SEVENTH EUROPEAN ROTORCRAFT AND POWERED LIFT AIRCRAFT FORUM

Paper No. 57

A REDUNDANCY CONCEPT

FOR A DIGITAL CSAS

P.Wüst, M.Keller

Bodenseewerk Gerätetechnik GmbH
Überlingen

September 8 - 11, 1981

Garmisch-Partenkirchen
Federal Republic of Germany

Deutsche Gesellschaft für Luft- und Raumfahrt e.V.
Goethestr. 1o, D-5ooo Köln 51, F.R.G.

A REDUNDANCY CONCEPT
FOR A DIGITAL CSAS

P.Wüst, M.Keller
Bodenseewerk Gerätetechnik GmbH
Überlingen

Abstract

The state of the art concerning guidance and control systems for helicopters, fixed wing aircraft and turbofan engines is characterized by replacing analog by digital systems.

One of the promises of digital technology is the possibility of implementing more intelligent monitoring techniques - for example self monitoring methods. However self monitoring procedures are only reluctantly accepted. As we believe, one of the main reasons for this is, that there is not yet enough operational experience with these methods.

That's why we try to give an impression of typical redundancy- and monitoring concepts, which have been realized in aircraft, helicopter and engine control systems.

Finally the paper describes in more detail a system which was originally not designed for a helicopter application but which shows all characteristics of a CSAS.

The system is based on two essentially autonomous computing lanes, each able to provide all the necessary control and monitoring functions. Additionally it is shown how the system works and how its effectiveness has been analyzed.

1. Introduction

For control systems in the civil and military aviation various means are provided to increase the safety of the system. These means are either of a passive nature (e. g. fail-safe behaviour by limiting the control system authority) or of an active nature (e. g. parallel redundancy) or a mixture of both.

The safety concept, which has a great influence on the amount of hardware depends

- o on the type of mission to be performed
- o on the operational conditions
- o on the concept of the primary flight control system
- o on the budget
- o on the degree of confidence in the reliability of the technology to be used.

As far as safety critical systems are concerned, we are in a phase of transition from analog to digital signal processing. The possibilities offered by digital signal processing will effect that advanced control systems will increasingly be used in helicopters.

Figure 1 shows the yaw-axis of the tank-attack-helicopter PAH-1 as an example of a typical helicopter CSAS and a control-demand-system for inertial velocities is given on figure 2 as an example for a future concept.

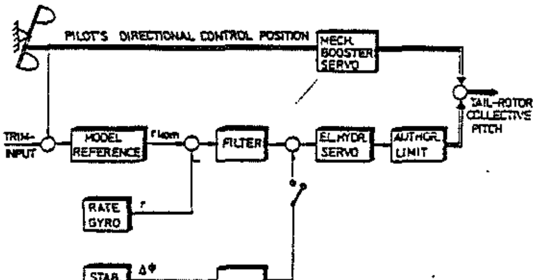


Fig.1: Typical Helicopter CSAS
PAH1-YAW-AXIS

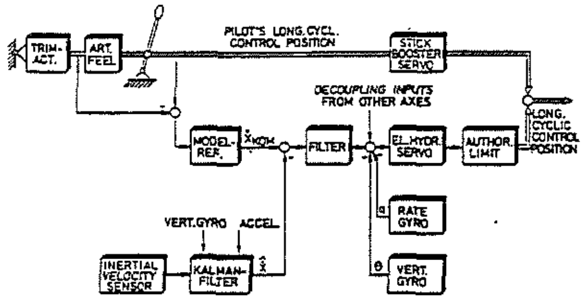


Fig.2: Advanced Helicopter (Hover) Control System - Pitch Axis

2. Definition of Command and Stability Augmentation Systems.

Command and Stability Augmentation Systems (CSAS) are used in almost each sector of aviation (fixed wing aircraft, helicopters, turbine engines) where

- o the inherent handling qualities are not satisfactory (the dynamic behaviour varies greatly as a function of flight condition and aircraft configuration, e. g. insufficient damping of the characteristic motions etc.)
- o the performance of critical missions without a control system would lead to increased pilot work load in case of external disturbances (e. g. turbulence)
- o the limits of a safe operation must continuously be monitored in order to avoid overloading (e. g. monitoring of the load factor, rotational speeds, temperatures etc.)

3. Why digital?

The perspectives of digital technology are

- o increased reliability by reducing the number of "black boxes" (provided the specification is identical)
- o a principally better testability and therefore an improved maintainability i. e. reduced life cycle costs.

In the following some examples are given on the statement "better testability".

- o Due to the practically unlimited number of possible test points, a digital system can be tested more extensively, thus improving the transparency of the system.
- o Tests of analog systems must run off continuously. Tests in a digital system can be nested.
  The majority of tests of a digital system concentrate on the test of the CPU, memory etc. without the need to test the (control)-function.
  The hardware of analog systems can only be tested by its function.

As an example, if the system comprises a filter with a great time constant, the test will last for a considerable amount of time. This may be a problem if there is little time left for the preflight-check.

Inspite of the enthusiasm for digital processing methods, one should not forget possible disadvantages. For example digital control systems may show a smaller stability margin than comparable analog control systems due to the finite computing speed of installed processors and by the resulting computer dead-time. This applies specially for control systems which are characterized by a high loop gain.

4. Survey of redundancy concepts of operational systems.

Besides the system performance the safety aspect plays a very important role in the design of a CSAS.

In order to achieve a specified reliability, redundancy is often necessary. As the redundancy concept has a great influence on the following system characteristics

- o weight/volume
- o power consumption
- o price
- o cost of maintenance and logistics

it obviously is of considerable importance.

When designing a safety critical flight control system, it is often helpful to know which solutions were chosen in similar cases. For this reason the redundancy concepts of different modern control systems are described in the following.

4.1 Fighter aircraft

TORNADO

The CSAS for the TORNADO is a triplex analog system. When it was developed, the required digital technology was not available. However it is already a Fly-By-Wire (FBW)-System but still with a mechanical back-up for the differential taileron. The requirement concerning the probability of a fatal failure is 10^{-8} per hour for the total CSAS, sensors included but with the exception of the actuators.

Fatal failure in that context means the system cannot switch to the mechanical back-up after a detected second failure. Figure 3 shows the LATERAL CSAS.

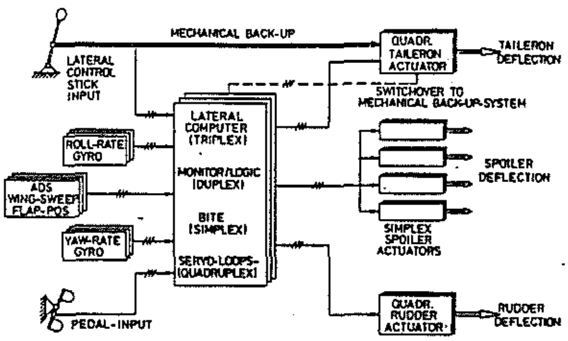


Fig. 3: TORNADO FULL AUTHORITY LATERAL CSAS

MIRAGE 2000

The MIRAGE 2000 is neutrally stable in clean configuration and slightly unstable in the pitch axis with external loads.

This aircraft has no longer a mechanical back-up. But it has an analog quadruplex system for the pitch axis and a triplex system for the roll- and yaw axes.

F16

The F16 is characterized by reduced static longitudinal stability. This aircraft has no mechanical back-up but an analog quadruplex CSAS.

F18

The F18, which is able to perform carrier landings, has a digital quadruplex FBW control system and additionally a mechanical back-up for the differential tail.

SAAB JA37 VIGGEN

As shown in figure 4 the digital Automatic Flight Control System (AFCS) is a system with a high but limited authority (25 %). But in spite of the authority limitation, the high band-width servos can command up to 1o g nose up or down in the most critical flight conditions, if they fail hardover and if the failure is not detected and isolated within a very short time. The requirement concerning the probability of a fatal failure was 10^{-6} in 1.5 hours (i.e. $7 \cdot 10^{-7}$ in one hour).

Rig- and flight tests started with dual comparison monitored digital computers but the series system uses a single computer only.

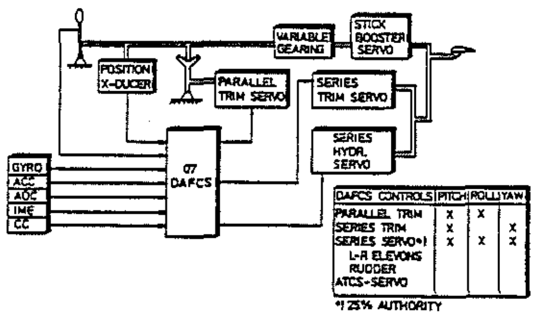


Fig. 4: SAAB VIGGEN JA-37 HIGH AUTHORITY DAFCS

4.2 Helicopters

PAH-1 (BO 105)

The CSAS for the yaw axis of the PAH-1 (see fig. 1) is a single channel analog system. Thus it is the most simple safety concept, which is adequate for the given case of application. The limitation of the control-system-authority does not impose any restrictions.

CH-53E

The AFCS (conventional inner loop stabilization, hover augmentation, force feel and outer loop stabilization) for a completely different type of helicopter has an essential property in common with the control system for the PAH-1: the limited authority. As weight problems do not play the same roll as in the case of a light antitank helicopter, it was certainly easier to decide in favor of active safety. The result is a dual channel digital system, in which self-test-methods are used extensively.

4.3 Civil Aircraft

AIRBUS A-310

The most stringent safety requirements on flight control/guidance systems for civil aircraft apply to the AUTOLAND-mode. An automatic landing under CAT III A conditions means to land at zero decision height. The hazard criteria (probability of a fatal failure) is 10^{-9} for the time period of this critical phase (3o sec). This probability is equivalent to about 10^{-7} in one hour.

In order to meet this requirement a duo-duplex solution has been chosen for the FCC (Flight Control Computer) as the most important subsystem of the digital AFCS.

DC-9-80

The integrated digital flight guidance system for the DC-9-80 aircraft does achieve this objective using only two computers, each having fail-passive properties for the critical functions. This is obtained by extensive use of selftesting, partial redundancy (dual RAM) and time redundancy (redundant computation).

4.4 Engine control

TORNADO

The control system for one multispool engine (RB 199) of the TORNADO shows all characteristics of a CSAS (improvement of handling qualities, monitoring of critical parameters etc.)

Pilot commands are transmitted by electrical signals only. There is no mechanical back-up. Each of the two engines has its own MECU (Main Engine Control Unit), which is an analog dual channel system.

4.5 Conclusion

The above description of redundancy concepts for flight- and engine control systems shows that due to different operational conditions and requirements, all types of safety systems are existing. They range from the analog single channel system with limited authority in case of the PAH-1 to the digital quadruplex system with mechanical back-up in case of the F18. However, the following general conclusions can be drawn:

- FBW-Systems are at least triplex (if a mechanical back-up is available) or quadruplex (if a mechanical back-up is not available).
- When analog systems are replaced by digital ones, it is intended to reduce the degree of redundancy (and therefore the amount of hardware and cost of maintenance and logistics) by use of

self monitoring procedures.

The digital AFCS for the DC-9-80 aircraft is a typical example, where only a dual system is used for critical phases such as AUTOLAND under Cat. III A conditions. Analog systems for this purpose were formerly triplex (AFCS for the TRIDENT aircraft) or duo-duplex (Airbus A300).

Civil aircraft do not (yet) have FBW-systems, but the mechanical control is practically not useful in case of a critical AFCS-Failure under the conditions of a CAT III-A approach (zero decision height).

However, even SAAB doubts, whether the future reduction of the degree of computer redundancy will go as far as with the digital AFCS for the SAAB JA-37 VIGGEN (single computer). Concerning the amount of hardware, cost of maintenance and logistics, a single-channel-system is the most preferable. The cost of verifying the required reliability however may be very high. This and the limited operational experience with self-monitoring-techniques are the reasons, why at present purely parallel redundancy is still more "believable". In case of competing proposals for a safety critical application the designer of a system using selftest-techniques is in general in a weaker position.

5. The Digital System

After the more general comments concerning redundancy concepts, a realized system will now be described in more detail.

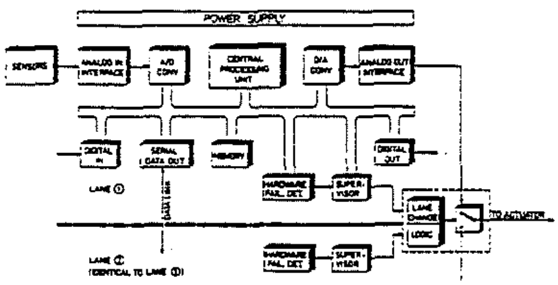


Fig. 5: BLOCK DIAGRAM OF THE DIGITAL CONTROL UNIT

The dual-channel system, whose structure is given in Fig. 5, was designed in cooperation with MTU-München as a control system for a turbine engine. The specification of the system is that of a typical CSAS:

- o typical CSAS functions (improvement of handling qualities, monitoring of critical parameters etc)
- o Sampling frequency ~ 25 Hz
- o MTBCD of one signal processing unit > 3000 hrs
- o probability of a critical failure (loss of control) caused by the digital signal processing electronics (including interface)

  $< 10^{-6}$ per hour
- o temperature range according to MIL-standard.

With a similar specification, we would develop a digital CSAS for a helicopter in the same way. One characteristic of the described system is that no mechanical back-up is available to transmit the pilot commands (throttle lever) to the "actuator" (fuel control unit). The use of FBW-technology with a dual channel system is possible because the TORNADO has two engines with separate control systems. This has concequences for the selection of appropriate monitoring schemes. The choice would be somewhat different if a mechanical back-up is available, as with the presently operational helicopters.

For monitoring purposes the selftest capability of digital computers is used extensively.

One channel is active, the other is on stand-by. After a first failure in the active channel, the second channel is in command. At the moment the crosstalk between the two channels is limited to the updating of the integrators of the standby channel (in order to minimize transients during lane change).

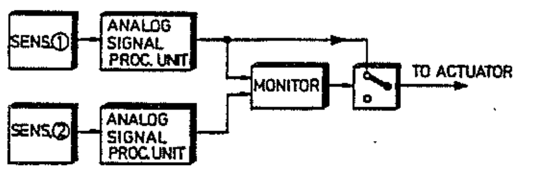
Thus both computers practically work in an asynchronous manner.

We are presently expanding the crosstalk to exchange sensor data and the accompanying validity information (derived by selftests). This will help to keep the system available in case of a sensor failure in the second channel by using "good" sensor data of the nonactive channel in the second channel (reconfiguration).

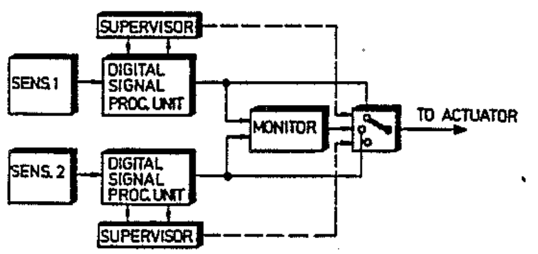
5.1 Reasons for the selection of a dual channel system

Using parallel redundancy only one should have had to use a triplex system in order to cope with the given reliability requirements. The decision for a dual-channel system with its less amount of hardware became attractive only because of the capability of digital computers to perform selftests.

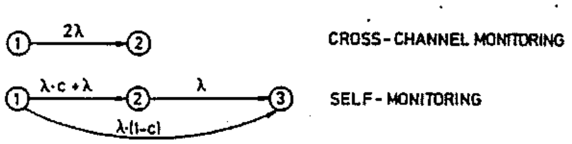
This will be explained in the following



ANALOG DUAL CHANNEL SYSTEM WITH CROSS CHANNEL MONITORING



DIGITAL DUAL CHANNEL SYSTEM WITH SELF-AND CROSS CHANNEL MONITORING



SIMPLIFIED STATE TRANSITION-DIAGRAMS FOR A DUAL-SYSTEM

Fig 6: COMPARISON OF DUAL CHANNEL SYSTEMS

A dual system with cross-channel monitoring only had to be switched off after the first failure. In the self-monitored digital system the first failure is detected and isolated with a certain probability C. The critical transition is characterized by a transition rate $\lambda\cdot(1-C)$, which decreases with increasing failure detection probability as shown in the state transition diagram.

To show the differences more clearly, the transition, which is caused by the critical lane change failure, was omitted because it influences both systems in the same manner.

5.2 Monitoring procedures

The monitoring procedures play an essential roll for the described dual channel system. The use of various independent procedures (hardware/ software) has proven very favorable (see Fig. 7).

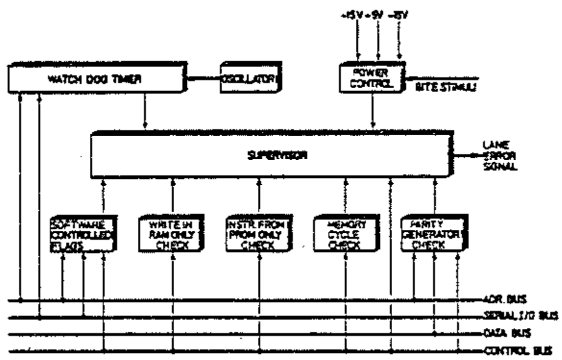


Fig. 7: SAFETY SYSTEM BLOCK DIAGRAM

The term coverage factor is of special importance in that context.

This coverage factor C is defined as a conditional probability that after a failure has occurred, this failure is detected and isolated (i.e. the system continues to be available)

$$C = P\,(\text{failure detected/failure occurred}) = \frac{P\,(\text{failure occurred and detected})}{P\,(\text{failure occurred})}$$

With P (failure occurred) = $\lambda \cdot \Delta t$
assuming an initially faultfree system, the probability that a failure occurred and is detected is

$$P_{FD} = \lambda \cdot \Delta t \cdot C$$

or the complement (failure occurred and not detected)

$$P_{F.ND} = \lambda \cdot \Delta t \cdot (1-C)$$

The probability, that a failure passes the barriers of different monitoring schemes (characterized by their failure detection probabilities C_1, C_2 etc.) is therefore

$$P_{FND} = \lambda \cdot \Delta t \cdot (1-C_1) \cdot (1-C_2) \cdots$$

This means for instance that two monitoring procedures with 90 % failure detection probability each will detect the failure with 99 % due to different failure consequences.

5.2.1 Discussion of monitoring procedures

All subsystems of a system have to be monitored:

- o actuators
- o sensors
- o signal processing electronics.

The procedures to monitor sensors and actuators are the same as used in flight control. They will be explained therefore by means of flight control examples.

Monitoring of actuators

Redundant actuators do often haven their own monitoring logics. If the degree of actuator redundancy is lower than that of the system analytical redundancy is applied in form of a model (image) of the actuator dynamics. Fig. 8 shows an example of that kind of redundancy (monitoring of the Autothrottle (ATH) actuator of the AIRBUS A 300).

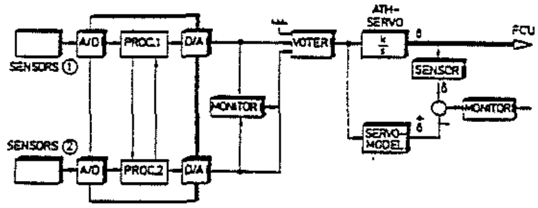


Fig. 8: AIRBUS A 300 ATH-SERVO MON. CONCEPT

Monitoring of sensors

For the monitoring of sensors analytical redundancy can be used in a similar way. The basis of analytical redundancy is always a mathematical model. This will be shown in the following:

Example 1:

In order to monitor rate sensors with the information from vertical and directional gyros, the relationship between angular rates and time derivatives of Euler-angles is used.

Example 2:

The diagram given in fig. 9 shows the monitoring of signals of a Doppler Navigation System (inertial velocities).

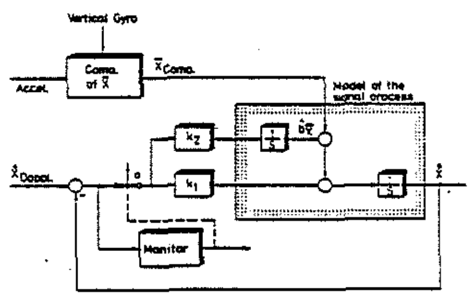


Fig. 9: MONITORING CONCEPT USING A KALMANFILTER

The relationship between acceleration and velocity is used as a model. The difference between the noisy measurement of the Doppler velocity and the estimated inertial velocity is monitored. This difference (residue) is also used to update the model. This process represents a simple Kalman-Filter with constant gains which estimates a practically unavoidable accelerometer bias in addition to the ground speed components.

This Kalman-Filter with the model equations

$$\ddot{X} = b_{xf} + \theta\cdot\{\sin\phi\cdot b_{yf}+\cos\phi\cdot b_{zf}\}$$
$$\ddot{Y} = \{\cos\phi\cdot b_{yf}-\sin\phi\cdot b_{zf}\}$$
$$\ddot{Z} = -\theta\cdot b_{xf} + \{\sin\phi\cdot b_{yf}+\cos\phi\cdot b_{zf}\}$$

ϕ, θ : roll angle, pitch angle
b_{xf}, b_{yf}, b_{zf}: signals of body axis accelerometers

and the resulting transfer functions (example)

$$\hat{\dot{X}} = \frac{[1+\frac{k_1}{k_2}s]}{[1+\frac{k_1}{k_2}s+\frac{1}{k_2}s^2]}\cdot\dot{X}_{DO} + \frac{\frac{1}{k_2}\cdot s}{[1+\frac{k_1}{k_2}s+\frac{1}{k_2}s^2]}\cdot\ddot{X}$$

has in consequence a double function:

Filtering and monitoring of the Doppler-signal. A compromise has to be made therefore. The gains k_1 and k_2 have to be chosen so that the filter states will not be updated too fast with the possible failure. This will allow for sufficient time for failure detection.

Example 3:

In a broad sense model concepts are also the basis for sensor monitoring by so-called plausbility tests:

- Comparison of the sensor signals with the extreme values possible for a given application.
- Comparison of the rate of change of the signals with possible extreme values.

Exceeding of the extreme values is interpreted as a sensor failure.

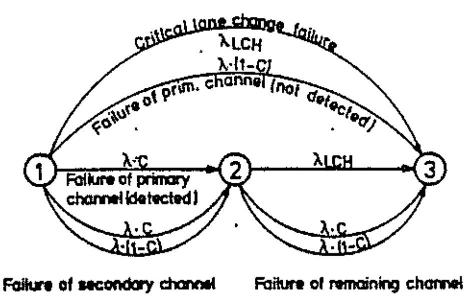
<u>Monitoring of the signal processing electronics</u>

Table 1 shows the different monitoring schemes (Built-In-Test). The table identifies the type of test and whether it is implemented by hardware or software and whether the specific test is performed during the preflight- or in-flight test.

6. Safety Analysis

As an example the safety analysis approach is explained for the computer unit (digital processing unit including data acquisition system, interface and lane change logic). The safety analysis of the complete system includes, of course, sensors and actuators. However, these subsystems are specific to the turbine application and are therefore excluded in the present paper.

As mentioned previously the system described here uses exclusively self-monitoring methods. The critical failures are those, which will not be detected respectively those failures of the lane change logic resulting in an undefined state of the system. Both types of failures will result in loss of control. Failure combinations can be neglected compared with these critical failures (see Fig. 1o).



State 1: System intact, no failures
State 2: One channel failed, system available
State 3: System defect, (loss of control)

$$P_3 \cong \Delta t\cdot\{\lambda\cdot(1-C)+\lambda_{LCH}\} + \frac{\Delta t^2}{2}\cdot\{C\cdot(3\lambda^2+2\lambda\cdot\lambda_{LCH})-(\lambda+\lambda_{LCH})^2\}$$

λ = Channel failure rate
C = Effective probability of detection (coverage factor)
λ_{LCH} = Rate of critical lane change failure

Fig 1o.: STATE TRANSITION DIAGRAM

Table 1: <u>BUILT-IN-TEST SUMMARY</u>

BUILT-IN-TEST-NAME	Description	IFL BIT	PFL BIT	REAL
INPUT RANGE LIMIT CHECK	Plausibility Test	X	X	S
INPUT RATE OF CHANGE LIMIT CHECK	Plausibility Test	X		S
ANALYTIC REDUNDANCY	Comparison with Model Variables	X		S
WRITE-IN-RAM-ONLY CHECK	Detection of erroneous Program Branching	X	X	H
INSTRUCTION FROM ROM-ONLY CHECK	Detection of erroneous Program Branching	X	X	H
UNUSED OP-CODE	Code-Verifier Check	X	X	H
PARITY-BIT	Data Transfer Test Memory-Test (RAM+PROM)	X	X	H
PROM-TEST	Memory Sumcheck	X	X	S
RAM-TEST	Read-Write Memory-Test	X	X	S
COMPUTER CYCLE-TIME	Proc. to Memory Access Time Test	X	X	H
WATCH-DOG TIMER	Protection against CPU/ Memory failures	X	X	H
WRAP-AROUND	Interface-Test CPU Arithmetic Test	X	X	H
CPU-TEST	Test of Instructions, address-modes, address-logic, arithmetic, etc.	X	X	S
INJECTED INPUT TEST	Test of Sensor Interface Test of Supervisor/Lane Change Logic		X	S,H
POWER SUPPLY TEST		X	X	H
CROSSTALK-DATA-LINK CHECK		X	X	S

IFL = Inflight

PFL = Preflight

H = Hardware

S = Software

The safety analysis approach (Failure Modes and Effect Analysis FMEA) was as follows:

- o Subdivision of the computer into functional groups - assignment of a failure rate λ
- o Determination of the independent failure consequence (j) of a defect in the functional group (i) and assignment of a failure rate λij. Caused by the nature of the sequential data processing a failure consequence (FC) can be combined by several elementary failure consequences (EFC) occurring quasi-simultaneously.
- o Calculation of the probability P_{ND} representing the occurrence of a failure in the functional group i with the consequence j which is not detected by any of the monitoring procedures

$$P_{ND}(ij) = \lambda ij \cdot \Delta t \cdot \prod_{\ell=1}^{m} (1 - c_{j\ell})$$

where

$c_{k,1}$ = detection probability (coverage factor) of FCj by the number 1-monitor

m = total number of monitoring procedures

If a failure consequence comprises several elementary failure consequences the following formula is valid:

$$P_{ND}(ij) = \lambda ij \cdot \Delta t \cdot \prod_{k=1}^{n} \cdot \prod_{\ell=1}^{m} (1 - c_{k,\ell})$$

where

$c_{k,1}$ = detection probability of EFC k by the number 1-monitor

m = total number of monitoring procedures

n = total number of elementary failure consequences representing failure consequence j

The summation of these individual probabilities over all failure consequences and functional groups results in the desired probability of a critical failure passing the barriers of the different monitor schemes.

A total number of 38 subgroups and 29 different failure consequences have been investigated. In many cases it was simple to decide, which monitoring scheme would detect which failure consequence (coverage factor 0 or 1).

In other cases experience with other systems was considered or estimations were performed on a statistical basis.

The assumptions concerning the division into system subgroups, estimation of the individual coverage factors etc. have been varied both optimistically and pessimistically. The resulting bandwidth for the probability of a critical failure for a 1 hour mission was

$$0.2 \cdot 10^{-6} < P_{ND} < 0.8 \cdot 10^{-6}$$

The failure rate of one channel electronic signal processing unit incl. interface (computing section) was

$$\lambda \approx 94 \cdot 10^{-6}/\text{hour}$$

The signal processing unit comprises a TI IIL 9900 CPU, 1 k RAM and 7 k PROM

Using highly integrated circuits this approach is at present the only feasible way due to the fact, that the information on failure physics or failure statistics given by the manufacturers is limited. In case of the automatic control systems of the SAAB JA-37 VIGGEN and the DC-9-80 even more detailed FMEAs were performed, partially using logic simulation. This was possible, because the manufacturers did use CPUs of their own development.

7. Conclusion

A comparative survey of redundancy concepts of operational safety critical control systems for aircraft, helicopters and turbine engines has shown that the present trend from analog to digital systems moves from the application of exclusively parallel redundancy to a combination of a reduced degree of parallel redundancy and selfmonitoring techniques. This is possible by making full use of the capabilities of digital signal processors.

The reasons for this trend are obvious:

- Reduction of the amount of hardware and therefore cost reductions for maintenance and logistics
- Savings of weight/volume and power consumption

Due to the special characteristics and operational conditions, these objectives are valid specially for helicopters.

At the present state of digital technology and of selfmonitoring techniques as well as of the procedures to verify the safety of a system (FMEAs), dual channel systems were realized with a probability of about 10^{-6} for the loss of control for a one hour mission.

This seems to be a feasible concept for the present helicopter generation, which is still equipped with mechanical controls. It is necessary to become more familiar with self-monitored systems and further experience must be obtained.

However, it is evident, that saving of hardware is paid with an increased expense to verify and demonstrate the safety of such systems. But this fact should not be discouraging. The use of self-monitoring techniques is a valuable supplement of the means to increase safety and to decrease the amount of hardware for flight control systems.

References

1. K.Folkesson
   Failure Management for the SAAB VIGGEN JA-37 AIRCRAFT AGARD-LS-1o9 (198o) Fault Tolerance Design and Redundancy Management Techniques 7-1/7-21

2. R.D.Murphy
   CH-53E Digital Automatic Flight Control System; INKA Conf.78-255-oo8 (1978)

3. S.Osder
   The DC-9-80 Digital Flight Guidance Systems Monitoring Techniques; INKA Conf.79-366-oo8 (1979)

4. E.Aiken, R.Merrill
   Results of a Simulator Investigation of Control System and Display-Variations for an Attack Helicopter Mission.
   36th Annual Forum of the American Helicopter Society Washington, May 1980
   Reprint No. 8o-28