Progress in Flight Dynamics, GNC, and Avionics **6** (2013) 231-248
DOI: 10.1051/eucass/201306231
© Owned by the authors, published by EDP Sciences, 2013

THE CHALLENGE OF ADVANCED MODEL-BASED FDIR TECHNIQUES FOR AEROSPACE SYSTEMS: THE 2011 SITUATION

A. Zolghadri

Automatic Control Group
IMS-lab, University of Bordeaux
351 Cours de la Libération, Talence 33405, France

For aerospace systems, advanced model-based Fault Detection, Identification, and Recovery (FDIR) challenges range from predesign and design stages for upcoming and new programs up to the improvement of the performance of in-service flying systems. However, today, their application to real aerospace world has remained extremely limited. 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

CUSUM	Cumulation Sum
DS1	Deep Space One
EFCS	Electrical Flight Control System
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
GNC	Guidance, Navigation, and Control
HMI	Human Machine Interface
LPV	Linear Parameter Varying
LTI	Linear Time Invariant
RLV	Reusable Launch Vehicle
SPRT	Sequential Probability Radio Test
TRL	Technology Readiness Level

This is an Open Access article distributed under the terms of the Creative Commons Attribution License 2.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article available at http://www.eucass-proceedings.eu or http://dx.doi.org/10.1051/eucass/201306231

1 INTRODUCTION

The impact that aerospace and aircraft industry has on today's modern society and world economy is very pronounced. As such, the aerospace industry continues at the forefront of engineering research and development technologies. Recent developments in control engineering, signal processing, and computer sciences have attractive potential for resolving numerous issues related to improved Guidance, Navigation, and Control (GNC) of the flying systems, including improved flight performance, self-protection, and extended life of structures. Innovative and viable fault detection and diagnosis (FDD), and fault tolerant control (FTC) and guidance (FTG) technologies that will improve spacecraft safe operation and availability pose new significant challenges, ranging from predesign and design stages for upcoming and new programs to improvement of the performance for in-service flying systems. The goal of the FDD unit is to detect, isolate, and estimate the severity of a fault. 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]. 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. Fault tolerant control systems seek to provide, at worst, a degraded level of performance in the faulty situations [2, 3]. For aerospace vehicles, FTG could provide a greater flexibility for an safe recovery in case of degraded flight conditions. This means onboard reshaping of the mission objectives. Fault tolerant control and guidance provide means by which a potentially dangerous behavior of the system is suppressed if possible, or means by which the consequences of a dangerous behavior are avoided. Aerospace industry needs continuous improvement including insertion of new technologies. However, so far, the advanced FDD, FTC, and FTG methods being developed by the academic research community have not been really accepted by the aerospace end-users. A widening gap does exist and the scope of this paper is to provide an analysis for this situation.

An attempt is made to answer the question: 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 are 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 brief overview of the industrial state-of-practice. Section 3 presents the interaction between FDD, FTC, and FTG at GNC level. Section 4 is devoted to the brief review of the available academic literature. Section 5 highlights the slow-developing progress

of the advanced academic methods to real-world aerospace systems. Section 6 is devoted to reconfiguration and recovery aspects. Finally, section 7 discuses some future challenges and opportunities.

2 BRIEF REVIEW OF THE INDUSTRIAL STATE-OF-PRACTICE

2.1 General Ideas

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 [4]. 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, etc.), 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 [5]. 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.

2.2 Aeronautics

The paper [5] focuses on a typical Airbus Electrical Flight Control System (EFCS) and provides a detailed description of the industrial practices and strategies for FTC and FDD in civil aircraft. The EFCS constitutes an industrial standard for commercial applications. It provides control of the aircraft and flight envelope protection functions. 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, coming from the aviation authorities. Note that the EFCS development on modern civil aircraft led also to a growing complexity of systems and equipments. Consequently, the number of failure cases to consider in the aircraft design has increased compared to the historical mechanical flight control system. In particular, system design objectives originating from structural load constraints are more and more stringent for satisfying the newer societal imperatives towards future "sustainable" aircraft (quieter, cleaner, smarter and more affordable). It can be demonstrated that improving the performances of the fault diagnosis in EFCS allows the designers to optimize the aircraft structural design (weight saving) and thus to improve the aircraft performance and de facto to decrease its environmental footprint (less fuel consumption and noise). The state-of-practice applied worldwide by aircraft manufacturers to diagnose these EFCS faults and obtain full flight envelope protection at all times consists in providing high levels of hardware redundancy in order to perform consistency tests and cross checks. This also ensures sufficient available control action (fault tolerance).

For example, a runaway is an unwanted control surface deflection that can go until moving surface stops if it remains undetected. This failure situation creates additional loads on the aircraft structure and could also disturb the aircraft control. Runaways are mainly due to electronic component failure, mechanical breakage, or Flight Control Computer (FCC) malfunctions. Figure 1 shows root causes located in the servoloop control of the moving surfaces: COM is the command channel and MON is the monitoring channel in the FCC. The COM channel provides the main functions allocated to the computer (flight control law computation and the servocontrol of moving surfaces). The MON channel

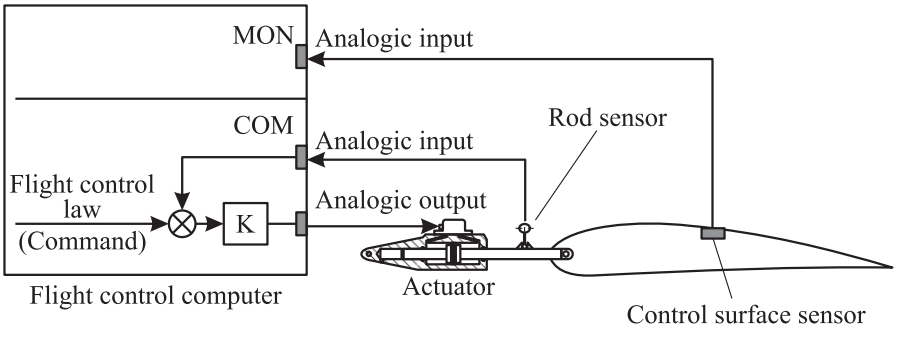

Figure 1 Control surface servoloop

ensures, mainly, the permanent monitoring of all the components of the flight control system (sensors, actuators, other computers, probes, etc). The industrial state-of-practice to detect control surface runaway generally consists in comparing the actual surface position to the theoretical surface position computed by the monitoring channel. An error signal is generated and the decision making corresponds to a threshold-based approach: if the signal resulting from the comparison is greater than a given threshold during a given time window, then fault detection is confirmed. A detected runaway will result in the servocontrol deactivation or computer passivation. Note that a smaller deflection means less loads generated on the aircraft structure, that is why a fast and robust FDD is needed.

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. Depending on the mission needs, FDIR functions are combined with other functions (data processing, orbitography, event-based commanding, and dynamic reprogramming) to achieve a desired level of availability, safety, and autonomy [6–8]. The 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, etc.). The validation assumes testing all possible cross-path situations which 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. 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. Today, a satellite is a smart embedded system that is able to react to some know events and to select a decision among a predefined set. Fault detection and diagnosis and tolerant control and guidance are related strongly to autonomy needs that vary with the mission scenarios and the expected benefits. 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, etc.) 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.

3 INTERACTION BETWEEN FAULT DETECTION AND DIAGNOSIS, FAULT TOLERANT CONTROL, AND FAULT TOLERANT GUIDANCE

Fault tolerant control follows FDD and provides means to continue to "control" the faulty system (maintains stability and achievable performance). Fault tolerant guidance would be necessary when the available on-board control resources are limited and when FTC would not be sufficient. All functions are integrated at the GNC level of the flying system (Fig. 2). Using air data and engine thrust data, the guidance loop computes the guidance demands to follow way-point scenarios. The flight control loop generates actuator signals for the control surfaces.

Note that FTG basically means "change the mission objectives." As an example, consider a typical atmospheric reentry trajectory. During the reentry mission, actuator failures and control effectors damage could lead to a substantial performance degradation and even instability of the closed-loop system. An important issue following the FDD consists, then, in engaging 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, such advanced algorithms may be insufficient to recover the vehicle. Significant aerodynamic characteristics change of the vehicle and a possible lack of control may require reshaping 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 so as to evaluate the remaining capabilities of the vehicle to be rotationally trimmed.

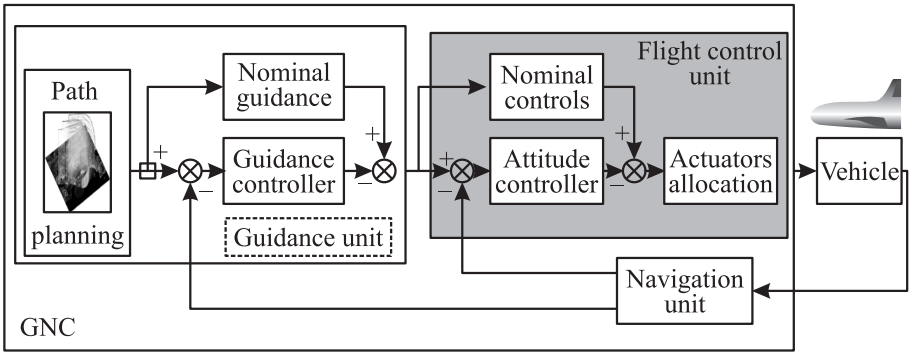

Figure 2 Guidance, navigation, and control level

4 BRIEF REVIEW OF ADVANCED ACADEMIC RESULTS

A large amount of literature on FDD and FTC is now available. The "web of Science" reports around 4000 published papers on FDD topic during the last decade in all engineering fields. The open literature dealing with FTG is much more limited. Good surveys about the academic state of the art can be found in [1, 9–20]. 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 offering many attractive features. The paper will focus mostly on FDD. The FDD methods are classified generally into three categories, which include the knowledge or history based methods [15, 21, 22], analytical model based methods, and signal based methods [10]. In this paper, the focus is on analytical model based approaches. The early studies on model-based FDD appeared about forty years ago. In [23–25], 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, 9, 11, 12, 26]. In the 1990s, a great number of publications dealt with specific aspects such as robustness and sensitivity, diagnosis oriented modeling or robust isolation [10, 12, 18, 27–31]. The European school has been very active in the development of this field, see, for example, and among others [11, 12, 18, 19, 32–39]. 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.

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 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 in 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, [10]). 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 [18,20]. The objective of any robust FDD 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 FDD problem, ranging from modeling problems (nominal system modeling, fault modeling, disturbance and uncertainty modeling, etc.) and FDD system design. The available design methods include the methods based on Linear Time Invariant (LTI), Linear Parameter Varying (LPV), and nonlinear/hybrid estimators/observers, robust designs inspired by robust control designs, unknown input observers, sliding modes methods, etc. The interested reader can refer, for example, to [18, 20] for recent surveys. Observer-based approaches have arisen as one of the most popular among fault detection and isolation (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 [40], providing a unified framework for analysis and implementation. The things get much more complex in the nonlinear case, from the design and also the analysis point of view. For a good survey on nonlinear FDD methods, the interested reader can refer to [19] 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.

The following section discusses potential application of FDD to aerospace systems.

5 ADVANCED MODEL-BASED FAULT DETECTION AND ISOLATION TECHNIQUES FOR AEROSPACE SYSTEMS

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 again the example of a range checking fault detection method devoted to the detection of runaways in aircraft control surfaces servoloops [41]. 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 exists a number of "case study" in the open literature which are fragmented across many journal and conference papers (see, for example and among others, [37, 42–57]). 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 [58]. The validation system was implemented in Ada and hosted on a Boeing X-33 prototype flight computer. In [59], 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 verification and validation when novel technologies are being deployed. For space missions, one can mention the precursor NASA's New Millennium Program [60]: 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 unrecoverable failures, and system-level fault protection [61]. The FDD challenges for aircraft flight control systems are being investigated within the European project ADDSAFE [62]. Analytical redundancy has been used on A380 for the detection of a very specific failure case [63]. However, to the best of the author's knowledge, implementation of modern FDD/FDIR techniques has been extremely limited onboard flying in-service systems. See, for example, many NASA technical reports available at http://www.sti.nasa.gov/ for other specific case studies.

Aerospace industry needs continuous improvement including insertion of new technologies that should be assessed by Technology Readiness Level (TRL) measure [64]. Technology readiness level 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, etc.). 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" does 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, [62]).

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, etc."

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 was pointed out in [4] where the author developed several clever ideas about redundancy management. Model-based techniques do not substitute for physical redundancy but they can be a useful and powerful supplement if implemented in a manner that properly exploits the physical redundancy.

6 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 [13]. The general objective is firstly to maintain stability and secondly to keep some performance level in fault situations.

For reconfiguration mechanisms to 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 a key point: generally, an 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 FDI system. In this case, hybrid control or switching control structures are commonly encountered in [65];

– 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 [66]; and

– using dynamic control allocation for overactuated systems. The fault control allocation problem is that of distributing a desired total control effort among a redundant set of healthy actuators [67].

The interested reader can refer to [68–73] and the references therein for more details. The majority of the available methods rely implicitly on the assumption that the FDD and automatic reconfiguration and 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, etc.) 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, the validation assumes testing of 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 [74]. In [75], 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, [65, 68–73]. 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 was made in [76] 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 was shown in [77] 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.

7 FUTURE CHALLENGES AND OPPORTUNITIES

7.1 Fault Detection and Diagnosis

Advanced FDD techniques have, probably, the strongest potentialities for widespread and real industrial applications in aerospace domain. Some facts allow 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. Of 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; and
- for aircraft applications, FDD can also be related to the situation awareness. 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 Human Machine Interface (HMI) concept of "sudden alarm." With this concept, the system health is given by OK/NON OK information which cannot be representative of the real status of the system. 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 [46] could provide such possibility for rapid recognition of faulty situations which have the potential for early detection [78, 79].

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 5. 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 tradeoffs 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 nonexpert operators. It should allow for easy integration of various kinds of specifications. It must also offer the possibility to reuse or to build around it, with adequate design and tuning engineering tools.

7.2 Fault Tolerant Control

Fault tolerant control 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 the aerospace industry. Industrial end-users are generally more skeptical about FTC benefits, although several successful demonstrations are available [2,3]. The reason is mostly related to the fact that any modification to flight control laws is considered to be a very critical technological device which needs very long validation and certification process. The FTC design methods should also provide an appropriate validation framework for testing of all possible cross-path situations.

7.3 Fault Tolerant Guidance

Fault tolerant guidance 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. Fault tolerant guidance 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.

8 CONCLUDING REMARKS

In this paper, the focus was to show that while the research on analytical and model-based FDIR techniques went forward since early 1970s, the design

methodology involving feasibility analysis and real world requirements specification is still missing. A representative problem area remains the lack of an effective process for maturing on-board implementation and certification process. In this paper, an attempt has been made to analyze major reasons for the slow progress in applying advanced fault diagnosis and fault tolerant control and guidance methods to real-world aerospace systems and to discuss some future challenges and opportunities.

ACKNOWLEDGMENTS

The author would like to thank Dr. Philippe Goupil (AIRBUS Operations SAS, Toulouse, France) for many fruitful discussions and his valuable comments.

REFERENCES

1. Isermann, R. 1997. Trends in the application of model-based fault detection and diagnosis of technical processes. *Control Eng. Practice* 5(5):709–19.
2. Edwards, C., Th. Lombaerts, and H. Smaili. 2010. *Fault tolerant flight control — a benchmark challenge*. Lecture notes in control and information sciences ser.
3. Lombaerts, T. J. J. 2010. Fault tolerant flight control. A physical model approach. Ph.D. Thesis. Delft, Netherlands: Technical University.
4. Osder, S. 1999. Practical view of redundancy management, application and theory. *J. Guidance Control Dyn.* 22(1).
5. Goupil, P. 2011. AIRBUS state of the art and practices on FDI and FTC in flight control system. *Control Eng. Practice* 19:524–39.
6. Durou, O., V. Godet, L. Mangane, D. P. Perarnaud, and R. Roques. 2002. Hierarchical fault detection, isolation and recovery applied to COF and ATV avionics. *Acta Astronautica* 50(9):547–56.
7. Lemai, S., X. OLive, and M. C. Chermeau. 2006. Decisional architecture for autonomous space systems. *9th ESA Workshop on Advanced Technologies for Robotics and Automation*. Noordwijk, the Netherland.
8. Ferell, B., M. Lewis, J. Perotti, R. Oostdyk, and B. Brown. 2010. Functional fault modeling conventions and practices for real-time fault isolation. Ames Research Center; Kennedy Space Center. http://ntrs.nasa.gov/search.jsp?R=20110004336.
9. Patton, R., P. M. Frank, and R. N. Clark. 1989. *Fault diagnosis in dynamic systems: Theory and application*. Englewood Cliffs, NJ: Prentice-Hall.
10. Basseville, M., and I. V. Nikiforov. 1993. *Detection of abrupt changes: Theory and application*. Englewood Cliffs, NJ: Prentice Hall.
11. Patton, R. 1997. Fault-tolerant control: The 1997 situation. *SAFEPROCESS'97*. Kingston Upon Hull, U.K.

12. Chen, J., and R. J. Patton. 1999. *Robust model-based fault diagnosis for dynamic systems*. Boston–Dordrecht–London: Kluwer Academic Publs.
13. Blanke, M., M. Kinnaert, M. Lunze, and M. Staroswiecki. 2003. *Diagnosis and fault tolerant control*. New York: Springer.
14. Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri. 2003. A review of process fault detection and diagnosis. Part I: Quantitative model-based methods. *Comput. Chem. Eng.* 27:293–311.
15. Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri. 2003. A review of process fault detection and diagnosis. Part II: Qualitative models and search strategies. *Comput. Chem. Eng.* 27:313–26.
16. Venkatasubramanian, V., R. Rengaswamy, K. Yin, and S. N. Kavuri. 2003. A review of process fault detection and diagnosis. Part III: Process history based methods. *Comput. Chem. Eng.* 27: 327–46.
17. Isermann, R. 2005. Model-based fault-detection and diagnosis status and applications. *Ann. Rev. Control* 29(1):71–85.
18. Ding, S. X. 2008. *Model-based fault diagnosis techniques. Design schemes, algorithms, and tools*. Heidelberg, Berlin: Springer.
19. Bokor, J., and Z. Szabo. 2009. Fault detection and isolation in nonlinear systems. *Ann. Rev. Control* 33:113–23.
20. Hwang, I., S. Kim, Y. Kim, and C. E. Seah. 2010. A survey on fault detection, isolation, and reconfiguration methods. *IEEE Trans. Control Syst. Technol.* 18(3):636–53.
21. Cordier, M. O., P. Dague, F. Lévy, J. Mountmain, M. Staroswiecki, and L. Travé-Massuyès. 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):2163–77.
22. Travé-Massuyès, L., T. Escobet, and X. Olive. 2006. Diagnosability analysis based on component-supported analytical redundancy relations. *IEEE Trans. Syst. Man Cybern. A, Syst. Humans* 36(6):1146–60.
23. Beard, R. V. 1971. Failure accommodation in linear systems through self-reorganization. Ph.D. Dissertation. Cambridge, MA: Dept. Aeronautics Astronautics, Massachusetts Inst. Technol.
24. Mehra, R. K., and J. Peschon. 1971. An innovations approach to fault detection and disgnosis in dynamic systems. *Automatica* 7:637–40.
25. Jones, H. L. 1973. Failure detection in linear systems. Ph.D. Dissertation. Cambridge, MA: Dept. Aeronautics Astronautics, Massachusetts Inst. Technol.
26. Massoumnia, M. A. 1986. A geometric approach to the synthesis of failure detection filters. *IEEE Trans. Automatic Control* 31(9):839–46.
27. Zolghadri, A. 1996. An algorithm for real-time failure detection in Kalman filters. *IEEE Trans. Automatic Control* 41(10):1537–40.
28. Douglas, R. K., and J. L. Speyer. 1996. Robust fault detection filter design. *AIAA J. Guidance Control Dyn.* 19(1):214–18.

29. Zolghadri, A., C. Goetz, B. Bergeon, and X. Denoise. 1998. Integrity monitoring of flight parameters using analytical redundancy. *UKACC Conference (International) on Control (CONTROL'98) Proceedings.* U.K. 1534–39.

30. Balas, M. J. 1999. Do all linear flexible structures have convergent second order observers? *AIAA J. Guidance Control Dyn.* 22(6):905–8.

31. Stoustrup, J., and H. H. Niemann. 2002. Fault estimation — a standard problem. *Int. J. Robust Nonlinear Control* 12:649–73.

32. Ganguli, S., A. Marcos, and G. Balas. 2002. Reconfigurable LPV control design for Boeing 747-100/200 longitudinal axis. *American Control Conference.*

33. Henry, D., and A. Zolghadri. 2005. Design and analysis of robust residual generators for systems under feedback control. *Automatica* 41:251–64.

34. Henry, D., and A. Zolghadri. 2005. Design of fault diagnosis filters: A multi-objective approach. *J. Franklin Inst.* 342(4):421–46.

35. Henry, D., and A. Zolghadri. 2006. Norm-based design of robust FDI schemes for uncertain systems under feedback control: Comparison of two approaches. *Control Eng. Practice* 14(9):1081–97.

36. Zolghadri, A., F. Castang, and D. Henry. 2006. Design of robust fault detection filters for multivariable feedback systems. *Int. J. Modeling Simulation* 26:17–26.

37. Yan, X. G., and C. Edwards. 2007. Nonlinear robust fault reconstruction and estimation using a sliding mode observer. *Automatica* 43:1605–14.

38. Zolghadri, A., D. Henry, and S. Grenaille. 2008. Fault diagnosis for LPV systems. *16th IEEE Mediterranean Conference on Control and Automation.*

39. Grenaille, S., D. Henry, and A. Zolghadri. 2008. A method for designing Fault Diagnosis Filters for LPV polytopic systems. *J. Control Sci. Eng.* 231697.

40. Alazard, D., and P. Apkarian. 1999. Exact observer-based structures for arbitrary compensators. *Int. J. Robust NL Control* 9:101–18.

41. Zolghadri, A., A. Gheorghe, J. Cieslak, *et al.* 2011. A model-based solution to robust and early detection of control surface runaways. *SAE AeroTechnical Congress and Exhibition.* Toulouse, France.

42. Deckert, J. C., M. N. Desai, J. J. Deyst, and A. S. Willsky. 1977. F-8 DFBW sensor failure identification using analytic redundancy. *IEEE Trans. Automatic Control* 22(5):795–809.

43. Menke, T. E., and P. S. Maybeck. 1995. Sensor/actuator failure detection in the VISTA F-16 by multiple model adaptive estimation. *IEEE Trans. Aerospace Electron. Syst.* 31(4):1218–29.

44. Zolghadri, A. 2000. A redundancy-based strategy for safety management in a modern civil aircraft. *Control Eng. Practice* 8(5):545–54.

45. Wilbers, D. M., and J. L. Speyer. 2002. Detection filters for aircraft sensor and actuator faults. *IEEE Conference (International) on Control Applications Proceedings.* Jerusalem, Israel.

46. Zolghadri, A. 2002. Early warning and prediction of flight parameter abnormalities for improved system safety assessment. *Reliability Eng. Syst. Safety* 16:19–27.

47. Chen, R. H., H. K. Ng, J. L. Speyer, L. S. Guntur, and R. Carpenter. 2004. Health monitoring of a satellite system. *AIAA Guidance, Navigation, and Control Conference Proceedings*.

48. Papageorgiou, C., and K. Glover. 2005. Robustness analysis of nonlinear flight controllers. *AIAA J. Guidance Control Dyn.* 28(4):639–48.

49. Rotstein, H. P., R. Ingvalson, T. Keviczky, and G. J. Balas. 2006. Fault-detection design for uninhabited aerial vehicles. *AIAA J. Guidance Control Dyn.* 29(5).

50. Ducard, G. J. J. 2007. Fault-tolerant flight control and guidance systems for a small unmanned aerial vehicle. Ph.D. Thesis. ETH Zurich.

51. Kurtoglu, T., S. B. Johnson, E. Barszcz, J. R. Johnson, and P. I. Robinson. 2008. Integrating system health management into the early design of aerospace systems using Functional Fault Analysis. *IEEE Conference on Prognostics and Health Management*.

52. Kim, S., J. Choi, and Y. Kim. 2008. Fault detection and diagnosis of aircraft actuators using fuzzy-tuning IMM filter. *IEEE Trans. Aerospace Electron. Syst.* 44(3):940–52.

53. Falcoz, A., D. Henry, A. Zolghadri, E. Bornschleg, and M. Ganet. 2008. On-board model-based robust FDIR strategy for reusable launch vehicles (RLV). *7th ESA Conference (International) on Guidance, Navigation and Control Systems*. County Kerry, Ireland.

54. Henry, D. 2008. Fault diagnosis of the microscope satellite actuators using Hinf/H-filters. *AIAA J. Guidance Control Dyn.* 31(3):699–711.

55. Henry, D., A. Falcoz, and A. Zolghadri. 2009. 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.

56. Patton, R., F. Uppal, S. Simani, and B. Polle. 2010. Robust FDI applied to thruster faults of a satellite system. *Control Eng. Practice* 18(9):1093–109.

57. Falcoz, A., D. Henry, and A. Zolghadri. 2010. Robust fault diagnosis for Atmospheric Re-entry Vehicles: A case study. *IEEE Trans. Syst. Man Cybernetics. Part A, Syst. Humans* 40:886–99.

58. Bickford, R. L., T. W. Bickmore, C. M. Meyer, and J. F. Zakrajsek. 1999. Real-time sensor data validation for space shuttle main engine telemetry monitoring. *AIAA/ASME/SAE/ASEE 35th Joint Propulsion Conference and Exhibit*.

59. Schwabacher, M. A., M. S. Feather, and L. Z. Markosian. Detection, isolation and recovery for NASA space system. http://ti.arc.nasa.gov/publications/170/download/.

60. James, M., and L. Dubon. 2000. An autonomous diagnostic and prognostic monitoring system for NASA's deep space network. *IEEE Aerospace Conference* 2:403–14.

61. 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. 1999. Spacecraft autonomy flight experience: The DS1 remote agent experiment. *AIAA Proceedings*. Albuquerque, NM. 28–30.

62. http://addsafe.deimos-space.com.
63. Goupil, P. 2010. Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy. *Control Eng. Practice* 18(9).
64. http://www.nasa.gov/topics/aeronautics/features/trl_demystified.html.
65. Oudghiri, M., M. Chadli, and A. El Hajjaji. 2008. Robust observer-based fault tolerant control for vehicle lateral dynamics. *Int. J. Vehicle Design* 48:173–89.
66. Staroswiecki, M., H. Yang, and B. Jiang. 2007. Progressive accommodation of parametric faults in LQ control. *Automatica* 43:2070–76.
67. Alwi, H., and C. Edwards. 2008. Fault tolerant control using sliding modes with on-line control allocation. *Automatica* 44(7):1859–66.
68. Liberzon, D. 2003. *Switching in systems and control*. Boston: Birkhäuser.
69. Marcos, A., and G. Balas. 2005. A robust integrated controller/diagnosis aircraft application. *Int. J. Robust NL Control* 15:531–51.
70. Gaspar, P., and J. Bokor. 2006. A fault-tolerant rollover prevention system based on a LPV method. *Int. J. Vehicle Design* 42(3-4).
71. Weng, Z., R. Patton, and P. Cui. 2008. Integrated design of robust controller and fault estimator for linear parameter varying systems. *17th World Congress IFAC*. Seoul, Korea.
72. Zhang, Y., and J. Jiang. 2008. Bibliographical review on reconfigurable fault-tolerant control systems. *Ann. Rev. Control* 32:229–52.
73. Ding, S. X. 2009. Integrated design of feedback controllers and fault detectors. *Ann. Rev. Control* 33:124–35.
74. Shin, J.-Y., and C. M. Belcastro. 2006. Performance analysis on fault tolerant control system. *IEEE Trans. Control Syst. Technol.* 14(9):1283–94.
75. Yang, H., B. Jiang, and M. Staroswiecki. 2009. Supervisory fault tolerant control for a class of uncertain nonlinear systems. *Automatica* 45:2319–24.
76. Cieslak, J., D. Henry, A. Zolghadri, and P. Goupil. 2008. Development of an active fault tolerant flight control strategy. *AIAA J. Guidance Control Dyn.* 31(1):135–47.
77. 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). Ph.D. Dissertation. Bordeaux: 1 University.
78. Trujillo, A. C. 1998. Pilot mental workload with predictive system status information. *4th Annual Symposium on Human Interaction with Complex Systems*. Fairborn, OH, USA.
79. Trujillo, A. C., and I. Gregory. 2011. Piloting changes to changing aircraft dynamics: What do pilot need to now? *30th Digital Avionics Systems Conference*.