Study on Safety and Reliability of ETOPS using Aircraft Operation Simulation

K. W. Nam* and C. Y. Kim**

남 기 욱 , 김 칠 영

Table

* 한국항공우주연구소 연구원
** 한국항공대학교 항공운항학과 조교수

ABSTRACT

A methodology has been developed for predicting aircraft reliability incorporating both C.C.F.s(Common-Cause Failures), and phased missions. Failure behaviour of an aircraft, or it's systems are predicted. Both independent failures, and C.C.F.s, are modelled by the Markov process, and simulated using Monte Carlo sampling with the robust variance reduction method. Prediction of safety and reliability is made through discrete-event simulation of aircraft operations. A case study is described for investigating the safety and reliability of the propulsion system of two-, three- and four-engined aircraft. This is particularly important for the design of ETOPS(Extended Range of Two-Engined Aircraft Operations) and results are presented for the cases with, and without the effect of C.C.F.s.

1 INTRODUCTION

Safety and reliability are essential issues in the design, development and operation of most aircraft. Modern aircraft and systems should meet safety requirements that are stipulated in the principal airworthiness codes, such as FAR. More stringent reliability requirements are included in aircraft specifications, by customers, to reduce unreliability costs as much as possible. These can be achieved only by including safety and reliability analyses in the design process, to evaluate the proposed design's potential for meeting these requirements, and to compare alternatives in design trade-off studies. This has led to the need for safety and reliability analysis tools that are simple to use in the aircraft design process, and can predict safety and reliability with good accuracy.

There are well-established techniques for predicting safety and reliability of aircraft and systems such as RBD[1](Reliability Block Diagram) or FTA[2](Fault Tree Analysis). Traditionally, these methods predict safety and reliability of aircraft and systems with the assumptions that failures are mutually independent, and missions consist of a single phase. However, real life produces C.C.F.s(Common-Cause Failures) which lead to simultaneous failures of more than one component or channel. Most aircraft systems are required to perform phased-missions, in which the system configuration is changed during consecutive time periods (phases), such as take-off, climb, cruise, etc. These traditionally would be modelled for each phase by means of separate RBDs, or fault trees incorporating C.C.F. events, but the model becomes quite complex. More fundamental limitations of RBD or FTA methods rise in modelling an operation of systems, which is critical in operational reliability prediction.

In this study, a methodology was developed for predicting aircraft safety and reliability incorporating both C.C.F.s and phased missions. Monte Carlo simulation of the Markov process is used for simulating system failure behaviour. Safety and reliability prediction is made through discrete-event simulation of aircraft operations. Since the ETOPS(Extended Range of Twin Engine Aircraft Operations) is an important issue in flight safety, a case study of aircraft propulsion systems has been conducted, to show the effect of diversion time and number of engines, with and without the existence of C.C.F.s, on aircraft safety and reliability.

2 TERMS AND DEFINITIONS

2.1 Independent Component Failure

Independent component failure is the failure of a single component which is not related to the failure of another component. For a system with independent component failure, the basic event, i.e., the lowest level of input to the system safety and reliability model, is single component failure and the model is represented down to the level of component failure modes. This is illustrated by the system fault tree in Fig.1, for a system of three components A, B, and C.

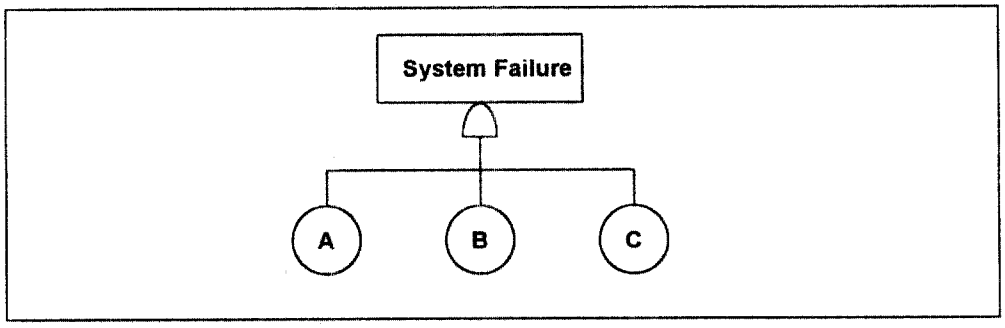


Figure 1 Basic System Fault Tree of 3 Component System

Since the basic events of a system with independent failure are single component failures, the input to the safety and reliability model is given as the failure rate of component and obtained from the following equation.

$$\lambda_i = \frac{N_i}{T} \qquad i = A, B, C, \cdots \tag{1}$$

where N_i is a number of failures of component i during the total exposure time of a system, T. For example, the failure rate of the components in the above example are obtained as:

$$\lambda_A = \frac{N_A}{T},\ \lambda_B = \frac{N_B}{T},\ \lambda_C = \frac{N_C}{T} \tag{2}$$

2.2 Common-Cause Failure

A common-cause failure is defined as a failure of multiple components due to a single failure cause. For a system with C.C.F.s, the basic events are the independent failure of one and only one component, and common-cause failure of more than one component. Therefore, safety and reliability models are represented by single and particular sets of components failed. For a component A of the foregoing example system, if we assume that common-cause failures can lead to either two or three components failing simultaneously, the total failure of component A is defined as:

$$A = a + ab + ac + abc \tag{3}$$

where

A = total failure of component A.
a = failure of component A from both independent and common-causes.
ab = failure of components A and B (and not component C) from common-causes.
ac = failure of components A and C (and not component B) from common-causes.
abc = failure of components A, B, and C from common-causes.

Total failure of component B and C are defined similarly. The system fault tree incorporating C.C.F.s is shown in Fig. 2, for a system with 3 components.

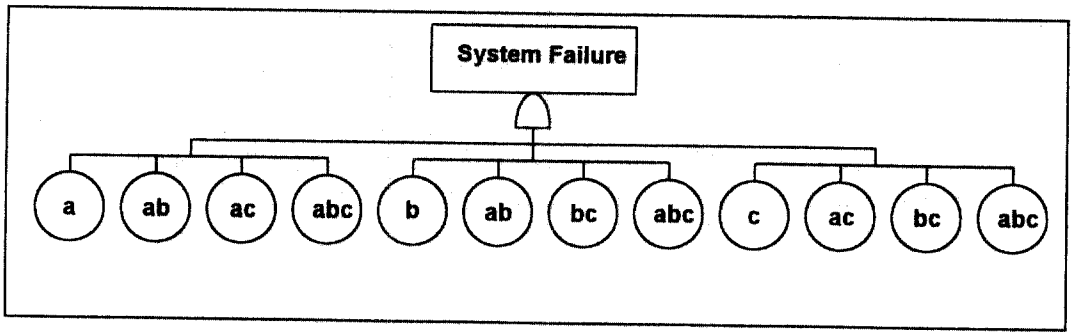


Figure 2 C.C.F. Integrated System Fault Tree of 3 Component System

Since the basic events of the system with C.C.F.s are failures of both single, and specific sets of multiple components, the input to the safety and reliability model are given as rates of single and common-cause failures, obtained from the following equation.

$$\lambda_j = \frac{N_j}{T} \tag{4}$$

where

j indicator of failure event - single or set of components failed
$j = a, ab, abc, \ldots$
N_j number of failures of event j
T total system exposures

For example, failure rates of a 3-component system for the previous example are:

$$\lambda_a = \frac{N_a}{T}, \quad \lambda_b = \frac{N_b}{T}, \quad \lambda_c = \frac{N_c}{T}$$
$$\lambda_{ab} = \frac{N_{ab}}{T}, \quad \lambda_{ac} = \frac{N_{ac}}{T}, \quad \lambda_{bc} = \frac{N_{bc}}{T} \tag{5}$$
$$\lambda_{abc} = \frac{N_{abc}}{T}$$

The total failure rate of a specific component can be obtained from the λ_j's. This can be seen from Eq. 3, where the failure of component A due to all causes is expanded in terms of the basic events. From Eq. 3 and using λ_a, λ_{ab}, λ_{ac} and λ_{abc} defined in Eq. 5, we get:

$$\lambda_A = \lambda_a + \lambda_{ab} + \lambda_{ac} + \lambda_{abc} \tag{6}$$

where λ_A is the failure rate of component A due to all causes.

3 PREDICTION METHODOLOGY

3.1 System Modelling

For the purpose of system modelling, we assume that a system consists of n components which are either operating, or have failed. The state of the system is determined by the combination of failed and operating components, and therefore there are 2^n system states in an n component system. The state of the system at a time t is represented by a system state vector X.

$$X = \{ x_1 \quad x_2 \quad \cdots \quad x_n \} \tag{7}$$

where x_i is component state variable of component i. If component i is operating, $x_i = 0$, else $x_i = 1$.

The system state is governed by the following two probability density functions:

$f(t|t', k')$ ≡ Probability density that the system will make a state transition at t given that it is at state k' at times t' $(t' \le t)$. (8)

$q(k|k')$ ≡ Probability that the system will enter state k, following a transition out of state k'. (9)

Under the assumption that only the time-independent failure rate is considered, the transition probability density function, Eq. 8 is written as :

$$f(t|t', k') = \lambda_{k'} \exp\left[-\lambda_{k'}(t-t')\right] \tag{10}$$

where $\lambda_{k'}$ is total failure rate of the system at state k'. The transition probability $q(k|k')$ from state k' to state k is $1/\lambda_{k'}$ multiplied by the failure rate of specific component, λ_i or by the failure rate of specific event, λ_j that must change states in order for the $k' \rightarrow k$ transition to take place. The transition probability for the system without C.C.F. is given as:

$$q(k|k') = \lambda_i^{k' \rightarrow k} \frac{1}{\lambda_{k'}} \qquad i = 1, 2, \cdots, n \tag{11}$$

where i is an indicator of component and n is number of components in the system. The transition probability for the system with C.C.F. is:

$$q(k|k') = \lambda_j^{k' \rightarrow k} \frac{1}{\lambda_{k'}} \qquad j = 1, 2, \cdots, m \tag{12}$$

where j is the failure event indicator including C.C.F. and m is number of possible failure event in the n component system.

3.2 Operation Modelling

The objective of the operation model is to describe the mission that the aircraft or systems perform. The typical operation of transport aircraft was modelled as follows. The flight route consisted of 5 phases: take-off, climb, cruise, descent, and landing. The flight began with take-off from the departure and ended with landing at one of three airports: departure, destination or alternate, or being terminated due to system catastrophic failure. The alternates were assumed to be located randomly over the route, within the allowed diversion time. A top-level logic flow diagram of the aircraft operation is shown in Fig. 3.

3.3 Simulation

A flow diagram of the simulation procedure is given in Fig. 5. The mission consists of the consecutive phases which the system performs. The system is initialised at the beginning of mission and starts with phase 1. In each phase of the mission, alternative samplings are carried out for the time of component failure event (transition time) and for the components involved in the failure event (transition state), either independent or common-cause failures.

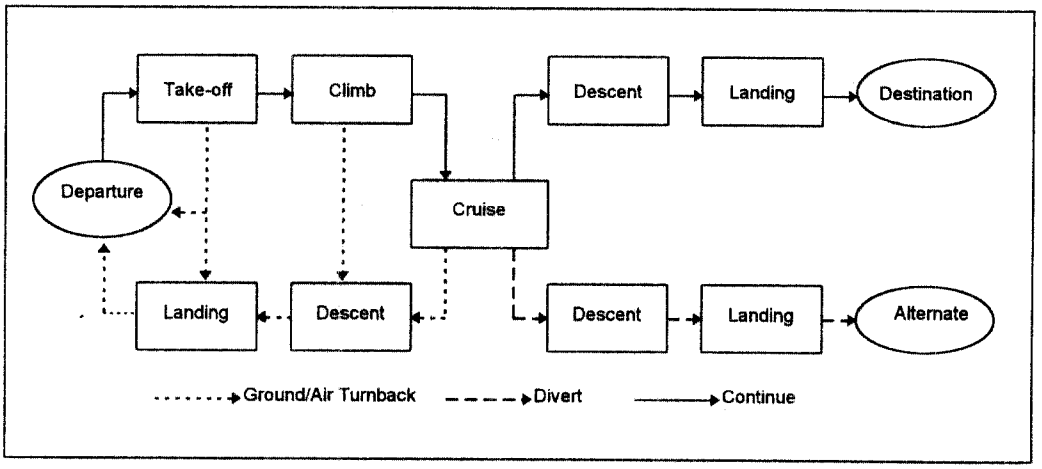


Figure 3 Aircraft Operation Flow Diagram

Transition time derivation is generated by Monte Carlo sampling of the probability density function, given by Eq. 10. At each sampling of transition time, the time of the component failure event, t_j is compared with the mission time of phase j, T_j to determine whether the component failure event has occurred or not during that mission phase. If the mission time of phase j, T_j is less than the sampling time of the component failure event, t_j, no component failure in the system is considered, and the system will continue to perform the next phase of the mission, with the system state unchanged. When the time of a component failure event is obtained for the failure event, which occurs before the completion of the phase of mission, the sampling of components failed in that event is carried out.

Sampling of a failed component, i due to independent failure cause, or a set of failed components, j due to common failure cause is done by Monte Carlo simulation of the transition probability function, given by Eq. 11 or Eq. 12. When a failed component i, or a set of components involved in failure event j, is determined, the corresponding indicator variable x_i of the system state vector $\boldsymbol{X}$ is set to 1. The system state k is then evaluated by decimalizing the system state vector $\boldsymbol{X}$.

The system functional status and operational logic for specific system states are represented by the system status-operation logic matrix $\boldsymbol{Q}$. They are derived from the system block diagram with the consideration of the method of system operation. The status and operational logic of the system in phase j, state k is then determined as q_{jk} from the system status-operation logic matrix $\boldsymbol{Q}$. When the system status is determined as a catastrophic failure, the mission is terminated, and the next mission begins with the initialised system. If the system does not fail, it continues a phase of mission in accordance with the operation logic. The mission ends when either the system catastrophic failure (q_{jk} = catastrophic failure) is reached or the last phase of the mission is finished. Statistics are then recorded after termination of the mission, for the system safety and reliability calculations.

3.4 Estimation

The system safety and reliability has been calculated from M independent simulations of a given mission. Safety is defined as the complement of the catastrophic failure probability and obtained from:

$$Safety = 1 - \frac{Number\ of\ Occurrences\ of\ Catastrophic\ Failure}{Total\ Missions} \tag{13}$$

Reliability is defined as the probability of completing the flight without enroute interruption, such as diversion or turnback, etc. This is called as Enroute Reliability and determined by:

$$Reliability = 1 - \frac{Number\ of\ Interruptions}{Total\ Missions} \tag{14}$$

4 USE OF THE METHODOLOGY FOR STUDY OF PROPULSION SYSTEM RELIABILITY

With the increased reliability of modern jet engines, coupled with an increased desire to maximise profitability, the diversion time imposed on ETOPS aircraft has been increased up to 180 minutes at one-engine speed[3]. However, the controversy about the flight safety of ETOPS aircraft still continues. A major topic of ETOPS safety is that longer diversion time leads to a corresponding potential increase in single-engined flight to an alternate. This may have significant adverse effects on flight safety, particularly due to the increase in consecutive IFSD (in-flight shutdown) probability. In this study, the investigation of safety and reliability of ETOPS aircraft has been attempted with the developed methodology. The safety and reliability of two-engined aircraft with 60, 120, and 180 minutes diversion times have been evaluated as functions of mission time. Safety and reliability of three- and four-engined aircraft were also evaluated, for comparison with two-engined aircraft.

4.1 System

4.1.1 System Description

The propulsion system consists of identical power plants, which are operating in parallel. The system block diagrams of two-, three-, and four- engined aircraft are shown in Fig. 4. The aircraft can continue the flight with one or more engines inoperative as long as the thrust required to propel the aircraft is provided by the propulsion system. The minimum thrust, i.e. a minimum number of engines, for an aircraft to fly depends on the flight phase.

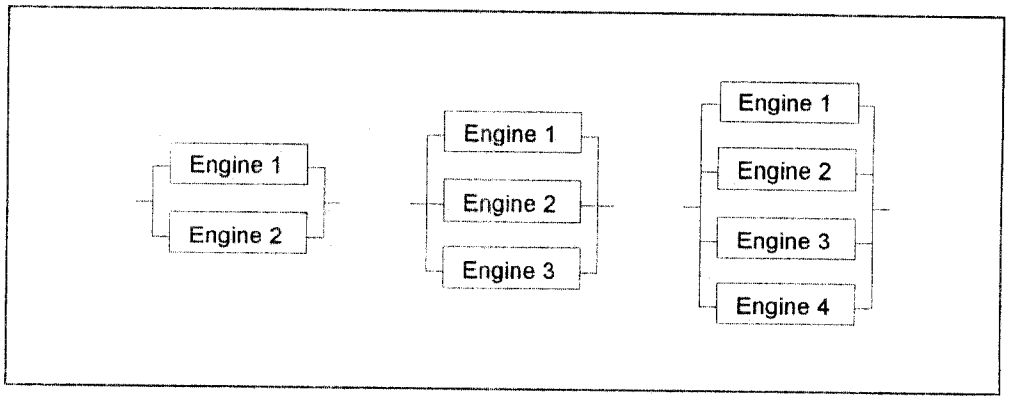


Figure 4 Block Diagram of Propulsion System of 2, 3, and 4 Engined Aircraft

An in-flight engine shut down, which causes immediate danger and prevents the continuation of the safe flight, is considered as an engine failure in this study. It is further assumed that there may be multiple IFSDs due to common-cause failures such as bird strike, volcanic ash, etc., in addition to IFSDs of individual engines.

4.1.2 Phased IFSD Rate

IFSD factors were used to consider the effect of flight phases on IFSD. They were used to convert an average IFSD rate to a flight phase-dependent IFSD rate. The severity factors were suggested in Ref.[4] and are presented in Table 1.

The phased IFSD rate was then obtained as an average IFSD rate multiplied by IFSD factor for each phase.

$$Phased\ IFSD\ Rate = Average\ IFSD\ rate \times IFSD\ Factor \qquad (15)$$

Table 1 IFSD Factor by Phase of Flight[4]

Phase	% Time Exposure*, $\frac{T_{Phase}}{T_{Mission}}$	% IFSDs, $\frac{N_{IFSD,Phase}}{N_{IFSD,Mission}}$	IFSD Factor, $\frac{\%\ time\ exposure}{\%\ IFSD}$
Take-off	1	4	4.0
Climb	14	31	2.0
Cruise	60	37	0.6
Descent	10	19	2.0
Approach/Landing	15	9	0.6

* The % time exposures are calculated based on the standard flight profile with a 1.6 hour duration.

4.1.3 C.C.F. Rate

The common-cause IFSD rate of two-engined aircraft can be estimated using the simple β-factor model[5]. This model postulates that the total failure rate of a component, λ consists of two parts: a random, independent failure rate, λ_{Ind} and a common-cause failure rate, $\lambda_{C.C.F.}$. The fraction of failures due to common-cause is represented by the parameter β. Thus, single-engine IFSD rate $\lambda_{1/2}$ due to independent causes and double-engine IFSD rate $\lambda_{2/2}$ due to common-causes for a propulsion system with two engine are obtained as:

$$\lambda_{1/2} = (1 - \beta)\lambda, \quad \lambda_{2/2} = \beta\lambda \tag{16}$$

where total IFSD rate, $\lambda = \lambda_{1/2} + \lambda_{2/2}$. To investigate the effect of C.C.F. on propulsion system safety and reliability, β-factors of 0.002 and 0.004 were used, for comparison purposes. β-factor of 0.002 has been taken based on the statistics of commercial jet aircraft accidents[6].

Since common-causes do not always fail all components of a system, C.C.F. rates of a system having a specific number of components are not necessarily the same as those of a system having a different number of components. This is called the system size effect of C.C.F.[7] Therefore, for all types of aircraft to have the same common-cause failure condition, the 2 engine common-cause IFSD rate, $\lambda_{2/2}$ of a two-engined aircraft should be adjusted to 2 and 3 engine common-cause IFSD rates, $\lambda_{2/3}$, $\lambda_{3/3}$ of three-engined aircraft and 2, 3, and 4 engine common-cause IFSD rates $\lambda_{2/4}$, $\lambda_{3/4}$, $\lambda_{4/4}$ of four-engined aircraft. This was done using BFR(Binomial Failure Rate) model[8].

4.2 Operation

4.2.1 Operation Logic

The aircraft operation logic and conditions of catastrophic failure are shown in Table 2. During the take-off/climb and descent/landing phases, all types of aircraft were assumed to have the same emergency strategy, i.e. turnback to departure before reaching cruise or continue to destination, after beginning to descend.

During the cruise, three operational IFSD strategies were used, according to the failure condition of the propulsion system. These are given in Table 3. An economy strategy was chosen when 1 engine IFSD event occurred in three- and four-engined aircraft. A safety strategy was used for two- and four-engined aircraft in the case of a 50% loss of thrust. An emergency strategy was applied for three- and four-engined aircraft when there was only one engine available.

Table 2 Aircraft Operation Logic and Catastrophic Failure Condition

Aircraft Type	Flight Phase	Failure Condition (Number of IFSD Engine)			
		1	2	3	4
Two Engined	Before V_1	Ground TB	Catastrophe	-	-
	After V_1	Air TB	Catastrophe	-	-
	Climb	Air TB	Catastrophe	-	-
	Cruise	Safety	Catastrophe	-	-
	Descent	Continue	Catastrophe	-	-
	Landing	Continue	Catastrophe	-	-
Three Engined	Before V_1	Ground TB	Ground TB	Catastrophe	-
	After V_1	Air TB	Catastrophe	Catastrophe	-
	Climb	Air TB	Catastrophe	Catastrophe	-
	Cruise	Economy	Emergency	Catastrophe	-
	Descent	Continue	Continue	Catastrophe	-
	Landing	Continue	Continue	Catastrophe	-
Four Engined	Before V_1	Ground TB	Ground TB	Ground TB	Catastrophe
	After V_1	Air TB	Catastrophe	Catastrophe	Catastrophe
	Climb	Air TB	Air TB	Catastrophe	Catastrophe
	Cruise	Economy	Safety	Emergency	Catastrophe
	Descent	Continue	Continue	Continue	Catastrophe
	Landing	Continue	Continue	Continue	Catastrophe

Table 3 Operation Strategy with IFSD during Cruise

Failure Condition	Strategy	Procedure
1/3, 1/4	Economy	Take the nearest airport between departure and destination.
1/2, 2/4	Safety	Turnback or continue when departure or destination is within allowed diversion time. Otherwise, divert.
2/3, 3/4	Emergency	Take the nearest airport amongst departure, destination, and alternate airports.

4.2.2 Phase Time

It was assumed that the phase durations for take-off, climb, descent, and landing segments were the same for all flights. From the phase percentages of flight time based on an average flight duration of 1.6 hours given in Ref.[6], the phase time of take-off, climb, descent, and landing were estimated as follows.

$$\begin{aligned}
&\text{Time for Take-off, } T_{Take\text{-}off} = 1.6 \text{ hrs} \times 1\% = 0.016 \text{ hrs} \\
&\text{Time for Climb, } T_{Climb} = 1.6 \text{ hrs} \times 14\% = 0.224 \text{ hrs} \\
&\text{Time for Descent, } T_{Descent} = 1.6 \text{ hrs} \times 10\% = 0.160 \text{ hrs} \\
&\text{Time for Approach \& Landing, } T_{Approach\ \&\ Landing} \\
&\qquad = 1.6 \text{ hrs} \times 15\% = 0.240 \text{ hrs}
\end{aligned} \tag{17}$$

The cruise time was determined by subtracting the phase time for the take-off, climb, descent, and landing segments from total mission time, $T_{mission}$.

$$\text{Time for Cruise, } T_{Cruise} = T_{Mission} - 0.64 \text{ hrs} \quad (18)$$

The critical engine failure speed, V_1, is the speed at which the average pilot could safely continue a take-off with a critical engine failure. The time taken to reach the critical engine failure speed, V_1, was given to distinguish a ground turnback from an air turnback. If an engine IFSD occurs before reaching the critical engine failure speed, V_1, the flight is terminated with an interruption classified as a ground turnback. If an IFSD takes place after reaching the critical engine failure speed, V_1, the aircraft continues the take-off and turns back to the airport. The time to critical engine failure speed, V_1, was assumed to be 0.01 hour.

4.2.3 Performance Considerations

When IFSDs occur, the speed of an aircraft is reduced, due to a decrease in thrust and an increase in drag. As a result of this, the original flight time increases in proportion to the speed reduction. In this study, it was assumed that the speed of an aircraft is proportional to the number of operative engines and the flight time is increased by the factor:

$$\textit{Speed Reduction Factor} = \frac{\textit{Number of Operating Engines before IFSD}}{\textit{Number of Operating Engines after IFSD}} \quad (19)$$

This factor is relatively simplistic, but is a reasonable representation for all types of aircraft for the purposes of comparison. Flight times after IFSD are then obtained as:

$$T_{Altered} = T_{Original} \times \textit{Speed Reduction Factor} \quad (20)$$

4.3 Simulation

The simulation of aircraft operations was conducted with various ranges of missions under the same flight route conditions for two-, three-, and four-engined aircraft. A two-engined aircraft was simulated with 60, 120, and 180 minutes diversion times. Operation of three- and four-engined aircraft were simulated with the same conditions as for two-engined aircraft having a 180 minutes diversion time.

Since an aircraft propulsion system is very reliable, the Monte Carlo sampling of engine IFSD events is too inefficient, if a conventional form of sampling technique is used. For four-engined aircraft having an engine with an IFSD probability of 10^{-3}, for example, only one event of all engine IFSD due to independent failure causes is expected from 10^{12} Monte Carlo samples. To improve the computational efficiency of the Monte Carlo simulation, two variance reduction techniques were used, namely forced transitions and failure biasing[9]. The forced transition technique produces an artificially large number of component failures, while the failure biasing technique increases the ratio of C.C.F.s to independent failures. In using these variance reduction techniques, a weight, initialised to one, is attached to each flight of the simulation, and modified appropriately at each biased sampling. This results in a substantial number of simulated flights that have IFSD events, but the IFSD events in those simulated flights will have weights much smaller than one. The safety and reliability estimation was carried out with weighted statistics. The detail of simulation method using the variance reduction technique is presented in Ref. [10], with it's validation.

4.4 Results and Discussion

Operational reliability, and probability of catastrophic failure of two-, three-, and four-engined aircraft are given in Fig. 6 and Fig. 7. The simulation results of two-engined aircraft are presented for 1, 2, and 3 hour diversion time, respectively. In each figure, the results were obtained with different β-factors to show the effects of C.C.F.s on safety and reliability of aircraft propulsion system.

4.4.1 Operational Reliability

Operational reliability is the probability of completing the flight without any interruptions, and is shown in Fig. 6. In the case of no common-cause IFSDs, two-engined-aircraft achieved better operational reliability than three- and four-engined aircraft in ranges up to 6 to 10 hours, depending on their ETOPS capability. Among two-engined aircraft, it is seen that longer diversion times are beneficial in operational reliability, over all ranges. In the long range missions, three-engined aircraft achieved higher operational reliability than two-engined aircraft while the operational reliability of four-engined aircraft has the lowest level. The main contribution to these results is the one-engine IFSD event. Since a one-engine IFSD before the mid-point of cruise causes flight interruptions for all types of aircraft, more engines in aircraft result in more interruptions. However, one-engine IFSD events of three- and four-engined aircraft after the mid-cruise point do not cause interruptions, due to their performance capability with one-engine IFSD. This makes the operational reliability of three-engined aircraft exceed the two-engined aircraft operational reliability for long-range missions. For four-engined aircraft, the higher probability of one-engine IFSDs surpasses the advantage of it's relative performance. Due to this, the operational reliability of four-engined aircraft is still lower than that of two-engined aircraft even for long-range missions.

When the common-cause IFSDs are incorporated in the simulations, better operational reliabilities are obtained than the case without common-cause IFSD for all types of aircraft. This is shown in Fig. 6-b and Fig. 6-c. This is due to the decrease in the independent IFSDs of single-engines, resulting in less interruptions. When the β-factor is increased, the fraction of common-cause IFSD increases and the independent IFSDs of a single engine decreases, since the total IFSD rate of the engine is kept the same. The results show that a three-engined aircraft gains the most benefit in the flight with C.C.F.s. Little difference is observed in the operational reliability between flights with low (β-factor = 0.002) and high (β-factor = 0.004) common-cause IFSD.

4.4.2 Safety

Safety, in this study, was measured by the probability of catastrophic failure of a propulsion system, resulting in the loss of an aircraft. This is different from the probability of all-engine IFSD because, in certain phases, the catastrophic failure of a propulsion system is caused by losing not only all, but also some of engines, e.g., two-engine IFSD of three-engined aircraft during the take-off, and is consequently more probable than the all-engine IFSD event. The simulation results of safety are presented in Fig. 7 with different β-factors.

Fig. 7-a shows that the probability of a catastrophic failure of the propulsion system, due to consecutive IFSDs is extremely low. When the common-cause IFSDs are incorporated, the probability of catastrophic failure increases by several order of magnitude for all types of aircraft (Fig. 7-b). The probability of catastrophic failure increases further with the increase in the β-factor (Fig. 7-c).

Mission time has strong effect on the safety of two-engined aircraft, regardless of the diversion time. This effect is accelerated by the β-factor. This is due to the system size effect of common-cause failures. That is, the probability of all-engine failure due to a common-cause, such as bird strike, etc., for a system having fewer engines is higher than a system having more engines. Therefore, with the same common-cause IFSD, more catastrophic failures are expected to two-engined aircraft than three- and four-engined aircraft.

5 CONCLUSIONS

This study has shown the potential of a simulation approach as a useful tool for predicting system safety and reliability in the aircraft design process. The methodology that was developed accommodates common-cause failures as well as operational characteristics of an aircraft, without using any complex mathematical models. The significant impact of common-cause failures on system safety is demonstrated through the case study. Safety and reliability analysis of the propulsion system draws out the following conclusions:

1) The number of engines has a major impact on both safety and operational reliability.
2) Three-engines is a good choice for a long range aircraft from safety and operational reliability points of view.
3) Diversion time has a minor impact on both safety and operational reliability.
4) Common-cause failure is the most critical factor to the safety of aircraft and systems.

More accurate safety and reliability predictions may be made by improving aircraft operation models.

REFERENCES

[1] U.S. Department of Defense, *Reliability Modelling and Prediction*, US MIL-STD-756B, 18 November 1981.

[2] U.S. Nuclear Regulatory Commission, *Fault Tree Handbook*, NUREG-0497, January 1981.

[3] U.S. Deptartment of Transportation, FAA, *FAA Advisory Circular*, AC 120-42A, 30 December 1988.

[4] The Boeing Commercial Airplane Company, *An Overview of Propulsion System Risks: 1959 through 1989*, 1990

[5] K.N. Fleming, *A Reliability Model for Common Mode Failure in Redundant Safety Systems*, Proceedings of the Sixth Annual Pittsburgh Conference on Modelling and Simulation, General Atomic Report GA-A13284, April 23-25, 1975.

[6] The Boeing Commercial Airplane Company, *Statistical Summary of Commercial Jet Aircraft Accidents, World Wide Operations: 1959-1989.*

[7] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge, D. M. Rasmuson, *Procedure for Treating Common Cause Failures in Safety and Reliability Studies*, Pickard, Lowe and Garrick, Inc., EPRI NP-5613, prepared for Electric Power Research Institute, February 1988.

[8] C. L. Atwood, *Common Cause Fault Rates for Pumps*, NUREG/CR-2098, prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.

[9] E. E. Lewis, F. Bohm, *Monte Calro Simulation of Markov Unreliability Models*, Nuclear Engineering and Design, No 77, pp 49-62, 1984.

[10] G. W. Nam, *Development of Safety and Reliability Prediction Methodology for Aircraft Systems with Common-Cause Failures*, PhD Dissertation, College of Aeronautics, Cranfield University, 1996.

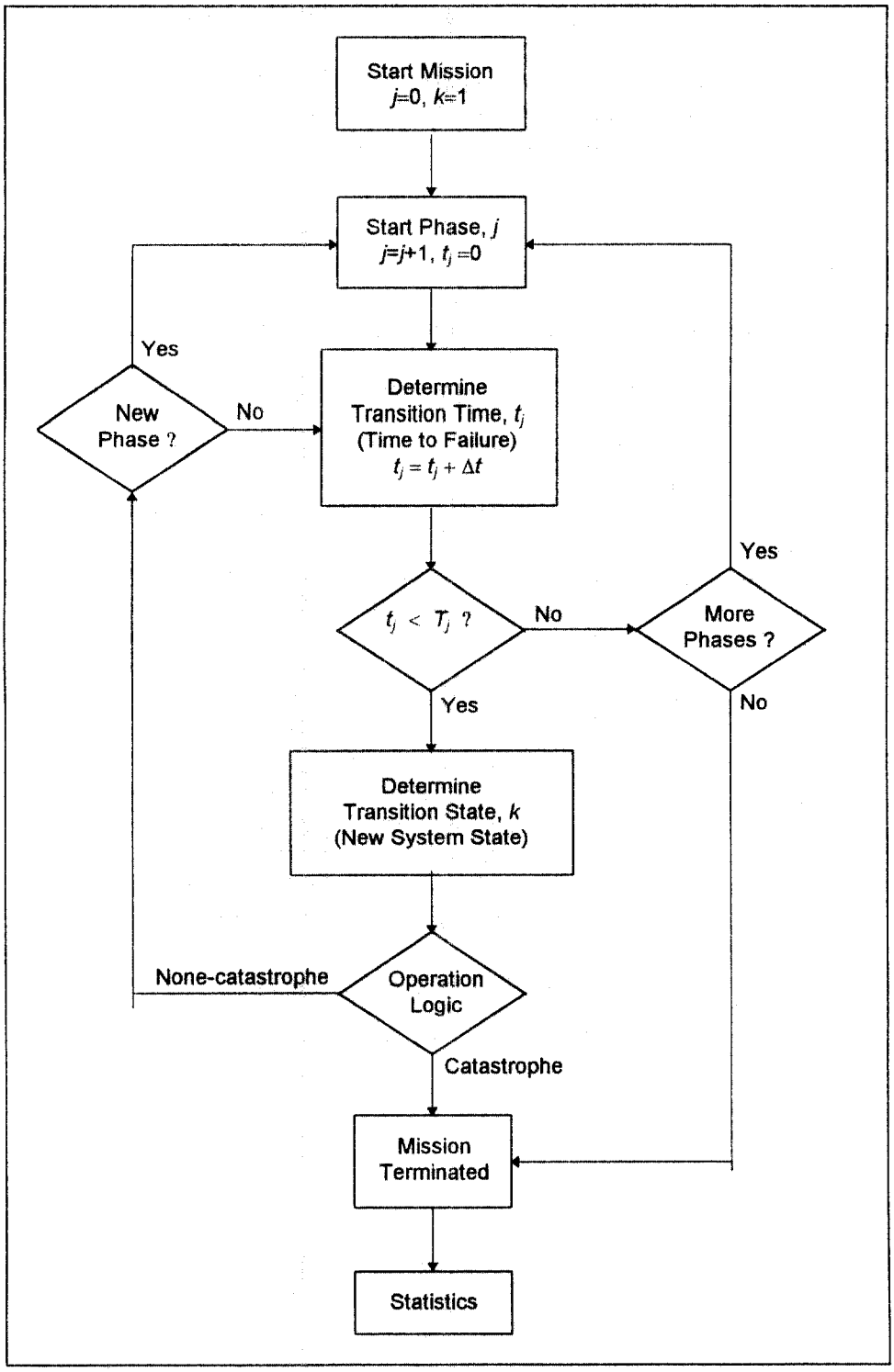
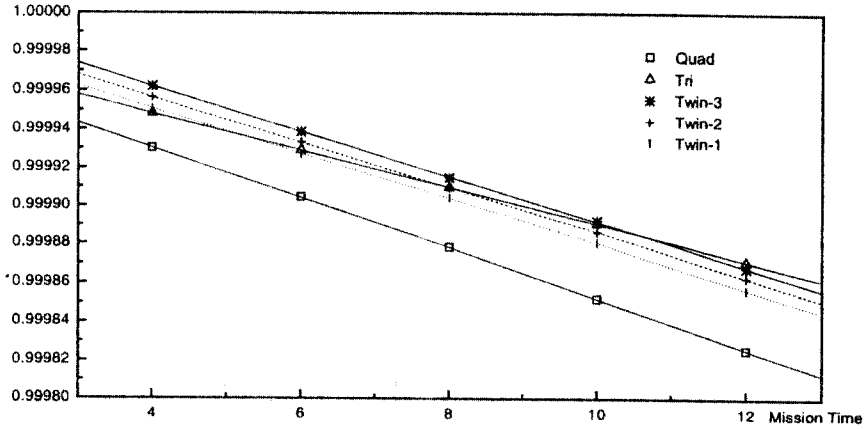
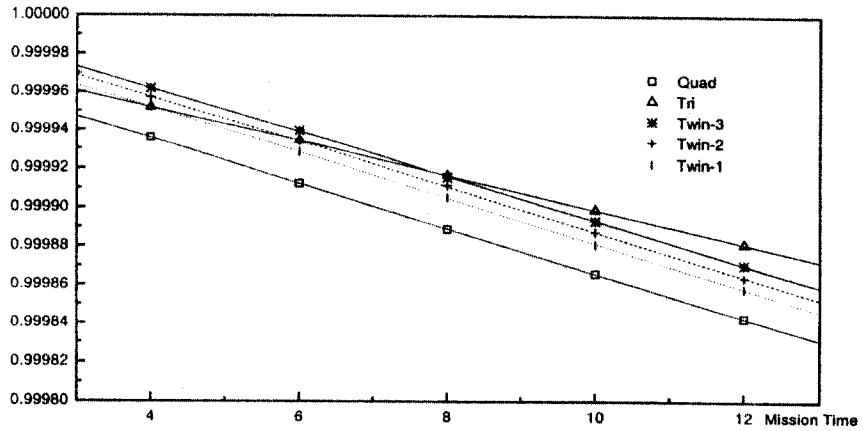


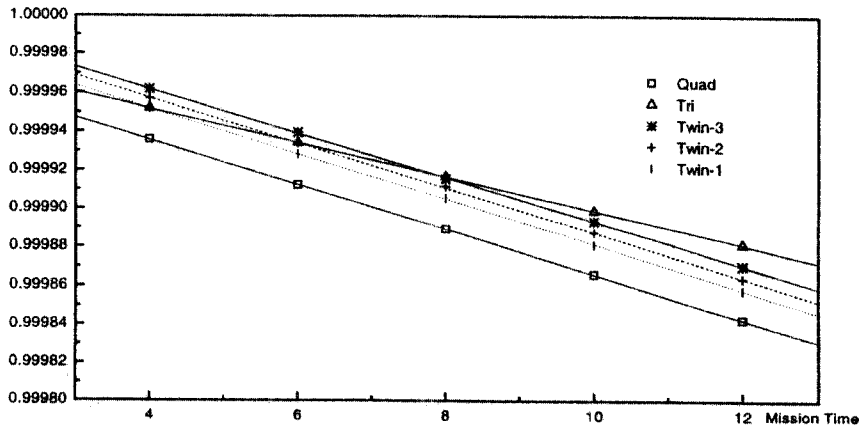
Figure 5 Procedure for Safety and Reliability Simulation



(a) IFSD Rate=0.015, Beta Factor=0.0

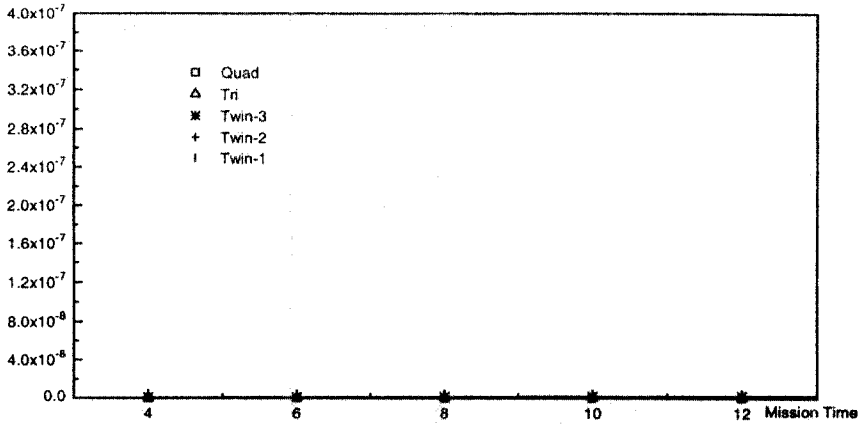


(b) IFSD Rate=0.015, Beta Factor=0.002

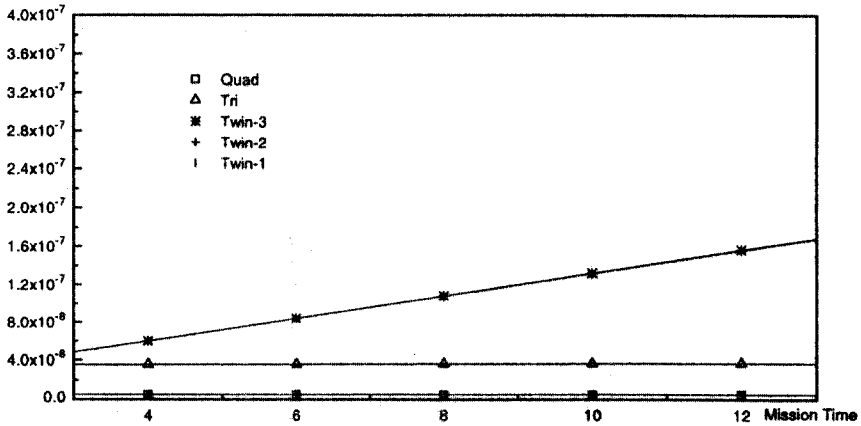


(c) IFSD Rate=0.015, Beta Factor=0.004

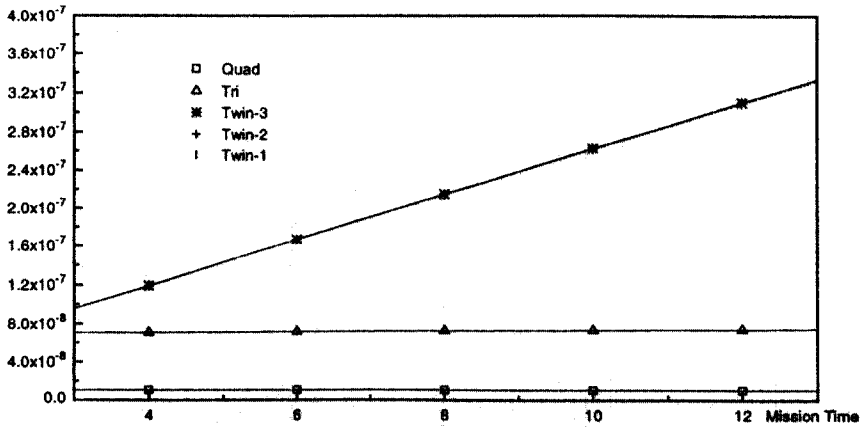
Figure 6 Operational Reliability



(a) IFSD Rate=0.015, Beta Factor=0.0



(b) IFSD Rate=0.015, Beta Factor=0.002



(c) IFSD Rate=0.015, Beta Factor=0.004

Figure 7 Probability of Catastrophic Failure