Aerobasics – An Introduction to Aeronautics

12. Safety in Aviation

S P Govinda Raju

S P Govinda Raju retired as professor from the Department of Aerospace Engineering, Indian Institute of Science in 2003. He is currently active as a consultant in wind tunnel testing and teaches short term courses in aerodynamics and flight mechanics.

Previous parts:
Resonance, Vol.13: p.836, p.971, p.1009, p.1107; Vol.14: p.19, p.191. p.272, p.328, p.650, p.916, p.1071.

Keywords
Safety level, notifiable accidents, Mean Time between Failures (MTBF), fail safety, engine failure, WAT curves, safe life.

Public awareness of airplane safety is very high due to the spectacular nature of airplane accidents. Partly as a result, civil airplane operations are tightly regulated at all levels from design to operation and maintenance. Scheduled airline operations have thus been able achieve a very high level of safety. In this article we quantify the safety of flight operations and indicate the design concepts like fail safety and safe life used in achieving a high level of safety. As an illustration, we consider the safety of a flight of a twin engine airplane in the event of one engine failure.

1. Introduction

Orville Wright flew a demonstration flight of his airplane in 1908 at Fort Myer (USA). His passenger was Lt. Thomas E Selfridge of the US army. The demonstration flight came to an abrupt end when the propeller of the airplane suffered a structural failure. The plane crashed from a height of about 125 feet. The passenger was killed and Orville suffered fractures. This was the first fatal accident in powered aviation. It highlights the fact that any technical problem on an airplane in flight can lead to very serious consequences. Airplane designers have always been conscious of this fact and devoted sufficient attention to make airplane flight as safe as possible.

In the years following the above accident, airplane technology developed rapidly. Airplane designers tried to enhance the safety of their designs by improving the reliability of the engines and other systems by various

methods. They introduced the concept of twin ignition systems (spark plugs and magnetos) to improve the reliability of piston engines of that era. As the engine could run normally on a single ignition system, failure of one ignition system in flight did not immediately disable the engine. As ignition systems of that period were very unreliable, this introduction of the concept of fail safety in ignition systems immediately reduced engine failures in flight. This concept is currently applied to many airplane systems and will be illustrated later in this section. In those days, failure of an engine in flight invariably led to a crash landing. As a further measure of safety in a crash landing, pilots started wearing crash helmets to escape head injuries on such occasions. This illustrates the second concept of containment of damage following a failure in flight and is currently applied to some airplane systems. For example, a structural failure on the rotor (like the failure of the compressor blades) of a jet engine in flight is prevented from damaging vital electrical, hydraulic and other systems on an airplane by making the engine casing strong enough to contain the damaged rotor. Similarly, fire extinguishers are provided in important areas for dealing with fire on board an airplane. As a further illustration, oxygen stored on board is made available to the passengers of a civil jet airplane in the event of loss of pressurization at cruise altitude. This literally provides breathing time (of about half an hour) to the passengers following the loss of airplane pressurization. The airplane can easily descend to a safe altitude within this time. In what follows, we quantify the concept of flight safety and illustrate it by an application to the specific case of one engine failure of a twin engine airplane. We shall be primarily concerned about safety of civil air transport operations.

As failures of airplane subsystems in flight will occur occasionally, safety of a flight is enhanced by the use of two concepts:
(a) redundancy of subsystems,
(b) containment of damage.

2. The Concept of Flight Safety

Flight safety is a statistical concept and is quantified in terms of accident rate. Accidents vary greatly in

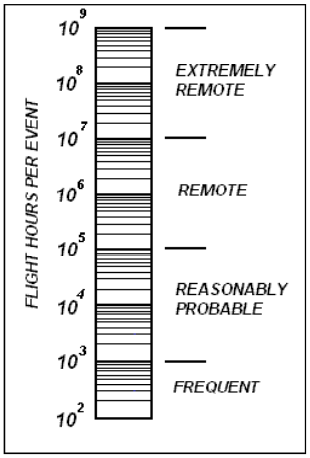


Figure 1. Scale of safety in aviation: Events having relevance to safety are generally compared on a logarithmic scale of flight hours per event as shown in the figure. Events are said to be frequent, reasonably probable, remote or extremely remote depending on their position on this scale. Major accidents are expected to be extremely remote with a frequency of occurrence of less than one in 10^7 flight hours.

severity and can be categorized as incidents and notifiable accidents. Incidents are minor events which affect or could affect the safety of airplane operations. An example would be the coming on of a fire warning indication during a flight. It may simply be a malfunction of the indicating system. Incidents are far more common than accidents. It appears that there are about 12 incidents for every accident in civil aviation.

According to the Indian Aircraft Rules, a notifiable accident is an event associated with a flight of an airplane in which any one of the following occur: (a) a person is seriously or fatally injured. (b) the airplane suffers serious damage or structural failure (c) the airplane is missing or completely inaccessible. Accidents are further classified according to the severity as (a) major notifiable accidents which exclude minor taxiing accidents and turbulence accidents involving no airplane damage, (b) fatal accidents which involve any fatality of persons on the ground or crew members and (c) major fatal accidents resulting in the death of one or more passengers. Major fatal accidents exclude those which involve only crew members or ground personnel as for example accidents during training flights. Major fatal accidents are rare and are in the range of a few per ten million flight hours.

Civil airplanes are designed to ensure a level of safety specified by the airworthiness authorities. In this context it is useful to define a safety scale as in *Figure* 1. In this figure, events on an airplane having relevance to safety are classified according to their frequency. Events can be considered frequent if they occur more often than once in a thousand flight hours. Events are considered reasonably probable if their frequency is one in 10^3 to 10^5 flights. They are considered remote if the frequency is in the range of one in 10^5 to 10^7 flights. Events are considered extremely remote if their frequency is less than one in 10^7 flights. As per current practice, civil

airplanes are to be so designed that major fatal accidents due to all causes are extremely remote on this scale. As design for safety often conflicts with economy of operations, a higher level then specified by airworthiness authorities is generally not attempted. Thus, during the certification of an airplane for civil operations, the manufacturer of an airplane has to demonstrate by calculation and tests that a fleet of airplanes when operated and maintained as per his recommendations will achieve the level of safety specified. However, accident statistics indicate that the actual safety of civil airplanes is slightly less than the design level. The actual level is to an extent dependent on the operator (airline). Statistical data from the carriers in the United States indicates for the last decade a frequency of fatal accidents of about 0.11 per million flight hours which is almost the design level. The frequency of accidents is much higher for airplanes in general aviation (for private airplanes) and for civil helicopters. *Figure* 2 compares the frequency of notifiable accidents of all these categories in the United States at the current time. The differences in safety levels are clear. It may be remarked here that the frequency of major fatal accidents is between five and ten times lower than for notifiable accidents.

Large civil airplanes are designed to achieve a level of safety better than one major accident in ten million flight hours.

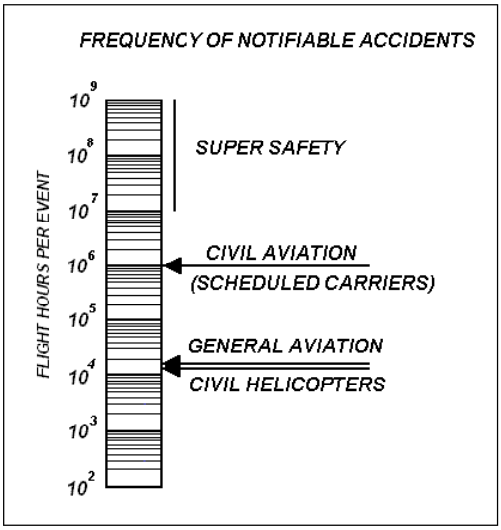


Figure 2. Actual safety levels achieved in aviation: Extensive statistical data is available regarding aircraft accidents. This data indicates that civil airplanes in scheduled operation have about one accident in a million flight hours. Not all accidents lead to passenger fatalities. Fatal accidents are less frequent. Only one in five accidents is fatal. Airplanes in general aviation (small private airplanes) and civil helicopters have a much higher accident rate of about one in 20,000 flight hours.

3. Design for Flight Safety

An airplane is a complex system having many subsystems each performing certain specific functions. One may consider the propulsion units, flight instrumentation, flight controls, structure including landing gears, passenger support systems and flight crew as major elements involved in the safe flight of an airplane. An accident can occur due to failure in any subsystem and it is for an airplane designer to ensure that a major fatal accident is extremely remote due to all possible failures on the airplane.

No subsystem on an airplane is perfect and this is indicated by an index of reliability associated with its operation. It is expressed as the mean time between failures (MTBF) of the subsystem. MTBF when expressed in hours is an indication of reciprocal of the frequency of failures of that subsystem in flight hours per failure. Thus it can be directly compared with the scale of safety of *Figure* 1. Experience indicates that many airplane subsystems have an MTBF of between 2000 and 40,000 hours and their failure in flight would be reasonably probable and is indicated in *Figure* 3. While

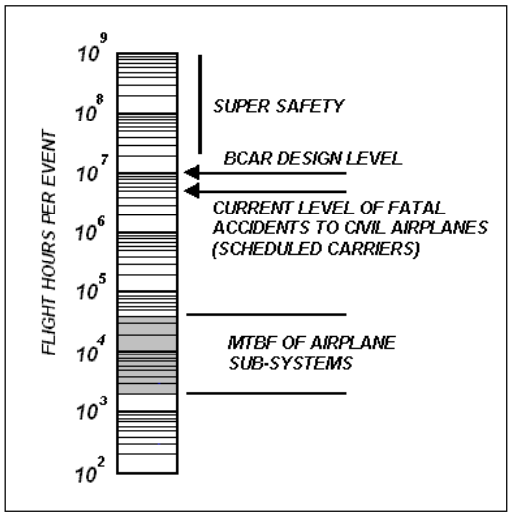


Figure 3. Failure rates of airplane subsystems: Many subsystems on an airplane fail on board once in 2,000 to 40,000 hours. If a single failure of any subsystem results in an accident, the desired level of safety corresponding to one accident in 10^7 flight hours cannot be achieved. Thus fail safety is an essential element of airplane subsystem design.

technical improvements enhance the MTBF of subsystems, it does not appear possible to increase the MTBFs on board an airplane so that subsystem failures are extremely remote.

Many airplane subsystems are designed to be fail safe. Fail safety implies that a single failure in any subsystem will not lead to an accident.

It is clear from the above that the design goal of major accidents being extremely remote cannot be met if every failure in a subsystem results in a major accident. Thus it is necessary to provide for fail safety in the various subsystems. The concept of fail safety implies that a single failure in any subsystem can be tolerated at least to the extent of safely completing a flight. A simple method of achieving this goal is to provide for two independent subsystems so that the flight can continue safely with only a single subsystem in operation. The probability of both subsystems failing together on a given flight (being the product of the probabilities of failures of each of the independent subsystems) can be seen to be extremely remote if the MTBF of each subsystem is about 3160 hours (square root of 10^7). This principle was first conceived in the context of ignition systems for airplane engines and is currently applied to a fair number of subsystems on an airplane. Increasing the number of subsystems involves cost and weight penalties and also increases the number of single subsystem failures on board. The concept is thus counterproductive beyond a point.

As illustrations of the above we may point out the following areas wherein fail safety is achieved by using redundancy in subsystems. Civil airplanes have at least two engines each with an electrical generator and a hydraulic pump to supply electric and hydraulic power for actuating flight instruments and flight controls. The control surfaces are often split into parts and each part is actuated separately. All the major flight instruments and controls are duplicated and are available for view or actuation from both the pilot's and the copilot's seat. On airplanes with fly-by-wire control systems, the main

Use of two engines will not guarantee safety in the event of an engine failure unless the airplane has adequate performance on a single operating engine.

flight control computer is a triplex or quadruplex unit with each computer supplied by an independent power source. Airplane landing gears employ more than one wheel on each leg. Fuel on airplanes is stored in many fuel tanks which are interconnected in such a manner that any fuel tank can supply any engine. Many emergency exits are available on airplanes for use in emergencies.

Mere duplication of a subsystem on an airplane does not constitute flight safety. It is necessary to demonstrate that failure in one subsystem will not lead to a major accident more often than once in 10^7 flights. We may illustrate this by considering the failure of one engine on a twin engine airplane during take-off.

4. Safety on Engine Failure in Flight

Engines that power aircraft are complex mechanism and they can suffer failure while powering the flight of an airplane. Piston engines of the earlier era had an in-flight failure rate of about one in a few thousand hours. On a single engine airplane, the failure of the engine in-flight leads to an accident rate which is the same as the engine failure rate. This being an unacceptably low level of safety, passenger carrying aircraft always had at least two engines so that the flight could be terminated safely with the power available from engine(s) still operating. Twin engine aircraft were and continue to be popular in civil aviation even though the engine failure rate in flight has come down substantially on current turbine engines to a level of about one in twenty to fifty thousand flights. Even this failure rate is inadequate to satisfy the airworthiness authorities who specify a higher safety level for civil aircraft (scheduled passenger carriers). Single engine airplanes are however permitted in general and military aviation where the lower level of safety is accepted.

An engine powering the flight of an airplane can fail during any phase of flight – take-off, climb, cruise or descent. The consequences of this failure will be different in different phases of flight, take-off being the most critical. During this phase, the engines of an airplane are operating at full power and under conditions of maximum thermal and mechanical stress. Should an engine fail during take-off, the airplane can abort the take-off or continue the take-off and reach a safe altitude and then come back and land. We shall consider this problem in some detail here.

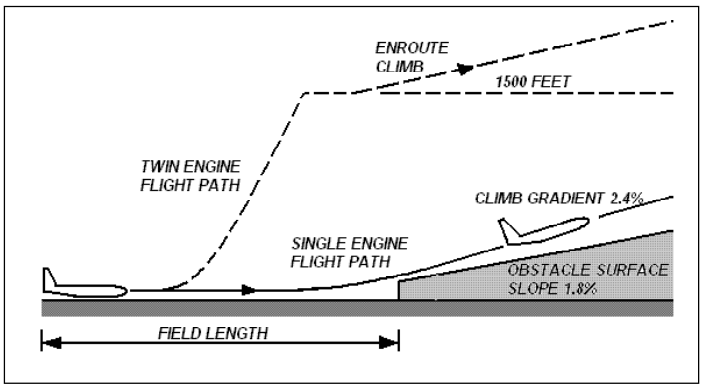
5. Single Engine Take-off

We first consider the normal take-off of a twin engine airplane from a certified airfield. The airplane loaded to a weight equal to or less than the maximum permitted for the particular airfield conditions (altitude and temperature) is positioned at the beginning of the runway. With brakes applied, the engines are raised to full power and then the brakes are released. The airplane accelerates on the runway until it reaches the take-off speed at which the pilot effects a take-off and the airplane climbs. The landing gears are retracted and the airplane climbs to about fifteen hundred feet before any changes in the airplane configuration (flaps) or engine power are effected. During the take-off run, the airplane uses only part of the runway length available and by the time the airplane flies over the end of the runway, it is way above the fifty feet level.

We next consider the possibility of one engine failure during the take-off phase of flight. After the engines are raised to full power at the beginning of the runway, an engine can fail at any instant. If the failure occurs close to the beginning of the runway, the pilot recognizes the failure and aborts the take-off by braking. The airplane will stop much before the end of the runway. If on the other hand, the engine fails when the airplane is close

to take-off speed, the airplane will have to continue the take-off on the other engine as it may not be possible to stop before the end of the runway. To meet this contingency, the power of the second engine is designed to be adequate for providing a climb gradient of 2.4% under these conditions provided that the airplane weight at take-off is restricted to a suitable value considering the airport altitude and temperature conditions. Thus the airplane after take-off will climb on the single engine at this gradient (or higher for a lower take-off weight). At this gradient the airplane flies about ten miles horizontally to reach an altitude of 1500 feet. In this region, the airworthiness authorities ensure that there are no obstacles like tall buildings, power lines, etc. in the path of the airplane. This is done by specifying that there shall be no obstacles within a surface extending from a point fifty feet in altitude at the end of runway and inclined to the horizontal at a gradient of 1.6 % as in *Figure* 4. Thus the airplane clears the obstacle surface by a gradient of 0.8 % on the average. This margin is an allowance for meeting statistical variations in airplane performance and piloting technique.

Figure 4. Airplane take-off following an engine failure. In a twin engine airplane, if an engine fails during take-off, safety of the flight depends on the following: (1) the airplane is able to stop before the end of the runway or (2) the airplane is able to continue the take-off and lift off before the end of the runway. After lift- off the airplane has to climb at a rate sufficient to clear the obstacle surface, reach an altitude of 1500 feet and then return for a landing. Thus the length of runway and performance of the airplane on one engine are critical.



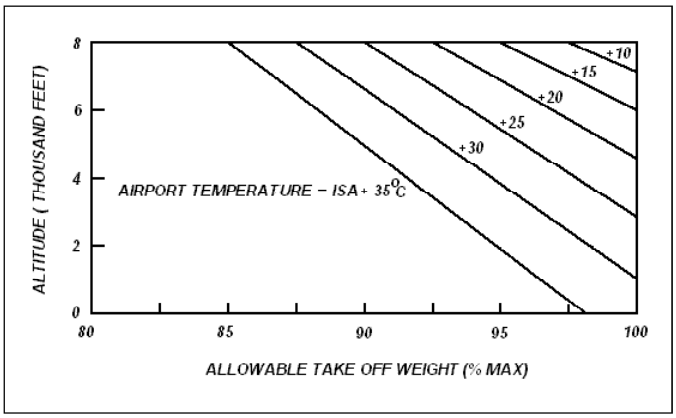


Figure 5. Allowable weight at take-off for an airplane: Every airplane is designed for adequate structural strength at its maximum take-off weight. However, on any given flight, the take-off weight may have to be restricted to a lower value to ensure adequate performance on one engine in the event of an engine failure (even though an engine failure is rare). In this figure, the allowable take-off weight of the airplane is indicated as a function of the altitude and temperature conditions of the take-off airfield. Particularly on hot and high airfields, the allowable take-off weight is significantly lower than the maximum take-off weight.

It will be clear from the above that for ensuring flight safety when an engine fails during take-off, two conditions need to be satisfied. The first pertains to the allowable weight of the aircraft at take-off for airfield conditions of altitude and temperature. This condition is met by establishing the allowable take-off weight by means of WAT (Weight–Altitude–Temperature) curves for the aircraft by flight tests and calculations. One such WAT curve is shown in *Figure* 5. It may be noted that WAT curves must be generated for all possible flap settings for a particular type of aircraft so that the allowable take-off weight applicable to a particular flight (altitude and temperature) can be selected from these curves depending on the flap setting used.

The second condition pertains to the length of the airfield required for take-off. From this point of view, the worst case corresponds to one engine failure as the airplane passes through the decision speed, V_2, lower than the take-off speed. At this speed, the pilot can shut the second engine, brake and stop or continue the take-off. In the first case, the airplane will stop just before the end of the runway. In the second case the airplane will lift off and reach an altitude of 50 feet above the runway surface at the end of the runway. The choice of the decision speed is such that the two alternatives need the same runway length. This runway length is called the

'balanced field length' and represents the minimum runway length for safe take-off when an engine fails. If an engine failure occurs before the decision speed, the pilot is advised to shut the second engine, apply the brakes and stop. If the failure occurs after the decision speed, the pilot is advised to continue the ground run, take-off and climb to 1500 feet, turn around, come back and land. It will be seen from the above that the balanced field length represents the minimum length of runway for safe operation of a civil twin engine airplane. Civil air operations are performed only from airfields larger than the balanced field length for any given type of airplane. Balanced field length for an airplane depends on the flap setting used for a take-off. Thus on a short runway, a larger flap setting (and the corresponding lower take-off weight) is appropriate.

It may be noted here that the weight of an airplane at take-off can only be reduced by reducing the disposable load (fuel, passengers or baggage). Thus on a hot day or from a high altitude airfield, take-off weight may have to be restricted to the allowable weight by restricting the number of passengers to less than the seats available. This affects the economy of the flight operation and is done as a last resort.

6. Safety of the Airplane Structure

The airplane structure which holds it together in flight is a major part of the airplane and constitutes about a quarter of its weight. The structure resists deformation due to various loads acting on it during a flight and can fail if the loads exceed its resisting capacity (strength) anytime during the complete life of an airplane which could reach up to about 30 years or 30,000 flight hours. The flight loads include those due to cabin pressurization, atmospheric gusts and flight maneuvers and are variable during flight. In the early days, the airplane structure was designed such that the structure

could with some margin for loss of strength due to repeated loading (fatigue) resist the maximum flight loads without significant deformation. The inadequacy of this design concept was dramatically demonstrated in the early 1950s when fuselage structures of Comet aircraft failed in flight only a short period after their introduction. From that time onwards structural failure due to fatigue has received much more attention and the design of airplane structures has included the concept of safe life. Safe life implies that the structure can resist the variable flight loads safely (without cracking) during the entire design life of the airplane. Structural elements without any redundancy like the landing gears are designed with this design concept. However universal application of this concept implies a large structural weight penalty and is unacceptable for the total structure. The concept of fail safety is used in the design of many structural elements in various forms. In this context fail safety does not imply a duplication of the structural element. It implies that a certain amount of damage can be tolerated in a flight structure due to redundancy of load paths. The structure is inspected and repaired before failure occurs in flight. This concept will be considered in some detail in the next part.

Suggested Reading

[1] **R H Howard, Planning for super safety: the fail-safe dimension, *The Aeronautical Journal*, Vol.104, No.1041, 2000.**

[2] **M R Ananthasayanam, R Narasimha and N Ramani, Airworthiness of aircraft. Part 2, Monte Carlo simulation of fleet performance history, *Proceedings of the Indian Academy of Sciences*, Vol.C1, No.4, 1978.**

[2] **Aeronautics Research Board, *The British Civil Airworthiness Requirements*, Civil Aviation Authority, UK, 1966.**

Address for Correspondence
S P Govinda Raju
Department of Aerospace Engineering
Indian Institute of Science
Bangalore 560 012, India.
Email: spg@aero.iisc.ernet.in