the twelve states has occurred. The relative frequency of occurrence of each of the states, obtained from performing the simulated launch many times, will then provide an estimate of each of the 12 state probabilities. If N launches are simulated with n_i occurrences of state i, i = 1,2,...,12, then an approximate (1-a) percent confidence interval for the true state probability p_i is defined by the probability

$$P[\hat{p}_i - Z_{a/2}\sqrt{\hat{p}_i(1-\hat{p}_i)/N} < p_i < \hat{p}_i + Z_{a/2}\sqrt{\hat{p}_i(1-\hat{p}_i)/N}\,] = 1\text{-}a$$

where $\hat{p}_i = n_i/N$ and $Z_{a/2}$ is the critical value of a Gaussian distribution.

In order to simulate possible sensor failures and HPFT overtemperature events, one must first generate two failure times as $t_{A,1} = -(\ln U_1)/\lambda_1$ and $t_{A,2} = -(\ln U_2)/\lambda_2$ where U_1 and U_2 and all subsequent U's are random numbers uniformly distributed between zero and one and the subscript A is used to denote one of the two sensors. Thus $t_{A,1}$ represents the time of disqualification and $t_{A,2}$ the time of erroneous vote to cut for sensor A. Of course, since a failed sensor does not recover, only the earliest time makes physical sense.

Hence, $t_{A,i} = \min(t_{A,1}, t_{A,2})$ is defined so that i = 1 if $t_{A,1} < t_{A,2}$ and thus yields a simulated disqualification. If $t_{A,2} < t_{A,1}$ then i = 2 and a vote to cut is given. It is further noted that if the failure time is greater than T, then sensor A does not fail at all, which is usually the case when the sensor failure rates are small.

In a similar manner, the failure times are generated for the other sensor, labeled B, as $t_{B,1} = -(\ln U_3)/\lambda_1$ and $t_{B,2} = -(\ln U_4)/\lambda_2$, and $t_{B,j} = \min(t_{B,1}, t_{B,2})$ is defined where j = 1 or 2 depending on similar conditions as for sensor A.

The time of turbine overtemperature is simulated according to the Weibull distribution and is given by

$$t_H = [-(\ln U_5)/a]^{1/b} \quad ,$$

where the subscript H is used to denote "Hot."

For each simulated flight, the sensor failure times and the time of HPFT overtemperature event are generated and then checked to see if any failures have occurred during the 520 sec time period. If not, state S1 (the all good state) is recognized as having occurred and the simulation is repeated. If one or more failures have occurred, the time ordered sequence of failures is examined to determine which one of the remaining eleven states has occurred. Table 3 shows the twelve states and their defining characteristics in terms of sensor and HPFT failure states, relative time of failure, and the computer voting logic that results in an engine shutdown or continue to fire command. Based on this table, it can be determined which of the states has occurred. This process is performed N times and the frequency of occurrences of each state is maintained from which the true state probabilities can be approximated.

EXAMPLE: Suppose that $t_{A,1}$ = 15 sec, $t_{A,2}$ = 320 sec, $t_{B,1}$ = 1500 sec, $t_{B,2}$ = 776 sec, and t_H = 420 sec. Then one has the situation where one sensor was disqualified, followed by a HPFT overtemperature event and the simulated state S7 is recognized as having occurred. If t_H had been greater than 520 sec, then it is noted that state S2 would have occurred.

E. Numerical Results

The 12 state probabilities are obtained by evaluating the equations in Table 2 using the four estimated parameters and setting the time variable to 520 sec. The integrals in these equations are evaluated numerically. These equations will be evaluated twice; once using the Model 71 sensor failure rates and once using the Model 81 sensor failure rates. The same estimates for the two Weibull parameters used for the time to HPFT overtemperature model will be used in each case. A comparison of these results will show what improvement in reliability has been achieved when changing from the Model 71 sensor to the Model 81 sensor.

First, using the Model 71 parameters, one obtains

P1 = 0.8927, P2 = 0.0793, P3 = 0.01442, P4 = 0.01075,

P5 = 0.001761, P6 = 3.21E-4, P7 = 3.322E-4, P8 = 3.202E-4,

P9 = 5.837E-6, P10 = 6.039E-5, P11 = 4.427E-6, P12 = 8.05E-7,

and it is noted that P1 + P2 +...+ P12 = 1 as required. The probabilities of interest are determined by:

A. The probability of erroneous engine shutdown is given by P6 + P9

B. The probability of not detecting a HPFT overtemperature event is given by P11 + P12

These results are tabulated below for the Model 71 and Model 81 sensors. The results are given for a single engine firing for 520 sec and three engines firing for 520 sec each. A number which is frequently of interest is N, where N is the solution to the equation $0.99 = (1\text{-}p)^N$ and is interpreted as the number of continuous successes in a row (p is the probability of a failure) for which the probability of this sequence of successes is 0.99. For example, the probability is 0.99 that 61 launches will occur without a single erroneous engine shutdown using the Model 81 sensor.

Probability

	Single Engine (520 sec)		Three Engines		N	
	A	B	A	B	A	B
Model 71	0.0003794	5.232E-6	0.001138	0.0000157	9	640
Model 81	0.0000546	7.463E-7	0.0001638	0.000002239	61	4489

Also of interest relative to engine testing are the following two conditional probabilities:

A. The probability that an overtemperature event occurred, given that the engine was shut down is (P4 + P7 + P10)/(P4 + P6 + P7 + P9 + P10).

B. The probability that an overtemperature event has not occurred, given that the engine was shutdown, is given by (P6 + P9)/(P4 + P6 + P7 + P9 + P10).

These results for the two sensor models are:

	Probability	
	A	B
Model 71	0.9671	0.03293
Model 81	0.9951	0.004874

The parameters for HPFT overtemperature events and the Model 71 sensor failure rate estimates were used in the Monte Carlo simulation and 60 million (N = 6E7) 520 sec single engine firings were simulated which is equivalent to 20 million Shuttle flights. The estimates of the twelve state probabilities and 95 percent confidence intervals are given below. The column labeled by P, which are the exact probabilities obtained from the analytical model, are the numbers that compare the estimates $\hat{p}$. Also note that the confidence intervals do cover the exact probabilities as desired.

			95% Confidence Interval	
	P	$\hat{p}$	Lower	Upper
P1	0.89267123	0.89264068	0.89256234	0.89271902
P2	0.07930107	0.07935365	0.07928526	0.07942204
P3	0.01441838	0.01440805	0.01437790	0.01443820
P4	0.01075076	0.01073278	0.01070671	0.01075886
P5	0.00176119	0.00176328	0.00175267	0.00177390
P6	0.00032102	0.00031962	0.00031509	0.00032414
P7	0.00033215	0.00033316	0.00032857	0.00033780
P8	0.00032022	0.00032137	0.00031683	0.00032590
P9	0.00005837	0.00006017	0.00005820	0.00006213
P10	0.00006039	0.00006172	0.00005973	0.00006370
P11	0.00000443	0.00000467	0.00000412	0.00000521
P12	0.00000080	0.00000083	0.00000060	0.00000106

CONCLUSION

A mathematical model has been developed which makes it possible to realistically estimate the risk of flying the Space Shuttle with and without turbine discharge temperature redline protection. This model accurately describes the computer voting logic for handling all possible combinations of sensor failures and turbine overtemperature events and, thus, makes possible the estimation of both the probability of erroneous engine shutdown and the probability of not detecting a fuel turbine overtemperature event.

A companion Monte Carlo computer simulation was also programmed which verified that the analytical model is correct. The simulation is also useful in the study of parameter sensitivity and model assumptions.

This investigation has provided estimates of the risk envolved in flying the Space Shuttle with and without SSME temperature redline protection which is necessary for making informed design and flight policy decisions concerning overtemperatures.

Upon consideration of the merits of using temperature sensors to detect HPFT overtemperatures, it is seen that flight without redline protection entails the risk of an undetected overtemperature event which, for the given data set, is estimated to be 0.033. By using two temperature sensors in the HPFT to detect overtemperatures, the risk is reduced to 1.57E-5 using the Model 71 sensor (a factor of 2101) and to 2.2E-6 using the Model 81 (a factor of 15,000). However, when temperature sensors are utilized, the risk of erroneous engine shutddown is introduced, which is estimated to be 0.00114 for the Model 71 sensor and 0.000164 for the Model 81 sensor.

If an erroneous engine shutdown is considered to be as equally undesirable as an undetected overtemperature event, then one must compare the risk of a HPFT overtemperature event during flight without redline protection versus the risk of either an erroneous engine shutdown or an undetected HPFT overtemperature event during flight with redline protection. This comparison shows that the risk is reduced by a factor of 29 when the Model 71 sensors are used and a factor of 199 when the Model 81 sensor is used and, thus, flight with redline protection is highly recommended.

It should be emphasized that these numerical results are based on the two referenced data sets and it is recommended that these results be periodically updated as new sensor and fuel turbine life statistics become available.

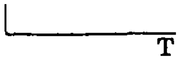
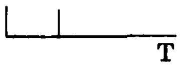
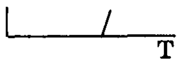
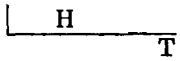
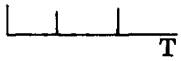
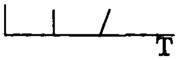
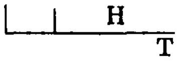
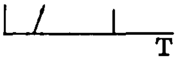
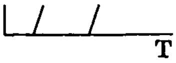
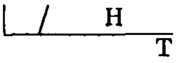
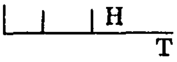
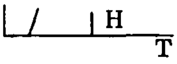
REFERENCES

1. Shooman, Martin L.: Probabilistic Reliability: An Engineering Approach. McGraw-Hill Book Company, 1968.

2. Golley, Paul, Chief, Sensors Branch, personal communication, March 1987.

3. Cikanek, Harry: Selection of SSME Test History Applicable to Determining the Hazard in Flying the Space Shuttle With/Without Turbine Discharge Temperature Redline Protection. NASA Memo ED14-05-87.

TABLE 1. THE TWELVE POSSIBLE STATES AND THE COMPUTER VOTING LOGIC

State	State Figure	State Description	Computer Reaction	Comments
S1		No sensor failures No overtemperature event	CTF*	Nominal State
S2		One sensor disqualified	CTF	Loss of redundancy
S3		One sensor erroneously votes to cut	CTF	Loss of redundancy
S4		HPFT overtemperature event	SD**	Correct decision
S5		Both sensors disqualified	CTF	Flying with no protection
S6		One sensor disqualified, the other later erroneously votes to cut	SD	Erroneous engine shutdown
S7		One sensor disqualified, and sometime later, an overtemperature event	SD	Correct decision
S8		One sensor votes to cut and then, sometime later, the other is disqualified	CTF	Flying with no protection
S9		One sensor erroneously votes to cut, and then sometime later, the other erroneously votes to cut	SD	Erroneous engine shutdown
S10		One sensor erroneously votes to cut. Later, there is an overtemperature event	SD	Correct decision
S11		Both sensors disqualified followed by an overtemperature	CTF	Undetected hot HPFT
S12		One sensor erroneously votes to cut, the other is later disqualified, followed by an overtemperature event	CTF	Undetected hot HPFT

Legend

|	a failing sensor is disqualified
/	a failing sensor erroneously votes to cut
H	HPFT overtemperature event
*	Continue to Fire
**	Shutdown

TABLE 2. STATE PROBABILITIES

STATE	PROBABILITY
S1	$P1(T) = e^{-2\overset{*}{L}T}\ e^{-\alpha T^{\beta}}$
S2	$P2(T) = \frac{2\lambda_1}{L}\ e^{-\alpha T^{\beta}}\ e^{-LT}\ (1 - e^{-LT})$
S3	$P3(T) = \frac{2\lambda_2}{L}\ e^{-LT}\ (1 - e^{-LT})\ e^{-\alpha T^{\beta}}$
S4	$P4(T) = (1 - e^{-\alpha T^{\beta}}\ e^{-2LT}) - \int_0^T 2L\ e^{-\alpha x^{\beta}}\ e^{-2Lx}\ dx$
S5	$P5(T) = \frac{\lambda_1^{\ 2}}{L^2}\ e^{-\alpha T^{\beta}}\ (1 - e^{-LT})^2$
S6	$P6(T) = \frac{2\lambda_1\lambda_2}{L} \int_0^T e^{-Lx}\ (1 - e^{-Lx})\ e^{-\alpha x^{\beta}}\ dx$
S7	$P7(T) = \frac{2\lambda_1}{L} \int_0^T e^{-Lx}\ (1 - e^{-Lx})\ \alpha\beta\ X^{\beta-1}\ e^{-\alpha x^{\beta}}\ dx$
S8	$P8(T) = \frac{\lambda_1\lambda_2}{L^2}\ e^{-\alpha T^{\beta}}\ (1 - e^{-LT})^2$
S9	$P9(T) = \frac{\lambda_2^{\ 2}}{L^2}\ e^{-\alpha T^{\beta}}\ (1 - e^{-LT})^2 + \int_0^T \frac{\lambda_2^{\ 2}}{L^2}\ (1 - e^{-Lx})\ e^{-\alpha x^{\beta}}\ dx$
S10	$P10(T) = \frac{2\lambda_2}{L} \int_0^T e^{-Lx}\ (1 - e^{-Lx})\ \alpha\beta\ X^{\beta-1}\ e^{-\alpha x^{\beta}}\ dx$
S11	$P11(T) = \frac{-\lambda_1^{\ 2}}{L^2}\ e^{-\alpha T^{\beta}}\ (1 - e^{-LT})^2 + \frac{2\lambda_1^{\ 2}}{L} \int_0^T e^{-Lx}\ (1 - e^{-Lx})\ e^{-\alpha x^{\beta}}\ dx$
S12	$P12(T) = \frac{-\lambda_1\lambda_2}{L^2}\ e^{-\alpha T^{\beta}}\ (1 - e^{-LT})^2 + \frac{2\lambda_1\lambda_2}{L} \int_0^T e^{-Lx}\ (1 - e^{-Lx})\ e^{-\alpha x^{\beta}}\ dx$

* $L = \lambda_1 + \lambda_2$

TABLE 3. SYSTEM STATES VERSUS FAILURE SCENARIOS

STATE	FAILURE SCENARIOS	COMPUTER DECISION
S1	$t_{A,i}, t_{B,j}, t_H > T$	CTF
S2	$t_{A,1} < T < t_{B,j}, t_H$ or $t_{B,1} < T < t_{A,i}, t_H$	CTF
S3	$t_{A,2} < T < t_{B,j}, t_H$ or $t_{B,2} < T < t_{A,i}, t_H$	CTF
S4	$t_H < T, t_{A,i}, t_{N,j}$	SD
S5	$t_{A,1} < t_{B,1} < T < t_H$ or $t_{B,1} < t_{A,1} < T < t_H$	CTF
S6	$t_{A,1} < t_{B,2} < T, t_H$ or $t_{B,1} < t_{A,2} < T, t_H$	SD
S7	$t_{A,1} < t_H < T, t_{B,j}$ or $t_{B,1} < t_H < T, t_{A,i}$	SD
S8	$t_{A,2} < t_{B,1} < T < t_H$ or $t_{B,2} < t_{A,1} < T < t_H$	CTF
S9	$t_{A,2} < t_{B,2} < T, t_H$ or $t_{B,2} < t_{A,2} < T, t_H$	SD
S10	$t_{A,2} < t_H < T, t_{B,j}$ or $t_{B,2} < t_H < T, t_{A,i}$	SD
S11	$t_{A,1} < t_{B,1} < t_H < T$ or $t_{B,1} < t_{A,1} < t_H < T$	CTF
S12	$t_{A,2} < t_{B,1} < t_H < T$ or $t_{B,2} < t_{A,1} < t_H < T$	CTF

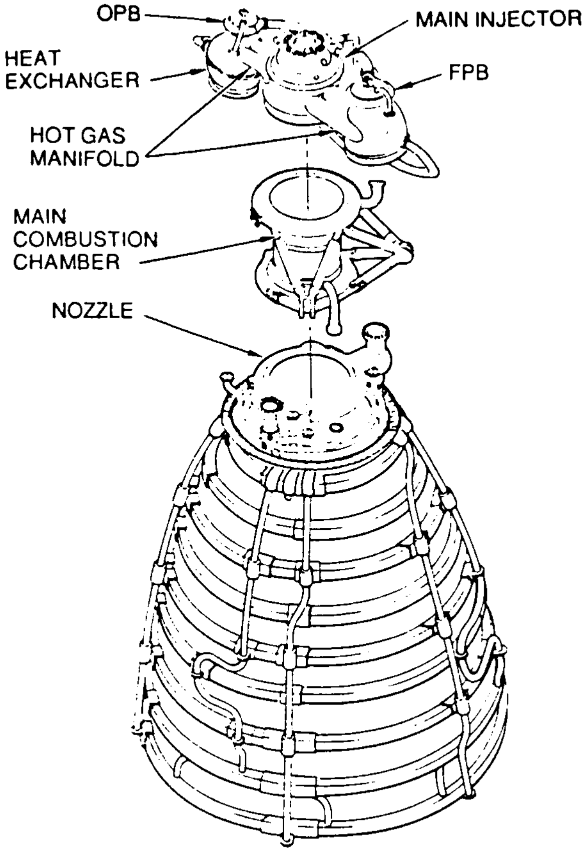


Figure 1a. SSME combustion devices.

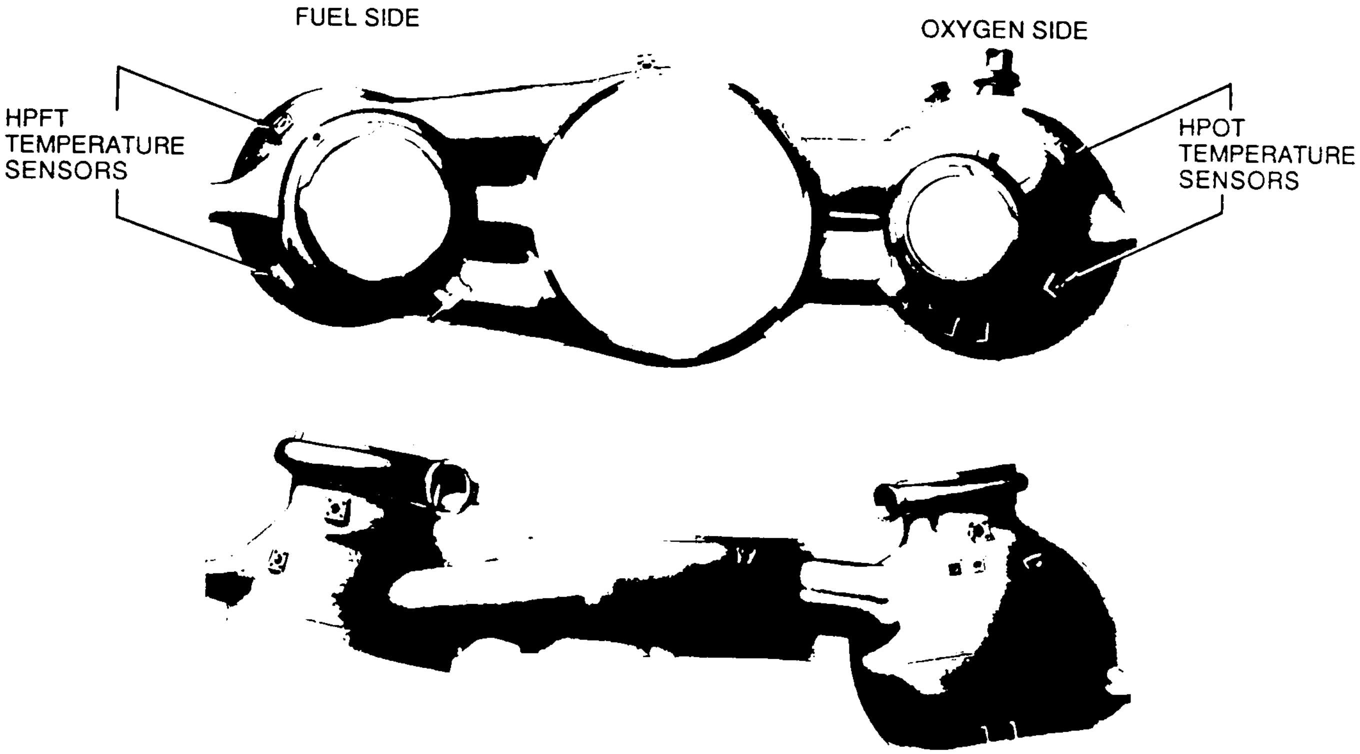


Figure 1b. SSME hot gas manifold.

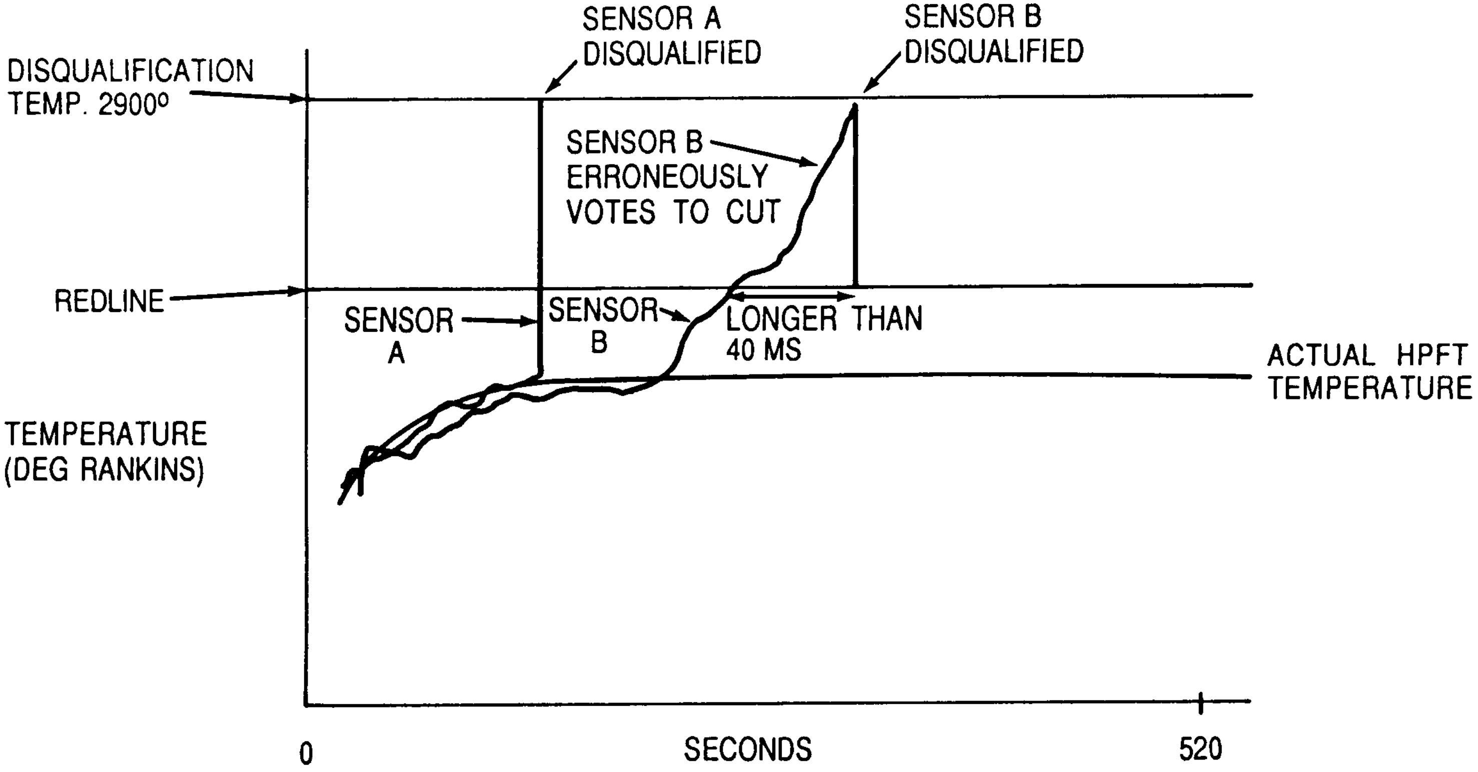
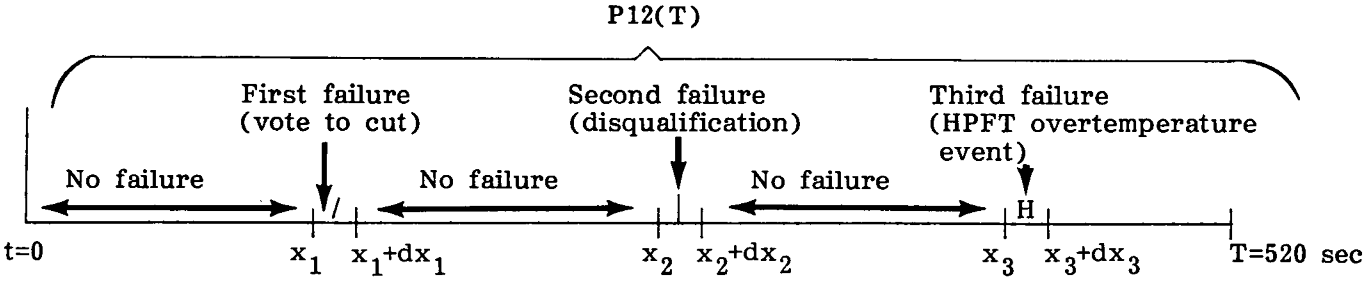


Figure 2. Sensor failure scenarios: sensor A is disqualified and sensor B erroneously votes to cut.


P12(T)
First failure (vote to cut)
Second failure (disqualification)
Third failure (HPFT overtemperature event)
No failure
No failure
No failure
H
t=0
x1
x1+dx1
x2
x2+dx2
x3
x3+dx3
T=520 sec

a. Time interval for compound-event of S12

$$P_{12}(T) = \int_0^T \int_0^{X_3} \int_0^{x_3} \underbrace{\left[e^{-2(\lambda_1+\lambda_2)x_2}\right]}_{\text{Probability of no sensor failures to } x_1} \underbrace{\left[2\lambda_2 dx_1\right]}_{\text{Probability of a vote to cut in } dx_1} \underbrace{\left[e^{-(\lambda_1+\lambda_2)(x_2-x_1)}\right]}_{\text{Probability of no failure } x_1 \text{ to } x_2} \underbrace{\left[\lambda_1 dx_2\right]}_{\text{Probability of remaining sensor being disqualified in } dx_2} \underbrace{e^{-\alpha x_3^{\beta}}}_{\text{Probability of no overtemperature event to } x_3} \underbrace{\alpha\beta\, X_3^{\beta-1}\, dx_3}_{\text{Probability of HPFT overtemperature event in } dx_3}$$

b. Construction of P12(T)

Figue 3. Construction of $P_{12}(T)$ using compound-event approach.

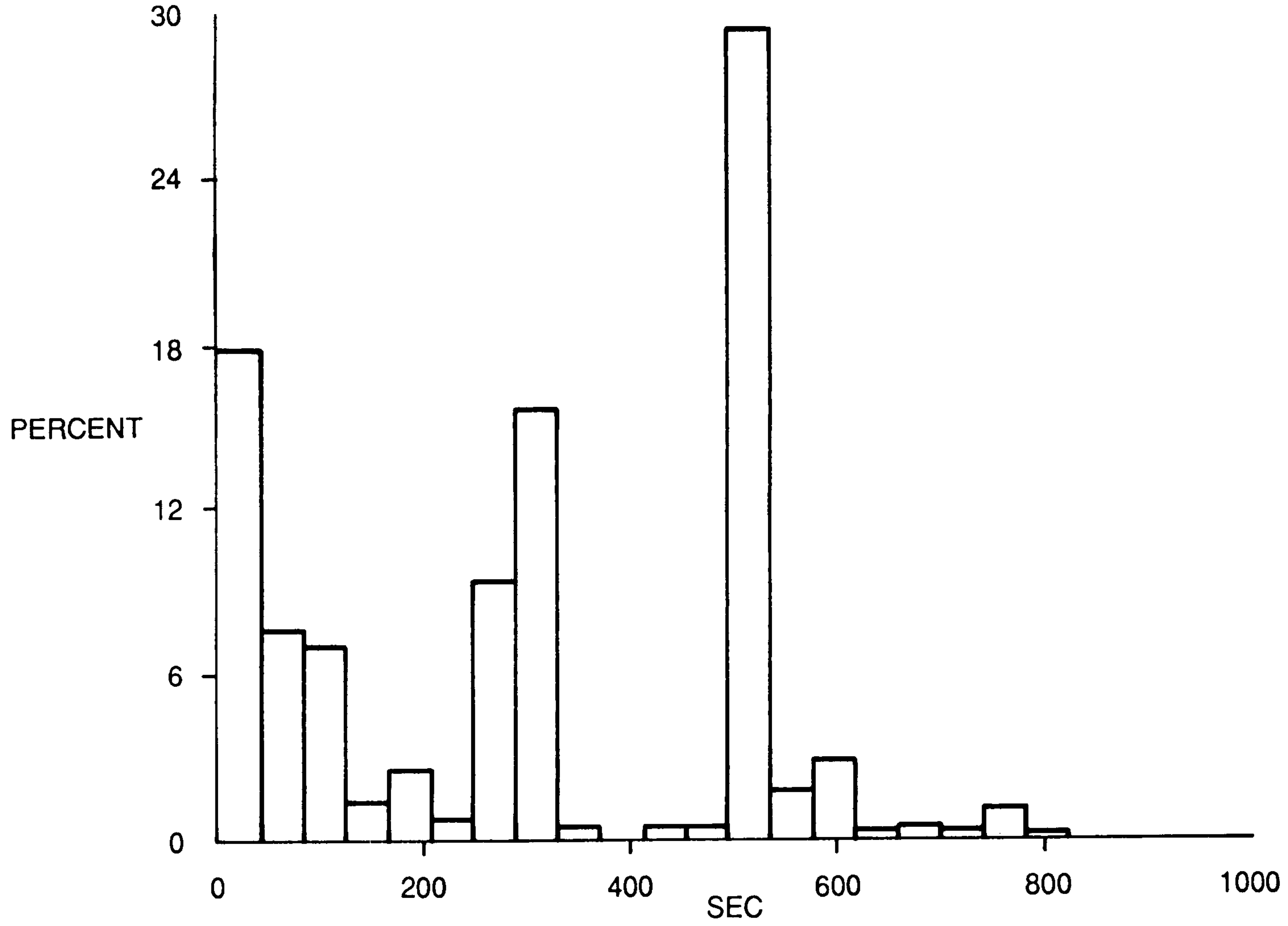


Figure 4. Frequency histogram of the duration of the 682 successful engine firings.

1. REPORT NO.
NASA TP-2759

2. GOVERNMENT ACCESSION NO.

3. RECIPIENT'S CATALOG NO.

4. TITLE AND SUBTITLE
Probabilistic Risk Analysis of Flying the Space Shuttle With and Without Fuel Turbine Discharge Temperature Redline Protection

5. REPORT DATE
August 1987

6. PERFORMING ORGANIZATION CODE

7. AUTHOR(S)
Leonard Howell

8. PERFORMING ORGANIZATION REPORT #

9. PERFORMING ORGANIZATION NAME AND ADDRESS

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

10. WORK UNIT NO.
M-567

11. CONTRACT OR GRANT NO.

12. SPONSORING AGENCY NAME AND ADDRESS

National Aeronautics and Space Administration
Washington, D.C. 20546

13. TYPE OF REPORT & PERIOD COVERED

Technical Paper

14. SPONSORING AGENCY CODE

15. SUPPLEMENTARY NOTES

Prepared by Structures and Dynamics Laboratory, Science and Engineering Directorate.

16. ABSTRACT

This paper presents an exact mathematical model of the Space Shuttle Main Engine computer voting logic in the presence of High Pressure Fuel Turbine (HPFT) overtemperature events and fuel turbine temperature sensor failures. The model provides estimates of the probability of erroneous engine shutdown and the probability of not detecting a HPFT overtemperature event.

Because it is believed that the likelihood of sensor failures and overtemperature events in the HPFT greatly overshadows those in the High Pressure Oxygen Turbine (HPOT), this modeling effort has been focused on the HPFT. However, because the redline protection logic is the same for both turbines, estimation of the model parameters using relevant HPOT data would provide estimates of the risk of erroneous engine shutdown and an undetected overtemperature event occurring in the HPOT.

Because of the complexity of the model, it was necessary to program the solution which thus makes it feasible to accommodate a changing data base. This is considered to be of great interest because of the subjective nature in determining the relevancy of certain failures and the fact that the data base is constantly changing as a result of the frequent engine tests.

17. KEY WORDS

Reliability, Temperature Sensors,
Space Shuttle, Stochastic Processes
Monte Carlo Simulation

18. DISTRIBUTION STATEMENT

Unclassified/Unlimited

Subject Category: 65

19. SECURITY CLASSIF. (of this report)
Unclassified

20. SECURITY CLASSIF. (of this page)
Unclassified

21. NO. OF PAGES
21

22. PRICE
A02

For sale by National Technical Information Service, Springfield, Virginia 22161

NASA-Langley, 1987