Chapter 2
Review and Basic Concepts

Acronyms

EFCS	Electrical Flight Control System
FBW	Fly-by-Wire
FCC	Flight Control Computer
FDD	Fault Detection and Diagnosis
FDI	Fault Detection and Isolation
FDIR	Fault Detection, Identification and Recovery
FTC	Fault-Tolerant Control
FTG	Fault-Tolerant Guidance
L/D	Lift-to-Drag Ratio
NEP	Nominal Exit Point
GNC	Guidance, Navigation, and Control
HMI	Human–Machine Interface
LTI	Linear Time Invariant
LPV	Linear Parameter Varying
RLV	Reusable Launch Vehicle
TAEM	Terminal Area Energy Management
TEP	TAEM Entry Point
TRL	Technology Readiness Level
α	Angle-of-Attack
M	Mach Number

A. Zolghadri et al., *Fault Diagnosis and Fault-Tolerant Control and Guidance for Aerospace Vehicles: From Theory to Application*, Advances in Industrial Control,
DOI 10.1007/978-1-4471-5313-9_2, © Springer-Verlag London 2014

2.1 Introduction

2.1.1 Fault Detection and Diagnosis, Fault-Tolerant Control, and Fault-Tolerant Guidance

Fault detection and diagnosis (FDD) is an important aspect of process engineering. The primary objective of an FDD system is early detection of faults, isolation of their location, and diagnosis of their causes, enabling correction of the faults before additional damage to the system or loss of service occurs. Abnormal situations occur when processes deviate significantly (outside the allowed range) from their normal regime during online operation. A fault can be defined as an unpermitted deviation of at least one characteristic property or parameter of the system from the standard condition [1]. A failure is a permanent interruption of a system's ability to perform a required function under specified operating conditions. Within the academic literature, the terminology is now more or less standardized.[1] Such malfunctions may occur in the individual unit of the plants, sensors, actuators, or other devices and affect adversely the local or global behavior of the system. Process abnormalities are usually classified into additive or multiplicative faults according to the effects on a process. In general, additive faults affect processes as unknown inputs, while multiplicative faults usually have important effects on the process dynamics and can cause unstable behaviors. Abrupt faults are sudden changes in behavior of the system (step like), while incipient faults are gradual and slow drifting faults. Permanent faults lead to the total failure of the equipment (once they occur they do not disappear), transient faults are temporary malfunctioning (appear for a short time and then disappear), and intermittent faults are the repeated occurrences of transient faults (they appear, disappear, and then reappear). Hidden faults are those which are present on standby equipment and visible only when this equipment is activated.

Throughout this book, we do not consider software and communication bugs for which the detection techniques are very different from the techniques used to handle physical faults.

Generally, the main desirable characteristics of an FDD system are:

- Early detection and diagnosis, i.e., detection delay should be minimized. This feature is highly related to the fault/failure criticality.
- Good ability to discriminate between different failures (isolability).
- Good robustness to various noise and uncertainty sources and their propagations through the system.
- High sensitivity and performance, i.e., high detection rate and low false alarm rate.

[1] See, for example, http://www.safeprocess.es.aau.dk/

Once faults are correctly detected, confirmed, and diagnosed, a reconfiguration mechanism may be used in order to achieve fault tolerance. The primary goal of fault tolerance is to prevent errors from propagating and leading to a dangerous, hazardous or off-normal system behavior. For many safety-critical systems, fault tolerance is founded on redundancy. If we have two or more identical components, we can ignore the faulty component or switch to a spare if the primary fails. For flight systems, recovery and reconfiguration actions may have different goals and characteristics depending on the considered mission. For example, for an observation satellite, reconfiguration mechanisms are based on redundant units switching and consist in action sequences, i.e., event sequences or onboard control procedures, which are a priori programmed and then executed as a reflex reaction following fault detection [2].

From a "control" point of view, one can distinguish two basic functions for reconfiguration: fault-tolerant control (FTC) and fault-tolerant guidance (FTG). FTC systems seek to provide, at worst, a degraded level of performance in the faulty situations. Generally, a fault-tolerant control does not offer optimal performance for normal system operation, but it can compensate effects of system failures by adjusting, for example, the controller parameters to recover the system from the faulty condition. In general, FTC strategies are classified into passive and active approaches. In the passive approach, a single control law is designed to keep stability and an acceptable level of performance in both fault-free situation, i.e., when all components are operational, and in the case of faults. It can be seen as a "super" or augmented robust control law. The price to pay for robustness to faults is that nominal and fault-free performance is deteriorated. An active FTC strategy requires FDD information for control reconfiguration (see, e.g., [3–5]). FTG could provide a greater flexibility for safe recovery in case of degraded flight conditions. In fact, onboard planning capabilities can be used to resume mission activities without ground intervention after a fault is detected and confirmed. It supposes a diagnosis capability and the possibility to take into account deteriorated resources in the planning process. FTC and FTG provide means to avoid and suppress a potentially hazardous, out-of-tolerance, or dangerous behavior of the system if possible or provide means by which the consequences of a dangerous behavior are avoided.

2.1.2 Interaction Between FDD, FTC, and FTG

Conceptually, the interaction between FDD, FTC, and FTG units can be illustrated as in Fig. 2.1. FTC follows FDD and provides means to continue to "control" the faulty system (maintain stability and achievable performance). FTG would be necessary when the available onboard control resources are limited and when FTC would not be sufficient.

For aerospace applications, the above functions are related to the GNC (guidance, navigation, and control) system. The GNC system gives the vehicle the ability to execute flight over a predefined path generated by a path planner. Guidance

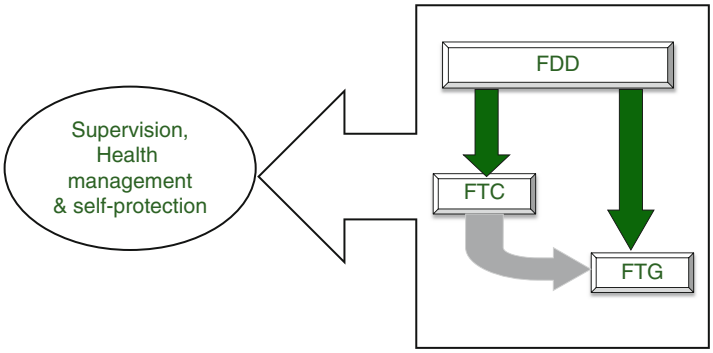

Fig. 2.1 Interaction between FDD, FTC, and FTG

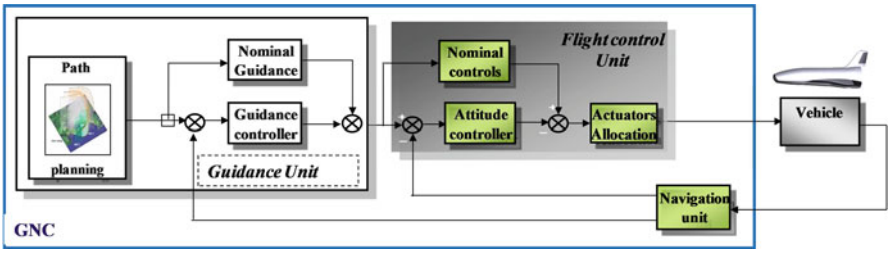

Fig. 2.2 GNC system

equipment (gyroscopes, accelerometers . . .) compute the location (or attitude) of the vehicle and the orientation required to satisfy mission requirements. Navigation tracks the vehicle's actual location and orientation. Usually control consists of two modes: automatic and manual. In the automatic mode, the primary avionics software system allows the onboard computers to control the guidance and navigation of the space vehicle. In the manual mode, the flight crew uses data from the GNC displays and hand controls for the guidance and navigation. Although GNC design is by far the most relevant aspect for aircraft and space vehicles, its treatment is well beyond the aim of this book. The interested reader can refer to many published materials on this subject, among others the dedicated conferences organized by AIAA (https://www.aiaa.org).

A simplified block diagram of the GNC is depicted in Fig. 2.2. Using air data and engine thrust data, the guidance loop computes the guidance demands to follow waypoint scenarios. The flight control loop generates actuator signals for the control surfaces. As aerospace vehicles are often over actuated, a control allocation (often static, sometimes dynamic) allows for distributing a desired total control effort among a redundant set of actuators.

A more detailed description of the FDD and FTC functions will be given in the following sections. Roughly speaking, FTG means "change the mission objectives." To illustrate the idea of FTG, consider a typical atmospheric reentry trajectory

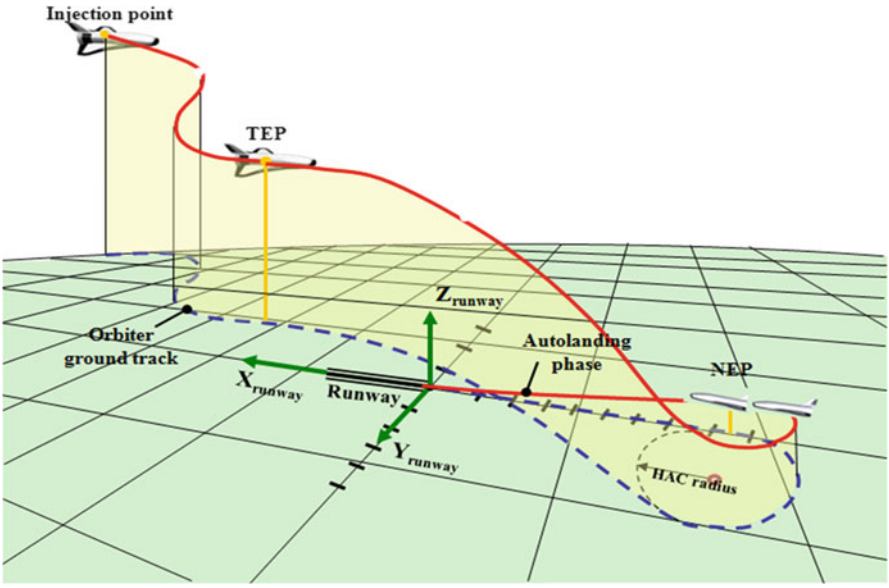

Fig. 2.3 Atmospheric reentry trajectory

(Fig. 2.3) for a medium- or high-L/D vehicle. It consists in performing three successive flight phases, namely, the hypersonic phase from about 120 km high down to TAEM handover, the TAEM phase from Mach 2 gate down to Mach 0.5 gate, and the auto-landing phase from Mach 0.5 gate down to the wheel stop on the runway. After having achieved the hypersonic path, the vehicle initiates the TAEM phase characterized by an entry point, called TEP, typically defined when crossing the Mach 2 gate and an exit point, called NEP, which is defined in terms of altitude, velocity, and distance to the runway. Finally, the landing path is defined in terms of desired altitude from the runaway threshold, and it is composed of three successive sections, i.e., a steep outer glide slope, parabolic pull-up maneuvers, and a shallow inner glide slope. During the reentry mission, actuator failures and damage of control effectors could lead to substantial performance degradation and even instability of the closed-loop system. An important issue following the FDD consists then to engage timely safe recovery actions to accommodate faults. The goal is to maintain control of the vehicle following actuator faults by means of the healthy control effectors. However, under some failure conditions, even advanced FTC techniques may be insufficient to recover the vehicle. Significant aerodynamics characteristic change of the vehicle and a possible lack of control may require reshaping of a new trajectory so as to land the vehicle safely and in compliance with the stringent operational and fight dynamics constraints. Key features for the success of such reshaping algorithms rely on the knowledge of the failed actuator position (reliable FDD information) so as to evaluate the remaining capabilities of the vehicle to be rotationally trimmed. The case of non-compensable faults can

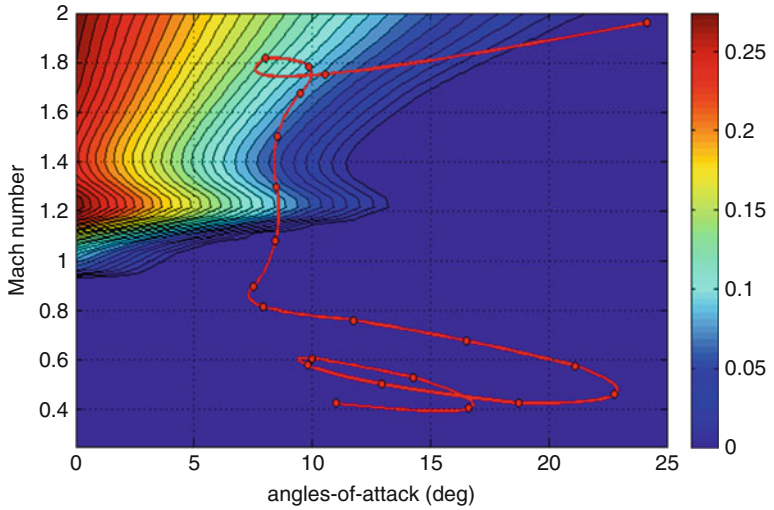

Fig. 2.4 Projection of the flight trajectory onto (M-α) plane: non-trimmable regions are not avoided

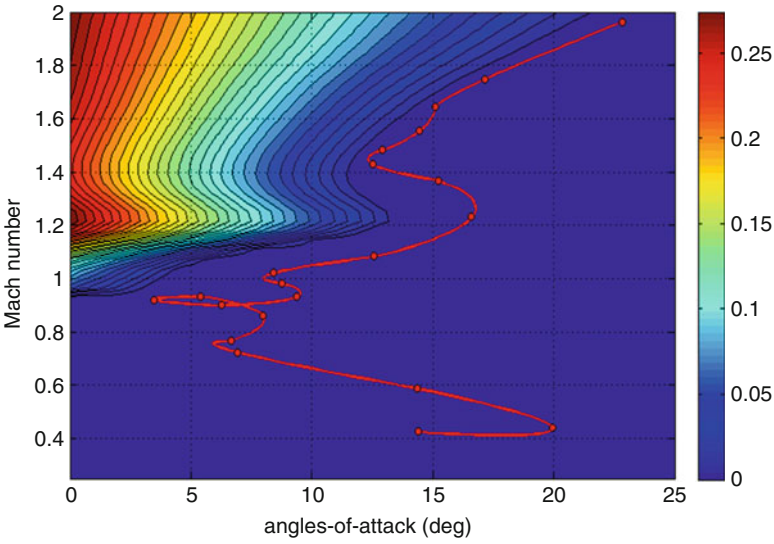

Fig. 2.5 Successful FTG: reshaped trajectory

be then studied as a trimmability-deficiency analysis problem which boils down to a static-fault compensability study. The goal is to define the flight envelope regions, for example, in the Mach-α space (see Figs. 2.4 and 2.5), where the vehicle cannot be rotationally balanced in the presence of faults. As a direct consequence, a fault is considered as non-compensable if the flight trajectory of the vehicle

(projected in the Mach-α space) crosses the non-trimmable region (see Fig. 2.4 for an illustration). It follows that the results after a successful FTG corresponds to a flight trajectory that does not cross the non-trimmable region (see Fig. 2.5 for an illustration). In Figs. 2.4 and 2.5, both flight trajectory (red) and trimmability-deficiency regions (from blue = trimmable regions to red = highly non-trimmable regions) are depicted.

2.1.3 Chapter Organization

This chapter is organized as follows. Section 2.2 presents a brief overview of the industrial state-of-practice. Section 2.3 is devoted to the review of the available academic literature. Section 2.4 highlights the reasons for slow-developing progress of the advanced academic methods to real-world aerospace systems. Finally, Sect. 2.5 is dedicated to final remarks and motivates the developments that will be presented in subsequent chapters.

2.2 Industrial State-of-Practice

2.2.1 General Ideas

The basic principles involving general health management architecture trade-offs changed little from the 1960s, although the hardware mechanizations of the earlier analog systems have been replaced largely with the software of the newer digital systems (see, e.g., [6, 7] for a historical review). The success of the Apollo program has been an important factor for the development of digital fly-by-wire technologies. In the late 1960s, engineers at NASA Flight Research Center (now NASA Dryden) proposed replacing bulky mechanical flight control systems on aircraft with much lighter weight and more reliable analog fly-by-wire technology. As the Apollo program came to completion in the early 1970s, NASA Dryden engineers developed a digital fly-by-wire solution using the specialized software and hardware developed for Apollo [7, 8]. A few years before in Europe, Aerospatiale (now EADS) engineers developed and installed the first analog electrical flight control system on Concorde.[2] In civilian and military aviation, this precipitated a revolution in aircraft design. The electrical flight control system, designed with digital technology on Airbus aircraft from the 1980s (on A310 aircraft for the spoilers, slats, and flaps only and then generalized on all control surfaces on the A320 in 1987), provided more sophisticated control of the aircraft and flight

[2] A supersonic passenger airplane jointly developed and produced by Aerospatiale (France) and the British Aircraft Corporation under an Anglo-French treaty (first commercial fly in 1969).

envelope protection functions. Physical separation of critical avionics functions from less critical functions has been always the primary strategy used by the designers of civil aircraft to produce safe avionic systems. Traditional avionics systems are built around federated architectures in which each processing site contains a single application such as an autopilot, flight management system, or display. Critical functions are protected from noncritical tasks by physical isolation. NASA used this approach on interplanetary spacecraft, where critical functions to the survival of the spacecraft are handled by an attitude and articulation control system, which is separate from the systems that control the science experiments.

Fault detection is generally based on the concept of redundancy, i.e., the comparison of duplicative signals generated by various hardwares, such as measurements of the same parameter given by two or more identical sensors. Fault detection and confirmation is mainly performed by cross-checks, consistency checks, voting mechanisms, and built-in test techniques (BIT, which include hardware sensors and software error correcting codes) of varying sophistication. The typical method for this is limit checking, i.e., verifying whether a parameter value goes outside of a specified range of values. Multiple ranges can be defined; one can specify a not-to-exceed value (high limit) and a low limit. Multiple high or low limits can be also specified, for example, an advisory range, a caution range, and a warning range. The limit can be applied directly to the instantaneous value of the parameter, the change from the previous value, or the trend of the value over time. For instance, a typical commercial aircraft's navigation sensing system can contain triple-redundant inertial references plus triple-redundant air data sensors. A voting scheme monitors and checks the performance of the individual sensors and detects abnormal behavior. A key issue relates to definition of failure thresholds, which reflect calibration tolerances and environmental effects on component specifications. Flight condition-based thresholds, once validated with all the known delays and uncertainties in the signal propagation (acquisition, processing . . .), are used for rapid recognition of out-of-tolerance conditions. The main advantage of fixed thresholds is that it allows designers and operators to use and manage them easily. In setting these thresholds, compromises have to be made between the detection size of abnormal deviations and false alarms because of normal fluctuations of the variables.

Fault tolerance relies mainly on hardware redundancy, safety analysis, dissimilarity, physical installation segregation, and hardware/software reconfiguration [9]. For a general analysis of fault-tolerance management in space vehicles, see, for example, [2, 7]. These hardware-based redundancy techniques are nowadays the standard industrial practice and fit also into current industrial certification processes while ensuring the highest level of safety standards.

2.2.2 Aeronautics

Firstly, let us look at fault management procedures in cockpit and flight deck. The today flight deck represents a highly automated mass of complex systems with

which the flight crew has to interact. The increase in automation has shifted the role of the pilot away from hands on flying and more toward system monitoring. Pilots rely on warning systems to generate alert messages at the earliest opportunity in order to allow maximum time for corrective actions. Each warning has an associated procedure. These procedures are listed in the *Quick Reference Handbook* and *Flight Operations Manual* on the flight deck or, in some cases, are displayed electronically. Basically, all alert messages can be plotted onto two axes: intervention immediacy and intervention importance. These two factors combined establish the alert's urgency. The situation being monitored is often complex with many components, influences, and interactions, and there is a need to take into account a large number of parameters in order to assess the situation see [10–13].

The paper [9] focuses on a typical Airbus EFCS and provides a detailed description on the industrial practices and strategies for FTC and FDD in civil aircraft. Today, the EFCS constitutes an industrial standard for commercial aircraft applications. It provides sophisticated control of the aircraft and flight envelope protection functions [14, 15]. The main characteristics are that high-level control laws in normal operation allow all control surfaces to be controlled electrically and that the system is designed to be available under all possible external disturbances. The EFCS is designed to meet very stringent requirements in terms of safety and availability, specified by the aviation authorities [16]. Compared to mechanical flight control system, it has brought more safety, increased performance, more availability, weight saving, a more accurate control, and an easiest way to update the whole system. However, the EFCS development on modern civil aircraft also led to a growing complexity of systems and equipment. Consequently, the number of failure cases to consider in the aircraft design has increased compared to the historical mechanical flight control system, and FDD has become of primary interest. The state-of-practice, applied worldwide by all aircraft manufacturers, to diagnose these EFCS faults and obtain full flight envelope protection at all times is to provide high levels of hardware redundancy and dissimilarity in order to perform consistency tests and cross-checks. This also ensures sufficient available control action (fault tolerance). The interested reader can refer, among others, to [17–29].

2.2.3 Space Missions

For space missions, health monitoring is managed through a FDIR hierarchical approach in which several levels of faults are defined from local component/equipment up to global system failures [2, 7, 30]. Depending on the mission needs, FDIR functions are combined to other functions (data processing, orbitography, event-based commanding, and dynamic reprogramming) to achieve a desired level of availability, safety, and autonomy [2, 31–33]. FDIR strategy can be divided between all levels: detection and local reconfiguration in the subsystems, fault diagnosis and global reconfiguration at the operational level, and prevention at the decisional level (detect in advance plans that no longer consistent with the actual resource

usage and may lead to further failures). The validation assumes testing all possible cross-path situations that becomes costly as the complexity of inboard hardware and software architectures increases. For early spacecraft, the above tasks were executed by sequential automata performing a priori known tasks. New-generation spacecraft has smart embedded systems, which are able to react to some known events and to select a decision among a predefined set. FDD, FTC, and FTG functions are strongly related to autonomy needs that vary with the mission scenarios and the expected benefits. Standardized degrees of autonomy can be found, for example, in [34]. See also [35] for an interesting discussion on autonomy needs for future space exploration missions. A low Earth orbit satellite can be endowed with an autonomous orbit control function to reduce ground operations. A deep space spacecraft, due to long communication delays, will require FDD and automatic reconfiguration capacities. For other space systems such as winged atmospheric reentry vehicles (e.g., space shuttle) which have aircraft-like configurations and more redundant control actuation, there are also more limited weight capabilities compounded because of more restrictive aerodynamic and controllability characteristics resulting from their lower lift-to-drag ratios. Note that, since the first flight of the Apollo mission where gain-variable Kalman filters were implemented into the Apollo lunar module first-generation digital flight computer, Kalman-based estimators are used in the flight control software of many space missions. Some estimated quantities could be used redundantly for fault detection and health management. The paper [36] describes the V&V challenges and approaches posed by the innovative FDIR technologies being employed and discusses additional certification considerations. The NASA technical report [37] discusses issues and lessons learned regarding designing, integrating, and implementing FDIR at Kennedy Space Center.

2.3 Review of Academic Advanced Results

2.3.1 Introduction

A large body of literature on FDD and FTC is now available. The open literature dealing with FTG is much more limited. Good surveys about academic state of the art can be found in [1, 3, 38–48]. FDD is a deep subject with hundreds of subtopics. The theory related to FDD has been developed since the early 1970s and can be considered today as a mature and well-structured field of research within the control community and offering many attractive features. FDD methods are classified generally into three categories, which include the knowledge or history-based methods [41, 49, 50], analytical model-based methods, and signal-based methods. For the latter, reference [44] gives a thorough review on the definitions and the methods for change detection with a main focus on the parametric statistical tools such as log-likelihood ratios and efficient scores. In this chapter, we will focus on analytical model-based approaches. Here by the term “model,” we understand quantitative model: use of static and dynamic relations among system variables

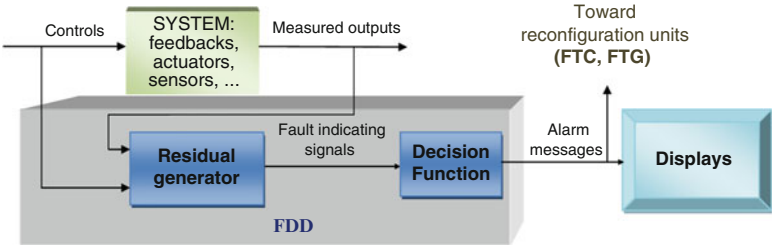

Fig. 2.6 Basic FDD structure

and parameters in order to describe system's behavior in quantitative mathematical terms. Note that the qualitative model-based methods, such as pattern recognition or rule-based approaches, capture discrepancies between observed behavior and that predicted by a qualitative model.

The early studies on model-based FDD appeared about 40 years ago. In [51–53], innovation signals are used to design detection filters. Many basic solutions have appeared during the 1980s: parity space and observer-based approaches, eigenvalue assignment, or parametric-based methods [1, 45–47, 54, 55]. In the 1990s, a great number of publications dealt with specific aspects such as robustness and sensitivity, diagnosis-oriented modeling, or robust isolation [38, 44, 47, 56–61]. The European school has been very active in the development of this field (see, e.g., and among others [38, 46–48, 62–71]). Today, and at least from a design point of view, model-based FDD can be considered as a mature field of research within the control community. The evidence of this can be seen through the very significant number of publications and dedicated international conferences.

2.3.2 Analytical or Model-Based FDD

The basic idea of model-based FDD is very simple and straightforward: residuals (fault indicating signals) are generated from comparison of the system measurements with their estimates. A threshold function (fixed or variable) can be used to provide additional levels of detection, while for fault isolation the generated residual has to include enough information to determine that a specific fault has occurred. The fault isolation is trivial in applications where the fault detector is dedicated to only one kind of fault.

The basic structure of a classical model-based FDD technique can be depicted as in Fig. 2.6.

The core element is the residual generation. Note that if only fault detection is of interest, reconstructing the fault rather than detecting its presence through a residual signal can be an alternative solution [64, 72–74]. Residual evaluation and decision making consist of checking the residuals and triggering alarm messages if the tolerances are exceeded. The thresholds can be set into different kinds. The

simplest way is to use a constant threshold. The big advantage with fixed thresholds is their simplicity and reliability. Adaptive thresholds could enhance the sensitivity of fault detecting with the optimal choice of the magnitude which depends upon the nature of the system uncertainties and varies with the system input. Adaptive thresholds can keep the false alarm rate small with an acceptable sensitivity to faults. In some applications, stochastic system models are considered, and the generated residuals are known or assumed to be described by some probability distributions. It is then possible to design decision tests based on adaptive thresholds. More robust decision logics use the history of the residuals and utilize powerful or optimal statistical test techniques. The well-known examples of these statistical test techniques are sequential probability ratio test (SPRT), cumulative sum (CUSUM) algorithm, generalized likelihood ratio test, and local approach (see, e.g., [44]). To enhance the robustness of FDD schemes against small parameter variations and other disturbances during residual generation, different design, and evaluation tools have been proposed [38, 39]. The objective of any robust FDD method is to make the residuals become sensitive to one or more faults while at the same time making the residuals insensitive to modeling errors and uncertain disturbance effects acting upon the system being monitored. Robust FDD can be achieved if the residual signals maintain the desired sensitivity properties over a suitable range of the system's dynamic operation. A huge literature is now available dealing with various aspects of an FDD problem, ranging from modeling problems (nominal system modeling, fault modeling, disturbance and uncertainty modeling) and FDD system design.

The available design methods includes methods based on LTI, LPV, and nonlinear/hybrid estimators/observers, robust designs inspired by robust control designs, unknown input observers, and sliding-mode methods. The interested reader can refer, for example, to [38, 39] for recent surveys.

Remark 2.1 A hybrid system consists of a set of discrete modes, which represent fault states or operational modes of the system, and a set of continuous variables which model the continuous quantities that affect system behavior. Usually, the term state refers to the combination of these, that is, a state is a mode plus a value for each continuous variable, while the mode of a system refers only to the discrete part of the state.

Observer-based approaches have arisen as one of the most popular among FDI design techniques. In the linear case, it has been shown that any linear fault detection filter can be transformed into an equivalent observer-based form [75], providing a unified framework for analysis and implementation.

Generally speaking, the difficulties with LTI models for FDD lie in the need to produce meaningful models which can be used for synthesis and in the need of a posteriori robustness/sensitivity analysis. As it will be seen in Chap. 7, the effect of guidance, navigation, and control should be carefully analyzed and taken

into account during model building. Modeling stage should also take into account uncertainties, stemming from a large variety of environmental disturbances and internal sources [76].

The things get much more complex in the nonlinear case from a design and also an analysis point of view. For a good recent survey on nonlinear FDD methods, the interested reader can refer to [48] and the references therein. Typically, the observer design problem is solvable if the system model can be transformed into a canonical form that may be a hard assumption to satisfy in many applications. An appealing approach to deal with some nonlinear problems is based on the LPV transformation. Consider, for example, a nonlinear system described by

$$\dot{x} = f(t, x, u, w),\ y = h(x) + v \tag{2.1}$$

where $x \in R^n$, $u \in R^m$, $w \in R^l$, $y \in R^p$, and $v \in R^p$ are, respectively, the state, the input, the disturbance, the output, and the measurement noise; $t \in R_+$ and the functions f, h are continuous with respect to all arguments and differentiable with respect to x and u. An LPV representation can be given by

$$\dot{x} = A(\rho(t))x + B(\rho(t))u,\ y = C(\rho(t))x + v \tag{2.2}$$

where the scheduling parameter vector $\rho \in \mathcal{P}$ is considered to be time varying (measured or estimated upon system operation) or unknown with known bounds; $\mathcal{P}$ is a set of functions that remain in a compact real subspace. The system (2.2) is an equivalent representation of (2.1), in the sense that all trajectories of (2.1) remain in the trajectories of (2.2). The basic idea is to replace nonlinear complexity of the model (2.1) by enlarged parametric variation in the linear model (2.2) which simplifies the design of an observer for (2.1). The main appeal of using the LPV formalism is that the solutions can be obtained using linear algebraic manipulations like those elaborated for LTI systems.

2.3.3 *Recovery Aspects: FTC and FTG*

The next step following the design of an FDD system is to decide appropriate recovery and corrective actions, based on all available actuator/sensor/communication resources. The recovery aspects have also been extensively studied (see, for instance, [3, 77]). The general objective is firstly to maintain stability and secondly to keep an acceptable performance level in fault situations. For successful reconfiguration actions, information about the failed element (fault identification) is necessary in order to access the remaining control resources. The interaction with the FDD system is a key point: generally FDD mechanism is supposed to detect and diagnose correctly any relevant signal degradation or failure. Obviously this must be done sufficiently early to set up timely recovery actions.

Usually the fault tolerance could be achieved through several potential solutions, for instance:

- Selecting a new precomputed control law depending on the faults which have been identified by the FDD system. In this case, hybrid control or switching control structures are commonly encountered in the literature [78].
- Synthesizing a new control strategy online. Such methods involve the calculation of new controller parameters once a failure has been identified by an online fault estimation scheme, following the typical design paradigm of adaptive control [79].
- Using dynamic control allocation for over actuated systems. The fault control allocation problem is that of distributing a desired total control effort among a redundant set of healthy actuators (without reconfiguration/accommodation of the controller) [80, 81].

The interested reader can refer to [82–87] and the references therein for further details.

The majority of the available methods rely implicitly on the assumption that the FDD and automatic reconfiguration and recovery systems are assumed to operate correctly, that is, the FDD outputs are supposed to be instantaneously available. The problem of guaranteeing stability and a certain level of performance of the overall fault-tolerant system, taking into account both the FDD performance (detection delay) and reconfiguration system, has not been sufficiently considered in the literature. Usually, the desired characteristics are checked a posteriori by means of Monte Carlo campaigns and nonlinear simulations. Note that for aerospace applications, validation assumes testing all possible cross-path situations that becomes costly with the GNC complexity increase and leads to intricate validation processes. Moreover, generally the sizing case corresponds to the worst performance that can be obtained in extreme situations. This procedure often limits the capability of "fail operational" strategies for some critical situations. Several more formal solutions have appeared recently. The effect of the FDD delay can be analyzed for linear systems [88]. In [89], a supervisory scheme uses a switching algorithm to fault isolation: a sequence of controllers is switched, until the appropriate one is found. Other works seek to combine a fault-tolerant controller and a diagnostic filter in both LTI and LPV settings (see, for instance, [82–85, 90]). However, the structure and parameters of the already in place control laws are generally modified. For aircraft systems, for example, this solution may lead to a new (long and expensive) certification campaign in fault-free situations. This could be a major concern for most safety-critical systems. Finally, FTG has been studied for some specific aerospace vehicles [4]. For example, for reusable launch vehicles (RLV), it has been shown in [91] that onboard autonomous FTG could be a promising solution, as it could provide a greater flexibility to account for off-nominal conditions or even to recover timely the vehicle from faulty situations.

2.4 Toward Advanced Model-Based Techniques for Flight Vehicles

2.4.1 Needs, Requirements, and Constraints

Aerospace industry needs continuous improvement including insertion of new technologies. Generally, new technologies are adopted in practice only when there is a clear cost or performance benefit. In aeronautics, at the same time, the main aircraft manufacturers tend more and more to use and adopt more sustainable technologies in order to decrease the environmental footprint of their airliners, feeding the needs for advanced strategies for accompanying any greener solutions. It should be noted that, from "a global air transport policy" point of view, much effort is being devoted to further improvement of sustainable and green air transport. The Single European Sky Air Traffic Management Research (SESAR) program in Europe and the Next Generation Air Transportation System (NextGen) in the USA seek to provide quicker flights, less fuel burn and emissions, shorter routes, and less congestion.

As an example, on the A380 airplane, the conventional hydraulic actuators have been replaced by a new generation of electrically powered actuators, the electro-hydrostatic actuator (EHA), mainly for reducing the number of hydraulic systems, generating significant weight and cost savings, and providing additional dissimilarity [92]. EHAs introduce new sources of faults that were tricky to detect with the state-of-practice FDD designs. However, any modification to the already proven and in-service solutions should undergo very long and stringent validation and verification process. Consider the example of a range checking fault detection method devoted to the detection of runaways in aircraft control surfaces servo-loops [93]. This simple technique provides sufficient fault coverage and ensures a perfect robustness without false alarm. The choice of any other "advanced" candidate solution should be clearly demonstrated in terms of added value from an industrial point of view. This means that any changes to existing and already proven scheme should provide a viable technological solution ensuring either better performance while guaranteeing the same level of robustness, or better robustness for the same level of performance, or better performance and better robustness and covering larger fault profile. More generally, the selection of an advanced solution at a local or global level for aerospace missions necessarily includes a trade-off between the best adequacy of the technique and its implementation level for covering an expected fault profile. For proper implementation, those techniques should be embedded within the physical redundancy structure of the system. New methods and technologies entail risk and thus, despite potential cost, performance, and sustainability advantages, must undergo extensive development, validation, and verification before they can be transitioned to real-world systems. That is why decision makers, by default, rely on already proven technical solutions. This is

especially true for space applications, as solutions cannot be tested beforehand due to the difficulties of reproducing space-representative conditions on Earth. For space missions, there exist however a number of challenging requirements to meet the autonomy needs of future space missions. Examples of which are Mars exploration missions and the in-the-drawing-board science missions involving multi-craft formation flying, Near-Earth Objects (NEO), or deep space exploration in general. For space systems, the usual implementation constraints found in aeronautics, such as computation load and complexity, are also encountered albeit to a greater degree due to the more limited weight and computational processing capabilities. These more restrictive limitations arise from the expensive cost for putting additional payload in space and by the lengthier testing and validation process required to classify any design as space ready. The weight limitation directly affects the system decisions related to hardware redundancy, while the processing limitation affects those decisions related to the choice of the onboard diagnosis capabilities and reconfiguration techniques. In the civil aircraft industry, compared to space missions, not only one model is manufactured but hundreds of aircraft are generally mass-produced during several decades. All along the aircraft production, some modifications can be envisaged: extended range, increased maximum take-off weight, extended passenger capacity, etc. In this context, one crucial requirement is the adaptation of the new methods to slightly different aircraft models. For example, a given FDD technique cannot be tuned on a case-by-case basis, but must be generic enough for different versions of the aircraft. In the same order of idea, another requirement concerns the adaptability of the design from one system to the other or even from one control surface to the other. Suppose, for example, that a given FDD technique has been developed for one inboard ailerons of the A380. This FDD technique may be called to be used on the outboard ailerons. If the FDD system requires a completely different tuning of the design via complex methods, it will be difficult to be mastered by the development teams and will penalize the transition to the industrial world. Easy-to-tune high-level input parameters are necessary for the adaptability of a new solution in the framework of mass-production. A limited number of tuning parameters is also desirable for shortening the validation and verification activities demanded for certification. These aspects will be discussed more in details in Chaps. 3 and 4.

2.4.2 Case Studies

One can find a lot of "case study" in the open literature which is fragmented across many technical papers. See, for example, and among others, [4, 62, 94–108], and many technical reports available at http://www.sti.nasa.gov/.

For space missions, one can mention the precursor NASA's New Millennium Program [109]: here, the so-called Deep Space One (DS1) Remote Agent Experiment was initiated to demonstrate onboard fault-protection capabilities, including failure diagnosis and recovery, onboard replanning following otherwise unrecov-

erable failures, and system-level fault protection [110]. Another example is L2 (Livingstone2) program [111] which flew on the Deep Space One spacecraft as part of the Remote Agent Experiment in May 1999. In Livingstone, diagnosis is done by maintaining a candidate hypothesis (in other systems more than one hypothesis is kept) about the current state of each system component and comparing the candidate's predicted behavior with the system sensors. Analytical redundancy and Bayesian decision theory were combined to produce a sensor validation system concept for real-time monitoring of Space Shuttle Main Engine telemetry [112]. The validation system was implemented in Ada and hosted on a Boeing X-33 prototype flight computer. In [36], the authors present a work related to the certification of a pilot application of advanced FDIR software at Ames Research Center and at the Jet Propulsion Laboratory (NASA). The authors underline the stringent requirements in terms of test effort and the value of rethinking V&V when novel technologies are being deployed.

In the open literature, there exist a great number of studies dealing with FDD and FTC in flight control systems (see, e.g., [4, 8, 70, 97, 98, 108, 113, 114]). In Europe, the FDD challenges for aircraft flight control systems were investigated within the ADDSAFE project [115]. Here, by introducing advanced FDD techniques, the goal was to contribute to achieve the European Vision 2020 challenges related to the "greening" of the aircraft. Analytical redundancy has been used on A380 aircraft for the detection of a specific failure case related to EFCS [116].

Insertion of new technologies is assessed by TRL measure [117]. TRL provides a significant input to risk assessment of including a technology in an existing or new program. Roughly speaking, academic activities cover TRL1 (basic principles) up to TRL3 (laboratory and case studies, validation on high-fidelity simulators). TRL6 (prototype demonstration) – TRL9 ("flight proven" through successful mission operations) correspond to technology integration. Often, despite clear needs, new technologies require several years of maturation to the point of practical usefulness, i.e., reaching high TRL. That is why we can observe a "Death Valley" corresponding to TRL4 − TRL5 (validation in relevant environment). This applicability gap has resulted in a real technological barrier. A number of ongoing works at NASA are devoted to bridge this gap. None of the above mentioned remarks are intended to minimize the importance of academic developments. However, it is important to recognize that the gap on the whole is large and warrants serious introspection by the research community. Bridging the gap, from the researcher's perspective, requires that new methods and techniques be communicated to engineers who are in a position to apply them. Motivations which are behind new academic developments should be presented in a more practically relevant way. As an example, many of the early published academic papers on model-based FDD start with the statements such as "hardware redundancy is expensive, heavy, less potentially reliable, it should be replaced by model-based techniques whereby additional knowledge of the system is leveraged instead of actual redundancy...." This basic and historical argument which played a driving role to motivate the early development of FDD academic research could be rather misleading when applied to the aerospace vehicles. A good balance between conventional, technically proven and in-service solutions, and advanced

model-based techniques is probably the only right solution in many applications. This observation has been pointed out in [6] where the author developed several interesting ideas about redundancy management. Model-based techniques do not substitute for physical redundancy but it can be a useful and powerful supplement, if implemented in a manner that properly exploits the physical redundancy.

2.5 Conclusions

There is a growing need to move toward greater onboard reconfiguration capacities and earlier robust diagnosis of system malfunctions. For space missions, this need is driven by the more challenging requirements for future space missions under limited weight and computational processing capabilities. For new-generation civilian aircraft, the need is driven by the more and more stringent requirements which would come in force for future and more environmentally friendlier programs.

The basic aim of this chapter was to give an overview of various model-based approaches to FDD and automatic reconfiguration and the state-of-the-art efforts in terms of industrial applications for aerospace systems. The picture is certainly not complete because of the huge number of various works and studies available in the literature. The focus was to show that while research went forward since the early 1970s, the design methodology involving feasibility analysis and real-world requirements specification is still missing, despite efforts in the past few years. Important issues are potential reduction of physical redundancy, overall reliability, robustness in harsh environments and worst-case performance evaluation. These issues will be discussed in the following chapters through a number of aerospace applications.

References

1. Isermann R (1997) Trends in the application of model-based fault detection and diagnosis of technical processes. Control Eng Pract 5(5):709–719
2. Olive X (2012) FDI(R) for satellites: how to deal with high availability and robustness in the space domain. Int J Appl Math Comput Sci 22(1):99–107. doi: 10.2478/v10006-012-0007-8
3. Blanke M, Kinnaert M, Lunze M, Staroswiecki M (2003) Diagnosis and fault tolerant control. Springer, New York
4. Ducard GJJ (2009) Fault-tolerant flight control and guidance systems, Advances in industrial control. Springer, London
5. Noura H, Theilliol D, Ponsart J-C, Chamseddine A (2009) Fault-tolerant control systems. Design and practical applications, Advances in industrial control. Springer, London
6. Osder S (1999) Practical view of redundancy management, application and theory. J Guid Control Dyn 22(1):12–21
7. Tomayko JE (2000) Computers take flight: A history of NASA's pioneering digital fly-by-wire project. NASA-SP-2000-4224. Available at http://www.nasa.gov/centers/dryden/pdf/182985main_DFBW_rev1.pdf

8. Philippe C et al (2011) Aerospace control. In: Samad (Honeywell) T, Annaswamy (MIT) A (eds) The impact of control technology, overview, success stories, and research challenges. IEEE Control System Society. Available at: http://ieeecss.org/general/impact-control-technology
9. Goupil P (2011) AIRBUS state of the art and practices on FDI and FTC in flight control system. Control Eng Pract 19:524–539
10. Palmer MT, Abbot KH (1994) Effects of expected-value information and display format on recognition of aircraft subsystem abnormalities. NASA TP-3395, March 1994, A technical paper 3395
11. Regal DM, Rogers VH, Boucek GP (1989) Situational awareness in the commercial flight deck – definition, measurement, and enhancement. In: Proceedings of the 7th aerospace behavioral technology conference and exposition. SAE, Warrendale, pp 65–69
12. Johnson DM (1996) A review of fault management techniques used in safety-critical avionic systems. Prog Aerosp Sci 32(5):415–431(17)
13. Trujillo AC (1998) Pilot mental workload with predictive system status information. In: 4th annual symposium on human interaction with complex systems, Fairborn, OH, pp 73–80
14. Favre C (1994) Fly-by-wire for commercial aircraft: the Airbus experience. Int J Control 59(1):139–157
15. Traverse P, Lacaze I, Souyris J (2004) Airbus fly-by-wire: a total approach to dependability. In: Proceedings of the 18th IFIP world computer congress, Toulouse, pp 191–212
16. FAR/CS 25, Airworthiness standards: transport category airplane, published by FAA, title 14, part 25, and certification specifications for large aeroplanes, published by EASA, CS-25
17. Alcorta-Garcia E, Zolghadri A, Goupil P (2011) Nonlinear observer-based strategy for aircraft oscillatory failure detection: A380 case study. IEEE Trans Aerosp Electron Syst 47:2792–2806
18. Briere D, Traverse P (1993) Airbus A320/A330/A340 electrical flight controls—a family of fault-tolerant systems. In: Proceedings of the 23rd international symposium on fault-tolerant computing, Toulouse, pp 616–623
19. Chen RH, Ng HK, Speyer JL, Guntur LS, Carpenter R (2004) Health monitoring of a satellite system. In: Proceedings of AIAA guidance, navigation, and control conference, Minneapolis, August 2004
20. Kumar M (2007) Fault detection identification and reconfiguration of flight control system using IMM estimator. In: Proceedings of the digital avionics systems conference, October 2007
21. Jung B, Kim Y, Ha C, Tahk MJ (2007) Nonlinear reconfigurable flight control system using multiple model adaptive control. Presented at the 17th IFAC symposium on automatic control aerospace, Toulouse, France, June 2007
22. Tang XD, Tao G, Joshi SM (2003) Adaptive actuator failure compensation for parametric strict feedback systems and an aircraft application. Automatica 39(11):1975–1982
23. Oppenheimer MW, Doman DB (2006) Efficient reconfiguration and recovery from damage for air vehicles. Presented at the AIAA guidance, navigation, and control conference, Keystone, CO, August 2006
24. Ganguli G, Papageorgiou, Glavaski S (2006) Aircraft fault detection, isolation and reconfiguration in the presence of measurement errors. Presented at the AIAA guidance, navigation, and control conference, Keystone, CO, August 2006
25. Cieslak J, Henry D, Zolghadri A (2010) Fault tolerant flight control: from theory to piloted flight simulator experiments. IET Control Theory Appl 4:1451–1464
26. Cieslak J, Henry D, Zolghadri A, Goupil P (2008) Development of an active fault tolerant flight control strategy. AIAA J Guid Control Dyn 31:135–147
27. Edwards C et al (2010) Fault tolerant flight control – a benchmark challenge. Lecture Notes in Control and Information Sciences
28. Lopez I, Sarigul-Klijn N (2010) A review of uncertainty in flight structural damage monitoring, diagnosis and control. Prog Aerosp Sci 46:247–273

29. Gheorghe A, Zolghadri A, Cieslak J, Goupil P, Dayre R, Le Berre H (2013) Toward model-based approaches for fast and robust fault detection in aircraft control surface servo-loop: from theory to application. IEEE Control Syst Mag, June 2013
30. Butler RW (2008) A primer on architectural level fault tolerance. NASA/TM-2008-215108. Langley Research Center, Hampton, VA
31. Lemai S, OLive X, Charmeau MC (2006) Decisional architecture for autonomous space systems. In: 9th ESA workshop on advanced technologies for robotics and automation, Noordwijk, The Netherlands, 28–30 Nov 2006
32. Durou O, Godet V, Mangane L, Perarnaud DP, Roques R (2002) Hierarchical fault detection, isolation and recovery applied to COF and ATV avionics. Acta Astronaut 50(9):547–556
33. Ferrell B, Lewis M, Perotti J, Oostdyk R, Brown B (2010) Functional fault modeling conventions and practices for real-time fault isolation. Ames Research Center; Kennedy Space Center. Available at http://ntrs.nasa.gov/search.jsp?R=20110004336
34. ECSS 70-11A (2005) Space engineering: space segment operability. European Cooperation for Space Standardization standard, August 2005
35. Truszkowski WF, Hinchey MG, Rash JL, Rouff CA (2006) Autonomous and autonomic systems: a paradigm for future space exploration missions. IEEE Trans Syst Man Cybern Part C Appl Rev 36(3):279–291
36. Feather MS, Markosian LZ (2008) Towards certification of a space system application of fault detection and isolation. In: International conference on prognostics and health management, Denver, CO, October 2008
37. Ferell B, Lewis M, Perotti J, Oostdyk R, Goerz J, Brown R (2010) Lessons learned on implementing fault detection, isolation, and recovery (FDIR) in a ground launch environment. Ames Research Center; Kennedy Space Center. Technical report available at http://ntrs.nasa.gov/search.jsp?R=20110004130
38. Ding SX (2008) Model-based fault diagnosis techniques: design schemes, algorithms, and tools. Springer, Berlin/Heidelberg
39. Hwang I, Kim S, Kim Y (2010) A survey on fault detection, isolation and reconfiguration methods. IEEE Trans Control Syst Technol 18(3):636–653
40. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN (2003) A review of process fault detection and diagnosis Part I: Quantitative model-based methods. Comput Chem Eng 27:293–311
41. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN (2003) A review of process fault detection and diagnosis Part II: Qualitative models and search strategies. Comput Chem Eng 27:313–326
42. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN (2003) A review of process fault detection and diagnosis Part III: Process history based methods. Comput Chem Eng 27: 327–346
43. Isermann R (2005) Model-based fault-detection and diagnosis status and applications. Annu Rev Control 29(1):71–85
44. Basseville M, Nikiforov IV (1993) Detection of abrupt changes: theory and application. Prentice Hall, Englewood Cliffs
45. Patton R, Frank PM, Clark RN (1989) Fault diagnosis in dynamic systems: theory and application. Prentice-Hall, Englewood Cliffs
46. Patton R (1997) Fault-tolerant control: the 1997 situation. In: SAFEPROCESS'97, IFAC Symposium on fault detection, supervision and safety, Kingston Upon Hull, UK
47. Chen J, Patton RJ (1999) Robust model-based fault diagnosis for dynamic systems. Kluwer Academic, Boston/Dordrecht/London
48. Bokor J, Szabo Z (2009) Fault detection and isolation in nonlinear systems. Annu Rev Control 33:113–123
49. Cordier MO, Dague P, Lévy F, Mountmain J, Staroswiecki M, Travé-Massuyès L (2004) Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. IEEE Trans Syst Man Cybern B Cybern 34(5):2163–2177

50. Travé-Massuyès L, Escobet T, Olive X (2006) Diagnosability analysis based on component-supported analytical redundancy relations. IEEE Trans Syst Man Cybern A Syst Hum 36(6):1146–1160
51. Beard RV (1971) Failure accommodation in linear systems through self-reorganization. PhD dissertation, Department of Aeronautics Astronautics, Massachusetts Institute of Technology, Cambridge
52. Jones HL (1973) Failure detection in linear systems. PhD dissertation. Department of Aeronautics Astronautics, Massachusetts Institute of Technology, Cambridge, MA
53. Mehra RK, Peschon J (1971) An innovations approach to fault detection and diagnosis in dynamic systems. Automatica 7:637–640
54. Massoumnia MA (1986) A geometric approach to the synthesis of failure detection filters. IEEE Trans Autom Control 31(9):839–846
55. Chow EY, Willsky AS (1984) Analytical redundancy and the design of robust failure detection systems. IEEE Trans Autom Control 29(7):603–614
56. Zolghadri A, Goetz C, Bergeon B, Denoise X (1998) Integrity monitoring of flight parameters using analytical redundancy. In: Proceedings of the UKACC international conference on control (CONTROL '98), Swansea, UK, pp 1534–1539
57. Zolghadri A (1996) An algorithm for real-time failure detection in Kalman filters. IEEE Trans Autom Control 41(10):1537–1540
58. Douglas RK, Speyer JL (1996) Robust fault detection filter design. J Guid Control Dyn 19(1):214–218
59. Chen J, Patton RJ, Zhang HY (1996) Design of unknown input observers and robust fault-detection filters. Int J Control 63(1):85–105
60. Balas MJ (1999) Do all linear flexible structures have convergent second order observers? AIAA J Guid Control Dyn 22(6):905–908
61. Stoustrup J, Niemann JH (2002) Fault estimation—a standard problem. Int J Robust Nonlinear Control 12:649–673
62. Zolghadri A, Castang F, Henry D (2006) Design of robust fault detection filters for multivariable feedback systems. Int J Model Simul 26:17–26
63. Bokor J, Balas G (2004) Detection filter design for LPV systems – a geometric approach. Automatica 40:511–518
64. Yan XG, Edwards C (2007) Nonlinear robust fault reconstruction and estimation using a sliding mode observer. Automatica 43:1605–1614
65. Henry D, Zolghadri A (2005) Design and analysis of robust residual generators for systems under feedback control. Automatica 41:251–264
66. Henry D, Zolghadri A (2005) Design of fault diagnosis filters: a multi-objective approach. J Franklin Inst 342(4):421–446
67. Henry D, Zolghadri A (2006) Norm-based design of robust FDI schemes for uncertain systems under feedback control: comparison of two approaches. Control Eng Pract 14(9):1081–1097
68. Zolghadri A, Henry D, Grenaille S (2008) Fault diagnosis for LPV systems. In: 16th IEEE Mediterranean conference on control and automation, Ajaccio, France
69. Grenaille S, Henry D, Zolghadri A (2008) A method for designing fault diagnosis filters for LPV polytopic systems. J Control Sci Eng. Article ID 231697, Vol 1, January 2008
70. Ganguli S, Marcos A, Balas G (2002) Reconfigurable LPV control design for Boeing 747-100/200 longitudinal axis. In: American control conference. Anchorage, Alaska, USA, 8–10 May 2002
71. Henry D, Zolghadri A, Monsion M, Ygorra S (2002) Off-line robust fault diagnosis using the generalized structured singular values. Automatica 38:1347–1358
72. Raissi T, Videau G, Zolghadri A (2010) Interval observers design for consistency checks of nonlinear continuous-time systems. Automatica 46:518–527
73. Efimov D, Zolghadri A, Raissi T (2011) Actuators fault detection and compensation under feedback control. Automatica 47:1699–1705

74. Saif M, Xiong Y (2003) Sliding mode observers and their application in fault diagnosis. In: Caccavale F, Villani L (eds) Fault diagnosis and fault tolerance for mechatronic systems: recent advances, vol 1, Springer tracts in advanced robotics. Springer, Berlin, pp 1–57
75. Alazard D, Apkarian P (1999) Exact observer-based structures for arbitrary compensators. Int J Robust NL Control 9:101–118
76. Zhou K, Doyle JC, Glover K (1995) Robust and optimal control. Prentice Hall, Upper Saddle River
77. Zhang Y, Jiang J (2008) Bibliographical review on reconfigurable fault-tolerant control systems. Ann Rev Control 32(2):229–252
78. Yang H, Cocquempot V, Jiang B (2009) Robust fault tolerant tracking control with applications to hybrid nonlinear systems. IET Control Theory Appl 3(2):211–224
79. Staroswiecki M, Yang H, Jiang B (2007) Progressive accommodation of parametric faults in LQ control. Automatica 43:2070–2076
80. Alwi H, Edwards C (2008) Fault tolerant control using sliding modes with on-line control allocation. Automatica 44:1859–1866
81. Hamayun MT, Edwards C, Alwi H (2010) Integral sliding mode fault tolerant control incorporating on-line control allocation. In: 11th international workshop on variable structure systems, Mexico City, 26–28 June 2010
82. Ding SX (2009) Integrated design of feedback controllers and fault detectors. Annu Rev Control 33:124–135
83. Gaspar P, Bokor J (2006) A fault-tolerant rollover prevention system based on a LPV method. Int J Veh Des 42(3–4):392–412
84. Liberzon D (2003) Switching in systems and control. Birkhäuser, Boston
85. Marcos A, Balas G (2005) A robust integrated controller/diagnosis aircraft application. Int J Robust NL Control 15:531–551
86. Weng Z, Patton R, Cui P (2008) Integrated design of robust controller and fault estimator for linear parameter varying systems. In: 17th World Congress IFAC, Seoul, Korea
87. Zhang Y, Jiang J (2008) Bibliographical review on reconfigurable fault-tolerant control systems. Annu Rev Control 32:229–252
88. Shin J-Y, Belcastro CM (2006) Performance analysis on fault tolerant control system. IEEE Trans Control Syst Technol 14(9):1283–1294
89. Yang H, Jiang B, Staroswiecki M (2009) Supervisory fault tolerant control for a class of uncertain nonlinear systems. Automatica 45:2319–2324
90. Oudghiri M, Chadli M, El Hajjaji A (2008) Robust observer-based fault tolerant control for vehicle lateral dynamics. Int J Veh Des 48:173–189
91. Morio V (2009) Contribution au développement d'une loi de guidage autonome par platitude. Application à une mission de rentrée atmosphérique (Shuttle orbiter STS-1). PhD dissertation, Bordeaux 1 university, Bordeaux, France
92. Van den Bossche D (2006) The A380 flight control electrohydrostatic actuators, achievements and lessons learnt. In: Proceedings of the 25th Congress of the International Council of the Aeronautical Sciences, Hamburg, Germany
93. Zolghadri A, Gheorghe A, Cieslak J, Henry D, Goupil P, Dayre R, Le Berre H (2011) A model-based solution to robust and early detection of control surface runaways. SAE Int J Aerosp 4:1500–1505
94. Kurtoglu T, Johnson SB, Barszcz E, Johnson JR, Robinson PI (2008) Integrating system health management into the early design of aerospace systems using Functional Fault Analysis. IEEE conference on prognostics and health management, Denver
95. Deckert JC, Desai MN, Deyst JJ, Willsky AS (1977) F-8 DFBW sensor failure identification using analytic redundancy. IEEE Trans Autom Control 22(5):795–809
96. Wilbers DM, Speyer JL (2002) Detection filters for aircraft sensor and actuator faults. In: Proceedings of the IEEE international conference on control applications, Jerusalem, Israel
97. Menke TE, Maybeck PS (1995) Sensor/actuator failure detection in the VISTA F-16 by multiple model adaptive estimation. IEEE Trans Aerosp Electron Syst 31(4):1218–1229

98. Kim S, Choi J, Kim Y (2008) Fault detection and diagnosis of aircraft actuators using fuzzy-tuning IMM filter. IEEE Trans Aerosp Electron Syst 44(3):940–952
99. Chen RH, Ng HK, Speyer JL, Guntur LS, Carpenter R (2004) Health monitoring of a satellite system. In: Proceedings of the AIAA guidance, navigation, and control conference, Boston, August 2004
100. Patton R, Uppal F, Simani S, Polle B (2010) Robust FDI applied to thruster faults of a satellite system. Control Eng Pract 18(9):1093–1109
101. Falcoz A, Henry D, Zolghadri A (2010) Robust fault diagnosis for atmospheric re-entry vehicles: a case study. IEEE Trans Syst Man Cybern Part A Syst Hum 40:886–899
102. Falcoz A, Henry D, Zolghadri A, Bornschleg E, Ganet M (2008) On-board model-based robust FDIR strategy for reusable launch vehicles (RLV). In: 7th international ESA conference on guidance, navigation and control systems, County Kerry, Ireland
103. Henry D, Falcoz A, Zolghadri A (2009) Structured H∞/H− LPV filters for fault diagnosis: some new results. In: 7th IFAC symposium on fault detection, supervision and safety of technical processes, Barcelona, Spain
104. Henry D (2008) Fault diagnosis of the microscope satellite actuators using Hinf/H- filters. AIAA J Guid Control Dyn 31(3):699–711
105. Zolghadri A (2000) A redundancy-based strategy for safety management in a modern civil aircraft. Control Eng Pract 8(5):545–554
106. Zolghadri A (2002) Early warning and prediction of flight parameter abnormalities for improved system safety assessment. Reliab Eng Syst Saf 16:19–27
107. Papageorgiou C, Glover K (2005) Robustness analysis of nonlinear flight controllers. AIAA J Guid Control Dyn 28(4):639–648
108. Rotstein HP, Ingvalson R, Keviczky T, Balas GJ (2006) Fault-detection design for uninhabited aerial vehicles. J Guid Control Dyn 29(5):1051–1060
109. James M, Dubon L (2000) An autonomous diagnostic and prognostic monitoring system for NASA's deep space network. Proc IEEE Aerosp Conf 2:403–414
110. Bernard D, Dorais G, Gamble E, Kanefsky B, Kurien J, Man G, Millar W, Muscettola N, Nayak P, Rajan K, Rouquette N, Smith B, Taylor W, Tung YW (1999) Spacecraft autonomy flight experience: the DS1 remote agent experiment. In: Proceedings of AIAA, Albuquerque, NM, pp 28–30
111. http://www.nasa.gov/centers/ames/research/technology-onepagers/livingstone2-modelbased.html
112. Bickford RL et al (1999) Real-time sensor data validation for space shuttle main engine telemetry monitoring. In: AIAA/ASME/SAE/ASEE 35th joint propulsion conference and exhibit, Los Angeles, CA
113. Lombaerts TJJ (2010) Fault tolerant flight control. A physical model approach. PhD thesis, TuDelft
114. Azam M, Pattipati K, Allanach J, Poll S, Patterson-Hine A (2005) In-flight fault detection and isolation in aircraft flight control systems. In: IEEE aerospace conference, 5–12 Mar 2005
115. http://addsafe.deimos-space.com
116. Goupil P (2010) Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy. Control Eng Pract 18(9):1110–1119
117. http://en.wikipedia.org/wiki/Technology_readiness_level

http://www.springer.com/978-1-4471-5313-9

Fault Diagnosis and Fault-Tolerant Control and Guidance for Aerospace Vehicles
From Theory to Application

Zolghadri, a.; Henry, D.; Cieslak, J.; Efimov, D.; Goupil, P.
2014, XVI, 216 p. 126 illus., 75 illus. in color.,
ISBN: 978-1-4471-5313-9