The challenge of advanced model-based FDIR techniques for aerospace systems: the 2011 situation

Ali Zolghadri
IMS lab, Université Bordeaux 1 - CNRS
351 cours de la Libération
33405 Talence cedex
France

Abstract

This keynote discusses some trends and recent advances in model-based Fault Detection, Isolation and Recovery (FDIR) for aero-space systems. The FDIR challenges range from pre-design and design stages for upcoming and new programs, to improvement of the performance of in-service flying systems. For space missions, optimization of flight conditions and safe operation is intrinsically related to GNC (Guidance, Navigation & Control) system of the spacecraft and includes sensors and actuators monitoring. Many future space missions will require autonomous proximity operations including fault diagnosis and the subsequent control and guidance recovery actions. For upcoming and future aircraft, one of the main issues is how early and robust diagnosis of some small and subtle faults could contribute to the overall optimization of aircraft design. This issue would be an important factor for anticipating the more and more stringent requirements which would come in force for future environmentally-friendlier programs. The paper underlines the reasons for a widening gap between the advanced scientific FDIR methods being developed by the academic community and technological solutions demanded by the aerospace industry.

Nomenclature

FDIR	=	Fault Detection, Identification and Recovery
EFCS	=	Electrical Flight Control System
FDD	=	Fault Detection and Diagnosis
FTC	=	Fault Tolerant Control
FTG	=	Fault Tolerant Guidance
GNC	=	Guidance, Navigation and Control
HMI	=	Human Machine Interface
LTI	=	Linear Time Invariant
LPV	=	Linear Parameter Varying
TRL	=	Technology Readiness Level

1. Introduction and problem setting

1.1. Industrial state-of-practice

Innovative and viable FDD, FTC and FTG technologies that will improve spacecraft safe operation and availability pose significant new challenges, ranging from pre-design and design stages for upcoming and new programs, to improvement of the performance for in-service flying systems. The basic issues involving general health management architecture tradeoffs 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 [36]. The conventional techniques currently in use in aerospace systems are now industrially well mastered and well characterized and all expected failures are anticipated and uncovered. The hardware redundancy-based technique is the standard industrial practice and provides high level of robustness and good performance. Fault detection is mainly performed by cross checks, consistency checks, voting mechanisms, and built-in test techniques of varying sophistication. 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. Flight conditions-based thresholds, once validated with all the

known delays and uncertainties in the signal propagation (acquisition, frequency, filtering . . .), are used for rapid recognition of out-of-tolerance conditions. 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 [35]. Today, these standard FDD techniques are implemented in all aerospace systems and also correspond to current certification processes. The main advantage of their simplicity is that it allows designers and operators to use and manage them easily. The paper [35] focuses on a typical Airbus EFCS and provides a detailed description on the industrial practices and strategies for FTC and FDD in civil aircraft.

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. 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 [41], [90]. FDIR strategy can be divided between all levels: detection and local reconfiguration in the subsystems, fault diagnosis and global reconfiguration at the operational level, 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 which becomes costly as the complexity of in-board hardware and software architectures increase.

1.2. Academic advanced results

A large body of literature on FDD and FTC is now available. The open literature dealing with FTG is much more limited. The interested reader may also refer to AIAA or IEEE databases for more specific FDD, FTC or FTG topics. Good surveys about academic state of the art can be found in [1]-[13]. 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. The goal of the FDD unit is to detect, isolate and estimate the severity of a *fault*. IFAC Technical Committee SAFEPROCESS defines a fault as an unpermitted deviation of at least one characteristic property or parameter of the system from the standard condition [7]. 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. The reconfiguration unit utilizes information on the estimated fault and adjusts the controller parameters to recover the system from the faulty condition. The recovery and reconfiguration actions can have different goals and characteristics depending on the considered system. FTC systems seek to provide, at worst, a degraded level of performance in the faulty situations [73], [93]. For aerospace vehicles, FTG could provide a greater flexibility for safe recovery in case of degraded flight conditions. This means on board reshaping of the mission objectives [72].
The paper will focus mostly on FDD. FDD methods are classified generally into three categories, which include the knowledge or history based methods ([5], [62], [63]), analytical model based methods and signal based methods [9]. In this paper, we focus on analytical model based approaches. The early studies on model-based FDD appeared about forty years ago. In [42], [43] and [44] innovation signals are used to design detection filters. Many basic solutions have appeared during the eighties: parity space and observer-based approaches, eigenvalue assignment or parametric based methods ([7], [10], [11], [12], [45]). In the nineties, a great number of publications dealt with specific aspects such as robustness and sensitivity, diagnosis oriented modeling or robust isolation [1], [9], [12], [15], [16], [46], [48], [50]. The European school has been very active in the development of this field, see for example and among others [1], [11]-[13], [56]-[61], [30], [54]. A large number of the most important studies originated from European researchers who have much contributed to the general field of model based FDD. 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[1]. Dedicated international conferences (IFAC SAFEPROCESS, IEEE SysTol ...) are organized periodically, and a large number of sessions in major international conferences on Control (CDC, ECC, ACC, IFAC WC, ...) is dedicated to FDD/FTC topics.

1.3. Advanced model-based techniques for aerospace systems

[1] The "web of Science" reports around 4000 published papers on FDD topic during the last decade in all engineering fields.

Coming back to the industrial point of view, it is obvious that any modification to the existing in-service systems should be motivated, first of all, by a real industrial need. Consider for example a range checking fault detection method devoted to the detection of runaways in aircraft control surfaces servo-loops [92]. 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 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 tradeoff 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.
There exist a number of "case study" in the open literature which are fragmented across many journal and conference papers (see among others [17]-[31], [91], [94]). For space missions, one can mention the precursor NASA's New Millennium Program [88]: 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 re-planning following otherwise unrecoverable failures, and system-level fault protection [89]. The FDD challenges for aircraft flight control systems are being investigated within the European project ADDSAFE[2]. Analytical redundancy has been used on A380 for the detection of a very specific failure case [34]. However, so far, the advanced FDD / FDIR methods have not been really accepted by the aerospace industry. A widening gap does exist between the advanced methods being developed by the academic community and those currently in use by the industrial end-users.
Aerospace industry needs continuous improvement including insertion of new technologies that should be assessed by TRL measure [95]. 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 and are well mastered by aerospace industry actors and end-users. However, a "dead valley" do exist which corresponds to TRL4-TRL5 (validation in relevant environment). This applicability gap has resulted in a real technological barrier which cannot be overcome without more coordinated and large scale actions federating academic and industrial actors, agencies and governments (see for instance [96]).
Many of the early academic published 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 ...". In light of the above observations, it appears that this basic and historical argument which played a driving role to motivate the early development of FDD academic research could be very misleading when applied to the aerospace vehicles. A good balance between conventional 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 [36] where the author developed several clever 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.

The question is: how the advanced methods being developed by the academic community could become a part of the innovative technological solutions demanded by the aerospace industry for their future programs. The analysis and conclusions offered herein is based on the author's personal experience and lessons learned through his involvement in several research projects with major aerospace actors in Europe.

The paper is organized as follows. Section 2 presents a general overview of model based FDD, reconfiguration aspects and interactions between FDD and reconfiguration unit. In this section an iterative refinement process for FDD is also briefly presented. Finally, section 3 discuses some future challenges.

2. Analytical FDD

2.1. Basic structure and ideas

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)

[2] Advanced Fault Diagnosis for Sustainable Flight Guidance and Control : http://addsafe.deimos-space.com

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 basic structure of a classical model based FDD technique can be depicted in figure 1:

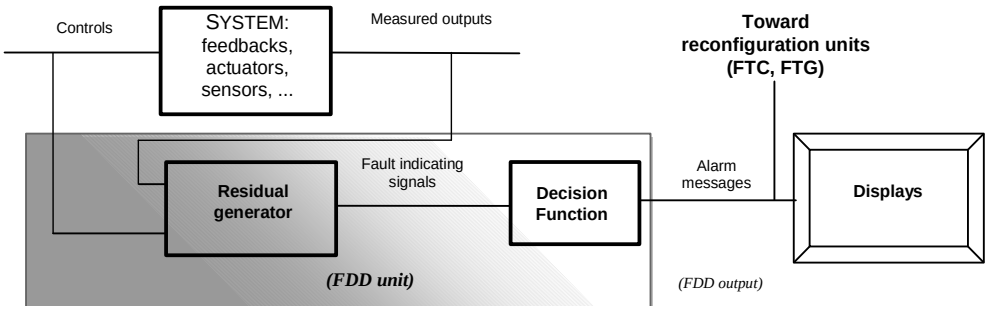

Fig. 1. FDD basic structure.

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 a nice alternative solution. 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 residuals generated 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 and trend 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 for example [9].

To enhance the robustness of FDI schemes against small parameter variations and other disturbances during residual generation, different design and evaluation tools have been proposed ([1], [2]). The objective of any robust FDI method is to make the residuals become sensitive to one or more faults whilst 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 these sensitivity properties over a suitable range of the system's dynamic operation. A huge literature is now available dealing with various aspects of a FDD problem, ranging from modelling problems (nominal system modelling, fault modelling, disturbance and uncertainty modelling ...) 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, sliding modes methods ... The interested reader can refer for example to [1], [2] for recent surveys. 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. The things get much more complex in the nonlinear case, from a design but also an analysis point of view. For a good survey on nonlinear FDI methods, the interested reader can refer to [13] 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 non linear problems is based on the LPV transformation. Consider for example a nonlinear system be described by:

$$\dot{x} = f(t, x, u, w), y = h(x) + v \quad \textbf{(1)}$$

where $x \in R^n$, $u \in R^m$, $w \in R^l$, $y \in R^p$, $v \in R^p$ 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:

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

(2)

where the scheduling parameter vector $\rho \in \mathsf{P}$ is considered to be time-varying (measured or estimated upon system operation) or unknown with known bounds, P is a set of functions that remain in a compact real subspace. The system (2) is an equivalent representation of (1), in the sense that all trajectories of (1) remain in the trajectories of (2). The basic idea is to replace nonlinear complexity of the model (1) by enlarged parametric variation in the linear model (2) which simplifies the design of an observer for (1).
Many FDD approaches have been restricted to linear systems or specific nonlinearities. In the next section, and among many other FDD methods, a solution is presented to illustrate more precisely a procedure for FDD filter design. This design solution has the advantage to take into account directly the controller actions within the design procedure and merges optimally all available information to build the residual signals. The design method is associated with a suitable post-analysis process, to establish an iterative refinement cycle to get a good balance between different design trade-offs, and to get "as close as possible" to the required robustness/performance specifications. The whole procedure is taken from [56]-[58].

2.2. An iterative refinement design/analysis process

Let be *y* the measured output, *u* the control input which is generated by a controller *K*. Let *z* be defined as a linear combination of *y* and *u*.

$$z = M_y y + M_u u \qquad \textbf{(3)}$$

where M_u and M_y are constant matrix of appropriate dimensions. The diagnosis filter, *F*, is supposed to generate an error signal

$$e = z - \hat{z} \qquad \textbf{(4)}$$

where $\hat{z}$ is an estimation of *z*. The H_∞ robust filtering problem is to find *F* which minimises the worst case estimation error energy $\|e\|_2$ over all bounded-energy external disturbances *d*, that is

$$\min_F \sup_{\|d\| \neq 0} \frac{\|e\|_2}{\|d\|_2} \qquad \textbf{(5)}$$

Hence, the robust H_∞ filter minimises the energy gain of the system from the disturbance *d* to the estimation error *e*. Using the L_2-gain property of the H_∞ norm, this problem is equivalent to the following H_∞ norm minimisation problem:

$$\min_F \|T_{de}\|_\infty \qquad \textbf{(6)}$$

where T_{de} is the transfer function from the disturbance *d* to the estimation error *e*. The robust problem is to find *F* such that:

$$\bar{\sigma}(T_{de}(j\omega)) < \bar{\sigma}(W_d(j\omega)) \qquad \forall \omega \qquad \textbf{(7)}$$

where $W_d(s)$ is a dynamic weighting function associated to the robustness constraint.

Now, let *f* be a fault vector affecting the plant. The condition for robust fault sensitivity requirement can be expressed as a worst-case criterion for the sensitivity of the residual signal to faults. Here, the smallest gain of T_{fe} is used to represent the fault sensitivity:

$$\underline{\sigma}(T_{fe}(j\omega)) > \underline{\sigma}(W_f(j\omega)) \qquad \forall \omega \in \Omega_f \qquad \textbf{(8)}$$

where $W_f(s)$ is a dynamic weighting function associated to the sensitive constraint and Ω_f is a pre-specified frequency grid where the robust fault sensitivity index needs to be optimised. The condition (8) guarantees the worst-case sensitivity of *e* to faults over the frequency range Ω_f . The requirements (8) and (7) are to be satisfied for all model perturbations such that:

$$\Delta \in \underline{\Delta}, \quad \|\Delta\|_\infty \leq 1 \qquad \textbf{(9)}$$

Where $\underline{\Delta}$ is an uncertainty structure containing all parametric variations and modelling errors.

The relations (7) and (8) can be written as

$$\left\|T_{de}(j\omega)W_d^{-1}(j\omega)\right\|_\infty < 1 \qquad \textbf{(10)}$$

$$\left\|T_{fe}(j\omega)W_f^{-1}(j\omega)\right\|_- > 1 \quad \forall \omega \in \Omega_f \qquad \textbf{(11)}$$

So, the equivalent scheme for robust fault detection filter design is shown below:

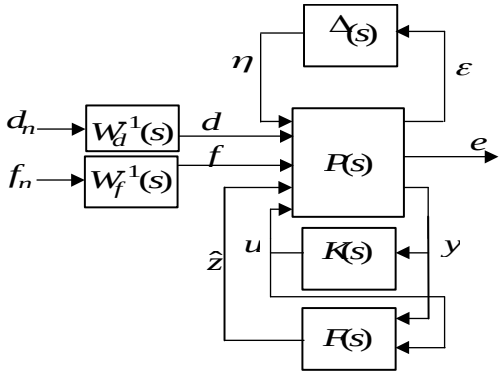

Fig. 2. General block representation for robust fault detection filter design.

It is obvious that in the above formulation, the user-chosen weights $W_d(s)$ and $W_f(s)$ are application-dependent. From a practical point of view, $W_d(s)$ and $W_f(s)$ can be determined by analysing transfer matrices $T_{d\to z}(s)$ and $T_{f\to z}(s)$. To solve the above problem in a H_∞ context, introduce a fictive output signal *r* as illustrated in the following figure:

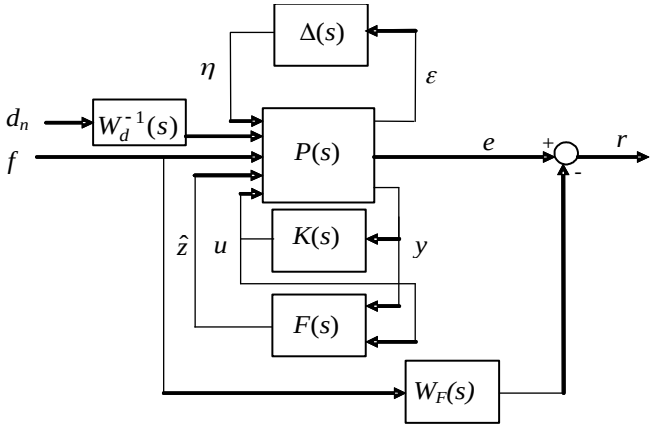

Fig. 3. General interconnection framework

Here W_F is a user-chosen weighting function which represents fault sensitivity objectives such that:

$$\inf_{\omega} \underline{\sigma}(W_F(j\omega)) > \lambda \quad \forall \omega \in \Omega_f \qquad \textbf{(12)}$$

where λ is a scalar. The initial min-max optimisation problem is then transformed into a maximum gain optimisation problem. The optimization problem can be efficiently solved by LMI techniques. Note that the condition (12) is only a sufficient condition and so it may introduce some conservatism in the design.

The above framework is reputed to give robust but conservative solutions. The problem comes from the fact that, once the diagnostic filter is designed, no systematic analysis procedure is proposed to refine and manage the design trade-offs. The design method should be associated with a suitable post-analysis process, leading to an iterative refinement process in order to get a good balance between different design trade-offs, and to get "as close as possible" to the required robustness/performance specifications. Testing the performance of residual generators results in a min-max optimization problem which is solved using a "generalized µ-analysis" procedure ([74]). Note that robust poles assignment and H_2 specifications can be integrated to the design process to tune the transient response and to enforce some minimum decay rate of the residuals. The question is: given the filter *F* designed as in the previous section, do the fault sensitivity objectives are achieved for all model perturbations? Under plant perturbation, the effect that the exogenous disturbances acting on the system have on FDI output can greatly increase. In most case, the fault detection performance will then degrade to the point of unacceptability. A robust performance test is then needed to indicate the worst-case level of performance degradation associated with a given level of plant perturbation. To proceed, consider the block diagram depicted in Fig. 2 and include the designed filter *F* into the model *P*. This leads to the set-up described by the block diagram shown on Fig. 4, where $R(s) = F_l(P(s), F(s))$. Here, we consider that all weighting functions are included in *R*. Δ is defined as in (9) and Δ_d is defined as in the previous section.

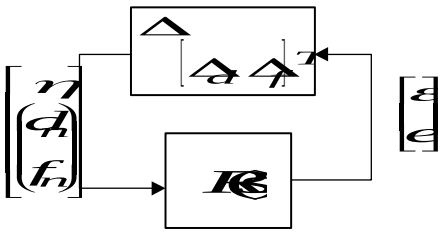

Fig. 4. General set-up for robust fault sensitivity

The solution to the robust sensitivity performance problem uses a procedure based on the recently developed generalised structured singular values (μ_g). μ_g guarantees stability with respect to block-structured perturbations, where some elements of the perturbation structure are bounded from above and some are bounded from below. The robust fault detection sensitivity problem is essentially a robust minimum gain problem, over a pre-specified frequency grid. An appropriate constant matrix test, i.e., the test for each fixed frequency $\omega \in \Omega_f$ can be formulated by using the μ_g function. For more details, see [74]. To summarize, the overall design/analysis refinement process provides a practically relevant framework in which various design goals and trades-off can be easily formulated and managed. The main characteristics are summarized below:

- Systematic formulation of different design trade-offs. H_∞ specifications are convenient to enforce robustness to model uncertainty (e.g. external disturbances, parametric uncertainties and neglected dynamics) and to take into account frequency-domain specifications. H_- specifications are useful for fault sensitivity requirements over specified frequency ranges. H_2 objectives allow us to take into account the stochastic nature of disturbances and measurement noises. H_{2g} specifications and regional filter poles assignment are convenient to tune the transient response and to enforce some minimum decay rate of the residuals. This feature becomes very important from a decision making point of view, as the residual is post-processed by a hypothesis-based test to make a final decision about the fault.
- The residuals structuration matrices (*static)* are jointly optimized with the dynamical part of the FDI filter. Their role is to merge optimally the available on-board measurement and control signals to build the fault indicating signal.
- The control system can be included explicitly in the design.
- The μ_g tool is used as FDD-oriented performance measure: similarly to the μ-analysis procedure that allows for checking the robust performance of any LTI control law, the μ_g tool can be used as a general FDD-oriented performance measure for LTI model-based fault diagnosis scheme.

An example ([27])
Microscope is a satellite on a circular, quasi-polar, sun-synchronous orbit at an altitude of 700km with ascending and descending nodes at 6:00 and 18:00 respectively [27]. To carry out its mission, Microscope combines two rotation motions: the first one is the rotation around the Earth with a constant velocity and the second one is the spin rotation at a constant velocity. To control the satellite trajectory, Microscope uses the coupling of six ultra-sensitive accelerometer sensors, a stellar sensor and a very precise electric propulsion system composed by twelve Field Emission Electric Propulsion (FEEP) thrusters. A FEEP actuator is also a ions extraction engine. If a FEEP thruster fault occurs, it can lead the mission to be failed since the satellite may not compensate for non-gravitational perturbations which are indispensable prior conditions for testing the Equivalence Principle (satellite mission).The faulty situations correspond to FEEP thrusters blocking themselves or closing during operating. Furthermore, simultaneous and multiple thrusters faults are considered, still the control law keeps stability. Nonlinear simulations show that faults are successfully detected and isolated, despite the presence of measurement noises, measurement delays, sensor misalignment phenomena and disturbances (i.e. third-body disturbances, J2 disturbances, atmospheric drag and solar radiation pressure). The results of the above procedure are depicted in figures below. Fig 5 shows an example of design: robustness to 11 thrusters, sensitivity to one. Fig 6 shows analysis results with μ_g.

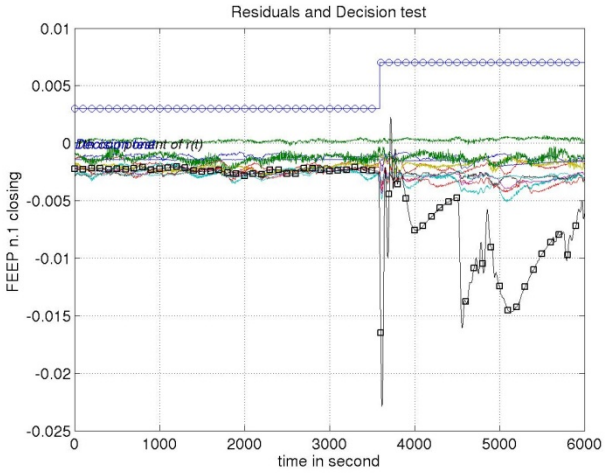

Fig. 5. Example for design

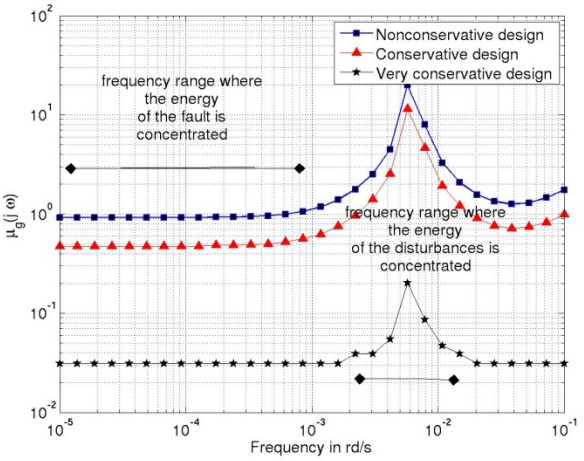

Fig. 6. Example for analysis

2.3. Recovery aspects

The next step following the design of an FDD system would be to set up appropriate recovery strategies, based on all available actuator/sensor/communication resources. The Recovery aspects have also been extensively studied [3]. The general objective is firstly to maintain stability and secondly to keep some performance level in fault situations. For reconfiguration mechanisms be successful, information about the failed element (fault identification) is necessary in order to access the remaining control resources. The interaction with the FDD unit is 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 pre-computed control law depending on the faults which have been identified by the FDI system. In this case, hybrid control or switching control structures are commonly encountered in the literature [85].
- 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 [83].
- 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 [76].

The interested reader can refer to ([77]-[80], [84], [87]) and the references therein for more details.

2.4. Interaction between FDD and recovery actions

The majority of the available methods rely implicitly on the assumption that the FDD and automatic reconfiguration & recovery units are assumed to operate correctly: outputs are instantaneously available to provide decisions and/or actions to other subsystems. The problem of guaranteeing stability and performances of the overall fault tolerant scheme taking into account both the FDD performances (detection delay ...) and reconfiguration system have not been sufficiently considered in the literature. Usually, the desired characteristics are checked (after the design) by means of a Monte-Carlo campaign through nonlinear simulations. Note that for aerospace applications validation assumes testing all possible cross-path situations which becomes costly with the GNC complexity increase, and leads to intricate validation processes. This process often limits the capability of "fail operational" strategies for some critical situations. Several more formal solutions have been published recently. The effect of the FDD delay can be analyzed for linear systems ([82]). In [86], a supervisory scheme uses a switching algorithm to fault isolation: a sequence of controllers is switched, until the appropriate one is found. Other works tempts to combine a fault tolerant controller and a diagnostic filter in both LTI and LPV setting (see for instance [77]-[81]). 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. An attempt to overcome this problem has been made in [71] where an active FTC strategy that takes explicitly into account the in service controls law. It was shown that for a given system, it is possible to design the family of all admissible FDD/FTC schemes that guarantees a given H_∞ performance level. However, as it is outlined by the authors, the problem to extract the best FDD and FTC parts for a given application remains open. Finally, FTG has been studied for some specific aerospace vehicles. For example, for reusable launch vehicles (RLV), it has been shown in [72] 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.

3. Future challenges

3.1. FDD

Advanced FDD has probably the most strong potentialities for widespread and real industrial applications in aerospace domain. Some facts allow us to be optimistic for the upcoming years:

- FDD methods and techniques are now well established and their conceptual and theoretical foundations are well mastered.
- FDD works in an "open loop" fashion with respect to the controlled system. So, FDD does not affect the stability and cannot bring the system into a dangerous configuration. Off course this fact depends on how the FDD information is managed by the local or global FDIR system.
- The innovative technological solutions used in modern spacecraft also introduce new sources of possible failures. The applicability of conventional techniques is becoming increasingly problematic when used in conjunction with the many innovative solutions being developed to increase performance. This feature motivates the use of more advanced FDD techniques. Moreover, increasing progress in on-board computational equipment and techniques has set the scene for the application of more sophisticated and powerful FDD methods.
- While clear-cut failures can be uncovered perfectly by the existing monitoring mechanisms, more subtle and soft drifting type failures must be detected and isolated by the use of more sophisticated FDD techniques.
- For aircraft applications, FDD can also be related to the situation awareness[3]. The early detection of a subsystem abnormality that is developing during flight would be potentially important, because the extra time before an alert range is reached may improve the crew's situation awareness. As situation awareness increases, the crew is increasingly able to think "ahead" of the aircraft, and do this for a wider variety of situations. *Predictive* FDD [29] could provide such possibility for rapid recognition of faulty situations which have the potential for early detection.

The academic literature on FDD is now saturated and the effort should be put toward the best suited FDD methods capable of handling the real-world aerospace FDD problems to overcome the "dead valley" as discussed in section 1.3. An important issue is the need for clear, systematic and formalized guidelines for tuning. A suitable candidate FDD method for any aerospace application should be able to manage stringent operational conditions in terms of

[3] The aircraft internal situation perception, which can be called "situation assessment", relies on existing systems which monitor parameters, detect the error once it occurs, and inform the crew by HMI concept of "sudden alarm". With this concept, the system health is given by OK/NON OK information which can be not representative of the real status of the system.

trade-offs for FDD specifications, computational burden (memory storage, CPU load) and design complexity. The design method should provide high-level design parameters (tuning parameters) that can be used by non expert operators. It should allow for easy integration of various kinds of specifications. It must also offer the possibility to reuse or to build taround it, with adequate design and tuning engineering tools.

3.2. FTC

FTC area has been investigated more recently, and took advantage of a number of available results in robust and adaptive control. It is a relatively challenging subject with low support from aerospace industry. Industrial end-users are generally more skeptical about FTC benefits, although several successful demonstrations are available [73], [93]. The reason is mostly related to the fact that any modification to flight control laws is considered to be a very critical technological divide which needs very long validation and certification process. FTC design methods should also provide an appropriate validation framework for testing all possible cross-path situations.

3.3. FTG

FTG area is not still sufficiently explored and needs more methodological work. The interaction between FTG and FDD/FTC at system level units needs more investigations. The concept could be very promising for space missions where ground intervention could be too complex, too long or temporarily impossible (i.e. in case of automated operation during a critical phase), and/or too costly. FTG could provide a greater flexibility to account for off-nominal conditions, in situations where FTC is not sufficient (in-board control resources limited after a failure) to recover timely the vehicle.

Acknowledgement
The author would like to thank Dr Philippe Goupil (AIRBUS Operations SAS, Toulouse, France) for many fruitful discussions about FDD/FTC industrial practice.

References

[1] Ding, S.X., Model-based Fault Diagnosis Techniques. Design Schemes, Algorithms, and Tools. *Springer, Heidelberg, Berlin*, 2008.
[2] Hwang, S. Kim, *Y.* Kim, A survey on Fault Detection, Isolation and Reconfiguration methods, *IEEE Transactions on Control Systems Technology, Vol. 18, N° 3, May* 2010.
[3] Blanke, M., Kinnaert M., Lunze M. et Staroswiecki M., Diagnosis and fault tolerant control. Ed. *Springer, New York*. 2003.
[4] Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri, A review of process fault detection and diagnosis part I: Quantitative model-based methods. *Comput. Chem. Eng.*, vol. 27, pp. 293–311, 2003.
[5] Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri, A review of process fault detection and diagnosis part II: Qualitative models and search strategies. *Comput. Chem. Eng.*, vol. 27, pp. 313–326, 2003.
[6] Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri, A review of process fault detection and diagnosis part III: Process history based methods. *Comput. Chem. Eng.*, vol. 27, pp. 327–346, 2003.
[7] Isermann, R. Trends in the application of model-based fault detection and diagnosis of technical processes. *Control Eng. Practice*, vol. 5, no. 5, pp. 709–719, 1997.
[8] Isermann, R. Model-based fault-detection and diagnosis status and applications. *Annu. Rev. Control*, vol. 29, no. 1, pp. 71–85, 2005.
[9] Basseville, M., I. V. Nikiforov, Detection of Abrupt Changes: Theory and Application. *Englewood Cliffs, NJ: Prentice Hall*, 1993.
[10] Patton, R., P. M. Frank, and R. N. Clark, Fault Diagnosis in Dynamic Systems: Theory and Application. *Eds. Englewood Cliffs, NJ: Prentice-Hall,* 1989.
[11] Patton, R., Fault-tolerant control: the 1997 situation. SAFEPROCESS'97, IFAC Symp. on fault detection, supervision and safety, Kingston Upon Hull, UK, 1997.
[12] Chen, J. and Patton, R. J., Robust model-based fault diagnosis for dynamic systems. *Kluwer Academic Publishers. Boston/ Dordrecht/London.*1999.
[13] Bokor, J. and Szabo, Z. Fault detection and isolation in nonlinear systems. In *Annual Reviews in Control*, 33, 113-123, 2009.
[14] Alcorta-Garcia E., Zolghadri A., Goupil P.. A Nonlinear Observer-Based Strategy for Aircraft Oscillatory Failure Detection: A380 Case Study. *IEEE Trans. Aerospace and Electronic Systems*. 2011 to appear.
[15] Zolghadri A., Goetz C., Bergeon B., Denoise X. Integrity monitoring of flight parameters using analytical redundancy. *Proc. UKACC international conference on control (CONTROL ‘98)*, UK, pp. 1534–1539, 1998.
[16] Zolghadri, A. An algorithm for real-time failure detection in Kalman filters. *IEEE Transactions on Automatic Control*, Vol. 41, N° 10, p. 1537-1540, 1996.
[17] Kurtoglu, T.; Johnson, S.B.; Barszcz, E.; Johnson, J.R.; Robinson, P.I. 2008. Integrating system health management into the early design of aerospace systems using Functional Fault Analysis. *IEEE conf on Prognostics and Health Management* 2008.

[18] Deckert, J.C., M. N. Desai, J. J. Deyst, and A. S.Willsky, "F-8 DFBW sensor failure identification using analytic redundancy," *IEEE Trans. Autom. Control*, vol. 22, no. 5, pp. 795–809, Oct. 1977.
[19] Wilbers, D.M., J. L. Speyer, Detection filters for aircraft sensor and actuator faults. *Proc. IEEE Int. Conf. Control Appl.*, Jerusalem, Israel, 2002.
[20] Menke, T.E., P. S. Maybeck, Sensor/actuator failure detection in the VISTA F-16 by multiple model adaptive estimation. *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 4, pp. 1218–1229, Oct. 1995.
[21] Kim, S., J. Choi, and Y. Kim, "Fault detection and diagnosis of aircraft actuators using fuzzy-tuning IMM filter," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 44, no. 3, pp. 940–952, 2008.
[22] Chen, R.H., H. K. Ng, J. L. Speyer, L. S. Guntur, and R. Carpenter. Health monitoring of a satellite system. *Proc. AIAA Guid., Nav., Control Conf.*, Aug. 2004.
[23] Patton, R., Uppal F., Simani S., Polle B., Robust FDI applied to thruster faults of a satellite system. Control Engineering Practice, vol. 18, nº9, pp. 1093-1109, 2010.
[24] Falcoz A., Henry D., Zolghadri A. Robust fault diagnosis for Atmospheric Re-entry Vehicles: a case study. *IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems & Humans*, vol 40 , pp. 886-899, 2010.
[25] Falcoz, A., Henry, D., Zolghadri, A., Bornschleg, E. and Ganet, M. On-board model-based robust FDIR strategy for reusable launch vehicles (RLV). *7th International ESA Conference on Guidance, Navigation and Control Systems*, County Kerry, Ireland, 2008.
[26] Henry D., Falcoz A., Zolghadri A., Structured H∞/H− LPV filters for fault diagnosis: Some new results. 7th *IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Barcelona, Spain, 2009.
[27] Henry, D. , Fault diagnosis of the Microscope satellite actuators using Hinf/H- filters. AIAA Journal of Guidance, Control, and Dynamics. vol.31, no.3, pp.699-711, 2008.
[28] Zolghadri, A. A redundancy-based strategy for safety management in a modern civil aircraft. *Control Engineering Practice*, Vol. 8, N° 5, pp 545-554, 2000.
[29] Zolghadri, A. Early warning and prediction of flight parameter abnormalities for improved system safety assessment. *Reliability Engineering and System Safety*. vol. 16, pages 19-27, 2002.
[30] Zolghadri A., Castang F., Henry D. Design of robust fault detection filters for multivariable feedback systems. *International Journal of Modeling and Simulation.* vol. 26 - pages 17-26, 2006.
[31] Papageorgiou, C. and K. Glover. "Robustness analysis of nonlinear flight controllers". AIAA Journal of Guidance, Control and Dynamics 28(4), 639–648, 2005.
[32] Favre, C., "Fly-by-wire for commercial aircraft: The Airbus experience," *Int. J. Control*, vol. 59, no. 1, pp. 139–157, 1994.
[33] Briere, D., P. Traverse, Airbus A320/A330/A340 electrical flight controls—A family of fault-tolerant systems. *Proc. 23rd Int. Symp. Fault-Tolerant Comput.*, pp. 616–623, 1993.
[34] Goupil, P., Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy. *Control Engineering Practice*, vol 18, issue 9, 2010.
[35] Goupil, P., AIRBUS state of the art and practices on FDI and FTC in flight control system. *Control Engineering Practice*, vol 19, pages 524-539, 2011.
[36] Osder, S., Practical view of redundancy management, application and theory. Journal of Guidance, Control and Dynamics, vol 22, N° 1, 1999.
[37] Palmer, M.T., K.H. Abbot. Effects of expected-value information and display format on recognition of aircraft subsystem abnormalities. *NASA Technical paper 3395*, 1994.
[38] Regal, D.M., V.H. Rogers, G.P. Boucek. Situational awareness in the comercial flight deck - definition, measurement, and enhancement. *Proceedings of the 7th Aerospace Behavioral Technology Conference and Exposition, SAE*, pp. 65-69, 1989.
[39] Johnson, D.M. A review of fault management techniques used in safety-critical avionic systems. *Prog. Aerospace Sci.*, Vol. 332, pp. 415-431, 1996.
[40] Trujillo, A.C. Pilot mental workload with predictive system status information. *4th annual symposium on human interaction with complex systems*. pp. 73-80, Fairborn, OH, USA, 1998.
[41] Lemai S., X. OLive, M.C. Chermeau. Decisional architecture for autonomous space systems. *9th ESA workshop on advanced technologies for robotics and automation, Noordwijk, the Netherland, November 28-30,* 2006.
[42] Beard, R.V., Failure accommodation in linear systems through self-reorganization. Ph.D. dissertation, Dept. Aeronautics Astronautics, Massachusetts Inst. Technol., Cambridge, Feb. 1971.
[43] Jones, H. L, Failure detection in linear systems. Ph.D. dissertation, Dept. Aeronautics Astronautics, Massachusetts Inst. Technol., Cambridge, MA, Feb. 1973.
[44] Mehra, R.K., J. Peschon, An innovations approach to fault detection and disgnosis in dynamic systems. *Automatica*, vol. 7, pp. 637–640, 1971.
[45] Massoumnia, M.A., A geometric approach to the synthesis of failure detection filters. *IEEE Trans. Autom. Control*, vol. 31, no. 9, pp. 839–846, Sep. 1986.
[46] Douglas R.K., J. L. Speyer, Robust fault detection filter design. *J. Guid., Control, Dyn.*, vol. 19, no. 1, pp. 214–218, 1996.
[47] Chen J., R. J. Patton, and H. Y. Zhang, Design of unknown input observers and robust fault-detection filters. *Int. J. Control*, vol. 63, no. 1, pp. 85–105, 1996.
[48] Balas, M.J., Do all linear flexible structures have convergent second order observers?. *AIAA J. Guid., Control, Dyn.*, vol. 22, no. 6, pp. 905–908, 1999.
[49] Chow, E.Y., A. S. Willsky, Analytical redundancy and the design of robust failure detection systems. *IEEE Trans. Autom. Control*, vol. 29, no. 7, pp. 603–614, Jul. 1984.
[50] Stoustrup, J., and Niemann, Fault estimation—A standard problem. *Int. J. Robust Nonlinear Control*, vol. 12, pp. 649–673, 2002.
[51] Bokor J., Balas G. Detection Filter Design for LPV Systems – a Geometric Approach. *Automatica*, 40, pp. 511−518, 2004

[52] Raissi T., Videau G., Zolghadri A. Interval observers design for consistency checks of nonlinear continuous-time systems. *Automatica*. vol. 46, pages 518-527, 2010.
[53] Efimov D., Zolghadri A., Raissi T. Actuators Fault Detection and Compensation under Feedback Control. *Automatica*, 2011
[54] Yan X.G., Edwards C.. Nonlinear robust fault reconstruction and estimation using a sliding mode observer. *Automatica*, 43, pp. 1605–1614, 2007.
[55] Saif, M., Xiong Y., Sliding mode observers and their application in fault diagnosis. In Fault Diagnosis and Fault Tolerance for Mechatronic Systems: Recent Advances, F. Caccavale and L. Villani, eds., vol. 1/2003 of Springer Tracts in Advanced Robotics, *Springer*, Berlin, pp.1–57.
[56] Henry, D. and Zolghadri, A., Design and analysis of robust residual generators for systems under feedback control. *Automatica*, Vol.41, pp.251-264, 2005
[57] Henry, D. and Zolghadri, A., Design of Fault Diagnosis Filters: A Multi-Objective Approach. *Journal of Franklin Institute*. Vol.342, No.~4, pp.421-446, 2005.
[58] Henry, D. and Zolghadri, A., Norm-based design of robust FDI schemes for uncertain systems under feedback control: Comparison of two approaches. *Control Engineering Practice*, vol.14, no.9, pp.1081-1097, 2006.
[59] Zolghadri A., Henry D., Grenaille S. Fault diagnosis for LPV systems. *16th IEEE Mediterranean Conference on Control and Automation*, 2008.
[60] Grenaille S., Henry D., Zolghadri A. A method for designing Fault Diagnosis Filters for LPV polytopic systems. *Journal of Control Science and Engineering*. Article ID 231697, 2008.
[61] Ganguli, S., Marcos, A., Balas, G., Reconfigurable LPV control design for Boeing 747-100/200 longitudinal axis. *American Control Conference*, 2002.
[62] Cordier, M.O., P. Dague, F. Lévy, J.Mountmain, M. Staroswiecki, and L. Travé-Massuyès. 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.*, vol. 34, no. 5, pp. 2163–2177, Oct. 2004.
[63] Travé-Massuyès, L., T. Escobet, and X. Olive. Diagnosability analysis based on component-supported analytical redundancy relations. *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 36, no. 6, pp. 1146–1160, 2006.
[64] Chen, R.H., H. K. Ng, J. L. Speyer, L. S. Guntur, and R. Carpenter, "Health monitoring of a satellite system," in *Proc. AIAA Guid., Nav., Control Conf.*, Aug. 2004.
[65] M. Kumar, "Fault detection identification and reconfiguration of flight control system using IMM estimator," in *Proc. Digit. Avionics Syst. Conf.*, Oct. 2007.
[66] Jung, B., Y. Kim, C. Ha, and M. J. Tahk, "Nonlinear reconfigurable flight control system using multiple model adaptive control," presented at the *17th IFACSymp. Autom. Control Aerosp.*,Toulouse, France, Jun. 2007.
[67] Tang, X.D., G. Tao, and S. M. Joshi. Adaptive actuator failure compensation for parametric strict feedback systems and an aircraft application. *Automatica*, vol. 39, no. 11, pp. 1975–1982, 2003.
[68] Oppenheimer, M.W., D. B. Doman. Efficient reconfiguration and recovery from damage for air vehicles. presented at the *AIAA Guid., Nav., Control Conf*., Keystone, CO, Aug. 2006.
[69] Ganguli, G. Papageorgiou, and S. Glavaski. Aircraft fault detection, isolation and reconfiguration in the presence of measurement errors. presented at the *AIAA Guid., Nav., Control Conf., Keystone*, CO, Aug. 2006.
[70] Cieslak J., Henry D., Zolghadri A. Fault Tolerant Flight Control: From Theory to Piloted Flight Simulator Experiments. *IET Control Theory and Applications*. 2010
[71] J. Cieslak, D. Henry, A. Zolghadri, P. Goupil. Development of an Active Fault Tolerant Flight Control Strategy. *AIAA Journal of Guidance, Control, and Dynamics*. 2008
[72] Morio, V., 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, 2009.
[73] Edwards, C. *et al.* . Fault Tolerant Flight Control – A Benchmark Challenge. *Lecture Notes in Control and Information Sciences*. 2010.
[74] Henry D., A. Zolghadri, M. Monsion, S. Ygorra, Off-line robust fault diagnosis using the generalized structured singular values. *Automatica* , August, 2002.
[75] Alazard D. & Apkarian P. Exact observer-based structures for arbitrary compensators. *Int. J. Robust NL Control*, 9, 101-118, 1999.
[76] Alwi, H., and Edwards, C. Fault tolerant control using sliding modes with on-line control allocation, *Automatica*, 2008.
[77] Ding S.X., Integrated design of feedback controllers and fault detectors, *Annual Reviews in Control*, vol 33, 124-135, 2009.
[78] Gaspar P. and J. Bokor (2006), A fault-tolerant rollover prevention system based on a lpv method, *International Journal of Vehicle Design*, vol. 42, no. 3-4, pp. 392–412, 2006
[79] Liberzon D. Switching in Systems and Control, *Birkhäuser*, Boston, 2003.
[80] Marcos A. & Balas G., A robust integrated controller/diagnosis aircraft application, *Int. J. Robust NL Control*, 15:531-551, 2005.
[81] Oudghiri M., Chadli M. & El Hajjaji A., Robust observer-based fault tolerant control for vehicle lateral dynamics, *Int. Journal of vehicle Design*, vol. 48, pp. 173-189, 2008.
[82] Shin J.-Y & Belcastro C.M., Performance analysis on fault tolerant control system, *IEEE Trans. on Contr. Syst. Techno.*, 14(9), 1283-1294, 2006.
[83] Staroswiecki M., Yang H and Jiang B. Progressive accommodation of parametric faults in LQ control, *Automatica* , 2007, (43), 2070-2076
[84] Weng Z., Patton R. & Cui P., Integrated Design of Robust Controller and Fault Estimator for Linear Parameter Varying Systems, *17th World Congress IFAC*, Seoul Korea, 2008.
[85] Yang, H., Cocquempot, V., & Jiang, B. Robust fault tolerant tracking control with applications to hybrid nonlinear systems. IET Control Theory and Applications, 3(2), 211_224, 2009.

[86] Yang H., Jiang B. & Staroswiecki M., 'Supervisory fault tolerant control for a class of uncertain nonlinear systems', *Automatica* 45, 2319-2324, 2009.
[87] Zhang, Y., and Jiang, J., Bibliographical review on reconfigurable fault-tolerant control systems, *Annual Reviews in Control*, (32), pp 229–252. 2008.
[88] James M. and L. Dubon, "An autonomous diagnostic and prognostic monitoring system for NASA's deep space network," in *Proc. IEEE Aerosp. Conf.*, vol. 2, pp. 403–414, 2000.
[89] Bernard D., G. Dorais, E. Gamble, B. Kanefsky, J. Kurien, G. Man, W. Millar, N. Muscettola, P. Nayak, K. Rajan, N. Rouquette, B. Smith, W. Taylor, and Y.-W. Tung, "Spacecraft autonomy flight experience: The DS1 remote agent experiment," in *Proc. AIAA*, Albuquerque, NM, pp. 28–30, 1999.
[90] Durou O., V. Godet, L. Mangane, D.P. Perarnaud, R. Roques. Hierarchical fault detection, isolation and recovery applied to COF and ATV avionics. *Acta Astronautica Vol. 50, No. 9, pp. 547–556,* 2002.
[91] Ducard, G.J.J. Fault-Tolerant Flight Control and Guidance Systems for a Small Unmanned Aerial Vehicle. PhD Thesis, ETH Zurich, 2007.
[92] Zolghadri A. *et al.* A model-based solution to robust and early detection of control surface runaways. *SAE AeroTech Congress & Exhibition*, 18-21 October, Toulouse, France, 2011.
[93] Lombaerts, T.J.J. Fault Tolerant Flight Control. A physical model approach. *PhD Thesis*, *TuDelft*, *Netherlands*, 2010.
[94] Rotstein H.P., R. Ingvalson, T. Keviczky, G. J. Balas. Fault-Detection Design for Uninhabited Aerial Vehicles. *Journal of Guidance*, *Control*, *and Dynamics* , Vol. 29, No. 5, September–October, 2006.
[95] http://en.wikipedia.org/wiki/Technology_readiness_level.
[96] http://addsafe.deimos-space.com