Fault Detection and Diagnosis in Aerospace Systems using Analytical Redundancy

Patton R.J. *

Summary: Performance requirements in aeronautics and the rapid growth of electronics, especially of digital computers, have gradually led to the combination of advanced control theories and fly-by-wire technology. This has resulted in designs for which the control systems are flight-critical. The required reliability is usually achieved by a multiplication of sensors, computers and actuators accompanied by a voting system. The on-board computer provides the possibility of replacing the sensor hardware replication, which is very expensive, with a management of the functional or analytical redundancy constituted by the knowledge of the system. Different techniques have been proposed; the aim of this article is to outline an review the state of the art and describe some of the studies of analytical methods of fault diagnosis procedures, based on fault monitoring in aircraft and spacecraft sensor systems.

1 Introduction

1.1 Problem statement and definitions

A fault is an unexpected change in a system, such as a component malfunction and variations in operating condition, that tend to degrade overall system performance.

We use the term "fault" rather than failure to denote a malfunction rather than a catastrophe. The term failure suggests complete breakdown, whilst a fault may denote something tolerable.

- **Why do we need fault detection?**
  - Early indication of incipient faults can help avoid major plant breakdowns and catastrophes
  - Fault detection and isolation has become a critical issue in the operation of high-integrity and fault-tolerant systems, such as used in aerospace applications.
- **Tasks of fault diagnosis**
  - Fault detection, i.e., the indication that something is going wrong in the system
  - Fault isolation, i.e., the determination of the exact location of the fault
  - Fault identification, i.e., the determination of the size and type or nature of the fault
  - Fault accommodation, i.e., the reconfiguration of the system using healthy components

We focus attention on the area of *fault detection and isolation* (FDI) methods which make use of analytical redundancy.

* **Senior Lecturer, Department of Electronics,**
University of York,
Heslington,
York YO1 5DD

- **Performance index of fault detection**
  - missed alarm, i.e., monitor does not indicate fault when a fault has occurred in the system
  - false alarm, i.e., monitor indicates a fault when the system is normal
  - detection delay, which has to be monitored for a fixed false alarm rate

1.2 Safety Specifications and Goals

In civil aircraft it is usually considered that the probability per hour of a ctastrophic failure (catastrophic fault) must be less than 10^{-7}. The probability of a mission abort must be 10^{-3} to 10^{-5} per flight hour. To these specifications must be added the ability of automatic flight control systems to accommodate faults according to the following classification:

(a) **"Fail passive":** when a malfunction of fault is detected the corresponding system is disengaged. Thus the faulty system must not be essential for aircraft safety.

(b) **"Single fail operate":** one failure can be detected, isolated and corrected so that the system will continue to operate with undegraded performance. The system is then considered to be *fail passive*.

(c) **"Dual fail operate":** the system becomes fail passive after two failures.

The aircraft requirements imply the reliability of the different devices and of the sensors: traditionally, the probability per hour of a sensor failure leading to a flight catastrophe must be less than 10^{-9}. As the probability of a single sensor failure can reach 10^{-4}, the traditional approach to providing this reliability has been to use multiple independent channels with a logic selection. According to the desired probability, duplex, triplex or quadruplex systems are implemented with the corresponding probabilities $2Q_c$, $3Q_c^2$ or $4Q_c^3$, where Q_c is the fault probability of one sensor with the monitoring assumed perfect. This solution involves substantial penalties in cost, volume, weight and maintainability. Westermeier (1977) has given a comparison between triplex and quadruplex fly-by-wire digital systems: maintainability and weight are increased by 18%, and cost by 42%. Moreover, voting supposes independent faults, but can systems operating in the same environment be considered independent? The necessity for independence implies the use of *dissimilar redundancy*, which is obtained by another system with the same function as the first, but built according to different principles and technologies. For sensors the hardware redundancy presents another difficulty, the implementation of the multiple sensors on the aircraft structure.

The implementation of on-board digital computers allows the development of fault detection exploiting the use of analytical rather than hardware redundancy. Analytical (or functional) redundancy has come to be known as *fault detection and identification* (FDI) as components of a dynamic system, for example the sensors, are monitored for health and consistency, whilst specific types of malfunctions are located and identified.

All the sensors on an aircraft are related by the flight mechanics equations, which can be used in procedures for fault detection. The principle of *analytical redundancy* diagnosis is to test whether sensor outputs satisfy these known relationships. A set of sensors is healthy if an equation which relates them is verified, and one sensor of the set has failed if the relationship is violated. Analytical redundancy management appears to be a promising approach; when implemented on the on-board computer it may offer reductions in price, weight and power consumption, whilst providing a substantial increase in system redundancy and reliability. Clearly, analytical techniques have to maintain conventional system performances and reliability. Thus, in aeronautics the tendency has not been to substitute analytical redundancy for the hardware alternative, but just to suppress some levels of replication, e.g. to replace quadruplex by triplex schemes employing analytical redundancy, or triplex by duplex, etc. However, to obtain all the benefits of analytical redundancy the algorithms have to be simple enough to fit on the on-board computer and fast enough to provide safe and reliable system reconfiguration during the onset of a fault.

The fault detection must also be *robust* in order to provide its nominal performance even in the presence of parameter variations, turbulence, and the effects of manoeuvres.

The reliability requirements provide a challenge for the development of suitable fault tolerant software methods. Consequently, in recent years a new field of the development of safety-critical software has emerged, although in this article we are not concerned with this aspect.

As an example of a challenging application, consider the flight of a VSTOL aircraft hovering close to the ground. The aircraft may develop a fault in a pitch rate gyro and a total fault in the associated control loop would render the aircraft unstable with obviously disasterous consequences. If the malfunction can be detected, and the faulty gyro located and the system reconfigured - and all these operations successfully completed within about 200 msecs, then safe hovering flight can be maintained. The fault detection algorithm employed for such a scheme must thus be computationally fast. However, some analytical redundancy methods may not meet computational speed requirements, simply because of the complexity of data processing and software implementation.

1.3 Traditional approaches to fault diagnosis

- **Installation of multiple sensors** (physical, hardware or genuine redundancy):
    - Back up safety-critical hardware and software using triplex or quadruplex arrangement
    - The measure is aimed especially at detecting and isolating sensor faults. Measurements of the same variable from different sensors are compared. Any serious discrepancy is an indication of a fault in at least one sensor
- **Limit checking:**
    - Plant measurements are compared with preset limits; the exceedance of a limit can indicate a fault situation
- **Installation of special sensors:**
    - These may be limit sensors basically performance limit checking in hardware (e.g., limit temperature or pressure) or ones measuring some special variables (e.g., sound, efficiency, vibration,....)
- **Frequency spectrum analysis:**
    - Some plant measurements have a typical frequency spectrum under normal operating conditions; any deviation from this is an indication of abnormality
    - Certain types of fault may even have a characteristic signature in the spectrum that can be used for fault isolation
- **Fault dictionary approach:**
    - Every type of fault has a special characteristic behaviour in the system

- A fault dictionary contains all known "characteristic behaviours"
- We can know if a fault occurs in the system or not, through comparing the system behaviour with repertoires of faults in the fault dictionary

Clearly, an important way of achieving fault-tolerance in safety-critical control systems is by means of multiple lanes of identical hardware. Two principle disadvantages of this approach are the weight penalty paid (particularly important in flight control) and the possibility of a common-mode (design) fault of the system remaining un-detected. Tools that are applicable to *both* of these problems can be developed using *model-based* or *knowledge-based* approaches, which can also be combined with a limited use hardware redundancy to maximise the effectiveness fault isolation.

1.4 Modern approaches to fault diagnosis

- **Model-based approach** (analytical or functional redundancy): This kind of fault detection approach makes explicit use of a mathematical model of the system, often known as the "model-based" approach. The implementation of on-board digital computers allows the development of fault detection, fault isolation and fault identification exploiting the use of analytical rather than hardware redundancy.

  The following gives a more detailed treatment of this approach.

- **Combination of hardware and analytical redundancy:** At the moment, analytical redundancy cannot be used to replace hardware redundancy. The analytical redundancy can be used to suppress some levels of replications, e.g.,to replace quadruple by triplex schemes employing analytical redundancy, or triplex by duplex.

- **Knowledge-based approach:** This approach makes explicit use of the human knowledge of fault and qualitative reasoning. It provides the means of combining numeric and symbolic models for performing the FDI task.

- **A combination of all the above** (Expert system approach): For a complex system, we can combine quantitative reasoning (analytical redundancy, hardware redundancy, etc) with qualitative reasoning (knowledge-based approach) to build an expert system for diagnosing faults. The apparent success of expert system concepts in providing a limited human-like decision-making capability with a well-defined problem domain, gives strong support to their use in the fault diagnosis.

1.4.1 Model-based approaches to fault detection

(a) General structure of model-based approach

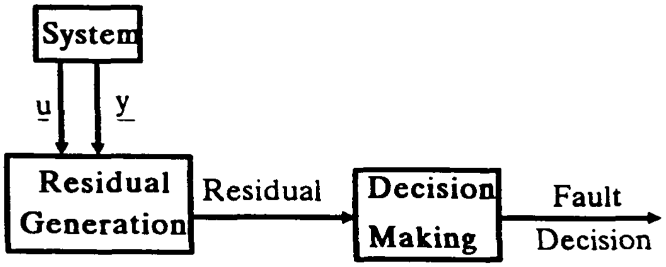


Figure 1: Two-stage structure of model-based approach

- The FDI procedure, based on analytical redundancy, consists of two stages:

  - residuals generation
  - decision making.

- Signals from system are initially processed to enhance the effect of a fault (if present) - so that it can be recognized.
- The processed measurements are called residuals, and the enhanced effect of the fault on the residuals is called the signature of the fault.
- Intuitively, the residuals represent the difference between various functions of the observed sensor outputs and the expected values of these functions in the normal (no-fail) mode.
- In the absence of a fault, residuals should be unbiased, showing agreement between observed and expected normal behaviour of the system; a fault signature typically takes the form of residual bias which is characteristic of a typical fault.
- Thus, residual generation is based on knowledge of the normal behaviour of the system.

(b) General structure of residual generation

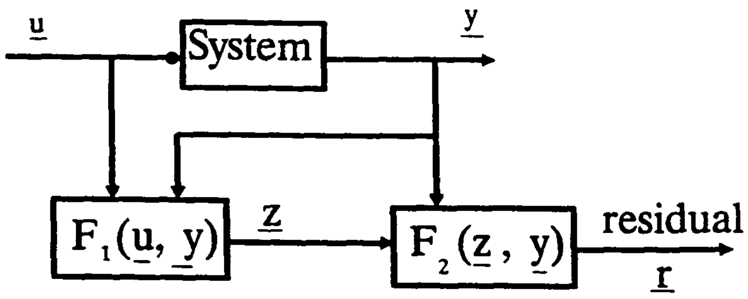


Figure 2: Mechanism of residual generation

The generation of the residuals $\underline{r}$ may be summarized as in the diagram of Fig.2. $\underline{u}$ and $\underline{y}$ are inputs and outputs of the system. $F_1(\underline{u}, \underline{y})$ and $F_2(\underline{z}, \underline{y})$ are operators (or systems), which are used to process the input and output data and provide the characteristic variables of the system. $\underline{z}$ is an estimate of the characteristic variable of the system.

2 Analytical redundancy in aerospace systems

The development of such techniques presupposes an analysis of the analytical redundancy constituted by all the knowledge of the system, together with the definition of detection filters that generate the error signals, and the monitoring of these signals. The analytical redundancy on an aircraft is provided by the mathematical model, the disturbance statistics, and the characteristics of the sensors and of their likely malfunctions.

2.1 Aircraft Modelling

The relationships between the different outputs are obtained by writing the classical rigid body flight mechanics equations, which are of two main types:

(a) Translational and rotational dynamics that relate inertial to aerodynamic forces. These depend on the aircraft, the flight conditions and the atmospheric disturbances.

(b) Translational and rotational kinematics that relate accelerations, velocities and positions. As these are only functions of the sensor implementation they are of great importance in the definition of the diagnostic filters.

These equations are all nonlinear, but some of the detection techniques, in a similar manner to the design of control systems, use linearised models derived about a particular flight condition. For an aircraft, the rigid body aerodynamics are usually well defined and the flight dynamics comprise a number of quite distinct modes. This is still true even when the dynamics have significant non-linearities, for example during a manoeuvre.

Certain decoupling structures can sometimes be assumed for fault detection design. For example, in the longitudinal motion, the *short period* mode can be represented by a pair of oscillatory poles with fast decay rate compared with the *phugoid* oscillatory mode. The separation of these modes on the complex-plane indicates that a timescale separation can be used to derive two (assumed decoupled) model sub-systems (Lipscombe, 1982). This decoupling is reasonable for the longitudinal motion of an aircraft, but is not so straightforward to apply in the case of the lateral motion as the modes are not so well separated.

In the case of modern transonic combat aircraft, the rigid body modes and flexible modes can interact, i.e. the flexible modes correspond to frequencies close to the main flight control bandwidths. For such cases, the simple modal decoupling approximations cannot be made so easily and higher order dynamic model information must be assumed essential.

2.2 Sensor analytical redundancy

Even after taking into account the sensor reduction obtained by control law modification and integration of the various avionic systems, a large number of on-board sensors often remain. The usual equipment includes acclerometers, gyros, rate gyros and a Mach meter, as well as more complex sensors such as inertial systems that deliver related outputs. Most of these sensors have a bandwidth greater than 10Hz and their dynamics can be neglected in the system model.

In contrast to this, even low frequency measurement noises should have an important part to play in the choice of fault monitor characteristics and in the choice of monitoring thresholds. These signals typically include electrical noises and errors such as bias and scale factor errors which are considered normal or admissible for satisfactory aircraft control.

To be able to detect sensor faults reliably it is clear that some form of redundancy is needed in the sensor set.

A sensor will be declared to have failed or to be faulty if it is operating outside its manufactured tolerances, and very often a failed sensor will only differ from a normal one by the size of the errors. Among the various faults considered there are: zero output, hardover bias faults and scale factor error. In addition drift faults, uncharacteristic dead-space, saturated outputs (stuck faults) and changes in noise level can all be included as malfunctions. These appear with different probabilities, zero output and biases being the most frequent. Since on aircraft systems any fault is possible, it seems unrealistic to use these statistics for fault detection.

All this *a priori* knowledge of the aircraft and its sensors constitutes the analytical redundancy, which may be classified in three main categories to which different fault monitors can be assigned.

(a) **Direct redundancy** in the case of parallel identical systems or when some dependency exists among the sensor set. This can include the classical hardware redundancy as a special case.

(b) **Static redundancy** if the measurements are related by algebraic equations. The strapdown inertial system with its *skewed sensor* arrangement is a particular example of this concept: 6 properly configured accelerometers have dual fail operative capabilities, whereas a multiplex system requires 12 accelerometers.

(c) **Dynamic (or temporal) redundancy** when the measurements are related by differential or difference equations, according to the dynamical structure of the system.

On an aircraft all these types of redundancy exist and the fault detection procedure has to be adapted carefully to the specific application. The applications are, however, quite different; for example, jet engines have a large number of sensors compared with the significant dynamic order of the system, to provide measurements of blade and gas temperatures, compressor speed sensing and pressure measurements. There is scope for a considerable number of measurements to be made. However, the engine sensor is one of the least reliable of the control system components as a consequence of its working environment. Hence, some form of sensor redundancy is necessary to achieve adequate closed-loop reliability. A typical engine has a degree of redundancy in hardware (eg duplex fuel lines, actuators and speed sensors), however some components, for example the temperature-sensing thermocouple pods, are only available in simplex configuration. The jet engine is an example for which there is a high degree of available static and dynamic redundancy. For the flight control system, on the other hand, there are rlatively fewer sensors compared with the dynamic order of the system, although the reliability of each sensor is known to be higher. These differences impose different constraints on the approach to fault and failure management using analytical redundancy.

2.3 Analytical redundancy management for large space structures

Future space missions may involve very large and highly flexible spacecraft that require active structural dynamics and control. This is a special appliction of a combination of fault management using analytical redundancy, together with special control methods. As an example of this type of problem, Wright (1981), considers a microwave radiometer over a 100 metres in diamter. Therein, many actuators and sensors were needed to meet the radiometry requirements. Montgomery and Williams (1985,1989) provide a detailed account of a study of analytical redundancy management of a large flexible grid structure situated in the laboratory at NASA Langley Research Center. In their work they demonstrate how analytical modelling techniques can be be used in a very powerful way to manage the sensors and actuators of this system.

3 Fault Detection Techniques

Fault detection techniques fall into the broad class of analytical (or functional) redundancy methods. The literature provides a large variety of diagnostic methods using analytical redundancy. There have been a number of important reviews of the subject with relevance to aerospace applications (Willsky, 1976; Walker, 1983; Gertler, 1988 ; Frank, 1989; Patton, Frank and Clark 1989). Most of the review papers include specific reference to aerospace applications of fault detection. There are, however, a substantial number of papers specifically describing flight control system and jet engine control system applications. Many of these papers, whilst based on application case studies, also provide some new insight into theoretical developments. Patton, Frank and Clark (1989) provide a table of many of the published application studies on the subject.

The main approaches of fault diagnosis are as follows.

3.1 Estimation Filter

Observation and estimation theories have provided numerous detection filters. Generally, the fault detection is obtained by a test on the difference between the outputs and the estimated outputs. Depending on the case, the outputs tested are reconstructed either from one output or from different outputs corresponding to different structures. In the simplest procedure, one of the outputs is accepted and the others estimated from it (Fig.3). This structure, proposed by Clark (1978a,b), allows the faulty sensor to be isolated with only one filter: a fault on the measurement used for the estimation produces a mis-comparison between all the outputs and their estimates, whereas a fault on any other sensor just produces a difference between its output and its estimated output. The opposite solution assigns an estimate to each output obtained from all the other measurements as shown in Fig.4. The isolation is realised by a bank of these filters.

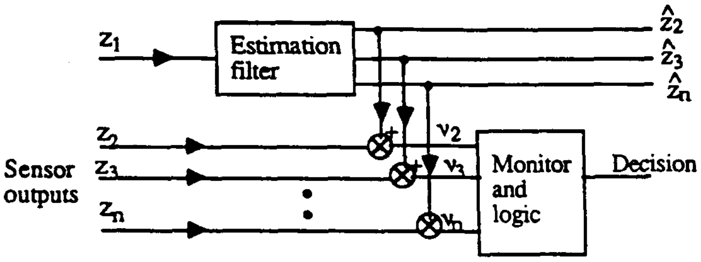


Figure 3: Estimation filter: one output is used to estimate the others

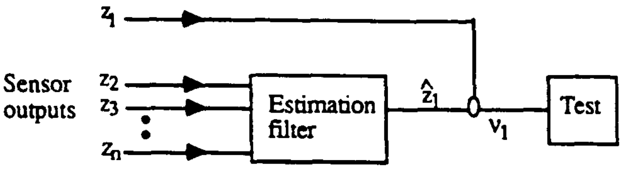


Figure 4: Estimation filter: each output receives an estimate obtained from all the other measurements

The estimation filters used are defined according to the nature of the redundancy.

(a) In the static case, the estimation is obtained by a classical least-squares method.

(b) In the dynamical but deterministic case, the estimation filter is a Luenberger observer, or a simple blender (i.e., a dynamical combination of the measurements). For example, the roll rate p may be estimated and tested by using the rotational kinematic equation:

$$p = -\dot{\Psi}\sin\theta + \dot{\Phi} \qquad (3.1)$$

together with the corresponding estimation filter, as shown in Fig.5. Disturbances and noises neglected in the design of these filters become important in the definition of the monitoring and in the robustness analysis.

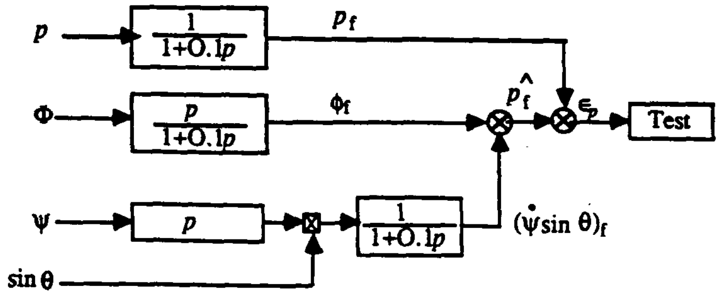


Figure 5: Luenberger observer or simple blender

(c) In the general stochastic case, the estimation filter can be a Kalman filter designed according to the measurement noises and the disturbance characteristics. There are a number of ways in which specially designed filters have been investigated for use in fault diagnosis. These fit broadly into the following categories:

3.2 Failure detection filter

The failure (fault) sensitive filters are filters or estimators that deliver signal characteristics of the faults. They have been introduced by Beard (1971) and Jones(1973) who used Luenberger observers designed not for their state estimation performances but for their fault sensitivity.

This theoretical work is useful for the analysis of fault detectability. It was reformulated as an eigenstructure assignment problem and applied to the design of detection filters for aircraft sensor and actuator faults (Wilbers & Speyer, 1989).

The failure detection filter theory focusses attention on the sensitivity of the filter to various faults, however, a new approach which uses this approach but also incorporates robustness aspects is the so-called **unknown input observer for fault detection** as reported by Viswanadham and Srichander (1988), Wünnenberg and Frank (1987), Patton (1988) and Patton, Frank & Clark (1989) describe a number of ways of using the concept of the decoupling of unknown inputs from the fault detection system to enable *robust fault diagnosis* to be achieved. Various approaches can be used to make a fault detection filter (or observer) become insensitive to unmodelled disturbances, whilst having specific sensitivity to individual sensor or actuator faults. Patton, Frank & Clark (1989) also show that, when a deadbeat observer is used, the fault detection filter,is equivalent to the *parity space* method of residual generation (Chow & Willsky, 1984; Massoumnia, 1986).

For the flight control application Patton, Willcox and Winter (1987) have used the modal structure in the longitudinal aircraft motion in the design of a fault detection filter. The fault decision signal is rendered insensitive to turbulence and parameter variations associated with the short period mode, by choosing an appropriate bandwidth in the fault monitor.

3.3 Fault Detection using Band-Limiting Filters

Faults in dynamic systems can be detected on the basis of the generation and cross-comparison of band-limited signals from dissimilar sources. Whilst signals measured at different points in the system may differ widely when viewed over a wide band-width, over limited pass bands Jones and Corbin (1988, 1989) have shown that simple relationships based on the used of band-limiting filters provide analytical redundancy for fault detection purposes. This approach can also be used to monitor the propagation, through the system, of information originating in the structure of the external inputs acting on the system.

3.4 Innovation Testing

In the preceding structures there is always a set of sensors tested with estimates obtained from another set, but a unique Kalman filter combining all the signals also offers fault detection capabilities. In normal operation the innovation vector, which is the difference between the measurements and their Kalman filter estimates, is a zero-mean white noise process with known covariance matrix. Mehra and Peschon (1971) proposed the use of different statistical tests on the innovation to detect a fault of the system. The fault isolation which is a more delicate operation is carried out by hypothesis testing, each fault having its own signature. This approach which looks like a multiple hypothesis test, is very sophisticated although a number of simplifications have been investigated (Willsky and Jones, 1976).

In the fault detection schemes, the monitors are as important as the detection filters. These operate on error signals, on innovation vectors or on likelihood functions generated by the detection filters. They are designed to maximise the detection probability with minimum false alarm rate, and their performances are reflected in the overall performance of the fault detection system. This detection problem has been widely investigated in the decision and signal processing literature (Sage and Melsa (1971), Basseville (1988)). The two main types of monitoring are as follows.

3.4.1 Threshold Logic

The signal magnitude is simply compared with a threshold function of the desired performances. This can give a fast detection of hard faults but for soft (incipient) faults the threshold has to be designed carefully in conjunction with a *robust fault detection filter* or using *robust parity space residual generation*. For rapid detection of an incipient fault, the residual or *fault decision signal* must be designed to be insensitive to disturbances, normal noise and aerodynamic (or plant) parameter variations. Clark (1989) has demonstrated some improvement in the fault detection capability of observer fault monitors by employing logic thresholds which are dependent on a combination of the magnitudes of the control signals. Alternative approaches to threshold selection ion have been used to improve the fault detection capabilities. An example of this is the comparison of the moving window average of the signal with the threshold. The threshold magnitude and the window size are then chosen to satisfy false alarm and missing alarm probabilities using Markov modelling techniques (Walker & Gai, 1979).

3.4.2 Sequential Probability Ratio Testing

Given a sequence of n observations, $x_1, x_2, \ldots, x_n$, the binary hypothesis test chooses between two hypotheses H_0 and H_1 according to the value of the probability ratio (Wald, 1947):

$$\Lambda_n = \frac{p(x_1 \, x_2 \ldots x_n \, / \, H_1)}{p(x_1 \, x_2 \ldots x_n \, / \, H_1)}$$

In the sequential probability ratio test (SPRT) the size of the sequence is not defined *a priori* and the test waits for another measurement if the information in the sequence is not sufficient to choose between the two hypotheses H_0 and H_1. Thus there are three possibilities:

- accept H_1 if $\Lambda_n \geq B$
- accept H_0 if $\Lambda_n \leq A$
- no decision if $A < \Lambda_n < B$

where the threshold magnitudes A and B are defined by the false alarm and missed alarm probabilities, respectively.

The SPRT, which has the interesting property of minimizing the average number of observations necessary to make a decision, offers a simple and efficient test to detect bias.

This bias test is also effective for other types of faults such as drift and scale factor errors. In general, SPRT offers the potential of efficient fault detection and can offer improved performance over the threshold logic approach in certain instances. It offers a quick decision for hardover faults, and can be sensitive to soft faults. The main disadavantage of the SPRT method is that it is a hypothesis test and not *a hypothesis change* test. To detect a change in the properties it must be modified by reinitialising the test when it has converged to one of the hypotheses H_0 or H_1. The detection time is then dependent on the fault onset time.

3.4.3 Generalized Likelihood Ratio Testing

The generalized Likelihood Ratio (GLR) which is used to test different hypotheses depending on unknown parameters (Willsky and Jones (1976)) provides a solution to *the change detec*tion problem. If the hypothes$_i$s Ho is associated with the normal system and H_1 with the faulty one. The detection consists of testing between the *no change hypothesis* H_0:

$$x_1, x_2, ..., x_n \text{ are under hypothesis } H_0$$

and the *change hypothesis* H_1

$$x_1, x_2, ..., x_{r-1} \text{ are under hypothesis } H_0$$

$$x_r, x_{r+1}, ..., x_n \text{ are under hypothesis } H_1$$

where r is *the unknown change* instant.

If the observations $x_1, x_2, ..x_n$ are independent, the decision rule is:

$$\text{Max} \prod_{k=1}^{n} \frac{p(x_k/H_1)}{p(x_k/H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda$$

where λ is a threshold.

3.4.4 Multiple Hypothesis Tests

The various faults define a set of hypotheses, for example:

H_0: no fault,

H_1: fault on sensor 1,

H_2: bias on sensor 2,

H_3: zero output on sensor 1,

which is tested using Bayesian decision theory. Each hypothesis requires a Kalman filter and a likelihood computation from the innovation signals as shown in Fig. 6.

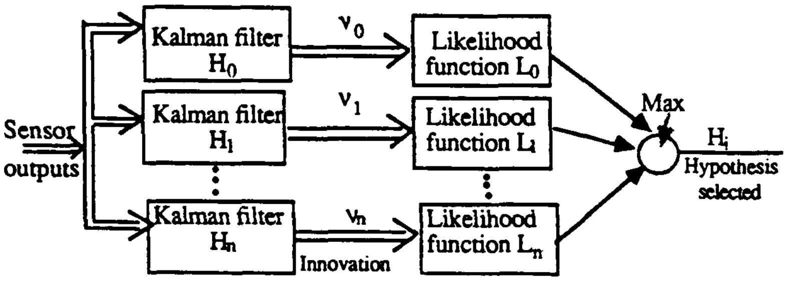


Figure 6: Multiple Hypothesis Test

If the time at which the fault occurs is unknown, this time is itself a hypothesis to test, and theoretically, an increasing bank of filters is needed. Various simplifications (Buxbaum and Haddad, 1969; Montgomery and Price, 1974; Wells, 1977) have been proposed, but these schemes remain complex and suppose known fault types.

4 Aircraft Sensor Fault Detection

Although almost all the fault detection techniques may be implemented on the aircraft, estimation procedures are the most used and seem to provide the best capabilities. These are model-based techniques which must be adapted to the varied flight conditions of the aircraft. For the aircraft application, the effect of measurement noises can usually be neglected as long as their magnitudes fall within an acceptable range for normal operation. Atmospheric turbulence effects may not, however, be ignored. We have also seen that different redundancy relations do not offer the same degree of redundancy and their definition can be rather variable.

Some knowledge of the dynamics modes of the aircraft and the way in which they are represented in the sensor signals allows the possibility of choosing a dynamic structure for a set of inter-connected subsystems. Each subsystem can then be incorporated into a fault detection monitor designed to be sensitive to particular faults. This idea of using the modal structure of the dynamic system can be combined with the notion of viewing the system over a well defined bandwidth in the frequency domain.

Use of frequency domain information in this way for aircraft sensor fault detection has been made by Jones and Corbin (1988) with band-limiting filters. Patton, Willcox and Winter (1987), use eigenstructure assignment of observers based on the filtering of certain modes of the aircraft. The filtering of the effect of, say the short period mode, acting on the fault detection signals, allows a lower threshold to be placed on these signals to minimise false alarm rates occurring during manoeuvres of the aircraft.

The actual non-linear aerodynamic force and moment equations of an aircraft can be incorporated into an analytical redundancy scheme in order to improve the fault detection reliability. Brockhaus (1985) has reported useful results on this topic based on flight-testing with a Dornier DO28 aircraft.

Expert systems have found favour in the literature as an interesting alternative to the model-based approach as reported by Handelman and Stengl (1989). Rule-based approaches based on *heuristic expert systems* are being combined with analytical redundancy methods in an attempt to accomodate the diagnosis of a wide range of aircraft system faults. Software architectures are being developed which integrate quantitative and qualitative methods for the purpose of enhancing the reliability of real-time fault-tolerant flight control and fault management systems. An important survey of knowledge-based approaches to fault diagnosis has been given by Tzafestas (1989).

Due to the required high integrity of an aircraft system some hardware replication is necessary so that applications of fault detection schemes are based on at least a duplex sensor arrangement. For such a case, the detection problem can become just one of isolation of the faulty sensor. However, even in a duplex sensor system *if in-lane monitoring* is to be used, then a separate monitoring system in each lane of hardware can be viewed as an independent fault-tolerant system providing detection and isolation of malfunctions within a lane. This offers the highest potential in reliability. Clearly, the hardware redundancy provides an indication of the fault onset time. In the dual case of combined analytical and hardware redundancy various techniques may be grouped into two main categories: *sensor set testing and individual sensor testing.*

4.1 Sensor Set Testing

In this approach, analytical redundancy is used to choose which of the two identical sets of sensors contains the fault. Only one filter is then necessary for each set of sensors, the error signal being the innovation as shown in Fig 7.

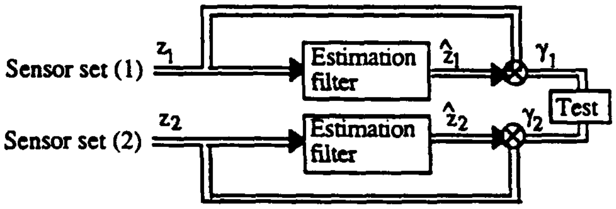


Figure 7: Sensor set test

Onken and Stuckenberg (1979) applied the scheme to design a fault detection monitor for the command and stability system of a flight control system. The system shown in Fig. 8 consists of two Luenberger observers with a logic scheme for the detection and isolation of sensor faults.

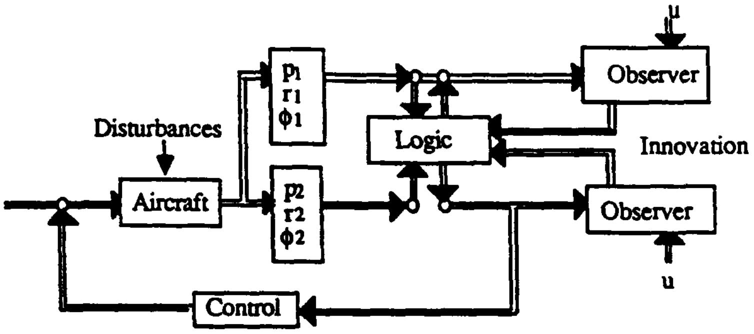
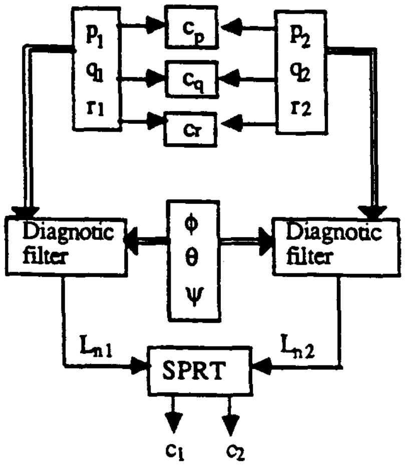


Figure 8:Fault detector for the command and stability system of a flight control system

Cunningham and Poyneer (1977) investigated a different concept: the use of a Kalman filter or observer as a diagnostic filter associated with logical tests or SPRT monitors. Fig. 9 represents the SPRT and Kalman filter solution. The SPRT that makes the choice between the two redundant sensor sets operates on the difference of the likelihood functions:

$$\Delta L_n = L_n^{(1)} - L_n^{(2)} = \sum_{i=1}^{n} (\gamma_i^{(1)} R^{-1} \gamma_i^{(1)T} - \gamma_i^{(2)} R^{-1} \gamma_i^{(2)T})/2 \qquad (4.1)$$



Faulty sensor			p_1	q_1	r_1	p_2	q_2	r_2
Logic	c_p		1			1		
	c_q			1			1	
	c_r				1			1
SPRT	c_1		1	1	1			
	c_2					1	1	1

Figure 9: Kalman filters and SPRT fault detection

where $\gamma_i^{(1)}$ and $\gamma_i^{(2)}$ are the innovation vectors of the Kalman filters using sensor set (1) and sensor set (2), respectively, and R is their covariance matrix. The decision is then:

$\Delta L_n \geq b$	fault in set(1)
$\Delta L_n \leq a$	fault in set(2)
$a \leq \Delta L_n \leq b$	no decision

As this is the only choice between the two sets, the false alarm probability depends only on the detection logic.

4.2 Sensor Testing

The sensor test approach takes advantage of the fact that the hardware duplication of the sensors provides the fault onset time. As estimates derived from the healthy sensors are not biased by the fault, in the absence of noises, the innovation signal is precisely an indication of the fault for this case. This scheme is illustrated in Fig. 10.

The major drawback of this structure is that it requires a different filter for each faulty sensor configuration. This variety of filter may, however, become an advantage; the filters may be simpler to implement and are designed for their detection performances.

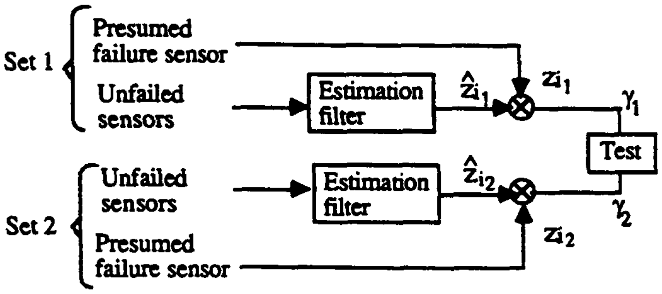


Figure 10: Sensor test

For their application to a NORD 262 aircraft, Labarrere *et al.* (1979) proposed using deterministic and dynamic relationships derived from the measurements and their derivatives by elimination of the unknown atmospheric disturbances. These relationships, which describe the redundancy of the system, are numerous and each one may be used to compute one of the outputs in terms of the others by *blending*, thus estimates of the questionable outputs can be derived in terms of the healthy measurements. Instead of using all the relationships, Labarrere *et al.* (1979) preferred to attach to each tested output an equation chosen according to a number of criteria: minimum noise on estimates, minimum number of measurements, minimum coupling of the equations, and insensitivity to model variations.

The procedure is organised in a parallel structure: the measurements of each couple of sensors are compared with a threshold; if a difference is detected three SPRTs are initiated, one detection SPRT on the output difference of the suspected sensor couple to corroborate or not the fault together with *two isolation* SPRTs acting on the difference between each measurement and its estimate. The diagnosis is obtained by a logical treatment of the SPRT results. This procedure has given good results on simulation and real flight data.

Deckert *et al* (1977) used a similar approach. The direct comparison between the two sensors delivers the fault onset time and allows the activation of several modified SPRTs operating on the residuals of the faulty sensor couple. Each residual sets are compared with a threshold; if there is a difference between a couple of sensors three SPRTs are initiated operating on the residuals of the faulty couple. Each residual is obtained from a kinematic (or dynamic) equation by a discrete blender technique. For example, the residual k for the roll rate gyro j at the time t_k obtained from the rotational kinematic equation:

$$p = -\dot{\Psi}\sin\theta + \dot{\Phi} \qquad (4.2)$$

is defined as follows:

$$\gamma_k^{\,j} = \sum_{i=1}^{k} \{p_i^{\,j}T - [\Phi_i - \Phi_{i-1} - (\Psi_i - \Psi_{i-1})\sin\theta]\} \qquad (4.3)$$

where T represents the sample period and an overbar denotes the average of the quantity over two samples.

The SPRT processing has been modified in two ways: first by the introduction of a time limit, then by a modification of the log likelihood ratio, which becomes:

$$u_n = \sum_{i=1}^{k} [\frac{m_k}{\sigma^2} (\frac{m_k}{2} - \gamma_k) + \frac{|m_k|}{\sigma^2} E_k] \qquad (4.4)$$

with m_k the bias value at time t_k

The last term, which differentiates the standard SPRT from the modified one, represents the worst-case error contribution in the test.

This analytical redundancy management has been implemented on the on-board computer of the NASA F8-DFBW aircraft with simulated sensor faults. All introduced bias and drift faults were correctly isolated. The only faults not isolated were the ones that did not produce appreciable output errors. Moreover, during the experiments, the procedure implemented detected undesired malfunctions (Szalai *et al.* 1980).

Various analytic detection techniques have been developed for sensor fault detection during the past few years. If they were sophisticated at the beginning, they became more and more simple, with increasingly robust performance, and easier to implement. Simulations and NASA flight tests have proved the validity of the analytical redundancy concept and the efficiency of the procedures. The detection is, of course, subjected to the aircraft and sensor modelling errors, and the performances depend on the sensors. Like voting systems, analytical redundancy has limitations; for real implementations on an aircraft, the sensors must not be opposed, but on the contrary, must be associated to improve the aircraft safety.

4.3 Jet engine fault diagnosis using analytical redundancy

In recent years hydro-mechanical implementations of turbine engine control systems have matured into highly reliable units. Engines and control systems have become more complex to meet ever-increasing performance requirements. This tendency has led, together with the revolution in digital electronics to the evolution of *full authority digital electronic control* (FADEC) implementations which must demonstrate at least levels of reliability as their hydro-mechanical predecessors. To improve the overall reliability of the FADEC system, various redundancy management techniques have to be applied to both the total control system and to individual components.

In order to maintain the operation of the engine in the event, for example, of a malfunction in a thermocouple sensor, it is important to use known functional (analytical) relationships amongst the various sensors. In this way a faulty sensor can be located and the control system can thus be re-configured with alternative feedback structures.

A number of investigators have studied the use of analytical redundancy methods for FDI in engine systems and the most advanced of these studies has recently been described by Merrill (1988). This paper also refers to a large body of NASA-funded research on this topic in the USA.

Recent work at Cambridge by Piercy (1989) has been focused on the problem of maximising the redundancy of an FDI method for jet engines, based on the detection filter. Piercy examines the *efficiency* of FDI methods and proposes some new ideas of design based on over-measured jet engine sensor systems. The central theme of this work is the use of *measures for redundancy* as a way of improving the efficiency of the detection scheme.

Patton and Chen (1990) have recently reported the application of a new approach to FDI for jet engines which makes use of robust unknown input observer decoupling.

4.4 Fault reconfiguration (or fault accommodation) in flight control

In current flight control system practice, flight safety is achieved in the face of control effector failures, by specifying functionally redundant control hardware. Hardware redundancy, however, can impose significant weight, complexity, and power consumption burdens on the aircraft. On the other hand, candidate configurations for future tactical fighter aircraft include unconventional control surfaces, such as canards. Their presence makes it possible to apply a given control force and moment to the airframe through a greater variety of combined control surface deflections than in more traditional configurations. This *control redundancy* has made the *reconfigurable*, or *self-repairing* flight control system concept attractive (Chandler, 1984; Howell et al., 1983). A reconfigurable or fault accomodating control law preserves closed-loop performance in the face of control effector malfunctions by redistributing force and moment commands over the impaired control suite to minimize the impact of the impairment.

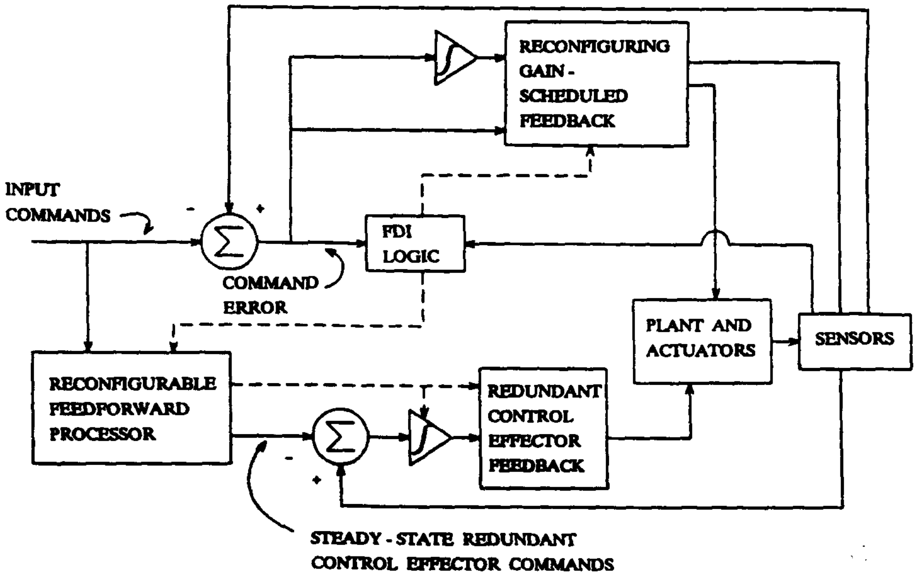

RECONFIGURING GAIN - SCHEDULED FEEDBACK
INPUT COMMANDS
-
+
FDI LOGIC
COMMAND ERROR
PLANT AND ACTUATORS
SENSORS
RECONFIGURABLE FEEDFORWARD PROCESSOR
REDUNDANT CONTROL EFFECTOR FEEDBACK
-
+
STEADY - STATE REDUNDANT CONTROL EFFECTOR COMMANDS

Figure 11: Block diagram of reconfigurable flight control

Fig. 11 (after Moerder, Halto, Broussard & Caglayan, 1989) shows the structure of a reconfigurable flight control system. FDI logic monitors the system's *control impairment status*, providing its current estimate to the optimal gain scheduling proportional & integral filter regulator and feedforward processor, as represented by the dotted lines from the FDI. In addition to forming steady-state control deflection commands, the feedforward processor switches off control surface command error integrators as surfaces drop out of the system.

This system typifies the complexity which must be used to provide a practicable and fault-tolerant reconfiguration scheme for flight control.

5 Bibliography

Basseville M 1988 Detecting changes in signals and systems - A survey. *Automatica* 24, no.3, 309-326.

Beard R V 1971 *Failure accommodation in linear systems through self-reorganization*, Report MVT-71-1, Man Vehicle Lab, MIT, Cambridge, Massachusetts.

Brockhaus R 1985 Analytical redundancy through nonlinear observers, *7th IFAC/IFORS Symposium on Identification and System Parameter Identification*, York, UK, July, 719-724, Pergamon Press, Oxford.

Buxbaum J P & Haddad R A. 1969 Recursive optimal estimation for a class of non Gaussian processes, *Proc. Symp. Computer Processing in Communications*, Polytechnic Institute of Brooklyn, New York

Chandler P 1984 Self-repairing flight control system reliability and maintainability program plan, US Air Force Flight Aeronautics Lab./Flight Dynamics Lab., Wright-Patterson, AFB, Ohio, February

Chow E Y & Willsky A S Analytical redundancy and the design of robust failure detection systems, *IEEE Trans. Auto. Control*, AC-29, 7, 603-14

Clark R N 1978a Instrument fault detection *IEEE Trans. Aero and Electron Sys,* 14, 3

Clark R N 1978b A simplified instrument failure detection scheme *IEEE Trans. Aero and Electron Sys*, 14, 4

Clark R N State estimation schemes for instrument fault detection, Chapter 2 in: *Fault Diagnosis in Dynamic Systems: Theory and Applications*, Patton R J, Frank P M & Clark R N, Prentice Hall, July 1989.

Cunningham T B & Poyneer R D 1977 Sensor failure detection using analytical redundancy, *Proc. Joint Automatic Control Conf.*, 378-87

Deckert J C Desai M N Deyst J J & Willsky A S 1977 F8 DFBW sensor failure identification using analytical redundancy, *IEEE Trans. Auto. Control* 22, 5

Frank P M 1989 Evaluation of analytical redundancy for fault diagnosis in dynamic systems, *Proc.IFAC/IMACS/IFORS International Symposium on Advanced Information Processing in Automatic Control - AIPAC '89,* Nancy, France, 3-5 July.

Gertler J J 1988 Survey of model-based failure detection and isolation in complex plants, *IEEE Control Systems Magazine*, 3-10, December.

Handelman D A & Stengl R F 1989 Combining expert system and analytical redundancy concepts for fault-tolerant flight control, *J. Guidance, Control and Dynamics*, 12, 1.

Howell W Bundick T Hueschen R & Ostroff A 1983 Restructurable controls for aircraft, Proceedings of the AIAA Guidance, Navigation & Control Conference, August

Jones G J & Corbin M J 1988 Analytical redundancy using band-limiting filters, *IEE Proceedings*, 135, Pt. D, No. 4, July, 257 - 265.

Jones GJ & Corbin M J 1989 A band-limiting filter approach to fault diagnosis, Chapter 6 in: Fault diagnosis in dynamic systems; theory and application, Patton, Frank & Clark (eds), Prentice Hall, 1989

Jones H L 1973 Failure detection in linear systems, PhD thesis, Massachussetts Institute of Technology

Labarrere M 1980 Detection de panne de capteurs d'avion par utilisation de la redondance analytique AGARD LS- 109, NATO Advisory Group for Aerospace Research and Development, Neuilly sur Seine, France.

Labarrere M, Pircher M, Gimonet B, Bucharles A 1979 Recherche de methodes de detection de pannes de capteurs, Rapport DRET/DERA 3/7170, ONERA-CERT, Toulouse.

Lipscombe J M 1980 Aerospace Systems, in: Modelling of Dynamic Systems, 1, Nicholson H (ed.), IEE Control Engineering Series, Peter Peregrinus Press

Massoumnia 1986 A geometric approach to failure detection and identification in linear systems, PhD thesis, Massachusetts Institute of Technology.

Merrill W C 1989 Advanced detection, isolation, and accommodation of sensor failures - a real-time evaluation, *J. Guidance,Control & Dynamics*, 11,No.6, Nov/Dec,1988, 517-526

Mehra R K & Peschon I 1971 An innovations approach to fault detection and diagnosis in dynamic systems,*Automatica*, 7, 637-40

Moerder D D Halyo N Broussard J R & Caglayan A K 1989 Application of precomputed control laws in a reconfigurable aircraft flight control system, *J. Guidance, Dynamics & Control*, 12, No.3, May/June, 325-333

Montgomery R C & Price D B 1974 Management of analytical redundancy in digital flight control systems for aircraft, *Proc. AIAA Mechanics and Control of Flight Conf.*, Anaheim, Calif.

Montgomery R C & Williams J P, Analytic redundancy management for systems with appreciable structural dynamics, Chapter 10 in: *Fault diagnosis in dynamic systems: theory and application*, Patton Frank & Clark (eds) Prentice Hall, 1989

Onken R & Stuckenberg 1979 Failure detection in signal processing and sensing in flight control systems, *Proc. IEEE CDC Conf.*, San Diego, Ca.,449-454.

Page E S 1954 Continuous inspection schemes. *Biometrika* 41, 00-115.

Patton R J 1988 Robust fault detection using eigenstructure assignment, *Proceedings of the 12th IMACS World Congress on Mathematical Modelling and Scientific Computation*, Paris, 2, 431-434, July 18-22, 1988

Patton R J & Kangethe S M 1989 Robust fault diagnosis using eigenstructure assignment of observers, Chapter 4: in *Fault diagnosis in dynamic systems: theory and applications*, Patton Frank & Clark (eds), Prentice Hall 1989

Patton R J & Chen J 1990 The design of a robust fault diagnosis scheme for a jet engine system, *IMACS Annals on Computing and Applied Mathematics Proceeding MIM-S2'90*, Sept. 3-7, 1990

Patton R J , Willcox S W & Winter S J 1987 A parameter insensitive technique for aircraft sensor fault analysis, *J. Guidance, Control and Dynamics*, 10, No 4,359-367.

Patton R J Frank P M & Clark R N (eds) 1989 Fault Diagnosis in Dynamic Systems: Theory and Applications, Prentice Hall.

Piercy N P 1989 *A redundancy approach to sensor failure detection with application to turbofan engines*, PhD thesis, department of Engineering, University of Cambridge

Sage A P & Melsa J L 1971 Estimation theory with applications to communications and control - Mc Graw Hill.

Szalai K J, Larson R R & Glover R D 1980 Flight experience with flight control redundancy management, AGARD LS 109, NATO Advisory Group for Aerospace Research and Development, Neuilly sur Seine, France.

Tzafestas S G System fault diagnosis using the knowledge-based methodology, Chapter 15 in: Fault diagnosis in dynamic systems:theory and applications, Patton, Frank & Clark (eds), Prentice Hall, 1989.

Viswanadham N & Srichander R 1987 Fault detection using unknown-input observers, Control Theory and Advanced Technology, MITA Press, 3, 2, 91-101.

Wald A 1947 *Sequential Analysis*, Dover, New York.

Walker B K 1983 Recent developments in fault diagnosis and accomodation, Proceedings of the *Proceedings of the AIAA Guidance, Navigation and Control Conference*, Gatlingburg, TN,

Walker B K & Gai E 1979 Fault detection threshold determination techniques using Markov theory, *J. Guidance and Control*, 2, No 4, July-August, 313-319.

Wells W R 1977 Failure detection for aircraft engine output sensors via bayesian hypothesis testing, AIAA Paper 77 838, American Institute of Aeronautics and Astronautics, New York.

Westermeier T F 1977 Redundancy management of digital FBW systems, *Proc. Joint Automatic Control Conf.*, 272-77

Wilbers D M & Speyer J L 1989 Detection filters for aircraft sensor and actuator faults Proceedings of the IEEE International Conference.on Control and Applications Jerusalem, April, 1989

Willsky A S 1976 A survey of design methods for failure detection in dynamic systems, *Automatica*, 12, 601-11

Willsky A S & Jones H L 1976 A generalized likelihood ratio testing approach for the detection and estimation of jumps in linear systems, *IEEE Trans. Autom Control* 21, 108-12

Wright R L 1981 The microwave radiometer spacecraft - A design study, NASA Reference Publication 1079, Dec. 1981.

Wünnenberg J & Frank P M 1987 Sensor fault detection via robust observers, In System Fault Diagnostics, Reliability and Related Knowledge-Based Approaches, S. Tzafestas, Schmidt and Singh (eds) D R Reidel Press, Vol1, 147-160.