FAULT-TOLERANT CONTROL SYSTEMS: THE 1997 SITUATION

Ron J Patton

The University of Hull,
School of Engineering,
Hull HU6 7RX, UK
Phone/FAX:0044 1482 46 5117/878
e-mail: *r.j.patton@eng.hull.ac.uk*

Abstract: The fault-tolerant control problem belongs to the domain of complex control systems in which inter-control-disciplinary information and expertise are required. This paper outlines the state of the art in a field which remains largely a theoretical topic with most application studies based upon aerospace systems. The directions in which the subject is going are summarised and some pointers are given as to the likely future issues and where new research effort is required. The paper provides a basic literature review covering most areas of fault-tolerant control.

Keywords: Fault-tolerant systems, fault diagnosis, adaptive control, robust control, redundancy control

1 INTRODUCTION

A conventional feedback control design for a process plant or vehicle system may result in unsatisfactory performance (even instability), in the event of malfunctions in actuators, sensors or other components of the system. In order to overcome the limitations of conventional feedback, new controllers are being developed which are capable of tolerating component malfunctions whilst still maintaining desirable and robust performance and stability properties. Research into fault-tolerant control has attracted many investigators and is now the subject of widely scattered publications (Stengel, 1991; Veillette, 1992; Patton, 1993; Stengel, 1993; Antsaklis, 1995; Rauch, 1995; Blanke *et al.*, 1997; Frank, 1995; Walker, 1997; Wu, '95-'97). Little information from *these* and other similar (academic) studies has ever been applied to real process plants or vehicles. The problem is partly due to a general view that practitioners have of sophisticated control systems techniques. "Simplistic" approaches to fault--tolerant control have been applied in many industrial and aerospace systems, e.g. for jet engines, flight control, electrical drives for railway traction, automotive engine management systems, etc. Fault--tolerant systems based on rather basic engineering fundamentals may require a significant amount of maintenance. However, the view is usually taken that it is better to work with principles that are easily understood and verifiable, rather than use more complex methods for which the fault-tolerant system behaviour may pose intolerable risks in terms of safety, cost, instability or unpredictable behaviour. There is an argument that simpler monitoring schemes, with fewer components or lines of software code are intrinsically more reliable. Most often, the main requirement is that the system should maintain some "acceptable" level of performance or degrade gracefully, subsequent to a malfunction. When it is proved that this can be achieved the fault-tolerant approach becomes acceptable to systems and control engineers. Further complexity would not be cost effective. This is the philosophy behind many day to day existing real engineering system.

We need to determine what the limitations of these "simple minded" methods are for each individual application problem. There is no doubt that fault-tolerant control is an application-specific field - strategies for fault-tolerance tend to be developed using available equipment, measurements and application-specific know-how. Ideally, not one but several alternative methods should be compared on the basis of cost, robust stability, degree to which the system behaviour is predictable and can be degraded gracefully (without loss of life/injury and/or significant economic loss). Computational burden is often a deciding factor. Complexity can decrease the overall system reliability.

Concerning fault-tolerant control theory, there is a substantial body of literature and the "academic" subject has advanced with reliability requirements of safety-critical systems. A number of studies are motivated by the possibility of application; examples include: hazardous chemical plants (Himmelblau, 1978); the control of nuclear power plant reactors (Kitamura, 1989; Garcia *et al.*, 1991; Eryurek *et al.*, 1995); space craft (Gelderloos *et al.*, 1982); Buckley *et al.*, 1995; Blanke *et al.*, 1997) and the control of unstable fly-by-wire aircraft (a non-exhaustive list) (Westermeier, 1977; Chandler, 1984; Meyer *et al.*, 1984; Looze *et al.*, 1985; Ostroff, 1985; Rattan, 1985; Razza *et al.*, 1985; Smith *et al.*, 1987; Caglayan, 1988a&b; Lane *et al.*, 1988; Moerder *et al.*, 1989; Gao *et al.*, 1990; Morse *et al.,* 1990; Ochi *et al.*, 1991; Rauch, 1995). However, research into fault-tolerant control is largely motivated by the control problems encountered in aircraft system design. the goal is to provide a "self-repairing" capability to enable the pilot to land the aircraft safely in the event of a serious fault. The interest has been specially stimulated since two commercial aircraft accidents in the late 1970's. In the case of DELTA flight 1080 (McMahan, 1978), the pilot successfully reconfigured the remaining lateral control elements and landed the aircraft safely; the elevator became jammed at 19 degrees up and the pilot had been given no indication that this malfunction had occurred. In the second accident the pilot had only 15s to react and the plane crashed. Subsequent studies showed that the crash could have been avoided (NTSB, 1979). These studies shave shown that prompt presentation of fault information to the pilot could enable him to take accommodating action. The pilot cannot, however, enable the aircraft to recover from some types of malfunctions for which a *redundancy management system* (Westermeier, 1977) with duplex redundant flight surfaces and/or actuators and sensors become essential. A system for aiding the pilot by providing special automatic fault accommodation strategies is necessary for both civil and military aircraft.

The main task to be tackled in achieving fault-tolerance is the design of a controller with suitable structure to guarantee stability and satisfactory performance, not only when all control components are operational, but also in the case when sensors, actuators (or other components e.g. the control computer hardware or software) malfunction. This has sometimes been referred to as a control system which possesses integrity or which has control loops which possess loop integrity (Owens, 1978). Some authors prefer to use the term *reliable control* (Birdwell *et al.*, 1986; Veillette *et al.*, 1992). Although, broadly speaking reliable control is equivalent to fault-tolerant control, there are some differences, as pointed out by Stengel (1991) who also give definitions of reliability reliability, maintainability and survivability:

> "Failure-(Fault-) tolerance may be called upon to improve system reliability, maintainability and survivability. The requirements for fault--tolerance are different in these three cases. *Reliability* deals with the ability to complete a task satisfactorily and with a period of time over which that ability is retained. A control system that allows normal completion of tasks after component fault improves reliability. *Maintainability* concerns the need for repair and the ease with which repairs can be made, with no premium placed on performance. Fault--tolerance could increase time between maintenance actions and allow the use of simpler repair procedures, *Survivability* relates to the likelihood of conducting an operation safely (without danger to the human operators of the controlled system), whether or not the task is completed. Degraded performance following a fault is permitted as long as the system is brought to an acceptable state."

Reliable control is an idealistic goal. However, several investigators have pursued a line of reasoning that robust control theory can be used to maintain acceptable system stability and performance when control loops malfunction (Birdwell *et al.*, 1986; Veillette *et al.*, 1992). Clearly, additional loops are required to make this possible.

As stated in Section 1, simpler ways of achieving fault-tolerance are used in practice. For example, consider the main longitudinal stability channel of an aircraft. If the pitch angle gyro signal or inertial navigation system is impaired, the longitudinal motion of the aircraft will be unstable. The fault must be isolated rapidly, to switch off the impaired signal, and to activate a correct control law with the use of the unimpaired (redundant) gyro signal. It is not always necessary to use sophisticated techniques to discern that the gyro has malfunctioned; a comparative scheme in dual redundancy will indicate that the fault has occurred by simply noting that there is a discrepancy between two gyro signals. Simple data conditioning can then be used to determine that one pitch rate measurement is out of range and that the corresponding gyro is faulty. The redundancy management system will thus switch the feedback function to the healthy instrument.

However, to decide that the gyro has a *developing* fault i.e. before the fault becomes serious, is more difficult, as the gyro output will still appear normal. It is then of interest to use methods which can, amidst effects of noise, turbulence etc, pick out the abnormal signal before the aircraft is unstable. There is also a principle that the pitch rate signal could be estimated from other measurements using kinematic relationships. This is the basis of an alternative form of "analytical" redundancy which can be used to detect and isolate very small faults. Hence, "modern" methods (based upon analytical redundancy techniques) for fault-tolerance could be used on this safety-critical application (Willsky *et al.*, 1975). The use of such methods will depend very much on their demonstrable advantages; this is the hard part!

Fault-tolerant control is not just a safety-critical issue; it is of interest to process plant operators who are keen to increase productivity and make more money. The reliability of a system component (including the controller) affects the plant operation economy. As an example, consider a tandem rolling steel mill. It is also important that the plant's operation is maintained in a closely checked envelope of performance throughout each operation shift. In a dangerous situation the mill can be shut down safely. However, there are situations (which are far from dangerous) in which small "fault" effects (e.g. undesirable strip thermal stresses) which degrade the quality of the steel and the performance of the mill. Ideally, the plant supervision system (or operator!) should have the capability of recognising such undesirable behaviour and reconfiguring the control action to improve performance and steel quality. One must not forget the role of the human operator in monitoring these activities.

Recent application studies (not safety-critical) include a rail electric traction system (Bennett *et al.*, 1997), a satellite system (Oested) for measuring the earth's magnetic field (Blanke *et al.*, 1997), a ship propulsion system (Izadi-Zamanabadi *et al.*, 1997), rudder surface electro-hydraulic aircraft actuator (Eich *et al.*, 1997), fault-tolerant model-based predictive control of a boiler system (Son *et al.*, 1997).

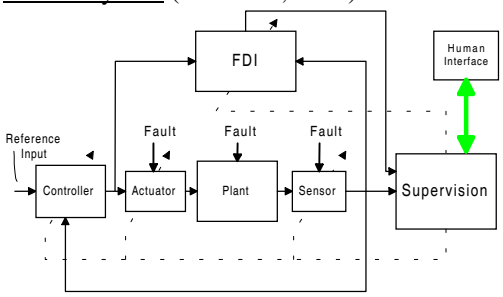

Fig 1.1 Scheme of fault-tolerant control system with supervision subsystem

Fig 1.1 shows the general schematic arrangement appropriate to many fault-tolerant control systems with four main components: the plant itself (including sensors and actuators), the *fault detection and isolation* (FDI) unit, the feedback (or feed-forward) controller, and the supervision system. The solid line represents signal flow, and the dashed line represents adaption (tuning, scheduling, reconfiguration or restructure). The plant is considered to have potential faults in sensors, actuators (or other components). The FDI unit is responsible for providing the supervision system with information about the onset, location and severity of any faults. Based on the system inputs and outputs together with fault decision information from the FDI unit, the supervision system will reconfigure the sensor set and/or actuators to isolate the faults, and tune or adapt the controller to accommodate the fault effects.

Fault-tolerant control is a strategy for reliable and highly efficient control law design. To achieve these requirements, it is also a systematic problem. Blanke *et al.* (1997) demonstrate the principles involved in the systematic design and development of a real fault-tolerant control application. As they point out, the effort to be expended affects the development of each stage and aspect of the overall system design. Fault-tolerance objectives are important from the plan to concept design and then to the final realisation. In principle, all relevant science/technology domains are included e.g. materials science, electronics, computer science, sensor technology, control theory and design, signal processing and even human factors. Here, attention is paid to the following fault-tolerant control aspects: **FDI, Robust Control, Reconfigurable or Restructurable Control, and Supervision.**

2 THE STATE OF THE ART

During the past two decades, there has been significant but scattered activity in the numbered areas of Fig 2.1.

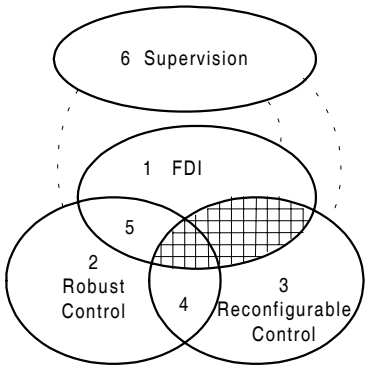

Fig 2.1 The scattered areas of fault-tolerant control research

Area 1: Most of the research in FDI to-date does not include the combined design of controllers with fault detection, fault isolation and fault identification (estimation). However, FDI research is now a very mature field providing many powerful quantitative and/or qualitative modelling tools and artificial intelligence. Key references to this work can be found in: Willsky (1976), Mironovski, (1980), Walker (1983), Isermann (1984), Milne (1987), Gertler (1988), Frank (1990), Patton & Chen (1991), Leitch *et al.* (1992), Patton & Chen (1993), Frank (1994), Isermann (1994), Krishnasaami *et al.* (1994), Patton (1995), Chen *et al.* (1996) and Isermann *et al.* (1996) and in books: Basseville *et al.* (1986), Patton *et al.* (1989), Brunet *et al.* (1990), Basseville *et al.* (1993), Pouliezos *et al.* (1994) and Patton (1997). These studies fall into area 1 in Fig 2.1, i.e. they do not deal with joint problems of robust control/robust FDI.

Area 2: Robust control design has been the hottest research topic since the late 1970's (Safonov, 1978; Morari, 1989; Maciejowski, 1989 and Zhou *et al.*, 1996). However, information concerning the effects of faults upon the controlled process is not usually considered. Few cases where insensitivity to faults has been considered are referred to (sometimes unwittingly) as the *passive* approach to fault-tolerant

control (Eterno *et al.*, 1985; Stengel, 1991; Patton, 1993; Frank, 1995). The distinction between active and passive fault-tolerance is discussed in Section 4.

Area 3: The *reconfigurable control problem* has attracted the attention of several investigators. For example, Lane *et al.* (1988) and Ochi *et al.* (1991) pursued the use of feedback linearisation and Gao *et al.* (1990, 1991) described the use of *pseudo-inverse methods*. Åström (1991, 1996), Ioannou, (1996) and others have considered *adaptive control* approaches. Huang *et al.* (1990), Morse *et al.* (1990) and Jiang (1994a) have made important contributions based upon *model-following* principles.

Area 4: This represents robustness issues which accompany reconfigurable control. Studies in this area are few. Wu ('92,'93,'95,'96,'97) addresses the problem of performance robustness during normal system operation versus fault sensitivity at the time a system component fault is determined. She uses a parametrised set of controllers satisfying a prescribed performance level. The set is optimised under a detection criterion sensitising the measurements to specific faults. Wu considers the integration issues as a control design problem, where the designer is largely free to choose one of a number of suitable FDI techniques. She also considers (1997) a performance measure based upon a "coverage interval", the size of the interval reflecting information deficiency. In this way the reliability and performance requirements of various modules can be related. Jiang (1994b) discussed how reconfigurable control can be achieved using eigenstructure assignment design.

Area 5: This covers joint design of robust controllers and robust fault estimation (Nett *et al.,* 1988; Valavanis *et al.* 1989; Helmicki *et al.,*1994*,* Tyler *et al.* (1994); Murad *et al.*, 1996; Åkesson, 1997, Eich *et al.*, 1997; Niemann *et al.*, 1997; Stourtstrup *et al.*, 1997). The fault estimation problem here is not the same as the quantitative modelling approaches taken in FDI, according to Area 1. These studies are based upon the idea that the robust controller optimisation and fault estimation designs are best combined (Tyler *et al.*, 1994), for example using H_∞ optimisation. The arguments for doing so are plausible. However, this approach leads to complex interaction between the controller and FDI robustness problems. This is simple to see as the design freedom is utilised to solve both problems simultaneously. The alternative way of performing "open-loop" FDI (as in Area 1) and separate controller designs obviates the design freedom complexity. The separate design approach also gives rise to a "one way coupling" in robustness - the controller affects the FDI robustness but not *vice-versa*. This is not the case in the joint control/ fault estimation problems.

Hatched area: Few studies combine the functions of FDI and reconfigurable control (Noura *et al.*, 1993; Chiang *et al.*, 1995; Jiang, 1994b). It is now often understood that the FDI function (together with suitable redundant equipment) can avoid the development of more serious faults. However, the combination of FDI/control reconfiguration is a complex issue as reported by Mariton (1989) who describes important consequences that the detection delay has upon system stability. Guided by practical constraints arising from application studies, Srichander & Walker (1993) proposed a stochastic approach to the stability analysis of some active fault-tolerant control systems employing FDI schemes. Such systems can be shown to have dynamic behaviour governed by stochastic differential equations as the faults/fault decisions occur randomly. The stochastic differential equation parameters vary randomly in time and the equations can be analysed using Markov theory. These stochastic approaches to robustness analysis are an emerging theoretical field in fault-tolerant control.

The hatched area of Fig. 2.1 represents a field ripe for an interesting harvest. There has been little research in combined robustness design with reconfigurable control and FDI. The challenge is to integrate together the design and implementation of a reconfigurable control scheme (based upon robust controller designs) and an FDI unit. As stated under Area 5, the joint design of robust controllers and robust fault estimation has been considered by several investigators However, these studies do not include the full function of FDI and because of the approach taken, the fault estimation affects the controller robustness (see Section 5). When fault detection and isolation is carried out using the "open-loop" approach (generating residuals which do not influence the controller - see for example Frank (1994) or Chen *et al.*, (1996)), the controller robustness problem is de-coupled from the FDI unit design, although the controller *does* affect the robustness of both the fault detection and fault isolation tasks.

Area 6: Rauch (1994), Buckley *et al.*, (1995), Eryurek *et al.*, (1995), and Polycarpou *et al.*, (1995) introduce different forms of selection logic and system management into the fault-tolerant system. Whilst supervision is essential for the active form of fault-tolerant control, few investigators have paid much attention to this area. The supervision system manages the fault decision information and selects the most suitable control function (parameters but sometimes structure), subsequent to the declaration that a fault has occurred. The supervision system must also determine whether a fault has a detrimental effect on the system's performance and stability to warrant controller changes. It is important that the FDI unit should be capable of providing diagnostic information in a suitable format to facilitate the adaption of the system's feedback.

3 PLANNING AND DESIGN FOR FAULT-TOLERANT CONTROL

Fault-tolerance in control requires effort at every stage and in all aspects of system design. Most papers in control systems research only consider problems which are based on mathematical models of the plant. There are other important non-mathematical

challenges. As stated in the introduction, fault-tolerant control should ideally be accompanied by a systematic and integrated approach to design. The strategy should (again ideally) commence with an understanding of the structure of the system, the reliability of different components, the types of redundancy available (or to be generated) and the types of controller function which are available and might be required. Some interesting studies, for example by Blanke *et al.* (1997) have paid attention to the development of the overall concept of systematic design for fault-tolerant control. They focus on the development of an overall concept of systematic design which gives a consistent design and assures system dependability.

Most studies in fault-tolerant control focus on a selection of one of the areas in Fig. 2.1 without considering the wider issues that might be involved.

3.1 Fault-tolerant system requirement analysis

The first stage of the development of a fault-tolerant system is the requirement analysis and system plan. The reliability distribution analysis is the key issue at the planning stage. This includes the following procedures (Blanke *et al.*, 1997):

> Possibility analysis for component faults; Failure Mode & Effects Analysis (FMEA); System reliability analysis; Reliability distribution.

The essential properties of a fault-tolerant control system must be acquired from some knowledge of previous and likely process fault conditions. Hence, all potential faults and their effects should if possible be determined. A number of investigators (Lege, 1978; Herrin, 1981; Bell, 1989; Hunt *et al.*, 1995) have discussed the use of *failure mode effects analysis* (FMEA) techniques to determine systematically how fault effects in components relate to faults at inputs, outputs, or elements within the components. Blanke *et al.* (1997) describe the development of a matrix FMEA approach using Bond graph system component modelling. They show how component models can be simplified into generic types which can be useful for fault-tolerant system design, with an emphasis on the development of degrees of criticality and the important issue of determination of control system action to faults. They also describe a three-level architecture for a supervisor-based fault-tolerant controller. Some completeness properties can be obtained using the Bond graph and *array theory* implementation of the supervisor logic.

Through possibility and system reliability analyses, and reliability distribution, it should be clear which component(s) suffer(s) more from certain faults than from others. The weakest link in the chain can then be determined.

3.2 *Redundancy design*

The second stage in the development of a fault-tolerant system is system redundancy design. At this stage, the nature and location of all redundancies in the process must be determined, i.e. the type of redundancy and whether it is suitable for the particular situation; the level of redundancy, etc. This stage includes:

> Fault criticality assessment; Fault detectability; fault detectability/isolability; Counter/remedial action design; fault accommodation requirements; Optimal sensor location.

In principle, in order to achieve fault-tolerance, system redundancy is necessary. *Direct redundancy* means that multiple independent hardware channels (e.g. triplex/quadruplex replication) with a majority vote selection of healthy system channels are used.

Even though direct redundancy can be realised by involving strictly hardware channel replication, in many cases, fault-tolerant and high integrity computer systems involve redundancy in terms of dissimilar software and hardware. Dissimilar redundancy, is achieved using another (different) subsystem or component (can be software) with the same function as the first, whilst built according to different principles and technologies. The advantage of dissimilar redundancy is that the necessity for independence can be satisfied.

A usual procedure in fault-tolerant control is that a non-impaired identical alternative (or redundant) component (e.g. sensor, actuator, control computer, etc) is brought into service to replace an impaired component when a fault occurs. This is known invariably as *hardware* (or software), *direct* or *parallel redundancy*.

The replacement is often done on the basis of "known reliability" (difficult to quantify!) - use up the best components first. In an *m-ary* (where $m > 2$) redundant scheme a majority voter can decide which component is "out of line" with the remaining components and thus considered faulty. The choice of the most reliable component can be achieved with a quadruplex redundant scheme to keep the system running with satisfactory performance.

It is not necessary to use direct or hardware redundancy; an alternative form of *functional redundancy* is often viable. Sometimes a combination of the two forms of redundancy is necessary (for example to keep the hardware redundancy index (m) down to, say 3). Making the best use of both direct redundancy and functional (analytical) redundancy provided by the systems, is a major task of fault-tolerant control system design. Functional redundancy is achieved by careful design or by arranging different subsystems to make the function of these subsystems overlap.

Flight control system example: In a flight control system, the vertical gyro can provide both the pitch and bank angle signals. If the horizontal gyro (which provides both bank and yaw angle signals) is used, there is a direct redundancy in the bank angle measurement. If one of these bank angle signals is

out of range, simple signal conditioning can point to the fault. The measurement system is therefore tolerant of a single bank angle fault - as long as the second gyro does not malfunction!

We assume for this example that the heading and pitch angles are reliable. Now add the roll rate gyro measurement, the rotational kinematics given by Eq. (3.1) can then be used to estimate the roll rate p (from other measurements) when the roll rate gyro signal is out of range (Labarrère *et al.*, 1993).

$$p = -\dot{\Psi} \sin\theta + \dot{\Phi} \tag{3.1}$$

Φ, Ψ and θ are the bank, yaw and pitch angles.

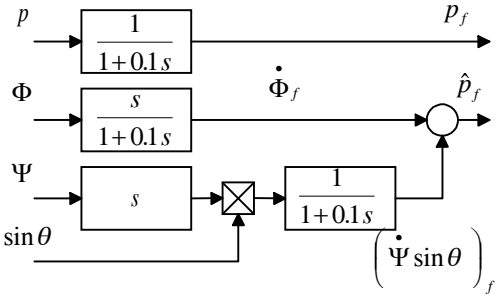

Fig. 3.1 Example of Analytical Redundancy

Analytical redundancy means the use of functional relationships between system variables. Fig. 3.1 illustrates how the filtered roll rate gyro signal ($\hat{p}_f$) can be generated from filtered estimates of the bank angle Φ_f , together with a filtered estimate of the product term $(\dot{\Psi} \sin\theta)_f$, according to Eq. (3.1). The estimated roll rate gyro signal $\hat{p}_f$ can be used to replace the measured gyro signal p_f . This filtered estimate $\hat{p}_f$ can also be used to compare with the filtered measurement p_f to yield a

Residual Signal: $r = p_f - \hat{p}_f$ (3.2)

where the subscript f denotes filtered signal, i.e., a low-pass/band-pass filter is used to eliminate the effects of unwanted high frequency disturbances. When all system components can be inter-related mathematically, all the analytical relationships constitute the complete dynamical system model. By using this model, estimates of many system variables can be derived for the purpose of providing extra redundancy i.e. to back-up the system's available measurements (Deckert *et al.*, 1977; Labarrère *et al.*, 1993; Lou *et al.*, 1986; Willsky, 1976) for fault diagnosis/controller reconfiguration.

Residual signals, as represented by Eq. (3.2) are generated singly or in vector form. These residuals can be generated functionally using linear or non-linear observers, parity equations or Kalman filters. Apart from parameter estimation these constitute the main methods of quantitative model-based analytical redundancy (Patton, 1995). Analytical redundancy provides higher system independence than direct redundancy. As it is based upon functional or model information, it suffers more from system non-linearity and parameter or model structure uncertainty. In aeronautical applications, there has been an increasing tendency to not substitute direct redundancy entirely by the analytical alternative, but to suppress some index of redundancy. It is now very appropriate to combine analytical and direct redundancy schemes to enable real time fault accommodation. **This powerful combination of redundancy methods is the key to the way forward in fault-tolerant control.**

Using redundancy, scenarios for detecting faults in every possible process component or subsystem can be listed out. The *fault detection coverage rate* can then be analysed as a direct correspondence with FDI techniques and the use of redundancy. If the coverage rate is lower than that which is required, a more efficient FDI approach should be utilised, or further independent sources of redundancy should be adopted. With knowledge of the *fault possibility* of certain components, the reliability of a component or subsystem can be obtained (Wu, 1997). If this reliability is too low the level of redundancy must be increased or more reliable component/subsystems should be built into the process.

Analytical redundancy is not only useful for isolating faults, it can also be used to provide an estimated measurement signal. The analytically-derived signal can be used instead of the impaired sensor signal, perhaps under limited authority. Alternatively, a new controller with different structure (using a different set of sensor signals) could be utilised when the fault has been detected.

If a fault occurs in a simplex actuator, the only way to accommodate the fault is to reconfigure the controller to operate in a restricted way according to the fault severity (perhaps to provide graceful degradation of the process performance). This is what is known as "single fail operate" as one fault can be isolated and corrected so that the system will continue to operate (albeit with degraded performance).

Without the fault-accommodating controller the system would be "fail passive" - once the faulty actuator is isolated it is disengaged and the actuator should not have been crucial to the safe operation of the system. In safety-critical situations this is rarely possible and a single-fail-operate level of fault--tolerance must be used as the closed-loop system is reconfigured. Some systems become "dual fail operate" i.e. they become fail passive after two isolated malfunctions. This is important in aircraft and other safety-critical systems.

In some aircraft systems it is desirable to have many control "effectors" independently driven to accommodate faults. A control reconfigurable combat aircraft (CRCA) has, typically 17 flight surfaces. Many fault-tolerant control techniques have been

developed for the CRCA system structure. For all "down to earth" applications this level of actuator redundancy would be impossible to achieve!

It is then clear that the design of location, number and multiplicity of actuators and sensors of a process are an important part of systematic procedure for fault-tolerant system design.

3.3 Fault Accommodation Design

Here, the control and input/output requirements for each fault must be determined to provide guidelines for the development of a reconfigurable control design. This includes:

> Guidance for setting up control and input/output requirements for each fault effect; Determination of controller configuration (including what sensors/actuators should be used); Determination of the concept, properties and requirements for controller reconfiguration; Reconfiguration system for complete fault-tolerant control system.

Section 4 provides more information on the realisation of fault accommodation.

4 FAULT-TOLERANT CONTROL METHODS

4.1 Decomposition of fault-tolerant control

Fig. 4.1 shows a taxonomy of fault-tolerant control methods, based upon either *passive* or *active* approaches.

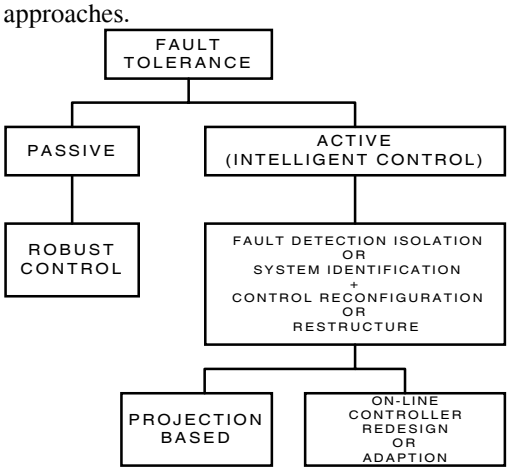

Fig. 4.1 Decomposition of fault-tolerant control

In active fault-tolerance, a new control system is redesigned using desirable properties of performance and robustness that were important in the original system, but with the reduced capability of the impaired system in mind. In order to achieve feedback control reconfiguration/restructuring of feedback control, an active fault-tolerant system requires either *a priori* knowledge of expected fault types or a mechanism for detecting and isolating unanticipated faults. In the latter case, decisions concerning the location and nature of faults are then used to reschedule the controller function.

Active approaches are divided into two main types of methods: projection-based methods and on-line automatic controller redesign methods. The latter involves the calculation of new controller parameters in response to a control impairment. This is often referred to as reconfigurable control (Huang *et al.*, 1990; Gao *et al.*, 1991). In projection-based methods, a new pre-computed control law is selected according to the required controller structure (i.e. depending upon the type of malfunction which has been isolated).

A reconfigurable or restructurable system, whose feedback action is changed automatically is a special form of an intelligent control system (Åström, 1991; Passino *et al.*, 1988; Stengel, 1991).

Reconfigurability implies that a system with fixed structure can be modified to account for uncontrollable changes i.e. faults in the system. In this case, restructurability subsumes reconfigurability, implying that not only parameters but the system structure itself can be changed to accommodate uncontrollable changes.

Active fault-tolerant systems based on unanticipated faults must have a mechanism for identifying abnormal system changes. This is essentially the function of a fault detection and isolation (FDI) scheme. Whilst it suffices to use the FDI procedures, it may also be important to identify the fault type and its severity as well as the reason for the fault development. When these functions are included along with FDI, we call it a *fault diagnosis* subsystem or scheme.

4.2 Passive Approaches

A closed-loop system can have limited fault-tolerance by means of a carefully chosen feedback design, taking care of effects of both faults and system uncertainties. Such a system is sometimes called a passive fault-tolerant control system (Eterno *et al.*, 1985; Stengel, 1991). Although there are systems in which a specially fixed controller can compensate for the effects of certain faults, usually information about the fault nature and location is required before the controller is able to react to the fault.

Passive approaches make use of robust control techniques to ensure that a closed-loop system remains insensitive to certain faults using constant controller parameters and without use of on-line fault information (Eterno *et al.*, 1985). The impaired system continues to operate with the same controller and system structure, i.e. the main objective is to recover the original system performance. The scheme effectiveness depends upon the robustness of the nominal (fault-free) closed-loop system.

The system is made "robust" to faults by assuming a restrictive repertoire of likely faults (usually one fault!) and the way in which they affect the control function. This is suitable in restricted cases, perhaps when a fault has a small effect on the system.

Passive fault-tolerance can be used in connection with *reliable control* (Birdwell *et al.*, 1986; Veillette *et al.*, 1992). Although reliability is an idealistic goal

requiring repeatability of system stability and performance, there has been a growing interest in robust design methods which seek to maintain a constant controller design under certain "loop failures". The system is over-designed, making use of the available functional redundancy so that the closed-loop behaviour is optimal when a sensor signal is removed. The design uses "inferred measurements" (analytical redundancy in the FDI literature) i.e. generating estimates of dissimilar quantities using available (healthy measurements).

For any control system, the robustness against disturbances and modelling errors is a difficult but basic requirement, because it is impossible to get a perfect match between the mathematical model and the real process, and to describe disturbances introduced by sensors, actuators, and plant components precisely. If the effects of faults are similar to those of modelling errors and disturbances, the robustness ability can also be used to develop controllers to be insensitive to certain faults. In practical applications, some faults have the effect of deviations on system dynamic parameters. These are effectively the multiplicative faults which affect the residual signal as a product of state/or control terms with parameters deviations. Other faults have an additive effect upon the system inputs and/or outputs and therefore affect the residual signals additively; we can refer to these as additive fault signals. In the additive case, if the fault signals are not physically separable from the signals in nominal system signal flow, i.e. with significant difference in frequency band or signal direction etc., it is difficult, sometimes impossible, to use one robust controller to deal with both nominal and faulty conditions. Hence, an FDI mechanism has to be engaged as a "filter" removing all unwanted signals from the system, whilst at the same time accentuating all fault effects to be monitored (detected and isolated). Fortunately there is a well developed field of state estimation for FDI which can provide very fast detection and isolation of faults as long as the faults have an additive effect upon the monitored system.

If it can be guaranteed that a fault will act as uncertainty upon the system in a way which can be bounded, fault-tolerant control can be achieved by a carefully designed robust controller, i.e. the is the so-called passive approach to fault-tolerant control.

Among those who have extended their work on robust control to deal with passive fault- tolerance are Horowitz *et al.*, (1985) and Keating *et al.* (1995) who use quantitative feedback theory, and McFarlane (1988) and Williams *et al.* (1990) who employed the frequency domain approach, based on H_∞ - norm optimisation. Nett *et al.* (1988), Tyler *et al.* (1994), Murad *et al.* (1996), Niemann *et al.* (1997) and Stourstrup *et al.* (1997) present robust design approaches to integrated control and fault estimation based upon the so-called *4 parameter controller*. Whilst this has some attractions, it suffers from two problems as follows:

The main disadvantage of their designs is that they consider large fault effects which do not challenge the robustness problem! A consideration of smaller or *incipient* (hard to detect) faults would have given a more realistic and challenging robustness problem to solve.

Fig. 4.2 shows the 4-parameter controller structure.

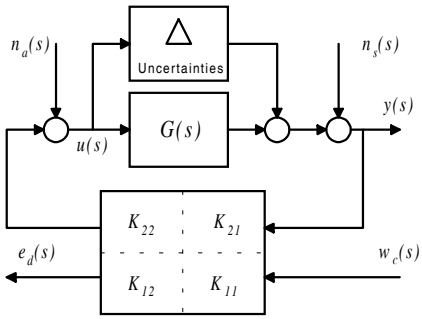

Fig. 4.2 Passive f-t control with fault estimation

Where $G(s)$ is the transfer function matrix of plant, Δ is additive uncertainty, w_c are exogenous inputs, e_d is diagnostic signal, $n_a = f_a + \eta_a$ and $n_s = f_s + \eta_s$ are used to model sensor and actuator noise (n_s, n_a) and faults (f_s, f_a), $u(s)$ is the control signal, $y(s)$ is the output, and K_{ij} are control parameters. The estimated control signal is given by:

$$u(s) = \begin{bmatrix} K_{21} & K_{22} \end{bmatrix} \begin{bmatrix} w_c(s) \\ y(s) \end{bmatrix} \tag{4.1}$$

and the estimated fault signal is given by:

$$e_d(s) = \begin{bmatrix} K_{11} & K_{12} \end{bmatrix} \begin{bmatrix} w_c(s) \\ y(s) \end{bmatrix} \tag{4.2}$$

The H_∞ optimisation approach is employed to achieve the following properties:

1) Plant output signal tracks reference commands and is insensitive to actuator faults;
2) Diagnostic output signal tracks actuator faults (abrupt and slow ramp-type faults);
3) Properties (1) and (2) hold in the presence of a bounded uncertainty.

Most studies using the 4 parameter controller are based upon actuator faults. However, if there is a sensor fault, the situation changes, no guarantee for performance and stability is then available.

In this integrated (fault estimation and control) design the closed-loop signals (reference input and system output) are used for the fault detection. This makes the fault detection task difficult as there is bi-lateral coupling between the controller and fault estimation (or FDI) robustness. The robust controller can de-sensitise the fault estimation and conversely faults can destroy controller robustness.

A further disadvantage of the 4-parameter controller approach is that, by combining together the roles of fault diagnosis and control into one design we have difficulty in knowing how to balance the degrees of design freedom.

The advantage of separate designs of fault diagnosis and robust control is that their separate robustness problems can be optimised; whilst the controller affects the robustness of fault detection and isolation, the "open-loop" approach to fault diagnosis does not in any way affect the controller design. Hence, by separate designs of controller and diagnosis functions, the degrees of freedom in controller design are not compromised.

In general, passive fault-tolerant control does not involve the joint estimation of control and fault signals. The basic idea of passive fault-tolerance is to make the closed-loop system robust against uncertainties and some very restrictive repertoire of likely faults. However, in many practical situations, the use of robust control alone to achieve fault-tolerance may be quite a risky thing to do. As a non--intelligent controller, without the use of diagnostic information and with no knowledge of fault occurrence - where and how serious the fault is - the passive system will have a very limited fault-tolerance capability. Basically, the passive controller will reject the fault only if can be de-sensitised to the fault effect just as if it were a source of modelling uncertainty.

All signals which are controller inputs/outputs have their roles in system stability and performance achievement. Hence, no guarantee of stability and performance can be made, if the impaired signals are used in the closed-loop system. This is true even though it is said that the controller can be robust against some special kinds of faults. Without the use of FDI, the system's fault-tolerance is limited.

All the passive fault-tolerant controllers are actually good examples of *baseline controllers* which can be used further in fault-accommodating (or active) controllers. The robustness being important during the detection and reconfiguration interval.

A robust baseline controller has a degree of passive fault-tolerance for a limited range of fault effects. For more significant faults the controller requires reconfiguration, re-scheduling or restructure.

4.3 Active approaches

Active fault-tolerance has this title because on-line fault accommodation is used. Active fault-tolerant controllers are generally variable in their structure. Whilst all use the concept of unanticipated faults, some use the FDI function and others do not. Some use a baseline controller and some do not.

We can more usefully classify active fault-tolerant control methods as to whether or not they are:

a) based on off-line (pre-computed) control laws;
b) on-line fault-accommodating;
c) tolerant to *unanticipated* faults using FDI;
d) dependent upon use of a baseline controller

The philosophies behind the various active methods are so different that it is sometimes difficult to use the above classification.

On-line restructuring or reconfiguration of control is a topic of ongoing research. For example, Huber *et al.* (1984) designed a self-repairing control system that utilised a *control mixer* concept to distribute control authority to remaining effectors, after a surface malfunction has occurred. Ostroff *et al.* (1984) applied a command-generator/proportional-integral filter control law to an experimental Boeing 707 aircraft at NASA Langley. Rauch (1995) provides the pre-computed control law re-scheduling approach to F/A-18 aircraft. This experimental system had induced control surface faults and was flight-tested under turbulent flight conditions. Looze *et al.* (1985) reported an automatic redesign technique that restructures the control such that a frequency-domain system performance metric is maximised.

Control law re-scheduling

The simplest way of achieving fault-tolerance is to store pre-computed gain parameters. The concept of control law re-scheduling originated in connection with the development of flight control systems. It is considered as a solution for dealing with changes in aerodynamic coefficients whilst the flight status, such as Mach number and altitude, change. In these applications, the re-scheduling mechanism is triggered by measured flight data. This approach is now used in many areas, such as flight control, space control, chemical process control, etc. Theoretical investigations of control law re-scheduling are relatively new (Shamma *et al.*, 1992; Rugh, 1991; Lawrence *et al.*, 1995; Kaminer *et al.*, 1995). This approach is particularly suitable for CRCA aircraft which have a significant level of flight surface redundancy.

The main features of control law re-scheduling are:

1. **Use of FDI Mechanism**
2. **State estimation information used for controller re-configuration**
3. **Control laws (gains or structure) pre-computed and stored**

Moerder *et al.* (1989) developed a realisable scheme using an FDI unit to monitor the system's *control impairment status*, and provides state estimates which are used in an optimal gain scheduling scheme. The latter is based on a proportional & integral controller with a feedforward processing element switches off control surface command error integrators as surfaces are taken out of the system.

Control law re-scheduling can be viewed as a system with feedback control where the feedback gains or structure are adjusted by feedforward compensation. It is clear that this adjustment is an open-loop action, because there is no feedback from the closed-loop

system performance to compensate the action of an incorrect re-scheduling. It implies that the correct operation of control law re-scheduling relies very much on the robustness of the FDI mechanism. Any false or missed alarm, or incorrect isolation may induce a disaster to the stability and performance of closed-loop systems.

Motivated by this robustness issue, Zheng *et al.* (1997) have developed another way of developing fault-tolerant control, based on FDI information. In their approach the theory of LMI is used to synthesise the control feedback as a function of "fault effect vectors". The latter are derived from the residual vector of the FDI mechanism. Whilst synthesising the controller, their approach also takes into account modelling errors and inaccuracies of the fault effect vectors as a robustness problem. The approach has been demonstrated on a longitudinal motion flight control system for an unmanned aircraft with non-linear dynamics.

Feedback Linearisation

Linear controllers generally work well for small variations of state or control variables. However, when an aircraft suffers a malfunction, coupled motions should be taken into account when restructuring the controller. The concept of *feedback linearisation* can be used to compensate for these non-linear dynamic effects, whilst also enabling flight control restructuring. Fig. 4.3 illustrates a typical flight control scheme.

During a control effector malfunction, the coupling between the lateral and longitudinal dynamics can become significant as non-linearities begin to effect the aircraft dynamic behaviour. Feedback linearisation is an established technique in flight control (Meyer *et al*, 1984; Smith *et al*, 1987; Lane *et* al, 1988 and Ochi & Kanai, 1991)

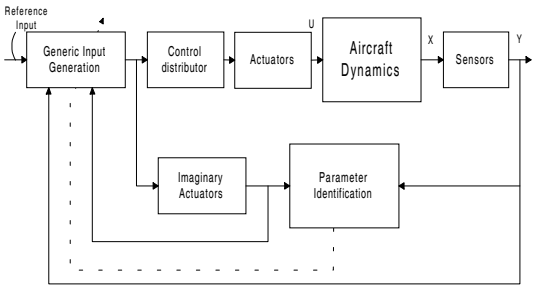

Fig. 4.3 Feedback Linearistion Approach

The faults are identified indirectly by estimating the parameters of the aircraft equations of motion in discrete-time using recursive least-squares. This way of fulfilling the FDI function can be related to the parameter estimation approach of Isermann (1984). The estimated parameters are used to update the new parameters of the controller. A important feature of feedback linearisation is the combined use of a *control distributor* (CD) and *generic inputs* (GI) (Ochi *et al*, 1991).

Recall that in active flight control it is desirable to have many control effectors independently driven to accommodate faults. During the design the number of inputs must be at least equal to the number of outputs to be controlled. The CD is introduced to reduce the real input vector to the GI vector which has the same number of elements as the output vector. When faults occur, the control law (rather than the CD) is changed using non-linear adaptation based on the parameter changes. As a CRCA has a large number of parameters, difficulties can arise in parameter identification due to independence of the longitudinal and lateral control variables. By using the GI in the identification procedure, problems arising from coupled motions are alleviated. However, the GI must be modified when real inputs are structured so that parameters can be identified correctly.

Ochi *et al.* also considered the actuator dynamics and use the concept of the *imaginary actuator* to generate a particular GI signal.

Model-following Approaches

Model-following is an alternative to feedback linearisation. There are basically three strategies as follows (with basic fault-tolerance properties):

Explicit (Morse *et al.,*1990): Limited on-line fault accommodation; no baseline controller; no FDI mechanism; capability of distributing control effort amongst effective control surfaces;

Implicit (Huang *et al.,* 1990): Very limited accommodation to control surface malfunctions; no baseline controller; limited use of simple FDI mechanism; emphasis on maintaining the nominal system eigenstructure (can be classed as robust);

Multiple model Kalman filtering (Napolitano et al., 1991): Multiple-model Kalman filtering used to estimate dynamics of damaged vehicle; limited use of simple FDI procedures.

Model-following is an attractive candidate for the redesign process associated with fault-tolerant control because the goal is to emulate the performance characteristics of a desirable model, with or without faults or failures. The ideal form of model-following is perfect model-following (PMF) in which the behaviour of the system can be completely specified (Erzberger, 1968). The Erzberger conditions are actually very restrictive since most systems have more states than inputs. An approximation to PMF can be accomplished *explicitly* (by requiring system outputs to follow those of the model in a least-squares sense) or *implicitly* (by minimising a quadratic function of the actual and modelled state rates) (Erzberger, 1968; Tyler, 1970).

Explicit model-following is normally less sensitive to parameter variations, but the model states must be generated, and feedback gains may be high for satisfactory performance. Implicit model-following on the other hand can be implemented more simply with lower gains, and the weighting matrices are

directly affected by the difference in plant and model dynamics.

The idea of controlling an impaired system so that it is "close", in some sense, to the nominal system, has been explored in numerous papers (Caglayan *et al.*, 1988a; Huber, 1984; Ostroff, 1985; Rattan, 1985; Gao & Antsaklis, 1990, 1991). The model-following reconfigurable flight control (MFRFC) system was first proposed by (Huang *et al.*,, 1990) who considered the suitability of the *Implicit Model-following Method* for reconfigurable control. Following this, (Morse *et al.*, 1990) described a scheme utilising a multi-variable model-following adaptive controller to directly adjust the controller gains in real time to force the plant to follow the trajectories of a desired model. The MFRFC system has the capability of distributing the control effort implicitly amongst the aircraft's effective surfaces without explicit knowledge of the malfunction.

Explicit knowledge that a fault has occurred is not needed for reconfiguration using this approach, direct reliance on FDI is removed and so is the danger that false alarms can have upon reconfiguration. On the other hand, it removes the necessity for a baseline controller, which provides good robustness during FDI time delays (Mariton *et al.*, 1989).

In their MFRFC scheme, Morse *et al.* made use of the Model-Following Adaptive Controller (MFAC) proposed by Sobel *et al.* (1982), which is based on the command generator tracker of O'Brien *et al.* (1980). This model-following adaptive controller has the following structure. The model which possesses the desired dynamic response is given by:

$$\left.\begin{aligned} \dot{x}_M &= A_M x_M(t) + B_M u_M(t) \\ y_M &= C_M x_M(t) \end{aligned}\right\} \qquad (4.3)$$

The model of the system or plant under control is given by:

$$\left.\begin{aligned} \dot{x}_P &= A_P x_P(t) + B_P u_P(t) \\ y_P &= C_P x_P(t) \end{aligned}\right\} \qquad (4.4)$$

where $A_M, A_P \in R^{n\times n}$, $B_M, B_P \in R^{n\times m}$, $x_M(t), x_P(t) \in R^{n\times m}$, $C_M, C_P \in R^{q\times n}$, $u_M, u_P \in R^{m\times l}$, and $q < m$. It is assumed that the plant matrices A_P and B_p and the initial states are unknown. The adaptive control law that forces the plant output to track the output of the model is given by:

$$\begin{aligned} u_P &= K_x x_M(t) + K_u u_M + K_e \left[y_M(t) - y_P(t)\right] \\ &= \left[K_l + K_p\right] s(t) \end{aligned} \qquad (4.5)$$

where:

$$s^T = \left\{ \left[y_M(t) - y_P(t)\right]^T, y_M^T(t), y_P^T(t) \right\} \qquad (4.6)$$

$$\left.\begin{aligned} K_P(t) &= e_y(t) s^T(t) \Gamma \\ K_l(t) &= -\mu K_l(t) + e_y(t) s^T(t) \Omega \end{aligned}\right\} \qquad (4.7)$$

where, $e_y(t) = y_M(t) - y_P(t)$ is the tracking error, Ω is a square *positive definite matrix*, and Γ is a square *positive semi-definite matrix*. The adaptive gains have been given the basic form corresponding to a proportional-plus-integral controller. The tracking error $e_y(t)$ can be shown to be asymptotically stable using *Lyapunov's second method*, provided that the plant can be stabilised using constant output feedback. Morse *et al.* (1990) provide a detailed discussion of how suitable stability properties can be achieved. They also describe the construction of a stability augmentation loop incorporating feed-forward action so that the MFAC scheme can be applied to non-minimum phase plants. However, with the feed-forward augmentation it is only possible to guarantee that tracking errors are bounded; there is no guarantee of asymptotic stability.

Morse *et al.* (1990) outline the difficulties involved in formulating a methodological process to optimise the elements of the required matrices. They proceed to give some general guide-lines, based on an example of reconfigurable flight control, based on a simulation of an experimental aircraft - the AFTI/F-16. In their study they considered only one type of fault, namely, a control surface that is centred and stuck. This is modelled by zeroing out its respective surface command input column vector within the input B_M matrix. They chose this fault type because of its modelling simplicity and its use as a standard test case in other reconfiguration studies. In their study they simulated:

(a) a right horizontal tail surface fault,
(b) double flaperon and rudder faults,
(c) double horizontal tail surface faults

They show that their proposed adaptive proportional-plus-integral MFRFC system can maintain performance, even in the presence of quadruple faults
Limited FDI - faults identified indirectly using parameter estimation; feedback linearisation based on parameter estimates.

Pseudo-inverse modelling methods

According to Gao *et al.* (1991), a viable alternative to the model-following approaches, a reconfigurable control approach known as the pseudo-inverse method (PIM) has been used reasonably well in flight simulation studies by (Huber *et al.*, 1984; Caglayan *et al.*, 1988a; Ostroff, 1985 & Rattan, 1985; Raza *et al.*, 1985). The PIM principle is to modify the constant feedback gain so that the reconfigured system *approximates* the nominal system in some sense. This method uses no FDI mechanism and certain fault models are assumed. The objectives of PIM in reconfigurable control are to:

a) maintain as much simplicity as possible in the controller design,
b) reconfigured system made to approximate nominal system closely, and
c) provide graceful degradation in performance, subsequent to a fault.

The open-loop plant model is given by Eq. (4.4). Assume further that the closed-loop system is designed using state-feedback with control law:

$$\boldsymbol{u = K_p\, x_p} \tag{4.8}$$

with $\boldsymbol{K_p \in R^{m\times n}}$ The nominal closed-loop plant system is thus:

$$\left.\begin{aligned} \dot{\boldsymbol{x}}_{\boldsymbol{P}} &= \left(\boldsymbol{A_P + B_P K_P}\right)\boldsymbol{x_p} \\ \boldsymbol{y_P} &= \boldsymbol{C_P\, x_P(t)} \end{aligned}\right\} \tag{4.9}$$

Suppose that the model of the system, in which faults are assumed to have occurred, is given by:

$$\left.\begin{aligned} \dot{\boldsymbol{x}}_{\boldsymbol{f}} &= \left(\boldsymbol{A_f + B_f K_f}\right)\boldsymbol{x_f} \\ \boldsymbol{y_f} &= \boldsymbol{C_f\, x_f(t)} \end{aligned}\right\} \tag{4.10}$$

where $\boldsymbol{K_f}$ is the *new* feedback gain matrix to be determined. The main idea of PIM is to modify the constant feedback gains of the nominal system, so that the reconfigured system *approximates* the nominal system in some well defined sense. This is attractive because of simplicity in computation and implementation. A measure of closeness between systems before and after a fault is the Frobenius norm of the difference between the closed 'A' matrices. Gao *et al.* (1990, 1991) showed that by minimising this norm, the bound in the variations of closed-loop eigenvalues due to faults is minimised.

There are several variants of the PIM method. Some fit into the category of active fault-tolerant control, others may be better classified as passive methods. The method due to (Ostroff, 1985) is based on the determination of $\boldsymbol{K_f}$ such that the closed-loop state transition matrix for the system derived from Eq.(4.10) approximates in some sense the transition matrix of the normal plant described by Eq.(4.9). Hence, we can require that the two closed-loop system matrices $\left(\boldsymbol{A_P + B_P\, K_P}\right)$ and $\left(\boldsymbol{A_f + B_f\, K_f}\right)$ are equated so that an approximate solution for $\boldsymbol{K_f}$ is given by:

$$\boldsymbol{K_f = B_f^{+}\left(A_P - A_f + B_P\, K_P\right)} \tag{4.11}$$

where $\boldsymbol{B_f^{+}}$ denotes the pseudo-inverse of $\boldsymbol{B_f}$ which can be defined using a *singular value decomposition* of $\boldsymbol{B_f}$. $\boldsymbol{K_f}$ can be calculated from Eq.(4.11) for many anticipated faults and be stored in the flight-control computer. Once the fault has been detected, isolated and identified (i.e. the model of the faulty system is obtained), the feedback gain is modified. This is a relatively fast solution to stabilise the impaired aircraft. This method has been used for anticipated faults see (Caglayan *et al.*, 1988b; Huber *et al.,* 1984; Ostroff, 1985; Rattan, 1985).

There is a severe drawback of the PIM method (in its original form) which limits its applicability (Gao *et al.,* 1991). The stability of the impaired system is not guaranteed and this may lead to undesirable effects in certain fault scenarios. To attempt to overcome this stability problem Gao *et al*. (1991) also describe a modified pseudo-inverse method (MPIM) in which the difference between the closed-loop 'A' matrices is minimised subject to stability constraints, whilst recovering the performance as much as possible.

The MPIM is based on results on the stability robustness of linear systems with structured uncertainty (Bartlett *et al.*, 1988; Barmish, 1988; Yedavalli, 1988; Zhou *et al*., 1987) as a constraint minimisation problem. It is first assumed that $\left(\boldsymbol{A_f, B_f}\right)$ form a stabilisable pair. If this assumption is not valid, stabilisation can be achieved using an inner-loop *stability augmentation.* The modification is based upon a consideration of structured uncertainty in the state-space model, i.e. by considering the perturbed state-space model, with perturbation matrix $\boldsymbol{\Delta A_p}$, such that:

$$\left.\begin{aligned} \dot{\boldsymbol{x}}_{\boldsymbol{P}} &= \left(\boldsymbol{A_P + \Delta A_P}\right)\boldsymbol{x_P(t)} + \boldsymbol{B_P\, u_P(t)} \\ \boldsymbol{y_P} &= \boldsymbol{C_P\, x_P(t)} \end{aligned}\right\} \tag{4.12}$$

It is assumed that a stability bound can be found such that if

$$\left|\boldsymbol{\bar{K}_f(i,j)}\right| < \boldsymbol{\delta}\,,\ (\boldsymbol{i=1,2,..,m\ \&\ j=1,2,...,n}) \tag{4.13}$$

then the system in (4.10) will be stable. Gao & Antsaklis (1991) describe in more detail how the bound $\boldsymbol{\delta}$ can be derived using Zhou's method (1987) or Yedavalli's method (1988). The algorithm for the MPIM reconfigurable control system is as follows:

Step 1 Calculate $\boldsymbol{K_f}$ from Eq. (4.11)

Step 2 Check the stability of Eq. (4.10) for the $\boldsymbol{K_f}$ obtained in Step 1

Step 3 If (4.10) is stable, stop; otherwise calculate $\boldsymbol{K_f}$ using

$$\boldsymbol{K_f} = \begin{cases} \boldsymbol{\bar{K}_f(i,j)} & \boldsymbol{if\ \left|\bar{K}_f(i,j)\right| \le \delta} \\ \boldsymbol{sgn\left(\left|\bar{K}_f(i,j)\right|\right)\,\delta} & \boldsymbol{otherwise} \end{cases} \tag{4.14}$$

McLean *et al.* (1991) used the same philosophy of PIM reconfiguration. Their idea is to redistribute the control commands in order to improve the closed-loop system stability. They proposed the *weighted control redistribution* method which actually falls more closely in line with the projection-based reconfiguration. After inspecting their method it becomes clear once again that closed-loop stability is still not guaranteed, in some cases.

There are however, two further limitations of PIM approaches:

Robustness in FDI: The PIM approaches make no explicit use of the robustness properties of the detection, isolation and identification of faults and they depend very much on the ability of the supervision system to determine the *fault signature*. Unfortunately, this is a very difficult problem which is overwhelmed by uncertainty not just in control - but also in fault detection and isolation!

Limitation to sate feedback: Unfortunately, the PIM theory has only been worked out on the assumption that the system to be reconfigured has a state feedback structure. For many real applications of control the state variables are not available so that, output feedback control is the only way to stabilise the plant. As output feedback severely restricts the freedom available in achieving either stability of performance robustness, the PIM approach becomes severely restricted.

The alternative use of state estimate feedback is troubled by loop-transfer recovery problems, unless specially designed robust observers are used. The use of robust observers can become a part of the robust FDI problem, although this aspect is seldom considered in the literature.

Unfortunately, when all these problems are considered, the PIM and MPIM methods are not as realistic and practically realisable as one may think at first sight.

There is an interesting link between the PIM (or MPIM) approach and linear model-following (LMF) for reconfigurable control. In both cases the plant is forced to attempt to follow a reference system, although in with LMF the plant *approximates* the reference model (e.g. using the output trajectory). In the MPIM case, the impaired system *imitates* the nominal system in terms of a norm or 'closeness' of the closed-loop state space 'A' matrices.

Hybrid Adaptive Linear Quadratic Control

An adaptive control approach which obviates the use of FDI procedures has been proposed by Ahmed-Zaid *et al.* (1991) who described the augmentation of a flight control system using a hybrid adaptive linear quadratic control (HALQC) scheme. This approach has an on-line capability of learning and accommodating to "drastic" changes in the aircraft dynamics, due to surface or hardware faults.

Their adaptive control system was designed for the reduced-order linearised dynamics of the AFTI/F-16 and was tested using the full-order non-linear model. Emphasis is placed on the use of reduced-order linearised models to decrease the number of adjustable parameters in the adaptive scheme. They use the Hankel Norm model reduction algorithm and verify carefully that the resulting reduced-order model matches the full-order dynamical system model within the frequency range of interest. These careful steps towards model design are made before the adaptive controller design. Although limited to control surface (actuator faults), the method has on-line fault-accommodation capability. No explicit knowledge of faults is required. The feedback system is gain-scheduled but augmented with HALQC.

5 ROLE OF FDI IN FAULT-TOLERANT CONTROL

FDI has an important role in the active way of achieving fault-tolerance. When using direct redundancy, extra hardware channels or components provide additional signals. These can be used to generate residual signals by direct comparison. Voting techniques can be used to indicate and possibly isolate a faulty component.

When analytical redundancy is used (see Section 3) analytical relationships are used to produce additional (or back-up signals, as well as the residual signals. When the system is fault-free, all of the residuals should be close to zero. After a fault occurs, the module that is used for residual generation and decision-making is responsible for finding out the location of the fault. The system can then be reconfigured or restructured so that any non-impaired or healthy channel (or component), or signals will be chosen to take a role in system operation. In some cases, an alternative pre-calculated controller will be activated or the parameters of the controller will be changed according to real time diagnostic information provided by the FDI unit.

The key problem for active fault-tolerant control is on-line reconfiguration (or restructuring) of the controller. For this to be possible detailed information about changes in the system parameters (or changes in the system operating point) due to either normal process changes or component (multiplicative) faults is required. The major task of FDI is to acquire this information, whilst it is the task of a supervision system to manage the controller reconfiguration (for example, by model-selection based upon FDI unit information). There is now an increasing interest in steps towards integrating the FDI mechanism efficiently into the design of a fault-tolerant controller (Jiang, 1994a; Kobi *et al.*, 1994; Chandler *et al.*, 1995; Åström, 1996).

At present, many reconfigurable controllers use real time estimates of system parameters provided by parameter estimation based FDI. It is often claimed that the parameter estimation approach to FDI can provide the controller with system information in a format more suitable for on-line reconfiguration than through the alternative approach to FDI based upon state estimation. Unfortunately, there are still many difficulties along the route to getting reasonably accurate parameters on-line. In order to get good estimates, it may be necessary to introduce perturbation signals to make sure that all the plant's modes are sufficiently excited. However, in many practical applications, it is impossible to apply additional perturbation signals. Additionally, the

parameter estimation algorithms are quite complicated and computationally time consuming. Furthermore, in many cases, the system model structure will change due to the faults. This is in turn causes further problems in achieving suitably accurate estimation.

In order to overcome the disadvantages of using parameter estimation, researchers are trying to use: (I) different controller reconfiguration mechanisms based on other kinds of FDI information (Rauch, 1995; Jiang, 1994b); (II) alternative ways to provide FDI information more efficiently and in ways more suited to the reconfiguration mechanism (Narendra *et al.*, 1990; Gevers, 1993; Van den Hof, 1995).

In addition to the signal and parameter estimation and residual generation, the FDI unit is also expected to provide more detailed information about faulty conditions. Recently, researchers have been trying to make the best use of all the information given by FDI to improve the ability of on-line controller reconfiguration (Noura *et al.*, 1993; Jiang, 1994a; Polycarpou *et al.*, 1995).

For some real applications, the possibility of occurrence of some kinds of faults is much smaller than that of others. However, no one can guarantee that faults with small possibility will not occur. In some iterative approaches for on-line reconfigurable controller design, as a consequence of considering just some special faults, explicit knowledge about the nature, location and the time of fault occurrence is not needed. However, the reliability of the operation of such iterative methods must be guaranteed by the use of an FDI unit. This implies that reconfiguration mechanisms of this type can be activated only by the decision that a fault has occurred (using an FDI unit).

Thus, the FDI mechanism appears to be quite necessary in a fault-tolerant control system.

5.1 FDI approaches & diagnostic information

Over the past two decades, many kinds of FDI approaches have been developed. Of these approaches, there are quantitative model-based approaches (Willsky, 1976; Mironovski, 1980; Walker, 1983; Isermann, 1984,1994; Himmelblau, 1986; Basseville, 1988; Gertler, 1988, 1991; Frank, 1990,1994,1995; Patton, 1991,1993,1994,1996) and books: (Himmelblau, 1978; Patton *et al.*, 1989 and 1997; Brunet *et al.* 1990; Pouliezos *et al.*, 1994), qualitative model based approaches (Arkin *et al.*, 1990; D'ambrosio, 1989; Dvorak *et al.*, 1989; Falkenhaimer *et al.*, 1988; Mavrovouniotis *et al.* , 1990; Pearce, 1988; Travé-Massuyes *et al.*, 1990; Leitch *et al.*, 1992), and knowledge based approaches (Hayes-Roth *et al.*, 1983; Bobrow *et al.*, 1984; Passino *et al.*, 1988; Tzafestas, '89, '94)

In order to design the controller, precise knowledge about the plant dynamic model should be known *a priori*. The same information is required for reconfiguring the control system. On considering these requirements, more emphasis has been traditionally placed upon quantitative model-based FDI approaches as these are reliant on detailed knowledge of system dynamic model and may finally provide more details about the changes in system dynamics, in keeping with the requirements for reconfiguration and closed-loop adaption.

The major emphasis therefore in the field of quantitative model-based FDI has been placed upon methods of detecting and isolating faults rapidly and accurately. There is an increasing research interest into answering the question of how the diagnostic information can be used more efficiently to compensate for or counteract the effects of *some* faults, rather than others - thus giving strong fault isolation possibilities, whilst taking care of modelling uncertainties (Chen & Patton, 1996).

At present, most FDI approaches can only provide a fault alarm or quite limited information about the nature of faults, such as which sensor or actuator is impaired, and how large the fault signal is. Most methods are also restricted to the assumption that the faults are additive on the system (i.e. sensor or actuator but not component faults).

Few studies have considered how much further information can be provided by the FDI unit. Similarly, there is little information available about the kind of fault information (for a particular application domain) that may be required by different reconfigurable controllers. It is clear therefore that mechanisms for achieving a systematic integrated design of both the FDI unit and the reconfigurable controller scheme are still awaited.

Model-based fault diagnosis can be defined as the detection, isolation and determination of the characterisation of faults in components of a system from a comparison of its available measurements, with *a priori* information represented by the system's mathematical model. Faults are detected by setting a (fixed or variable) threshold on a residual signal generated from the difference between real measurements and their estimates using the mathematical model. The generalised way of doing this is given by Eq. 3.3. A number (or vector) of residuals can be designed with each component having special sensitivity to specific faults (or sets of faults) occurring in different locations in the dynamic system. The subsequent analysis of each residual, once a threshold is exceeded, then leads to fault isolation and also fault categorisation.

The major sub-classes of model-based FDI (using quantitative models) are state estimation approaches (using state or output observers), parameter estimation approaches, and parity equation approaches.

5.2 Robustness problem for FDI

All the quantitative model-based approaches require that the process can be described by a time-domain or frequency domain mathematical model.

Unfortunately, there is almost never an exact agreement between the process and its model. As model-based FDI is based upon the use of mathematical models of the supervised system, the FDI function performance is always deteriorated by modelling errors and disturbances. Hence, the robustness of FDI against modelling uncertainty is of primary interest.

Put another way, the main property of interest in the FDI function is the achievement of a low missed-alarm and low false-alarm rates. If a fault occurs and the FDI unit cannot confirms this accurately, then the controller, which is normally suitable for the fault-free system, has to take up a new role in the faulty condition. In this case, there is a risk of loosing system stability or deteriorating system performance seriously.

If there is a false-alarm which triggers the reconfiguration mechanism to adjust the controller on-line, it may give rise to a risk of putting an unsuitable controller into closed-loop action.

The FDI robustness implies that residuals must be only *certain* sensitive to faults, even in the presence of model-reality differences (e.g. parameter variations), turbulence, and the effects of manoeuvres. Clearly, analytical techniques have to maintain conventional system performance and reliability and the robustness problem in FDI is at the heart of this.

FDI system reliability must be higher than the monitored system. The better the model used as a representation of the dynamic behaviour of the system, the higher will be the chance of improving the reliability and performance in detecting and isolating faults.

However, this reliability is limited as perfect modelling is impossible for complex engineering systems, and hence is dependent upon the insensitivity properties of *both* the detection and isolation functions to normal disturbances and effects of system parameter variations. Usually, parameter variations and disturbances act upon a real process in an uncertain way, so that in the presence of modelling errors and disturbances, increasing the fault detection coverage whilst at the same time decreasing the false-alarm rate is a very tough challenge. This problem is now well recognised and one can refer to a number of effective solutions (Frank, 1995; Patton & Chen, 1996; Gertler *et al.*, 1993). There have been several important survey studies on model-based FDI techniques covering a two-decade span (Willsky, 1976; Isermann, 1984; Patton *et al.*, 1989; Frank, 1990; Patton *et al.*, 1995, 1996; Gertler, 1991; and Gertler *et al.*, 1993).

5.2.1 *FDI residual generation robustness*

In order to design robust FDI schemes, we need the description of normal disturbances and system uncertainties (modelling errors) acting upon the system, during typical process plant operation. Considering the basic fact that the characteristics of modelling uncertainty can never be fully known (!), one way of dealing with system uncertainties is to incorporate all of these effects into one signal known as the "unknown input" acting upon the system (Watanabe *et al.*, 1982; Massoumnia, 1986; Frank, 1990; Patton, 1995; Patton *et al.*, 1996). In the context of using *unknown inputs* the system can be described as:

$$\begin{aligned} \dot{x}(t) &= A\,x(t) + B\,u(t) + R_1\,f(t) + E_1\,d(t) \\ y(t) &= C\,x(t) + D\,u(t) + R_2\,f(t) + E_2\,d(t) \end{aligned} \qquad (5.1)$$

where the state variables are $x(t) \in R^n$, the measured process outputs are $y(t) \in R^m$, the control signals are $u(t) \in R^p$, the fault signals are $f(t) \in R^n$ with distribution R_1 or R_2. The unknown inputs representing uncertainty and disturbances are $E_1\,d(t)$ and $E_2\,d(t)$. In the time-domain, disturbance decoupling methods, such as *the unknown input observer* (Kudva *et al.,* 1980) and used in the context of FDI by Watanabe et al. (1982); Massoumnia, (1986); Wünnenberg *et al.*, (1988, 1996)); *eigenstructure assignment* (Patton *et al.*, 1989, 1991, 1996; Duan *et al.*, 1997), and *robust parity equation* approaches, are now well understood. An important assumption upon which these methods are based is that the unknown input distribution matrices E_1 and E_2 must be known *a priori*. Unfortunately, their derivation is, (apart from very simple examples), a very complex problem. The most significant term is $E_1\,d(t)$ and Patton *et al.* (1991,1993, 1995, 1996) have proposed a number of methods for computing E_1, based on the assumption that can be ignored.

In order to achieve disturbance decoupling, the key principle is to find a $p \times n$ matrix H to satisfy the equation $H\,E_1 = 0$. If $rank(E_1) \le n - p$, the equation has solutions and exact disturbance decoupling is possible. However, in practice, as the matrix E_1 is derived via considering all uncertain factors contributing to the unknown input(s) (Chen *et al.*, 1996), it is most often the case that $rank(E_1) > n - p$ and hence the equation $H\,E_1 = 0$ has no solution and *exact* decoupling is impossible. In order to achieve the decoupling, a low rank matrix E_1^* is used to approximate the original matrix E_1 and is then used to achieve $H\,E_1^* = 0$, with the Frobenius norm (chosen for computational convenience) $\left\| E_1 - E_1^* \right\|_F^2$ is minimised.

Even though many successful applications are based on this kind of time domain method (Chen *et al.*, 1996), research into time-domain approaches to robust

FDI is still a very open matter for research. One important aspect for future consideration is that if:

$$Ker\left(R_I^T\right) \cap Ker\left(\left(E_I^*\right)^T\right) \neq \phi$$, considering for example the eigenstructure assignment approaches, fault signals corresponding to some fault mode with respective to:

$$Ker\left(R_I^T\right) \cap Ker\left(\left(E_I^*\right)^T\right)$$ are also de-coupled whilst integrated disturbances have been decoupled. Unfortunately, for a complex system with a many factors of uncertainty, this is a common situation. Hence, the decoupling of a residual from a set of integrated disturbances sometimes makes the residual completely or partially insensitive to some faults.

In the frequency domain, Marquez *et al.* (1992) developed a new observer structure for FDI, based on unstructured uncertainty. However, their work belongs essentially to a class of frequency domain approaches, based on sensitivity optimisation. In an attempt to overcome the limitations on achieving suitable sensitivity imposed by the structure of classical state observers, Marquez *et al.* were motivated to find a new generalised observer structure which provides additional degrees of freedom in shaping the observers sensitivity to unknown inputs. They gave a parametrisation of all stabilising generalised observers, through an observer sensitivity minimisation problem, via H_∞ optimisation.

In recent years, frequency domain approaches for FDI design have attracted much attention using H_∞ - based factorisation methods (Ding *et al.*, 1991; Frank (1994); Qiu *et al.*, 1994; or the complete approach to an H_∞ solution (Edelmeyer *et al.*, 1997; Sadrnia *et al.*, 1997).

Chen *et al.*, (1994) proposed a systematic approach based on multi-objective optimisation to robust residual design for detecting incipient faults. To reduce false- and missed-alarm rates, a number of performance indices were introduced into the observer design. Some performance indices are expressed in the frequency domain to take account of the frequency distribution of faults, noise signals and modelling uncertainties. All objectives are reformulated into a set of inequality constraints on the performance indices.

5.2.2 Robustness in decision-making The goal of robust decision-making is to minimise the false- and missed-alarm rates against the effects of modelling uncertainties and unknown disturbances. Emami-Naeini *et al.* (1988) and Frank (1994) reported how efforts to enhance the robustness of FDI can be made at the decision-making stage. Due to inevitable parameter uncertainty, disturbance and noise encountered in a real application, one will rarely find a situation where the conditions for a perfectly robust residual generation are met. This is especially true for unstructured uncertainties. It is therefore necessary to provide sufficient robustness not only in the residual generation stage but also in the decision-making stage. When the decision-making stage of FDI is made robust against uncertainty, we can speak of *passive robustness* in FDI (Patton *et al.*, 1991) in which case it may not be necessary (or it may be difficult) to make the residual robust. Passive robustness can be achieved in several ways, e.g. by statistical data processing, averaging, by finding and using the most effective threshold, or by using fuzzy decision-making techniques (Frank, 1994).

The methods of passive robustness in FDI which have received the most attention are based on the use of adaptive thresholds (Emami-Naeini *et al.*, 1988), i.e. each threshold becomes a function in some way of measurable quantities. Another idea makes use of fuzzy logic techniques for decision-making (Frank, 1993).

6 FDI AND CONTROL ROBUSTNESS INTERACTIONS

In a closed-loop control system, the model-based process of detecting and isolating faults can operate in two different ways depending on the availability of system signals. It is by far the most usual to employ an observer or parity equation FDI in such a way that it has no effect upon the controller function - in other words an "open-loop" approach as shown in Fig.6.1. In this structure, the control command *u(t)* to the actuators is available for the FDI purpose and this signal together with the measured output signal *y(t)* is used to generate a residual signal. When the residual signal exceeds a threshold, the variation is due to either to a fault or to the effect of uncertainty.

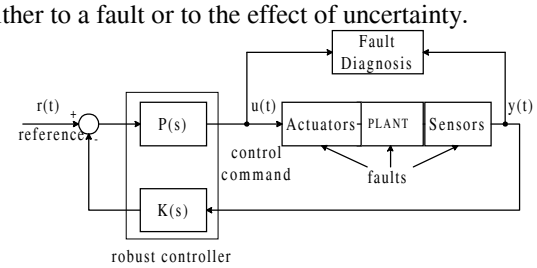

Fig. 6.1 Closed-loop system with "open-loop" FDI

The basic principle of model-based FDI is to check the consistency between the system input and output utilising the input-output relationship provided by the mathematical model. Referring to Fig. 6.1, the relationship between *y(t)* and *u(t)* is described by the **open-loop** system model which means that the FDI system can be designed *separately*. Using this approach in contrast to the 4-parameter controller approach of Nett *et al.* (1988) (the work of Area 5 in Fig. 2.1 and under Section 4.2), the FDI unit has no effect on the controlled system. In the alternative approach of Fig. 4.2, the robust control and fault signals are estimated using a robust estimator. In this case there is a clear two-way interaction between the

robustness of the residual signal to uncertainty and the controller robustness to uncertainty. This is seen by the FDI community as a clear disadvantage under the goal to achieve reliable fault diagnosis for reconfigurable control.

Whilst the "open-loop" form of FDI (Area 1 in Fig. 2.1) has no effect upon the controller, the control signal directly influences the FDI residual when there is modelling uncertainty present. A robust controller can then have the effect of *de-sensitising* the residual signal to faults and ruin the FDI unit's capability of detecting and (more particularly) isolating incipient faults (Wu, 1992). To overcome this difficulty, some extra constraints must be imposed on the controller robustness, i.e. to make the FDI system sensitive to faults and at the same time insensitive to the control signal and to the uncertainty.

It is feasible to design the robust control and FDI systems together by optimising a set of mixed control and fault detection/fault isolation objectives. Due to the extra design constraints imposed, the performance and stability robustness of approaches based upon the 4 parameter controller structure ("closed-loop" approach) of Nett *et al.* (1988) it will not, in general be possible to achieve the same level of robustness from the controller as would be possible via the system with separately designed controller and FDI systems. This structure should be avoided in the fault-tolerant control system configuration.

The effect the control signal has on the "open-loop" FDI residual can be seen through the following simple analysis based upon an observer-generated residual.

Consider the model of Eq. (6.1) with the variables defined in Eq. (5.1):

$$\begin{aligned} \dot{x} &= A\,x + B\,u \\ y &= C\,x + D\,u \end{aligned} \tag{6.1}$$

The real plant dynamics are:

$$\begin{aligned} \dot{x} &= A_p + B_p\,u + R_1\,f \\ y &= C_p\,x + D_p\,u + R_2\,f \end{aligned} \tag{6.2}$$

where $A_p = A + \Delta A$, $B_p = B + \Delta B$, $C_p = C + \Delta C$, $D_p = D + \Delta D$.

The observer dynamics are:

$$\left.\begin{aligned} \dot{\hat{x}} &= A\,\hat{x} + B\,u - L\,C\,\hat{x} + L\,y \\ \hat{y} &= C\,\hat{x} + D\,u \end{aligned}\right\} \tag{6.3}$$

Then, we have:

$$\begin{aligned} \dot{e} &= \dot{x} - \dot{\hat{x}} \\ &= A_p\,x - A\,\hat{x} + B_p\,u - B\,u + \left(R_1 - L\,R_2\right)f \\ &\quad + L\,C\,\hat{x} - L\,C_p\,x + L\left(D - D_p\right)u \\ &= \left(A - L\,C\right)e + \left(R_1 - L\,R_2\right)f \\ &\quad + \left(\Delta B - L\,\Delta D\right)u + \left(\Delta A - L\,\Delta C\right)x \end{aligned} \tag{6.4}$$

The Laplace transformed residual vector is given by:

$$\begin{aligned} r(s) &= W e(s) \\ &= W\{R_2 + C\left(sI - A + LC\right)^{-1}\left(R_1 - L\,R_2\right)\}f(s) \\ &\quad + WC\left(sI - A + LC\right)^{-1} \\ &\quad \left(\left(\Delta B - L\,\Delta D\right)u(s) + \left(\Delta A - L\,\Delta C\right)x(s)\right) \end{aligned} \tag{6.5}$$

where W is a $\in R^{pxm}$ design weighting matrix. From Eq. 6.5 we see that because of modelling errors and system non-linearity, the control signal $u(s)$, which is also input to the FDI observer, will affect the estimation error $e(s)$, and hence also the residual signal $r(s)$ which is a function of $e(s)$. The terms $\left(\Delta B - L\,\Delta D\right)u(s)$ and $\left(\Delta A - L\,\Delta C\right)x(s)$ here work as additive disturbances to the residual generator and compete with fault signal, thereby making the discrimination between faults and uncertainty a difficult problem. Put another way, the residual generation becomes de-sensitised to faults through the effect of modelling uncertainty, with the term $\left(\Delta B - L\,\Delta D\right)u(s)$ illustrating the special effect that the controller has upon the residual. The smaller the control deviations the lower the effect of the control on the FDI, and so on.

7 SUPERVISION

Supervsion for fault-tolerant control is actually the least developed of the areas shown in Fig 2.1. However, a variety of schemes of supervision have been developed for managing diagnostic information and on-line redesign or restructure of the controller These studies use wide-ranging methodologies - from the use of FMEA (Blanke *et al*, 1997) to ideas based upon the use of intelligent computing (Rauch, 1995; Kwong, 1995; Napolitano *et al.*, 1995; Werbos, 1995), such as fuzzy logic (FL), neuro-computing (NC), genetic algorithms (GA), and probabilistic reasoning (PR). Generally speaking, FL is a methodology for dealing with imprecision, approximate reasoning, rule-based systems and computing with words; NC is based upon system identification, learning and adaptation; GA is systemised random search and optimisation; and PR

inolves decision analysis and management of uncertainty (Zadeh, 1996).

Undoubtedly, the integration of these powerful intelligent computing tools within the framework of fault-tolerant control will give us new scope for research in this area.

8 CONCLUSION

A fault-tolerant control system must be planned carefully and designed using systematic and well integrated procedures. This means that this is a truly multi-disciplinary field of research. This is one reason why it has not fully emerged as a mature field of research. There are significant challenges to be overcome as investigators widen their scope and understanding of the required complexity of fault-tolerant control systems. The subject is not just about tolerating faults but rather more about reliability, redundancy, reconfiguration, robustness and supervision. In addition to system theoretic control and diagnosis concepts, research effort must be expended in examining carefully fault-tolerant system requirements. Some tools for establishing these requirements are possibility analysis for component malfunctions, failure mode and effects analysis, system reliability analysis, reliability distribution and redundancy design.

There are also a number of important areas of research. Fig. 2.1 illustrates these areas and Section 2 has discussed the concepts and results that are widely scattered in diverse literature, making it difficult to establish the precise nature of fault-tolerant control and the directions that should be taken to make it more useful and relevant to the needs of practising engineers and scientists.

A fundamental but ideal requirement is that the reliability of all components of a dynamical system be understood. The possible redundancies (both analytical and parallel) need to be known in order to provide maximum reliability through on-line system repair and tolerance to faults.

The redundancy is used to substitute impaired functions by healthy "backup". It is also used to detect and pinpoint the location of faults in various components - actuators, sensors, computers and other more process-specific components. Without this FDI role, the fault-tolerant capability of control systems is limited. Indeed systems which do not include the FDI function can only be fault-tolerant to some special kinds of faults (in most case just one fault), with minor influence on the closed-loop system. However, in real applications, even though the possibility for some kinds of faults is smaller than it is for others, no one can guarantee that the faults with small possibility will not occur. Hence, the safety conditions for the operation of those control systems must be enhanced through reliable detection and isolation of faults. Reliability of the FDI function actually means that the models used to generate the analytical forms of redundancy must replicate accurately the plant dynamic behaviour. This degree of modelling precision is impossible to achieve in practice and hence there is an accompanying robustness problem in FDI as discussed in Section 4.2.1. The drive towards strong discrimination between the response effects of modelling uncertainty and faults in carefully designed residual signals has been at the heart of a very well defined area of research (Area 1 in Fig. 2.1).

Rapid detection and isolation of faults is necessary to minimise the undesirable effects of detection and reconfiguration delays. These delays lead to serious instability unless the controller which operates at the baseline (the baseline controller) has high integrity and stability and performance robustness.

So robust control is another important function in fault-tolerant control (Area 2 in Fig. 2.1). Many researchers working in robust control have not appreciated that fault-tolerance is as important a challenge as the robustness problems themselves.

However on its own, robust control is a passive way of providing limited tolerance to faults (this is indeed the baseline control function). More powerful approaches require active controller reconfiguration/restructuring over and above the baseline function - Area 3 of Fig.2.1. There must be no false or missed alarms in FDI for the reconfiguration to work correctly. The stochastic nature of this problem means that the active fault-tolerant control system is exceedingly complex.

The paper has reviewed the literature in these various topics and described the areas of overlap - Areas 4, 5 & 6 in Fig. 2.1. Bearing in mind the need for robust FDI, robust baseline control together with reliable and robust reconfigurable control, an important direction for future research is marked by the hatched region of Fig. 2.1. Very few papers considering the fault-tolerant control problem have properly examined the FDI and baseline control functions. It is important to note that whilst the FDI and robust control designs can be integrated, the robustness of the FDI system should not influence the passive robustness of the controller. This has not been the case for the approach based upon the 4-parameter controller. On the other hand when the FDI robustness and robust controller problems are designed using the "open-loop" FDI approach, the FDI robustness does not influence the controller robustness.

With *both* approaches, the controller influences the robustness of the detection and isolation of the faults. This is a topic which investigators can pick up on immediately and produce useful solutions.

The fault-tolerant control system must have a form of supervision system to decide on the severity of faults and select the most appropriate control function (Area 6). This is best done using artificial intelligence -

probably based upon fuzzy rules and fuzzy controller selection.

Finally, it would be helpful to develop the awareness of the issues involved, their complexity and the multi-disciplinarity of this work. To the author's knowledge this is the first paper to bring these issues together albeit in a limited way. There are no easy solutions, but if we can achieve a cross-fertilisation of ideas and concepts into the various areas loosely covered by fault-tolerant control, we will make great progress in this field.

9 ACKNOWLEDGEMENTS:

The author is indebted to members of his research group, Dr Jie Chen, Dr Hassen Benkhedda and Zheng Chen, for many valuable discussions. A special thanks is due to Professor Bruce Walker from the University of Cincinnati for his helpful guidance in field of fault-tolerant control.

REFERENCES

Ahmed-Zaid F, Ioannou P, Gousman K & Rooney R (1991), Accommodation of failures in the F-16 aircraft using adaptive control, *IEEE Con. Sys. Mag.*,**11**(1), 73-78

Antsaklis P J (1995), On Autonomy and Intelligence in Control, *IEEE Con. Sys. Mag.*, **16**(3), 61-62.

Arkin R C & Vachtsefanos G (1990), Qualitative fault propagation in complex systems, *Proc. 29th CDC*, Honolulu, 1509-1510

Åkesson M (1997), Integrated control and diagnostics for a mechanical servo process, *SAFEPROCESS'97,* Hull, 1252-1257

Åström K J (1991) Intelligent Control, *Proc. ECC '91*, Grenoble, 2328-2329

Åström K J (1996) Tuning and Adaptation, *13th IFAC World Congress, San Francisco*, June 30.

Barmish B R (1988), New tools for robustness analysis, *Proc. 27th CDC*, Austin,1-6

Basseville M & Benveniste A (Eds) (1986), *Detection of abrupt changes in signals & dynamic systems*, LNCIS No.77, Springer

Basseville M (1988), Detecting changes in signals and systems - A survey. *Autom.* **24**, (3), 309-326

Basseville M & Nikiforov I V (1993), DEtection of abrupt changes: Theory & application, Prentice Hall

Bell T E (1989), Managing Murphy's law: Engineering a minimum-risk system, *IEEE Spectrum*, June

Bennett S, Patton R & Daley S (1997), Using bilinear motor model for sensor fault-tolerant rail traction drive, *Proc. IFAC SAFEPROCESS'97, 783-788*

Birdwell J D, Castanon D A & Athans M (1986), On reliable control system designs, *IEEE Tr. Sys., Man, & Cyb.*,**SMC-16**, (5), 703-711

Blanke M, Izadi-Zamanabadi R, Bogh S A & Lunau Z P (1997), Fault-tolerant control systems - a holostic view, *J. Con. Eng. Prac.*, **5**, (5), 693-702, May

Bobrow D & Hayes P (1984), Qualitative reasoning about physical systems: An introduction, *Artif. Intel.,* **24**, 1-5

Brunet J, Jaume D, Labarrère M, Rault A & Vergé M (1990), *Détection et diagnostic de pannes: approche par modélisation*, Hermes Press

Buckley A P (1995), Hubble Space Telescope Pointing Control System Design Improvement Study Results*, IEEE Contr. Sys. Mag.*, **15**, (2), 34-42

Caglayan A K, Allen S M & Wehmuller K (1988a), Evaluation of a second generation reconfiguration strategy for aircraft flight control systems subjected to actuator failure surface damage, *Proc. Nat. Aero. & Electron. Conf.,* Dayton, May, 520-529

Caglayan A K, Rahnamai K & Allen S M (1988b), Detection, identification and estimation of surface damage/actuator failure for high performance aircraft, *Proc. ACC'98*

Candau J, de Miguel L J & Garcia-Ruiz J (1997), Controller reconfiguration system using parity equations and fuzzy logic, *Proc. IFAC SAFEPROCESS '87, 1258-1263*

Carpentier T, Litwak R & Cassar J-P (1997), Criteria for the evaluation of FDI systems: Application to sensors location, *Proc. IFAC SAFEPROCESS'97, 1083-1088*

Chandler P (1984), Self-repairing flight control system reliability & maintainability program executive overview, *Proc. Nat. Aero. & Electr. Conf.*, May, Dayton,586-590

Chandler P, Pachter M & Mears M (1995); System-Identification for Adaptive and Reconfigurable Control, *J. Guid. Contr. & Dyn.*, **18**, (3), 516-524

Chen J & Patton R J (1996), Robust fault detection and isolation (FDI) systems, *Contr. & Dyn. Sys*., Mita Press, **74**, 171-223

Chiang C Y & Youssef H M (1995), Neural fuzzy appraoch to F/A-18 Aircraft failure isolation and reconfiguration design, *Proc. Guid. Nav.& Contr., Paper AIAA-95-3179-CP,Baltimore, August*

D'Ambrosio B (1989), *Qualitative process theory using linguistic variables*, Springer-Verlag

Deckert J, Desai M, Deyst J & Willsky A (1977), F8 DFBW sensor failure identification using analytical redundancy, *IEEE Tr. Auto. Contr.* **AC-22**, (5), 795-803

Ding X & Frank P.M (1991), Frequency domain approach and threshold selector for robust model-based fault detection and isolation, *Proc. IFAC Symp. SAFEPROCESS'91*, Baden-Baden, Sept, 307-312.

Doyle J C, Glover K, Khargorekar P P & Francis B A (1989), State space solutions to standard H_2 and H_∞ control problems, *IEEE Tr. Auto. Cont.*, **34**, 831-847

Duan G R, Patton R J & Chen J (1997), A parametric approach for robust fault detection in linear systems with unknown disturbances, *Proc. IFAC Symp. SAFEPROCESS '97, 318-322*

Dvorak D & Kuipers B (1989), Model-based modelling of dynamic systems, *Proc. 11th Joint Conf. Artif. Intell.*, Detroit, 1238-1243.

Edelmeyer A, Bokor J & Keviczky L (1997), A scaled L_2 optimisation approach for improving sensitivity of H_∞ detection filters for LTV systems, *Proc. IFAC SAFEPROCESS '97, 543-548*

Eich J & Sattler B (1997), Fault-tolerant control system design using robust control techniques, *SAFEPROCESS'97*, Hull, 1246-1251

Emami-Naeini A E, Akhter M M & Rock S M, (1988), Effect of model uncertainty on failure detection: the threshold selector, *IEEE Tr. Aut. Contr.*,**AC-33** (2),1106

Eryurek E & Upadhyaya B R (1995), Fault-tolerant Control and Diagnostic for Large-Scale Systems, *IEEE Con. Sys. Mag.*, **15**(5), 34-42

Erzberger H (1968), *Analysis and design of model-following control systems*, *Proc. ACC '68*, 572-581

Eterno J S, Looze D P, Weiss J L & Willsky A S (1985), Design issues for fault-tolerant restructurable aircraft control, *Proc. 24th CDC*, Fort Lauderdale, 900-905

Falkenhaimer B & Forbus K D (1988), Setting up large scale qualitative models, *Proc. Nat. Conf. on Artif. Intel.*

Frank P M & Wünnenberg J (1989) Robust fault diagnosis using unknown input schemes, in: Patton, Frank & Clark, *Fault diagnosis in dynamic systems: theory & application*, Prentice Hall, 47-98

Frank P M (1990), Fault Diagnosis in dynamic system using analytical and knowledge based redundancy - A survey and some new results, *Autom.*, **26**, (3), 459-474

Frank P M (1991), Enhancement of robustness in observer-based fault detection, *Proc. IFAC Symp. SAFEPROCESS'91*, Baden-Baden, 275-287

Frank P M (1993), Advances in observer-based fault diagnosis, *Proc. TOOLDIAG '93*,Toulouse,April, 817-836

Frank P M (1994), Application of Fuzzy Logic Process Supervision and Fault Diagnosis, *IFAC* Symp. *SAFEPROCESS'94, 597-612*

Frank P M (1995), Advances in Fault-tolerance by Model-Based Fault Diagnosis, *Proc. ESF Workshop, COSY'95*, Sept, 1995, Rome

Gao Z & Antsaklis P J (1990), Pseudo-inverse method for reconfigurable control with guaranteed stability, *Proc. 11th IFAC World Congress*, Tallin

Gao Z & Antsaklis P J (1991), Stability of the pseudo-inverse method for reconfigurable control systems, *Int. J Control*, **53**(3), 717-729

Garcia H E, Ray A & Edwards R M (1991), Reconfigurable control of power plants using automata, *IEEE Con. Sys. Mag.*, **11**(1), 85-92

Gelderloos H & Young D (1982), Redundancy management of shuttle flight control rate gyroscopes and accelerometers, *Proc. ACC*, June, 808-811

Gertler J J (1988), Survey of model-based failure detection and isolation in complex plants, *IEEE Con. Sys. Mag.*, **8**(6), December, 3-11

Gertler J J (1991), Analytical redundancy methods in failure detection and isolation, *IFAC Symp. SAFEPROCESS'91*, Baden-Baden, Sept., 9-22

Gertler J J & Kunwer M M (1993), Optimal residual decoupling for robust fault diagnosis, *Proc. TOOLDIAG'93,* Toulouse, April, 436-448

Gevers M (1993), Towards a joint design of identification and control? In Trentelman & Willems (eds), *Essays on Control: Perspectives in the Theory & Its Applications*, 111-151, ECC'93, Groningen, Birkhauser

Hayes-Roth *et al.* (1983), *Building Expert Systems*, Addison-Wesley

Herrin S A (1981), Maintainability applications using the matrix FMEA technique, *IEEE Tr. Rel. **30**(3)*

Huang C Y & Stengel R F (1990), Restructurable control using proportional-integral implicit model-following, *J. Guid. Contr. & Dyn.*, **13**, (2), 303-309

Himmelblau D M (1986), Fault detection and diagnosis - Today and tomorrow, *Proc. 1st IFAC Workshop Fault detection and safety in chemical plants*, Kyoto, 28th Sept - 1st Oct, 95-105

Himmelblau D M (1978), *Fault detection and diagnosis in chemical and petrochemical processes*, Elsevier

Horowitz I (1991), Survey of quantitative feedback theory, *Int. J. Control*, **53**, 255-291

Horowitz I, Arnold P B & Houpis C H (1985), YF-16-CCV Flight control system reconfiguration design using quantitative feedback theory, *Proc. Nat. Aero. & Electr. Dayton*, May, 578-585

Houpis C H, Sating R R, Rasmussen S, Sheldon S (1994), Quantitative feedback theory technique and applications, Int. J. Contr., **59**, (1), 39-70

Huber R R & McCulloch B (1984), Self-repairing flight control system, SAE Tech. paper series 841552, 1-20.

Hunt J E, Pugh D R & Price C J (1995), Failure Mode Effects Analysis - A practical application of functional modelling, *App. Artif. Intel. **9**(1), 33-44*

Isermann R (1984), Process fault detection based on modelling and estimation methods: A survey, *Autom.*, **20,**387-404

Isermann, R (1994), Integration of fault detection and Diagnosis Methods*, IFAC Symposium SAFEPROCESS '94*, Helsinki, 597-612

Isermann R & Ballé P (1996), Trends in the application of model based fault detection and diagnosis of technical processes,13th IFAC World Congress, S Fran., **N**,1-12

Izadi-Zamanabadi R & Blanke M (1997), A ship propulsion system as a benchmark for fault-tolerant control, IFAC Symp. *SAFEPROCESS'97*,26-28 Aug., Hull, 1074-1082

Jiang J (1994a), Design of Reconfigurable Control Systems Using Eigenstructure Assignments, *IJC*, 1994, **59**(2), 395

Jiang J (1994b), Fault detection/diagnosis and controller reconfiguration in dynamic systems, Proc. IFAC Symp. *SAFEPROCESS '94*, Helsinki, 81-86

Kaminer I, Pascoal A M, Khargonekar P P, Coleman E E (1995), A velocity algorithm for the implementation of gain-scheduled controllers, Automatica, **31**(8), 1185-1192

Keating M S, Pachter M & Houpis C H (1995), QFT applied to fault-tolerant flight control system design, Proc. ACC, Seattle, June

Kitamura M (1989), Fault detection in nuclear reactors with the aid of parametric modelling methods, in: Patton et al., *Fault diagnosis in dynamic systems: theory & application*, Prentice Hall

Kobi A, Nowakowski, S & Ragot J (1994), Fault Detection isolation and control reconfiguration, *Maths. & Comp. in Simulation*, **37**, 111-117

Krishnasaami V & Rizzoni G (1994), A survey of oberver-based residual generation for FDI, IFAC Symposium *SAFEPROCESS '94*, Helsinki, June, 34-39

Kudva P, Viswanadham N & Ramakrishna A (1980), Observers for linear systems with unknown inputs, *IEEE Tr. Aut. Contr.* **25**(2): 113-115

Labarrère M & Patton R J (1993), Aircraft sensor failure detection, *Concise Encycl. of Aero. & Space Sys.*, Pelegrin & Hollister (eds.), Pergamon

Lane S H & Stengel R F (1988), Flight control design using non-linear inverse dynamics, *Autom.*, **24**(4), 471-483

Lawrence D, Rugh W (1995), Gain scheduling dynamic linear controllers for non-linear plant, Autom., **31**(3),381

Legg J M (1978), Computerised approach for matrix-form FMEA, *IEEE Tr. Rel., **27**(1), 154-157*

Leitch R, Quek C (1992), Architecture for Integrated Process Supervision, *IEE Proc.-D Control Theory & Applics*, ***139**(3), 317-327*

Looze D P, Weiss J L, Eterno J S & Barrett N M (1985), An automatic redesign approach for restructurable control systems, *IEEE Con. Sys. Mag.*, **5**(2),16-22

Lou X, Willsky A, Verghese G (1986), Optimally robust redundancy relations for failure detection in uncertain system, Autom., **22**(3), 333-344

Maciejowski J M (1989), *Multivariable feedback design*, Addison Wesley

Mariton M (1989), Detection delays, false alarm rates & the reconfiguration of control systems, *Int. J. Con.*,**49**(3), 981

Marquez H J & Diduch C P (1992), Sensitivity of failure detection using generalised observers, *Autom.*, **28**, 837

Massoumnia M A (1986), *A geometric approach to failure detection and identification in linear systems*, PhD thesis, MIT, Dep. Aero. & Astro.

Mavrovouniotis M & Stephanoupoulos G (1990), Formal order-of-magnitude reasoning in process engineering, in Weld & Kleer (eds) *Readings in qualitative reasoning about physical systems*, Morgan Kaufmann

McFarlane D C (1988), *Robust controller design using normalised coprime factor plant description*, PhD Thesis, Univ. of Cambridge

McLean D & Aslam, M (1991), Reconfigurable flight control systems, *Proc. CONTROL 91"*, IEE Pub 332, **1**, 234-242

Mc Mahan J (1978), Flight 1080, *Air Pilot*

Meyer G & Hunt L (1984), Application of non-linear transformations to automatic flight control, *Autom.,* **20**(1), 103-107

Milne R (1987), Strategies for Diagnosis, *IEEE Tr. on Sys. Man & Cy.*, **17**(3), 333-339

Mironovski L A (1980), Functional Diagnosis of Dynamic System - a Survey, Autom. & Remote Control,**41**,1122

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. Guid., Con. & Dyn.*, **12**(3), 325-333.

Morari M & Zafirou E (1989), *Robust process control, Prentice Hall*, New Jersey

Morse W D & Ossman K A (1990), Model-following reconfigurable flight control system for the AFTI/F-16, *J. Guid., Con. & Dyn.*, **13**(6), 969-976.

Murad G A, Postlethwaite I & Gu D-W (1996), A robust design approach to integrated controls and diagnostics, 13th IFAC World Congress, San Francisco,June, **N**, 199-

Napolitano M R & Swaim R L (1991), New technique for aircraft flight control reconfiguration, *J. Guid. Con.& Dyn.*, **14**(1), 184-190.

Narendra K S, Parthasarathy K (1990), Identification and control of dynamical systems using neural networks, *IEEE Tr. Neur. Net*, **1**, 4-7

Nett C N, Jacobson C A, Miller A T (1988), An integrated approach to controls and diagnostics: the 4 parameter controller, *Proc. 1988 ACC, 824-835*

Noura H, Aubrun C, Sauter D & Robert M (1993), A Fault Diagnosis and Reconfiguration Method Applied to a Thermal Plant, *TOOLDIAG'93* Toulouse 995-999

NTSB (1979), National Transportation Safety Board accident report of the American Airlines DC10 crash at Chigao-O'Hare International Airport, *NTAB-AAR-79-17*,

Ochi Y & Kanai K (1991), Design of restructurable flight control systems using feedback linearisation, *J. of Guid., Contr. & Dyn.*, **14**, (5), 903-911

Ochi Y (1993), Application of feedback linearistion method in a digital restructurable flight control system, *J. of Guid., Contr. & Dyn.*, **16**, (1), 111-117

Ono T, Kumamaru T & Kumamaru K (1984), Fault diagnosis of sensors using a gradient method, *Tr. Soc. Instr. & Con. Engin.*, **20**, 22-27

O'Brien M J, Broussard J R (1980), Trajectory tracking for a capacity planning-model, IEEE Tr. Sys. Man & Cyber., **10**(10), 650-652

Ostroff A (1985), Techniques for accommodating control effector failures on mildly statically unstable airplane, *Proc. ACC '85*, 906-913

Ostroff A & Hueschen R (1984), Investigation of control law reconfigurations to accommodate a control element failure on a commercial airplane, *Proc. ACC'84*, 1746

Owens D H (1978), *Feedback and multivariable systems*, P Peregrinus, 1978

Passino K M, Antsaklis P J (1988), Inverse stable sampled low-pass systems, Int. J. of Control, **47**(6), 1095-1913

Patton R J (1991), Fault detection and diagnosis in aerospace systems using analytical redundancy, *IEE Comp. & Con. J.*, **2**(3), 127-136

Patton R J (1993), Robustness Issues in Fault-tolerant Control, Plenary paper, *TOOLDIAG'93*, Toulouse

Patton R J (1995), Robustness in Model-Based Fault Diagnosis: The 1995 Situation*, IFAC Workshop: On-Line Fault Detection & Supervision in the Chemical Process Industries, Newcastle*, June

Patton R J & Chen J (1990), The design of a robust fault diagnosis scheme for a jet engine system, *IMACS Annals Comp. & App. Maths, MIM-S2'90*, Sept. 3-7

Patton R J & Chen J (1991), Robust fault detection using eigenstructure assignment: A tutorial consideration & some new results, *Proc. 30'th CDC*, 2242-2247, 11-13

Patton R J & Chen J (1993), A survey of robustness in quantitative model-based fault diagnosis, *Appl. Math. & Comp. Sci.*, **3**(3), 399-416

Patton R J & Chen J (1994), A review of parity space approaches to fault diagnosis for aerospace systems, *J. Guid., Contr.& Dyn.*, **17**(2), 278-285

Patton R J & Chen J (1996), Robust Fault Detection and Isolation (FDI) systems, *Con. & Dyn. Sys. (ed C Leondes)*, **74**, 171-224, Mita Press

Patton R J, Chen J & Nielsen S B (1995); Model-based methods for fault diagnosis: some guide-lines, *Tr. Inst. Meas. & Con.*, **17**(2), 73-83

Patton R J, Frank P M & Clark R (1989), *Fault diagnosis in dynamic systems: Theory & Application*, Prentice Hall

Patton R J, Frank P M & Clark R (1997), *Advances in fault diagnosis for dynamic systems*, Springer-Verlag

Patton R J & Hou M (1997), Unknown input de-coupled optimal filtering, *Proc. IFAC SAFEPROCESS'97, 335*

Pearce D A (1988), The induction of fault diagnosis systems from qualitative models, *Proc. Nat. Conf. on Artif. Intel. (AAAI-88)*, 353-357

Polycarpou M M, Helmicki A J. (1995), Automated Fault Detection and Accommodation: A Learning Systems Approach, *IEEE Tr. Sys. Man & Cyb*, **25**(11)

Pouliezos A D & Stavrakakis G S, (1994), Real time fault monitoring of industrial processes, Kluwer Academic

Qiu Z, Gertler J (1994), Robust FDI System and H_∞ Optimisation, *IFAC Symp. SAFEPROCESS'94*, Helsinki, June, 260-265

Rattan K S (1985), Evaluation of control mixer concept for reconfiguration of flight control system, *Proc. Nat. Aero. & Electr.,* Dayton, 560-569

Rauch H E (1995), Autonomous Control Reconfiguration, *IEEE Con. Sys. Mag*, **15**(6),37-48

Raza S J & Silverthorn J T (1985), Use of the pseudo-inverse for the design of a reconfigurable flight control systems, *Proc. Nat. Aero. Electr,* Dayton, 349-356

Rugh W J (1991), Analytical framework for gain scheduling, IEEE Con. Sys. Mag., **11**, 79-84

Sadrnia M, Chen J & Patton R (1997), Robust H_∞/H_- observer-based residual generation for fault diagnosis, Proc. IFAC *SAFEPROCESS'97*, 147-153

Savonov M G (1980), *Stability and robustness of multivariable feedback systems*, MIT Press.

Shamma J, Athans M (1992), Gain scheduling: Potential hazards and possible remedies, IEEE Con. Sys. Mag., **10**(3), 101-107

Smith G A & Meyer G (1987), Aircraft automatic flight control system with model inversion, *J. Guid. Contr. & Dyn.*, **10**(3), 269-275

Sobel K M, Kaufman H & Balas M (1982), Implicit adaptive control for a class of MIMO systems, *IEEE Tr. Aero. & Elect. Sys.*, **AES-18** (5), 576-589

Son W-K, Kwon O-K & Lee M E (1997), Fault-tolerant model-based predictive control with application to boiler systems, *Proc. IFAC SAFEPROCESS '97, 1240-1245*

Srichander R & Walker B K (1993), Stochastic stability analysis for continuous-time fault-tolerant control systems, *Int. J. Con., **57**(2),433-452*

Stengel R F (1991), Intelligent failure-tolerant control, *IEEE Con. Sys. Mag.*, 14-23

Stengel R F (1993), Toward Intelligent Flight Control, *IEEE Tr. Sys.Man & Cybernetics*, **23**(6) 1699-1717

Travé-Massuyes L A, Missler & Pierra (1990), Qualitative models for automatic control process supervision, *Proc. 11th IFAC World Congress*, Tallin

Tyler J (1970), The characteristic of model-following systems as synthesised by optimal control, *IEEE Tr. Aut. Con.,* **AC-15**(3), 326-333

Tyler M & Morari M (1994), Optimal and robust design of integrated control and diagnostic modules, Proc. ACC'94,

Tzafestas S G (1989), System fault diagnosis using the knowledge-based methodology, in: Patton *et al.*, *Fault diagnosis in dynamic system: Theory & applications*, Prentice Hall

Tzafestas S & Watanabe K (1990), Modern approaches to system/sensor fault detection & diagnosis, *J. A*, **31**(4), 42

Veillette R J, Medanic J V & Perkins W R (1992),Design of Reliable Control Systems, *IEEE Tr. Auto.Con.*,37,(3) 290

Van den Hof P M J & Schrama R J (1995), Identification and Control - Closed-loop issues, *Autom.*, **31**(12), 1751

Viswanadham N & Srichander R (1987) Fault detection using unknown-input observers, *Cont. Th. & Adv. Tech.*, MITA Press, **3**(2), 91-101

Werbos P J (1995), Neural networks and flight control: Overview of capabilities and emerging applications, *Proc. Guid. Navi. & Contr. Conf. (Paper No AIAA-95-3272-CP),* Baltimore, August

Walker B K (1983), Recent developments in fault diagnosis and accommodation, *Proc. AIAA Guid., Nav. & Con. Conf.*, Gatlingburg, August

Walker B K (1989), Fault detection threshold determination using Markov theory, in: Patton *et al.* (eds) *Fault Diagnosis in Dynamic Systems: Theory & Application*, Prentice Hall, 477-508

Walker B K (1997), 1056-1067

Watanabe K & Himmelblau D M (1982) Instrument fault detection in systems with uncertainties, *Int. J. Syst. Sci.*, **13**, 1982, 137-158

Westermeier T F (1977) Redundancy management of digital FBW systems, *Proc. ACC'77.,* 272-272

Williams S & Hyde R A (1990) A comparision of characteristic locus and H_∞ design methods for VSTOL flight control system design, *Proc of ACC '90*, San Diego, May, 2508-2513

Willsky A S, Deyst J J and Crawford, B S (1975) Two self-test methods applied to an inertial system problem, *J. Spacecraft & Rockets*, **12**, 434-437

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

Wu N E (1992) Failure sensitizing reconfigurable control design, Proc. of the 31st CDC, Tuscon, Dec., 44-49

Wu N E (1993) Reconfigurable control design: Achieving stability robustness and failure tracing, Proc. 32nd CDC, S Antonio

Wu E (1995) Robust failure detection with parity check on filtered measurements, IEEE Tr. AES. **31**, 489-491

Wu E (1996) Feedback design in control reconfiguration systems, Int. J. Rob. & Non-Lin. Con., Wiley, **6**, 561-570

Wu E (1997), Reliability criteria-based reconfigurable control system design, *Proc. IFAC SAFEPROCESS'97, 1068-1073*

Wünnenberg J & Frank P M (1987) Sensor fault detection via robust observers, In System Fault Diagnostics, in: Tzafestas, Schmidt & Singh (eds), *Reliability & Related Knowledge-Based Approaches*, Reidel Press, **1**, 147-160.

Yedavalli R K (1988), Stability Robustness measures under dependent uncertainty, *Proc. ACC'88*, 820-823.

Zadeh L (1996), Fuzzy Control: Issues, Contentions and Perspectives, *13th IFAC World Congress*, S Francisco

Zheng C, Patton R J & Chen J (1997), Robust fault-tolerant systems synthesis via LMI, *Proc. IFAC SAFEPROCESS'97, 347-352*

Zhou K & Khargonekar P P (1987), Stability robustness bounds for linear state-space models with structured uncertainty, *IEEE Tr. Aut. Contr*, **AC-32**, (7), 621-623

Zhou K, Doyle J & Glover K (1996), *Robust and optimal control*, Prentice Hall