

9th May 2012

**COMMON CAUSE FAILURES,
PARTICULAR RISKS AND ZONAL SAFETY
ANALYSIS**



1 Common Cause Failures

Common Cause Failures are often the limiting factor on the integrity of complex systems, and yet they are often overlooked in the safety assessment process. In this module consideration is given to the various forms of Common Cause Failures that have the potential for compromising the reliability of aircraft systems and the possible methods for identifying them during the design process.

1.1 THEORY V PRACTICE

It is normally expected that if the probability of failure of one channel in a given period is X and there are N channels, any of which may achieve the intended function, then the probability of all channels failing is:

$$X^N \dots\dots\dots \text{Equation 1}$$

The impact of Common Cause Failures on an aircraft electrical power generation system was assessed from a study carried out by Hawker Siddeley Aviation in the 1970s. The study was carried out on an in-service aircraft that had three otherwise independent electrical power generation channels.

For this aircraft, the average failure rate for each of the channels was found to be approximately:

$$9.5 \times 10^{-4} \text{ per flight}$$

Now if the aircraft had only two electrical power generation channels then the probability of both failing due to independent causes might be expected to be :-

$$\begin{aligned} &(9.5 \times 10^{-4})^2 \text{ per flight} \\ &= 9 \times 10^{-7} \text{ per flight (approx.)} \end{aligned}$$

And for the three-channel system:

$$\begin{aligned} &(9.5 \times 10^{-4})^3 \text{ per flight} \\ &= 8.6 \times 10^{-10} \text{ per flight (approx.)} \end{aligned}$$

However, when the in-service record for the subject aircraft was investigated it was found that multi-channel failures occurred at a much greater frequency than predicted by this simple theoretical approach. A comparison between what might be expected if failures were totally independent and what was actually achieved on the in-service aircraft is illustrated in Figure 1. (The curve for the failure probability of the in-service aircraft has been adjusted to account for there being three ways in which two channels may fail in a three channel system.)

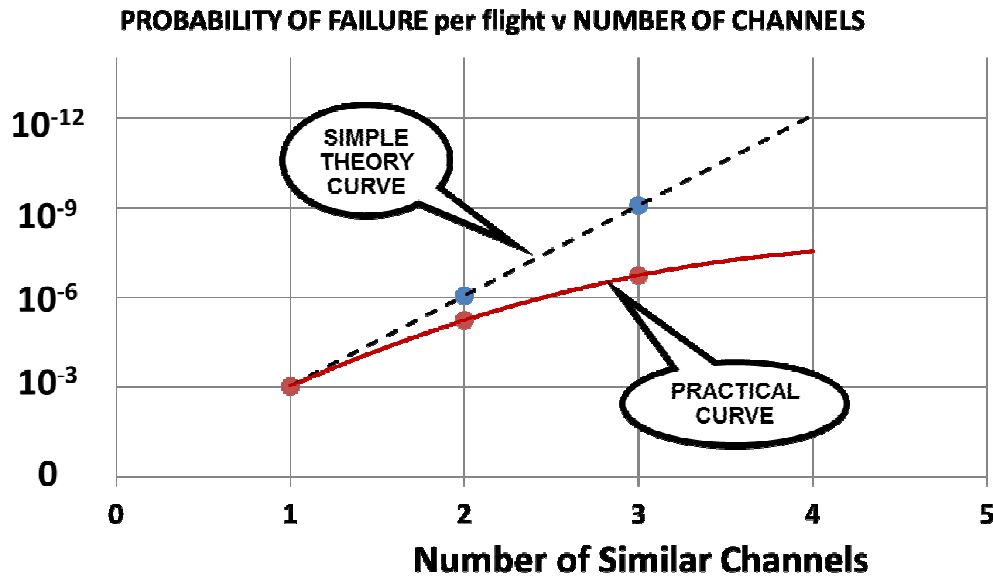


Figure 1 - Probability of Failure against number of channels for an aircraft electrical power generation system

It can be seen from Figure 1 that for the three-channel system the frequency of total system failure is several hundred times greater than the simple theory suggests. A further study carried out by Hawker Siddeley Aviation relating to hydraulic systems illustrated that the difference between the simple theory and what is actually achieved was also exhibited by aircraft hydraulic systems as illustrated in Figure 2.

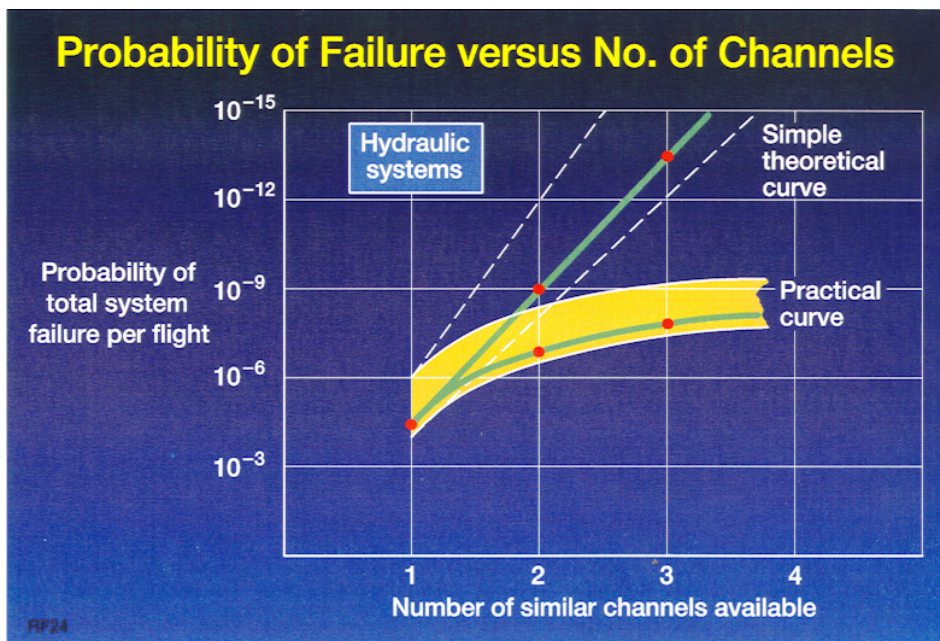


Figure 2 - Probability of Failure against number of channels for aircraft hydraulic systems

This marked difference between the simple theory prediction, and what is actually achieved in terms of the probability of multiple system failures, is likely to be exhibited in other, probably all, multi-channel aircraft systems.

The simple theory expressed in Equation 1 is predicated on there being no significant dormancies in the system. However, in most complex systems there could be a number of faults that are not normally detected until system checks are carried out during maintenance. The system designer needs to concentrate on arranging the system architecture to reduce the number of dormant faults; those remaining require a maintenance check set at an interval such that their probability of occurrence, in combination with other failures, is to an acceptable level.

However, the primary reason for the differences between the simple theoretical curve and the practical curve shown in Figure 1 is that channel failures are not totally independent and that Common Cause Failures have a significant influence on the probability of total system failure actually achieved.

Following their identification, consideration should be given to design changes, manufacturing techniques, maintenance actions and system operating procedures to eliminate or mitigate Common Cause Failures. Whilst not an exhaustive list, the foregoing sections address some of the most frequently occurring Common Cause Failures that may present a “threat” to most aircraft types. Those external to the system may be caused by a variety of occurrences, many of which are known as Particular Risks.

1.2 COMMON MODE FAILURES

The simple theory of multi-channel failure is predicated on failure independence amongst the channels. However, in order to optimise the design most multi-channel systems will have similar components. These similar components will have similar failure modes known as Common Mode Failures. Manufacturing or design faults resulting in high early life failure rates can have a pronounced effect on the probability of total system failure. A similar situation arises from “wear-out” failures.

Consider a component in a two-channel system exhibiting the failure rate characteristics shown in Figure 3.

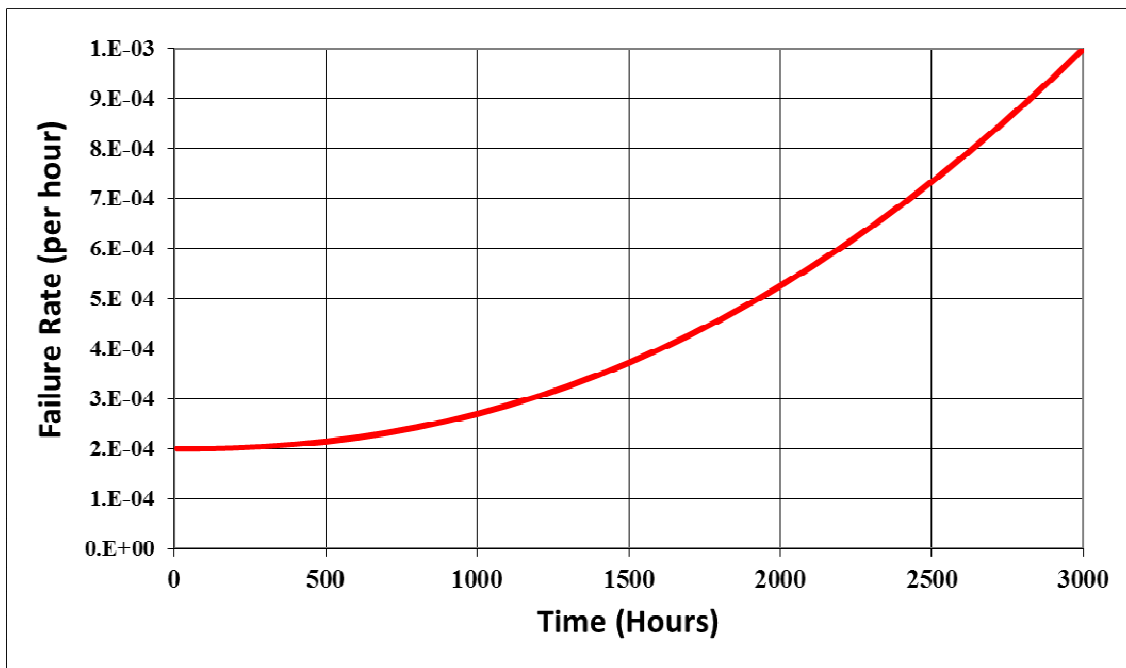


Figure 3 - Component exhibiting “wear-out” characteristics

When the aircraft first enters service, the component has a failure rate that is approximately 2×10^{-4} per hour. However, if the component survives in both of the channels for 3,000 hours their failure rates increase to approximately 1×10^{-3} per hour. For an aircraft that has an average flight time of one hour the probability of both channels failing due to this component, when the aircraft first enters service, is approximately $(2 \times 10^{-4})^2$ - equal to 4×10^{-8} per hour.

However after the aircraft has been in service for 3,000 hours the probability of both channels failing due to this component is approximately $= (1 \times 10^{-3})^2$ equal to 1×10^{-6} per hour. Hence, the probability of both channels failing due to this component has increased by a factor of **25**. A similar situation exists if the component exhibits an infant mortality failure rate characteristic, perhaps resulting from manufacturing or maintenance induced defects.

Another frequent form of Common Mode Failure is mal-assembly or mal-rigging of similar equipment in multi-channel systems. Despite the precautions taken to

prevent failures occurring due to errors of this kind, they still present a significant risk to the integrity of vital aircraft systems.

On an aircraft test flight inadvertent operation of the stall recovery system occurred just after take-off due to the incorrect rigging of the microswitches on the leading edge slat. The two microswitches were in each of two channels in the stall recovery system. The mal-rigging of both microswitches resulted in the stall recovery system being in the slats retracted mode, which at take-off speed resulted in stick pusher operation.

Of course, dissimilar redundancy can sometimes alleviate the “threat” from Common Mode Failures. The BAe 146 Electrical Power Generation System represents a good illustration of the way in which dissimilar redundancy may be used to good effect. It has two engine-driven generators, one Auxiliary Power Unit (APU) driven generator, an hydraulically driven generator and a battery. This degree of dissimilar redundancy provides a good measure of protection against Common Mode Failures.

However, this approach is not always practical since systems are designed to optimise the exacting requirements demanded of them. Therefore, any variation in this standard must result in penalties in terms of performance, weight, cost, operational reliability or any other of the design parameters. In most cases, the designer is forced to use similar equipment on all system channels, and must rely on close attention to the design, maintenance checks and operating procedures in order to achieve the levels of integrity required.

1.3 CASCADE FAILURES

Most multi-channel systems are designed so that under normal operating conditions they share the total system demands. It therefore follows that failure of a single channel will usually result in the remaining channels taking an increased load. This increase in load almost invariably produces a consequential increase in failure probability.

Although cascade failures of this type are readily understood for structural components, they are not often expected in electrical systems.

Multi-channel electrical systems are usually designed so that any one channel is capable of meeting the requirements of essential services. However, following a channel failure the increase in load on the other channels is likely to result in an increase in their probability of failure.

Attempts have been made to quantify the relationship between load and failure rate for electrical components - the results of this work are contained in MIL-HDBK-217 "Reliability Prediction of Electronic Equipment." Figure 4 shows the relationship between failure rate and load for a 125 VA transformer using the data from MIL-HDBK-217. It may be seen that for this particular component there is a marked difference between the predicted failure rate at rated power, 125 VA, and half-rated power. Most components will demonstrate an adverse relationship between failure rate and load, although not necessarily as severe as the example shown in Figure 4.

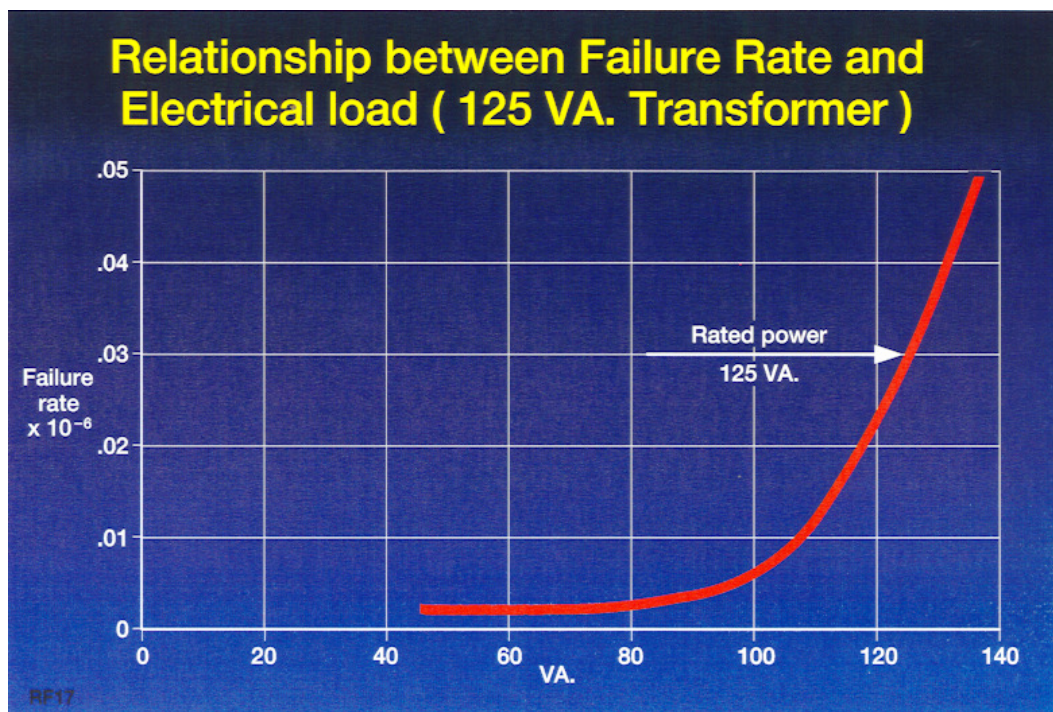


Figure 4 Relationship between Failure rate and Electrical Load for a 125 VA Transformer

Assuming that the failure rate of two similar components in a dual channel system is unaffected by any changes in load the probability of total system failure is given by the following expression:

$$\lambda_1 \lambda_2 t^2 \text{ per flight}$$

Where **t** is the flight time in hours and the failure rates are on a per hour basis.

However, if the system is prone to Cascade Failures this expression becomes:

$$\lambda_1 \lambda_2 m t^2 \text{ per flight}$$

Where **m** is the magnitude of the change in component failure rate due to the increased load.

It is not known whether data of this nature is available for non-electrical systems. However, it is evident that an adverse relationship between load and failure rate is likely to exist for hydro-mechanical systems, where component failures can adversely affect the duty cycle experienced by the surviving components.

1.4 SINGLE ELEMENT FAILURES

Almost without exception, all multi-channel systems have a "single element" - failure of which could result in total system loss. Although in most cases this single element is readily identifiable, this is not always the case.

Considering the system shown in Figure 5, the circuit has been duplicated upstream of the actuator terminal block in order to improve the reliability of operation. However, any single short circuit in the system, loss of the earth, busbar failure, or disconnect of the power supply to the actuator will result in loss of the entire system. The probability of this occurrence is likely to be significantly greater than that of independent failures in the two relay channels.

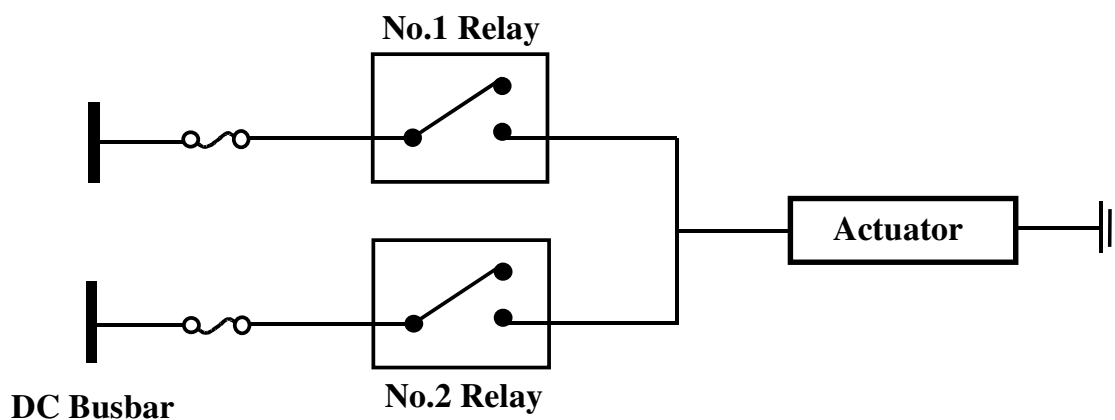


Figure 5 Electrical System Single Element Failures

Of course, in practice, the effects of short circuits would be limited by the addition of diodes, but this does have the disadvantage of increasing the potential for failure in the system.

This type of multi-channel failure is not restricted to electrical systems and similar failures can be found in both mechanical and fluid systems. Mechanical flying control systems are often duplicated in areas where failures could produce critical effects on aircraft safety. However, when the failure causes of single element systems are analysed, it becomes evident that in certain instances their resultant effect would have been the same even when duplicated systems are employed. An example of this is illustrated by the flying control system failure that resulted from the cable being incorrectly routed around a structural element of the system. This remained undetected until the continual movement of the cable over this area caused fraying and subsequent fracture of the cable. It is not difficult to imagine that even if the cables were duplicated, the failure would still have occurred. They would probably have both been incorrectly routed and this would not have been detected until both cables had frayed.

An incident occurred on an in-service aircraft when due to mal-assembly of a flying control, servo loads were induced into the structure such that fracture occurred of the jack attachment. The jack was assembled so that there was a restriction to fluid flow. This mal-assembly was not detected during the checks, carried out on the jack, following overhaul. When fitted to the aircraft the high flow rates demanded of the faulty servo by the adjacent units resulted in a build-up of pressure in the jack significantly beyond the normal levels. The loads produced by these pressures were sufficient to cause failure of the jack attachment point. Fortunately, in this instance the weakest structural member of the system was not a single element but the independent jack attachment points, however if the resultant structural failure had occurred closer to the flying control surface the resultant effect could have been more serious.

A further example of a "single element" mechanical failure may be found in cases where structural deformation has resulted in flying control mechanisms being restricted in movement. The designer would ensure that flying controls were not impeded by any structural movements likely to be encountered over the normal flight envelope. However, the cases where permanent structural deformation, due to rapid cabin decompressions, have resulted in restricted authority over the primary flying controls, are only too well known. The following accident is an example of such an occurrence:

On 3-Mar-1974 a Turkish Airlines DC-10-10 registered as TC-JAV departed Orly airport, Paris, France. The aft cargo door on the left-hand side was not latched properly. The accident was the result of the ejection in flight of the aft cargo door on the left-hand side. The sudden depressurisation which followed led to the disruption of the floor structure, causing six passengers and parts of the aircraft to be ejected, rendering No. 2 engine inoperative and impairing the flight controls (tail surfaces) so that it was impossible for the crew to regain control of the aircraft.

The aircraft literally disintegrated on the subsequent impact at very high speed in a forest.

Of the 12 crew and 334 passengers on board, all occupants suffered fatal injuries.

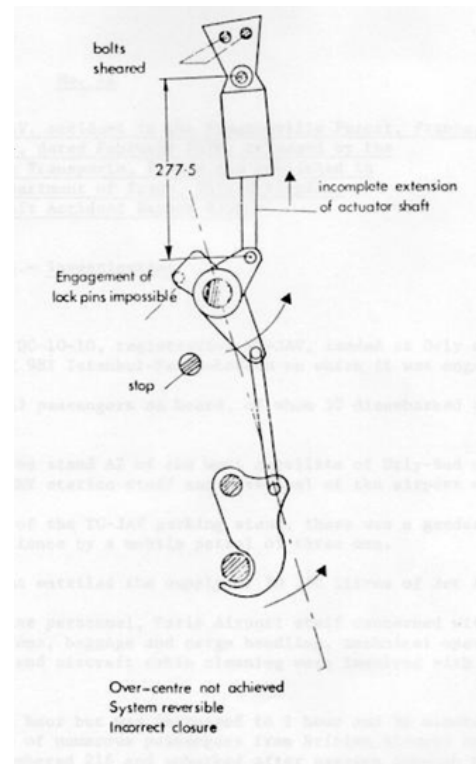


Figure 6 DC 10-10 Door Locking Mechanism

The following account of a fatal accident to a MD-83 aircraft illustrates another example of a single element mechanical failure:

On January 31, 2000, about 1621 Pacific standard time, Alaska Airlines, Inc., flight 261, a McDonnell Douglas MD-83, N963AS, crashed into the Pacific Ocean about 2.7 miles north of Anacapa Island, California. The 2 pilots, 3 cabin crewmembers, and 83 passengers on board were killed, and the airplane was destroyed by impact forces.

The NTSB determines that the probable cause of this accident was a loss of airplane pitch control resulting from the in-flight failure of the horizontal stabilizer trim system jackscrew assembly's acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airlines' insufficient lubrication of the jackscrew assembly.



Figure 7 MD-83 horizontal stabilizer trim system jackscrew

Failures of this kind are not restricted to faults of components required for the functioning of the system, but may also involve indicating systems. An incident occurred to an aircraft when the flight crew tripped all generation channels because the frequency was out of tolerance. It was later discovered that the frequency meter, which was used for all generation channels, was faulty.

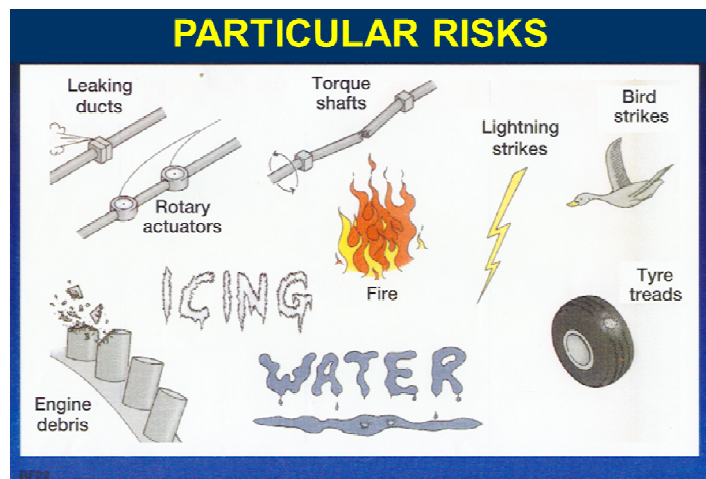
2 Particular Risks

Particular risks are defined as those events or influences, which are outside the systems concerned. Examples are fire, leaking fluids, bird strike, tire burst, high intensity radiated fields exposure, lightning, uncontained failure of high energy rotating machines, etc. Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects or influences, which may violate independence. AMC 25.1309

Whilst some Particular Risks will not necessarily result in a Common Cause Failure, they need to be considered in any Common Cause Analysis, since they often have the potential to compromise multichannel systems.

The following list is not considered to be exhaustive and consideration may need to be given to other Particular Risks that could affect system integrity or aircraft safety.

- Released Debris from high energy rotating devices (including Engine Non Containment)
- Released Debris from pressurised vessels
- High Pressure Air Duct Rupture
- High Temperature Air Duct Rupture
- Tyre Debris
- Flailing Tyre Tread
- Flailing Shafts
- Wheel Debris
- Runway Debris
- Fire
- Leaking Fluids
 - Fuel
 - Hydraulic Oil
 - Battery Acid
 - Water
- Bird Strike
- Hail, Ice, Snow
- Lightning Strike
- Electromagnetic Interference
- High Intensity Radiated Fields



The following sections address some of the more significant Particular Risks in greater detail.

2.1 BIRD STRIKES

The EASA CS-25 requirements relating to bird strike damage state:

CS 25.631

"The aeroplane must be designed to assure capability of continued safe flight and landing of the aeroplane after impact with a 4 lb bird when the velocity of the aeroplane (relative to the bird along the aeroplane's flight path) is equal to V_C at sea level or $0.85 V_C$ at 2438 m (8000 ft), whichever is the more critical."

AMC 25.631

"Consideration should be given in the early stages of the design to the installation of items in essential services, such as control system components, and items which, if damaged, could cause a hazard, such as electrical equipment. As far as practicable, such items should not be installed immediately behind areas liable to be struck by birds."

Throughout design, attention is directed towards routing of systems such that a single bird strike does not result in failure of vital systems. However, difficulties may be encountered when assessing probabilities of bird strikes to the airframe, since there are many factors affecting the probability of a strike. These factors include aircraft speed, altitude, angle of attack, airfield location, time of day, time of year, local air traffic density, airfield bird preventative measures, size of bird, etc.

However, from an analysis of in-service records, it appears that bird strikes to aircraft operating in Europe occur, on average, at the rate of 3.5 per 10,000 movements. Less than 1% of strikes involve birds greater than 4 lb. and approximately 85% occur below 8000 feet. However, current studies suggest that the incidence of strikes from larger birds, and in particular Whistling Swans, has increased over recent years.

Based on a study carried out by the UK CAA, published in 1982, the distribution of bird strikes by height above ground level is as illustrated in Figure 8.

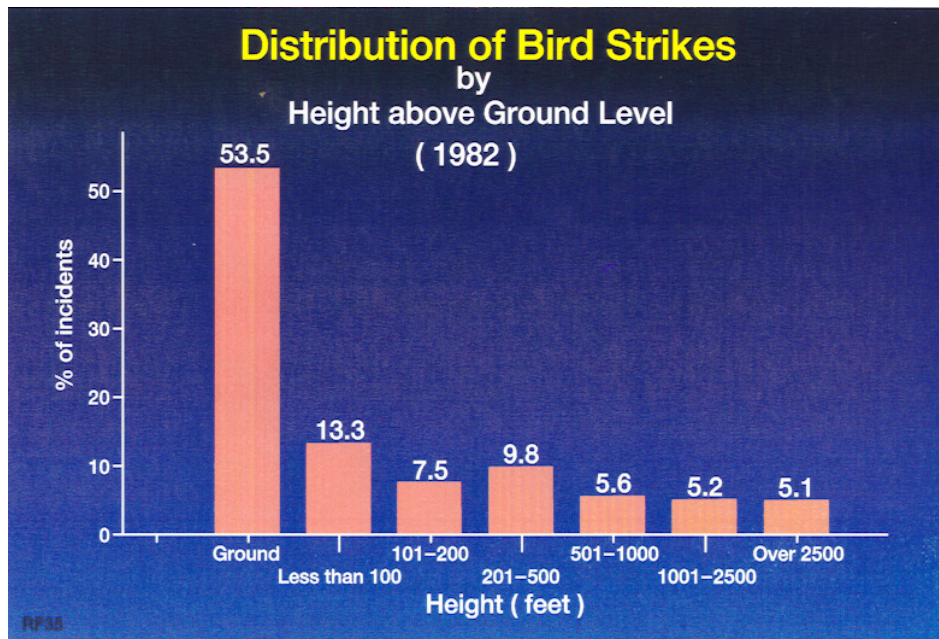


Figure 8 - UK Distribution of Bird Strikes by height above ground level

These statistics help in giving guidance to the designer but they must be used with caution since they represent average values under limited conditions.

Bird strikes are a classic example of events that are not independent. Since birds tend to congregate in flocks, there is a risk that even segregated multi-channelled systems could sustain critical damage due to strikes by more than one bird. Flocks of birds are a very significant form of Common Cause Failure, and have resulted in many instances of multiengine flameouts.

The following account of an accident to a Boeing 737 aircraft illustrates the potential that bird strikes have to cause failure of aircraft critical systems:

“On Sunday 28 November 2004, a Boeing 737-400, suffered a bird strike in the area of the nose landing gear during rotation. The investigation determined that the accident probably happened because during the take-off a bird strike broke one of the cables of the nose wheel steering system of the aircraft and jammed the other, which made that the nose wheels were rotated to the left when they touched down during landing, causing a veering to the left that could not be arrested by full rudder deflection as the aircraft decelerated. The aircraft suffered major damage. There were no serious or fatal injuries to the occupants.”

2.2 TYRE DEBRIS

Other potential environmental hazards to multi-channel systems, for example, torque shaft fractures and tyre tread shedding, are considered during the design stage by means of the "Zonal Safety Analysis." Most Failure Analyses techniques consider each system in isolation; however, one of the purposes of a Zonal Safety Analysis is to consider the interaction of different systems. For example, the fracture of a flap torque tube may result in secondary damage to adjacent electrical cables, flying controls or hydraulic pipes due to flailing of the failed shaft.

In a similar way, equipment located in proximity to the undercarriage may be damaged by the shedding or bursting of a tyre tread. Once the failure cases have been identified, the appropriate corrective action should be taken to eliminate them where practicable. However in some instances it is not feasible to totally isolate critical system's components from potential tyre debris areas and an assessment of the risk level may be made using a similar technique to that used for engine debris. The following tyre-debris model is typical of that used for risk assessment:

Debris Size & Mass taken as a piece of the tyre with dimensions appropriate to a square with sides equal to the width of the tyre. (Based on data from actual in service tyre tread incidents and also corresponds to the size suggested in early standards of FAR 33)

Speed taken as a typical landing/take-off speed

Point of Release assumed that the probability is constant for any point on the circumference not in contact with the ground

Trajectory is taken as being 10° from the vertical, either side of the tyre, at a point emanating from the ground/tyre contact point for a deflated tyre. (Based on dynamometer test results)

It is evident that tyre debris models should be aircraft specific to accommodate for such factors as varying speeds and tyre debris sizes. One aircraft manufacturer assumes a maximum debris size of up to 3 kilograms and a trajectory of $\pm 15^\circ$ - approximating to a Gaussian distribution.

2.3 ENGINE NON-CONTAINMENT

Despite the stringent requirements, and the steps taken by manufacturers, there is a risk on all turbine engines of disc or blade failures resulting in high-energy debris being ejected through the engine casing. In some instances, this debris has sufficient energy to cause secondary damage to the aircraft systems and structure.

The airframe systems designer must do all that he can to segregate vital multi-channel systems in order to minimise the risk of total system failures from single pieces of engine debris.

Experience to date suggests that debris is ejected from engines at the rate of approximately one incident every million flying hours. Fortunately, the vast majority of incidents have not resulted in a catastrophe. However, the risk of this occurrence must be relatively high and in order to maintain an adequate level of safety, it is essential that the design engineer carries out a detailed assessment of the vulnerability of the aircraft and its systems to engine debris. Special attention is directed towards failures that could have hazardous or catastrophic effects.

2.3.1 Accident Experience

Examples of the degree of damage that can be sustained by the aircraft and its systems due to engine non-containment are illustrated by the following accidents:

Albuquerque DC-10-10

"On 3-Nov-1973 a National Airlines DC-10-10 registered as N60NA was operating as a scheduled passenger flight between Miami, Florida and San Francisco, California, with intermediate stops at New Orleans, Louisiana, Houston Texas and Las Vegas, Nevada.

While cruising at 39,000 feet 65 nautical miles south-west of Albuquerque, New Mexico, the number 3 engine fan assembly disintegrated and its fragments penetrated the fuselage, the number 1 and 2 engine nacelles and the right wing.

The resultant damage caused decompression of the aircraft cabin and the loss of certain electrical and hydraulic services. One cabin window, which was struck by a fragment of the fan assembly, separated from the fuselage and the passenger who was sitting next to that window was forced through the opening and ejected from the aircraft.

The flightcrew initiated an emergency descent and the aircraft was landed safely at Albuquerque International Airport 19 minutes after the engine failed. The 115 passengers and 12 crewmembers exited the aircraft by using the emergency slides.

The aircraft was damaged substantially.

Of the 12 crew and 116 passengers on board, 1 passenger suffered fatal injuries as a result of being ejected from the aircraft. 4 crew and 20 passengers were treated for smoke inhalation, ear problems and minor abrasions."

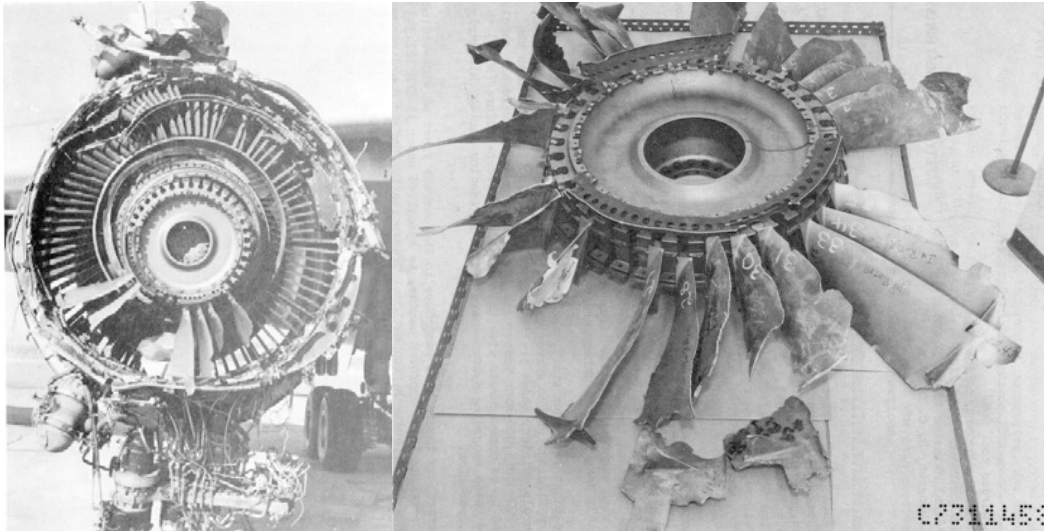


Figure 9 - Albuquerque DC-10-10 November 1973 - Number 3 engine fan assembly

Sioux City DC-10-10

"On July 19, 1989, at 1516, a DC-10-10, N1819U, operated by United Airlines as flight 232, experienced a catastrophic failure of the No. 2 tail mounted engine during cruise flight.

The separation, fragmentation and forceful discharge of stage 1 fan rotor assembly parts from the No. 2 engine led to the loss of the three hydraulic systems that powered the aeroplane's flight controls. An off duty check airman assisted the crew by controlling the aircraft using only the engine power levers. The aeroplane touched down on the threshold slightly to the left of the centerline on runway 22 at 1600. First ground contact was made by the right wing tip followed by the right main landing gear. The aeroplane skidded to the right of the runway and rolled to an inverted position. Witnesses observed the aeroplane ignite and cartwheel, coming to rest after crossing runway 17/35. Firefighting and rescue operations began immediately, but the aeroplane was destroyed by impact and fire.

There were 285 passengers and 11 crewmembers onboard. One flight attendant and 110 passengers were fatally injured."

Brisbane 727

"At 0707 hours, on 4 July 1992, Boeing 727-277 aircraft VH-ANA took off from runway 01 at Brisbane Airport on a regular public transport flight to Sydney. As the landing gear was retracting, the

crew heard a loud bang emanate from the rear of the aircraft. This was followed by cockpit indications of a fire in, and a loss of thrust from, the no. 2 (centre) engine. Ground witnesses saw large flames streaming from the rear of the aircraft. The crew shut down the engine, completed the engine-fire checklist; and flew a circuit for a landing on runway 01.

During the landing roll, the crew were advised that there were still signs of fire around the centre engine, so a decision was taken by the aircraft captain to evacuate the aircraft. During the evacuation, two passengers received minor injuries. The fire was extinguished quickly by airport fire personnel.

The investigation revealed that a fatigue failure had occurred in the first-stage compressor fan disc of the no. 2 engine leading to disruption of the engine. The fire resulted when a section of engine disc severed the main fuel line to the engine. Deficiencies were also revealed in the Brisbane Airport emergency plan and in some aspects of the training of rescue and firefighting personnel. Of the 9 crew and 96 passengers aboard, two passengers received minor injuries during the evacuation of the aircraft.”

Atlanta DC-9

“On 08-Jun-1995 a ValuJet DC-9-32 registered as N908VJ was taking off from the William B. Hartsfield Atlanta International Airport, Atlanta, Georgia. As the aircraft began its takeoff roll, a loud "bang" was heard by the aircraft occupants and air traffic control personnel. The right engine fire warning light illuminated. The flight crew of a following aircraft reported to the ValuJet crew that the right engine was on fire and the takeoff was rejected. Shrapnel from the right engine penetrated the fuselage and the right engine main fuel line and a cabin fire erupted. The aircraft's fuselage was destroyed. There were 5 crew and 57 passengers on board. 1 flight attendant suffered serious injuries. Another flight attendant and 5 passengers suffered minor injuries.”



Figure 10 - Atlanta DC-9

Pensacola MD-88

“On 6-Jul-1996 a Delta Air Lines MD-88 registered as N927DA was taking off from the Pensacola Regional Airport, Pensacola, Florida and was destined for Hartsfield Atlanta International Airport in Atlanta, Georgia.

During the initial part of its takeoff roll, the aircraft experienced an engine failure. Uncontained engine debris from the front compressor front hub (fan hub) of the left engine penetrated the left aft fuselage. The takeoff was rejected and the aircraft stopped on the runway.

There were 5 crew and 137 passengers on board. 2 passengers suffered fatal injuries. 2 passengers suffered serious injuries. 5 crew and 133 passengers escaped with minor or no injuries.”



Figure 11 - Pensacola MD-88

2.3.2 The Airworthiness Requirements

CS/FAR 25.903 (d) states:

*“Turbine engine installations. For turbine engine installations-
Design precautions must be taken to minimise the hazards to the
aeroplane in the event of an engine rotor failure.....”*

*{N.B. As with any requirement a check should be made with the
Authorities on their current policy as to their interpretation}*

It should be noted that the prime requirement is to minimise the risk. As with all areas of safety analysis, the practical engineering aspects must take precedence over any probabilistic justification of the design and hence all practical design precautions must be taken to minimise the risk. These may include:

- Locating critical equipment outside of the debris zone
- Duplication and adequate separation of critical components
- Protection by substantial airframe structure etc.

In certain instances this may not be completely feasible and, in order to determine that the risk is kept to an acceptable level, assessments are made of the probability of “critical strikes” by engine debris.

This involves the use of an “Engine Debris Model”.

2.3.3 Proposed Engine Debris Model

The suggested engine debris model is described in AMC 20-128A. However, alternate models may be used for a particular engine where this can be justified by particular design features or in-service data particular to the engine.

Table 1 shows the primary characteristics to be considered for the engine debris suggested in AMC 20-128A. It should be noted that the information relating to mass and energy is only pertinent when prior agreement with the Authorities has been obtained to take energy considerations into account.

Table 1 Engine Debris Size

	Maximum Dimension	Angular Spread	Mass	Energy
<i>Single one third disc fragment</i>	One third of the disc with one third blade height	$\pm 3^\circ$	One third of the bladed disc mass	Translational
<i>Intermediate fragment</i>	One third of the bladed disc radius	$\pm 5^\circ$	One thirtieth of the bladed disc mass	Translational
<i>Multiple small fragment except Fan</i>	Half of Blade Aerofoil	$\pm 15^\circ$	Half of Blade Aerofoil	Consult with the engine manufacturer
<i>Fan Blade fragment</i>	One third of Blade Aerofoil	$\pm 15^\circ$	One third of Blade Aerofoil	Translational

SSA COURSE MASTER 3 DAY (23)/DEBRIS DATA

The one third and intermediate fragment sizes are shown diagrammatically in Figure 12 and Figure 13.

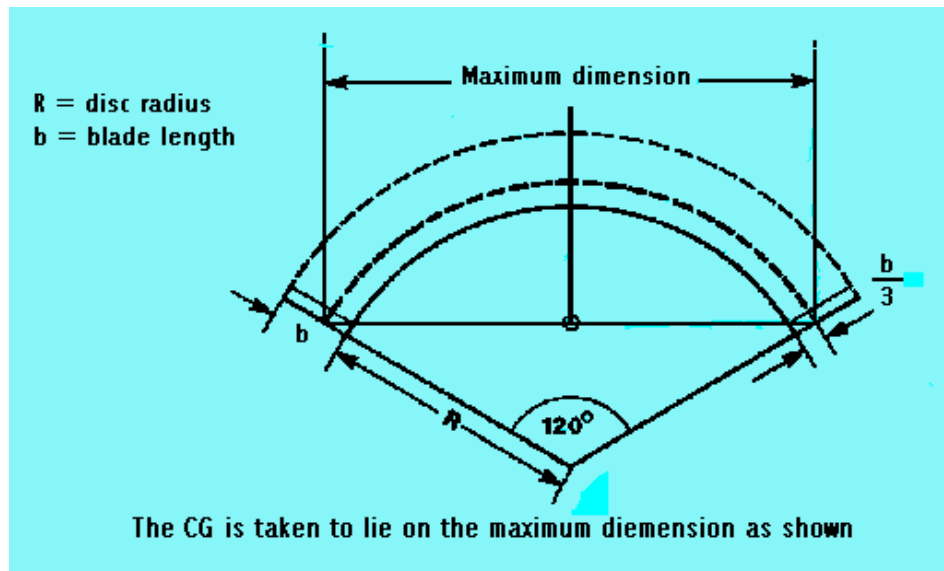


Figure 12 - Dimensions for a Single one third Disc Fragment

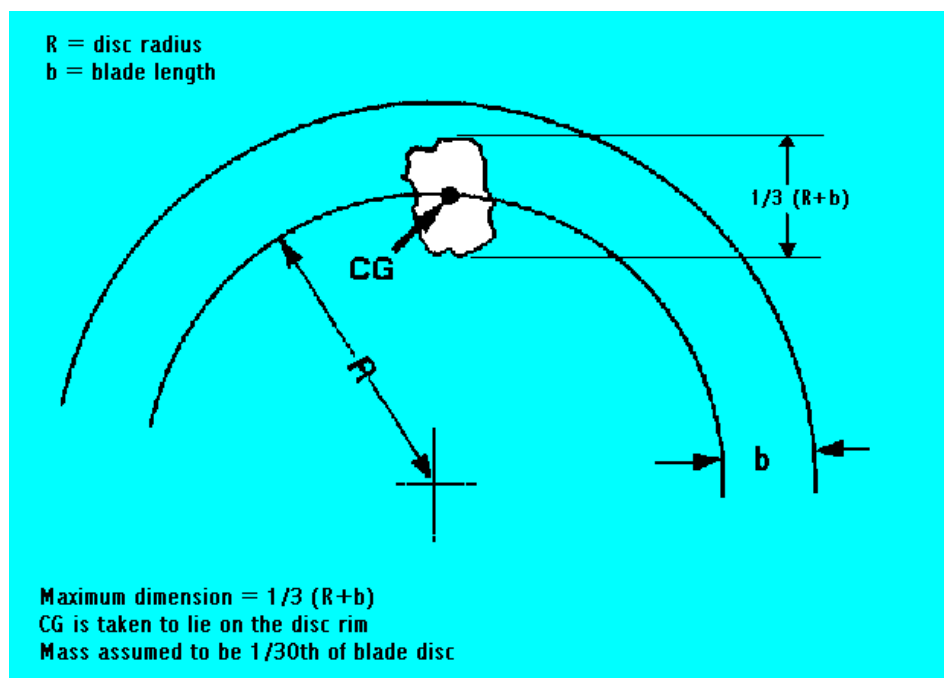


Figure 13 - Dimensions for an Intermediate Fragment

The maximum dimensions specified are critical to the extent of the damage to the aircraft and systems that may be incurred from the release of debris.

The spread angles shown in Figure 14 are relative to the plane of rotation of the disc.

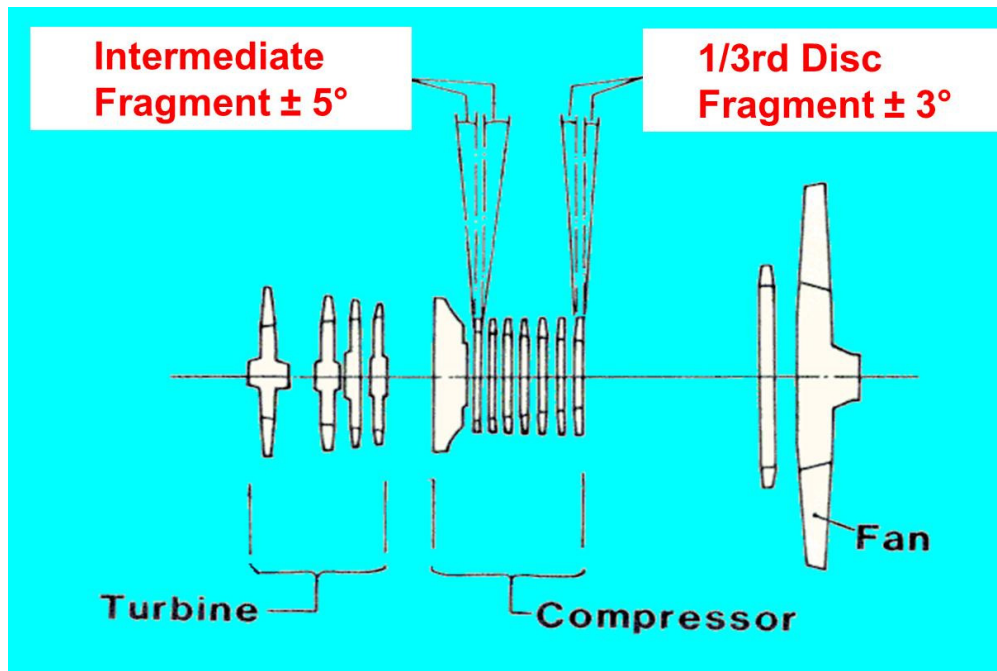


Figure 14 - Spread Angles for a one-third of a disc and an Intermediate fragment

The small fragment maximum dimension of half the aerofoil height is shown in Figure 15.

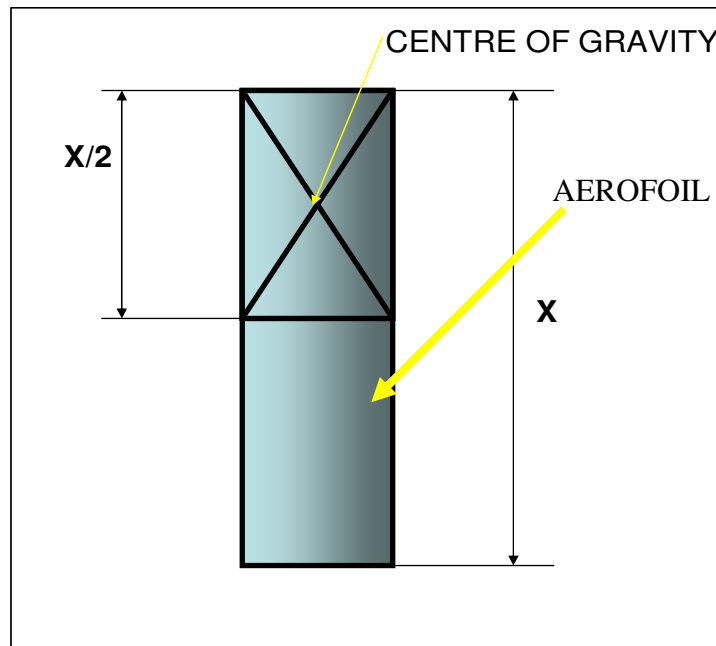


Figure 15 - Small Fragment maximum dimension

The fan blade fragment maximum dimension of half the aerofoil height is shown in Figure 16.

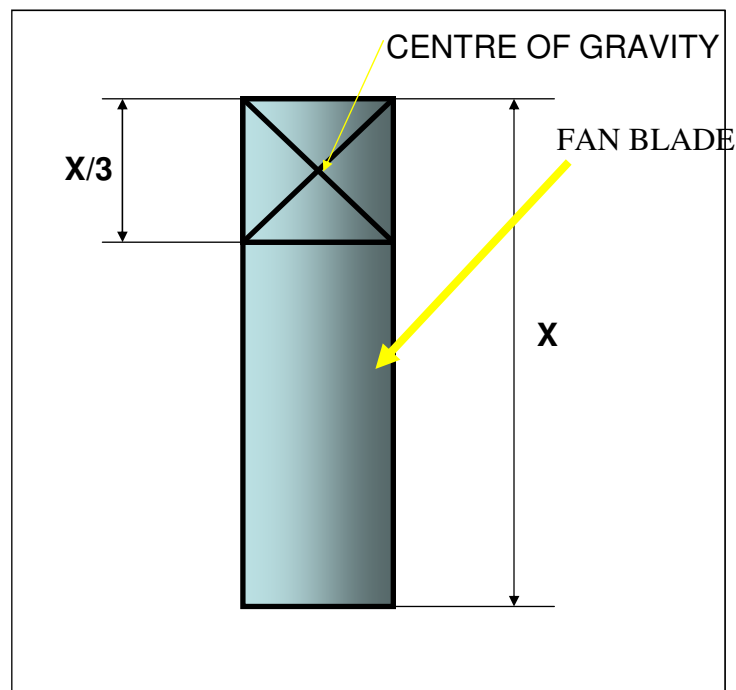


Figure 16 - Fan Blade Fragment Definition

As an alternative to using the single one third of a disc fragment and the Intermediate fragment described above a single piece of one-third disc may be used with a +/- spread angle of 5° .

Consideration must also be given to the random simultaneous release of three one-third pieces of disc and their effect on critical multi-channel systems. The debris characteristics are as defined previously for a one-third piece of disc.

2.3.4 Acceptable Levels of Risk

Table 2 - Acceptable Levels of Catastrophic Risk

	<i>Average Catastrophic Risk</i>
<i>Single one third disc fragment</i>	1 in 20
<i>Intermediate fragment</i>	1 in 40
<i>3 one third fragments of disc</i>	1 in 10

SSA COURSE MASTER 3 DAY (23)/DEBRIS DATA

A numerical risk assessment is not required for the single blade fragments, small fragments, and APU and engine rotor stages, which are qualified as contained. The levels of risk shown in Table 2 are mean values obtained by averaging those for all discs, on all engines, of the aeroplane assuming a typical flight. Individual discs or engines need not meet these risk levels nor need these risk levels be met for each phase of flight if either:

- No single disc shows a higher level of risk, averaged throughout the flight, which is greater than twice the values shown in the Table 2.
- Allowance is made for failures that would be Catastrophic only during particular phases of flight

Figure 17 shows the distribution of non-containments by phase of flight contained in the AMC 20-128A. Data such as these may be used for assessing the risk of a critical non-containment during specific phases of flight.

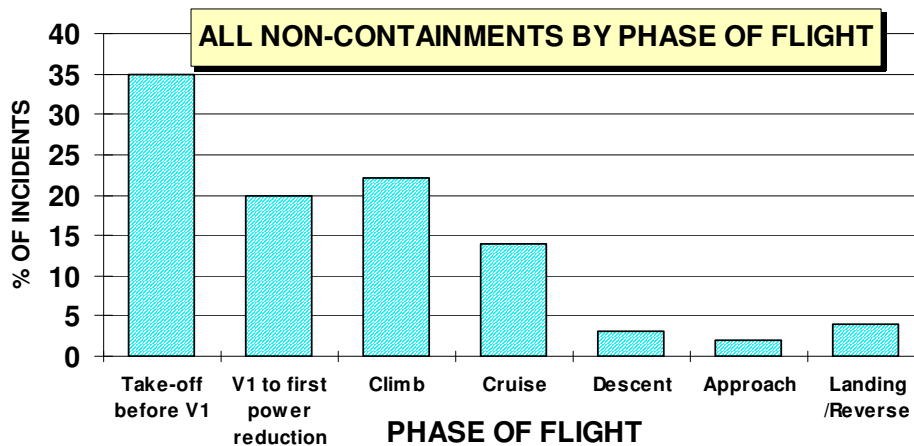


Figure 17 - Non-Containment by Phase of Flight

2.3.5 The Assessment of Risk

One procedure employed for assessing this risk is based on a calculation of the “window area” or areas of strike that could result in significant damage to the aircraft systems or structure. This window area, as well as being dependent on the size, location, and distance of the critical area from the engine rotor is also dependent on the debris size. The larger the debris under consideration, the larger the “window area”.

The “window area” is plotted on a graph, the scales of which represent the axial spread angle (abscissa) and the total radial angle of 360° (ordinate).

Figure 18 shows an example of a window diagram for a single rotor disc. For clarity, the figure shows only that portion of the graph containing the window area - not the full 360°. The view portrayed by the graph is that which would be seen from the engine stage under consideration. The advantage of this method is that relatively accurate assessments may be made of the probability of debris strikes to critical areas. Hence, the probability of critical impact following non-containment, may be simply calculated by the ratio of the exposed angular “window area” to the total angular area. Typically, for a one-third piece of debris with an assumed spread angle of 6° (3 degrees either side of the plane of the disc) this probability is given by the expression:

$$\frac{\text{Window area (square degrees)}}{6 \times 360}$$

This process lends itself to, and is greatly facilitated by, the use of customised software.

When the debris strike is only critical during certain flight phases the probability factor derived from the “window diagram” will need to be multiplied by the probability of the engine non-containment occurring during the critical flight phase.

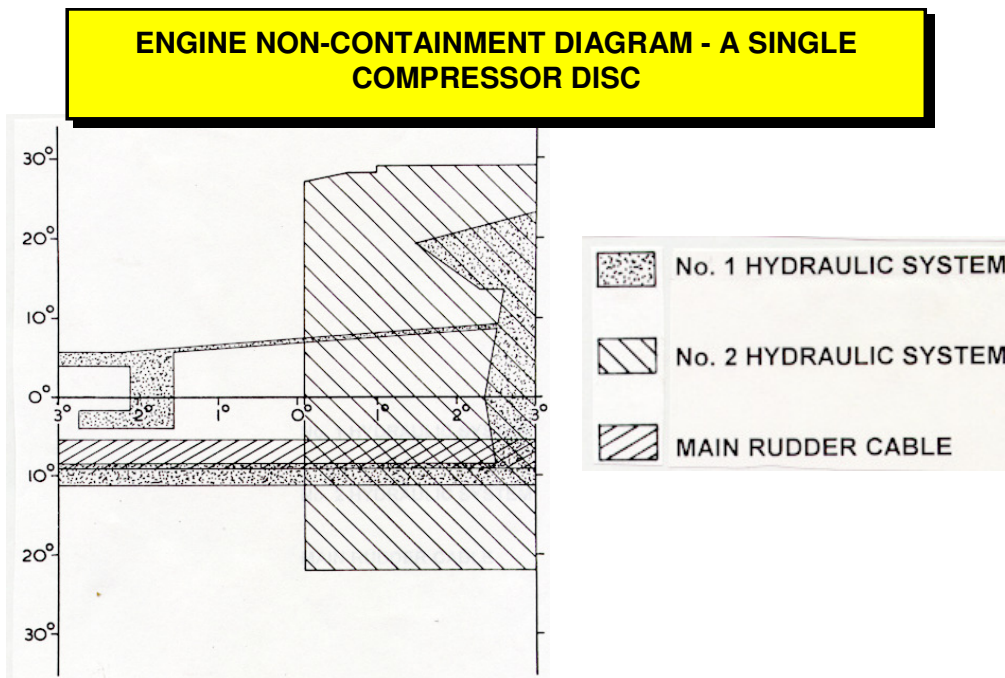


Figure 18 - Typical Window Diagram

In certain instances, the probabilities specified in the advisory material may not be met due to the broad configuration of the aircraft. In this respect the AMC 20-128A states:

“The Degree of minimization that is feasible may vary depending upon airplane size and configuration and this variation may prevent the specific hazard ratio from being achieved”

2.4 FIRE

The effects of aircraft fires may be compounded if all channels of a vital system are lost due to their close proximity. Special attention must be given to the segregation of channels and their location in relation to possible fire sources when planning the installation of aircraft systems.

Based on a study of past accidents carried out for the FAA the assessed distribution of the time, for a potentially catastrophic in-flight fire becoming non-survivable is as shown in Figure 19.

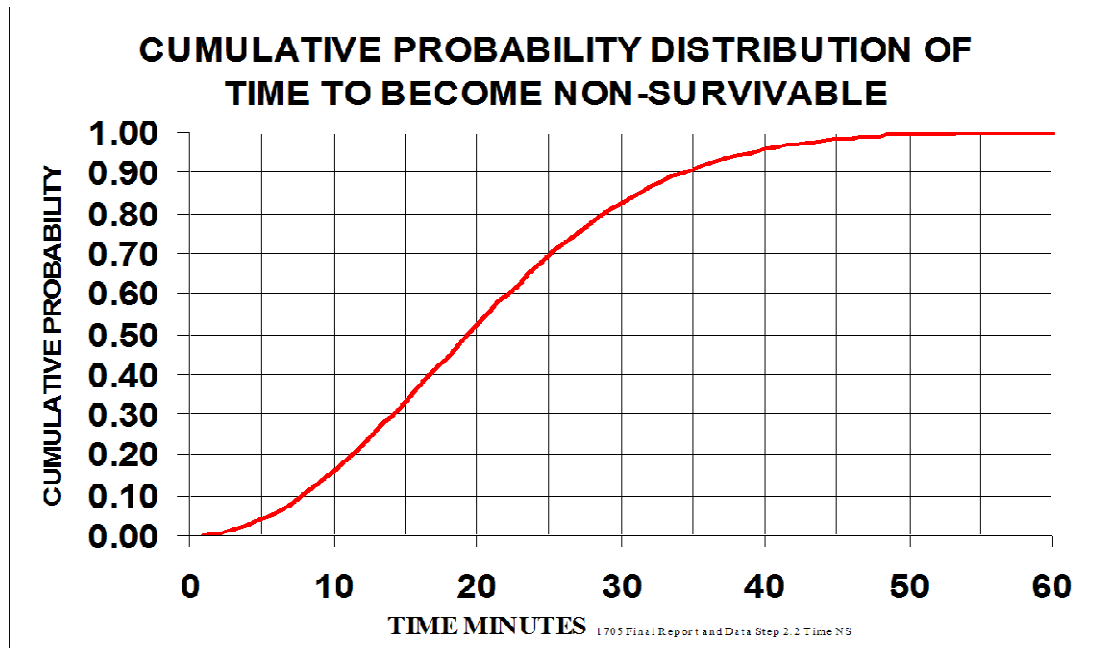


Figure 19 Cumulative Probability Distribution of Time to become non-survivable following an in-flight fire occurrence.

The following accidents illustrate the potential that exists for on-board fires to seriously endanger the safety of aircraft:

2.4.1 Swissair MD-11

“On 2 September 1998, [MD-11, registration HB-IWF] Swissair Flight 111 departed New York, United States of America, at 2018 eastern daylight savings time on a scheduled flight to Geneva, Switzerland, with 215 passengers and 14 crew members on board.

About 53 minutes after departure, while cruising at flight level 330, the flight crew smelled an abnormal odour in the cockpit. Their attention was then drawn to an unspecified area behind and above them and they began to investigate the source. Whatever they saw initially was shortly thereafter no longer perceived to be visible. They agreed that the origin of the anomaly was the air conditioning system. When they assessed that what they had seen or were now seeing was definitely smoke, they decided to divert. They initially began a turn toward Boston; however, when air traffic services mentioned Halifax, Nova Scotia, as an alternative airport, they changed the destination to the Halifax International Airport.

While the flight crew was preparing for the landing in Halifax, they were unaware that a fire was spreading above the ceiling in the front area of the aircraft. About 13 minutes after the abnormal odour was detected, the aircraft's flight data recorder began to record a rapid succession of aircraft systems-related failures. The flight crew declared an emergency and indicated a need to land immediately. About one minute later, radio communications and secondary radar contact with the aircraft were lost, and the flight recorders stopped functioning. About five and one-half minutes later, the aircraft crashed into the ocean about five nautical miles southwest of Peggy's Cove, Nova Scotia, Canada.

The aircraft was destroyed and there were no survivors.”

2.4.2 Delta – Boeing 727

The following fire-related accident occurred on the ground and did not result in injuries to personnel, however if the fire had occurred in flight, circumstances may have been somewhat different:

“On 14-Oct-1989, a Delta Airlines Boeing 727-232 was parked at the gate at Salt Lake City, Utah, USA.

The crew heard a muffled explosion and saw flames coming from the vent near seat 3D. The fire prevented the crew from returning to the cockpit to notify crash, fire & rescue. Passengers and crew evacuated the aircraft. The second officer, last to leave, could not reach the rear airstairs and exited via the emergency window exit after having difficulty in locating an exit because of smoke.

A mechanic noted low passenger oxygen supply during pre-flight and replaced oxygen cylinders. While exiting the electrical equip bay the mechanic saw a white flash engulf the oxygen system flow control unit. He attempted to have crash, fire & rescue notified of the fire using a hand held radio to no avail.

The passenger oxygen system had 6 low oxygen quantity maintenance write-ups during the previous 30 days but was not "flagged" by the company automated trend analysis program. Inspection of Delta's fleet revealed 35 oxygen system leaks on other aircraft.

There were 22 occupants on board the aircraft and all occupants were uninjured in the accident."

3 Zonal Safety Analysis

3.1 INTRODUCTION

ARP4754 states:

“Advisory material relating to systems establishes the need to address common cause faults (AC/AMJ 25.1309). The potential for this type of fault exists in any system architecture that relies on redundancy or uses components or software that are also used by other systems. The need to provide a fail-safe design will serve to separate a function from its applicable backups and/or protective mechanisms, or may separate redundant backups and/or protective mechanisms from each other. Once the applicable separation and isolation requirements have been identified, the common cause analysis should proceed to address the common cause fault potential across each boundary, and should identify the fault containment strategies to be used, along with the rationale supporting the fault coverage provided.

Common Cause Analysis is subdivided into the following areas of study to aid in the assessment:

- a. Zonal Safety Analysis*
- b. Particular Risks Assessment*
- c. Common Mode Analysis”*

3.2 ANALYSIS

The Zonal Safety Analysis (ZSA) forms just one part of the Common Cause Analysis, and is intended to primarily identify installation errors and violations of independence between systems. A ZSA can be conducted at any point during the design process. Typically, an early assessment will identify possible installation problems that may be encountered, such as fouling of structure or the interaction between pieces of equipment. ARP 4754 states:

“A Zonal Safety Analysis should examine each physical zone of the aircraft to ensure that equipment installation and potential physical interference with adjacent systems do not violate the independence requirements of the systems”

The objectives of a Zonal Safety Analysis are to identify problem areas that could give rise to failures that result from, or are exacerbated by, the installation of aircraft systems and equipment or from incorrect maintenance.

The first step in carrying out the analysis is to identify specific zones of the aircraft bounded by spars, bulkheads, floors etc.

It is essential that the work required commences at an early stage in the design in order that the cost of any changes that may be required are minimised. Hence the analysis is undertaken initially on drawings, but as the project progresses the aircraft mock-up and eventually the aeroplane itself is utilised.



The four aspects of a Zonal Safety Analysis are as follows:

i) Compliance with the Installation Rules

These rules have been developed over many years, and utilised on most of the major European civil aircraft projects. The rules provide a guide for designers and can be considered as a code of good engineering practice.

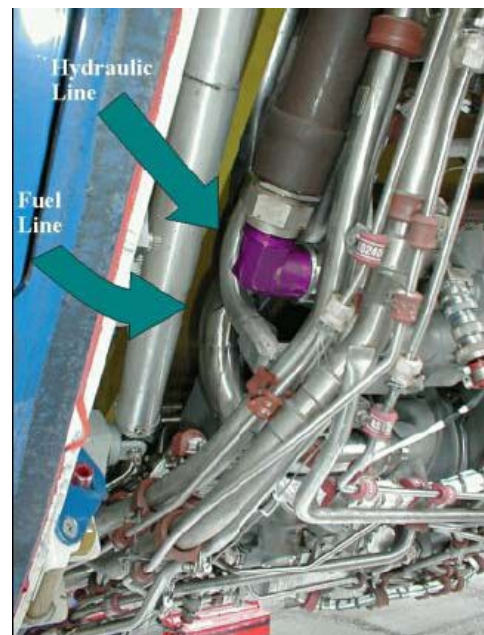
An example of such a guideline is that air-conditioning and engine bleed ducting will not normally be routed below hydraulic equipment. This is to prevent leaking hydraulic fluid from permeating the lagging on hot air ducts with a consequential fire risk.

ii) Interaction between Systems

The Zonal Safety Analysis is also intended to ensure that failures in an aircraft system do not cause "Cascade Failures" in other aircraft systems. Such failures could occur if, for example, a leak originating from a hot air duct causes damage to adjacent equipment because of being subjected to elevated temperatures. The Zonal Safety Analyst's task is to identify such problems and to ensure that the appropriate action is taken.

iii) Maintenance Errors

Problems often occur in-service as a result of equipment being incorrectly installed on the aircraft. One of the functions of the Zonal Safety Analysis is to identify such possibilities for mal-assembly. The engineer carrying out the analysis can then consider the implications of such an error and ensure that any changes that may be required to the design are incorporated. Such an error occurred on an A330 aircraft when a post-mod hydraulic pump and fuel tube were fitted next to a pre-mod hydraulic tube. Due to the different mod status, the tubes came into contact causing fuel line rupture and subsequent fuel exhaustion



iv) Environmental Effects on Systems

Consideration is also given to the implications of environmental effects such as icing, lightning strike, fire and water ingress, and once again any design changes that may be needed can be identified.

3.3 PROCESS

In most instances the design specialist concerned will already have considered the aspects identified by the four headings above. The task of the Zonal Safety Analyst is to act as a further check on the design and to ensure there are no unacceptable interactions between aircraft systems.

The process normally adopted by the industry is that for each aircraft zone the analyst works through checklists noting each problem that is identified. Experience has shown that taking photographs is often useful. Any problems identified can then be analysed in greater depth to assess the impact of the problem and subsequently discussed with the responsible designer.

4 Useful References

1. SAE, The Engineering Society for Advancing Mobility Land Sea Air and Space, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, ARP 4761, December 1996, United States of America Author.
2. *E. Lloyd & W. Tye, Systematic Safety, July 1982, UK Civil Aviation Authority*
3. *RGW Cherry & Associates Limited, (January 2011), the Cabin Safety Research Technical Group Accident Database, Prepared for Transport Canada, the Federal Aviation Administration and the UK Civil Aviation Authority. United Kingdom: <http://www.rgwcherry-adb.co.uk> .*
4. European Aviation Safety Agency, *Design Considerations For Minimizing Hazards Caused By Uncontained Turbine Engine And Auxiliary Power Unit Rotor Failure*, AMC 20-128A Germany Author.
5. SAE, The Engineering Society for Advancing Mobility Land Sea Air and Space, *Report on Aircraft Engine Containment - AIR 4003*, September 1987, United States of America Author.
6. SAE, The Engineering Society for Advancing Mobility Land Sea Air and Space, *Report on Aircraft Engine Containment - AIR 1537*, 1996, United States of America Author.