DOI: 10.13009/EUCASS2017-692

Turning model-based FDIR theory into practice for aerospace and flight-critical systems

Ali Zolghadri

University of Bordeaux - CNRS, IMS lab
France
Email: ali.zolghadri@ims-bordeaux.fr

Abstract

Modern control theory offers a huge number of various designs, techniques and methods related to advanced FDIR and fault tolerant Control & Guidance. On the other hand, aerospace and flight-critical applications provide numerous grounds where such techniques are needed to support conventional industrial practices. However, today, we have to recognize that the assessment is not overly enthusiastic in terms of real-world applications. The main focus of this talk is on a number of practical design considerations that should go along with any model-based FDIR design in order to provide a viable technological solution. Such considerations are decisive for the survivability of the design during ground/flight Validation & Verification (V&V) activities. The views reported in this paper are based on lessons learnt and results achieved through actions undertaken with Airbus during the last decade. One of the model-based monitoring methods that the author developed with Airbus received certification on new generation A350 aircraft and is flying since January 2015.

Key words. Fault Detection, Identification and Recovery; Fault tolerant Control & Guidance; Aerospace and flight-critical systems.

ACRONYMS

EFCS	=	Electrical Flight Control System	LOC-I	=	Loss Of Control In-flight
FBW	=	Fly-By-Wire	LPV	=	Linear Parameter Varying
FCC	=	Flight Control Computer	ADIRS	=	Air Data Inertial Reference System
GNC	=	Guidance, Navigation and Control	V&V	=	Validation & Verification
FDIR	=	Fault Detection, Identification and Recovery	TRL	=	Technology Readiness Level
FTC	=	Fault Tolerant Control	SIB	=	System Integration Bench
FTG	=	Fault Tolerant Guidance	SCADE™	=	Safety Critical Application Development Environment
GNC	=	Guidance, Navigation and Control			

1. Introduction

The aerospace industry is a powerful engine of innovation as it has to meet more and more aggressive performance targets in reliability, efficiency, safety, weight, range, environmental impact and emissions, etc. The challenges today are far greater than those faced in the past and continue to grow as individual systems evolve and operate with greater autonomy and intelligence within a networked and cyber-physical environment [1]. Regulatory standards evolve as the industry matures, and evolutionary improvements to existing systems should be supplemented by revolutionary technologies and concepts to support conventional industrial practices. Innovative FDIR systems are required to achieve improved flight performance and efficiency. The primary objective of a FDIR system is (i) early detection of faults and abnormal events, isolation of their location and diagnosis of their causes, and (ii) planning subsequent automatic reconfiguration actions in case of degraded flight conditions. Varying degrees of FDIR sophistication have been around for more than five decades for aerospace systems. For technical and development reasons, FDIR functions of a spacecraft are conventionally arranged in a hierarchical architecture in which several levels of faults are defined from local component/equipment/unit level up to global system failures. The higher the level, the more critical the fault but lower the occurrence probability of the fault. Fault recovery and system reconfiguration is achieved by switching to redundant units and backup mode using inactive hardware redundancy schemes. See for example [2] for a survey. On the other hand, FDIR issues have spurred on substantial research effort within the academic community and an impressive array of publications have been generated. Among others, see for example [3-14] and the references therein. When exploring this rich literature, one may have the feeling that advanced FDIR designs and methods have already found many applications into aerospace arena. By application, it is understood “tangible and marketable aerospace technologies which can generate economic added value and benefits to society”. However, we have to recognize that in terms of applications the assessment is not overly enthusiastic and the today situation reveals a mixed picture. It is hoped that the views reported in this paper can be

DOI: 10.13009/EUCASS2017-692

helpful to think about where the effort should be put to improve this situation in the future. For this, we need to understand how we got to be where we are today. The analysis is grounded in author's experience in model-based FDIR research[1], and the conclusions reached embrace mainly the European situation, although beyond the old continent one can find certainly strong parallels and similarities with the situation in other places.

To begin with, it is thought that a brief history of modern control design can be helpful to better situate the emergence of fault tolerant control and fault diagnosis problems which have been widely motivated by flight-critical applications. The field of modern control may sometimes appear as a collection of disparate topics, tricks and modifications to the earlier works; one is often confused and overwhelmed by the vast number of what appear to be unconnected and separate designs and methods. So, to set the scene and before going through the FDIR era, the paper starts with a short background of linear control theory. This rapid overview is presented in the following section in the form of two acts and four scenes. Links with aerospace and flight systems are briefly traced. Section 3 is dedicated to industrial state of practice in aerospace. Section 4 is an attempt at explaining the widening gap between advanced methods being developed by the academic control community and technological solutions demanded by the aerospace industry. Section 5 provides an example and some concluding remarks and final thoughts are provided in Section 6.

2. Historical academic perspective: from control to FDIR

2.1. Classical control theory

In the 1940s, the concept of linear control systems and feedback theory emerged with the work of Bode, Ziegler and Nichols using graphical techniques in the frequency-domain. The controllers that were built where PI and PID controllers, they were not model-based. The controllability was defined as the ability of the process to achieve and maintain the desired equilibrium value [15]. Robustness concepts were incorporated in the design techniques in the form of gain and phase margins. Frequency domain techniques and PID control are still the tool of choice in flight control analysis and design. For example, the longitudinal and lateral equations of motion can be approximated by a set of linear differential equations and the frequency tools help aerospace control engineers gain helpful insight on how to improve robustness and performance of feedback loops.

2.2. Modern control theory

In the 1960s, and following the seminal work of Kalman [16], linear stochastic control has emerged and Linear Quadratic Gaussian (LQG) control and model reference control became major new design techniques. The major impact of Kalman's work was the replacement of graphical design techniques by model-based certainty equivalence control design [17], [18]. However, the Achilles' heel of the model-based control era of the sixties and seventies was plant model uncertainties. LQG design had failed to address the "essential requirement that changes of loop gains in all combinations should leave the system with an adequate stability margin" [19–22]. During this period, the gap between academic theory and engineering practice in the control field increased. In the late 70s and early 80s, a renewed interest appeared in the problem of plant uncertainty. At about the same time, some significant results were being reported on the analysis of multivariable systems in the frequency domain and a multivariable robust design philosophy emerged, which was identified as the LQG/LTR (linear-quadratic-Gaussian/ loop transfer recovery) approach. Robust multivariable feedback design methods flourished in the early 80s, where the main focus was the use of singular values in the design of robust multivariable systems in the frequency domain [23–27]. A good retrospective analysis is provided in [28]. On the other hand, interest in adaptive control grew significantly from the mid-1950s [29–30]. A great number of ideas on adaptive control were proposed since then: model reference adaptive system, the self-tuning regulator or dual control [31]. The stability problem was an important challenge that led to interesting developments in stability theory. Barbalat's lemma constituted the corner stone of providing stability for adaptive systems [31]. Here, again, the role of simplified models and the robustness to neglected dynamics were major questions. In the above mentioned developments, flight control has been often a driving force. Supersonic flight posed new challenges for flight control and control systems for ballistic missiles emerged as an important topic in the post-Sputnik era [32]. Several flight-tested systems based on model reference adaptive control are mentioned in [32].

2.3. Fault Detection and Diagnosis

In the early 1970s, Fault Detection and Identification (FDI) has emerged within the control community. Generally, the main desirable characteristics of a FDI system are early detection, good ability to discriminate between different

[1] One of the model-based monitoring methods that the author developed with Airbus received certification on new generation A350 aircraft and is flying since January. 2015.

DOI: 10.13009/EUCASS2017-692

failures, good robustness to various uncertainty sources, and high sensitivity and performance, i.e. high detection rate and low false alarm rate. In the early works, innovation signals were used to design detection filters. See for example [33–35]. Many solutions have appeared during the 1980s: parity space and observer-based approaches, eigenvalue assignment or parametric based methods. In the 1990s, a great number of publications dealt with specific aspects such as robustness and sensitivity, diagnosis oriented modelling or robust isolation. Among others, see for example [3–14]. More recent design methods include, nonlinear local filtering and nonlinear observers, geometric and set membership methods, robust, LPV and multi-model designs, or sliding mode techniques. Today, model-based FDI design 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 conferences. For flight vehicles, off-normal behaviors are complex, often resulting from an array of causal and contributing factors acting habitually in combination. The diverging effects of a fault may take shape gradually, interact with other factors within the subsystem, and its consequences spread slowly throughout the vehicle. Malfunctions may occur in sensors, actuators or other devices. For example, the aircraft state is measured by a set of sensors delivering e.g. anemometric and inertial measurements that characterize the aircraft attitude, speed and altitude. The data is acquired using an acquisition system composed by several dedicated redundant units. The measurements are processed to compute consolidated flight parameters to be used by FCC. Usual failures include oscillations, bias, drift, loss of accuracy, calibrations errors, freezing… Another example is malfunctions in control surface servo-loops (elevators, ailerons, rudders…). For instance, an oscillatory failure could excite the airplane structure producing undesirable structural loads [36]. In [37] one can find a comprehensive analysis on redundancy management in aircraft systems. See also [38] and the references therein for a comprehensive survey. A lot of aerospace case studies have been reported in the open literature, see for example many technical reports available at: http://www.sti.nasa.gov/.

2.4. Automatic reconfiguration

Formalized designs for automatic reconfiguration appeared more recently. Once faults are correctly detected, confirmed and diagnosed, a reconfiguration mechanism should be used in order to achieve fault-tolerance and avoid unsafe or off-normal system behavior. For successful reconfiguration actions, information about the failed element is necessary in order to assess the remaining on-board control resources. For flight vehicles, one can distinguish two basic functions for reconfiguration: Fault Tolerant Control (FTC) and Fault Tolerant Guidance (FTG). FTC seeks to provide, at worst, a degraded level of performance in the faulty situations. FTG could provide a greater flexibility for safe recovery in case of extremely degraded flight conditions by, for example, replanting flight trajectories. FTC area took advantage of a number of available results in robust and adaptive control (see section 2.2). Fault tolerance could be achieved through several potential solutions: selecting a new pre-computed control law, synthesizing a new control strategy online, or using dynamic control allocation for over actuated systems (without reconfiguration/accommodation of the controller). The interested can refer to [6], [12–14] for more details. The majority of the available methods rely implicitly on the assumption that the FDI and automatic reconfiguration & recovery systems are assumed to operate correctly. The problem of guaranteeing stability and a certain level of performance of the overall fault tolerant system, taking into account both the FDI performance (detection delay ...) and reconfiguration system, has not been sufficiently considered in the literature. Regardless the method, FTC is basically a full-authority solution which makes the transition to a degraded mode by on-board automatic control systems reconfiguration. This can also present several inherent drawbacks in terms of pilot workload, conflicts / mode confusion, authority sharing and decision making.

3. Industrial aerospace perspective

Flight vehicles are designed to prescriptive airworthiness codes and regulations. Traditional avionics architectures consist of set of individual avionics functionality hardware units having its own computing resources. The systems are coupled with multi-function displays and communication units, multi-mode interactive instruments for control, guidance and navigation, fault management systems and health monitoring diagnostic capabilities. The basic principles involving general health management architecture trade-offs changed little from the 1960s, although the hardware mechanizations of the earlier analog systems have been replaced largely with the software of the newer digital systems. See for example [37] and [39] for a historical review. The GNC (Guidance, Navigation and Control) system gives the vehicle the ability to execute flight. Navigation tracks the vehicle's actual location and orientation. Guidance equipment (gyroscopes, accelerometers…) compute the location (or attitude) of the vehicle and the orientation required to satisfy mission requirements (Fig. 1).

3.1. Aeronautics

The success of the Apollo program has been an important factor for the development of digital Fly-By-Wire (FBW) technologies. In the late 1960s, engineers at NASA Flight Research Center (now NASA Dryden) proposed replacing

bulky mechanical flight-control systems on aircraft with much lighter weight and more reliable analog Fly-By-Wire technology. In the early 1970s, NASA Dryden engineers developed a digital fly-by-wire solution using the specialized software and hardware. See for example C. Philippe et al. in [40].

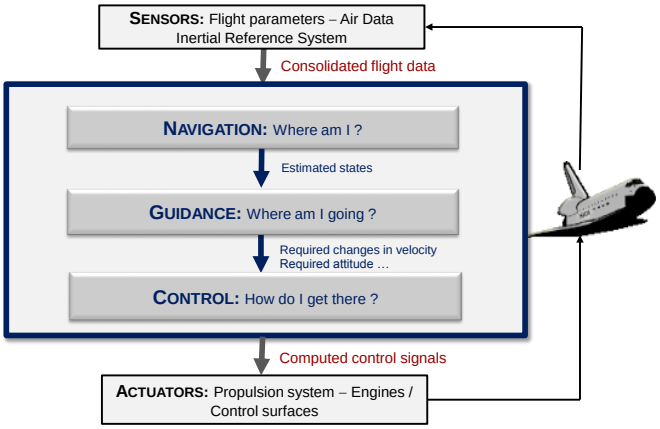

Figure 1: The GNC system for a flight vehicle.

In Europe, Aerospatiale (now Airbus Group) engineers developed and installed the first analog EFCS on Concorde[2]. In civilian and military aviation, this precipitated a revolution in aircraft design. The F/A-18 aircraft was one of the first military aircraft to use FBW technology (first flight: November 1978). The electrical flight control system designed with digital technology on Airbus aircraft from 1980s provided more sophisticated control of the aircraft and flight envelope protection functions.

3.1.1. Fault monitoring and fault tolerance

The today flight deck represents a highly automated mass of complex systems with which the flight crew has to interact. Physical separation of critical avionics functions from less critical functions has been always the primary strategy used by the designers of civil aircraft to produce safe avionic and airborne systems. The state-of-practice to detect unexpected events and to obtain full flight envelope protection at all times is to provide high levels of hardware redundancy in order to ensure sufficient available control action. Fault monitoring is mainly performed by cross checks, consistency checks, voting mechanisms, and Built-In Test techniques (which include hardware sensors and software error correcting codes) of varying sophistication. A key issue is the specification of flight conditions-based thresholds for fault detection. Each warning has an associated procedure which is listed in the flight operations manual or displayed electronically. Today, these standard techniques are implemented in all modern airplanes systems, and are the standard industrial practice, and fit into current industrial certification processes. Fault tolerance relies mainly on hardware redundancy, safety analysis, dissimilarity, physical installation segregation and hardware/software reconfiguration ([41–42], [36–37]).

3.1.2. Flight envelope protection

All automatic flight control systems contain a flight envelope protection which prevents the aircraft from exceeding the structural/aerodynamic limits. The flight envelope is defined as the region in which aircraft can fly safely and is defined in terms of several flight parameters such as Mach number, angle of attack, airspeed, load factor, etc. See for example [43-50] for some flight envelope protection and limit avoidance techniques. The current types of protections differ between aircraft manufacturers. For example, Airbus makes use of hard limitations while Boeing prefers soft protections. Hard protections setup means that it is impossible for a pilot to exceed the envelope boundaries in normal law, although the crew can fly beyond flight envelope limits by selecting an “alternate” control law (see here and [36]). Soft setup means that using excessive force on the controls, pilots can still override the flight envelope protection boundaries if they need to [51].

3.1.3. Pilot situation awareness and care-free handling

In flight deck, flight mission efficiency is strongly related to the pilot situation awareness [52-56]. Off-nominal types of situations, while not involving a system failure or major operational incident, can potentially lead to higher pilot workload. After occurrence of a failure, flight crews may inadvertently find themselves outside of a shrunken safe flight envelope resulting in LOC-I (Loss of Control In-flight) which includes significant, unintended departure of the

[2] A supersonic passenger airplane, jointly developed and produced by Aerospatiale (France) and the British Aircraft Corporation. First commercial flight in 1969.

DOI: 10.13009/EUCASS2017-692

aircraft from usual flight attitudes [44–46]. LOC-I always takes the flight crew by surprise. With incipient LOC-I situations the available time-span to make an initial response can be quite short. Statistics show that LOC-I source of causality is often related to the crew understanding, in an early stage, the implications of certain system faults that are developing during the flight on the capability of other aircraft systems, leading to crew mismanagement of critical systems (engines, autopilot, etc.) and aircraft upset [59]. Care-free maneuvering system allows the aircraft to fly safely within the permitted envelope, leading to improved handling qualities and pilot workload redaction [57].

3.2. Space missions

For technical and development reasons, FDIR functions of a spacecraft are arranged in a hierarchical architecture. Several levels of faults are defined from local component/equipment/unit level up to global system failures [2]. The higher the level, the more critical the fault but lower the occurrence probability of the fault. Fault recovery and system reconfiguration consist in switching to redundant units and backup mode using inactive hardware redundancy schemes (cold redundancy). The criticality of surveillance in a dedicated mode is described by the capability of continuing the current operations after reconfigurations. Each failure is recovered at the lowest layer to limit the impact on the mission. Reaction time for robust FDI, and ability to recover from a failure are sizing elements of the satellite/spacecraft availability [58]. Standardized degrees of autonomy can be found for example in [78]. See also [60] and [61] for a discussion on autonomy needs for future space exploration missions. For other space systems such as winged atmospheric re-entry vehicles (see for example here and [62]), there are more limited weight capabilities compounded because of more restrictive aerodynamic and controllability characteristics resulting from their lower Lift-to-Drag ratios. In [63] the authors describe the V&V challenges and approaches posed by the innovative FDIR technologies being employed and discuss additional certification considerations. The paper [64] discusses issues and lessons learned regarding designing, integrating, and implementing FDIR at Kennedy Space Center. The implementation of recovery actions in modern spacecraft of the European Space Agency (ESA) is based on preprogrammed on-board control procedures that represent the system's event-triggered reflex reaction to FDIR alarms [2]. Several ESA deep space missions apply this concept for FDIR operations, e.g. Rosetta (launched 2004) and Venus Express (launched 2005). Finally, long-term programs for robotic and manned space exploration have been established within governmental space agencies around the world, where detection of unexpected events and recovery are key to improving the reliability of many of the systems deployed in this endeavor.

4. From theory to practice

As briefly described in section 2, modern control theory offers a huge number of various designs, techniques and methods related to fault diagnosis, fault recovery and fault tolerant control and guidance. Moreover, many successful aerospace demonstrations exist, a simple keyword search on internet yields hundreds of examples. On the other hand, aerospace and flight-critical applications provide numerous grounds where FDIR is needed. However, today, few real "applications" can be identified beyond the use of Kalman filter which is the standard approach in aerospace industry for integrating multi-sensor navigation and guidance systems [65], [66]. A number of reasons can be put forth to explain this gap, and high among them is that new techniques are only adopted when there is a clear need in terms of cost or performance benefit that cannot adequately addressed through conventional employed techniques. Introducing structural modifications to the in-service solutions entails risk and may require up to several years of V&V activities and maturation. Yet, the issue is that every time such needs are put on the table by industrial actors, many academic solutions appear to be ineffectively prepared and equipped to move toward real-world systems. In fact, the design methodology involving feasibility analysis and real-world requirements specification and implementation is still not fully developed in many cases. This includes for example tuning, complexity and real time capability, modularity and possibility to reuse or build around it with adequate engineering tools, evaluation of worst-case performance and robustness in harsh environment, poor excitation and FCC reset, fault detectability and model observability in situations where some flight parameters are missed, post-design analysis and validation, etc. For flight-critical systems, a major issue which is often highly underestimated by academics is that good average performance is of course necessary but not sufficient at all. The sizing element is the achievable performance and robustness in extreme, unusual, non-standard and rare flight situations. The trouble is that in such situations, many academic designs appear to reveal poor performance or lack of robustness. This issue will be emphasized in the following section devoted to an example. Another important issue is that many available designs are not really associated with clear and formalized tuning guidelines. A simple and rudimentary well-mastered method may work quite better than a complex design that cannot be tuned properly by the end-user. Easy-to-tune and limited high-level parameters are decisive for the survivability of an advanced solution during V&V activities. A major barrier is certification of a new technique, particularly if it is structurally different to the in-service solutions. The situation can be better observed on TRL scale which is used to assess the maturity level of a particular technology, and is based on a scale from 1 to 9 with 1 being the basic concepts and 9 being the most mature technology. Broadly, classical

DOI: 10.13009/EUCASS2017-692

academic activities cover TRL1 and TRL2 and sometimes TRL3, if feasibility and proofs of concept can be established. TRL6 up to TRL9 correspond to technology integration (fully functional prototype up to flight proven, successful mission and certification). Levels 4 and 5 represent mostly the applicability gap, or the "death valley". The above discussion is to be situated within an underlying trend in the academic world. Academic research evaluation is based mainly on scientific publications which measure academic creativity to produce new knowledge[3]. Focusing on applications is however much less rewarding. Going through the whole story of innovation is time-consuming, hard and risky from an academic perspective: in the "death valley", the priority is coming up with tangible and transferable technical results as soon as possible, not preparing publications. Problems can arise over whether and when to publish because of proprietary concerns. Joint ownership intellectual property in collaborative research projects is often a major point of contention for development of effective and close co-operation between academic world and industry.

5. A case study

Deterministic models are highly appreciated by aerospace engineers as they can lead to deterministic model-based systems for monitoring, fault tolerance, reconfiguration, prediction… A model is deterministic if given the initial state and the inputs, the model defines exactly the same behavior, meaning that given the same inputs it will always produce the same outputs. However, the trouble is that generally the real world is not deterministic. For example, an aircraft is a cyber-physical system combining physical dynamics with computational processes: multiple behavioral modalities interacting with each other that can change with context, etc. So, when it comes to apply a model-based FDIR design to real-world flight systems, the main issue is how to operate that design within harsh non-deterministic environment while satisfying specified operational constraints.

This section provides an example of a model-based monitoring technique which has reached level 5 on Technological Readiness Level (TRL) under V&V investigations at Airbus. The overall method is essentially stochastic and the big issue is how to make its behavior as deterministic as possible. The monitoring strategy can be divided in two steps. Firstly, on-line parameter estimation of an appropriately chosen model structure, and secondly, an appropriate parametric test decision which is applied to an identified direction in the parameter space sensitive to the occurrence of the researched faults. As it will be seen, a great advantage of this approach is that it can be used and generalized for different kinds of actuator models, different moving surfaces or different aircraft families. The section focuses on fault detection problem in control surface servo-control loops related to the Electrical Flight Control System. The failure case studied is runaway with various dynamic profiles. A runaway is an unwanted, or uncontrolled, control surface deflection that can go until the moving surface stops if it remains undetected. This failure is mainly due to an electronic component failure, mechanical breakage or FCC malfunctions. Low speed runaway results in an undesired pitch maneuver that may significantly degrade the aircraft controllability and that may increase the pilot workload. High speed runaways generally do not impact the aircraft trajectory but lead to additional loads that must be taken into account in the aircraft structural design objectives (Fig. 2). The detection of the runaway must be accomplished before the control surface position exceeds a few degrees from its trimmed value. A detected runaway will result in the servo-control deactivation or computer passivation, depending on the failure source.

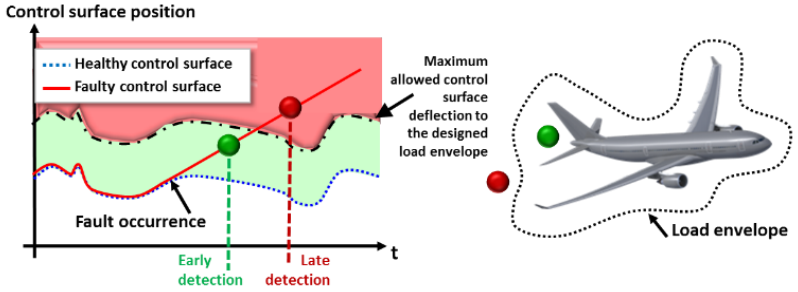

Figure 2: Link between load effects and improved runaway monitoring

The methodology is considered to be a credible option to supplement (not rule out) the current state of practice for Airbus aircraft for achieving enhanced performance.

5.1. System description

[3] Academic over-production is transforming the "publish or perish" process into a "publish and perish" process: one estimate is that about one third of the papers published got almost no citations.

DOI: 10.13009/EUCASS2017-692

The Airbus Fly-By-Wire (FBW) system includes dedicated surveillances for control surfaces. For Airbus airplanes, the simplified functional bloc of servo-loop control of moving surfaces is depicted in Fig. 3 [36]. Here COM represents the command channel and MON is the monitoring channel in the Flight Control Computer (FCC). The COM channel is in charge of servo-loop computation. The MON channel ensures, mainly, the permanent real-time monitoring of the COM channel and of all the components of the flight control system (sensors, actuators, other computers, probes…).

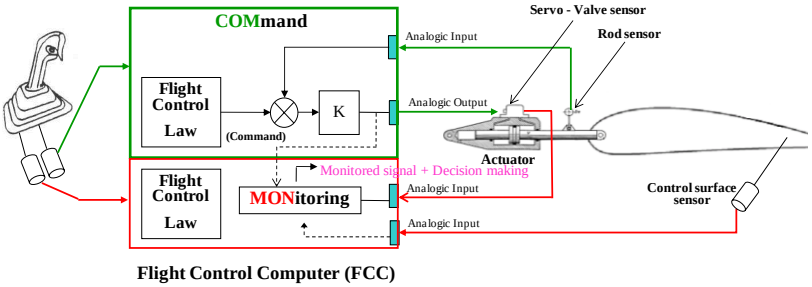

Figure 3: Simplified block diagram of control surface servo-loop.

Faults can be located in the servo-loop of the moving surfaces, between the FCC and the control surface, including these two elements.

5.2. Current industrial practice for runaway detection

For detection of runaways, a residual is generated by comparing the signal delivered by the servo-valve sensor, which represents an image of the current command sent by the COM channel to the actuator, to a kind of theoretical current computed in the MON channel from the actual control surface deflection (generally sensed directly on the control surface by a dedicated sensor) and from the command computed with dedicated redundant sensors in the MON channel. The error signal is computed as follows:

$$\varepsilon = i_{COM} - i_{MON} = i_{COM} - K(u_{MON} - y_{MON}) \quad (1)$$

where K is the servo-control gain, u_{MON} is the command computed in the MON channel, y_{MON} is the control surface position acquired in the MON channel (Fig. 3) and i_{COM} is the command current directly sensed on the servo-valve. Decision making corresponds to a flight condition-based threshold-based logic. Alarms are triggered when the signal resulting from the comparison exceeds a given threshold during a given time window or confirmation time. By setting the threshold, a trade-off must be made between the false alarm rate and the detection of failures with weak amplitudes.

5.3. Need for improvement

Aircraft certification regulations (for instance CS 25.302, see reference FAR/JAR 25) state that the system must be designed so that it cannot produce unexpected high loads on the aircraft. The current monitoring techniques described are industrially well mastered and well characterized, and provide sufficient fault coverage and achieve a good robustness without false alarms. These systems are designed with very stringent safety requirements. Yet, as composite materials are more and more used, reduced structural loads on the aircraft is needed. For instance, a smaller surface deflection when the runaway is confirmed, means less loads generated on the aircraft structure, thus weight saving, better performance and reduced fuel consumption. From load point of view, aircraft certification is obtained when it is proven that the structure complies with the dedicated regulations. For future programs, and in order to fulfil the dedicated regulation from certification point of view, an improvement of the current detection techniques is required in order to decrease the detection time and the position reached by the control surface when the failure is confirmed.

5.4 Practical design considerations

For application to real aircraft, a number of practical design considerations should be taken into account for assessment of the industrial relevance during V&V activities. Among others:
- Complexity of the design: real-time capability, modularity and possibility to reuse or build around it, evaluation of worst-case performance and robustness in harsh environment. The number of input parameters is also an important issue as it impacts and shapes the V&V workload and consequently the system development duration.
- Capacity of adaptation and genericity: if the method is designed for an elevator, can it be applied to an aileron on the same aircraft, or another aircraft without substantial modifications?

- Clear procedure for step-by-step tuning of the design: the number of steps required to get a good trade-off. In fact, many available design methods are not really associated with clear tuning guidelines: a simple and rudimentary well-mastered method may work quite better than a complex design method, if the end-user cannot tune it properly. Easy-to-tune and limited high-level parameters are decisive for the survivability of a new solution during flight V&V activities.
- Initializations: the design should work under any flight conditions, e.g. FCC (Flight Control Computer) reset, etc.
- Good average performance is necessary but not sufficient at all. What is important, and the sizing element, is what can be achieved in unusual and non-standard flight situations.
- Poor excitation, fault detectability and model observability (in situations where one or some flight parameter are missed), are among important issues that should be addressed in an early stage of development.

5.5. Model-based monitoring strategy

The overall strategy can be divided in two steps. Firstly, on-line parameter estimation of an appropriately chosen model, using a modified RLS algorithm with exponential forgetting factor. It will be shown that there exists a direction in the parameter space which is sensitive to the occurrence of the researched faults. Secondly, an appropriate parametric test decision is applied to that direction to detect and confirm faults. This approach differs from the techniques that use a physical model where the focus is on the estimation of physical model parameters derived from flight dynamics. So, the method can be used and generalized for different kinds of actuator models, different moving surfaces or different aircraft families.

5.5.1. Parametric model estimation

The first step consists in recursive parameter estimation of the control surface servo-loop single-input (the commanded control surface deflection computed by the FCC according to the pilot order) single-output (the control surface position) dynamic system. Using all available measurements up to the current time, the input-output process dynamics can be described by: $y(k) = \varphi^T(k)\theta(k-1) + \varepsilon(k)$ where k denotes the sampling index, $y(k)$ is the output to be predicted and $\varepsilon(k)$ is a term describing the noise effect on the system output. $\varphi(k)$ contains input and output measurements available at time k and $\theta(k)$ represents the unknown time-varying parameters. An estimated $\hat{\theta}$ can be obtained by minimizing the loss function $J = \sum_{i=1}^{k} \lambda^{k-i} (y(i) - \hat{y}(i))^2$ where λ is the forgetting factor and $\hat{y}$ is the predicted value of the output: $\hat{y}(k) = \varphi^T(k)\hat{\theta}(k-1)$. It is well-known that poor excitations might lead to the exponential growth of the covariance matrix and as a result the estimator becomes extremely sensitive and therefore susceptible to numerical and computational errors (the so-called covariance wind-up), [67], [68] and [69]. One method to deal with wind-up is the well-known directional forgetting, see for instance [67]. In [70], an algorithm was proposed by adding a multi-step penalty for parameter variations to the objective function of the normal least squares algorithm to prevent the singularity problem that leads to estimation windup. Finally, the U-D Bierman decomposition [70] is used to factorize the covariance matrix and to avoid numerical instabilities. A simple model structure is finally chosen as

$$\hat{y}(k) = \hat{b}(k-1)u(k-d) + \hat{a}(k-1)y(k-1) \tag{2}$$

where $\hat{a}$ and $\hat{b}$ are the unknown time-varying estimated parameters and the time delay d between the control surface servo-loop input and output is chosen according to in-flight recorded data sets. In some situations, there could be a bias between input-output data. A recursive bias estimator (a constant gain Kalman filter) can be run to estimate every constant or slow drifting bias between incoming input and output data and to make them unbiased. The following test can be run to check if sufficient excitation is available. If not, the update of parameters could be stopped waiting for sufficiently rich inputs. Note that another solution could be to use the generalized damped least squares algorithm [71], suitable for poorly excited situations. This algorithm has properties almost equivalent to those of the normal least squares method.

Sufficient excitation Test: *The test is based on the Eigen behaviour of the RLS to evaluate deficient excitation. In [72], it was shown that n-1 eigenvalues of an estimator of order n are constant and lie on the unit circle (z=1) despite one,* $l_n(k)$ *, which is time-varying and depends explicitly on the process input-output data representing the excitation of the system (P is the covariance matrix):* $l_n(k) = \lambda / (\lambda + \phi^t(k)P(k-1)\phi(k))$. $l_n(k)$ *lies inside the unit circle of the z-plane. If excitation of the RLS is missing,* $l_n(k)$ *converges to* λ *, otherwise it converges to zero. Here,*

DOI: 10.13009/EUCASS2017-692

if the pilot order and the control surface position remain constant, we have $\phi(k) = \phi(k-1) = ... = \phi_0$ *and after some simple calculations we get*

$\lim_{i \to \infty} \phi_0^T P(k+i)\phi_0 = 1-\lambda$ *and so in this case* $l_n(k) \to 0$.

5.5.2. Selection of a fault indicator

In this sub-section, it is shown that the estimate of $b(k)$ can be taken as a fault indicating signal for control surface runaway detection, *i.e*: $\hat{b}(k) \neq 0$ when no fault is present (robustness) and $\hat{b}(k) \to 0$ when there is a fault (sensitivity). The detection performance will be investigated in the next section through a parametric decision test.

Robustness: It is easy to show that under sufficient excitation, the estimated parameter values are different from zero.

Sensitivity: One should show that when a fault occurs, $\hat{b}(k)$ will converge asymptotically to zero. Suppose that the fault occurs at $k=k^*$ and note $y(k^*) = y^*$. During the runaway, $y(k^*+1) = y^*+\delta, ..., y(k^*+j) = y^*+j\delta$ where $\delta \neq 0$ models the runaway rate and $j > k^*$. After time k^*, the input information does not contribute to minimising the prediction error anymore and so the best prediction of the output at time k^*+j will be the output at time k^*+j-1: $\hat{y}(k^*+j) \approx y(k^*+j-1)$. This corresponds to an AR model $\hat{y}(k^*+j) = \hat{a}\, y(k^*+j-1)$ where $\hat{a} \to 1$ leads to the best (minimum) estimation error. This implies also that $\hat{b} \to 0$ in the model (2). The estimated parameter $\hat{b}(k)$ can then be taken as a fault indicating signal. In the following sub-section, a decision test in parametric space is used to detect and confirm the occurrence of a fault.

5.5.3. Two Confidence Region (CR2) decision test

The CR2 test has been initially developed for avionics applications of integrated navigation involving coordinated use of multiple simultaneous sensor subsystems [73]. The CR2 test is based on the overlap between the confidences regions associated with two estimates: one on-line estimate and another estimate which is computed from *a priori* information only. In [74], a resolution procedure in parametric space has been proposed that does not call for any optimization procedure and so offers the advantage of low computational expenditure. Let $\hat{b}_0$ be *a priori* nominal value of b estimated off-line, $\hat{P}_0$ nominal estimated covariance relative to $\hat{b}_0$, $\hat{P}(k)$ on-line estimated covariance relative to $\hat{b}(k)$ and α the detection threshold. The simplified mechanization equations (one-dimensional case) for the CR2 algorithm are summarized below (see [73] for the general case):

a) First verify that: $\frac{(\hat{b}(k)-\hat{b}_0)^2}{\hat{P}_0} > \alpha$. *If this inequality does not hold, the procedure stops (the confidence regions overlap).*

b) Find the unique negative root λ_0 *of F(λ) (a 2nd order polynomial for one-dimensional case), where :* $F(\lambda) = \frac{V^2(\lambda)}{\hat{P}(k)} - \alpha$ *and* $V(\lambda) = \frac{\hat{P}(k)(\hat{b}(k)-\hat{b}_0)}{\lambda\hat{P}_0 - \hat{P}(k)}$ *. In fact, it is shown in [74] that* $F(-\infty) = -\alpha$ *and* $F(0) > 0$. *One can compute easily the unique negative solution, starting with an initial value A<0 so that F(A)<0.*

c) Let be $W = V(\lambda_0)$. *If* $\lambda_0^2 \frac{W^2}{\hat{P}_0} > \alpha$ *then the two confidence regions do not overlap and a fault is detected.*

Nominal parameter and covariance matrix are estimated off-line using a real data set. The threshold α ensures the balance between detection delay and false alarm rate which are compliant with the structural design requirements and the operational constraints. In general case, the probability of a wrong decision can be formally expressed. In the following, rather an empirical procedure is adopted. To start with, the Chi-squared table is used to establish an initial range of variations for α. The design parameter is then refined by injecting runaways on a real data set. With various thresholds within the operating range, different simulations are made in order to test the non-detection and the false alarm rates. The following section presents some experimental results obtained from the implementation of the above strategy on Airbus test facilities.

5.6. Experimental results

The technique proposed in the previous section is extensively evaluated on different V&V means:
- An aircraft model developed by Airbus;
- Real recorded flight datasets coming from A350 and A380 airplanes;
- An industrial Airbus actuator bench, also called System Integration Bench (SIB) after the implementation of the solution in a Flight Control Computer using SCADE™ as the coding language.

Airbus benchmark and real flight data sets

The aircraft Airbus benchmark is a highly representative benchmark developed by Airbus which includes aerodynamic, engine, atmospheric and gravity models. Actuator and sensor characteristics are taken into account, together with models for external disturbances. This benchmark has been used to investigate two realistic failure sources involving a runaway occurrence:

- A bias event that occurs on the rod sensor measurement during its acquisition in the COM channel. Two kind of faults are considered: "liquid" and "solid" failures. The liquid failure (denoted LMEAS) adds a bias to the normal signal (inside the control loop) while the solid failure (denoted SMEAS) substitutes the normal signal by a bias.
- A servo-valve malfunction creating a bias on the current generated by the FCC. The acronym LCUR and SCUR will be used for liquid and solid failure cases of this situation respectively.

Some initial simulation results have been reported in [75]. Here, new validation results have been obtained using real recorded flight data sets of A350 and A380 airplanes for further testing and tuning activities. In all situations, the robustness appears to be very good (no false alarm) and all runaway faults have been detected within the allowed time window. Due to lack of space, the simulation results are not presented here. In the next section, some experimental results on Airbus ground testbed platforms are briefly mentioned (V&V investigations at Airbus).

Industrial validation using SIB

Firstly, the proposed monitoring scheme has been implemented in the FCC by using the limited set of SCADE graphical symbols (adder, integrator, filter, look-up tables, etc.). This process allows for describing each part of the algorithm in dedicated "functional specification sheets" according to the industrial state of practice. Then, an automatic generation tool produces the code to be directly implemented in a flight control computer. The developed strategy uses approximately 0.1% of the total CPU. This computation load is approximately 4.5 times higher than the in-service state-of-practice solution. The SIB is built around a real control surface actuator with simulated command inputs, aerodynamic forces and dedicated hydraulic circuit. This bench offers also the possibility to validate the designed system in several configurations, for example the situation when:

- The aircraft is in flight (aerodynamic forces have been simulated) or on the ground (no aerodynamic force);
- The servo-controlled actuator has been affected by one of the four aforementioned faulty situations involving a runaway occurrence.

During this industrial validation campaign, the use of rod sensor and control surface position sensor have been considered. Due to space limitation, the results obtained by using the control surface position sensor have been omitted. First, the robustness has been assessed during pure lateral maneuvers, pure longitudinal and during mixed maneuvers (combining lateral and longitudinal motions in the same maneuvers). Both smooth and dynamic maneuvers can be performed, as for example auto-pilot maneuvers, flight control checks, take-off and landing, etc. The results are summarized in Table 1 and show a very good robustness for the chosen α. FA denotes the false alarm rate in %. S flight and L flight denotes a short and a long experimental simulation time respectively. The detection performance (missed detections and detection time) has been evaluated and compared to the in-service monitoring solutions. The results are summarized in Table 2. The behaviour of residuals for different runaway speeds are not presented here. In this table, DTP (Detection Time Performance index) is given by: $DTP = (t_{\text{detect}} - t_{\text{occurence}}) / T_0$ where $t_{\text{occurence}}$ and t_{detect} are the time instants where the runaway occurs and is detected respectively. T_0 is the detection delay obtained by the state-of-practice monitoring scheme. $DTP < 1$ means an improvement of detection delay and $DTP = NaN$ corresponds to a missed detection.

Table 1: Robustness assessment

	Ground tests		In flight - cruise		In flight – approach	
	S flight	L flight	S flight	L flight	S flight	L flight
FA (%)	0	0	0	0	0	0

Table 2: Fault detection performance

	Runaway speed	Ground tests	In flight – cruise
LMEAS	high	$DTP < 1$	$DTP < 1$
	low	$DTP < 1$	$DTP < 1$
SMEAS	high	$DTP < 1$	$DTP < 1$
	low	$DTP < 1$	$DTP < 1$

DOI: 10.13009/EUCASS2017-692

LCUR	high	$DTP = 1$	$DTP < 1$
	low	$DTP = 1$	$DTP < 1$
SCUR	high	$DTP > 1$	$DTP = 1$
	low	$DTP < 1$	$DTP = 1$

6. Final thoughts

The so-called technology-push model of innovation considers innovation and technology transfer as a linear sequence of functional activities where the results from basic research "trickle down" into empirical reality in a logical sequence: basic research, applied research and development, products and commercialization [76]. A comprehensive time-based taxonomy of this model, whose source goes back to 1950s, is provided in [77]. The large bias that we can observe today between modern control theory and real-world aerospace systems is broadly due to the influence of this conception, as it shapes the way in which we try and manage innovation and transfer of technology. Today, few people defend such a linear understanding of innovation anymore, but the model is still going strong and the "rules of the game" are widely accepted. This model needs to be transformed to boost more resourcefully and effectively control research effort toward developing credible, innovative and unconventional solutions for real-world flight systems. This means a more interactive and dynamic model in which phases are over-lapped with feedbacks and loops, and which can deal appropriately with a much wider range of factors and their complexity which influence innovation process.

Aerospace systems provide numerous exciting challenges and opportunities that lie ahead for many research FDIR topics. Evolutionary and incremental improvements to existing systems should be supplemented (not rule out) by revolutionary technologies and concepts to support conventional industrial practices. As an example, in civil aviation, air traffic is expected to have doubled by 2035, and by 2050, 16 billion passengers will be flown annually. As traffic increases, so do concerns about capacity and safety. The aviation safety targets established within Europe and the USA for accident mitigation and prevention seek to reduce the aircraft accident/incident rate by approximately 80% by 2030-2035. The magnitude of this challenge is daunting and cannot be faced only by evolutionary improvements to existing systems alone - which are currently strained and can hardly be scaled to meet this expected demand. Moreover, reducing separation distances between aircraft to increase traffic capacity will require moving more functions to the flight deck which will result in increased complexity of in-flight operations. In this context, new FDIR methods will be required to enable paradigm shifts in tomorrow flight operational issues management. In space domain, the recent loss of ESA's ExoMars Schiaparelli spacecraft during its final descent through the Martian atmosphere may raise the question, amongst other things, of the need of more extended fault coverage and smart FDIR actions of the systems deployed for deep space missions.

To conclude, it is good to remind a great quote from Abraham Lincoln which is very relevant to this topic: "The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with[4] the occasion. As our case is new, so we must think anew and act anew. We must disenthrall[5] ourselves".

REFERENCES

[1] Sampigethaya K., R. Poovendran. Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport. Proceedings of the IEEE, Vol. 101, No. 8, August 2013.
[2] Wander A., R. Förstner. Innovative fault detection, isolation and recovery strategies on-board spacecraft: state of the art and research challenges. 2012. Available at: here.
[3] Gao Z., Cecati C., S.X. Ding. A Survey of Fault Diagnosis and Fault-Tolerant Techniques—Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches. IEEE Transactions on Industrial Electronics. Vol. 62, No. 6, June 2015.
[4] 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.
[5] Basseville, M., I. V. Nikiforov. Detection of Abrupt Changes: Theory and Application. Englewood Cliffs, NJ: Prentice Hall, 1993.
[6] Blanke, M., M. Kinnaert, M. Lunze, M. Staroswiecki. Diagnosis and fault tolerant control. Ed. Springer, New York. 2003.
[7] Patton R. J., P.M. Frank. Issues of fault diagnosis for dynamic systems. London: Springer-Verlag, 2000.
[8] Zolghadri, A. A redundancy-based strategy for safety management in a modern civil aircraft. Control Eng. Practice, Vol. 8, N° 5, pp 545-554, 2000.
[9] Cieslak J., Henry D., A. Zolghadri. Fault Tolerant Flight Control: From Theory to Piloted Flight Simulator Experiments, IET Control Theory & Applications, Vol 4, Issue 6, 2010.
[10] Isermann, R. Model-based fault-detection and diagnosis status and applications. Annu. Rev. Control, vol. 29, no. 1, pp. 71–85, 2005.

[4] Not rise to it, rise with it.

[5] There are ideas that all of us are enthralled to, our minds are hypnotized by them, and we have to disenthrall ourselves of some of them.

[11] Isermann R. Fault-diagnosis systems: an introduction from fault detection to fault tolerance, Berlin Heidelberg: Springer-Verlag, 2006.
[12] Ducard G. Fault-tolerant Flight Control and Guidance Systems. Springer, Advances in industrial control, 2009.
[13] Edwards C., Lombaerts T., H. Smaili. Fault Tolerant Flight Control: a benchmark challenge, Lecture Notes in Control and Information Sciences, Springer Ed, 2010.
[14] Zolghadri A., D. Henry, J. Cieslak, D. Efimov, P. Goupil. Fault Diagnosis and Fault-Tolerant Control and Guidance for Aerospace Vehicles, from theory to application. Springer, Series: Advances in Industrial Control. 2014.
[15] Ziegler and Nichols. Process lags in automatic-control circuits. Trans. of the ASME, 65, 433-444, 1943.
[16] Kalman R.E. Contribution to theory of optimal control. Bol. Soc. Mathematica Mexicana. pp. 1012-119, 1960.
[17] Kalman R.E. When is a linear control system optimal? Transactions of the ASME. Part D (Journal of Basic Engineering), 86, 51–89.
[18] Trentelman H.L., J.C. Willems. Essays on Control: Perspectives in the theory and its applications. Progress in Systems and Control Theory, Birkhäuser, 1993.
[19] Rosenbrock H.H, and P.D. McMorran. Good, bad or optimal? IEEE Transactions on Automatic Control, AC-16(6), 529–552, 1971.
[20] Athans M. Special issue on linear-quadratic-Gaussian problem. IEEE Trans. Autom. Control, vol. AC-16, no. 6, pp. 847–869, Dec. 1971.
[21] Horowitz I. and U. Shaked, "Superiority of transfer function over state-variable methods in linear time-invariant feedback system design," IEEE Trans. Autom. Control, vol. AC-20, no. 1, pp. 84–97, Feb. 1975.
[22] Doyle J. Guaranteed margins for LQG regulators. IEEE Trans. Autom. Control, vol. AC-23, no. 4, pp. 756–757, Aug. 1978.
[23] Youla D.C., J.J. Bongiorno. A Feedback Theory of Two-Degree-of-Freedom Optimal Wiener-Hopf Design. IEEE Trans. Autom. Control, vol. AC-30, no. 7, July. 1985.
[24] Doyle J., G. Stein. Multivariable feedback design: Concepts for a classical/modern synthesis. IEEE Transaction of Automatic Control, AC-26, pp 32-46, Feb, 1981.
[25] Zames G. Feedback and optimal sensitivity: Model reference transformations, multiplicative semi norms, and approximate inverses. IEEE Trans. Aut. Control, vol. AC-26, no. 2, pp. 301–320, Apr. 1981.
[26] Safonov G., A. J. Laub, and G. L. Hartmann. Feedback properties of multivariable systems: The role and use of the return difference matrix. IEEE Transaction of Automatic Control, AC-26, pp 32-46, Feb, 1981.
[27] Maciejowski J.M. Multivariable Feedback design, Addison-Wesley, 1989.
[28] Safonov G. Origins of robust control: Early history and future speculations. Annual reviews of control, 36, pp 173–181, 2012.
[29] Aseltine J.A., A.R. Mancini, and C.W. Sarture. A Survey of Adaptive Control Systems. IRE Trans. on Atomatic Control pp. 102-IOR, 1958.
[30] Bellman R., Adaptive Control Processes-A Guided Tour. Princeton University Press, Princeton, NJ, 1961.
[31] Aström K.J and B. Wittenmark, Adaptive Control, Addison-Wesley, MA, 2nd cd., 1995.
[32] Aström K.J. Adaptive Control Around 1960. 34th IEEE Conference on Decision and Control, New Orleans, LA. Dec. 14, 1995.
[33] Beard R.V. Failure accommodation in linear systems through self-reorganization. Ph.D. dissertation, Dept. Aeronautics Astronautics, Massachusetts Inst. Technol., Cambridge, Feb. 1971.
[34] Mehra, R.K., J. Peschon, An innovations approach to fault detection and diasgnosis in dynamic systems. Automatica, vol. 7, pp. 637–640, 1971.
[35] Jones, H. L. Failure detection in linear systems. Ph.D. dissertation, Dept. Aeronautics Astronautics, Massachusetts Inst. Technol., Cambridge, MA, Feb. 1973.
[36] Goupil P., AIRBUS state of the art and practices on FDI and FTC in flight control system. Control Eng. Practice, vol 19, pages 524-539, 2011.
[37] Osder S. Practical view of redundancy management, application and theory. Journal of Guidance, Control and Dynamics, vol. 22, N° 1, 1999.
[38] Marzat J, H. Piet-Lahanier, F Damongeot, E Walter. Model-based fault diagnosis for aerospace systems: a survey. Journal of Aerospace Engineering. January 6, 2012.
[39] Tomayko J.E. (2000). Computers Take Flight: A History of NASA's Pioneering Digital Fly-By-Wire Projec. Available at here.
[40] Samad T., A. Annaswamy. The Impact of Control Technology: Overview of success stories and research challenges. IEEE Control Systems Society. 2011. Available at: here.
[41] Traverse, P., I. Lacaze and J. Souyris. Airbus Fly-By-Wire: A Total Approach to Dependability. Proc. 18th IFIP World Computer Congress, Toulouse, France, pp.191-212, 2004.
[42] Favre C. Fly-by-wire for commercial aircraft: the Airbus experience. International Journal of Control, 59(1), 139-157, 1994.
[43] Van Oort E.R., L. Sonneveldt, Q. P. Chu and J. A. Mulder. Full Envelope Modular Adaptive Control of a Fighter Aircraft using Orthogonal Least Squares. Journal of Guidance, Navigation and Dynamics, 33(5), 2010.
[44] Lombaerts T., S. Schuet, D. Acosta, J. Kaneshige. On-Line Safe Flight Envelope Determination for Impaired Aircraft. EuroGNC, Toulouse, France, 2015.
[45] Lombaerts T., G. Looye, J. Ellerbroek, M. Rodriguez y Martin. Design and Piloted Simulator Evaluation of Adaptive Safe Flight Envelope Protection Algorithm. AIAA GNC Conference, San Diego, USA, 2016.
[46] Schuet S., T. Lombaerts, D. Acosta, K. Wheeler, J. Kaneshige. An Adaptive Nonlinear Aircraft Manoeuvring Envelope Estimation Approach for Online Applications. AIAA GNC, Maryland, 13-17 January 2014.
[47] Allen R., G.K. Harry. Maneuverability and envelope protection in the prevention of aircraft loss of control. 8th IEEE Asian Control Conference, June 2011.
[48] Tang L., Roemer M. G. Jianhue, A. Grassidis, J.V.R. Prasad, C. Belcastro. Methodologies for adaptive flight envelope estimation and protection. AIAA report available at: here.
[49] Pandita R., P. Seiler, G. Balas. Reachability and region of attraction analysis applied to GTM dynamic flight envelope assessment. AIAA report available at: here
[50] Tekles N., J. Chongvisal, E. Xargay, R. Choe, D. A. Talleur, N. Hovakimyan, and C. M. Belcastro. Design of a Flight Envelope Protection System for NASA's Transport Class Model. AIAA Journal of Guidance, Control, and Dynamics. 2016.
[51] Bartley, G. F. The Avionics Handbook, chap. Boeing B-777: FBW Flight Controls, CRC Press LLC, 2001. Retrieval date: October 17, 2016.
[52] Endsley M.R., Garland D.J., Shook R.W., Goello J., Bandiero M. Situation Awareness in General Pilot Aviation. Annual report, Year 1, prepared for NASA Ames Research Center, 2000.
[53] Young S.D., T.S. Daniels, E. Evans, M. Uijt de Haag, P.P. Duan. Understanding Crew decision making in the presence of complexity– A flight simulation experiment. Conference, Guidance, Navigation, and Control and Co-located Conferences, (AIAA 2013-4894).
[54] Bailey R.E., K.E. Ellis, C.L. Stephans, E.K. Kyle, L.S. Chad. Test and evaluation metrics of crew decision-making and aircraft attitude and energy state awareness. 2014. AIAA report available at: here
[55] Battiste1 V. and Bortolussi M. Transport Pilot Workload: A Comparison of Two Subjective Techniques. SAGE Journals, October 1988 vol. 32 no. 2, 150-154. 1988.
[56] Uhlarik J., D.A. Comerford. A Review of Situation Awareness Literature Relevant to Pilot Surveillance Functions. Final report, Office of Aerospace Medicine, Washington DC, 2002. Available at: here.

DOI: 10.13009/EUCASS2017-692

[57] Sahani N. Envelpe protection systems for piloted and unmanned rotorcraft. PhD thesis. The Pennsylvania State University, 2005.
[58] Tipaldi M., B. Bruenjes. Survey on Fault Detection, Isolation, and Recovery Strategies in the Space Domain. Journal of Aerospace Information Systems, Vol. 12, No. 2, pp. 235-256, 2015.
[59] Jacobson S. R. Aircraft Loss of Control Causal Factors and Mitigation Challenges. NASA Dryden Flight Research Center, Edwards, California, 2010.
[60] 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, Y.W. Tung. Spacecraft autonomy flight experience: The DS1 remote agent experiment. Proc. AIAA, Albuquerque, NM, 1999.
[61] Olive X. (2012). FDI(R) for satellites: how to deal with high availability and robustness in the space domain. Int. J. Appl. Math. Comput. Sci., 2012, Vol. 22, No. 1, 99–107.
[62] Falcoz F., D. Henry, and A. Zolghadri, Robust fault diagnosis for atmospheric re-entry vehicles: a case study. IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems & Humans, vol. 40, no. 5, pp. 886–899, 2010.
[63] Schwabacher M.A., Feather M.S., Markosian L.Z. Detection, Isolation and Recovery for a NASA Space System. 2008.
[64] Ferell B., Lewis M. Perotti J., Oostdyk R., Goerz J., Brown R. Lessons Learned on Implementing Fault Detection, Isolation, and Recovery (FDIR) in a Ground Launch Environment. Ames Research Center; Kennedy Space Center, 2010. Available at: here.
[65] Grewal M., A.P. Andrews. Applications of Kalman Filtering in Aerospace 1960 to the Present. IEEE CSM, 2010.
[66] Hutchinson C.E. The Kalman filter applied to aerospace and Electronic systems. IEEE TAES. Vol 20, no 4, July 1984.
[67] Campiy M. Performance of RLS Identification Algorithms with Forgetting Factor: A Phi_mixing approach. Journal of Mathematical Systems, Estimation, and Control, Vol. 4, No. 3, 1994.
[68] Lindoff B., J. Holst. Convergence analysis of the RLS identification algorithm with exponential forgetting in stationary ARX-structures. International J. of Adaptive Control and Signal Processing, Feb 1997.
[69] Niui S., D.G. Ficher. Detecting parameter identifiability problems in system identification. International Journal of Adaptive Control and Signal Processing. Vol. 11, 1997.
[70] Ljung L. System Identification: Theory for the User (2nd Edition), Englewood Cliffs NJ: Prentice-Hall, 1998.
[71] Chang K.Y., Su W.S., In-Beum L. Generalized damped least squares algorithm. Computers and Chemical Engineering, 27, 423-/431. 2003.
[72] Kofahl, R.J. Robustness and eigenvalue analysis of least squares estimators for parameter adaptive control. IFAC Workshop on Robust adaptive Control. Newcastle, Australia, 1988.
[73] Kerr T. H. Decentralized filtering and redundancy management for multi-sensor navigation. IEEE Trans. Aerospace Electronic Syst., vol.23, pp. 83-118, 1987.
[74] Zolghadri A. An algorithm for real-time failure detection in Kalman filters. IEEE Transactions on Automatic Control 41 (10), 1537-1540. 1996.
[75] Zolghadri, A., Le Berre, H., Goupil, P. Gheorghe A., Cieslak, J., Dayre, R. Parametric approach to fault detection in aircraft control surfaces. AIAA Journal of Aircraft. Vol. 53, No. 3, pp. 846-85, 2016.
[76] Storbacka.K. Does publish or perish lead to stylish rubbish? J Bus Mark Manag (2014) 7(1): 289–295, 2014.
[77] Godin B. The Linear Model of Innovation: The Historical Construction of an Analytical Framework, 2005. Available at: here.
[78] ECSS 70-11A, Space engineering: Space segment operability, European Cooperation for Space Standardization standard, 2005.