Fault Tolerance – Background and Recent Trends
Sato Masayuki, Georges Hardier, Gilles Ferreres, Christopher Edwards, Halim Alwi, Lejun Chen, Andres Marcos

To cite this version:

HAL Id: hal-01831956
https://hal.science/hal-01831956
Submitted on 7 Jul 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
Fault Tolerance – Background and Recent Trends

Masayuki SATO* · Georges HARDIER** · Gilles FERRERES** · Christopher EDWARDS*** · Halim ALWI*** · Lejun CHEN*** · Andres MARCOS****

* Japan Aerospace Exploration Agency, 6-13-1 Osawa, Mitaka, Tokyo, Japan
** ONERA The French Aerospace Lab, DTIS, Toulouse, France
*** College of Engineering, Mathematics & Physical Sciences, University of Exeter, U.K.
**** Aerospace Engineering Department, University of Bristol, BS8 1TR, U.K.

E-mail: sato.masayuki@jaxa.jp

Key Words: fault tolerant control, fault detection and identification, adaptive control, sliding mode control/observer, \( H_\infty \) control.

1. Introduction

In 1985, a Boeing 747 airplane crashed on Mt. Osutaka with over 500 persons dead. Japan Transport Safety Board investigated the accident, and concluded that the power loss of the main control devices, which was caused by the break of the aft pressure bulkhead, led to this fatal accident\(^1\). This accident illustrates the importance of fault tolerant flight control.

In this article, several schemes related to the field of Fault Detection and Isolation (FDI), Fault Detection and Diagnosis (FDD), and Fault Tolerant Control (FTC) are presented both from a theoretical perspective and, more importantly, from an application perspective. The focus of the applications is the aeronautical domain and they cover a range of projects undertaken during the last two decades. These projects (some of them funded by the European Commission) showcase the timeline followed in Europe for the evolution and transfer of aircraft Fault Detection, Identification and Reconfiguration (FDIR) scheme, which include FDI/FDD/FTC modules, from academia to the industrial sector.

Three main approaches are presented: (i) Adaptive control (Section 2), (ii) Sliding Mode Control/Observers (SMC/SMO) (Section 3), and (iii) \( H_\infty \) control (Section 4).

2. FDD/FTC via indirect adaptive control

It is well established that Fly-By-Wire (FBW) improves the safety of aircraft significantly. However, the implementation of advanced capabilities for detecting, protecting and optimizing guidance and control\(^2\) requires the availability of aircraft (A/C) states, especially for critical parameters such as the Angle of Attack (AoA) and the Calibrated Air Speed (CAS). Hence, a major issue for the implementation of these FBW advances is their capability to cope with faulty situations (of the corresponding sensors) in order to avoid switching to degraded control modes (i.e., reduced control laws and flight envelope protections). This capability can only be achieved using specific FDD and FTC schemes against these types of faults.

This section focuses on the augmentation of control laws’ availability to provide the Flight Control System (FCS) with the ability to automatically accommodate potential failures or unexpected events. To fill the gap between academic FDD/FTC and industrial practice\(^2\),\(^3\), it is always required to use high-fidelity, nonlinear simulators as well as industrial implementation constraints that address realistic, onboard issues\(^4\),\(^5\).

Specifically, when some key parameters are missing (e.g., the airspeed), the approaches described in this section consist in scheduling the control laws according to estimated versions of those parameters. This must be achieved without degrading the performance and is based on “advanced flight control laws” (see the corresponding block in Fig. 1). Two possible alternatives are examined in here: to replace the faulty measurement by an estimated value (virtual sensing) while keeping the same scheduling strategy (subsection 2.1), or to schedule the laws based on another type of parameter, namely some model coefficients (subsection 2.2). In both cases, the presented approaches rely on so-called Linear Fractional Transformation (LFT) forms (subsection 2.2), and results in analytical scheduling expressions that facilitate the use of robust control design and analysis tools.
2.1 Flight Parameter Estimation (FPE)

Most civil/military aircraft (by Boeing and Airbus) use majority voting mechanisms that rely on multiple sensing channels, e.g., a triplex configuration of Air Data and Inertial Reference Units (ADIRU) as shown in Fig. 1. These configurations assume that a fault will result in inconsistent signals and perform a comparison between the redundant measurements. A more advanced solution relies on analytical redundancy, which refers to the use of existing dynamical relationships between A/C states. This solution relies on sensor data supplemented by a model-based simulation of the flight mechanics to deliver the estimation of the required parameters (the “state estimation” block of Fig. 1). These estimates can be processed in parallel with the measured signals contributing to the way the flight parameters are consolidated (the “advanced FDD” block in Fig. 1).

The concept of analytical redundancy for FCS is not new while that of virtual sensors is more recent. ONERA has been working with Airbus on this topic for a decade and has developed adaptive versions of several nonlinear state estimation techniques to deliver AoA and CAS estimates in faulty conditions. A major obstacle to an operational use of this kind of approaches springs from their implementation in real time (especially from the computational burden of the algorithms) but also from the certification process (which impose stringent requirements to be fulfilled). Several solutions have been proposed by ONERA to limit the complexity of the developed Adaptive Extended Kalman Filter (AEKF): for example, the use of kinematic relationships and random walk processes for the process equations, as well as introducing a priori knowledge only in one output equation (vertical load factor) by means of a simplified modeling of the lift aerodynamic coefficient. The latter approximation is achieved by a set of surrogate models that facilitate on-board implementation and signal differentiation. More details are given in 9) in regards to these surrogate models and the principles of the techniques that permit to obtain rational-type representations (using the APRICOT library of the SMAC Toolbox, w3.onera.fr/smac/?q=apricot, developed by ONERA). As the FDD module is a component of the AEKF, the gain matrix calculation can be adapted continuously, in case of detected/isolated faults, by simply omitting their values in the sequential update process. The tedious linearizations are also replaced by analytical derivations (for the process equations that only involve kinematic expressions as well as for those outputs that rely on surrogate models).

This monitoring/estimation process called FPE was evaluated in RECONFIGURE European project by means of Monte-Carlo campaigns (using the high-fidelity simulator provided by Airbus as well as realistic flight conditions reproducing in-service and worst-case extreme events). Patents are currently being registered by Airbus and ONERA (see 10) for a preliminary version), and advanced validation work is on-going.
It is noted that by using the AoA and/or CAS consolidated estimates as scheduling parameters (for protection or control laws) either the nominal control architecture can be kept or a new gain-scheduled controller can be designed based on the estimated signals. Their principles are given in the next subsection.

2.2 Indirect Adaptive Control

Gain-scheduling is classically used by industry to control an airplane throughout its flight envelope. When a scheduling parameter is unavailable due to a sensor fault, adaptive control is an attractive solution to recover closed loop performance by scheduling the gains with respect to, for example, the aerodynamic model coefficients instead of the usual flight parameters. The principle is to estimate some of the model parameters (identification block in Fig. 1) and to adjust the controller on-line using the updated estimates.

For the gain-scheduling control design component, several state-space techniques are available based on the use of time-varying or time-invariant scheduling parameters. In the approach proposed in [12], the modal technique of [13] is used as it appears especially suitable for A/C applications. It requires building first an open loop LFT model using ONERA’s LFR Toolbox (w3.onera.fr/smac/?q=lfrt) using the main aerodynamic coefficients as model parameters (whose ranges of variation correspond to the set of linearized models used to design the controller). Then, a static output feedback placing the main closed loop poles is synthesized also in an LFT form. In [12], a surrogate model of the LFT gains was derived off-line to minimize the onboard computation (using also the SMAC/APRICOT Toolbox).

The second issue of the adaptation process requires the model parameters to be estimated on-line [14] with the capability to track time-varying coefficients in the face of measurement noise, poor data content, and external disturbances (turbulence). Residual errors will sometimes be large and a measure of the parameter accuracy should also be provided so that some logic can be introduced: e.g., if the estimated parameters are not reliable enough, one can switch to a robust back-up controller ensuring minimal performance properties [14]. To address this issue, algorithms for recursive parameter estimation are used, for example: Time Domain (TD) methods are based typically on recursive least-squares, or on Extended Kalman Filter (EKF) when coping with non-linearities. However, onboard computer limitations preclude the use of these methods, e.g. any iterative algorithm resulting in some unbounded computation loop through the data. Hence complex operations like non-analytical matrix inversions should be avoided. Accordingly, TD algorithms seem preferable as the most basic versions only involve very simple operations (matrix inversion replaced by a scalar division) [15]. Another solution comes from the Frequency Domain (FD) techniques which have many desirable features [14]: e.g. computation time is reduced by processing only a limited amount of frequencies within the bandwidth of interest, and the resulting indirect filtering of the wide-band disturbances (e.g., low frequency mismatch or high frequency noise) improves estimation accuracy [16], [17].

Otherwise, TD and FD estimation schemes can rely on a fully recursive algorithm (i.e. using measurements as soon as they are available) or alternatively on a kind of sequential procedure, processing moving data windows with a lower rate to get a succession of piecewise constant values. Such an approach was used for actuator faults’ FDD during the ONERA/DLR research project IMMUNE [17], [18]. In [12], [14], it is shown that FD approaches can also be simplified to reduce their complexity, similarly to what is done for TD formulations, and they can also include similar advanced mechanisms such as data forgetting [15], [19]. It can also be used for FDD purposes by monitoring the changes in the parameters to diagnose unexpected behaviors [17].

The described indirect adaptive process has been evaluated also within the RECONFIGURE project using the high-fidelity simulator provided by Airbus [20]. It is also noteworthy that the worst-case validation of a similar adaptive scheme was already investigated by Airbus and ONERA [20].

3. FTC and FDI via Sliding Mode Scheme

SMC schemes have a number of interesting properties, which fuelled the continued research interest in this field since the 1960s. Perhaps the key property is its inherent insensitivity (at least theoretically) to so-called matched uncertainty – i.e. uncertainty acting in the channel of the input control signals [21], [22]. Many different paradigms for the design of linear sliding surfaces for uncertain linear systems have been
developed, and this area of research is quite mature \cite{21, 22}. In conventional sliding modes the closed-loop behaviour can be split into two well-defined distinguishable phases: a) the pre-sliding phase in which the controller drives the system states towards the sliding surface prior to achieving a sliding mode; and b) the reduced order sliding motion which occurs once the surface is attained and the states are forced to evolve along this surface. Since actuator faults can be considered as matched uncertainty, sliding mode control is a good candidate paradigm for FTC. The combination of SMC with Control Allocation \cite{23} (thought of as a mechanism for distributing control signals in over-actuated systems) has the benefit of providing SMCs with access to redundant actuators, and thus enabling the overall control scheme to handle actuator failures in addition to faults.

### 3.1 FTC via Sliding Mode Control

Figure 2 illustrates the overall FTC strategy \cite{24} where it is assumed that the Control Application (CA) module depends on the effectiveness of the actuators. The information necessary to compute these quantities on-line can be supplied by a FDI/FDD scheme, or by using a measurement of the actual actuator deflection compared to the demanded deflection. If an actuator fault occurs, the actuator effectiveness (written as $W$ in Fig. 2) will be changed online and the control input is reallocated to minimize the use of the faulty surfaces \cite{24}.

![Fig. 2 Control allocation strategy](image)

To ensure robustness and performance over a wide range of operating conditions, the original sliding mode control allocation scheme presented in \cite{24} has been extended within a Linear Parameter Varying (LPV) framework \cite{25}. This FTC-SMC scheme has been implemented on various industrial applications. For example, during the GARTEUR FM-AG16 project \cite{26} it was applied to the ADMIRE and the RECOVER benchmark aircraft models (to cope with elevator and stabilizer failures) and then tested on the Technical University of Delft SIMONA piloted motion simulator \cite{25, 26} (Fig. 3).

Continuing the above research, during the RECONFIGURE project \cite{27}, an Integral Sliding Mode (ISM) approach was adopted \cite{22} to deal with random elevator failures. The resulting industrial evaluation of the scheme showed a very low computational load indicating no limitations for future onboard implementation. The main advantage of the scheme, as shown in Fig. 4, is that it can be retro-fitted to existing control loops without the need for their redesign.

### 3.2 FDI via Sliding Mode Observers

Sliding mode ideas can also be considered in an observer context. The novelty of SMO is their ability to reconstruct un-measurable signals within a process by appropriate scaling and filtering of the so-called “equivalent output error injection” \cite{22}. This is a unique property of SMOs which emanates from the fact that the introduction of a sliding motion forces the outputs of the observer to perfectly track the plant measurements.

As part of the RECONFIGURE project, the problem of estimating fault signals using SMOs was considered based on an additive perturbation model of the form

$$\dot{x}(t) = Ax(t) + Bu(t) + Ff_i(t, u) + M\xi(t, y, u)$$
where $f_i$ represents actuator faults and $\xi$ encapsulates uncertainty. The aim was to design an SMO of the form

$$\dot{z}(t) = Az(t) + Bu(t) - G_\ell y(t) + G_n v(t)$$

where $e_y = C(z - x)$ and $v(t) = -\rho_o(t, y, u)\text{sign}(e_y)$, to force and maintain sliding on $S = \{e : Ce = 0\}$ with $e = z - x$ representing the state estimation error.

The reconstruction signal is designed by choice of $H, G_n$, so that: (i) it tends to $f_i$ when $\xi = 0$ (at worst asymptotically), and (ii) the $L_2$ gain $\gamma$ between $\xi$ and the fault residual is minimised (a convex problem).

The ADDSAFE benchmark included a scenario with a potentially faulty yaw rate signal emerging from the air data and inertial reference system. A sliding mode scheme based on the observer structure above was “flight-certified” coded for this scenario and validated on the Airbus Flight Control Computer (FCC) demonstrating its FDI performance and robustness via Monte Carlo campaigns.

4. FDD and FTC via $H_\infty$ Control

FDD and FTC approaches based on $H_\infty$ optimization have been proposed and consolidated in academia for the last 20 years. Very relevant success stories of $H_\infty$ controllers flying (or flown) are: telecommunication satellites, the Ariane launcher, and spacecraft such as the European Automated Transfer Vehicle (ATV), ESA Rosetta, and CNES MICROSCOPE. In this section a brief review of FDI/FTC $H_\infty$ theory and its use on aerospace projects is presented.

4.1 Theory of Model-Based Approach

The essence of model-based FDI/FDD problem, on which $H_\infty$ theory is based, is depicted in Fig. 5 and can be formalized as follows (assuming no uncertainty or disturbances besides faults):

**FDI/FDD problem:** Given a model of a nominal system $Gu$ and knowledge (measured or estimated) of the inputs $u$ and outputs $y$ of the system, the FDI/FDD problem consists of finding a filter $F = [F_u F_y]^T$ that provides a fault estimate $res$ containing information on the actual faults $f$ entering the system (through $G_f$).

The fault estimate (also known as residual) $res$ can provide just an indication of the fault’s presence (fault detection) or also the fault location and source (fault diagnosis). Fault detection requires only a single (scalar) value while fault diagnosis requires a set (vector) of fault estimates to distinguish between different faults. The residual definition is given by:

$$res = F_y y + F_u u = F_y (G_f f + G_\alpha u) + F_u u = F_y G_f f + (F_u + F_y G_\alpha) u$$

It is now straightforward to identify the main objectives of an FDI/FDD scheme: i) Maximize the fault effects (using $F_y$ and the knowledge of the fault effects on the system $G_f$), and ii) minimize any other effect (e.g. controller input $u$, uncertainty, disturbances, other subsystem faults, etc.).
By adding the disturbance $d$ effects to the output of the system $y$, the equation above is transformed into:

$$res = F_y G_f f + F_y G_d d + (F_u + F_y G_u)u$$

This clearly shows that if a fault affects the system along the same direction as a disturbance (i.e. $G_f = G_d$) then it is not possible to detect such fault. The above discussion is based on an open-loop FDI/FDD design perspective, and although it is also possible to apply them to closed-loop systems, open-loop is typically favoured.

### 4.2 $H_\infty$ FDIR Optimization

The problem of designing a robust FDI/FDD scheme is generally divided in to two main stages: robust residual generation and robust residual evaluation (if reconfiguration is also desired there is a third step that uses the latter’s signals to compensate fault effects). Within the task of residual generation, and from the $H_\infty$ perspective, the idea is to obtain a filter $F = [F_u \ F_y]^T$ so that: i) $F_u$ cancels the effects of the known inputs $u$, and ii) $F_y$ maximizes the effects of the faults $f$ (while minimizing the effects of the disturbances $d$ based on the frequency regions they act upon). This is accomplished using so-called weighting filters $W_z$ which embed this frequency content knowledge as well as the desired design objectives into the $H_\infty$ optimization framework. A general methodology is given in 36), 40) ~ 42).

In order to exemplify the methodology, assume a nominal LTI plant $G = [G_f \ G_d \ G_u]^T$ is given and it is desired to design an FDD filter $F = [F_u \ F_y]^T$ following a design rationale based on fault model-matching (this strategy has several advantages for FDD, see 29) and 42)). First, the $H_\infty$ FDI interconnection, see Fig. 6, is set then in this case three weights are defined to drive the optimization: $W_f$ (shaping the ideal fault knowledge and/or desired filter behaviour), $W_d$ (shaping the disturbances) and $W_u$ (for shaping the control command). The optimization will minimize the induced $L_2$-norm of the transfer function from the inputs to the error. The shaping filters are used to emphasize the frequency regions where it is desirable to achieve these objectives, resulting in a direct way to perform the design trade-off.

### 4.3 Aerospace applications of $H_\infty$ FDI/FTC

Similar to the previous Sections 2 and 3, the $H_\infty$ approach has been matured from an aircraft FDIR perspective during the past 20 years. An incomplete list of projects and applications is given here, see the detailed survey of 30) for a more broad presentation.

1. Boeing 747 aircraft simulation model

The work of 42) is considered as the first instance that an $H_\infty$ FDI filter was designed for a high-fidelity, full nonlinear aircraft simulation model. The nonlinear time results (including sensor noise and gust) showed the good properties of the $H_\infty$ filters despite aircraft motion changes arising from longitudinal maneuvers. This demonstration led to an active European-based impetus on the FDI/FTC topic starting with the establishment in 2004 of the GARETEUR FM-AG16 “Fault Tolerant Control” which ran until 2008 and included verification of a number of FDI approaches (see also previous sections) in a nonlinear simulator based on that from 43) and up to pilot simulations in SIMONA.

2. Piloted simulations in DLR ATTAS aircraft

As part of the German Aerospace Center (DLR) “Saturation Alleviation In-Flight Experiment” (SAIFE) test campaigns an $H_\infty$ FDI scheme following that of 42) was demonstrated in piloted simulations. The SAIFE campaigns were performed on DLR Advanced Technologies Testing Aircraft (ATTAS), and focused on assessing the effectiveness of advanced anti-windup compensators against saturation. As these effects can be construed as unknown faults, FDI filters were designed using $H_\infty$ and $\mu$ synthesis tools for the residual generation, and online thresholding algorithms for the residual evaluation. The results showed good FDI capabilities under quite demanding one-axis maneuvers.
(3) Industrialization FDI: ADDSAFE EU project

For the ADDSAFE project\(^4\), and following the above two references\(^{42,46}\), an $H_\infty$ FDI filter was designed for detecting aileron actuator faults in the ADDSAFE Airbus benchmark. The specific scheme\(^47\) followed a global aircraft $H_\infty$ FDI scheme for the residual generation (i.e. using sensor measurements from the aircraft as opposed to only inputs/outputs of the actuator) and a simple time/magnitude logic for the residual evaluation (tasked with fault isolation between left and right inboard ailerons). The design was evaluated in a Monte Carlo campaign and was one of five (out of 13) qualified by Airbus as ready for industrial validation\(^48\).

An additional outcome from ADDSAFE, but not related to $H_\infty$, was that one of the teams was able to further develop their design in collaboration with Airbus and recently it has been certified and implemented on the A350 family\(^49\) for servo-loop oscillatory failures\(^50\).

(4) Industrial FTC: RECONFIGURE EU project

In reference 50), an FTC design based on the structured $H_\infty$ synthesis approach (a more recent synthesis algorithm) was presented against elevon malfunctions for the RECONFIGURE benchmark. The structured $H_\infty$ approach uses non-smooth optimization to obtain the gains of a pre-defined control architecture (thus preserving the legacy knowledge from industry) within an $H_\infty$ formulation (thus allowing for a direct performance versus robustness trade-off). The standard aircraft C* control architecture\(^51\) was used for the FTC law, and its effectiveness was demonstrated using the Airbus benchmark\(^52\).

5. Current Project

From March in 2016, a new Europe-Japan collaborative project called “VISION” (Validation of Integrated Safety-enhanced Intelligent flight cONtrol) has started. The main objective of this project is to increase Technology Readiness Level (TRL) for filling-up the gap between theories and practical systems on FTC/FDD schemes\(^51\). To this end, one of JAXA’s research airplane MuPAL-α is used to demonstrate the usefulness and to examine the possible drawbacks of the methods above. In addition, Simple Adaptive Control (SAC) will be also implemented as a candidate of FTC control scheme.

Finally, all authors appreciate the funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 690811 and the Japan New Energy and Industrial Technology Development Organization under grant agreement No. 062800, as a part of the EU/Japan joint research project entitled “Validation of Integrated Safety-enhanced Intelligent Flight cONtrol (VISION).” (Received January 19, 2018)

References

1. 日本航空 123便の岡山機長事故に関する航空事故調査報告書についての解説：運輸安全委員会 (2011)
2. P. Goupil et al.: AIRBUS efforts towards advanced real-time fault diagnosis and fault tolerant control, 19th IFAC World Congress, Cape Town (2014)
18. C. Döll, G. Hardier, A. Varga, and C. Kappenberger: IMMUNE: Intelligent Monitoring and Managing of UNexpected


60 A. Marcos: Assessment on the ADDSAFE Benchmark Simulator of an $H_{\infty}$ Fault Detection Design for Aircraft, 8th IFAC SAFEPROCESS, Mexico (2012)

61 P. Goupil and A. Marcos: Industrial benchmarking and evaluation of ADDSAFE FDD designs, The 8th IFAC SAFEPROCESS, Mexico DF, Mexico (2012)


63 A. Marcos: Revisiting the aircraft $C^\infty$ control law: a comparison between classical and structured H-infinity designs, 1st *IEEE Conference on Control Technology and Applications*, Hawaii, USA, August (2017)
