The Achievement of Reliability in V.T.O.L. Autocontrol Systems

by

R. W. Howard

Elliott Flight Automation Ltd, Rochester

Introduction

There is probably no word in practical engineering terminology today which is more loosely used than 'reliability'. One accepted definition for reliability is "The measure of the ability of a device to perform a task to a specified standard when required". It should be noted that there is no implication in the definition that any particular reliability technique should always be used. In fact there are many ways in which any task can be performed and all must be carefully weighed and perhaps mutually compounded if the optimum solution is to be obtained. The techniques available to the systems designer fall into two main categories, those which depend upon design and manufacturing experience to produce system elements of high quality, and very low failure probability in the environment in which they must be used, and secondly, those which employ redundancy techniques of one sort or another. The treatment required for each element of a system to obtain an overall satisfactory level of reliability must obviously vary according to experience, background, and understanding of the failure or wear-out mechanism of each particular element. Where a choice between "extreme quality control' or "redundancy" design approach is not clear on technical performance grounds than further factors must be cosidered, the most important being "maintainability" which is the measure of the ability to maintain the performance of a device to the required standard by defined procedures.

Thus the wide operational support requirements of a system must be considered, in addition to design, manufacture safety and performance requirements, and the overall cost is then a parameter in the evaluation of the implementation of the requirement, as the same task might be achieved by different processes at widely varying cost.

This is a far cry from exclusive concentration on the improvement in quality of devices which have no ability to survive a failure when it occurs, and no hope of achieving the "reliability" made possible by employing the most simple redundancy technique.

The modern systems design approach is best summarised by an overall definition from which the requirements of basic design, operational performance and maintainability can be deduced, in sensible proportions. This is "a requirement to achieve the performance necessary to complete a 'mission' with a specified high probability of success at minimum cost".

Some of the methods and techniques now being employed in pursuit of this overall design criterien are discussed below.

1. The Tools of Reliability

There are several reliability "tools" available to the systems designer and the main ones can be catagorised as the (a) exercise of quality control, (b) the use of failure-preventive maintenance and (c) the use of redundancy to give a failure detection or failure survival capability. These will now be considered in turn,

1.1. Quality Control

If the quality of a device is to be accurately controlled then what it is that constitutes quality in the device must be clearly understood. A corollary of this is that the relevant "failure mechanisms" of the device must be recognisable and understood for the environment in which it is to be used.

Failures can be attributed to many causes; inadequate equipment design, an error in manufactoring processes, misuse, bad maintenance, poor packaging in transit and probably many others. Normally however a component or device will not be chosen for incorporation into aircraft equipment unless it has a record of successful use, or is similar in design to an acceptable device, or it has been adequately tested in the environment in which it must work. Hence, having chosen the basic components, quality control normally relates to the task of ensuring in manufacture, that some minimum standard is always achieved. If we consider as an example, the electronic components such as resistors, capacitors and semiconductors used in aircraft autopilot computers, then the average failure rate now achieved is about 0,1% per 1000 hours, i. e. an equipment having 10,000

components can expect to have an M.T.B.F. (Mean Time Between Failures) of about 100 hours. These are relatively "good" components by present-day standards and it is known from experience that only a small percentage of "good" components should fail in the time-scale of operation of modern autopilot equipment, although actual failures are unpredictable. If, therefore, before they are built into equipment, all components are subjected to some test designed, by knowledge of the failure mechanisms, to search out an impending failure, then the maximum equipment reliability can be assured.

A great deal of work has been done throughout the world to discover and understand the basic failure mechanisms of commonly used electronic components, and as new ones are devised, considerable effort is being devoted to this aspect. As an example of the test techniques used, the following is a practical example. A certain high stability carbon resistor was formed by depositing carbon on a ceramic cylinder. When failures were investigated it was noticed that in nearly all cases the carbon film was "crazed". All of these resistors were subsequently tested by passing a small current through them and at the same time subjecting them to varying mechanical stress. It was then easy to eliminate the potential failures by observing the higher noise level. There are many much tests which can be devised for different components by studying their failure mechanisms. By this means between 5% and 10% of the total number of electronic components can be eliminated during manufacture so that most subsequent failures in service are due to random unpredictable causes.

When a well designed and tested piece of equipment has been in production, and in service for some time, say greater than one year, then a level of reliability will be obtained which can only be further improved by most extraordinary means, which is normally very expensive in terms of analysis and design modifications. The level of reliability achieved may still fall short of many current requirements, such as for the design of V.T.O.L. autostabilisation systems and in such cases predictable failures are more easily handled by using failure survival redundancy techniques, rather than by attempting to improve the basic reliability beyond reasonable levels of achievement in manufacture and operation. This is discussed further in sections 1.3. and 3.

1.2. Maintenance

In section 1.1. the importance of understanding the failure mechanism of a component or device was stated. If the time-scale of failure development is also known, as is normal in cases where wear, for example, is involved, then the device can be subjected to "failure preventative" maintenance. That is, a replacement is effected when a failure is imminent, but before it happens. This technique for greatly improving "in-flight" reliability is rarely applicable to modern electronic devices which do not generally exhibit a wear-out type of characteristic in any reasonable operating timescale, but it is applicable to most mechanical, electromechanical hydraulic devices and to structures which are subject to fatigue. As an example, the engines used on large jet transports if left operating without overhaul, would have a high probability of failure after about 4000 hours. In fact shutdowns of engines due to failures in flight occur at a rate of about one in 25,000 hours which gives some measure of the efficiency of failure preventative maintenance in this case.

1.3. Redundancy

The use of redundancy in an equipment or system design will increase the rate at which failures occur depending upon the level of redundancy employed. However, this does not constitute a decrease in reliability, as the first failure, when it occurs, does not put the equipment out of action and the aircraft may then complete a mission which it might otherwise have been forced to abandon.

The use of redundancy to achieve lower failure probability per mission is a relatively new technique for electronics and control system designers, although it has been one of the important design principles upon which safe heavier-than-air aircraft have been developed.

A wide range of redundancy techniques are now being developed for application to airborne automatic control equipment. These can be classified broadly into the categories of multiplexing, comparison monitoring, integral redundancy and dissimilar redundancy. It is likely that the detailed design techniques will be as varied and complex as those used in the design of structures and mechanisms but a number of fundamental design principles are now arising from a wide consideration of various requirements. First the type of redundancy to be

used in a particular application should be chosen on the basis of performance and safety requirements, bearing in mind that the level of redundancy need not necessarily be uniform according to the requirements of the worst element. Then the system operating tolerances acceptable on serviceability grounds should be considered, to determine the form of lane balancing required. If possible, the basic system elements should be failsafe or have first-failure characteristics which cause deterioration only, no matter what form of redundancy is used, so that alarming and rapid correcting actions are never required. Whichever redundancy technique is employed there must be some positive means of indicating partial failure either at the instant it occurs, or during subsequent normal inspection checks if adequate reserve reliability is inherent. For the most stringent safety requirements, say where safety is continuously involved, dissimilar redundancy should be employed, so that the effect of remote common hazards is avoided as much as possible.

2. Redundancy Techniques in Automatic Control System Design

2.1. Automatic Failure Detection Techniques

In many new automatic control system applications, especially those associated with V.T.O.L. aircraft, it is very important that equipment failures be immediately detected. This may be required either to give an indication demanding rapid pilot action, or it may be the prologue to an automatic failure isolation and survival action. Automatic failure detection techniques fall into three main categories, (a) absolute measurement, (b) performance measurement and (c) comparison monitoring and various combinations of these are used in practice.

2.1.1. Absolute Measurement

All means of failure detection involve either a measuring or a comparison process and a failure of the measuring or comparison device is always indetectable from a failure of the device being examined, unless a third suitably coherent device is also available and is used in such a manner that similar failures cannot occur in two or more of the devices at the same time. That is, any direct or indirect cross-connection required to allow the measurement or comparison to take place, must not introduce cross-dependence.

In relation to absolute measurement (absolute monitoring) for

example, the presence of an electrical voltage or hydraulic pressure can be detected and measured with simple automaic instruments. Similarly by absolute measurement one can check signal line and power circuit continuity, load and source impedances, radio carrier transmission levels, modulation depths, relative gain and phase etc. However, a complete failure detection system based on such principles if possible would be very complex indeed and it would be extremely difficult to prove that failures could not occur which could go undetected, especially between the measuring points. Perhaps the greatest difficulty however, is making any sort of assessable measurement when the system is in a dynamic state. For example, the computation of an exponential flare-out demand from radio altimeter signals would be impossible to check by direct measurement as it occurs, and the assessment of independent flare path or rate of descent measurements is also too difficult in this critical manoeuvre.

It is possible in certain cases to inject an excitation signal into part of a system, assess its effect and then cancel it before it appears as an output. This technique of absolute response monitoring has been investigated for "on-line" checking of simple yaw dampers but usually it is more economical and certainly more complete to use performance of comparison monitoring techniques.

2.1.2. Performance Measurement

There are often modes of operation both of single devices and of full systems which lend themselves to overall performance checking. For example, a simple case is that of a feedback servo-mechanism which if operating corretly will not develop an input-output error demand greater than a certain value in a given time, this being a function of the type of input which it receives. This value can be constantly checked and this constitutes a failure detection means. On a broader scale this principle can be applied to autopilot "hold" facilities. For example, in a height lock system, a deviation from the height originally selected by more than some predetermined amount, measured on an independent sensor, can be taken as a failure. In this example, it is important that the failure detection circuit is independent of other equipment and in addition various precautions are taken such as having a mechanical bias applied to the monitor sensor pick-off to avoid the possibility of missing a failure on a normally "null" circuit.

2.1.3. Duplexing

The duplex system comprises two independent subsystems, complete in every respect, which are compared at their outputs, and both are permitted to operate in parallel as long as there is an acceptable measure of agreement. If a disagreement occurs, both systems are automatically disengaged. An example duplex aircraft control axis is shown diagrammatically in fig. 1. The disadvantages of such a system are, excessive weight, and the necessity for output synchronisation in order to eliminate the effect of different manufacturing tolerances in the two channels.

2.1.4. Comparison Monitoring

Comparison monitoring in its most advanced form, is in fact best described by considering its derivation from a duplex system, which is its extreme case. The development of the "duplex" system into the more economical "comparison monitored" system is shown progressively in figs. 2B, C and D. This example relates to the automatic landing of conventional aircraft. Fig. 2B substitutes a monitored radio altimeter, with two outputs and a "disconnect" demand line, for the two original radio altimeters, while keeping the same overall failure detection capability. In fig. 2C this principle is applied to all sensors (examples are given later in this section of the design of two such "monitored sensors".

In fig. 2D, the fullest economy is effected by eliminating also one of the two output actuators. The second actuator is not required for control purposes and serves only to give a temporary control lock in the event of a hardover demand. This is a doubtful advantage in a large transport aircraft in the automatic landing mode, as it is necessary in any case to disengage the automatic control immediately following a failure. The operation of the remaining actuator servo in fig. 2D is checked by inversing its output response, thus producing synthetically its input demand, and comparing this with similar demand from the comparison computer. A size reduction in the comparison computer occurs due to the elimination of the actuator amplifier and other driving elements. Some advantages of the comparison monitored arrangement as a "failure detection" plus "fail-soft" system are, reduction in overall weight due to the selective nature of the redundancy used, detection of failures at the point at which they occur so that disconnect limits in each case are related only to the

equipment in which the failure occurs, and elimination of the need for cross-synchronisation because signal consolidation is effected at the output of each element of the system. Experience has shown that the monitor additions if carefully designed will increase the weight of a single axis of an autopilot by only 25%.

In order to realise the comparison monitored system of fig. 2D self-monitored sensors are required, and examples of monitor techniques for two of the four sensors in fig.2 A.D.S. (Air Data System) and RR (radio altimeter) are illustrated in figs. 3 and 4 respectively.

Fig. 3 is a monitored pressure altitude sensor in which a single servo follow-up device, nulls the pick-off of two independent capsule mechanisms. Any failure in the system will be indicated as it will cause the disconnect output to deviate from some constant preset value. This principle is applicable also to barometric airspeed sensing for automatic throttle control systems, and to the derivation of information for instrument presentation.

On figure 4 is shown a monitored radio altimeter which has two receiver elements R_1 and R_2, instead of one. R_2 receives its signals via a delay line, equivalent to a height Hc, and a failure of any part of the monitored altimeter will cause a demand on the disconnect line. (Tis is normally hiassed so that null failures due to broken wires etc. are not overlooked.)

Systems employing sensors using the above, or similar principles, are now under test in the VC.10.

The use of selective redundancy in the self-monitored form described is now being widely adopted throughout the world in new advanced aircraft control systems.

2.2. Failure Survival Techniques

In the technology of electronics and automatic control system design, "failure-survival" or "fail-operative" inevitably implies the use of some form of redundancy. Much is now being learned from the designers of structures and mechanisms, to whom redundancy techniques are normal design tools. Examples of the various techniques now being employed by control system and and electronics designers are outlined in the following sections.

2.2.1. Multiplexing (Example: Triplex)

This is the purest form of equipment redundancy for single failure survival and the least economical. For example, a triplex system is illustrated in block diagram form in fig. 5. It comprises three independent subchannels, the outputs of which combine to drive the control surface. If a significant failure occurs in one subchannel, then by virtue of its subsequent disagreement with the other two subchannels it will be overriden and then disconnected. The two remaining subchannels will then continue to drive the qutput and in the rare event of a second failure, the two will oppose each other and the comparator and disconnect device will then disengage both.

The disadvantages of such systems are excessive weight(at least 3 times a single channel), the use of one more control servo than is necessary (a single one is never used alone) and the requirement for low speed cross synchronisation between the "independent" sub-channels to compensate for differential datum and gain drifts due to unavoidable manufacturing tolerances. The latter fundamentally sets a limit to the frequency of failure (or rate of error development) which can be detected.

Multiplex systems are best applied in simple control systems such as electrical signalling and rate stabilisation.

2.2.2. Multiple Monitored System (Example: Duplicate Monitored)

The multiple monitored system seeks to achieve a failure survival capability by using selective redundancy as described in section 2.1.4. In certain cases,such as the duplicated-monitored system shown in fig.6, the associated technique of autochangeover allows freedom from the effect of differential manufacturing tolerances between the systems.

The system of fig.6 comprises two comparison monitored systems as described in section 2.1.4. The control surface is normally driven from system one, while system two is synchronised in a standby condition. In the event of a failure system one will automatically disengage, and in doing so, will automatically demand the engagement of system two via the autochangeover relay. A second failure will cause the disengagement of system two. Such a system can only be applied in cases where changeover times up to 1 second in duration are acceptable and it is most applicable to automatic approach and landing applications where a large complex of control sensors, computers and pilots controllers are involved.

2.2.3. Integral Redundancy

In recent years much effort has been devoted to the design of failure-survival systems which do not require complete triplication, cross-synchronization, monitoring, and so on. Some redundancy is clearly necessary, but it can be applied more economically and effectively. A new technique now being used is to give each element of a system failure-survival capability within itself, by means of built-in or integral redundancy. Such elements connected together into a control system allow multiple paths for control signals and it is, therefore, highly probable that numerous internal failures will not put the system cut of action, while, for example, pure triplication with a majority vote comparator can survive only one fault. Partial failure may cause slight performance deterioration, but this can normally be tolerated.

Fig. 7 illustrates the greater survival capability of integral redundancy. Each of the three channels (or lanes) of the triplicated system in this case includes four elements, each with a failure probability of $\frac{1}{1000}$. Overall failure probability of this system is therefore

$$3\left(\frac{4 \cdot 1}{1000}\right)^2 = 48 \cdot 10^{-6}$$

The integral redundancy system shown has only two of each element, but they are arranged in failure-survival pairs. Its overall failure probability is

$$4\left(\frac{1}{1000}\right)^2 = 4 \cdot 10^{-6}$$

Although the weight of the system has been reduced by roughly one-third, its failure probability has decreased by a factor of 12. This integrally redundant system can survive a maximum of four selected failures, or a maximum of "n" selected failures if there were "n" elemental pairs. Even if the various devices for consclidating the outputs of the individual pairs are heavier than the comparator in the triplicated system - which is doubtful - the integrally redundant system offers a very great survivability advantage.

Integral redundancy, new being applied in the more advanced control systems, is well known in its passive-element form to the designers of fail-safe airframes. Fig. 8 shows diagrammatically a rate-demand and stabilization system incorporating such principles wherever possible. The rate gyro is duplicated, having two rotor and gimbal assemblies rigidly coupled at their output axes and driving a twin pick-off. These in turn, feed an amplifier containing multiple parallel circuits constructed either with completely solidstate circuits or thin-film units with very low impedance outputs so that certain failures of one will not affect the remainder.

If more conventional components are required, multiple series/parallel resistors, capaciters and inductors may be used with "flip-over" replacement transistor stages. Such circuits have been demonstrated by Elliott and practical designs for aircraft are now feasible. The amplifier feeds a multiple control actuator which will probably be a triplex or quadruplex package so that a failed element can be overridden by the remaining outputs. Changes in performance (gain, frequency-response, etc.) will result as partial failures occur in the integrally redundant elements, and in the most accurate systems where this cannot be tolerated certain loop gain, damping ratio or other model self-adaptivity can be used to lesson the effect.

2.2.4. Dissimilar Redundancy (Example: A Hypothetical V.T.O.L. Control Arrangement).

The layout of a hypothetical V.T.O.L. control axis having an aerodynami surface, a group of vertical lift units which can accept thrust modulation and a bleed-air nozzle control is shown in fig. 9. This system incorporates a realistic combination of three different types of automatic controls which perform different tasks with different degrees of efficiency, but which overlap sufficiently to give the overall system a considerable failure survival capability.

The three different automatic controls are

a) Autostabilisation, which is a limited authority system employing a limited degree of integral redundancy, similar to that describe in section 2.2.3. (fig. 8);
b) Group Thrust Compensation, which comprises a simple fail-safe pneumatic detector/actuator which is operated from pressure tappings from the group of lift units such that a thrust reduction of any one engine below a predetermined norm will initiate an increased thrust demand from the whole group by moving the throttle control runs and
c) Force and Moment computation, which is a high response control system, working on engine thrust measurements,

which constantly adjusts the lift units and control nozzles to maintain a force and moment balance.

This system is an example of the employment of dissimilar redundancy techniques and the high survival capability can be seen from a further description of the system followed by a failure analysis.

In the manual control mode in wingborne flight, lock A is disengaged and the control surface can be operated by the pilot through the series actuator on the powered control, and its demand will not appear on the pilot's control, mainly because of the resistance of the artificial feel unit. Large-authority autopilot operation can also be obtained in this mode by engaging lock A and replacing mechanical with electrical feedback. Lock A is designed to yield at some predetermined artificial-feel load to provide torque limitation at a level determined by safety requirements. A force pick-off on the pilot's control column can also be engaged to operate the controls, the power follow-up of the mechanical runs, operated by lever B pivoting around lock A, giving a low feel force.

The V.T.O.L. controls on nozzle and engines follow the powered control output from the connectionrod C, and can also obtain series inputs from the force and moment actuator D on the main powered control assembly. The engine group has an associated Group Thrust Compensator. Between the autostabilizer actuator and Force and Moment actuator sections of the powered control is a hydraulic switch arrangement which has been called a Control Fault VETO. This empowers the autostabilizer actuator to freeze the output of the Force and Moment actuator if the latter makes a demand not in agreement with autostabilizer action- a normal relationship between the two systems determines the operating characteristics of the VETO! Other aspects of the system are explained by the diagram. The overall safety philosophy can be better understood by considering the effects of various failures in the hover as follows:

NULL FAILURES OF PILOT'S CONTROL FORCE PICK-OFF OR ITS CONNECTIONS: Pilot's demands are not satisfied with small stick forces, but increased pressure causes lock A to release and direct mechanical, operation of the powered control is obtained. The autostabilizer system will still operate.

AUTOSTABILIZER FAILURE: If the autostabilizer has complete integral redundancy, the first internal failure should at most cause only slight performance deterioration. For the most stringent safety requirements if, for example, lateral stabilization is critical during transition, duplicated autostabilizers each with integral redundancy would avoid the remote possibility of a single system being put out of action by physical damage. A carefully designed duplicated system of this kind will have catastrophic failure probability lower than that of the aircraft structure.

NOZZLE OR DUCTING FAILURE: Any type of nozzle or ducting failure could be counteracted, and full control maintained by thrust modulation of the lift units.

A SINGLE LIFT UNIT FAILURE: This would be fully counteracted by the Group Thrust Compensator and high authority Force and Moment Control, and, to a lesser extent, by the autostabilizer system.

FAILURE OF THE FORCE AND MOMENT CONTROL SYSTEM: Integral redundancy would ensure that the first internal failure would cause at most only slight performance deterioration. Any subsequent failure involving a significant demand will activate the autostabilizer VETO and the autostabilizer itself will then balance out any small disturbance which does occur. If a lift unit failure occurs after failure of the Force and Moment Control, the effect will be counteracted by the appropriate Group Thrust Compensator plus the autostabilizer. Depending on the type of failure, some minor assistance may be required from the pilot.

GROUP THRUST COMPENSATOR FAILURE: The GTC is very simple and has only a passive failure characteristic. Any lift unit failure subsequent to a GTC failure would be counteracted by the Force and Moment Control.

The hypothtical system of fig.9 is an example of the use of dissimilar redundancy for achieving safety in automatic control, and shows the high degree of survivability which can be achieved without using full multiple redundancy. Such systems could certainly be applied to most combat aircraft, where mechanical control runs are relatively short, provided the short-period movements on the pilot's control column in the fully engaged mode were not disturbing to the pilot. For large transport aircraft it would probably be desirable to employ only

electrical connections. This could be affected in the system in fig.9. by removing rod E and connecting pivot F to "earth". The electrical link shown would have to be upgraded to achieve the required integrity with the mechanical link removed. Throttle run G could be replaced by electrical signalling connections.

There are other alternatives. If the direct mechanical connections are satisfactory, the stickforce sensor and powered control engage lock can be removed, and short-period auto-stabilizer demands will not appear at the pilot's controls. Complete aircraft systems based on the principles outlined could achieve failure probabilities less than 1 in 10^8 per hour.

3. System Cost Optimisation.

From the foregoing it is obvious that both component basic reliability and redundancy can have a significant effect on overall "mission" reliability and various results can be obtained, at widely varying cost if the best combinations of the two aspects are not obtained.

This is also unlikely to occur "naturally" when different sections of an organisation (e.g. the armed services) usually deal with different aspects of an equipment programme (e.g. there are normally different and separate budgets covering development, purchase, maintenance etc.). Systems can now be cost optimised if component reliability and redundancy techniques are both considered in the design stages with due consideration. to the overall object which should be 'to achieve the performance necessary to complete a 'mission' with a specified high probability of success at minimum cost". It can be shown that different type of systems (i.e. single systems and systems with various types of redundancy) each have optimum applications depending on particular requirements and in some cases completely different systems can achieve the same reliability by different means for the same cost. For example, in fig.10 is shown a plot of system cost against system M.T.B.F. Looking first at the unimodular system curve (single system), this is made up of three basic curves. First, there is an initial cost element (not shown separately in fig.10) and then two other curves, one of which shows the relationship cost and component failures, and the other the relationship between cost and development of high component reliability. Curves are also shown for bimodular and trimodular systems.

It is interesting to note that a system M.T.B.F. of X can be be obtained either with a unimodular system with a high component reliability development and quality control or with a dimodular system with a fairly low level of component reliability, at the same cost. This cost is also higher than the minimum possible with an optimised unimodular system. (level y).

The graph of fig. 10 is drawn only for illustration purposes and will obviously vary considerably depending upon the values of particular parameters.

4. Conclusion

It has been postulated that the development of high basic reliability in the components of automatic control equipment can lead to a high level of failure predictability and scheduled maintenance. However, failures when they do not occur will put a system out of action unless some form of redundancy is also employed. Techniques now being developed for automatic control systems should make the use of redundancy more acceptable in the future and it will carry a greater responsibility for aircraft safety than in the past.

A basic component reliability development will be very expensive in the future for failure survival systems, the design aim should be to develop it only to the level required for a reasonably acceptable level of servicing. Then second order redundancy (i.e. monitored duplication, triplexing or dimodular integral redundancy) should be all that is necessary to give the highest survival capability which is practically sensible. Any higher order implies inadequate basic reliability and excessive servicing requirements, or alternatively a reserve capability which ist outside the bounds of sensible design.

Finally, it is well known that the failure probabilities now being specified for many aircraft applications are so small that proof of the levels finally achieved can never be obtained in any practical series of trials. In such cases redundancy cannot only provide an operational system solution, but also, by its very nature the practical means for assessing the levels likely to be achieved.

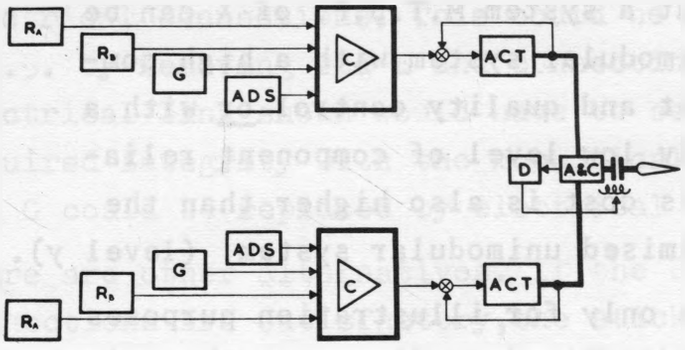
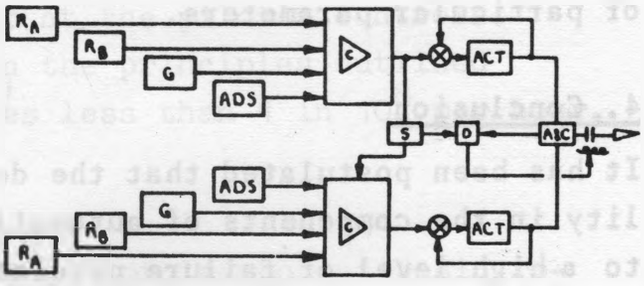


Fig.1: A duplex system

Legend

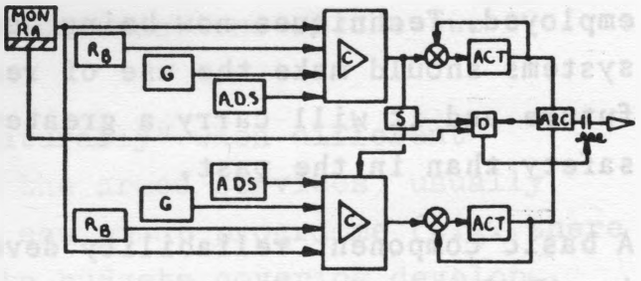
R_A	Radio Altimeter
R_B	Ground Guidance Receiver (ILS)
G	Gyro
C	Computer
ADS	Air Data System
S	Synchroniser (Low Authority)
D	Disconnect Device
ACT	Actuator
A&C	Adder & Comparator
INV RESP	Inverse Response of Actuator Servo
MON R_A	Monitored Radio Altimeter
MON R_B	Monitored Radio Receiver (EG ILS)
MON G	Monitored Gyro
MON ADS	Monitored Air Data System

A)



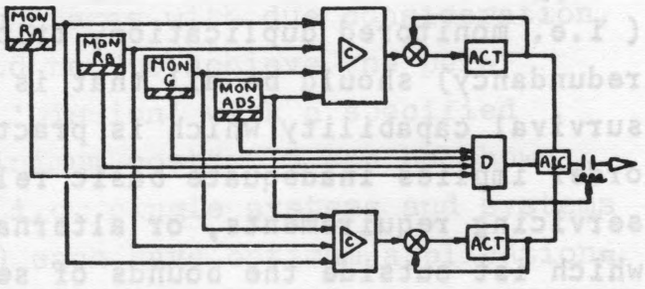
A DUPLEX SYSTEM WITH SYNCHRONISATION

B)



A DUPLEX SYSTEM WITH R_A MONITORED

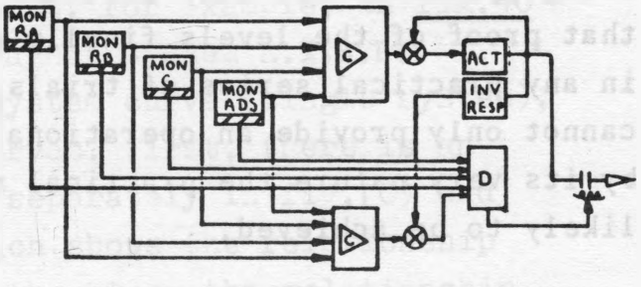
C)



A DUPLEX SYSTEM WITH ALL SENSORS MONITORED

Fig.2: The Derivation of an Automatic Monitored System from a Duplex System (by the Application of Selective Redundancy)

D)



A SINGLE MONITORED SYSTEM

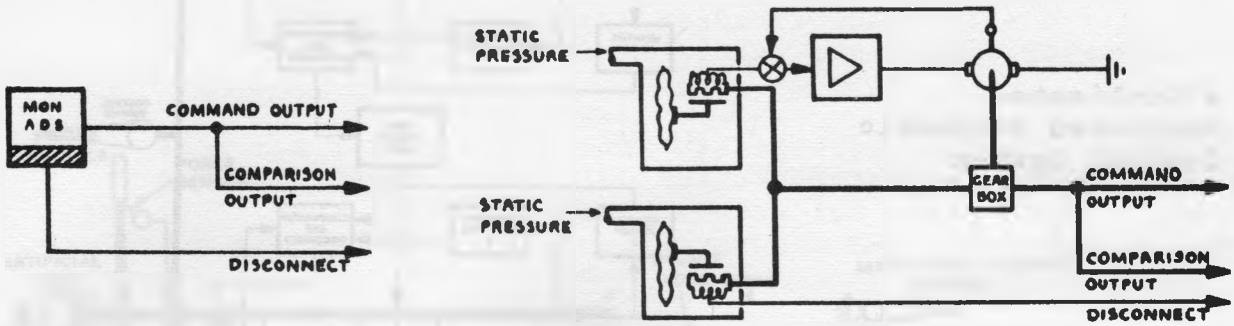


Fig.3: A Self-Monitored Pressure Altitude Sensor

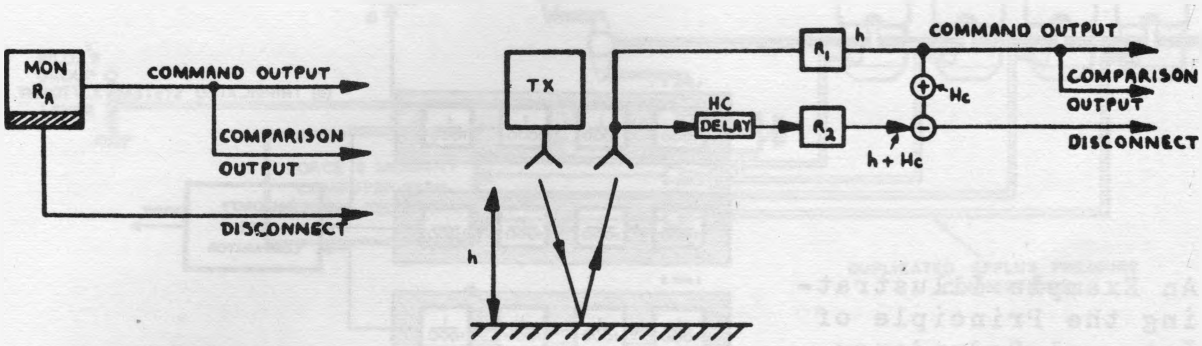


Fig.4: Self-Monitored Radio Altimeter

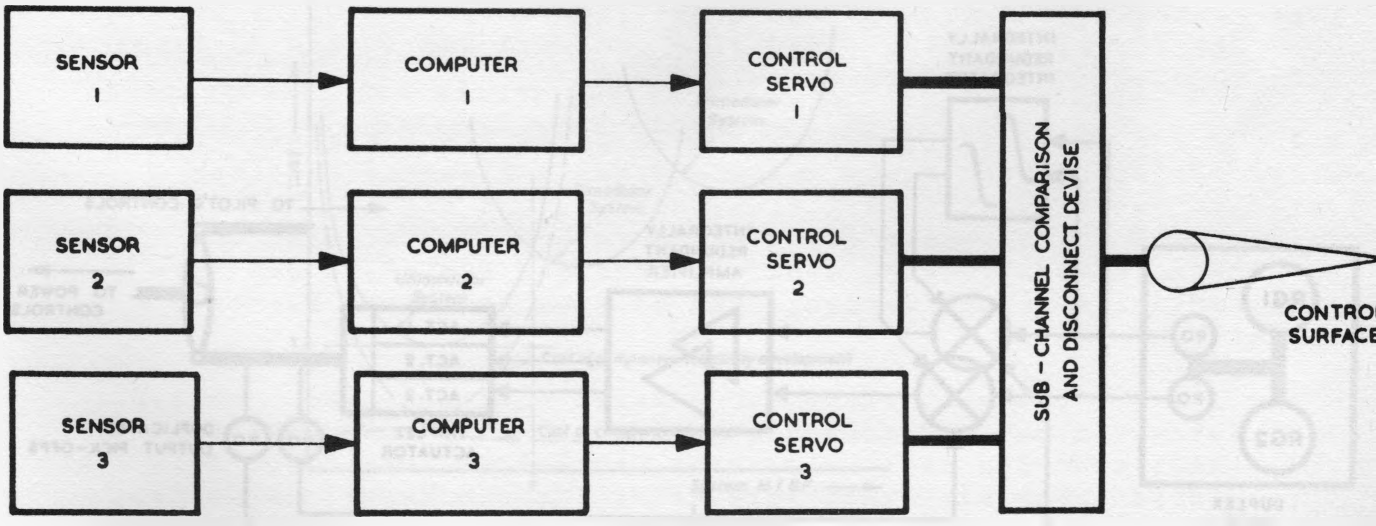


Fig.5: A Triplex Automatic Control System

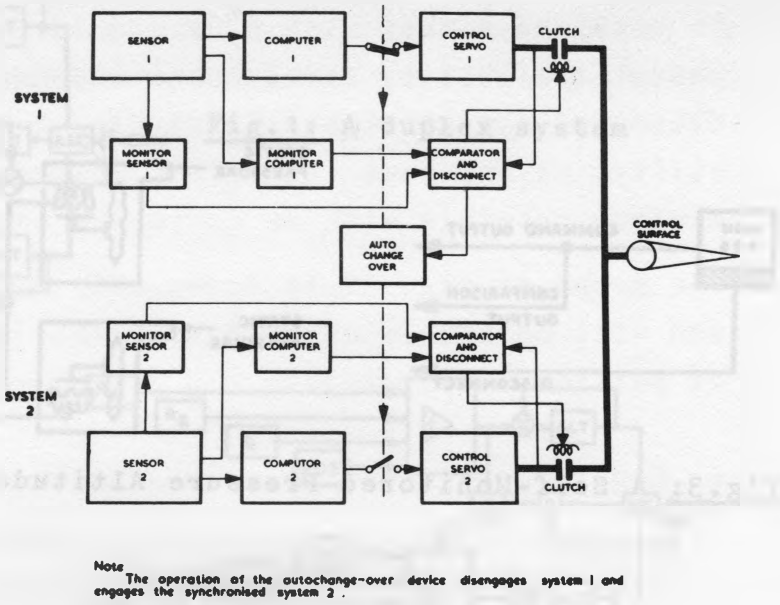


Fig.6: A Duplicate-Monitored Automatic Control System

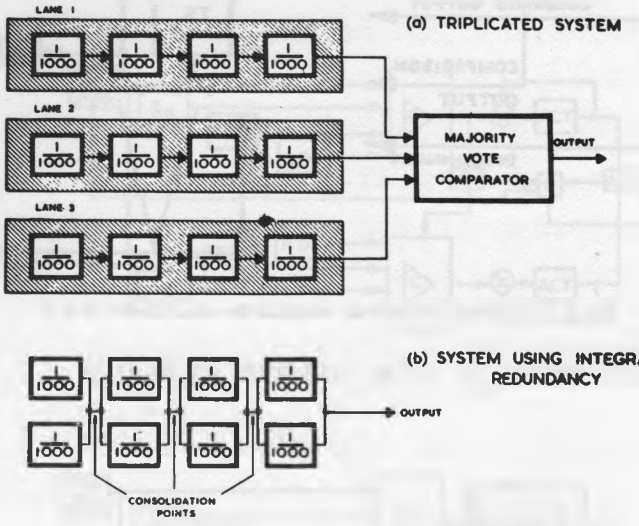


Fig.7: An Example Illustrating the Principle of Integral Redundancy

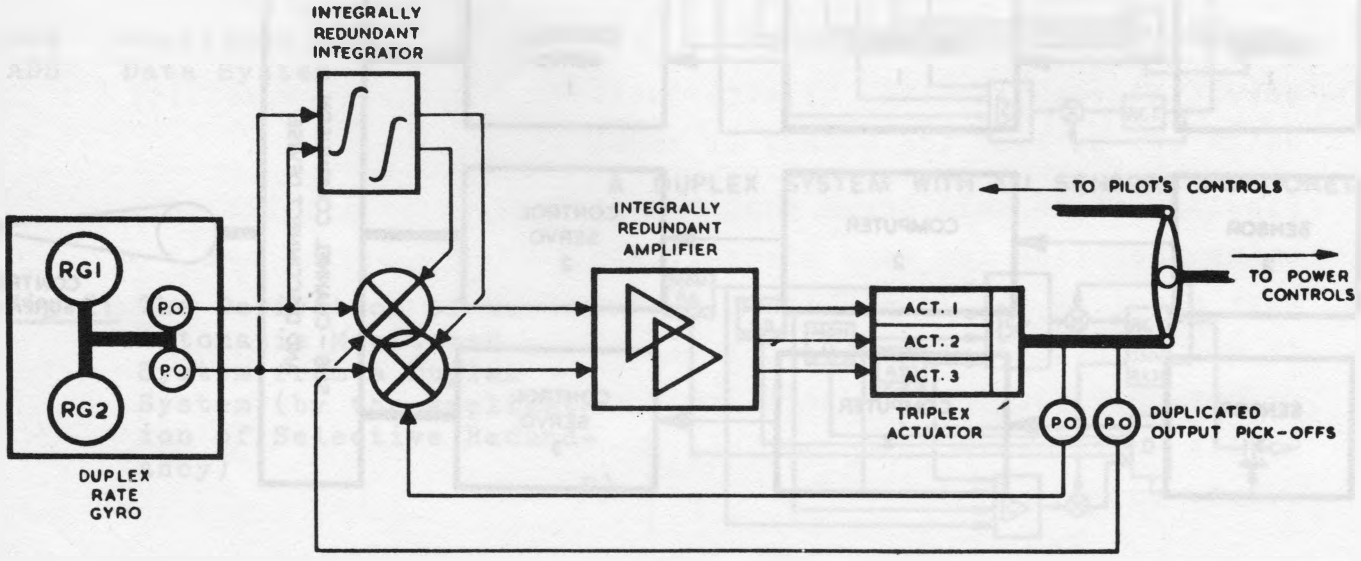


Fig.8: Rate Demand and Autostabiliser System Using Failure-Survival Integral Redundancy

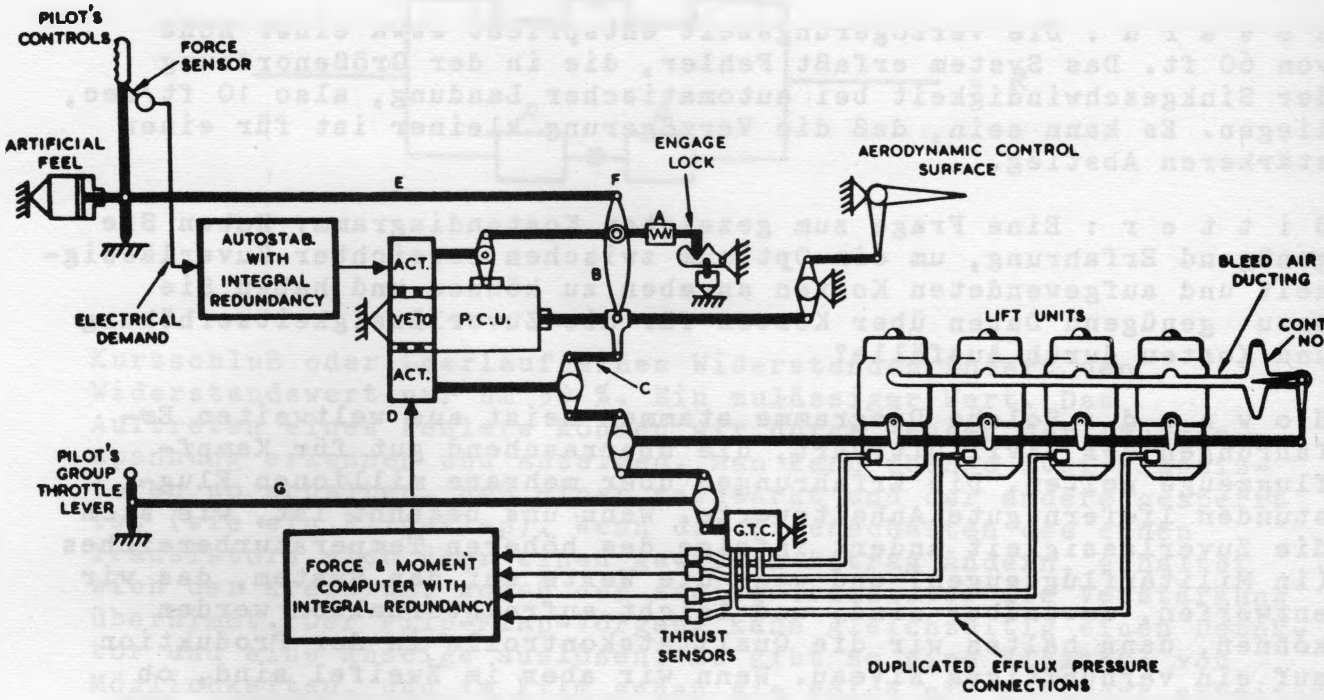


Fig.9: A Hypothetical V.T.O.L Control Arrangement

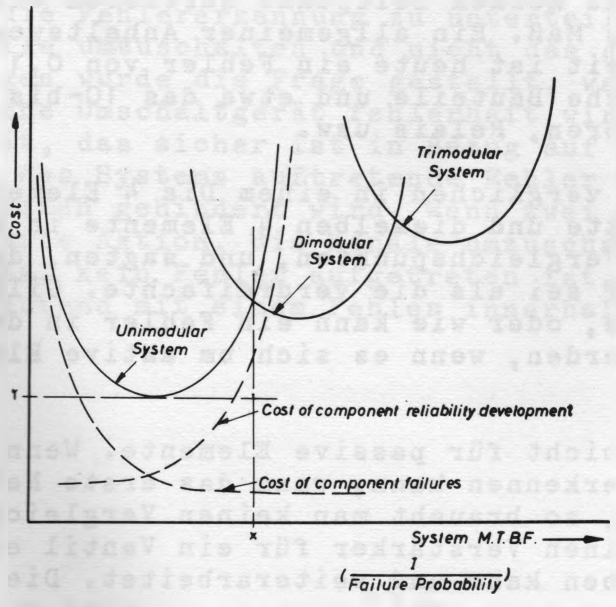


Fig.10: System Cost Optimisation

Aus der Diskussion

S c h w e i z e r : Welche Verzögerungszeit ist in dem erwähnten Radiohöhenmesser eingebaut, welche minimalen Fehler können erfaßt werden?

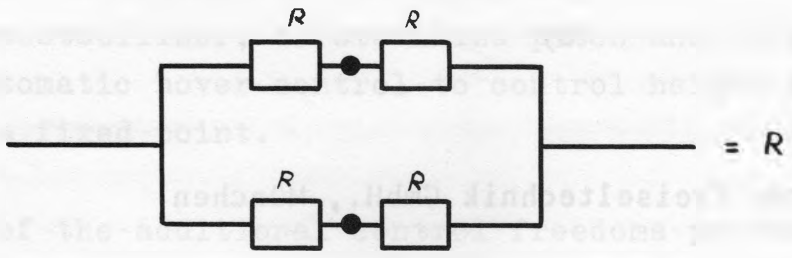
H o w a r d : Die Verzögerungszeit entspricht etwa einer Höhe von 60 ft. Das System erfaßt Fehler, die in der Größenordnung der Sinkgeschwindigkeit bei automatischer Landung, also 10 ft/sec, liegen. Es kann sein, daß die Verzögerung kleiner ist für einen stärkeren Abstieg.

B i t t e r : Eine Frage zum gezeigten Kostendiagramm: Haben Sie genügend Erfahrung, um ein Optimum zwischen erreichter Zuverlässigkeit und aufgewendeten Kosten angeben zu können und haben Sie dazu genügend Daten über Kosten für die Zuverlässigkeitserhöhung und Kosten durch Ausfälle?

H o w a r d : Solche Diagramme stammen meist aus weltweiten Erfahrungen der Zivilluftfahrt, die überraschend gut für Kampfflugzeuge gelten. Die Erfahrungen über mehrere millionen Flugstunden liefern gute Anhaltswerte. Wenn uns bekannt ist, wie sich die Zuverlässigkeit ändert infolge des höheren Temperaturbereiches (in Militärflugzeugen) und wenn die Werte auf das System, das wir entwerfen, anwendbar sind, und leicht aufrechterhalten werden können, dann halten wir die Qualitätskontrolle in der Produktion auf ein vernünftiges Niveau. Wenn wir aber im Zweifel sind, ob diese Zuverlässigkeitswerte dauernd erreicht werden können, vervielfachen wir. In einigen Fällen tun wir das innerhalb der Netzwerke. Z.B. zeigte ich im Film, daß wir jetzt in neuen Entwürfen Dünnschicht-Widerstände und Kondensatoren benutzen, die auf einer Dünnschicht-Unterlage aufgebracht sind, und wir finden, daß es nicht notwendig ist, diese Komponenten zu vervielfachen, da ihre Zuverlässigkeit sehr hoch ist. Dagegen ist es immer noch nötig, Transistoren zu vervielfachen, da uns nicht alle Ursachen für Fehler im Transistor bekannt sind. Wir können also nie positiv sagen, daß kein Fehler zu keinem Zeitpunkt auftreten wird. Die MTBF ist hier kein gutes Maß. Ein allgemeiner Anhaltswert für Komponentenzuverlässigkeit ist heute ein Fehler von 0,1 % pro 1000 Std für elektronische Bauteile und etwa das 10-bis 30-fache für Komponenten wie Motoren, Relais usw.

D i e r s t e i n : Sie verglichen in einem Dia 4 Elemente in einer verdreifachten Kette und dieselben 4 Elemente in einer verdoppelten Kette mit Vergleichspunkten, und sagten, daß die verdoppelte Kette besser sei als die verdreifachte. Gilt das nur für passive Elemente, oder wie kann ein Fehler in den Vergleichspunkten erfaßt werden, wenn es sich um aktive Elemente handelt?

H o w a r d : Das gilt nicht für passive Elemente. Wenn man z.B. zwei Netzwerke hat und erkennen kann, wann das erste Netzwerk fehlerhaft geworden ist, so braucht man keinen Vergleich. Beispielsweise haben wir einen Verstärker für ein Ventil entworfen, der jeden Fehler überleben kann und weiterarbeitet. Die passiven Elemente in diesem System sind sehr einfach. Es sind Widerstände in Parallel-Reihenschaltung.



Kurzschluß oder Leerlauf eines Widerstandes ändert den Widerstandswert nur um 50 %. Ein zulässiger Wert. Das Auftreten eines Fehlers können wir durch Messen der Brückenspannung erkennen und anzeigen. Man kann ebenso zwei Transistoren so schalten, daß einer verstärkt und der andere gesperrt ist (wie ein Flip-Flap). Wenn die Eigenschaften des einen Transistors sich über einen gewissen Betrag ändern, schaltet sich der Kreis um, sodaß der zweite Transistor die Verstärkung übernimmt. Der Flip-Flap-Vorgang kann gleichzeitig einen Detektor und eine Anzeige auslösen. Es gibt so eine Vielzahl von Möglichkeiten, und im Film sahen sie solch ein Netzwerk arbeiten.

P f a f f: Welche Umschaltzeiten ergeben sich beim Umschalten vom Haupt- zum Standby-Kanal?

H o w a r d: Dieses Reglersystem wird in der VC 10 eingesetzt. In der VC 10 hängt es von der Art des Fehlers und seiner Wichtigkeit ab, welche Umschaltzeit benötigt wird, sodaß diese zwischen 0,1 sec und 1,2 sec variiert. Wie Sie in Ihrem Dia zeigten, wo einzelnen Elementen jeweils ein Monitor beigeordnet war, ist es möglich, die Fehlererkennung zu unterteilen und nur die fehlerhaften Teile umzuschalten und nicht das gesamte System. Heute morgen wurde die Frage gestellt, was passiert, wenn das automatische Umschaltgerät fehlerhaft wird. Wir haben ein Umschaltgerät, das sicher ist in Bezug auf eigene Fehler. Jeder innerhalb des Systems auftretende Fehler bewirkt, daß es am Weiterarbeiten gehindert wird. Wenn zwei Fehler auftreten ist seine nächste Aktion, die Kanäle umzuschalten, selbst wenn im ersten Kanal kein Fehler aufgetreten ist. Wir sagen, daß dies gleichbedeutend mit einem Fehler innerhalb des Systems ist.