Planning for super safety: the fail-safe dimension

R. W. Howard
Former Chairman
GEC Avionics
Rochester, UK

ABSTRACT

It has long been a requirement in air transport that no single failure can have a catastrophic effect. As nothing can ever be failure free, fail-safety in design and operation must be provided in all respects. This paper explores the design background, application and history of the concept of fail-safety in air transport and the vital role it plays in overall safety. It is suggested that fail-safety is the most important discipline of all those involved in safety in design and operations. Without it, the current air transport safety levels, even using the latest technologies, would not be possible.

In the modern air transport system, all accidents are due either to fail-safety implementations breaking down, or not having been adequately provided, or due to extremely remote multiple coincident failures. It can be argued that inadequacies in fail-safety provisions at the very low target failure rates now demanded, is the main reason for the near constancy of the accident rate, and the consequent increase in numbers of accidents as the world fleet grows. In the forefront of fail-safety problems is the inadequacy of its use in the management operations of crew in the modern air transport cockpit.

1.0 THE ACCIDENT RATE PROBLEM

It is well known that over the past 25 years air transport safety has improved very little. The world accident rate remains more or less constant on the large commercial aircraft, which means that the more aircraft that are put into service the more accidents there are\(^1\).

Figure 1 shows the annual numbers of fatal accidents per million flying hours since the beginning of airline history. Flying hours are used as the measure rather than numbers of landings or passenger miles/kilometres as this better relates to the basic reliability of the aircraft and its constituent parts which is central to the substance of this paper. (Note: Some of the statistics had to be converted.)

The curve on the left of Fig. 1 is the UK record\(^2\)\(^3\) over the first 40 years comprising mainly piston-engined aircraft. UK records are used here because reliable world figures for the early years of commercial aviation are unavailable, but the UK numbers are thought to be reasonably representative.

For the first 25 or so years the numbers of accidents reduced year on year, despite substantial fleet increases, but started to flatten out after WW2.

The curve on the right is a world rate\(^4\)\(^5\) which shows a surprising upward leap over the 1960 UK figures around the time that the population of the large turbine-powered transports was becoming significant, but in five years this settles back to the earlier UK record trend\(^6\)\(^7\), and on average becomes almost flat from the 1980s.

The two curves from different sources are surprisingly consistent in the longer term trend towards a flattening out of the accident rate, despite the very significant developments in technology from the 1950s, which might have been expected to yield noticeable downward steps.

Figure 2 shows the same information more clearly on a logarithmic scale. This clarifies the present very low rate of fall, which has now reached between 0.6 and 1 per million aircraft hours flown.

This paper considers the prospects of improving this level by a factor of 10, to around 1 accident every 10 million hours flown, or a rate of 1 in 10\(^7\) per hour. It is referred to here as the super-safety level, an accident rate low enough not to attract public unacceptability.

Putting this into perspective, there are at the moment about 13,000 large jets in the world, flying a total of about 50 million hours per year, and having about 50 fatal accidents. All accidents are unacceptable, but in terms of total fatalities in human transportation the air proportion is not unreasonable. However, the public perception is that they are too many and too horrifying. At the proposed super-safety level the fatal accident rate would reduce to 5 per annum with the current world fleet.

If air safety is to be improved it would be well to ask first how the present standard was reached. In fact how air transport safety is achieved is both unique and uncomplicated in principle, although this is not well known generally, and not fully appreciated in much of the industry itself. The basic principle is that all safety-critical elements of the overall flying system and all hazardous operations must be designed and organised so that when a potentially hazardous failure occurs it is nullified by some means, so that it has no significant effect and safe flight continues. This applies to the aircraft in the engineering and performance sense, and also to any external hazardous influence, human or environmental. This is a necessary concept of air transportation which distinguishes it from its ground and water counterparts.
the expected operating life of the aircraft, usually now expected to
The numerous sub-systems with their different known failure rates in the range 2,000 to 40,000 hours, combine to achieve a basic overall average failure rate for the aircraft, which comes out at about 1,000 hours. Clearly one failure every 1,000 hours is a long way from the achieved probability of one in a million hours (the 1 in 10⁶ per hour shown at the top left of Fig. 3), and this is where ‘fail-safety’ enters the act through the use of fail-safe ‘architecture’. Fail-safety ensures that by one method or another, usually using multiple redundancy, the one in 1,000 hours is reduced to the one in a million per hour current accident rate shown at the top.

Fail-safe architecture stands squarely on the shoulders of basic reliability. It is effectively a large package of different techniques used for surviving failures and hence giving high effective safety levels, and thus a low accident rate. Later, in Section 4.37, a sample classification of fail-safe architectural designs is made, but first it is necessary to continue with the explanation of the basic concepts.

In the broadest overall sense, today’s fail-safe architecture provides for surviving one failure, although in some cases this can be two, or even three, depending on basic reliability figures. The ‘deferred-maintenance computers’ used in fly-by-wire have even higher survivability levels. However, as a rule-of-thumb on the survivability provided by fail-safe architecture, a single-failure survivability can be taken as a minimum in considering the basic principles. It follows that fail-safety architecture must provide at least duplication or similar back-up of all safety-critical sub-systems. So referring again to the sample ‘1,000 hour’ group of sub-systems previously postulated, this must in practice be expanded to a minimum equivalent of two separately usable ‘1,000 hour’ groups in parallel, giving a compound failure probability product of (1/1,000 × 1/1,000) per hour, if the total aircraft and crew are to reach the 1 in 10⁶ hours current safety level on the top left of the diagram. This is illustrated in the expansion of this diagram in Fig. 4, which includes the overall system MTBFs arising from the sums of the individual sub-systems.

Two overall independent systems at 1,000 hours MTBF each can theoretically achieve the 1 in 10⁶ per hour safety level in flight, but there is a downside to overall duplication in that there will now be some safety-critical first-failure on an aircraft on average every 500 hours at the reliability level, as shown on the left of the diagram. Thus the price paid for greatly increased safety in this example is a halving of the aircraft reliability, which means a doubling of the number of in-flight safety-critical first-failures.

The great majority of these are carried for the remainder of a flight, and will be handled by part replacement or repair at the flight destination, but on rare occasions there may be one which is potentially more hazardous and require a return to base or other diversion if the time to destination is considered to be too long. (The prime example of this is an engine failure on an extended range operation of a twin-engined transport (ERTOPS).) There are other rare first-failures which may result in situations which are sufficiently hazardous to be classed as incidents, which may later demand procedural or design modifications. The ICARUS committee of the Flight Safety Foundation found the ‘incident’ frequency in practice to be 360 per fatal accident, equating to around one every 3,000 hours, or one in six out of the rule-of-thumb assessment level of one first-failure every 500 hours per aircraft. In the current world fleet of 13,000 large commercial jets this first-failure rate amounts to about 250 per day.

Figures of these magnitudes are facts of life in air transport, the only transport system which is designed around continued operation while carrying failed parts. An individual passenger may not have a high probability of ever experiencing one of the worldwide 250 per day in any particular flight, but unfortunately too many are the subjects of alarming reports in a generally ill-informed media which has a penchant for treating everyday operational events as accidents. There are very few who appreciate that daily failures in a vastly complex modern flying machine are a normal consequence of its fail-safety design concept in action.

The right-hand-sides of Figs 3 and 4 assess what might be

![Diagram](image-url)
required fundamentally to achieve super-safety. In simple numbers
an increase of the overall 1,000 hours basic reliability to at least
3,200 hours (the square root of ten million) is required in order to
achieve the super-safety level of 1 in $10^7$ per hour. In the next decade
or so the engineering MTBF range may go up to the necessary 5,000
to 60,000 hour bracket in the normal course of older products
maturing and newer ones using newer technology, but there is no
clear reason to believe that there will be likewise improvements in
the pilot equivalent MTBFs in cockpit management.

But in any case this is only part of the problem. It is doubtful if
basic reliability improvements alone will play the major role in
achieving super-safety in much of the running world fleet. Improve-
ments in fail-safety will probably play a bigger role. Some of this
will be in engineering architecture, in the degree and efficacy
of multiplication, such as the use of more ‘maintenance-deferral’ type
redundancy, and some will be in improved common-mode failure
avoidance. The biggest area for improvement is undoubtedly
required in the fail-safety of crew activity in cockpit management,
by greatly improved cross-monitoring and a higher level of indepen-
dence between two pilots in conducting situation evaluations. This is
discussed at greater length in Sections 7 and 8.

It will be appreciated that the balance of relationship between the
’reliability’ of an individual sub-system and the specific ‘fail-safe’ archi-
tecture associated with it will vary widely in practice. For example in
modern structures design safe-life reliability undoubtedly plays a greater
role than fail-safety in the achievement of overall structures safety. On
the other hand in the example of electrical power generation, the redu-
dancy architecture will make a greater contribution to the system safety
achieved than the reliability of individual generators. This balance will
also vary as technology changes in in a particular area. There are
numerous examples. The high reliability of digital microcircuit devices
requires less redundancy than the old discrete component analogue
designs. It is doubtful if ERTOPS operations could ever have been
contemplated with piston engines, and so on. The fail-safety provisions
are applied to achieve the safety contribution required by each sub-
system on the foundation of its individual reliability.

3.0 THE FAIL-SAFE DIMENSION

3.1 Definitions

From the foregoing it is clear that the ‘fail-safe dimension’ is funda-
mental to current safety, and therefore likely to be vital to the
achievement of the future super-safety. For a better understanding of
fail-safety in its broadest sense some definitions are required. Unfor-
luckily ‘fail-safety’ is used both as an overall generic descriptive, as
it is in the title of this paper, and also as a specific category within
this. This is a long established minor confusion which is lived with
in the aircraft industry and which is accepted in this paper.

‘Fail-safety’ is a concept which ranges in different forms across
all the design disciplines and operations involved in air transporta-
tion, machines and humans. It implies the acceptance of the notion
that there is no single safety-critical element or process in any part of
an airborne system or associated external guidance, control, cockpit
management or support system which can ever have a sufficient
level of reliability to be relied upon without some manner of alterna-
tive back-up or protection. Some action must therefore be taken to
implement this ‘back-up’ for every safety-critical element or action.

It therefore follows by definition that all fatal accidents must be the
result of a loss of fail-safety in the specific circumstances. (It also
follows that all accident investigations should aim primarily to find
why fail-safety was absent, or not working in the circumstances, as
well as the discovery of the root cause, a process not always
followed.)

The term ‘fail-safe’, when used in relation to a particular flight
application, will normally imply that degradation of some sort will
follow the failure, which will then require timely repair action, prob-
ably at the end of the particular flight operation. Indeed a definition
of ‘fail-safe’, which first put in an appearance in The Oxford Dictio-
nary in the mid 1950s shortly after the final reports on the Comet
disasters, says ‘revert to danger-free condition in event of break-
down etc.; become weaker or less efficient.’ Not a bad definition!
However there are further developments of the concept, such as ‘failure survivability’. ‘Failure survivability’ is an ‘up-market’ version of fail-safety, where a failure does not normally result in a loss of performance. ‘Fault-tolerance’ is a vague notion which sits somewhere between fail-safe and failure-survival. ‘Damage-tolerance’ is in the same family as ‘fault-tolerance’ and is used almost exclusively by structures designers. Failure-survivability is most widely implemented by using some form of separate back-up or multiple redundancy, but fail-safety may not always require this. Devices or systems without any protective provisions are normally not ‘safety-critical’ and are sometimes described as ‘single-lane’, ‘simplex’ or as having ‘single-point’ failure modes, although the last is also used to describe ‘common mode’ failure points in redundant systems.

The top of the failure-survival tree is the system which can absorb multiple failures without any correction action being taken for most of the operating life of the aircraft. There are very few of these of any complexity. Some structures get near to it, and so now do a few electronic systems, the so-called ‘deferred-maintenance’ fly-by-wire computers on the Boeing 777 being perhaps the most notable example. The whole gamut of failure-counteraction design techniques used in the aviation design business gets to its end-point with ‘crashworthiness’ on land or sea, protection and restraints for passengers and crew, and safe evacuation provisions.

3.2 Fail-safety in action

Having attempted to define fail-safety, it can now be described in a more specific applications sense. Fail-safety in air transport systems is applied in design and operation within all disciplines. To the aircraft/engine designers it can primarily be the ability to survive an engine failure, even if structurally damaging. It can mean to a structural designer that the propagation of a particular crack is contained or that structural sacrificial fuses are appropriately positioned. To an electrical systems engineer it can mean that a failed generator will remove itself from a power supply bus automatically, or with crew intervention, without loss of critical services or the damaging of other on-line devices. To a hydraulics or electro-hydraulics engineer it can mean that a high pressure line burst or pump drive failure is limited and contained without mechanical damage or fire risk. To the landing gear designer it can mean safe recovery after tyre bursts in take-off or landing. To the automatic controls or autopilot designer it can mean catching a computer failure or freezing a runaway actuator or trim system drive before dangerous controls forces or movements can be applied. To the designer of secondary controls it may mean the locking of control runs to ensure symmetry after a demand failure, or automatic retraction of spoiler/speed brakes in an emergency full-throttle climb. To the systems designer of advanced fly-by-wire controls it may mean automatic assistance or overriding of pilot commands where in extreme conditions the aircraft could be endangered by excessive manoeuvres or attitude changes. To a pilot it will mean the ability to override any errant happening by demanding an alternative operational action or taking personal manual control of an automatic system. It also means in cockpit management the constant cross-monitoring between crew members to seek out errors arising from differences in their situation awareness. To the air traffic controller it could mean the timely detection of an ‘altitude-bust’ or control area conflict and hence avoidance of a penetration of the imposed traffic separation margins, or it could be the detection of a pilot’s incorrect readback of a misunderstood instruction or correction of a spurious communication. These are a few examples from an extensive range in each of the disciplines mentioned, and representative of the type of failure nullification required by the fail-safe concept.

3.3 Practical limits of fail-safety

The highest level of safety is achievable through the use of the fail-safety concept, and by the same token the level of safety actually achieved is limited by the effectiveness of the fail-safety concept as it is applied. The effectiveness is determined by two main factors, the first being the quality of the architectural design and the second being any limits imposed by rare external influences causing common-mode failures in redundant systems. These are vital factors which come to the fore at the very low failure/error probabilities which now prevail.

The first involves the design process in getting whatever fail-safe architecture is applied to each individual system or sub-system to work correctly. It is a fallacy to assume that because redundant systems are provided, that survivability is assured. It is not much good having two engines if the wrong one is shut down after a failure. It is not much good having a pilot manual back-up for the control of various automatic systems if the back-up provisions is inoperable when required. It is not much good having two independent sets of instruments in the cockpit if their readings are never compared. In many cases additional redundancy is applied to assist with failure detection, using majority voting methods, but where possible more economic measuring indicators or failure ‘tell-tales’ are used. It is vital always to know automatically or through obvious crew knowledge if partial system failures which deplete fail-safety levels are present.

The second limitation in the effectiveness of fail-safety provisions is the often obscure one of common-mode failures, which are of a nature to undermine independence in redundancy provisions, whatever form these might take. One does not expect designers to fail prey to the obvious ones, but there are remote and more obscure examples which can be expected to enter at a lower level than the basic redundancy provisions are designed to achieve. For example a sub-system with a basic MTBF of 5,000 hours, when duplicated to provide two lanes for comparison, might be expected by good design in lane isolation to achieve a total failure probability of $(1/5,000)^2 = 4 \times 10^{-6}$ per hour. But if ‘common-mode’ failures find their way into both lanes at a rate of $1 \times 10^{-6}$ per hour then the total failure probability reduces to the near $10^{-5}$ limit of $4 \times 10^{-6} + 10^{-6}$ per hour, which destroys the pure redundancy-based expectation.

In today’s aircraft, operational and maintenance systems, there are no safety critical areas which are acceptable if they have an individual failure rate higher than $10^{-6}$ per hour, and $10^{-7}$ is normally expected, whereas in the 1960s and 1970s a figure at $10^{-8}$ was considered satisfactory. Unfortunately the designer’s human perception of common-mode causes and their avoidance does not improve significantly with time, so the danger they present has increased and even more extensive special precautions are required. The degree to which fail-safety concepts are employed in the safety-critical aspects of an aircraft design and in its operational environment is essential to the achievement of a satisfactory air transport system, and must, in effect, be total.

4.0 THE EVOLUTION OF THE FAIL-SAFETY CONCEPT

Sections 1 to 3 have defined a current view of the philosophy of air transport safety and the vital importance of fail-safety principles in achieving acceptably low accident rates. The history of air transport development in machines and operations does not display a strong continuous acceptance of these principles as a mainstream factor in design and development. The design principle that no single failure should ever cause a fatality is embedded in overall requirements and certification clauses but is not normally elucidated in specific design instructions. Rather it is in the minds of designers as ‘good practice’. Indeed the subject of fail-safety has always been varied and somewhat obscure, as it is implemented in so many different ways. In some disciplines it has almost a secret presence. It is multi-discipline, not normally taught or recognised in academic or training establishments, and has an appallingly low recognition in aerospace literature, almost to the point of silence. No other design discipline makes a bigger contribution to safety in flight, and yet its application and certification approval is not always an adequate or ordered procedure.

In the early days of powered flight the perception of safety was also ambiguous. On the one hand most of the early fatal accidents were due to loss of control by the pilot, but the pursuit of safety concentrated mainly on the engineering ‘airworthiness’ of the machine. It seemed to
be taken for granted that there would be good pilots and bad pilots, the
good ones would survive and provide adequately safe piloting, and
good safe mechanical machines would progressively be developed for
them to fly. In fact for perhaps half of the history of powered flight the
machine was considered to be less reliable than the human pilot. The
performance and exploits of single pilots, or captains, dominated even
when more than one crew member was present. This continued even
into the early jet age. The role of the first officer (or copilot) in a
Boeing 707 was said to be 'to enable the captain better to fulfil the
functions of pilot skill and command' (5). Hence the concepts of fail-
safety which did gradually evolve had a strong bias towards the engi-
neering design of machines rather than piloting.

A review of this background history throws considerable light on the
more recent slowing down in the rate of safety improvement. This
section explores some relevant aspects from the earliest days of
powered flight, starting with the Wright Brothers and then working
through some significant aircraft design milestones chosen on the basis
of the numbers of fail-safety application areas planned and imple-
mented in each design. The author's definition of and choice of 'fail-
safety areas' for the purposes of this paper is covered in an Appendix.

4.1 The Wright flyer: fail-safety milestone 1

The Wright Flyer, Fig. 5, had no fail-safety in its design, as might be
expected, although there was a strong desire by the Wright brothers
and their early contemporaries to do something to protect pilots
against the low speed hazard of loss of control.

4.2 Doutre speed maintainer/stick-pusher: 1912

There were countless proposals for speed control devices (6). One
example was the Doutre speed maintainer (7,8), Fig. 6, which used the
air pressure on a forward facing spring loaded plate to operate a
pneumatic motor which could depress the elevator.

4.3 Wright automatic stabiliser

Orville Wright tested and patented an automatic stabiliser (6,9), Fig.
7, a more elaborate device than the speed maintainers. The sensor
was a weight balanced incidence vane, (the prime piloting instru-
mant which the Wrights) which used a pneumatic ‘engine’ to
operate the elevator. The stabiliser was only developed to an experi-
mental stage, and was probably pursued to some extent as a
concession to world opinion at the time. This was basically in
conflict with the concept of pilot control which epitomised the
Wrights’ achievements.

4.4 Crash helmets

Some pilots decided as a result of loss of control experiences (10)
that the best protection was the wearing of crash helmets. Figure 8
shows Hap Arnold and Tommy Milling with a Wright machine.
(Lieutenant Selfridge, the first fatality in powered aviation, died of
head injuries on 17 September 1908 in an accident while flying
with Orville Wright.)

4.5 Lawrence Sperry automatic stabiliser

The most successful attempt at engineering an automatic stabilisation
solution to the loss of control problem came from the American
Lawrence Sperry who designed a free gyrosopic/wind vane system (11,12),
Fig. 9. It was demonstrated in Paris in 1914 and was awarded a prize
in a safety competition conducted by the Aero Club of France. His
system protected the aircraft while it was working, but the pilot
needed to be constantly on the alert to correct the potentially dire
consequences when it failed, which on occasions it did, and he was
not! The Sperry Stabiliser was the first practical autopilot, and this is
the place it finally occupies in history.
4.6 Farnborough BE2C

The British at Farnborough finally came to the rescue in this saga with two major contributions. First the mathematician/pilot Edward Busk, using the theoretical work of Professor G.H. Bryan and others, and a great deal of test flying which he did personally, modified Geoffrey de Havilland’s BE2 aircraft into an intrinsically stable machine. This was the BE2C, Fig. 10, which in still air could be flown for hours hands-off(13). This went a little too far for the fighting-scout pilots, who demanded instant manoeuvrability, but the theoretical basis for design stability to various degrees was established. Second, Harry Hawker and Major F.W. Goodden separately discovered the method of unstalling wings as the precursor to pulling out of spins, and F.A. Lindemann (later Lord Cherwell) pursued the then growing theoretical knowledge of aerodynamic stability to measure, analyse and personally demonstrate a standard spin recovery(14).

These developments, combined with increased speed margins over the stall and the WW1 experiences in handling highly agile machines, brought to an end any thought that flying should to any extent be taken out of the hands of pilots, and they became the unchallenged custodians of flying safety. (A curiosity today is that the basic principles of recovery from extreme flight upsets is not a standard part of airline pilot training, although it would have been done by those coming from military service. Uncorrected loss of control in flight (LOCIF) has by no means been eliminated as a cause of civil transport accidents(15).)

4.7 Early structures

Fail-safety contributions came about by default in the field of structures in that there were many designs including monocoque and...
others with intrinsic redundancy in stiff, light-weight arrangements. These got off to a good start as early as 1908. One fuselage structure with many redundant members was demonstrated at the first Paris Aeronautical Salon(16), Fig. 11. The ubiquitous biplane used stiff wooden strut interplane bracing supplemented with tensioned and duplicated lift wires and drag wires(17).

4.8 Duplicated flying controls cables

Many wartime aircraft used duplicated flying control cables, particularly for rudder and elevator, running both on the inside and the outside of the structure and skins. The outside portions simplified rigging and checking for damage, Fig. 12.

4.9 Engine ignition systems

Early IC engines had single ignition systems, the magnetos and spark plugs of which were notoriously unreliable. Figure 13 shows the single ignition de Havilland Iris used in the early BE2 aircraft. Dual systems were introduced in 1912, the first coming from Austro-Daimler using Bosch magnetos(18), and were universally used during WW1 and thereafter to the present day for spark-ignition aero engines. The Bentley Rotary (BR2), with dual ignition on nine cylinders, Fig. 14, was fitted to numerous aircraft in WW1 including the notable Sopwith Camel(19).

The introduction of dual ignition improved combustion as well as providing failure-survivability, so from the fail-safety viewpoint it had the essential feature of indicating partial failures through ‘rough running’. Dual ignition must go down in history as one of the most important and enduring fail-safety actions in aviation. (It is in the fail-safe architecture category of primary redundancy illustrated later in Fig. 38.)

4.10 Multiple engines

The most significant fail-safety action was of course the adoption of multiple engine configurations which allowed continued flight after a failure. From 1911 until the outbreak of WW1 and throughout it, many types of two, three, four and even five engine military aircraft were designed and produced in large numbers. Notable types were by Sikorsky, Caudron, Wagenfabric Gothaer (Gotha), Zeppelin-Staaken and Handley Page. Only the Russian Sikorsky was really highly viable after any engine failure when loaded. For the others survivability was forced by limited production.

The four-engined version of the Sikorsky ‘Bolshoi’ was the first aircraft deliberately designed and demonstrated to survive engine failures(20,21), even two on one side, when carrying a substantial payload. With a wingspan of over 100 feet it was built and first flown in St Petersburg in 1913 by the 22 year old Igor Sikorsky with the aim of providing a high speed transport for the Tsar to navigate over his vast Russian empire. It had a high survivability and fully loaded carried 18 passengers and crew, a heated dining room and a rope-enclosed observation deck.

The passenger carrying design was curtailed by the requirements of WW1 during which 90 successors, the types ‘Kievsky’ and ‘Ilya-Mourometz’ (IM), were built as bombers, having four engines along the leading edges of the lower wings. They were remarkably successful, only three or four being lost in several years and many hundreds of missions on the Eastern front. But they were denied to the Western participants, who did not attempt to produce equivalent designs until the war was nearly over.

The ‘IMS’, as the various types became known generically, were taken over by the Cossack revolutionaries. (If one had been available to the Tsar and his family at the end of 1917 the course of Russian history may have been very different). A number of Sikorsky’s colleagues were executed, but he escaped out of Murmansk to the United States where he opened a new chapter in his illustrious career. The Ilyo-Mourometz demonstrated exceptional fail-safety in service, but unfortunately it was a totally isolated achievement and not therefore a milestone in the progress towards world-wide air transport safety. In western Europe there were a number of multiple engine types which emerged near the end of WW1 and came into service just before the Armistice. These exerted the continuing influence on fail-safety development, albeit from a position of lesser capability at the time than the earlier IMs.

The twin-engined Vickers Vimy, which was designed to carry an Imperial ton of bombs to Berlin, saw no wartime service, but is famous for making in 1919 the first Atlantic non-stop flight, and the epic one from England to Australia. It is therefore chosen as the next example for state-of-the-art fail-safety assessment, Fig. 15.

over his vast Russian empire. It had a high survivability and fully loaded carried 18 passengers and crew, a heated dining room and a rope-enclosed observation deck.

The passenger carrying design was curtailed by the requirements of WW1 during which 90 successors, the types ‘Kievsky’ and ‘Ilya-Mourometz’ (IM), were built as bombers, having four engines along the leading edges of the lower wings. They were remarkably successful, only three or four being lost in several years and many hundreds of missions on the Eastern front. But they were denied to the Western participants, who did not attempt to produce equivalent designs until the war was nearly over.

The ‘IMS’, as the various types became known generically, were taken over by the Cossack revolutionaries. (If one had been available to the Tsar and his family at the end of 1917 the course of Russian history may have been very different). A number of Sikorsky’s colleagues were executed, but he escaped out of Murmansk to the United States where he opened a new chapter in his illustrious career. The Ilya-Mourometz demonstrated exceptional fail-safety in service, but unfortunately it was a totally isolated achievement and not therefore a milestone in the progress towards world-wide air transport safety. In western Europe there were a number of multiple engine types which emerged near the end of WW1 and came into service just before the Armistice. These exerted the continuing influence on fail-safety development, albeit from a position of lesser capability at the time than the earlier IMs.

The twin-engined Vickers Vimy, which was designed to carry an Imperial ton of bombs to Berlin, saw no wartime service, but is famous for making in 1919 the first Atlantic non-stop flight, and the epic one from England to Australia. It is therefore chosen as the next example for state-of-the-art fail-safety assessment, Fig. 15.
4.11 The Vickers Vimy — 1919: fail-safety milestone 2

An inspection of the Vimy design and parts lists shows that it had planned fail-safety in around ten design areas. The Vimy basic design was an example of a fairly standard layout which persisted into the 1930s. It had dual ignition in the two Rolls-Royce Eagle VIII engines, but it cannot be credited with a clear ability to survive a full-load engine failure. It had fully duplicated flying control surfaces, twin elevators and twin rudders in a box frame construction, and two sets of ailerons on upper and lower wings. Each pair of surfaces was operated by its own cable circuit, with balance interconnections. However the Vimy, like most aircraft at the time, provided controls for only one pilot, although there were two seats in the front cockpit.

4.12 Engine failures and forced landings

In contrast to the Vimy, its larger German contemporaries, some of which were pressed into limited commercial service after 1918, could carry four crew up front including two flying. Figure 16 could be a
single engined Gotha or even a five-engined Zeppelin-Staaken. It has spacious accommodation, with all occupants wearing crash helmets, perhaps in anticipation of rough or forced landings. Two pilots were probably required to handle heavy controls forces.

This demonstrates the diversity of design opinions about survivability at the time. As to engine failures there was of course a major advantage in the low flying speeds of the early machines because it also meant low landing speeds and short landing distances. An astute pilot would fly only over open country as glider pilots mainly do even now, and in the event of an engine failure, by far the most likely problem in good weather, he would descend into a convenient field. Even the larger passenger aircraft in the 1920s did this not infrequently.

Sir Alan Cobham, in 1966 recalled these early problems:

“...in the early days of flying, one lived as a pilot by virtue of one’s ability to accomplish a forced landing, because one never knew from one moment to another when the engine would fail to operate. Anything could happen, a faulty propeller, a bad fuel system, pumps that packed up, broken inlet valves, broken valve springs, conrods broken and even a split crank case”.

Not all were convinced that multiple separate engines gave increased safety. A retarding factor in the progress towards the use of fail-safe combinations of engines was that, under the pressure of war, great advances had been made in their reliability, so the problem receded and the debate continued as to the numbers of engines which were really necessary for passenger-carrying operations. This indicates, not surprisingly, a lack of appreciation at the time of the ultimate potential of air travel, and a similar shortfall in any quantitative understanding of how safety should be improved. Many pilots considered that having two engines merely doubled the chance of a failure, and the remaining engine only slightly prolonged the agony of carrying out the inevitable forced landing.

Harry Hawker and Lt Cdr Mackenzie-Grieve attempted an Atlantic crossing several weeks before Alcock and Brown in a modified Sopwith passenger transport (named the ‘Atlantic’) and powered with a single 360hp water-cooled Rolls-Royce Eagle. Hawker’s choice of a single-engined aircraft was almost certainly one of availability. His employer T.O.M. Sopwith did not have any multi-engined machines! But in answer to criticism he said:

“Hardly any multi-engined machine can fly with full fuel load with less than all its engines operating. If it lost one engine, then it would have to come down just as would the single-engined ‘Atlantic’. Also, the single-engined machine had a better height performance to rise above bad weather and navigate by the stars”.

In the event Hawker had to exercise these advantages, but the Atlantic was finally forced to ditch near a Danish steamship due to an engine coolant failure.

One school of thought was to have a two engine installation designed to be serviced in flight. There were precedents in principle. It was not unknown for a crew member to do a little wing walking between the struts and bracing wires to replenish oil or coolant or even put out a fire. Boulton and Paul designed and flew an all-metal machine for the War Ministry over the period 1922-26 named the Bodmin, which used the principle of a central engine room in the fuselage. This housed two Napier Lions which drove by gears, shafts and belts, four airscrews on the wings, two tractors from one engine and two pushers from the other.

The ultimate in the in-flight servicing concept was reached in 1929 with the giant Dornier DoX, which had twelve 600hp engines and their associated electrical and other systems serviceable in flight, using a trolley arrangement within the wing. None of these ideas survived and in the end it was the advent of commercial airlines which forced the adoption of a sensible and safe multiple engine concept which would stand the test of time.

4.13 Commercial airlines

The world’s civil airline operations got under way quickly after WW1. In 1919 there were a number of companies in Germany, France and England, operating adapted wartime designs. These were mostly single-engine types, but also larger transports modified from the most recently designed twin-engined bombers, which saw little if any service before the Armistice. The most widely used of these were the Handley Page 0/400 (The bloody Paralyser), which became the HP12, and the Farman F50 which progressed through to the F60 Goliath. The 0/400 was the same size as the IM except for having only two engines. Both Handley Page and Farman operated their own airlines.

There were four and five-engine aircraft also built near the end of the war. Handley Page produced prototypes of the four-engined V1500 and Zeppelin had had the five-engined Staaken series in wartime service. If developed for commercial use these would have offered very high engine failure survivability, but the economics were not acceptable to the struggling private airline companies. The same fate met the French contender. Farman produced prototypes for a four-engined ‘Super Goliath’ F140, which broke a number of performance records, but was never built for commercial service.

As the numbers of twin-engined converted bombers inevitably reduced either by crashing or otherwise being disposed of, new replacements were demanded and in a competition held in 1920 by the UK Air Ministry the winners were the four-seat Westland Limousine in the single engine class, and the new Handley Page W8 in the large twin-engine class. Surprisingly the W8 could not demonstrate the ability to survive an engine failure, even after the Ministry substantially reduced its certification passenger load from the proposed 15 to 12, only two or three more than the old 0/400.

So the new airline industry continued to rely upon successful forced landings as the means of surviving engine failure. Pilots kept in mind a string of preslected emergency landing fields along their land routes, but many forced landings still became crashes. The inability to operate at night or in poor visibility was a severe revenue earning restriction. There was also no easy solution to the engine failures which not infrequently caused ditchings in the English Channel and North Sea. The pressure for solutions prompted Handley Page to develop the W8e and W8f, both of which had a third engine in the nose. But these proved to be not much better than the twin-engine versions. One by one the European private airlines received subsidies from their governments, and this was followed in the UK in the form of allocated aircraft purchased direct from manufacturers, and this led in effect to govern-
Imperial Airways, the W10, went back to two engines. Unfortunately as gilding the lily and a new machine produced specifically for the service in the 8-10 passenger class, but there were continuing losses and after a year the remaining single engine types had to be scrapped.

Not surprisingly, by 1925 Handley Page had developed and flown another three-engined version of the W8, called the W9a Hampstead, which could maintain height with one engine stopped. So the year 1925 marks the time in England (and probably Europe) when fail-safety in commercial operations was achieved for engine failures, 12 years after the little recognised Sikorsky Ilya Mourometz. But only the one W9a was built, and by 1926, three engines would appear to have been considered as gilding the lily and a new machine produced specifically for Imperial Airways, the W10, went back to two engines. Unfortunately one of these soon went down in the Channel following engine failure and the crew and passengers had to be pulled out of the sea. So the progress towards getting aircraft into service which could survive engine failures in all the necessary circumstances was excruciatingly slow, despite the technical solutions being available for more than a decade. Another W10 went into the Channel in 1929, drowning four passengers.

Engine failures did not of course account for all crashes. Some were due to weather, other failures or mishandling, but the engine one was seen as the biggest problem. Records during the years of the 1920s show a steady decline in the accident rate, (Fig. 1), due partly to increases in reliability with hours flown as the efficiency of airline operations grew. Although in the 1920s the W8 and its derivatives flew more cross channel services than any other type, after 1926 in Imperial Airways there was a steady retirement of these and the single-engined types and a build up of a fleet of three-engined machines. These were the Armstrong-Whitworth Argosy and the de Havilland DH66 Hercules which then played a major part in its passenger operations up to the 1930s, when the world’s first four-engined commercial aircraft, the Handley Page HP42 was commissioned.

The multiple engine saga has been explored in the case of the UK passenger airline operations, this being the first example. But it is only one of perhaps six areas worldwide where manufacturers and airlines were co-owned in the 1920s and had similar problems in establishing safe operations. The counteracting pressures in the economics in first cost, running costs and revenue generation took precedence over safety in the early days resulting in very slow progress and this has not changed over the remainder of the 20th century despite the frequent protestations to the contrary.

4.14 Handley Page HP42 airliner — 1930: fail-safe milestone 3

The new Handley Page HP42 design, Fig. 17, was the world’s first four-engined airliner and the last of the big biplanes. It was also the first machine designed for fail-safety in every practical way, not only in respect of engines. It incorporated about 15 planned fail-safety design areas, and is represented here as fail-safety milestone 3.

The HP42 was the largest passenger carrying biplane ever built. It was primarily of metal frame construction, replacing the wood of its predecessors, and skinned with both fabric and metal. The wings were braced with Warren-girder type struts, giving an extremely strong mainplanes structure which also carried four engines grouped closely and safely above the non-seating area in the centre fuselage. The layout gave exceptionally low yawing moments in the event of an engine failure, thus simplifying asymmetrical flying. The wings also incorporated automatic anti-slab slats, a favourite invention of Frederick Handley Page.

The wing attachments to the fuselage, Fig. 18, were made to a redundant strut box giving fail-safety for any individual strut failure. The structure in most respects was a copy in duralumin or steel of the previous wooden equivalents but replaced all tensioned bracing wires with metal members. There were multiple elevators and rudders, Fig. 19, each with individual cable sets and similarly with the ailerons.

The HP42 represents, with hindsight, an historic dividing line between the early development of civil airliners aimed at performance, and development for planned safety, which was realised in a long fatal accident free operating life. Most important in the light of the enduring problem with engine failures in the decade after WW1, was that the HP42 with its four engines and significant excess power finally set a new standard for survivability of engine failures. During its proving trials the HP42 gave impressive flight demonstrations of manoeuvres at low level with three engines shut down. In its later service it could gain valuable time against its higher speed rivals by taking off directly from the air terminal apron and avoiding the line-up queues.

But the HP42 was the end of the era of very large biplanes. The era of higher speed metal monoplanes with higher altitude cruise performance and carrying more sophisticated onboard systems, some safety-critical, was all waiting in the wings. Blind flying instruments, lower weight more practical radio communications equipment, radio navigation and ground approach aids and extended air traffic control systems would...
enable scheduled night flying and oceanic flying with land planes. The new aircraft would inherit the standards for safety demanded in the 1930s, but the long struggle to achieve survivability using multiple engines would be repeated many times over with other safety-critical systems and sub-systems in the progress to the highest levels of safety in the new generations of design. This continues to the present day, either due to economic pressures or due to lack of understanding of fail-safe standards by new designers addressing new technology applications.

4.15 All-metal aircraft

All-metal aircraft were built around 1910 by both Hugo Junkers and Claudius Dornier. These were more robust and offered better damage tolerance than wood and fabric. But in 1919, Rohrbach in Germany introduced the concept of ‘stressed-skin construction’ which was taken up enthusiastically by the Americans in what became a revolutionary approach to construction. The first of these all-metal modern airliners was the Boeing 247 in 1933, to be followed quickly by the Douglas DC-1, the DC-2 in 1934 and in 1936, the DC-3, Fig. 21, which by 1939 carried 90% of all the world’s airline traffic.

4.16 Douglas DC-3 — 1935: fail-safety milestone 4

Over 13,000 of the DC-3 design were produced in WW2 as C-47s (Dakotas in UK) and 500 of the total were still operating commercially 35 years later. The DC-3 was a rugged reliable aircraft but it cannot be said that design for fail-safety in this and other metal monoplanes extended to more than 15-20 areas, not a huge advance on the HP42. The new safety-critical candidates included retractable undercarriages, manual variable pitch, constant speed and feathering propellers, deicing systems and some navigation equipment.

4.17 WW2 US four-engined commercial transports: fail-safety milestone 5

A new spate of piston-engined transports were developed in the USA during WW2, Fig. 22, primarily the DC-4 in 1942, the Lockheed Constellation in 1943, the Boeing Stratocruiser in 1944 and the Douglas DC-6 in 1946. These and their derivatives were to dominate the immediate post-war transport scene.

These were machines which cruised at altitudes of 17,000 to 20,000 feet and required new safety-critical installations including cabin pressurisation, variable pitch propellers and synchronisers and reversing propellers for braking the higher landing speeds. Communications, navigation equipment and low visibility landing instrumentation further complicated the safety provisions and the planned fail-safety design areas grew to at least 20 to 25 in number. A major flying controls problem also entered at this time. Pilot control force demands had been continuously increasing and the aerodynamic assistance using surface tabs and balancing of various types had design limitations. Hydraulic power boosted controls were therefore introduced, Fig. 23.

4.18 Boosted flying controls with manual reversion: 1950

These were safety-critical and employed fail-safety in the form of complex manual reversion linkages(43), which in practice could be more hazardous than the pure boosters and were not liked or trusted by pilots. The hydraulic power came from pumps driven by electric motor/gearboxes, which were unreliable, and pilots kept switching them on and off to check their availability. Rapid development of ideas for fully powered safe controls therefore ensued.

4.19 Fully powered flying controls arrangements

The first certificated commercial aircraft fully-powered systems were used, it is believed, on the world’s first passenger jet aircraft, the de Havilland Comet. The UK/ARB (Air Registration Board) made the key decision to accept that a hydraulic piston could not jam in its cylinder, a vital factor necessary to ensure the failure-survivability of parallel multiple power control connections to single surfaces.

Figure 24 shows a number of the many redundant arrangements of dual parallel or tandem pistons, multi-loadpath actuator rods and split
surfaces. Some hydraulics designers in the USA used valves with redundant inner and outer spools to overcome the effects of single seizures, the last being in the category of primary redundancy in fail-safe architecture as illustrated later in Fig. 38.

4.20 The Comet disasters

The Comet fuselage structural failures in the early 1950s sparked off in the aircraft design and certification world the most extensive rethink, not only of the safety of structures but of all aspects of safety in design.

The Comet accidents showed that the safe-life design criteria then employed backed by static load tests were inadequate to predict the life of the structure in the presence of varying load cycling which produced fatigue failure. Attempts to analyse the effects of fatigue for design purposes and predict failures due to it, were not determinate and repeatable, wide variations being observed with different designs and materials. The failure mechanisms were only partly understood. Many therefore felt that a fail-safety element in design must be added to the safe-life considerations, some even believing that it should become the dominant design criterion.

There then developed the concept that structures should be damage tolerant, and that emerging failures (cracks) could be allowed to develop to acceptable levels in the designated life of the structure. This would be done within an envelope of fail-safety design as a substitute for the previous safety-factor provision. Within limits crack development could be controlled with crack stopper holes or section thickening plates.

The extensive structural testing and analysis done in the United Kingdom following the Comet disasters was widely reported and absorbed by the aircraft design community and changed the whole philosophy of thinking about safety in design and its implementation and certification in all the aircraft engineering disciplines. The descriptive ‘fail-safe’ entered the English language at this time and became attached to the underlying concept of all aircraft design areas, not just structures. What had previously been achieved by default or in specialist equipment design was now formalised into requirements.

The new design thinking was supported in the United States and one opinion was outlined in a paper in April 1956 by J.F. McBrearty of Lockheed Aircraft, who strongly supported a move to fail-safe airframe design. He thought there had been a gradual evolution of the fail-safe concept, stating that “Much of the structure of today’s aeroplanes is now fail-safe (although perhaps not intentionally so) and it is believed that rather simple research, testing and analysis will show the way to a completely fail-safe airframe”.

Figure 22. Four-engined US commercial transports (WW2). Kenneth Munson: Peerage Books.

Figure 23. Power-boosted flying controls. Howard.

Figure 24. Fully powered flying controls. Howard.
4.21 Formalised fail-safety in design

In the areas of hydraulic, electro-hydraulic and electronic systems, new fail-safe designs were pursued which allowed considerable advances in capability hitherto ruled out as being intrinsically unsafe in relation to passenger aircraft standards. Early examples were electro-hydraulic yaw damping through rudder control, automatic coupled approaches to low level and later fully automatic landing (46,47).

One of the first aircraft to be designed in the UK in this period was the Vickers-Armstrongs VC10, which from the safety in design viewpoint will be taken as the next milestone example for the post-1950s. Whereas the HP42 was chosen as a milestone example which epitomised the outcome of everything learned about fail-safety up to 1930, the VC10 is the example for what was seen to be required from around 1960 onwards.


The four-engined VC10, Fig. 25, employed planned fail-safety in around 40 design areas, up to 50 per cent more than the number in the aircraft of the late piston-engine era. It was built for BOAC (British Overseas Airways Corporation) as a super-safe dependable aircraft for round-the-world use. Fail-safety was of the essence, and this was implemented in a manner and to an extent which in the majority of areas of design has not been exceeded in later generation aircraft (48).

The wings are a torsion box structure continuous across the fuselage and skinned with machined planks. The wings have both structural fail-safety in an alternative load path design and a safe-life which greatly exceeded its transatlantic contemporaries, being designed for hot-and-high airfield operations on ‘empire’ routes. New metal alloys with much improved fatigue characteristics were already in general use, and extensive anti-corrosion protection is applied. The fuselage makes extensive use of large machined skin panels along the sides which incorporate exit and window cut-outs.

Stringers are top-hat or Z-section for minimising corrosion. Extensive protection by sealing and pressurisation enhances the safety of the integrated fuel tanks and all fuel distribution systems and other systems incorporate extensive fail-safety. Space in this paper will not allow all of the fail-safe systems developments and applications to be covered (a list is given in the Appendix). However one major fail-safety complex is that of the flying controls systems, and their associated electrical and hydraulic power supply arrangements, and this will be briefly described as an example.

4.23 VC10 primary flying controls

The VC10 was designed as a completely power controlled aircraft, with no manual reversion. Control about each axis can be effected by one of two independent means so that in the event of a failure of one, the aircraft can be successfully flown and landed on the other.
The primary flying controls, Fig. 26, are split into multiple sections. Each section has its own electrohydraulic powered flying control unit incorporating a self-contained electrically pumped hydraulic supply. Multiple electrical supplies are provided from engine driven alternators.

The secondary controls surfaces, six spoilers, the multi-section slats and flaps and the tailplane (horizontal stabiliser) are split-powered from two hydraulic systems, each of these being fed by two engines, all four engines having variable delivery hydraulic pumps. The tailplane also has an independent back-up drive from a hydraulically driven ball-screw. Should the complete electrical system fail, the aircraft can be flown in pitch solely on the hydraulically driven tailplane, normally only used for trimming. In the roll control axis either ailerons or spoilers can control the aircraft in the event of a failure of either the electric or hydraulic system. In the remote event of extreme engine failures emergency power is maintained from a dual drop-out ram air turbine system, one driving an alternator and the other a pump.

4.24 VC10 artificial feel system (Hobson)

The wide stick force per ‘g’ range for the VC10 demanded an artificial feel system which is a duplicated fail-safe design, being completely unaffected if one system fails (Fig. 27). This extensive failure-survival capability was also supplemented by an extreme alternative ability of the aircraft to be flown manually on secondary controls alone combined with differential operation of the four throttle levers. There was a full-time duplicate-monitored automatic pilot system, the first ever, the engagement of which was effected directly into the integrated hydraulic power control actuators, so that in the event of any flying controls cables or rods becoming broken or jammed, the aircraft could be flown via the autopilot controller (itself internally duplicated) mounted on the pedestal between the pilots.

4.25 Power-by-wire power controls: Boulton Paul/Elliott

The power controls, Fig. 28, were each energised by an internal electrical drive to a small hydraulic pump system and the controls surfaces would be engaged normally in the full powered manual mode, or alternatively in an electrically coupled mode via a spring-loaded lock for autocontrol. The latter involved the substitution of electrical position feedback for the locked out mechanical feedback. So the arrangement was power-by-wire, a high safety capability still not provided in any current aircraft. The spring loaded lock was also calibrated to limit the force which could be reacted against the artificial feel unit. This provided two very important safety features. First it limited the demand which the autopilot could exert on the control surfaces, suitably geared by the artificial Q-feel, and second it limited (and caused indication of) any overriding force improperly applied by the crew when the aircraft has the autopilot and automatic trim engaged.

4.26 Triple series yaw dampers

On the VC10 the designers took the bold step of providing a triple series yaw damper system, Fig. 29, which had clearly visible survivability because of the split surfaces and separated power controls, operated from different electrical power buses. Full dependence on electrics and electronics was allowed for this vital system, the first time this had been done on any transport aircraft.

4.27 VC10 systems fail-safety by self-monitoring

The triple series yaw damper is an example of the use of full multiple redundancy (secondary redundancy as defined in Fig. 38). Most of the VC10 electronic sub-systems, for economy in overall design, used both primary and secondary redundancy, the former being called ‘self-monitoring’.

The desire to ensure the maximum possible realisation of fail-safety in the VC10 analogue automatic controls systems caused a special design modus-operandi to be adopted. The process required that ‘self-monitored’ safety-critical systems be first modelled in the style of full multiple redundancy with so-called ‘brick wall’ separation between lanes, and then be progressively studied to produce economic reductions which did not decrease the integrity implicit in the original model. Extensive testing and FMEA (failure
mode and effects analysis) were then conducted to ensure that the failure separation criteria were maintained in the resultant design\(^{51}\). ‘Absolute’ or ‘computation performance’ monitoring was not favoured as this could not be guaranteed to cover all potential failures. (Unfortunately such monitoring in the form of various data validity checks has come into wide use in digital systems, and should be treated with suspicion for safety-critical system application if it is single-thread and not a part of a wider multiple redundancy arrangement.)

4.28 The numbers game

The development of the VC10 and its contemporary in the UK the de Havilland Trident, with their greatly increased use of advanced fail-safety, combined with a general pressure from the aftermath of the Comet structural failures, made it desirable that a more analytical approach using a formalised numerical analysis should be adopted to assist in safety certification. This proceeded in parallel with the design and development of the aircraft and was dubbed ‘The Numbers Game’.

The prime problem was blind landing, so a joint industry–government–airline ‘Committee on Landing and Take-Off Aids for Civil Aircraft’ was formed by the ARB. The chairman was their chief technical officer Walter Tye, who had had a close involvement with fatigue research on the Comet investigations, which motivated the thinking on the certification of all safety-critical systems in the future. The ARB confirmed that numerical safety assessment methods using statistical data should be employed in the design and certification of the new automatic landing and other control systems, on the lines of recent work in other aircraft design areas, and left it to the industry designers to determine how this should be accomplished\(^{52}\). The analysis would for the first time spread over ‘systems of systems’, covering both ground and airborne installations in performance and survivability as an integrated whole.

4.29 VC10 automatic landing: 1960

The aircraft specified failure-survival automatic landing (Fig. 30). The author had the responsibility of launching the associated equipment programme across the various companies involved, and around 1960, drew this illustrated block diagram, which was subsequently widely reproduced\(^{53}\). This was the opening diagram of a set covering the separate constituent systems details, and launched the concept of using self-monitored sensors in duplicate-monitored systems (primary and secondary redundancy in Fig. 38). Neither government officials nor airport authorities were pleased with one of the consequences of fully automatic landing which was the future need to duplicate airport ground radio-guidance installations!

4.30 In-service automatic landing

The VC10 automatic landing system, Fig. 31, came into service in BOAC several years later, along with the Trident in BEA (British European Airways), by which time the Concorde SST automatic systems designs had followed directly from the VC10 in fail-safe design, but used new microcircuit technology and intermediate hydraulic control actuators to mix fly-by-wire, autopilot and pilots controls inputs, before passing the total demands to the main surface power controls.

4.31 The Concorde supersonic transport

The Concorde development brought to fruition the wide acceptance of electronics into safety-critical use in commercial aircraft. Figure 32 illustrates the full flight regime FBW (fly-by-wire) and AFCS (automatic flight control system)\(^{54}\). There were other major fail-safe systems notably the digital engine-intake controls. From the intensive Concorde
activity grew the sequence of CAA, SAE, FAA and JAA specifications and requirements leading to today’s design certification background. The wide-bodied aircraft which dominate the current world fleet maintain the same basic configurations of the earlier generations of jets but with some increases in the areas of coverage of safety-critical systems.

4.32 The Boeing 777 — 1995: fail-safety milestone

As an example the Boeing 777, Fig. 33, is estimated by the author’s criteria to have planned fail-safety in around 50 design areas.

4.33 Boeing 777 fly-by-wire

In one of the new areas, the fly-by-wire system, Fig. 34, each of three computers (in secondary redundancy architecture) incorporates in primary redundancy architecture, a triple dissimilar integral concept designed to absorb rare and unpredictable hardware and software internal failures.(55) This is a super-safety standard which also gives a ‘deferred’ maintenance capability amounting to almost the life of the aircraft. ‘Deferred’ maintenance is a potential bonus in a removable item when its level of design redundancy greatly exceeds the minimum certification safety requirements, and its reliability is high in practice. The equipment has performed much better than design estimates, and achieves an average time to first failure of over 50,000 hours, even before the deferred capability is invoked.

4.34 Integral redundancy (primary) redundancy fail-safe architecture

The Boeing 777 primary flight computers employ the principle of internal electronic failure-survivability, or integral redundancy, first developed in analogue form for fly-by-wire application in 1962 by Elliott Flight Automation, later to become GEC Avionics Ltd.(56). A working computer was demonstrated at the Farnborough Air Show in that year, Fig. 35. Digital microprocessor technology allowed a more extensive implementation to be applied as primary redundancy in the architecture of the B777 fly-by-wire computers.

4.35 Boeing 777 primary flight controls computers

It can now be said that the computers in the Boeing 777, Fig. 36, have a reliability in performing defined tasks at least 20 times greater than any human being, the ramifications of which are very relevant to the super-safety target to be discussed later.

4.36 The evolution of fail-safety performance in aircraft engineering

The history outlined has shown that from approximately the year 1912 there was a growing realisation that special means would need to be provided in the design of heavier-than-air flying machines to protect the machine and its occupants against the inevitable failures which would occur during their operation. This was the birth of the design and operational concept of fail-safety, and its growth to the present day has been broadly estimated in terms of the numbers of ‘fail-safety areas’ in each of the ‘milestone’ aircraft examples described (see Appendix). In Section 3.1 it was also postulated that all fatal accidents must now be the result of the loss (or lack of adequate implementation) of a fail-

---

Figure 34. Boeing 777 Primary flight controls computer architecture. BAE Systems.

Figure 35. Electronic integral (primary) redundancy concept (1961) and fly-by-wire computer demonstrator. BAE Systems.

Figure 36. Boeing 777 Primary flight controls computer. BAE Systems.
It is of interest now to consider the quotients $\frac{B}{C(-5)}$ and $\frac{B}{C(-15)}$. These are the ratios of the accident rates attributed to engineering causes in Graph B to the fail-safe state-of-the-art applications five and 15 years earlier in Graph C. This will give some indication of the accident rate attributed to each fail-safe design area after the five to 15 year delay, assuming that these rates are all roughly equal, which they should be, considering the sequential nature of the historic development and application of individual fail-safe sub-systems. The later figures are also a guide for the many future designers in each discipline as to what they need to achieve to pull their weight in attaining higher overall safety in a complete aircraft. The results are plotted in Graphs D5 and D15 respectively.

A number of general observations can now be made on the historic evolution of the use of fail-safe concepts.

1. Over the 70 year period from 1925 to 1995 the average accident rate attributable to each fail-safety design area dropped steadily year on year from $3.6 \times 10^{-6}$ per hour to $0.0023 \times 10^{-6}$ per hour, a remarkable factor of over 1,500 (70 times in the first 35 years and over 20 times in the second 35 years). This would have required first, a considerable improvement in both the reliability and fail-safe architecture in existing areas, and second, no increase of accident attribution by any of the new areas of design involved in getting improved performance and capability. The former would be accounted for partly by considerable technology improvements, for example in structures, the early move from wood and fabric to specialist metals and stressed skins and later to the inclusion of composites; in engines, the change from internal combustion to gas turbine; in systems, the vast impact of the last 45 years of high pres-sure electro-hydraulics and electronics in most controls areas. The second point derives from the unwritten principle in civil aircraft design, usually ensured by certification authorities, that no new technical advance applied in any safety-critical area should decrease the safety contribution already made by the existing design in that area. In fact new designs invariably improved the area safety contribution (i.e. decreased the failure probability in that area) and so the overall system safety improved, usually for both the basic reliability and fail-safety architecture reasons. So as capacity, speed, height and navigation accuracy improved, the additional complexity was always self-supporting in the safety dimension. The question today is whether this is continuing at the low probability levels now involved. From 1960 to 1980, the accident rate attributed to each fail-safe area reduced from $5 \times 10^{-6}$ per hour to $0.6 \times 10^{-6}$, a factor of around 8. From 1980 to 2000 the reduction will be a factor of 3, a significant fall-off. It is the author's view that the overall reduction in the efficacy of fail-safety in the engineering area is a contributing cause of the flattening of the accident rate, and a strong pointer to other root causes in the piloting and operational areas.
2. The large numbers of fail-safety areas progressively introduced throughout aircraft development history, and the corresponding decrease in the accident rate attributed to each, now makes it increasingly difficult for designs in each fail-safety area to be validated. It is real possible to prove in any practical testing that individual fail-safety provisions are alive and working, as the failure-probability figures are far too small. For example if the overall ‘engineering’ accident rate is now taken as $0.15 \times 10^{-6} \text{ per hour}$, then with 50 fail-safe areas, each will need to be designed to be better than $0.15/50 \times 10^{-6} = 3 \times 10^{-9} \text{ per hour}$, i.e. between $0.1 \times 10^{-6}$ and $1 \times 10^{-6} \text{ per hour}$. This difficulty did not always exist. In early history the extent of the protection which could be given by dual ignition in an i.c. engine, for example, was not difficult for all to grasp. But 80 years later the degree of safety designed into a digital fly-by-wire computer is not so easily understood. Its safety contribution can only be established theoretically, based on the redundancy levels used, and on the assumption that the multiple parts are truly independent, which has practical but generally unknown limits. A matter of interest in this is to see at what time in history the architecture of fail-safety ceased to work at probability levels which were within the everyday experience and appreciation of the designers and engineers responsible for formulating and supporting sub-system designs. The author’s experience in the aerospace field is that probabilities in one in a million hours, which is somewhat less than once in a lifetime, represent the limit of design or operational error prediction that can be mentally appreciated, and only after many years of experience with failure-survival systems. Anything lower than this becomes a mathematical quantity only and is difficult to comprehend as a physical reality. After this designers will have little feel for the probability of fail-safe architecture breakdown such as might be the result of common-mode failures in multiple redundant systems. The assessments in Figure 37 now indicate that the one in a million ‘appréciation barrier’ might have been reached around the time of the DC3 going into service in the 1930s, and through to the development of the new range of larger post DC3 transport aircraft in WW2. The wartime operations damage expert-ences would have given a considerable boost to the engineering apprehension of design for survivability. By the late 1940s fatal accident probabilities per fail-safe design area were moving towards $1 \times 10^{-6}$ and were accelerated by the actions taken following the Comet accidents in the early 1950s. Later in the 1950s numerical analysis and rules for fail-safe design were developed and the VC10 design programme has been described as an important example of the outcome from this. But the need for $1 \times 10^{-6}$, $10^{-7}$ and $10^{-8} \text{ per hour}$ has moved safety-in-design achievement quite positively into a ‘dark’ area from which there can never emerge sufficient evidence to know if sub-systems achieve these figures or not. If they do not, this would be a factor in the flattening of the accident rate. So the understanding of design engineers moved from direct practical apprehension, to a need to understand probability predictions as part of the process of designing to achieve remote failure-rate values. The best assurance that designers can devise to accommodate this when employing multiple sub-systems comes from great attention to isolation criteria, an outstanding example being that between engines, and otherwise wide-scale use of dissimilar redundancy or other dissimilar back-up in as many of the fail-safety applications as possible. (There is an ultimate limit. When the ability to achieve adequate isolation of the redundant elements of a fail-safe system ‘bottoms out’, the common-mode failure “barrier” has been reached. When all fail-safe sub-systems and back-up provisions reach this limit, whatever level it is, perhaps $10^{-7}$ or $10^{-8} \text{ per hour}$, then increasing their number will no longer just limit the accident rate as it did at higher levels, but increase it! But the consolation prize is that the accident rate should then be so low as to be of any concern.)

3. As safety levels are totally dependent on fail-safety, and most high level fail-safety now resides in the ‘dark area’, the question must be raised as to what extent modifications based upon ‘failures already experienced’ in service is useful. In the case of fatal accidents, which in the engineering area would have involved multiple remote failures, the answer may be that not much will be achieved because there will be a large number of such very remote possibilities. In the case of repeated first or partial failures, or repeated similar incidents, a potential breakdown in a fail-safety system might be implied, and these should be within the compass of normal engineering understanding and can usually be corrected. However such action will not be demanded of all first failures which evolve into incidents. Most will never be repeated, but will be replaced by others not yet experienced or predicted. There is much to be said for concentrating accident investigations first on why ‘fail-safety’ failed, rather than on the individual root causes, which should reveal themselves when the fail-safety breakdown is uncovered. In practice these approaches are frequently mixed, but the separate elements are not always delineated.

4.37 Categories of fail-safe architecture

In Section 2, the concept of fail-safe architecture was introduced as a vital element in the achievement of high levels of safety. It was described as a family of multiple package of different techniques used for surviving failures. The background history described in this Section 4, along with many other examples of modern design in the commercial aviation field, now invites a detailed classification of fail-safe architecture in its various forms.

Fail-safe architecture may be considered as comprising three main categories. These are illustrated in the block diagram of Fig. 38, a derivative of the earlier Fig. 3, and described as primary redundancy, secondary redundancy and damage protection redundancy. The primary and secondary redundancy categories each have sub-categories which cover the various methods used to achieve fail-safety. The figure gives examples of practical implementations in engineering and piloting which fall into the various sub-categories, this being a representative rather than a complete list. The reader is reminded that this paper is concerned with the safety of engineering and piloting of large transport aircraft and not with safety of performance and this is not included or inferred in the representations in Fig. 38.

Primary redundancy is applied in two senses, first where it is the only practical fail-safe method possible, and second as a forerunner to the further use of secondary redundancy. This is both the oldest and the newest architectural technique in fail-safety, which is sometimes referred to as ‘integral redundancy’. Primary redundancy was important in early structural design, but the manner of its use has varied considerably throughout aviation history. In pioneer aircraft the structural load was taken entirely by fabric covered wooden structure and fail-safety was achieved, to some extent inadvertently, by internal redundant stiffening members and on the large biplanes with multiple struts and bracing wires between the wings. The required degree of robustness determined the minimum dimensions of members, and stiffness the numbers used, so it transpired that redundant members arrived by default. The same applied when wood was replaced by metal. Much multiple (secondary) redundancy ceased to be applicable on modern metal monoplanes, but the advent of stressed skin changed the means for getting alternative load paths. However, the analytical problem of proving the safety of such structure was not sufficiently definitive. So the design safety was assessed instead from static load testing on rigs and estimates of safe-life based on measured gust accelerations coupled with the application of a generous design safety factor.

The Comet accidents investigations then uncovered the depth of the metal fatigue problem, and the variability of results on sample testing encouraged for a while a new attempt at designing for fail-safety. However fatigue-failure accidents continued to occur and manufacturers and certification authorities preferred the higher certainty of results obtained from dynamic rig testing of basic safe-life designs, which have continued until the present day. This has been further justified by the wide scale use of large forgings and machining of skin/web planks with integrally stiffened exit and window openings which have useful crack diversion properties. There is also now the use of layered and stitched composite elements
in many parts of a total structure. In the context of this paper (refer-
ence Fig. 3), current design practice in structures amounts to greatly
increased reliability in the basic structural parts and a much
decreased requirement for fail-safety in the overall design, although
the ratio of the two will vary considerably, particularly for example
with the different requirements for fuselage, wings and other
surfaces. Primary redundancy is now mainly confined to the
fastening areas and joints of the large metal sections and assemblies
which make up complete structures.

Landing gear safety design is in the category of primary redun-
dancy, employing partial redundancy where possible, such as
wheels, tyres and brakes and steering. It also has graded structural
fusing of struts and braces and free-fall backup to powered actuation.
It is a complex integrally redundant system with planned alternate
and fail-safe degradation if overloaded.

In this primary redundancy category is also one of the historic
‘firsts’ of all fail-safety design actions, the use of dual ignition on
piston engines, which was adopted from 1912 to counteract the then
notoriously bad reliability of spark plugs and magnetos. A more
recent example is the engine-mounted multiple FADECs (full
authority digital engine controls). In this high integrity category also
is the triple dissimilar microprocessor structure in the Boeing 777
primary controls fly-by-wire system computers which achieves an
effective reliability so high that it is given ‘deferred maintenance’
status, in effect absorbing internal failures for periods which could
be up to the life of the aircraft.

There are four mainstream fail-safety sub-categories under the
secondary redundancy architecture which cover the range of design
implementations from multiple systems and sub-systems through
crew manual backup to alternative flying controls and other systems
reconfigurations and also special envelope monitoring systems such
as GPWS (ground proximity warning system) and TCAS (traffic
collision avoidance system). Some systems employ both primary and
secondary redundant architecture, notable examples being electro-
hydraulic and hydraulic powered controls. A relatively new example
is the fly-by-wire system of the Boeing 777 which triplicates the
integrally redundant computers described above.

Damage protection redundancy covers failures which can cause
hazardous cascade damage outside the system or subsystem area in
which a root failure occurs. The prime examples involve the release
of high energy failed metal parts, usually from rotating machinery,
examples being loss of turbine blades due to bird strikes and even
the rare release of a turbine disc. Energy absorbing blade catcher
rings are standard and disc release protection is now also provided
by some engines, a very expensive protection. However not all
damage protection is so costly, it can be as simple as stress-relieving
hole-stoppers at the ends of cracks in structure, some of which can
have the effect of improving the safety above the original design
level. An important major example is the planned release of engine
pods by structural fusing in the event of very severe loading which
might otherwise cause the departure of a complete wing. Energy
absorbing containers have also been designed to protect against
terrorist bomb explosions in luggage. Other examples in the damage
protection category are listed in the diagram.
lower than desired in a modern transport aircraft. Pilots make more mistakes than they ever need to admit to, and the situation has worsened with the use of new cockpit automation and fewer crew, who now lack the continuous awareness involvement of earlier designs. Second, the vital cross-monitoring in the cockpit, the fail-safety element, does not appear to work very well in the modern workload environment, another consequence of inadequate visibility in the automation which was meant to ease the workload problem. A review of the history in the jet age reminds us that new technology encouraged a change in direction from the long developed crew/cockpit management set-up. Cockpit management in the first generation jets, supported by separate instruments and individual director/autopilot mode selector switches gave very satisfactory performance and safety at the time.

5.0 CREW FAIL-SAFETY

The evolution of fail-safety described in Section 4 was dominated by engineering development, and while it did not exclude the piloting aspect, it is only in the last few decades that aircraft overall safety has become progressively to be dominated by crew performance. It is now vitally important to consider how this might be significantly improved. Whereas the engineering aspects of aircraft moved steadily into the use of more and more fail-safety in design as performance demands increased, design for safety in the cockpit has fluctuated.

Fail-safety in crew operations is as vital as in engineering machine operations, but it has lacked any numerical evaluation means which could be used to analyse overall system improvements or limitations. Much of the numerical evaluation conducted in the human factors area has been taken no further than single pilot performance, and is therefore unrealistic in an overall safety assessment context. On the face of it, a crew of two pilots with strong cross-checking in their cockpit activity should be well up the scale in safety contribution. A single commercial pilot who makes one potentially fatal flying management error in a whole career of say 25,000 hours flying (and most retired pilots will admit to at least one), could be said to have, at a high confidence level, a failure probability of around one in 7,000 hours. With a comparable independently minded partner, this should yield an average accident level as low as \((1/7,000)^2\), or better than two in 100 million hours. We know that the average world figure is about 100 times worse than this, so what is wrong?

The probable answer is twofold. First the pilot reliability at best is lower than desired in a modern transport aircraft. Pilots make more mistakes than they ever need to admit to, and the situation has worsened with the use of new cockpit automation and fewer crew, who now lack the continuous awareness involvement of earlier designs. Second, the vital cross-monitoring in the cockpit, the fail-safety element, does not appear to work very well in the modern workload environment, another consequence of inadequate visibility in the automation which was meant to ease the workload problem. A review of the history in the jet age reminds us that new technology encouraged a change in direction from the long developed crew/cockpit management set-up. Cockpit management in the first generation jets, supported by separate instruments and individual director/autopilot mode selector switches gave very satisfactory performance and safety at the time.

5.1 The VC10 cockpit

Figure 39 reminds us that the above process was assisted by having four crew, as in this VC10, and the later descent to three and then two crew, overlapping with the development of integrated CRT (cathode ray tube) instruments, took cockpit safety into an area of indeterminacy and ambiguity. This downward progression can be understood from a comparison between cockpit management in earlier conventional instrument cockpits and later generation glass cockpits. A suitable candidate for the former is the most advanced ‘first/second’ generation jet, the Concorde SST.

5.2 The Concorde cockpit

The Concorde, Fig. 40, has an automatic mode complexity not very different from that in the current generation of jet aircraft, and a flight is progressed from mode to mode through discrete pilot actions\(^{(54,57)}\). A new mode is selected when it is required, by pilot action, and an old one is discarded when required, by pilot action. If a failure occurs in any mode, automatic error detection by absolute or cross-monitoring alerts the crew. The discrete step by step progress between modes can be managed and monitored by the two (or three) pilots, against a thorough understanding and awareness of the current situation because they are there and taking the actions in real time. If air traffic changes are demanded, they can be inserted directly into the current instrument panel selection, with no question about any incompatibility with a previous existing or pre-programmed selection.

Panel instruments are also not multi-functional. A pilot knows that each instrument in its place gives one specific piece of data only for building and maintaining his situation awareness picture. Information cannot be cross-fed from one display to another other than by a pilot switch action, which remains visible or continuously indicated. There is a continuous aura of total situation awareness from single data sources which are duplicated and provide a complete but simple means for crew cross-monitoring. The dual autopilot controller is a single unit, the first ever to be mounted in the centre of the coaming, clear and unambiguous in use. This now ‘much-dated’ 1960s design clearly employed what is now called ‘human-centred automation’, not a new idea, merely a recently resurrected one.

5.3 Cockpit automation

After Concorde and the earlier subsonic jets, as technology advanced, there was an irresistible desire to automate cockpit selections, using the new programming potential made possible by the advent of airborne digital computers and glass cockpit (CRT and flat panel) displays. It was seen against the increasing complexity of the operating environment that a seamless progress could be made from mode to mode in flight operations through preselected programmes of automatic control, instrument display and radio frequency selections, all planned and loaded before take-off. Thus was born the full concept of cockpit automation and the creation of the automated flight management system (FMS).
Unfortunately experience now seems to show that despite the attractive new technology, and reductions in pilot work-load, there has been a backward movement in the long established standards of safety management by humans in the cockpit. Numerous FMS/Glass cockpit systems are now in service, each customised for the particular aircraft.

5.4 The cockpit of the Airbus A320

Figure 41 illustrates the new level of reading clarity and elegant simplicity which modern equipment and technology allows. This reflects the second generation of development in ‘glass’ cockpits, the first using video displays, the second using liquid crystal flat panel displays (LCDs). Airbus has written that “this was designed to meet the continuous increase of aircraft sophistication required to improve the level of safety and efficiency ... and is intended to ensure that the fail-safe concept applied to the crew, as well as to system management, that the ergonomic principles were effective, and more visibility and comfort were offered. This implied that every task could be performed by both crew members, that they could cross-check each other.” This could not have been better said, and other aircraft manufacturing companies also put such new sophistication into the hands of the airlines and their crews.

But it has not turned out as well as the designers expected. The new glass cockpits and flight management systems have not justified the move to two crew. This was a cavalier decision by a committee pressed by airlines and manufacturers for economic reasons, and the committee’s conclusion that safety was unaffected cannot be justified by statistical samples of experience or numerical evaluation. There are few crews who would not welcome back the pilot/flight engineer officer. However the clock can probably not be turned back. It is certain that not enough serious thought was given at the time by the key certification authorities to the full safety implications of these developments for the users. There is continuing evidence that pilots are still not adequately employing or understanding the ramifications of what they have now got. Before the cockpit automation era, pilots were thoroughly acquainted with and normally understood completely the range of data presented to them and the overall picture conveyed. There is admittedly evidence throughout flying history that sometimes valid instrument readings were ignored by the crew, but prior to the automated cockpit there were few if any occasions when a pilot said “I don’t know what’s going on----I have lost the picture.” Now they are not always so sure, and cockpit questions such as “why did it change mode?” are normal in a day’s flying, which would seem to imply that the crew is no longer in full charge. It is said that ‘pilots used to know exactly what they were controlling, but now the FMS runs the pilots’.

Some pilots will insert erroneous data to achieve what they want rather than what the FMS wants. With enhanced FMS and ACARS (automatic communications and reporting system) the pilots can respond to suggestions from Centre merely by pushing an ‘acknowledge’ button. The FMS will be ‘in the picture’ but will the crew? Today the pilot-error proportion of accident responsibility is too large and the level too high, and it is likely that it was better 20-30 years ago than it is today.

Two pilot cockpits now dominate and it should be reasonably expected that, analogous with engineering, the ingredients of pilot reliability and fail-safe cross-monitoring will provide the necessary safety. However there is considerable doubt whether current cockpit systems make this feasible and whether the trend in two-crew cockpit automation development is heading towards a viable safety future, or whether some changes in direction may be required. Certainly there needs to be a greater emphasis in the displays community on safety targets rather than performance targets, and this is attracting a great deal of attention from the human factors community, but so far there is more analysis (much of it wrong) than progress.

6.0 CREW PROGRESS IN FAIL-SAFETY EVOLUTION

The history from the viewpoint of fail-safety in both ‘engineering’ and ‘piloting’ has now been discussed and the achievements can be illustrated in a summary version of the reliability/architecture structure originally described in Fig. 3. Figure 42 depicts this diagrammatically in the form of different paths taken by the prime contributors over the history of aircraft development through increasing reliability and varying fail-safe architecture. Structures, engines, equipment and avionics elements have all got to significant levels, as previously described, but in recent years the crew fail-safety would appear to have had a reversal.

One reason for the dichotomy between ‘engineering’ and ‘crew’ achievements in safety is the lack of a measure of relative crew performance. There is a reluctance by the design community to attempt any numerical analyses in the piloting case of the sort that has guided the very significant advances in safety in engineering developments since the Comet days. Crew operational analysis has been almost totally neglected or become bogged down in pilot-error human factors analyses which largely neglect the importance of fail-safety and pursue recommendations which are in general either unusable or already well-known to experienced designers of cockpit and automatic systems. Crew-error has been known for some time to be the major element of the accident rate of large transports, and methods of assessment which could fit it into the numerical analysis picture of the flying machine and its operations would give the total picture for determining future safety design strategy.
7.0 AN APPROACH TO ERROR ASSESSMENT IN A TWO-CREW COCKPIT

The normal approach aircraft systems designers would take towards achieving higher safety in an existing system would involve the assessment of the redundancy architecture, either to determine why it was not working to the level required, or to introduce new elements where fail-safety design was lacking. The parallel for the cockpit would be to assess the adequacy of the multiple information presented to the two crew members, the nature and degree of the comparison cross-monitoring assessment carried out between them, and the validity of any ensuing action. There are strong analogies between the well-established engineering machine safety management previously outlined and human information processing management. The crew can be considered as a duplicated management system in the same way as one would treat the duplicated flight management software/hardware system.

7.1 Flight deck system 1

Aerospace systems engineers will be familiar with the layout of the flight deck system block diagram Fig. 43, as being of the family used in planning hardware/software failure-survival systems architecture. In principle it comprises independent lanes which are cross-compared to detect failures. It is assumed that insofar as information is passed to the displays on both sides of the cockpit from the Flight management system computing, that this is loaded and checked independently and not merely copied from one to the other, either by computing software or crew action. By the same token any demand changes by a crew member on his/her side of the cockpit is assumed not to be automatically transferred to the other side. This diagram differs from its engineering counterparts only in that it is solely an information processing and pilot action flow diagram. The flight deck concept is that information presented by cockpit sensor and computer displays is assessed separately and more-or-less continuously by the two pilots, decisions for action or inaction are taken as required and then implemented by way of the cockpit resources management (CRM) process by pilot/flying or pilot/monitoring.

The sensor and flight management computer information is duplicated, one set being presented direct to each pilot, but cockpit layouts allow both pilots a reasonable sight across the whole dual panel layout and this is indicated by the crossed dotted arrows. CRM (cockpit resources management) determines the flying and non-flying (monitoring) tasks and actions which follow. The warnings box is shown as receiving information from both display/computer systems, and these will comprise both a cross-comparison set and a system self-checking set, suitably displayed in practice on central or distributed warning panels. It is also the area from which aircraft system failure management requirements will be indicated for crew action. At the top of the diagram are two functions describing the accident probabilities of the ‘awareness’ and ‘action’ sections, which should now be explained.

7.2 Crew awareness analysis

In the strictest sense, assuming the pilots operate independently, the general probability of a hazardous crew awareness error leading to an accident $P_d$ will take the form, shown in Fig. 43, of

$$P_d = (P_1 P_2 + P_1 P_2 + P_2 P_1) + (P_{1A} P_{2A})$$

where $P_1$ and $P_2$ are the probabilities of each of the two individual pilots generating awareness errors which could singly lead to an accident, and $P_{1A}$ and $P_{2A}$ are the corresponding probabilities of each of the two partner pilots failing to detect and counteract the other’s awareness error (58, 59). For the highest cross-monitoring performance $P_{1A}$ and $P_{2A}$ would approach zero. (Note: $P_1$ and $P_2$ do not necessarily designate respectively ‘pilot-flying’ or ‘pilot-non-flying’ as these could be either allocations.) $P_{1A}$ and $P_{2A}$ in Fig. 43 are the probabilities of ‘pilots’ action’ errors and $P_{1A}$ and $P_{2A}$ are the corresponding

Figure 43. Flight deck system concept and crew accident probability (two crew). Howard.
probabilities of ‘pilots’ cross-monitoring’ not detecting such errors, and these are consolidated in the equation as \( P_1 \) and \( P_2 \).

In the case of ‘engineering’ systems, such probabilities are evaluated for design using the MTBF (mean time between failures) formula derived from the Poisson distribution of failure probability

\[
P = (1 - e^{-\lambda t})
\]

where \( \lambda \) is the failure rate and \( t \) is the period at risk. If the MTBF = \( M \) then the Poisson distribution converts to:

\[
P = (1 - e^{-\lambda t/M})
\]

where \( M \) is the inverse of the failure rate provided failures have a random probability of occurrence at an average constant rate. Further, \( P \) approximates to \( t/M \) where \( t \) is considerably smaller than \( M \), as it is in all practical aircraft system cases.

The MTBF concept is not normally used for assessing human failure rates, but in the context of continuous two crew cockpit management (excluding periods of aircraft manual handling) which is the prime activity in automated cockpit operations, it would seem to be applicable. It is therefore suggested that ‘management’ activity can be considered as a continuous flow of incoming information demanding ‘awareness’ decisions and ‘actions’, with pilot errors arising as randomly distributed occurrences.

A better understanding of this pilot management model is obtained by defining error potential in the major crew tasks, which can be divided into four main groups, which of course may be intermingled.

- **Group 1** would cover incorrect action or inaction on, or selection of, autopilot modes, navigation parameters, fuel management, ATC instructions, communications channels, altimeter settings or similar operational functions which at the time could lead to hazardous situations such as loss of power, loss of control or in-flight collision.

- **Group 2** would cover errors in conduct of procedures for shutting down failed elements of fail-safe (redundant) systems, singly or in dependent cascade groups as necessary, and in setting up flight diversions if demanded by certification or airline company requirements.

- **Group 3** would cover errors in carrying out standard procedures to deal with detected hazards caused by fire, icing, clear air turbulence, microbursts, volcanic dust, loss of control and other comparable hazards.

- **Group 4** would cover failures resulting from crew intervention in automatic protection systems or provisions or automatic redundancy management. Such capability is designed into those systems where excessive demands may need to be countered or when quick isolation of failed elements is necessary to avoid dangerous structural overloads or rapid progression towards unacceptable conditions. It is important in systems which are providing automatic flight envelope protection or are part of the controls complex such as the primary and secondary flying controls hydraulic and electrohydraulic actuators and fly-by-wire computers, and also automatic pilots, trim systems and comparable systems.

So far the flight deck piloting system has been described as analogous to the corresponding hardware system counterparts, but there are in fact two important differences to take into account. The first is that the degree of comparison cross-monitoring is variable, depending on personalities, checking skills, and the working relationship between the two crew members. Second, the LHS and RHS ‘awareness’ lanes are not strictly independent in practice, so the probability equation is unlikely to be valid to the lowest levels achieved by the analogous fail-safe ‘engineering’ systems as discussed in Section 3. Both of these differences should be accommodated as far as is feasible in formulating any numerical solution, and will be returned to later in this section.

The probability function \( P_2 \) is best explored graphically for a range of parameters, as no specific values are available, and some simplifications are desirable to enable this. First while \( P_t \) and \( P_3t \), were included for completeness, their product is relatively small in practice and can be neglected for the purposes of the broad assessment intended. A simplification can also come from allowing the two pilots to have the same error generating probability \( P \), giving \( P_1 = P_2 = P \), and likewise the same cross-monitoring error probability \( P \), giving \( P_1 = P_2 = P \).

The standard technique used in the design of engineering systems can then be followed as proposed above by expressing the probabilities of form \( P \) and \( P \) as equal respectively to the forms \( t/M \) and \( t/M \), where \( t \) is the time of exposure and \( M \) the mean time between awareness failures (MTBAF) for pilot-generated awareness errors, and \( M \) the MTBAF of pilot cross-monitoring errors, the latter accounting for trans-cockpit inaction as well as varying efficiency in performing the wide range of cross-checking actions.

Some further manipulation then reduces the crew accident probability equation to:

\[
P_{CV} = \left(1 + 2/M \right) - M/M
\]

where the \( M/M \) ratio is introduced as a convenient measure of a variable cross-monitoring effectiveness. \( M/M \) is a floating ratio and therefore may not be an ideal basis for assessment. But for fully trained and experienced pilots \( M \) might be expected to be relatively fixed, and it has already been assumed above that there is equality in this respect across the cockpit. Hence \( M/M \) can be taken as being reasonably proportional to \( M \), and therefore an acceptable measure of the level of cross-monitoring.

On the matter of constancy of error rate in the Poisson expression it is not unreasonable to assume that the continuous train of safety-critical tasks handled by pilots in the cockpit management process would result in a constant error rate determined by their performance in the workplace circumstances. This does not exclude variable failure rates as envisaged in the extremes of the classic ‘bath tub’ curves for engineering ‘components’ which include infant mortality and wear out. In engineering, infant mortality is all but eliminated by automated manufacture and the use of ‘burn-in’ in the manufacturing process, and wear-out by scheduled maintenance or redundancy.

The corresponding analogous mitigations also exist in the case of pilots. It can be argued that individual pilots exhibit equivalent ‘bath-tub’ curve extremes in the form first of early inexperience, and finally in the end-of-career complacency and inability to learn new skills. But as with engineering, these are counteracted in the pilot case by a high level of early training, including the extensive simulation activity, and at the other extreme by a relatively early retirement age.

It is frequently argued that the type of assessment suggested cannot be applied to human pilots as it does to equipment, as humans may be influenced by day to day problems with their families, colleagues, management or health. But the concept of fail-safety reasonably assumes that there should not be a high probability of coincidence of such problems in crew members which could destroy ‘cross-monitoring’ and generate hazardous situations. There are certainly workload and operations pressures which will affect two pilots at the same time and these are discussed later under ‘common-mode’ errors.

So reiterating, crew numerical evaluation can be pursued on the assumption, previously defined, that crew activity comprises continuous ‘awareness’ assessment by both pilots, punctuated by decisions leading to cockpit actions throughout a flight, these being implemented by either pilot and monitored by the other according to cockpit resources management (CRM) procedure as determined by the captain as pilot-in-charge. Errors made by pilots in their ‘management’ and ‘monitoring’ modes will be considered to have a random distribution and occur at a constant average rate, and can therefore be described by a Poisson probability distribution, manifested in an MTBF equation. For the remainder of this paper the abbreviation MTBF will be reserved for its standard use in relation to engineering systems, and MTBAF (mean time between awareness failures) will be used to refer to pilot management failures. The crew accident probability \( P_{CV} \) is now plotted as a function of \( M/M \) in this MTBAF equation, Fig. 44.
7.3 Crew accident probability: per-hour general basis

$P_c$ is shown for $t = 1$ hour plotted against $M/M$ (the ratio of cross-monitoring error rate to management demand error rate) over the range 0.02 to 1.5 for values of $M = 1,000, 2,000, 3,000, 5,000, 7,000, 10,000, 20,000$ and $50,000$ hours.

The horizontal line at $0.6 \times 10^{-6}$ has been chosen to be reasonably representative of the currently achieved world average accident probability which is due to the management content of ‘pilot-error’. (There is also a ‘manual handling’ content of pilot-error which cannot be assessed on an MTBF basis, but this is a relatively small portion of total pilot-error and it is therefore convenient to exclude it from this analysis.)

It can be seen that the pilot MTBAF would have to be at least 2,500 hours for the current safety level to be achieved and this would need to be supported by a cross-monitoring performance of $M/M = 0.9$ or greater. A pilot prime error rate with an MTBAF of 5,000 hours could also achieve the current accident rate with only minimal help from cross-monitoring, $M/M$ being around 0.15. However, experience tells us that on a world average basis what is most likely is that $M/M$ is around 0.4, and that the corresponding pilot MTBAF is around 3,000 hours. The curves all become asymptotic to a high failure probability at low $M/M$ where even the best pilots are unlikely to meet the current safety level without the support of some cross-monitoring.

While the assumptions made in arriving at Fig. 44 give both pilots equal error making and error cross-checking performance, the required current safety level can only be sensibly achieved with MTBAFs above 3,000 hours. It will be apparent therefore that the left hand side of this graph set is more likely to be the domain of the dominant low-error rate captain, while the right hand side is more likely to be the domain of more democratic management on the flight deck, and there is in practice a wide population range.

Moving to the super-safety target rate, as ‘pilot-error’ in cockpit ‘management’ is the largest contributor to the accident rate, it is reasonable to ask as a target that this alone should have at least a 10 times improvement requirement imposed. So this is represented by the horizontal line at $0.06 \times 10^{-6}$. It is clear from this that even with very significant cross-monitoring ($M/M > 1$), an MTBAF of at least 7,000 hours is required, more than double the existing level. 10,000 hours would be more likely.

These curves illustrate that if the average cross-monitoring performance in practice is at the lower end of the scale, then improvement in this by the imposition of mandatory procedural cross-monitoring could yield very significant improvements without any need for change in pilot MTBAF. For example an exceptional and dominant captain at the 7,000 hours MTBAF level operating with a low cross-monitoring ratio could move down to the super-safety level merely by encouraging his partner pilot (also at 7,000 hours in this assessment) to be critical of his captain’s awareness opinions when the necessity arose. As the level of cross-monitoring world-wide is thought to be pretty poor, this is the most likely path for improvement. However if in practice the average level of cross-monitoring is high, the relative flatness of the curves will not allow for much improvement through a tightening up of procedures, and the much more difficult route of pursuing substantial improvements in MTBAF would be necessary to aspire to super-safety levels.

There are many in the business of making and operating aircraft who share the view that a large jump in human performance will be very difficult to achieve. There are many also who would support the pursuit on a world-wide basis of more democracy in the cockpit and the consequent advantages of a wider use of the potential of cross-monitoring fail-safety through procedural mandate. (There is an opinion widely held that one of the reasons for the high operational safety achievements of Australian and Canadian airlines stems from their national dislike of overt authority. One Australian report states...
This will result in all the pilot MTBAF curves previously presented in Fig. 44 being squeezed closer together on the plot so that they become asymptotic towards $k/10^6$ for higher values of $M/M$. Below this level, the accident probability from crew causes can no longer improve with advances in reliability (MTBAFs) gained from better ergonomics and training.

Some guidance in the determination of a likely value for $k$ can be obtained from the fact that if the current accident rate attributed to crew management is around $0.6/10^6$ per hour, a worst case value for $k$ will also be around 0.6 otherwise no pilots on average at any MTBAF level would be able to meet the current accident rate. A pessimistic view could be that this is the determining factor in the flattening of the accident rate, that the limit has been reached in the ability of two pilot cockpits to get below a certain accident rate because of pilot mutual cross-influence. Even with the best cross-monitoring, cross-influence can put a limit on pilots’ independence in their awareness of hazardous situations. However, taking $k = 0.6$ would be to assume that no new cockpit automation developments and pilot training could make any improvement in the current situation, which is unlikely, although the possible levels are open to considerable debate. So a lower value of $k$ should be considered. In the author’s opinion this will lie somewhere between the present value of 0.6 and a value of 0.1, the latter being the ubiquitous $1/10^6$ per hour. We are considering here the range of rare probabilities within which two pilots may be misled by inadequate or incorrect information into making a mutually agreed but wrong decision in a safety-critical situation, and thus suffer a ‘common-mode failure’. No figures are available to evaluate this, but a plot of the effect of a limiting value of $k = 0.1/10^6$ on the probability function $P_c$ would be of interest. This is shown in Figure 45, which plots:

$$P_{(k)} = \left(1/\frac{M}{M'}\right)\left(1 + 2/\frac{M}{M'}\right) + 0.1/10^6$$

over an $M/M$ range of 0.1 to 1.5, and MTBAFs from 1,000 to 20,000 hours.

As might be expected the picture does not change significantly from Fig. 44 around the current safety level, but of major interest is that a common-mode failure limit at the not unreasonable level chosen, would prevent the super-safety level from ever being reached, even with the relatively high 7,000 hour MTBAF discussed earlier. The consideration of common-mode errors therefore remains problematical and speculative, as it always has been in the engineering area, but with a lesser capability for evaluation in the human crew case.

The general assessment of crew accident probability conducted so far, which has been on a ‘per hour’ basis, that is, for a 1 hour period of risk, has not been completely definitive, but the combination of limited analysis and background experience would point towards certain interim conclusions which might be summarised as follows:

1. Pilots appear to operate at a reliability level around 3,000 hours MTBAF when assessed in a similar manner to that applied to ‘engineering’ sub-systems in transport aircraft. This is a human performance level which has probably been such for a very long time. It is well below that achieved in modern machine systems performing comparable, albeit unintelligent, duties. Piloting history indicates that this basic reliability is unlikely to improve. Indeed modern cockpit automation and aircraft and operations complexity have probably combined to decrease pilot basic reliability. Cockpit reliability is therefore likely to be improved only by simplification of pilot and crew tasks.

2. The current accident rate attributable to pilot-error is much better than can be achieved by pilot reliability alone, and some level of cross-monitoring between pilots must be making a contribution to reducing overall crew error levels. However, it is likely that the level of cross-monitoring is too low, and could be improved through procedural actions.

3. In general a lowering of the accident rate attributed to the human crew in pursuit of super-safety would require significant increases in both pilot reliability and crew cross-monitoring.

Figure 45. Common mode failure effect on graphs of figure 44.

Howard.
4. The inherent problem of the common-mode cross-influence factor in decreasing the ability of error detection in a two-crew cockpit may be at a level which prevents the achievement of super-safety. The only solution to this may be the introduction of a third comparison element, which may be a completely independent human or ‘electronic associate’ pilot. The former solution would be partially satisfied by the engineer/pilot employed in earlier generation aircraft cockpits.

These interim conclusions arise from the general one hour analysis. This raises another question about pilot MTBAF assessments. The assessment of pilots using MTBAF methods differs from that for engineering equipment. The latter has a relatively constant failure probability performance throughout a whole flight, as the operational and environmental stresses applied to it are relatively constant. In contrast the stresses on crew can only be considered as constant over a particular phase of a flight, each phase having different machine management requirements and timescale pressures. Pilot MTBAF assessments must therefore be related to the time phases of flight, and different values may apply in different phases. Values specific to the particular phase will need to be used for any overall aircraft system safety analysis involving both ‘engineering’ and ‘piloting’.

In line with this observation the following two sub-sections assess two specific flight phases, first a sample cruise period of three hours, and second an approach and landing period of 15 minutes.

7.4 Crew accident probability: three hour basis: cruise

In Fig. 46 the graphs are drawn on a three hour basis $(t = 3)$, which is selected as one example for a ‘cruise’ period. The current accident probability level is calculated from the product of attributable accident rate per hour in ‘cruise’ (taken as $0.25/10^6$), the crew proportion $(0.6)$ and the exposure time (3 hours), giving $0.45/10^6$ for the three hour example period. The graphs indicate that in cruise the pilot equivalent operating MTBAFs for the current accident probability are around the 8,000 to 10,000 hour level, and for super-safety ($\times 10$) would need to be around 30,000 hours. The cruise phase gives a significantly better value for pilot equivalent reliability when compared with ‘engineering’ sub-system figures, than the general one hour assessment. It reflects a more benign situation in the cockpit in cruise, the implication being that on average there is a relaxed atmosphere in this flight phase in which pilot reliability and cross-monitoring activity is at its best, which probably correlates also with a low common-mode failure probability. The MTBAF figures would support the comments about potential pilot reliability made in the introduction to Section 5 and hence indicate that safety in the cruise generally is already acceptable and not a cause for any action. There would therefore seem to be no need for the $\times 10$ super-safety target figure, which in any case would be so high even in cruise terms to be out of practical reach. The
MTBAFs probably become effectively large because of inactivity. There will be many who have heard the crew comment that in the cruise their workload is low except for occasional ‘cabin’ problems, but when nearing the destination ‘all hell breaks loose’.

### 7.5 Crew accident probability: 15 minute basis: approach and landing

In Fig. 47 the graphs are drawn on a 15 minute basis ($t = 0.25$), which is applicable to approach and landing. The current accident probability level is calculated from the product of attributable accident rate per hour in approach and landing, taken as $(0.5/10^6)$, crew proportion $(0.6)$ and exposure time $(0.25$ hours) giving $(0.075/10^6$ for the 15 minute example period. The graphs show that in the approach and landing phase the pilot equivalent operating MTBAFs are in the range 1,500 to 2,500 hours for current safety and would need to be between 5,000 and 7,000 hours for super-safety. These relatively low figures reflect the higher pressure atmosphere in the cockpit in approach and landing, when compared with those in the cruise. The lower values are likely to prevail as cross-monitoring activity will not be at its best.

The level of the common-mode failure constant in this approach and landing example must be less than $0.075/10^6$, for the reasons discussed in sub-section 7.3, but it is also near to the figure of $0.1/10^6$ or $1/10^7$ which in practice is a likely limit level. If such a limit constant was included in Fig. 47, all of the MTBAF curves would be compressed into the area below the 1,000 hours curve and the current safety line. This would represent a nearly static crew accident probability at the current level for all values of crew MTBAF, which would not seem to be realistic. On the other hand it could indicate that the common-mode pilot-error level was already dominating the achieved accident rate. It would seem, as previously inferred, that in the absence of detailed data the effect of rare common mode failures will remain problematical and speculative.

### 8.0 RECOMMENDATIONS FOR SUPER-SAFETY

It now remains to make some recommendations and translate what has been said into a view of what the actions and strategy should be to move towards super-safety. Hopefully it has been made completely clear that despite the widely dispersed nature of air transport in management, engineering, operations and support, there is a single stem from which the ‘rules’ of safety grow, and this is set in the architecture of ‘fail-safety’. Any single safety-critical demand, operation or action which bypasses fail-safe architecture will destroy the ability of the overall system to meet the super-safety target of one in 10 million hours or lower accident rate figure. The crux of every technical suggestion made will therefore be fail-safety, in one or other of the forms previously defined.
8.1 The integrity of fail-safety mechanisation

The first recommendation concerns the very low levels of failure probability now demanded in systems and sub-systems to achieve the current accident rate, and even lower levels for super-safety. It has been mentioned that the working of fail-safety mechanisms is often obscure at the very low safety levels which now determine the achieved accident rate, and therefore they may or may not be adequate.

Such design limitations can occur quite independently of the problem posed by common-mode failures in a redundant system. Both are in a category of rare failures which occur at very low probability levels. But design shortcomings are not random failures in the normal sense, but failures in the redundancy design concept which reveal themselves only as a result of a rare combination of circumstances which defeat the design implementation. There has recently been considerable concern about such problems in the mechanical and hydraulic equipment fields. Overall experience tells us that these occur in sub-systems at probabilities usually lower than $1 \times 10^{-8}$ per hour, but in sufficient numbers of sub-systems to limit the overall fail-safe design effectiveness and contribute to the levelling out of the overall accident rate. These failures, which determine the limits to the effectiveness of redundancy, are generally all classed under the descriptive of ‘common-mode’ failures, but this may be too narrow a classification.

The total of such rare failures including ‘common-mode’ failures might be categorised as:

1. Flaws in the design of the methods used to compare and isolate failures which prevent the ‘alternative solutions’ from taking over. This can occur anywhere across the full machine, software and human range of individual fail-safe provisions.
2. Loss of redundancy (alternative solutions) in a rare obscure way which is undetected by the comparison provisions.
3. Multiple common internal failure where fail-safety is implemented by multiple redundancy (i.e. common-mode internal failure).
4. Rare external environmental hazards which destroy the performance of all redundant elements in the same way at the same time.
5. Failure warnings and indications which require human intervention, but which are misunderstood or ignored.
6. These factors are the prime ones responsible for limiting progressive reduction of the air accident rate in the area of aircraft engineering design and normal operations, and their reduction is vital to the achievement of significant safety improvement. However to achieve the ten times step from the already relatively high level of air transport safety will require a broader-based and more formalised approach to fail-safe design and operations and a higher density application than has hitherto been used. Correspondingly there must be a higher degree of formal audit of such by the world’s certification authorities.

The basic principles of fail-safe design will not change, but the key to achievement of the necessary improvements will be the substantial reduction by design of the vital common-mode failure levels which limit its current achievements. This may in future require teams of people who work together to achieve a greater comprehension of rare ‘systems of systems’ frailties that are beyond the comprehension of one individual. But more likely solutions lie in the spread across the full machine, software and human range of individual fail-safe provisions.

8.2 Controls reconfiguration

The second main recommendation relates to controls reconfiguration. The ubiquity of fly-by-wire actuation in present generation aircraft, and the high integrity computing now available makes it a relatively straightforward engineering design task to produce aircraft which can have a wide variety of control sources for attitude and speed command.
Airbus aircraft have a limited controls reconfiguration capability as part of their fly-by-wire extreme failure protection. Some capability was also provided 40 years ago on the VC10, described in Section 4. More extensive possibilities exist. The numbers and distribution of primary controls actuators on the Boeing 777, Fig. 49, illustrates an extensive potential in this respect, quite apart from secondary controls and thrust control potential additions.

Implementing various reconfigurations would appear to be a matter mainly of planned aerodynamic capability and limitations, and designing the necessary controls software in the FBW computer complex. An attraction is that reconfiguration to cover severe failures in control systems is a feature which could be developed in future by upgrading in existing aircraft, and hence the economics of protecting against very rare failures for whatever remote reason becomes more palatable. Airbus Industrie did extensive demonstration of controls reconfiguration capability as part of the A320 fly-by-wire development and certification mentioned above, and more recently in the United States a remarkable demonstration was conducted of a complete approach and landing using engines throttle controls only for full manoeuvre demands.

There is also the further engineering possibility of using engine bleed air operating through dedicated vectoring nozzles for attitude control in extreme failure of the conventional flying or secondary controls surfaces, as has been done for many years on military VTOL aircraft and space vehicles. Special ancillary systems on auxiliary power units would be one solution worthy of investigation, especially for an emergency alternative for tailplane control.

It would be expected that computer controlled reconfiguration for use in extreme emergencies would be implemented to operate through the normal stick, pedals and throttles, thus retaining apparent conventional control and not requiring rare skills from the pilots. Indeed the range of capability would far exceed any pilot skill solution. Reconfiguration would be expected to be computer optimised and initiated automatically and not require active crew assessment or intervention. Emergency reconfiguration should also be considered for electronic engine controls, especially for ETOPS aircraft. This should be acceptable if based on fibre optic transmission of data so as not to breach isolation requirements in normal engine operation. Such a system was used in the digital FBW autocontrols for the Coanda effect engine operation in the Boeing YC-14 AMST (advanced medium STOL transport) demonstrator in the mid 1970s(62).

An allied but different automatic control system used on military combat aircraft is that of ‘care-free handling’ which performs automatic recovery from loss of control due to excessive manoeuvre demands, when the flying controls are operating correctly. This is a more extreme capability than the ‘alpha-floor’ and suchlike controls in commercial fly-by-wire systems. Such a capability can be implemented through the fly-by-wire system and may become standard in future if the incidence of upsets becomes excessive and the training of crew to maintain competence in handling them is uneconomic. It would appear that the whole subject of controls reconfiguration for correction of extreme loss of control conditions is now primarily a matter of economics and development, not engineering feasibility.
8.3 The crew and pilot error

The third recommendation is a group relating to various aspects of crew and pilot-error, continuing from the crew accident probability analyses made in Section 7. Pilot-error is producing more than half of all air accidents. It is now closely coupled with the new generation of flight management systems in the context of glass-cockpit automation, and the apparent deterioration of the average pilot situation awareness, which are the subjects of much human factors study.

It is a matter of concern that perhaps over 90% of what has been published on this, and pursued in symposia, in which are included the 51 recommendations in the FAA human factors team report of 1996(63), makes almost no mention of the vital necessity for planned fail-safety in the cockpit. The majority of studies address ‘pilot’ performance only, when the most relevant safety issue is one of ‘crew’ performance.

The FAA team report is an outstanding appraisal of human factors problems which may assist in devising improvements which give increased pilot ‘reliability’. But it should not be assumed that any implementation of its recommendations, or any equivalent ones, will have a significant affect on safety in the absence of improvements in crew fail-safety ‘architecture’.

8.3.1 Human factors studies

It is therefore suggested that human factors studies be redirected to emphasise the analysis of crew fail-safety, rather than only individual pilot-error. Indeed the fail-safety element should receive the most attention in the light of the widely held opinion that individual pilot error in the cockpit is already very low in human capability terms. Studies should embrace the vital concept of cross-monitoring and direct attention to crew procedures, coupled to flight management system operating structure, with the intention of imposing strict fail-safe cross-checking on every safety-critical action. This would restore the safety principles which were implicit in the cockpits of the pre-FMS era. If the basic ‘reliability’ of pilot activity, however much enhanced, is not processed through crew procedural ‘fail-safe architecture’, cockpit safety will never reach its full potential.

It must also be recognised here that there is an unfortunate tendency in recent human factors studies to attribute the more obscure safety problems to human factors when a root difficulty, if there is one, can be seen by aircraft systems designers to lie in a straight-forward engineering implementation, operating procedures or a remote failure area. Such attributions are yielding very little of practical use to aircraft designers or operators. It would save much valuable time for all concerned in future if no human factors committees were formed, symposia conducted or reports written without the involvement of at least a 50% experienced design engineering and operations active membership. It is not satisfactory just to ask for comments or opinions from these areas.

8.3.2 Awareness enhancement with advanced displays

The recommendations in Section 8.3.1 should not be taken as ruling out the pursuit of every opportunity for individual pilot ‘awareness enhancement’ means as both short term and long term contributions to safety. A major additional potential is one already in hand, Fig. 50, which is the introduction into the cockpit of head-up situation awareness enhancement. The most valuable EVS (enhanced visual systems) are likely to use fused combinations of infrared and millimetre wave imaging. A cockpit installation is illustrated in Fig. 51, with examples of infrared and millimetre wave imaging shown separately in Fig. 52 and Fig. 53 respectively.

8.3.3 Electronic third pilot

It would seem unlikely that the economics of air transportation will ever allow a full-time three-pilot operation, despite the fundamental advantage of a third vote in enhancing the validity of cockpit decisions. However, the further progressive development is recommended of the so-called ‘electronic third pilot’ (or pilot-associate), Fig. 54. This is intended to display a computed digestion of aircraft flight and demand data, perhaps with some
artificial intelligence (AI) prediction. Some information is already provided in this category, in effect, by installations such as GPWS and TCAS. Much work on this concept has been done in Europe and the United States. It would be desirable to present third pilot information in an attention-getting advisory sense. One implementation would be to alert the crew if there is some disagreement when actions are to be taken, commencing with an ‘Are you sure?’ query if time for a reappraisal exists.

8.3.4 Cockpit management in the long term

It must now be considered what may be required in flight management in the much longer term, perhaps into the 2030s or later. Despite the potential of third sources of information in enhanced displays and special advisory electronic devices, these still operate through the basic two-human-crew management and control concept. The reliability analyses described in Section 7 still prevail overall and leaves considerable doubt as to whether the super-safety level can ever be achieved by human crew in the approach and landing phase of flights. The author’s view is that it cannot, and may not even if a third crew member were reintroduced with the cockpit systems now established and the increasing pressures in this phase of flight. The likelihood is that human control will need to be replaced in due course by automatic control. After nearly 50 years of involvement in the aircraft controls business, the author considers the possibility of this to be a feasible and correct path, rather than the impossibility of it.

Let us review the background. The airworthiness side of fully automatic approach and landing was solved for commercial safe use over 40 years ago. At present it is set up, initiated, managed and monitored by the crew. Guidance accuracy and its fail-safety still remains with ground-based instrument landing system (ILS) or equivalent radio transmitters. Alternative guidance information fused from inertial and GPS data, and supported by MLS/ILS as available, is waiting in the wings. Ground-based air traffic management using the massive capability of modern digital computing is delicately poised worldwide on the threshold of automatic, fail-safe, traffic management.

Going fully automatic in the approach and landing phase of aircraft flight requires only two overall new concepts. First, ‘automatic only’ traffic control areas must be delineated around airports for commercial traffic. This would have a large number of 4D (range, height, position and speed) gates for incoming aircraft, to be entered under crew control, much as originally envisaged for MLRS. The second new concept would be that after acceptance at a gate, the aircraft acceptance at a 4D gate, the outer loop-control authority would be taken over by the ground ATC computing and remain with it until roll-out after the automatic landing. The crew would completely monitor the approach and landing, with aircraft safe flying limits still in their command. In the event of some aircraft emergency or a remote failure of ATC command control, it would have in the early stages the ability to exit through the ‘automatic area’ climb-out or overshoot ceiling, or at a late stage in the approach to exercise manual takeover and landing. An enormous advantage of such an automatic system would be the ability to prove that adequate safety was achieved. This would be effected by computer simulation of its performance in fast time, as was done many years ago in the development of fully automatic landing and the determination of Atlantic enroute separation standards. The simulation model could have any numbers of aircraft within reason in the
‘automatic’ box, and would allow the collection of data samples that are statistically meaningful at the probability levels required to achieve super-safety.

It is envisaged that the basic technical problems of such a system could easily be solved in the next 10-15 years. But it is anybody’s guess as to when this or any comparable fully automatic ATC management system might find its way through both internal and international political approval hurdles, and accomplish the changes in airports equipment and investment involved. It may only ever be desirable and possible at the main air traffic hubs. However, if improvements in safety are to match the increases in the world fleet, there may be no alternative.

CONCLUSION

It is a fact that at some time aircraft engineering, piloting or flight operations will fail however much their reliability is improved. It is an essential requirement of design for safety in all aspects of air transport that the effects of such failures must not be hazardous. It is a fundamental principle of fail-safe design that any failure having potentially dangerous consequences, whatever the cause, must be identified and must have an associated design feature that renders the failure safe. This is ‘the fail-safe dimension’ which has been the subject of this paper.

The success rate of the commercial air transport industry in achieving universal fail-safety is already high. But it is not high enough in a world populated with 13,000 large aircraft and many more smaller ones in the air every day, to realise an accident rate so low that it has public acceptance. The paper suggests possible solutions in principle, all of which will involve extra expenditure to achieve results which will not be realised in the life of those who make the decisions to pursue them. Accident probability improvements many times lower than once in a lifetime do not generate tangible competitive advantages or short term profits. So the key to some aspects of the problem of lowering the accident rate must lie with the regulation authorities in the setting of fewer general requirements and more specific ones aimed at guaranteeing the necessary levels of design safety and not allowing it to fall to competition on the borderlines.

It will be appreciated that the subject of fail-safety is too broad to be completely defined in one paper. It is the intention of this paper to be thought-provoking in this vital area of air transport design which is widespread but not widely understood. It is also hoped that it will remind a new generation of designers that some design history is thought-provoking in this vital area of air transport design which the borderlines.

The views expressed in this lecture are entirely those of the author from his own experience and do not necessarily reflect those of any other individual or organisation including any company, agency, foundation, committee or team.

The author acknowledges the use of the illustrations from the sources noted and data from the list of references, and additional information from Aviation Week and Space Technology, Flight International, Aeroplane, CAA(UK), FAA(US), NTSB(US), NASA(US), Flight Safety Foundation, Airbus Industrie, The Boeing Company, BAE Systems and general background information from the Wright Brothers Papers by Marvin W. MacFarland.

The author is grateful for the considerable assistance given by the library of The Royal Aeronautical Society, London, and by the Systems Engineering and Evaluation Centre of the University of South Australia, and for comments and advice from John Chaplin, Harry Hopkins, John Scott-Wilson, Brian Tucker and Ivan Yates.

The author is indebted to BAE Systems, Rochester for technical advice (Andrew D. Hills, John R. Taylor and John Aplin) and on illustrations and text (Richard Cummings).

REFERENCES

2. Te, W. Civil airworthiness, JRAeS, Jan 1966, 70, (661), pp 253-257.
9. Wright flying machine stabiliser. Improvements in or connected with flying machines, 6 Feb 1909, UK patent 2913.
35. MUNSON, K. *Airliners from 1919 to the Present Day*, Ibid, p 112.
47. HOWARD, R.W. and BISHOP, G.S. The development of reliability in airborne electronic equipment with some reference to the VC10 automatic landing system, RAeS/IEE Joint Conference, Session 3 - Paper 2, Feb 1962.
52. HOWARD, R.W. and BISHOP, G.S. A consideration of equipment reliability requirements for automatic landing systems, Air Registration Board Committee on landing and take-off aids, Document ARB-LTA-19 March 1960 (Public Records Office, Kew).
63. Human factors team report on the interfaces between flight crews and modern flight deck systems, Federal Aviation Administration, 18 June 1996.

---

**APPENDIX: PLANNED FAIL-SAFE AREAS IN AIRCRAFT ENGINEERING DESIGN**

<table>
<thead>
<tr>
<th>Main Area</th>
<th>Sub-area</th>
<th>Flyer</th>
<th>Vimy</th>
<th>HP42</th>
<th>DC-3</th>
<th>VC10</th>
<th>B777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure</td>
<td>Fuselage (Main)</td>
<td>Wooden frame/redundant members</td>
<td><em>A</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>fabric covered/wire bracing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal frame/redundant members/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>metal &amp; fabric clad</td>
<td><em>A</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal monocoque/load sharing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal frames &amp; stringers/stressed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>metal skin/multi-load-path redundancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal frames &amp; stringers/stressed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>metal skin/machined window &amp; exit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>planks/multi-load-path redundancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal integrally machined skin &amp;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>webs/joined in large sections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metal &amp; composites in construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plug doors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wing/fuselage centre-plane box</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rear pressure bulkhead</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wings</td>
<td>Wooden spars and ribs/redundant members/fabric covered</td>
<td><em>A</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Metal spars, ribs, stringers/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>redundant members/fabric covered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interplane struts &amp; redundant bracing wires</td>
<td><em>A</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: 1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter ‘A’ adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.*
Note: 1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter 'A' adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.
<table>
<thead>
<tr>
<th>Main Area</th>
<th>Sub-area</th>
<th>Flyer</th>
<th>Vimy</th>
<th>HP42</th>
<th>DC-3</th>
<th>VC10</th>
<th>Super</th>
<th>B777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flying controls</td>
<td><strong>Spoilers</strong> (inc structure) (cont)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Six (two sets of three surfaces each with two jacks) combined with</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>airbrakes/coupled with ailerons/dual cable sets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 each with fly-by-wire actuators including two combined spoiler/speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>brakes with back-up cables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Elevators</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual cables/pulleys/levers/rods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>: two surfaces wood &amp; fabric covered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>: two surfaces metal &amp; fabric covered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two surfaces/tabs/dual cables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two pairs of split surfaces/dual cables/rods/pulleys/quadrants/cranks/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tensioners &amp; power-by-wire PCUs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual artificial feel &amp; centering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two surfaces each with dual Fly-by-wire actuator &amp; PCUs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Rudders</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual cables/rods/pulleys/levers/rods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>: two surfaces wood &amp; fabric covered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>: three surfaces metal &amp; fabric covered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single rudder/tab/dual cables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single rudder/tab/hydraulic power/dual cables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Three rudders/tabs/dual cables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Three section split surface/dual cables/rods/pulleys/quadrants/cranks/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tensioners &amp; power-by-wire PCUs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>One surface/carbon fibre epoxy sandwich/tab/triple actuators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single trim system/feel &amp; centering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Flaps</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two trailing edge surfaces/hydraulic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two sets five section modified Fowler</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Four torque tube coupled surfaces/hydraulic &amp; electrical alternative</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>motor drives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two Krueger surfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Flaperon</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two each with dual fly-by-wire actuation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Slats</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two sets four piece/torque tube coupled/screw jacks/dual hydraulic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>supplies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic slots/top-plane/metal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 surfaces/torque tube coupled single and multi-movement/hydraulic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&amp; electrical alternative motor drives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Horiz stab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual hydraulic motors/worm screwjack/hydrat back-up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual hydraulic actuators &amp; cable backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: 1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter ‘A’ adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.
### Engines

<table>
<thead>
<tr>
<th>Sub-area</th>
<th>Flyer</th>
<th>Vimy</th>
<th>HP42</th>
<th>DC-3</th>
<th>1. DC-4</th>
<th>2. L049</th>
<th>3. B377</th>
<th>4. DC-6</th>
<th>VC10</th>
<th>B777</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.C. &amp; props.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two engines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Four engines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual ignition &amp; other accessories</td>
<td>*</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full propeller feathering controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fully reversible propellers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>2,3,4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPM synchronisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>2,3,4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crew propeller protection guards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broken propeller protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Fuel Tankage

| Main (each side)                             |       |      |      |      |         |         |         |         |      |      |
| Landing gear (Retractable)                   |       |      |      |      |         |         |         |         |      |      |
| Single wheels & brakes                       | *A    |      |      |      |         |         |         |         |      |      |
| Single wheels, differential brakes & tailskid|       |      |      |      |         |         |         |         |      |      |
| Dual wheels/nose skid/tail skid              | *A    |      |      |      |         |         |         |         |      |      |
| Dual wheels & brakes                         | *A    |      |      |      |         |         |         |         |      |      |
| Four-wheel bogey/brakes/antiskid             |       |      |      |      | *       |         |         |         |      |      |
| Six-wheel bogey/aft-axle main gear steering coupled to nose-wheel axis | *A | | | | | | | | | |
| Brakes & antiskid (digital automatic)        |       |      |      |      |         |         |         |         |      |      |
| normal & alternate                           | *A    | *A   | *A   | *A   |         |         |         |         |      |      |
| Hydraulic retraction system                  | *A    | *A   | *A   | *A   | *       |         |         |         |      |      |
| Alternative systems operation                |       |      |      |      |         |         |         |         |      |      |
| incl free fall                               |       |      |      |      |         |         |         |         |      |      |
| Structural fusing                            |       |      |      |      |         |         |         |         |      |      |

### Nose wheel

|                     |       |      |      |      |         |         |         |         |      |      |
| Nose wheel          |       |      |      |      |         |         |         |         |      |      |
| Single wheel        |       |      |      |      |         |         |         |         |      |      |
| Dual wheel          | *A    | *A   |      |      |         |         |         |         |      |      |
| Dual tillers/pedals alternate/alternate cable|       |      |      |      |         |         |         |         |      |      |
| Structural fusing   |       |      |      |      |         |         |         |         |      |      |

### Crew

|                    |       |      |      |      |         |         |         |         |      |      |
| Crew               |       |      |      |      |         |         |         |         |      |      |
| Two crew (pilot/engineer)                    |       |      |      |      | *A      | *A      |         |         |      |      |
| Two pilots (captain/copilot)                  |       |      |      |      | *       |         |         |         |      |      |
| Five crew (captain/copilot/navigator/radio officer/flight engineer) |       |      |      |      |         |         |         |         |      |      |

### Note

1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter ‘A’ adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.
<table>
<thead>
<tr>
<th>Main Area</th>
<th>Sub-area</th>
<th>Flyer</th>
<th>Vimy</th>
<th>HP42</th>
<th>DC-3</th>
<th>VC10</th>
<th>B777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crew (cont)</td>
<td>Mechanical basic instruments/ dual and/or standby set on pilot panels</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blind flying panel &amp; related instruments</td>
<td>*A</td>
<td>*A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine &amp; fuel instruments on pilot panels and/or engineer panels</td>
<td>*</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrated HDI/CDI electromechanical with standby set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LCD integrated displays with standby set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
</tr>
<tr>
<td></td>
<td>Dual autopilot controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
</tr>
<tr>
<td></td>
<td>Dual nav/coms controllers</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine indication and crew alerting system (EICAS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td>Electrical power generation</td>
<td>Generators on all engines</td>
<td>?</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Four generators/constant speed drive/load controllers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Back-up generators on all engines</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generator on APU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generator on drop-out ram</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Air turbine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Permanent magnet generators on all engines (FBW back-up)</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Separated bus wiring</td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic electrical load monitoring and sharing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
</tr>
<tr>
<td>Hydraulics</td>
<td>Multiple pumps &amp; reservoirs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Four engine variable delivery pumps/ two pipe circulation systems</td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple pumps on constant speed drives &amp; bleed air</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Drop-out hydraulic ram air turbine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auxiliary power unit</td>
<td>Pneumatic &amp; electrical supplies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Airstart system/multiple dissimilar start provision</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Hydraulic equipment</td>
<td>Power-by-wire PCUs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Primary power actuators</td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secondary power actuators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Motors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avionics</td>
<td>Air data &amp; pitot static systems (dual)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inertial reference system (multiple)</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flight director systems (dual)</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gyro vertical &amp; horizontal reference systems</td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fly-by-wire controls system</td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single standard autopilots</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Autopilot (duplicate-monitored or triple)</td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Autopilot backdrive of pilots controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: 1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter ‘A’ adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.
### Howard Planning for Super Safety: The Fail-Safe Dimension

**Note:**
1. An * indicates that the sub-area has planned fail-safety in the example aircraft. A letter ‘A’ adjacent to an * in any group designates a fail-safe area.
2. The table is a guide derived from general records, illustrations and service manuals but cannot pretend to be complete.

<table>
<thead>
<tr>
<th>Main Area</th>
<th>Sub-area</th>
<th>Flyer</th>
<th>Vimy</th>
<th>HP42</th>
<th>DC-3</th>
<th>VC10 Super</th>
<th>B777</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avionics (cont)</strong></td>
<td>Automatic landing (failure-survival)</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yaw dampers (multiple series)</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Radio communication systems</td>
<td>*</td>
<td>*</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Radio navigation systems (multiple dissimilar)</td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inertial navigation systems (INS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ILS Localiser &amp; glide path</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Marker beacon receiver</td>
<td>*</td>
<td></td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Radio altimeter</td>
<td>*</td>
<td></td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weather radar</td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Satellite navigation system (GPS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ground proximity warning system (GPWS)</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic collision avoidance system (TCAS)</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aircraft communication addressing &amp; reporting system (ACARS)</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aircraft information management system (AIMS)/duplicate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flight management computers (duplicated &amp; software system-partitioned &amp; self-monitored)</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data bus triple ARINC 629 system</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Redundant system LRUs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installations widely separated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hard wiring/partitioned installation/fireproof ducting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td><strong>Cabin management</strong></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
</tr>
<tr>
<td></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td><strong>Air-conditioning</strong></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>&amp; cooling</td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td><strong>Oxygen/crew</strong></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td><strong>Oxygen/cabin</strong></td>
<td>System redundancy</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td><strong>Anti-icing</strong></td>
<td>Deicing boots &amp; air</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dual engine bleed-air/APU</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine bleed air</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary &amp; back-up anti-ice &amp; anti-fog</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td></td>
</tr>
<tr>
<td><strong>Fire detection &amp; extinguishing</strong></td>
<td>Engines/APU/lavatory</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
</tr>
<tr>
<td><strong>Emergency evacuation</strong></td>
<td>Multiple evacuation means</td>
<td></td>
<td></td>
<td></td>
<td>*A</td>
<td>*A</td>
<td>*A</td>
</tr>
</tbody>
</table>

**Pressurisation system**

**System redundancy**

**A**2,3,4 **A** **A**