December 2008

COMMON CAUSE FAILURES

1 Theory versus Practice

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. 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.

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:

$$X^N \quad \text{. . . . . } \textbf{Equation 1}$$

However, it is known that this simple theory is not representative of in-service experience. This point is demonstrated by an analysis that was carried out on the triplex electrical power generation system on a civil airliner.

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

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

Based on the simple x^N theory it would be expected that for a two-channel system, the probability of all channels failing in one flight is:-

$$\mathbf{(9.5 \times 10^{-4})^2} \textbf{ per flight}$$

$$\mathbf{= 9 \times 10^{-7}} \textbf{ per flight (approx.)}$$

(NOTE: for two channels, failing in a three-channel system the probability is three times the above value)

And for a three-channel system:

$$\mathbf{(9.5 \times 10^{-4})^3} \textbf{ per flight}$$

$$\mathbf{= 8.6 \times 10^{-10}} \textbf{ per flight (approx.)}$$

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 the simple theory. Figure 1 shows both the simple theoretical, and the practical, relationship between the probability of total systems failure and the number of systems or channels available.

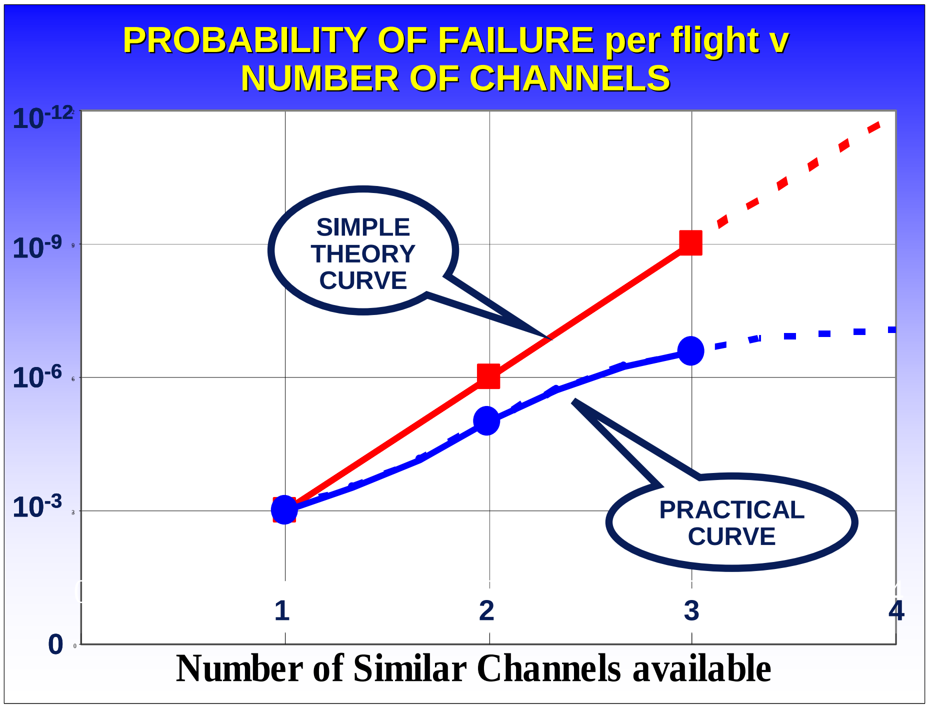


Figure 1 Probability of Failure against number of channels for an aircraft electrical power generation system

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. Significant differences also exist, between practical experience and the simple theory prediction, for aircraft hydraulic systems as illustrated in Figure 2.

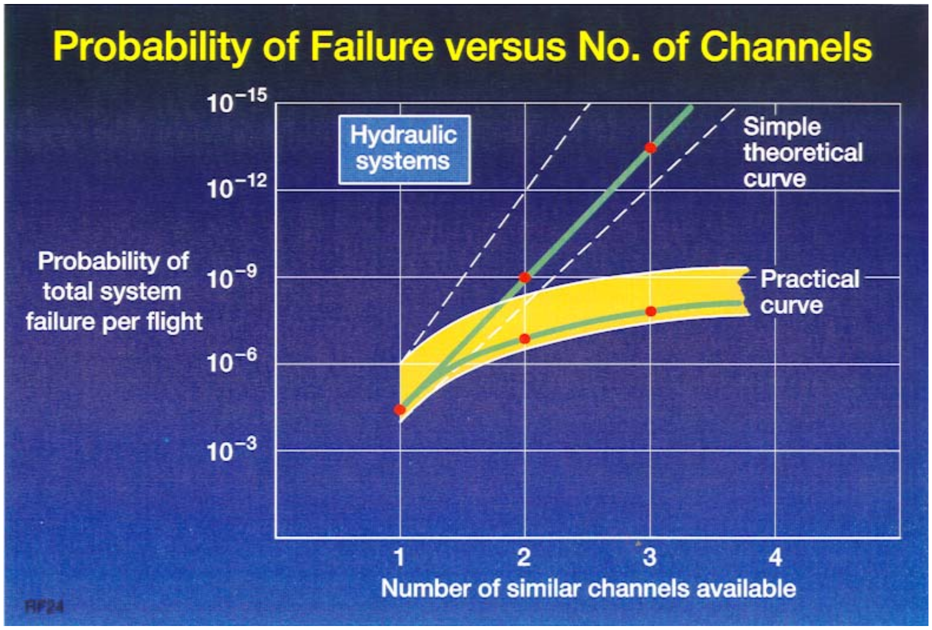


Figure 2 Probability of Failure against number of channels for an aircraft hydraulic power generation system

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 and Figure 2, 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.

These Common Cause Failures may occur both internally and externally to the system. Those internal to the system may be categorised as follows:

- Common Mode Failures
- Cascade Failures
- Single Element Failures

Those external to the system may be caused by a variety of occurrences, many of which are known as Particular Risks.

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.

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 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.

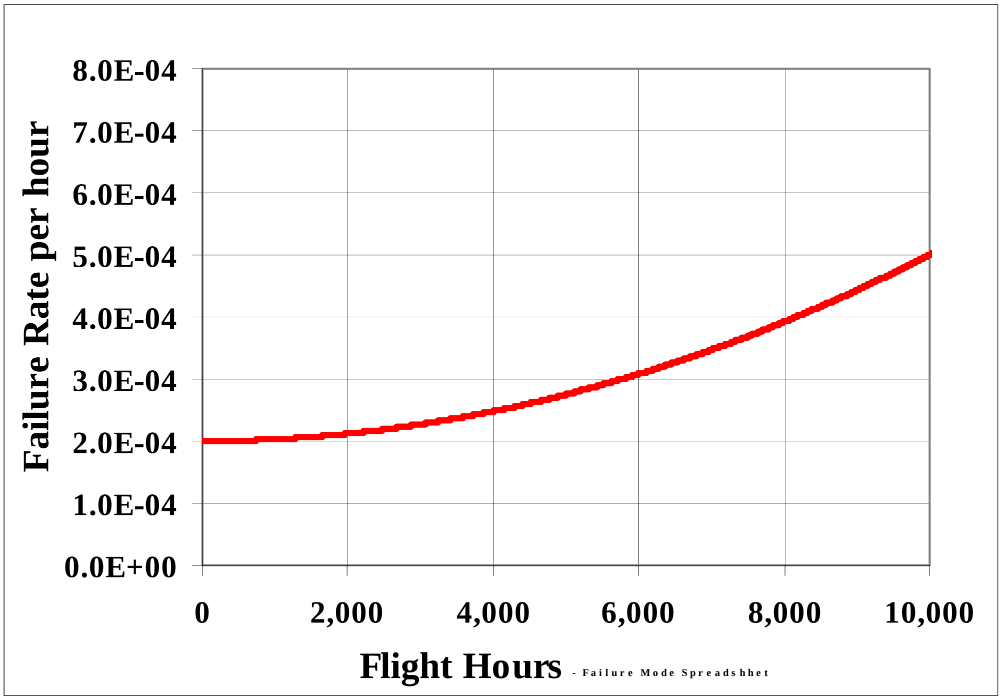


Figure 3 Multi-channel system component exhibiting "wear-out" characteristics

When the aircraft first enters service, the component has a failure rate that is approximately **2 x 10^{-4}** per hour. However, if the component survives in both channels for 10,000 flight hours each of the similar components will have a failure rate of approximately **5 x 10^{-4}** 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 x 10^{-4})^{2}** - equal to **4 x 10^{-8}** per hour. However after the aircraft has been in service for 10,000 hours the probability of both channels failing due to this component is approximately = **(5 x 10^{-4})^{2}** equal to **25 x 10^{-8}** per hour. Hence, the probability of both channels failing due to this component has increased by a factor of **6.25**. 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 detail design, maintenance checks and operating procedures in order to achieve the levels of integrity required.

Common Mode Failures may be identified from detailed Fault Trees and Failure Mode and Effect Analyses.

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.

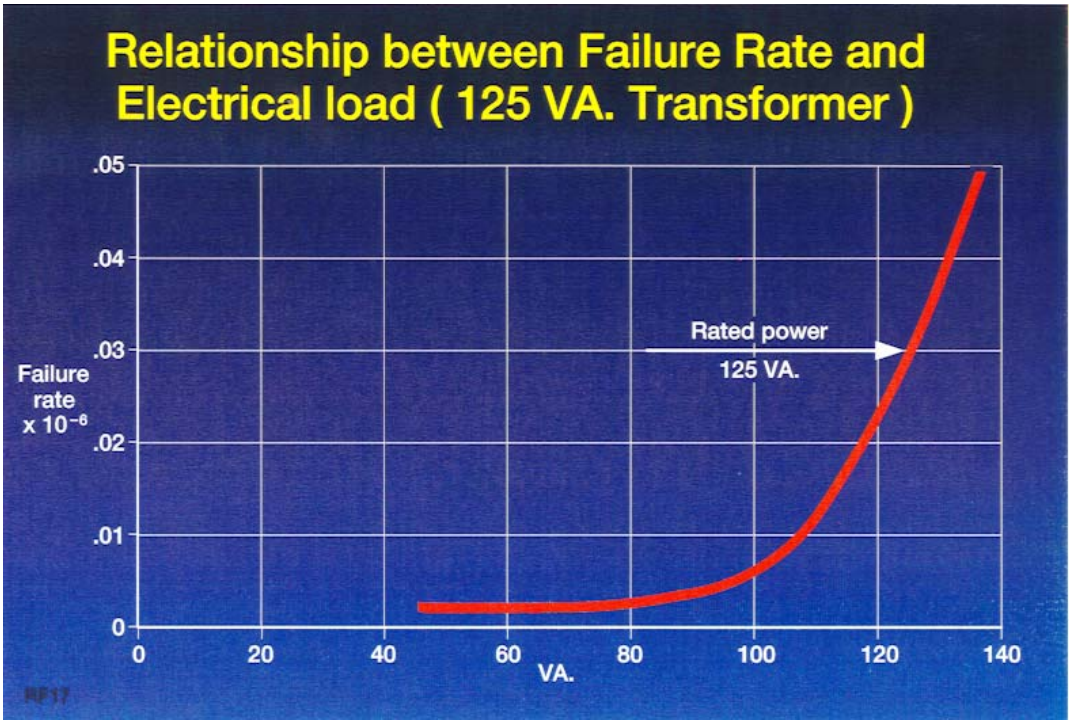


Figure 4 Relationship between Failure rate and Electrical Load for a 125 VA Transformer

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.

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:

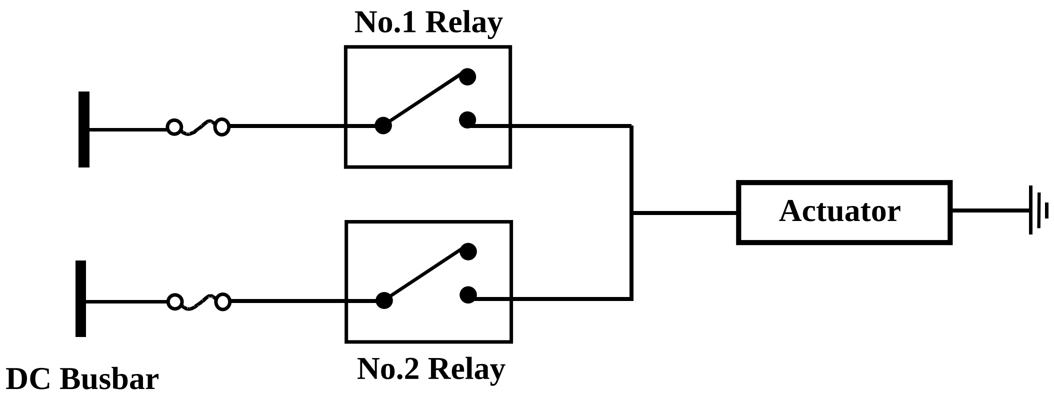
$$\lambda_1 \lambda_2 m t^2 \text{ per flight}$$

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

4 Single Element Failures

Almost without exception, all multi-channel systems have a "single element"-failure 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 below, 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 will result in loss of the entire system and, since there are two micro-switches, the probability of this occurrence is significantly greater than that of a single channel system.



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.*

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.*

Failures of this kind are not restricted to faults to 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.

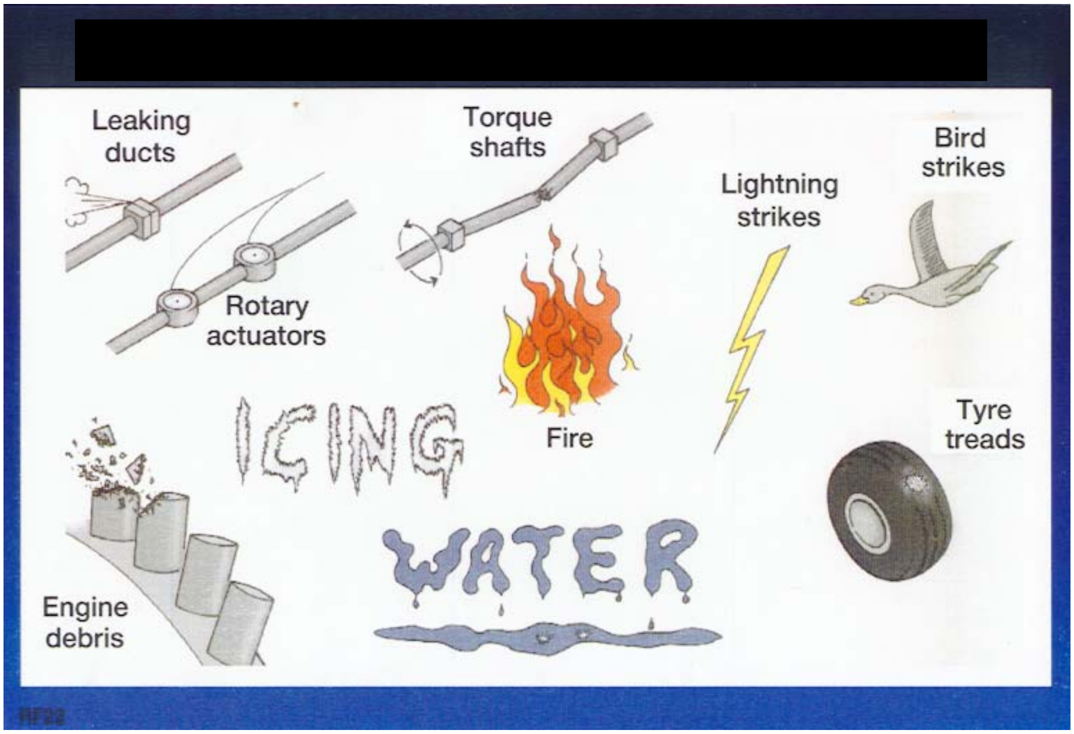
5 Particular Risks

Particular Risks are defined as:

> *"… those events or influences which are outside the system(s) and item(s) concerned, but which may violate failure independence claims."*
>
> (see Reference 2)

The type of multiple failure described by this broad heading may be produced by any one of many factors. In most cases the basic cause of failure emanates from outside of the system and may be influenced by its design, manufacture, the manner in which it is operated and maintained, or to the environment in which it functions.

Many Particular Risks are the subject of specific airworthiness requirements, for example bird strikes and engine non-containment. However, in many instances, the mechanism of failure is peculiar to one particular design or installation. Figure 5 illustrates some examples of Particular Risks that may need to be considered by the designer.



[redacted]

Figure 5 Examples of Particular Risks

It is not feasible within this course to address fully all Particular Risks. However, some of the more commonly encountered are given further consideration.

5.1 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. The following accident is an example of such an occurrence:

> *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.*

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 equipment 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.*

It is often not appreciated how rapidly an in-flight fire can progress. Based on a study of past accidents carried out for the FAA the assessed distribution of the time for a potentially catastrophic fire becoming non-survivable is as shown in Figure 6.

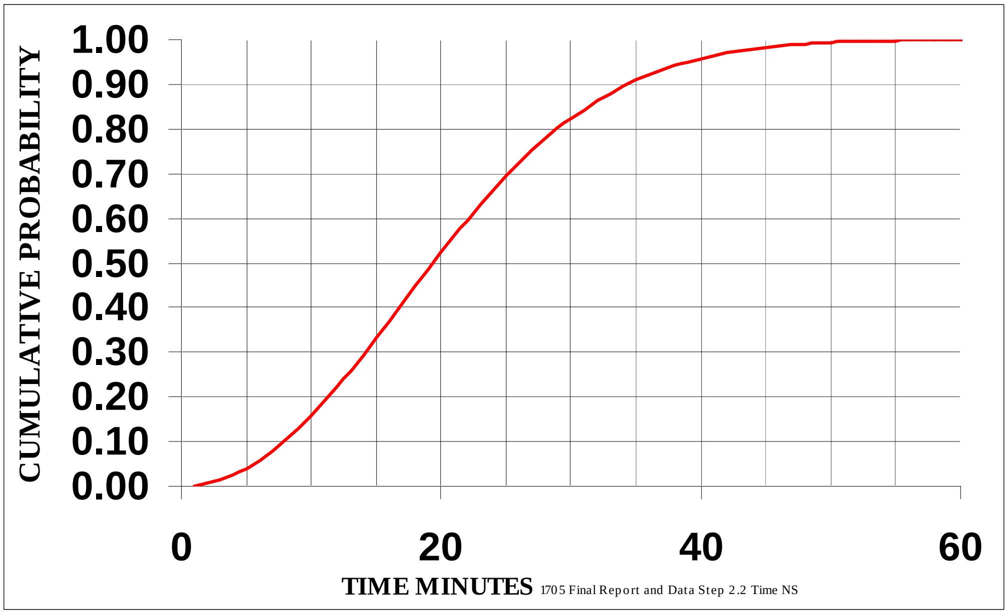


Figure 6 Cumulative Probability Distribution of Time to Become Non-survivable following an in-flight fire occurrence.

5.2 Tyre Debris

Equipment located in proximity to the undercarriage may be damaged by the shedding or bursting of a tyre tread. The EASA CS-25 requirements relating to tyre failures state:

CS 25.631

"Protection of equipment on landing gear and in wheel wells.
Equipment that is essential to the safe operation of the aeroplane and that is located on the landing gear and in wheel wells must be protected from the damaging effects of –

> *(1) A bursting tyre, (see AMC 25.729(f));*
> *(2) A loose tyre tread unless it is shown that a loose tyre tread cannot cause damage"…*

AMC 25.729 (f)

> *"The use of fusible plugs in the wheels is not a complete safeguard against damage due to tyre explosion.*

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 isolate totally 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 a short-range aircraft type certificated for 100 passenger seats:

Debris Size *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 speed*

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

Trajectory *taken as being 10^{o} from the vertical either side of the tyre at a point emanating from the ground/tyre contact point for a deflated tyre.*

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 ± 15^{o} - approximating to a Gaussian distribution.

As with most areas in the safety analysis field it will be necessary to seek guidance from the appropriate airworthiness authority and airframe constructor when making assumptions concerning the tyre debris model.

5.3 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 VC 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 7.

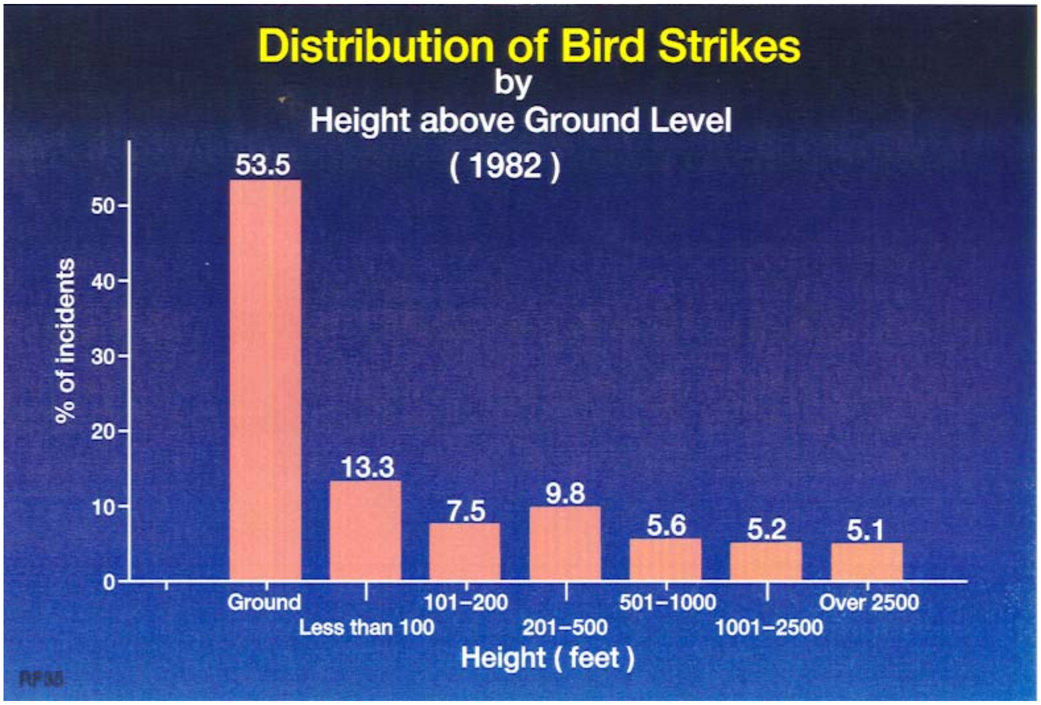


Figure 7 UK Distribution of Bird Strikes by height above ground level

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 multi-engine 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.*

5.4 Other Particular Risks

The following are examples of non aircraft-specific Particular Risks.

5.4.1 Lightning Strikes

Aircraft systems may be compromised by both the primary and secondary effects of lightning strikes. Whilst aircraft systems are designed to accommodate the likely threat, accidents can still result from encountering severe lightning strike occurrences. The following example illustrates the potential:

> *"On 4 December 2003, at 0909, Kato Airline Dornier 228-202, registration LN-HTA, impacted the ground and slid onto the runway following a lightning strike during approach to Bodo Airport, Norway. Up to 30 percent of the wires on individual bondings between the fuselage, horizontal stabilizer and elevator may have been broken before the lightning struck. The aircraft was hit by lightning containing a very large amount of energy. The aircraft's bondings were not able to conduct the electric energy from the lightning and the transfer rod from the cockpit to the elevator was broken. As a result of the reduced control of the aircraft's pitch and difficult wind conditions, the sink rate was not sufficiently stabilized on short final. The crew were unable to prevent the aircraft from hitting the ground.*
>
> *The two flight crew were seriously injured and the two passengers suffered minor injuries."*

5.4.2 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.

The subject of Engine Non-containment is addressed in detail elsewhere in this course.

5.4.3 Ice or Water Contamination

A poorly installed retrofit galley resulted in water leaking from the galley sink drain onto the aircraft's rear pressure bulkhead. The water impinging on the cold surface of the rear pressure bulkhead caused ice to form, which resulted in the jamming of the aircraft rudder controls.

The following extract from an FAA Airworthiness Directive relates to a similar problem on DC9 series aircraft:

> *"The FAA has received numerous reports indicating water leakage from the slant pressure panel into the wheel well of the main landing gear (MLG) on certain McDonnell Douglas Model DC-9 series airplanes. The water froze on the lateral control mixer and control cables. If the slant pressure panel drain valve is clogged, or a drain system is not installed, any water that accumulates during flight will be squeezed out of the panel into the wheel well due to damaged sealant. Accumulation of water in the wheel wells of the MLG could freeze on the lateral control mixer and control cables, resulting in restricted lateral control and consequent reduced controllability of the airplane."*

Water contamination can also present a potential risk of short circuits to electrical components. The following is an example of an FAA Airworthiness Directive relating to such an issue:

> *"This proposed AD would require installation of a closeout panel and moisture curtains for the main equipment center. This proposed AD would also require changing the drain tubes for the power drive units and the pitot static tubes and installing larger moisture shrouds. This proposed AD results from a report of water contamination in the electrical and electronic units in the main equipment center. We are proposing this AD to prevent the malfunction of one or more electrical and electronic units in the main equipment center, which could adversely affect the airplane's continued safe flight."*

6 Analysis Techniques for Identification of Common Cause Failures

Zonal Safety Analysis, Failure Mode & Effect Analysis and Fault Tree Analysis have proven to be useful in identifying Common Cause Failures.

Zonal Safety Analysis provides a means for identifying potential areas of unreliability that could result from a deficiency in the installation of aircraft systems and equipment or incorrect maintenance. It is particularly useful for identifying aircraft specific Particular Risks (e.g. Leaking Hot Air Ducts)

The principle of Fault Tree Analysis is to identify all combinations of failures that could result in a given system state. For a complex, high integrity system, multiple failures are required in order to produce a critical system state. The Fault Tree will present the multiple failures in groups under an "AND" gate. Failures in each of these groups are required in order for the critical failure of the system to occur. Since Common Cause Failures are multiple failures resulting from a common cause, it follows that if each of the failures below "AND" gates is compared then common causes for the failures may be found.

7 Useful References

1. MIL-HDBK-217 Reliability Prediction of Electronic Equipment. Department of Defense Washington DC 20301

2. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment - ARP4761, SAE (The Engineering Society for Advancing Mobility Land Sea Air and Space)

3. Systematic Safety, E. Lloyd & W. Tye, UK Civil Aviation Authority

4. Report on Aircraft Engine Containment - AIR 4003, SAE (The Engineering Society For Advancing Mobility Land Sea Air and Space)