SOME CONSIDERATIONS OF SAFETY IN AUTOMATIC FLIGHT CONTROL

By A. M. A. MAJENDIE

Director Operational Requirements
Smiths Aircraft Instruments Ltd.

Summary—The importance of the automatic pilot in transport operations is reviewed. The difficulty of providing sufficient authority without prejudicing safety is considered in the light of practical experience. Various compromise solutions adopted in the past are discussed. Increases in operating Mach number and altitude demand a new approach to the safety problem, as does automatic landing.

The use of a multiplex autopilot, having two or more sub-channels for control about each axis, is then considered. The limitations of duplex or duplicated autopilot installations are demonstrated. The conclusion is drawn that future requirements demand the use of triplex or quadruplex systems.

Failure rates on current equipment are analysed. On this basis estimates are made of failure probabilities for various combinations of autopilot and radio guidance equipment. The future safety of automatic landing is shown to depend on the overall reliability of the radio guidance intelligence.

Simulated examples of the use of a triplex system for control of the landing are illustrated, including the effects of various types of malfunction.

1. INTRODUCTION

THE importance of the automatic pilot in the modern transport aircraft has increased considerably in recent years for a number of reasons. The strain on the operating crew has tended to increase, in step with the increased performance of the aircraft, and also as a result of the more complex and stringent requirements imposed by Air Traffic Control. The use of the automatic pilot not only relieves the pilots of the burden of manual flight, but also by virtue of its more elegant and precise control can make its own contribution to the more economic use of a high performance aircraft.

If full advantage is to be taken of the facilities of the automatic pilot in transport operations, a high level of overall serviceability is obviously needed. If this can be achieved the use of the automatic pilot can have a highly significant effect on the crew complement, and thereby on the economics of a given operation. It can also go some way to mitigating the effects of turbulence in passenger carrying flights, and in providing some relief to the structure[1].

The growing use of automatic approach couplers in recent years has introduced another significant factor. The automatic pilot is now capable of making a major contribution to the achieved level of approach success

in bad weather operations. For this to be exploited a very high level of safety and reliability must be obtained from the equipment. W. J. Charnley has recently given an account of the experimental work on automatic landings carried out in the United Kingdom at the Blind Landing Experimental Unit, and has shown that the technical problems have, in general, been solved[2]. G. W. H. Gardner, Director of the Royal Aircraft Establishment, also referred to this work in the Forty-Sixth Wilbur Wright Memorial Lecture given before the Royal Aeronautical Society, and gave some figures of the large number of experimental automatic landings already successfully carried out[3]. If such techniques are to be used in regular operations an even higher level of safety and reliability is clearly necessary than that already imposed by the requirements of the approach phase alone.

The arrangements that must be made on conventional autopilot installations in order to achieve safety in the event of malfunction all depend on a limitation of the authority of the equipment. This paper reviews the limitations of such an arrangement in the light of the considerations set out above, and the conclusion is drawn that a conventional autopilot installation, with a single channel for each axis of control, can no longer meet the operational requirements on future high performance transport aircraft. An examination is then made of the implications of fitting a genuine multiplex autopilot system, employing duplicated, triplicated, or quadruplicated sub-channels for each axis of control. It is shown that there are serious limitations in duplication and that very real advantages can be derived from going to triplication, or even to quadruplication. The further conclusion is drawn that such arrangements are alone capable of providing the necessary authority at an acceptable level of safety to meet all the envisaged requirements.

2. THE GENERAL AUTOPILOT SAFETY PROBLEM

When a conventional autopilot is installed in a given aircraft the desire is to provide an installation with sufficient authority over all flying controls to give satisfactory performance. At the same time it is necessary to ensure that the aircraft response to an Autopilot malfunction in the worst combination of circumstances cannot exceed specified limits, set by considerations of aircraft strength, attitude, passenger comfort or proximity to the ground. These two requirements are mutually opposed, the first calling for wide authority and the second for its limitation. On current aircraft an uneasy compromise peculiar to the individual aircraft type has had to be reached, and, since safety is an absolute requirement, performance has in many cases had to suffer. The greater the range of operating Mach number and altitude the more difficult does the problem become; and the position can easily be reached when the autopilot must labour all its life under restrictions which considerably limit its usefulness, in order that it may not break the aeroplane in the exceedingly unlikely event of a

runaway in the worst combination of flight conditions and loading. The safety problem on the new generation of civil transport aircraft is going to be extremely formidable. With present-day safety arrangements, such as torque limiters, it is quite possible that a position will arise when the problem will become insoluble; that is to say, if an installation in some future aircraft meets all requirements for safety, it may well be unacceptable from the performance point of view. The nature of this problem will now be examined in the light of the experience gained over the last decade with the Smiths range of automatic pilots.

Before 1954 normal practice in the United Kingdom was to install standard servomotors of suitable nominal torque in each channel; the aircraft response to simulated runaways in the air was then checked, and clearance was based on the results of these runaways. In some instances limit switches were fitted to cut out the autopilot at a fixed control angle. It was known, however, that actual torque could vary widely from nominal owing to variations in supply voltage and frequency, manufacturing tolerances, and so on. Making the assumption that all tolerances might be cumulative in one or other direction a range of 4 : 1 on torque could be found. The use of this figure, together with variations in aircraft response per unit torque over the flight range, rendered the safety problem using plain servomotors quite insoluble even on relatively simple aeroplanes. The expedient of fitting limit switches did little to help matters since the system, though safe, could not be made immune from inadvertent "nuisance cut-outs".

A form of cut-out operating on torque rather than displacement seemed to offer some alleviation, and therefore development of such a device was begun. The first of these devices was the spring strut introduced in 1955, and now fitted to VISCOUNT and BRITANNIA aircraft. The rotary torque limiter, operating on the same principle, came shortly afterwards and was fitted to several aircraft. The definite limitation of torque, regardless of variations and tolerances, which the spring strut and rotary torque limiter provide, eased the problem for several years, and it was not until more advanced aircraft began to appear that this method of achieving safety started to be inadequate.

As a result of the difficulties of achieving safety by the limitation of authority using either displacement or torque, further consideration has been given to safety devices operating on response. The first of these was the roll error cut-out, which detects a misalignment between the demanded and achieved bank attitudes. This was introduced to meet the case of excessive bank angles in a 5 sec aileron runaway on the cruise, which proved difficult to cover with torque limitation while at the same time allowing adequate roll control in manoeuvres. The second such device to suggest itself was the use of a "g" switch as an obvious safeguard in pitch. Unfortunately calculations indicate that such a device is not sufficient to prevent excessive normal accelerations in all flight conditions

unless it is set to such a low value that it is practically useless in turbulence. The addition of a term in angular acceleration, however, turns the "g" switch into an effective device. It may then present new problems in how it should be tested, and in its own safety and reliability. Experience of the manufacture of automatic pilots, accumulated over a long period, has shown which safety requirements are likely to be critical on each axis in a conventional autopilot installation. A brief account of the significant points now follows, starting with the pitch axis.

Safety about the Pitch Axis

This is generally speaking the most difficult of the three axes. The requirement for civil aircraft is that the maximum normal acceleration increment in a runaway shall not greatly exceed 1·0 g, and the structural limit is in any case in the region of 2·0 g incremental. An additional requirement concerns height loss on approach, and the maximum height loss in a runaway determines the height below which the autopilot must be disengaged. Other requirements concern the attainment of stalling or buffet lift coefficients in the nose up runaway case, and of excessive airspeed or Mach number in the nose down runaway case.

The opposing requirement for manoeuvre in pitch calls for at least enough incremental "g" to execute turns up to the maximum bank angle, with a margin to allow for pitch disturbances while turning. This means that at least 0·2 g increment is needed. Thus the ratio between maximum allowable "g" and minimum acceptable "g" is only about 4 : 1 or 5 : 1. For the simplest aeroplane with no compressibility or distortion effects, stick force per "g" is theoretically constant throughout the speed range for a fixed weight and centre of gravity. It is also directly proportional to weight and to the distance of the centre of gravity forward of the stick free manoeuvre point. Elevator angle per "g", on the other hand, varies as $1/(V_i^2)$ in the simple case, where V_i is the equivalent airspeed (approximately indicated airspeed). The reason for choosing torque limitation in preference to limit switches is now obvious, since limit switches set to 1·0 g at 400 knots would only allow 1/7 g at 150 knots, without centre of gravity and weight variations being taken into account.

Real aeroplanes do not follow the above simple laws since modifications occur due to the effects of compressibility, distortion, slip-stream, use of flap, spring tabs, and so on. On one type of large jet aircraft, which did not go into service, it was estimated that whatever artifices were resorted to in the control system, the range of stick force per "g" due to weight and centre of gravity variation alone, would be about 9 : 1, and compressibility and distortion might have modified this figure adversely. No solution to the safety problem in terms of torque or angle limitation could be foreseen on this aeroplane up to the time of its cancellation.

Height loss due to autopilot malfunction on the approach is computed in the U.K. on the assumption of the time taken for the pilot to intervene

being 2 sec. Even assuming 1·0 g increment downwards, only 64 ft can be lost in this time, so that including the recovery there is the possibility of losing 130 ft or so in all. In spite of this simple calculation, however, troublesome height losses have been encountered on occasion, and it must be remembered that a break-off height of only about 200 ft is the requirement.

The problem of buffet or excessive Mach number tends to become critical on the jet transport and requires consideration also on propeller turbine types. The margin of "g" to reach buffet can be small enough to affect the autopilot runaway problem considerably. In such a case the autopilot authority over the elevator may have to be seriously curtailed.

Safety about the Roll Axis

The roll axis will next be considered. Here the strength limitation is that the Autopilot shall be unable to apply aileron in excess of the maximum permissible angle. This angle is full aileron below a certain equivalent airspeed and then falls roughly as $1/(V_i^2)$. For this reason torque limitation is the obvious choice with normal V_i^2 feel on the controls, since the torque to reach the limiting angle is then roughly constant. Spring tabs modify this law, and plain spring feel causes other difficulties. Fortunately (and this is relevant to torque limitation in general) airworthiness regulations define various minimum control forces to reach limiting conditions, in order to protect the structure against overstressing by the human pilot, thus too light an aileron feel at high speeds is unacceptable. In some aeroplanes wing stressing is not critical from the autopilot point of view, and attention then shifts to the cases discussed below.

The other considerations limiting aileron authority are the maximum bank angle in a 5 sec runaway under cruise conditions, and the height loss and lateral divergence from the beam centre line in a 2 sec runaway on the approach. In both cases reasonable pilot action must be assumed for the recovery, and the whole manoeuvre including this must be considered. As already stated, the roll error cut-out is a valuable protection against excessive attitudes after a runaway, and can be set to cut out at about 10 or 15° of bank instead of the 60° which is regarded as the upper limit for the cruise runaway case.

Turning now to the question of minimum authority, the requirement is that the ailerons shall be able to produce the demanded rate of roll in all flight conditions with a reasonable margin for accelerating into the roll and for turbulence. The use of a phase advance network in the aileron channel has a marked tendency to increase the aileron angles demanded on the initiation of a rolling manoeuvre. Since for the simple rigid aeroplane, rate of roll per degree of aileron is proportional to true airspeed, the largest steady control angles are called for in the approach case. For the same reason, maximum runaway bank angles in a given time are usually found in the high altitude case, at low speed for a torque limited system and at high speed for a limit switch arrangement.

Safety about the Yaw Axis

The critical consideration about the yaw axis is the strength of the fin. The most severe type of runaway considered is where the rudder is assumed to run at maximum rate up to an angle limited by a torque limiter or otherwise, and to be held on while the aeroplane yaws. Since the natural damping in yaw is low, considerable overswing occurs, and at the peak sideslip angle the rudder is assumed to be released and to return to the trailing position. This produces the peak fin load, and the authority is calculated to give not more than proof load. The function of the rudder control in current autopilots is yaw damping and sideslip suppression only, and for these functions the limitation of authority arrived at in this way has usually been acceptable. An additional requirement which may sometimes be critical is that the autopilot shall hold an engine cut without disengaging, and the case of an approach with asymmetric power must also be considered, since power and speed changes will then affect rudder trim and may lead to "nuisance" cutting-out.

The prospect of achieving safety in the future by conventional methods, such as those discussed above, is not encouraging, and it is clear that a new approach to the safety problem is due. The possibility has been raised in some quarters of fitting a duplex autopilot installation with a comparator system to effect cut-out on disagreement between the two elements of the installation. Furthermore, the principle of redundant multiplicity, which has recently entered the aircraft structures field to provide fail-safe characteristics, has now also been proposed to overcome the difficulties of safety clearance, and to meet the requirements of automatic landing. The safety problem reaches its ultimate peak of difficulty in this manoeuvre since virtually no divergence from the flight path can be tolerated after a malfunction, and the operator is forced either to accept multiplicity or to face the statistical risk of a catastrophic runaway just before touchdown. This risk is not acceptable in civil operations, and since reliability is likely to demand at least duplication of the automatic control system in the future, the multiplicity principle solves both problems. The implications of such systems will now be examined in more detail.

3. THE MULTIPLEX AUTOPILOT

The first arrangement to be considered is the use of a duplex system: that is a system with two sub-channels for each axis of control. It would be possible to arrange this so that when either of two such sub-channels ran away or failed to function correctly, a device which compared the output of the two sub-channels would immediately cut out the autopilot, and the aircraft would then be returned to manual control. Such a prospect is relatively unattractive in that the total failure rate of the components of the autopilot system would be double that associated with the corresponding single system, and the system as a whole would therefore be half

as reliable. The safety problem would to some extent be solved, except that in the event of the autopilot cutting out during a manoeuvre the aircraft might be returned to the pilot in an unacceptable flight condition. It has been suggested that facilities should be provided for re-engaging one of the two autopilot sub-channels after a failure. There are two objections to this. The first is that spring struts, torque limiters, or the like, would then have to be fitted to each of the two sub-channels which would increase the weight of the installation and at the same time would provide just that limitation of its authority which it is desirable to remove. The second objection is that the pilot might have no idea which of the two sub-channels had become faulty, and in these circumstances it could be inadvisable to re-engage either sub-channel alone.

The difference between a duplex arrangement, such as that just considered, and an installation comprising duplicated autopilots of conventional single channel design must be emphasized. The duplicated installation provides no better solution to the safety problem than the conventional limitation of authority; it does, however, double the reliability of the autopilot installation considered as a whole, when compared with a conventional single system. The duplex arrangement goes some way to solving the safety problem, but is clearly not capable of handling such manoeuvres as automatic landing, as every malfunction leads to complete cutting out; it has the further disadvantage of seriously lowering reliability.

With a triplex arrangement, having three sub-channels for each axis of control, it is possible to arrange a comparison system which operates in such a way that each sub-channel is continuously compared with the other two. In the event of a malfunction, the faulty sub-channel is switched out, and the remaining two sub-channels continue to control the aircraft satisfactorily. In the event of a further failure, the comparator cuts out both sub-channels and the aircraft is returned to manual control. It is important that each sub-channel should have sufficient power to control the aircraft in its own right so that in the event of the disengagement system failing to work correctly, the aircraft will still be under satisfactory automatic control after the failure of one sub-channel. Provided that the failure rate of the individual sub-channels is sufficiently low, such a triplex scheme can provide a very high degree of safety, for example, when carrying out an automatic landing. Before proceeding to dependence on scheduled automatic landing, however, it is essential to provide a full quadruplex arrangement, with four sub-channels for each axis of control. Only by this means can the probability of successfully accomplishing an automatic landing at the end of a flight be made sufficiently high, despite the risk of component failures en route.

Clearly there are difficult problems to be overcome in the development of a satisfactory multiplex autopilot system. No attempt will be made to discuss these here. Furthermore it will be readily appreciated that the lengths to which it may be necessary to carry the multiplicity arrangements

can only be resolved after a careful examination of the particular operational requirements which it is desired to meet. Most of the remainder of this paper will be concerned with some statistical guess-work to try to estimate the levels of safety and reliability which can be achieved with various different arrangements of the multiplex principle.

Since this discussion is being developed along general lines, there is no direct evidence on which to base the probability of failures in the sub-channels of a multiplex equipment. There is, however, a considerable history of operating the commercial series of Smiths S.E.P. autopilots. Data have been gathered and analysed covering about 300,000 hr of operation of these autopilots in airline service. Not all reported failures would necessarily have caused a cut-out of one sub-channel in a multiplex system, but no attempt has been made to classify failures on this basis. The results are to this extent pessimistic and the conclusions drawn from them are extremely conservative in assessing safety or reliability. Even if these conclusions are in error by as much as an order of magnitude it will be seen that the outcome of the discussion is not seriously affected.

It is found that the failure rate of the later series autopilots is almost exactly half the rate of the earlier ones, in spite of the increased complexity of the former compared with the latter. Much of the difference can be attributed to improvements resulting from the development of particular components. In view of the fact that those components which will be used in any new system will be further developed using the experience already gained, there is every reason to anticipate that failure rates will be reduced still further. However, in order to make a conservative estimate for any such new equipment, the earlier and higher failure rate has been adopted as the basis for the following estimates. Where multiple sub-channels are used an allowance is made for the failure rate of comparator circuits by adding an arbitrary 50% on to the rate for the basic channels.

In addition to the above autopilot data, the failure rates of certain types of radio navigation equipment have also been obtained and analysed. On the basis of failures per flying hour, such radio equipment is found to be several times less reliable than the autopilot equipment. In a general study of safety and reliability it is therefore essential to take careful account of the effect of radio failures.

The results of this analysis are shown in Table 1.

TABLE 1

Failure rate per flight of 5 hr *duration*

Autopilot channel or sub-channel	Basic	4×10^{-3}
	+50% (for comparator)	6×10^{-3}
Radio guidance	Basic	16×10^{-3}
	+50% (for comparator)	24×10^{-3}

It is important to consider carefully just what is wanted from the automatic control system. If scheduled automatic landing is the aim, then it is vital that the probability of not being able to accomplish this, despite component failures in flight, shall be very small indeed. This probability can most reasonably be considered in relation to the number of flights or landings which will be made in the life of a fleet of aircraft. Let us assume a fleet of thirty-five aircraft with a life of 30,000 hr each and an average flight time of 5 hr. The total number of flights and landings is then 210,000, so that the probability referred to above must be in the region of 10^{-7} or less in order to reduce the risk from malfunction to acceptable proportions.

If automatic landing is to be provided on a non-scheduled basis the probability of in flight failure is less important, since loss of the facility during flight is not operationally so serious, but the probability of a failure during the landing phase must still be considered. There are various possible kinds of malfunction between 200 ft and touch-down, such as autopilot runaway, autopilot disengagement, and failure of the radio guidance. These are not all equally dangerous, but they are considered together on the grounds that they are all most undesirable in a large aircraft at this critical stage of the flight.

Using the data referred to above, the probability of failure or malfunction has been calculated for a number of different conditions, and for various configurations of autopilot and radio equipment. These results are summarized in Table II. The various different arrangements will now be considered in turn.

(1) *A system with single channels in the autopilot and a single source of radio guidance*

It is not proposed that automatic landing should be effected in the civil transport field by means of such a system. However, as it has been used for experimental purposes, the probabilities have been examined in order to show the magnitude of the calculated risk taken in using it. As it is possible that the rudder channel may in any case be duplicated (to provide yaw damping), and as it may not be essential for automatic approach, the probability of rudder channel failure has been neglected. In this case the probability of arriving at 200 ft at the end of a 5 hr flight with the equipment unserviceable for automatic landing (assuming it was fully serviceable at take-off) is $2{\cdot}4 \times 10^{-2}$. The probability of a malfunction during the subsequent automatic landing, between 200 ft and touch-down, is 4×10^{-5}.

(2) *A system using single autopilot channels but with two sources of radio guidance*

In view of the relative unreliability of the radio, the first step is to duplicate it. This improves the overall probability of being serviceable at 200 ft to make an attempt at automatic landing, but does not

reduce the risk of a malfunction occurring during the actual landing phase, since there is no opportunity of changing radio sets under these critical conditions. Thus, again neglecting the rudder channel, the probability of being unserviceable at 200 ft is 8×10^{-3} (since the probability of double radio failure is negligible by comparison with the risk of autopilot failure), whilst the probability of malfunction during the landing is still 4×10^{-5}, as in case (1) above.

(3) *A duplex autopilot (two sub-channels for each axis of control) and two sources of radio guidance*

This is a less satisfactory system than the previous one, since the probability of failure is increased with no advantage except the substitution of cut-out for runaway if one sub-channel runs away. It is assumed that either radio set may be selected by the pilot. In this case the probability of being unserviceable at 200 ft is $2{\cdot}4\times10^{-2}$, and the probability of malfunction during the landing is $6{\cdot}7\times10^{-5}$.

(4) *A triplex autopilot (three sub-channels for each axis of control) and two sources of radio guidance*

Normally such an autopilot having an axis of control in which less than two sub-channels are serviceable would not be used for automatic landing, but the facility for using a single sub-channel in real emergency might be provided. As this particular system is vulnerable from only one fault during the landing phase, owing to the limited scale of radio equipment, such provision would seem to be not unreasonable. In this case the probability of being unserviceable at 200 ft to effect an automatic landing is $4{\cdot}7\times10^{-4}$, and the probability of malfunction during the landing phase between 200 ft and touch-down is $2{\cdot}7\times10^{-5}$. Here the probability of autopilot failure during the landing is negligible in comparison with the probability of radio failure, so that the safety of automatic landing with a triplex system cannot be further improved without increasing the overall reliability of the radio guidance equipment.

(5) *A triplex autopilot (three sub-channels for each axis of control) and three sources of radio guidance*

Such an arrangement can be made to provide a genuine triplex control system for the achievement of automatic landing. As such, protection can be provided against malfunction arising from the failure of any single component in the system, up to the level of a single sub-channel, or radio guidance element. Owing to the considerably improved level of safety achieved thereby, as compared with the previous example (case (4) above), no account will be taken of the possibility of using the system in emergency at less than a duplex level, and the use of a single unmonitored sub-channel by itself in real emergency is not admitted. Under these conditions the probability

of being unserviceable at 200 ft to effect an automatic landing is $1{\cdot}2\times10^{-3}$. If the system is fully serviceable at 200 ft the probability of malfunction during the landing phase is $3{\cdot}3\times10^{-9}$. If we discount the radio guidance equipment, and consider the triplex autopilot alone, the probability of being unserviceable at 200 ft is $2{\cdot}4\times10^{-5}$, whilst the probability of malfunction during the landing becomes 6×10^{-10}.

(6) *A quadruplex autopilot (four sub-channels for each axis of control)*

The type of radio guidance system for use with fully certificated automatic landing is not yet known. No attempt will therefore be made to estimate the failure probabilities of a complete system composed of a quadruplex autopilot and its associated scale of radio guidance equipment. However, if the quadruplex autopilot is considered by itself, the probability of being unserviceable at 200 ft to effect an automatic landing is $1{\cdot}1\times10^{-8}$, and the probability of a malfunction whilst landing is only 8×10^{-15}, if all sub-channels were serviceable at 200 ft.

The failure probabilities which have been discussed above may be in error by an order of magnitude, but it is thought that they are conservative. They make the point quite clearly that the level of safety provided by a duplex autopilot is insufficient for automatic landing, and further, that in one flight in forty the autopilot (or its associated radio) will fail. The latter objection can, of course, be overcome by providing a duplicated installation of conventional equipment. In this case, however, conventional methods of providing safety in the event of malfunction are required.

With a triplex autopilot dependent on two conventional sources of radio guidance, neither the reliability of the system at the end of a flight, nor the level of safety during the actual automatic landing, can be considered acceptable. If a full triplex system is provided, including the radio guidance, the safety of the actual landing is quite acceptable, if the equipment is fully serviceable at 200 ft on the approach; but the reliability to achieve this is lacking, if total dependence is to be placed on the system on a scheduled basis. In certain circumstances the level of reliability might be considered adequate, when taking other operational considerations into account.

Even accepting the rather pessimistic basis on which the failure probabilities have been estimated, it is clear that the level of both reliability and safety provided by a quadruplex autopilot is adequate to enable it to be used for scheduled dependence on automatic control of flight in general, and on automatic landing in particular. The reliability and safety of automatic landing will then be dependent on the development of suitable radio guidance. It is thought that the reliability of radio altimeters and of the simple aids likely to be used for azimuth guidance during automatic landing, can be sufficiently improved to match that of the

autopilot in the period which will be required for the development and installation at suitable airports of the appropriate ground aid for azimuth control.

TABLE 2

Scale of equipment		Probability of	
Number of sub-channels in multiplex auto-pilot for each axis of control	Number of sources of radio guidance	Arriving at 200 ft unserviceable to effect an automatic landing	Malfunction of the system during an automatic landing if equipment fully serviceable at 200 ft on the approach
1	1	$2{\cdot}4\times10^{-2}$	4×10^{-5}
1	2	8×10^{-3}	4×10^{-5}
2	2	$2{\cdot}4\times10^{-2}$	$6{\cdot}7\times10^{-5}$
3	2	$4{\cdot}7\times10^{-4}$	$2{\cdot}7\times10^{-5}$
3	3	$1{\cdot}2\times10^{-3}$	$3{\cdot}3\times10^{-9}$
3	Discounting radio	$2{\cdot}4\times10^{-5}$	6×10^{-10}
4	Discounting radio	$1{\cdot}1\times10^{-8}$	8×10^{-15}

4. FAILURE DURING AUTOMATIC LANDING

It might be thought that the difficulty of achieving effective multiplex control in an automatic pilot would be such that the risk of a serious disturbance to the flight path would still remain, in the event of a serious malfunction occurring in one of the sub-channels. Such a disturbance would clearly be quite unacceptable during the final stages of an automatic landing. The investigation of a particular multiplex system has now been carried to the point where it can be demonstrated that this need not be so. It is not within the scope of this paper to discuss the technical details of any such system, but the practical conclusions to be drawn from such an investigation are of paramount importance in following the general theme.

In order to simplify the treatment, consideration will only be given here to the use of a triplex system controlling the flare phase of an automatic landing in the vertical plane alone. In order to investigate this particular aspect of the problem a triplicated multiplex system was built in the laboratory for control about the pitch axis. This was coupled to an analogue computor representing the approach characteristics (ignoring ground effect) of a large, four-jet aircraft. Figures 1 to 4 were obtained with the aid of this equipment.

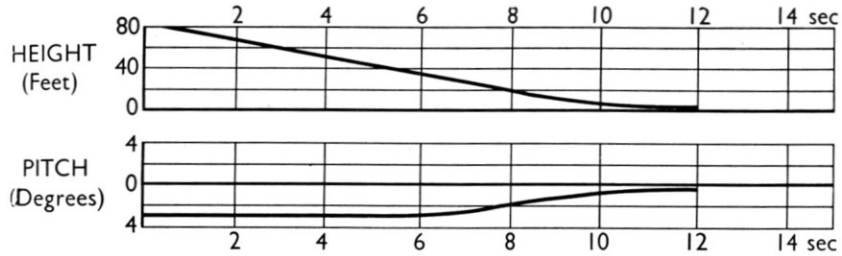

FIG. 1. Three sub-channels engaged . . . no fault.

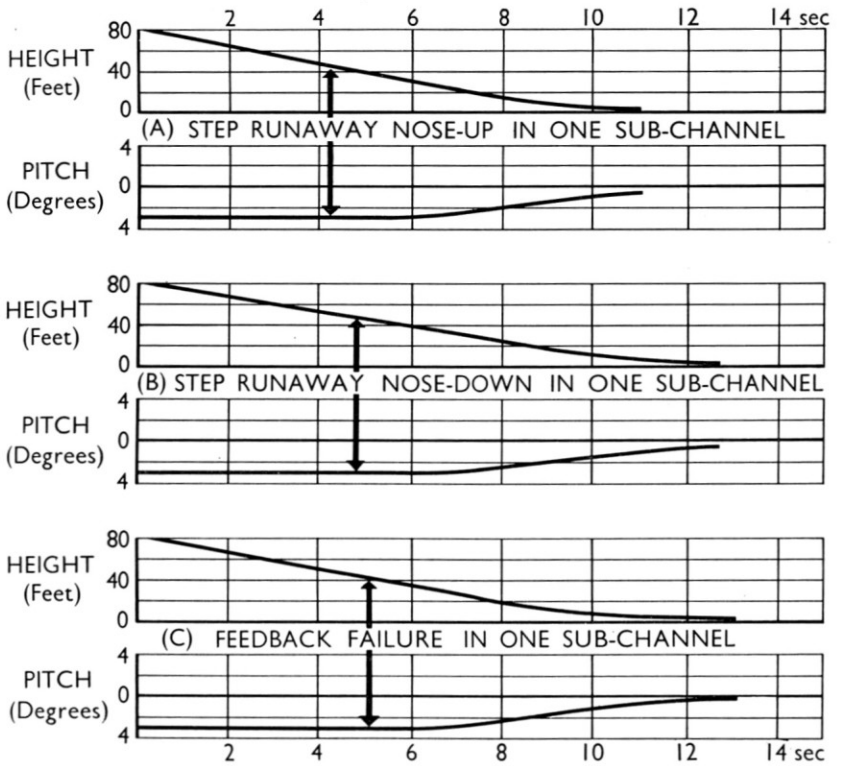

FIG. 2. Three sub-channels engaged with automatic disengagement.

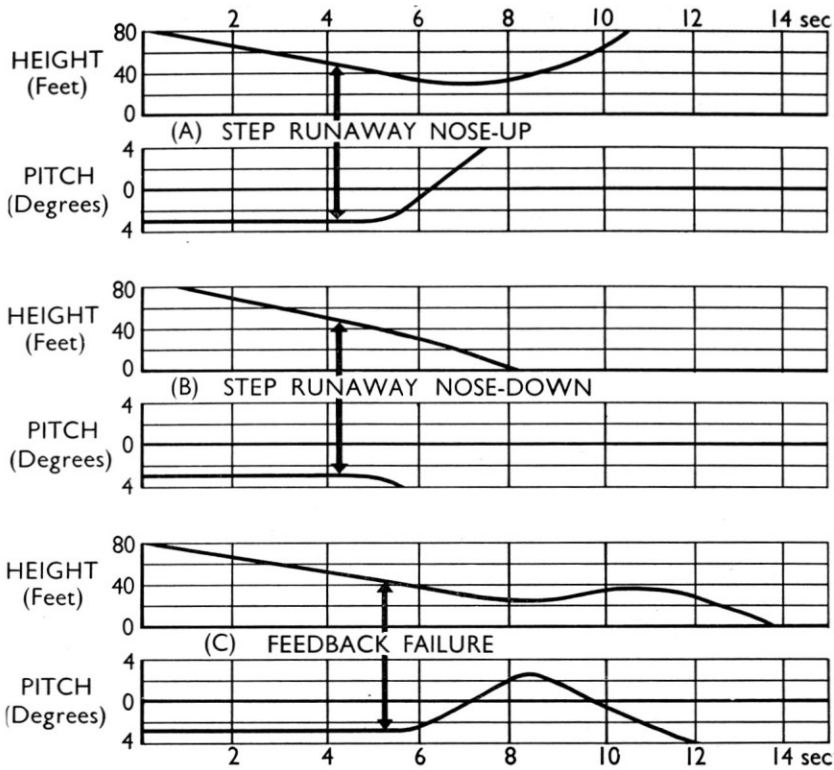

FIG. 3. One sub-channel engaged.

In each figure two curves are shown. The upper one is a trace of height above the runway plotted as ordinate, against time as abscissa. The lower one shows the corresponding changes in pitch attitude plotted as ordinate, against the same time scale as abscissa. The datum of the pitch scale is empirical.

The following cases of attempted control to touch-down are illustrated:

FIG. 1. Using the triplicated multiplex system.

FIG. 2(A). As Fig. 1, but a nose-up step function runaway injected into one of the three sub-channels.

FIG. 2(B). As Fig. 2(A), but a nose-down sense on the runaway.

FIG. 2(C). As Fig. 1, but feedback failure introduced into one of the three sub-channels.

FIG. 3(A). Using one sub-channel only, with a nose-up step function runaway injected into it.

FIG. 3(B). As Fig. 3(A), but a nose-down sense on the runaway.

FIG. 3(C). Using one sub-channel only, with feedback failure introduced into it.

In each of the cases illustrated so far, using the full triplex system, reliance was placed on the automatic disengagement of a sub-channel in

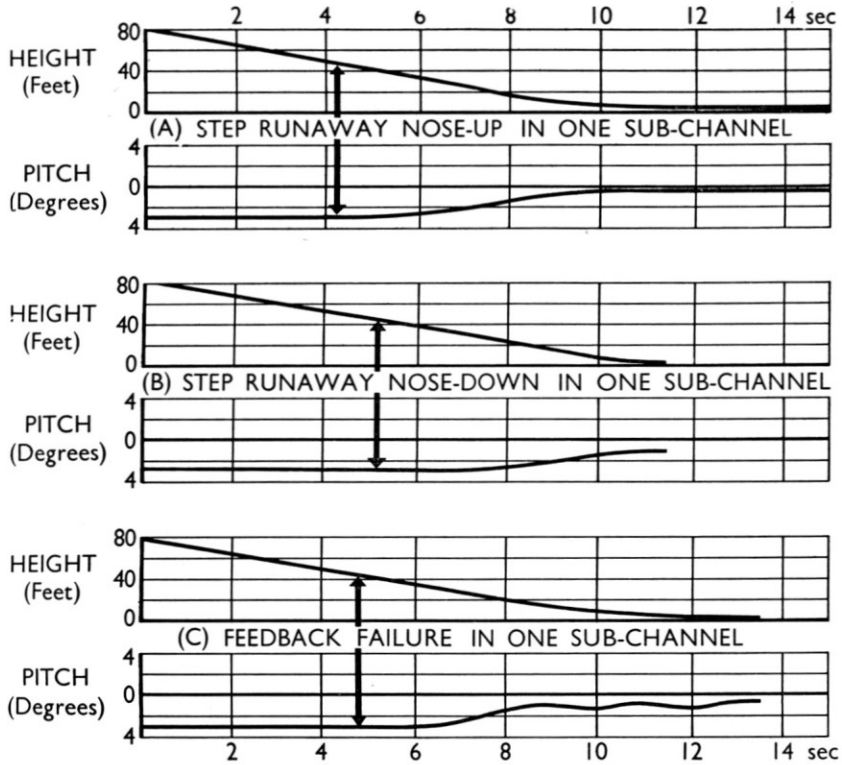

FIG. 4. Three sub-channels engaged without automatic disengagement.

the event of malfunction. Each sub-channel has sufficient power to provide the necessary control when acting on its own. If the disengagement system should fail, control is still retained by the two serviceable sub-channels overpowering the one that has failed.

The following cases of automatic control are illustrated using the triplex system without disengagement of the faulty sub-channel:

FIG. 4(A). A nose-up step function runaway injected into one of the three sub-channels.

FIG. 4(B). As for Fig. 4(A), but a nose-down sense on the runaway.

FIG. 4(C). Feedback failure introduced into one of the three sub-channels.

It will be appreciated that a safe touch-down would have been achieved in practice in every case illustrated using the full triplex system, notwithstanding the faults injected into it, and even when the automatic disengagement of a faulty sub-channel was inoperative.

5. CONCLUSIONS

The importance of the modern automatic pilot in transport operations has been reviewed above. At the current stage of its development this is

based on three factors. Firstly its ability to relieve the strain on the operating crew, and thereby possibly to reduce the crew complement. Secondly to achieve more effective flight control, and thereby to improve the overall efficiency in the use of the transport aircraft. And thirdly to assist in raising the current level of approach success under instrument conditions. Automatic landings are now being carried out as routine at experimental establishments, and we need not look too far into the future to see such techniques being exploited in scheduled transport operations.

Notwithstanding these important benefits which the modern automatic pilot is capable of bestowing on transport operations, it has also been shown that serious difficulties are now being encountered in providing the necessary authority to the equipment in a safe manner. This leads inevitably to the consideration of using a multiplex autopilot system, in order to overcome the difficulties of safety clearance. Although the safety problem can be partly met by using a duplex installation, the penalty of an unacceptably high failure rate has to be accepted with this solution. A triplicated multiplex installation not only overcomes the failure rates inherent in the duplex installation, but also makes possible the use of non-scheduled automatic landing at a high level of safety, subject to the development of radio guidance equipment with an equally satisfactory overall failure rate. If in the years to come it becomes necessary to base an operation upon the certainty of certificated automatic landing, then the choice will inevitably be to install a quadruplicated multiplex installation, with the appropriate radio guidance equipment to match it.

Finally I must acknowledge my indebtedness to my colleagues in Smiths Aircraft Instrument Ltd., without whose considerable assistance this paper could not have been written, and in particular, to K. Fearnside, Manager of the Research Department and T. B. A. Boughton its chief Aerodynamicist.

REFERENCES

1. K. FEARNSIDE, A Study of the Longitudinal Response to Vertical Gusts of an Air craft under Autopilot Control. Working paper presented to the Tenth Technical Conference of the International Air Transport Association, Miami, November 1957.
2. W. J. CHARNLEY, A Study of Approach and Landing Aids. Presented at the Convention on Radio Aids to Aeronautical and Marine Navigation, at The Institution of Electrical Engineers, London, March 1958.
3. G. W. H. GARDNER, Automatic Flight—The British Story. The Forty-Sixth Wilbur Wright Memorial Lecture, given before the Royal Aeronautical Society, London, May 1958.

DISCUSSION

A. STRATTON*: Mr. Majendie has presented a stimulating and provocative paper. In spite of what he says about a statistical risk of a catastrophic runaway not being acceptable in civil operations his paper is, in fact, concerned with reducing this risk to acceptable proportions. It is on this question of acceptable risk that I would like to pose my first question.

Mr. Majendie poses, for argument, a fleet of aircraft with 10^6 hrs operation and suggests that there should not be more than a 1 in 20 chance of failure (during landing) in the whole of this period. If the chance of a failure being catastrophic is lower by an order of magnitude, as Mr. Majendie suggests, then the chance of a catastrophe due to the autopilot is being put at 1 in 200 or less in 10^6 hr. I would like to ask Mr. Majendie if he has been able to obtain any comparable statistics from the aircraft manufacturers or operators on their achievements, aims, and expectations, from the airframe and engines, and also whether any manufacturer or operator present would be as bold as to supply these data.

The second point I would like to raise is on the measures necessary to achieve this aim. Whilst suitable multiplexing can multiply probabilities of failure, where extremely low failure rates are aimed at it is vitally important that there is no correlation of failures, that is the systems must be truly independent, or the probability of failure reverts to that of the common component or feature. The comparator, for example, would have to be very carefully designed if it were not to be a common factor, and I am not sure that I agree with Mr. Majendie's allocation of a nominal 50% extra probability of failure. Other common factors in such an installation would be, power supplies, wiring liable to damage from a common cause, switching, etc.

I would like therefore to ask Mr. Majendie the extent to which he has considered the question of correlated failure, due possibly to factors outside the control of the autopilot designer.

Finally, I would like to comment on the alternate solution proposed by Mr. Majendie—namely, complete quadruplication. Although he has been careful to state at various stages that, if certain hypotheses are in error by an order of magnitude, it will not affect the conclusions, I have a feeling that there are many orders of magnitude concealed in the various factors, and that a combination of a reassessment of the acceptable risk together with an increase in component reliability might enable the quadruplicated system to be avoided, for I believe it will be very difficult to avoid correlated failures in such a system.

A. M. A. MAJENDIE: Mr. Stratton asks whether we have been able to obtain comparable statistics to those quoted for the automatic pilot covering the engines, airframe, and general operation of aircraft. The short answer is no, and we would very much like to have such additional information, as without it, it is difficult to set our own figures into proper perspective. We have endeavoured to estimate the human malfunction rate during the approach and landing phase on contemporary aircraft, and our best estimate is that there is a risk of serious human failure in about 1 in 10^5 approaches. This figure might not be correct for the newer types soon to enter service.

The second question posed by Mr. Stratton concerns the measures needed to ensure a genuine measure of independence between the various sub-channels in a multiplex installation. Clearly there can be no half measures here, and the principle must be carried throughout the whole installation right back to the power supplies. Very careful attention is needed on cable routing, etc. The systems which we are developing do not use an electronic comparator; comparison is carried out mechanically between the output torques of the sub-channels. Such an arrangement is

* Senior Principal Scientific Officer, Ministry of Supply, Royal Aircraft Establishment, Farnborough.

both fundamentally sound and fairly easy to protect from becoming a source of common failures.

Mr. Stratton's last comment is of course correct. The degree of multiplicity required to satisfy a particular level of safety can only be settled after a very careful analysis of the operational requirement which must be met. A triplex system may well meet most practical requirements for automatic landing. The problems of installing a quadruplex system are clearly greater than for a triplex system, but pose no additional difficulties of a fundamental nature.

D. M. JAMESON*: The suggested trend in autopilot design was to be welcomed, since

(a) the aeroplane would cease to be in the hands of a "pupil" autopilot, from which control may have to be snatched in a critical phase of the flight—it was good to see the "pupil" growing up;
(b) some emergency drills might be eliminated from the ever-growing total which at present impose a mental load on the pilot, this load being possibly in proportion to the number of *combinations* of such drills which might have to be used;
(c) the use of a multiplex system for a vital service enables its operational reliability to be assessed relatively early in the life of the aeroplane, and at minimum risk.

In examining the presently achieved fatal accident rate from all causes, it appeared that a risk per flight of $2\frac{1}{2} \times 10^{-6}$ per hr of flight (total risk) or 1×10^{-6} per hr of flight (airworthiness risk) was roughly the figure being achieved in scheduled transport.

If this safety level was to be maintained, the target maximum risk per hr from each of the major causes (as distinct from components) such as fire, structural failure from manoeuvre loads, structural failure from gusts, loss of climb performance, failure of a vital system, etc., should be kept down to 10^{-7}. Bearing in mind the existence of other systems besides that of the autopilot, Mr. Majendie's proposals appeared to aim at a reliability of the right order.

The author's point about the reliability of ground aids was a real one, and deserved more attention: the aircraft power supply should also receive careful attention, though the modern "split" electrical system represented a considerable advance in this field.

A. M. A. MAJENDIE: Mr. Jameson's remarks are most valuable, as they provide authoritative supporting evidence that the level of safety at which we have been aiming is of the right order. I strongly endorse his remarks concerning the careful attention needed in the design of the aircraft power supply in the future.

G. ERNST: La solution proposée par Mr. Majendie suppose toutes les chainez en marche. Après un certain temps de fonctionnement, la sécurité est diminuée (par l'usure) également pour toutes les chaines. On peut donc envisager de n'utiliser qu'une chaine et laisser les autres en repos. Indépendant de la question du démarrage des toupies ou du chauffage des amplificateurs, ces chaines présentent donc plus de sécurité que la chaine usagée.

Avez-vous fait des études de comparaison ou des calculs de probabilité pour une conception de ce genre ?

A. M. A. MAJENDIE: We have not specifically studied a system along the lines suggested by Mr. Ernst, except in the case of a simple duplicated installation as discussed in the paper. We have, however, considered a duplex system with a third channel as stand-by. This study did not reveal any significant advantage from the point of view of reliability over a triplex installation.

* Air Registration Board, England.