EuroGNC Navigation Guidance Control CEAS Bristol, UK June 11th-13th 2024
University of BRISTOL ROYAL AERONAUTICAL SOCIETY AIAA

Evaluation of an Independent Flight Control Law Monitor

Dominik Hübener Research Assistant, Technische Universität Berlin, Department of Flight Mechanics, Flight Control and Aeroelasticity, 10587, Berlin, Germany. d.huebener@tu-berlin.de

Robert Luckner Professor, Technische Universität Berlin, Department of Flight Mechanics, Flight Control and Aeroelasticity, 10587, Berlin, Germany. robert.luckner@tu-berlin.de

Guido Weber Senior Expert Primary Flight Control Systems, Liebherr-Aerospace Lindenberg GmbH, Chief Engineering Flight Controls and Actuation Systems, 88161, Lindenberg, Germany. guido.weber@liebherr.com

ABSTRACT

Electronic flight control systems are safety-critical and complex. Such systems require highest levels of integrity and availability. This is why the development process for embedded flight control laws has to ensure rigorous validation and verification. However, complete absence of development errors – especially in the requirements - cannot be guaranteed. Usually, there is one requirement set from which flight control laws and their software are developed. Accordingly, undetected errors in the flight control law requirements represent a potential single point of failure. One possible approach is to develop independent flight control law monitoring functions. This paper integrates potential Independent Monitoring Functions into an overall Independent Monitor for flight control laws. It evaluates its effectiveness and robustness, using a simulation environment with a flight mechanical model of a commercial aircraft and its flight control laws for manual flight.

Keywords: Development Error; Flight Control Law; Independent Monitoring; Requirement Error; safety critical functions

Nomenclature

Ψ, θ, ϕ	=	Euler angles (azimuth, pitch, bank)
p, q, r	=	Angular rates (roll, pitch, yaw)
α, β	=	Angle of attack, side slip angle
$\eta_{cmd}, \xi_{cmd}, \zeta_{cmd}$	=	Control surface commands (elevator, aileron, rudder)
$H_{msl}, \dot{H}$	=	Height above mean sea level, vertical speed
V_{CAS}, V_{TAS}, Ma	=	Calibrated airspeeds, true airspeed, mach number
n_z, n_y	=	Normal load factor (z axis), lateral load factor (y axis)
$\dot{\chi}, \dot{\gamma}$	=	Rate of change track, rate of change flight path angle
THS	=	Trimmable horizontal stabilizer
fh	=	Flight hour

1 Introduction

Electronic flight control systems are safety-critical and complex. Such systems require highest levels of integrity and availability. This is why the development process for the embedded flight control laws (FCL) has to ensure rigorous validation and verification. In typical fly-by-wire architectures, flight control laws are developed based on a common set of requirements. The FCL software is implemented in dissimilar computing lanes, often called control and monitor lane, and the outputs of the lanes are compared to detect faults. References [1],[2],[3] describe flight control system architectures of modern commercial aircraft. The dissimilar implementation of both lanes is state-of-the-art, and it ensure that hardware faults and the effects of implementation (coding) errors can be detected. This approach assures fail-passive behaviour if the lanes disagree.

However, nearly all serious incidents and accidents, in which software was involved, are related to requirement flaws and not to coding errors. This phenomenon is observed in different industrial sectors [4]. As the complexity of FCL increases, so does the risk of undetected requirement errors, which can be a source of common mode errors and subsequent failures. Generally, development assurance is used to mitigate the risk of development errors. However, the European Union Aviation Safety Agency (EASA) highlights in MOC SC-VTOL.2300 [5] that "Full reliance on Development Assurance […] as sole mitigation of a common mode failure […] shall be avoided as far as practicable." and recognizes in a non-published generic certification review item[1] [6] that "monitoring of the Flight Control Laws may be a possible mitigation against common mode errors". An FCL monitor that is independent from the FCL requirements could be key to achieve fault tolerance against FCL requirement errors. Therefore, the EASA has launched a project [7] to investigate if such an Independent Monitor can detect effects caused by FCL development errors.

Reference [8] discusses principles for functions of such a monitor and proposes two concepts: Comparator and Plausibility Check[2]. Reference [9] assesses the feasibility of the proposed concepts and compares the effectiveness and robustness of both concepts. In this paper, the monitor functions, investigated in [9], are adapted to another example aircraft. They are improved and combined to an independent monitor. To evaluate the monitor's effectiveness, the effects of potential FCL requirement errors that the monitor shall detect are simulated by pseudo failure injection, either by replacing a control surface command by a faulty signal (e.g. command runaway) or by manipulation of the source code (e.g. by falsifying gains). Its robustness is investigated in manoeuvres, which are more aggressive as in Reference [9], as well as in gusty and turbulent flight conditions.

In Section 2 concepts for independent monitor functions of FCL are described. Section 3 outlines the evaluation approach. Section 4 discusses the results. The paper concludes with an assessment of the evaluation results and an outlook on future validation activities.

2 Concepts for FCL Monitors

The primary objective of an independent monitor for FCL (IM-FCL) is to mitigate the effects of common mode development errors, i.e. requirement errors. The IM-FCL should detect a failure before

[1] A Certification Review Item (CRI) is a formal administrative means within the certification process. It provides a structured means of recording subjects regarding the certification basis and its interpretation throughout a certification project. The intent is to reflect the current certification practices and to facilitate future certification projects. A specific number is allocated to the CRI at each project.

[2] Reference [8] uses the term A*cceptability Check* instead of *Plausibility Check* to describe this concept.

it becomes hazardous, but it must not cause false alarms, and it must be functionally independent from the FCL that it monitors. That means, requirements for the IM-FCL have to be defined that differ from the FCL requirements. From those requirements, independent monitoring functions have to be developed. In order to minimize the likelihood of additional development errors within the monitor requirements, it is necessary to keep the monitoring functions as simple as possible.

Reference [8] describes principles and concepts for independent monitoring of FCL. Multiple Independent Monitoring Functions (IMFs) form an IM-FCL. It is assumed that signal integrity is assured by existing functions (*Input Monitoring & Consolidation function*) that are not part of the FCL. Furthermore, it is assumed that there is an alternative to which the FCS can switch automatically after a failure has been detected. Such an alternative could be an FCL that is so simple that absence of errors can be proven. However, the system reaction after the monitor trips, e.g. switch to such an error-free law, is out of scope of this paper.

2.1 Example Independent Monitoring Functions

Concepts for IMFs can be categorized by their decision mechanism. A decision mechanism is a function that adjudicates, arbitrates, or otherwise decides on the acceptability of the results obtained by two independent variants. Two concepts are investigated: *Comparator* and *Plausibility Check*.

A *Comparator* compares the outputs of the Normal Mode (NM) FCL to the outputs of a functionally independent alternative, like the Direct Mode (DM) FCL. Reference [9] provides an example for a comparator IMF.

A *Plausibility Check* verifies that the behaviour of the FCL software is acceptable in the sense of plausibility rather than correctness, based on predictions on the anticipated system state. Possible Plausibility Checks can be categorized into three groups:

- *Limit Checks*,
- *Behaviour Checks (*comprising *hands-free, sign* and *controllability checks)*, or
- *Command Checks (*comprising *protection function, command sign*, and *pitch trim drift check*s*)*.

Limit Checks check for a violation of flight envelope limits that the aircraft must not exceed. *Behaviour Checks* check the plausibility of the aircraft reaction under consideration of the pilot demand. They include *hands-free checks* that monitor that the aircraft response does not exceed a predefined limit without a corresponding pilot input; *sign checks* that monitor that the aircraft response does not contradict the pilot demand; and *controllability checks* that monitor whether the aircraft response to pilot inputs is sufficient to allow normal manoeuvres. Reference [9] provides examples for limit, hands-free and sign checks. Table 1 gives an example of a controllability check for the roll rate. The requirement for the controllability check that monitors a vertical trajectory change ($\dot{\gamma}$) is defined analogously.

Command Checks comprise checks for plausibility of the FCL commands to the control surfaces. The control surface commands are monitored under consideration of the pilot demand. Three types of command checks are used: *protection function checks, aileron command sign check,* and *pitch trim drift check*.

Table 1 Requirement for the roll rate controllability check.

Requirement	IMF shall trip if pilot right wing down/(left wing down) input exceeds 50%, AND roll rate p falls short of 3.4 °/s / (stays above −3.4 °/s), AND aircraft is operated in normal flight envelope.
Rational	Sufficient lateral control must be available to provide a peak roll rate necessary for safety. Roll response must allow normal manoeuvres (such as recovery from upsets produced by gusts and the initiation of evasive manoeuvres).
Type	Behaviour Check

Protection function checks monitor the plausibility of the FCL control surface commands while a protection function is active. Table 2 gives an example of the overspeed protection check. This function checks that the elevator command from the overspeed protection function would not lead to increased airspeeds. Requirements for the bank angle, pitch angle, and angle of attack protection function checks are defined analogously.

Table 2 Requirement for the overspeed protection check.

Requirement	IMF shall trip if the overspeed protection is active, AND no pilot pitch input, AND the FCL commands elevator deflections that lead towards an increasing airspeed.
Rational	Above the limit for the maximum operational speed (VMO), the overspeed protection should generate pitch-up elevator commands (positive load factors) that return the airspeed (calibrated airspeed $VCAS$) into the range: $VCAS \leq VMO$.
Type	Command Check

The *aileron command sign check* IMF is like the roll rate sign check IMF described in [9]. Instead of roll rate, it monitors whether the initial aileron command induces a roll motion according to the pilot demand, while the aircraft is operated in the normal flight envelope, i.e. no protections are active. If not, the IMF trips.

The *pitch trim drift check* monitors whether the automatic trim function decreases the elevator hinge moment. Table 3 shows the requirement for this IMF.

Table 3 Requirement for the pitch trim drift check.

Requirement	IMF shall trip if the elevator command η_{cmd} exceeds (/falls below) the neutral elevator deflection η_0, AND the THS command rate is nose-up (/nose-down), AND aircraft is operated in the normal flight envelope.
Rational	The automatic trim function should decrease the elevator hinge moment.
Type	Command Check

2.2 Investigated Independent Monitoring Functions

Table 4 lists the investigated independent monitoring functions (IMFs). Twenty-four IMFs are investigated for both effectiveness and robustness. The eleven IMFs investigated in [9] are improved, e.g. by added confirmation times to improve robustness. Additionally, thirteen new IMFs are implemented. Table 11 in the Annex lists all IMFs with their corresponding number.

Table 4 List of proposed IMFs.

Function (number of IMFs)	Monitored Parameter	Example	Type
Limit Checks (5)	V_{CAS}, n_z, θ, α and ϕ	Ref. [9], [8]	Limit Check
Hands-free Checks (5)	p, ϕ, n_z, β and n_y	Ref. [9]	Behaviour Check
Sign Checks (3)	p, q and n_z	Ref. [9], [8]	
Controllability Checks (2)	p and $\dot{\gamma}$	Table 1	
Protection Function Checks (4)	η_{cmd} and ξ_{cmd}	Table 2	Command Check
Command Sign Check (1)	ξ_{cmd}	Ref. [9], [8]	
Trim Drift Check (1)	THS command	Table 3	
Command Comparison (3)	η_{cmd}, ξ_{cmd} and ζ_{cmd}	Ref. [9]	Comparator

3 IM-FCL Evaluation Approach

Many of the concepts on which the proposed IMFs are based, have been used in other applications or for other purposes. For example, Airbus aircraft make use of an Abnormal Attitude Monitor, which is similar to the limit checks described in this paper. However, this function was introduced to enable switching to a simpler control law when the aircraft is in an abnormal situation far beyond the protected flight envelope [10]. For such extreme attitude conditions, it cannot be assured that the flight mechanical models for the design of the NM FCL are sufficiently accurate, for example, non-linear and local effects at high angles of attack. Also, the NM FCL relies on the integrity of other systems (e.g. sensors) that cannot be guaranteed for abnormal attitudes.

To the authors knowledge, none of the functions described in Section 2 have been applied to detect the effects of FCL errors. Reference [9] demonstrates the feasibility of the proposed limit checks, hands-free checks, and the comparator concept. In this paper, the previously investigated IMFs are supplemented with confirmation times to improve their robustness. They and additional IMFs are implemented on a different aircraft to evaluate the effectiveness and robustness of an Independent Monitor of the FCL, comprising all IMFs described in Section 2. The objective of this paper is to demonstrate that the overall IM-FCL can effectively detect the effects of FCL development errors, while being robust under foreseeable operational conditions. Furthermore, it is investigated which IMFs are essential for detection, which are sufficiently robust, and which are dispensable.

3.1 Simulation Environment

The validation activities make use of a closed-loop flight simulation consisting of an aircraft flight mechanical model, representing a regional twin jet aircraft (VFW614), plus a set of state-of-the-art flight control laws that comprise a Normal Mode and a Direct Mode as back up. The aircraft model and the flight control laws were developed in an earlier technology project, in which new technologies for an Electronic Flight Control System were developed and demonstrated. The FCL were flight-tested from the year 1999 to 2000 [11]. Therefore, the flight simulation environment provides a highly representative platform for the IM-FCL evaluation activities.

Based on the existing real-time flight simulator software, a desktop Flight Simulation Environment was prepared for offline simulations during development of IM-FCL. The desktop Flight Simulation Environment has been extended to evaluate the monitor's effectiveness. The effects of potential FCL

requirement errors that the monitor shall detect are simulated by pseudo failure injection, either by replacing a control surface command by a faulty signal (e.g. command runaway) or by manipulation of the source code (e.g. by falsifying gains).

The test cases for the monitor evaluation are grouped into two test categories, effectiveness tests and robustness tests. Effectiveness tests check for the timely detection of pseudo failures as described in [8]. Robustness tests check for spurious detections under failure-free operating conditions including operational manoeuvres and substantial external disturbances. Under these conditions, the monitor is robust if it does not trigger a false alarm. A test case comprises a trim point, a pseudo failure or an external disturbance and a manoeuvre.

3.2 Selected Trim Points

Representative trim points for the operational flight envelope of the aircraft have been selected. Figure 1 shows the selected trim points, and the flight envelope limits (V_{TAS} and H_{msl}) of the aircraft. The red line defines the flight envelope limits that shall never be exceeded. The green dashed line represents FCL protection limits. Normal Law protection functions are active in the area between the green dashed and the red lines. The selected trim points are shown as blue circles. Filled circles represent steady straight horizontal flight conditions and unfilled circles are steady horizontal turns ($\phi = 25°$).

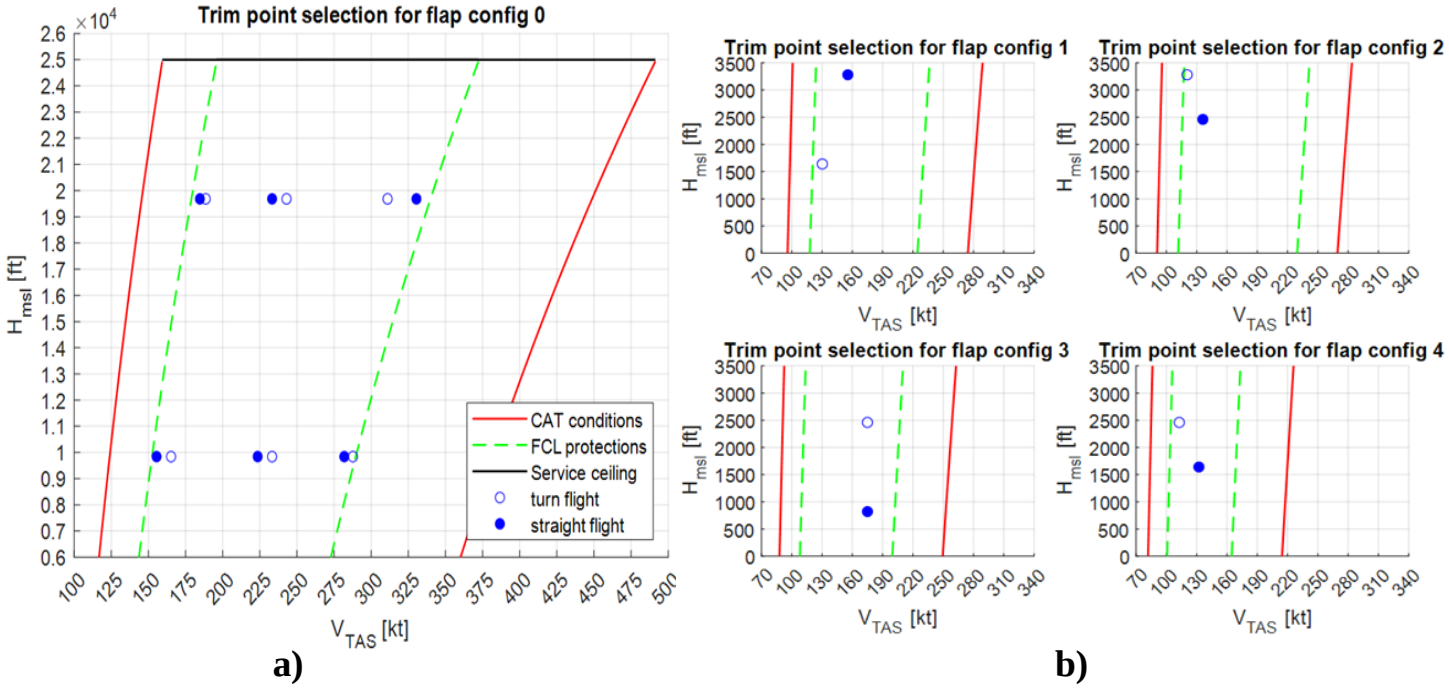

Fig. 1 Selected trim points at a) middle and high altitude in clean configuration and b) low altitude and flaps deflected.

The selected trim points are used for both effectiveness and robustness evaluation. The focus of the investigation lies on the high and medium altitude trim points, as the aircraft is operated in this area of the flight envelope most of the time. Additionally, some trim points at low altitudes have been selected.

The risk of FCL errors being manifested is higher at the corners of the flight envelope where complex functionality is engaged. However, if the IM-FCL cannot be shown to be effective and robust in the normal operational flight envelope, the chances of developing a good IM-FCL for the whole flight envelope are close to zero.

3.3 Effectiveness Tests

To investigate the effectiveness of the IM-FCL, it is assumed that a potential FCL requirement error would result in a catastrophic (CAT) failure condition. Such failure conditions are defined. As exemplary requirement errors are not available, their potential worst-case effect is mimicked by so-called pseudo failures. Most pseudo failures are injected by replacing the FCL output with a predefined signal, e.g. runaway signal. Additionally, more complex pseudo failures are injected by direct manipulation of the FCL source code, e.g. high gain, or sign error. For simplicity, the term failure is used in the following text.

A preliminary hazard assessment of the proposed failures at the selected trim points is performed. A failure is considered CAT if continued safe flight and landing is not possible. Continued safe flight and landing cannot be demonstrated if the failure results in excessive structural loads, high airspeeds, high bank angles or loss of flight path control (e.g. stalls or loss of manoeuvrability) [12]. CAT thresholds for the structural loads, airspeed, bank angle and angle of attack have been defined based on aircraft design limits and engineering judgement. A simplified approach is used to assess the manoeuvrability of the aircraft. Sufficient manoeuvrability is assumed if:

- $n_z \leq 0.8\ g$ within 2 seconds after a push-over manoeuvre, AND
- $n_z \geq 1.3\ g$ within 2 seconds after a pull-up manoeuvre, AND
- $|\Delta\Phi| \geq 45°$ within 3.8 seconds after a full roll input.

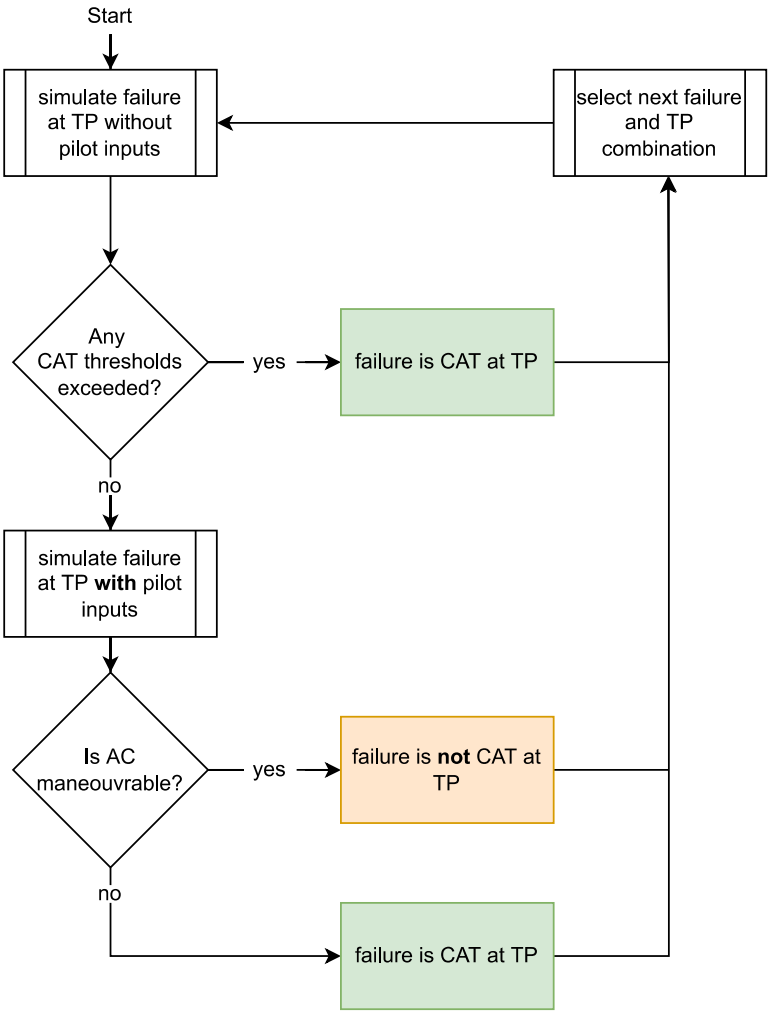

Fig. 2: Flowchart of preliminary hazard assessment.

Figure 2 shows the simplified procedure used to assess the hazard of a proposed failure at a given trim point. First, the failure is simulated at a specific trim point without any pilot inputs. If the failure leads to exceedance of any CAT threshold, it is considered CAT at the given trim point. Otherwise, the failure is simulated with additional pilot inputs to assess the manoeuvrability. If the aircraft cannot be manoeuvred any more (loss of control), the failure is considered CAT at the specific trim point. This procedure is repeated for each possible combination of trim points and failures.

Twenty-six failures are CAT at least for one of the selected trim points. Those failures include runaway-like failures of each control surface commands as well as command freeze of the elevator and the aileron commands and additionally, more complex failures, i.e. erroneous activation of protection functions, high gains in the flight control functions and sign failures in the protection functions. Table 5 lists the failures used for effectiveness tests.

Table 5: Selected pseudo failures for effectiveness tests.

Failure	Description
IHCRNWSN	THS command runaway slow negative.
IHCRNWFN	THS command runaway fast negative.
ETCRNWFP	Elevator command runaway fast positive.
ETCRNWFN	Elevator command runaway fast negative.
ETCRNWSP	Elevator command runaway slow positive.
ETCRNWSN	Elevator command runaway slow negative.
ETCOHLD	Elevator command hold.
XICRNWASS	Aileron command asymmetric runaway (right wing down) slow.
XICRNWASF	Aileron command asymmetric runaway (right wing down) fast.
XICRNWASS2	Aileron command asymmetric runaway (left wing down) slow.
XICRNWASF2	aileron asymmetric runaway (left wing down) fast.
XICHLD	Aileron command hold.
ZECRNWFN	Rudder command runaway fast negative.
ZECRNWFP	Rudder command runaway fast positive.
ZECRNWSN	Rudder command runaway slow negative.
ZECRNWSP	Rudder command runaway slow positive.
SP34CRRNWF	Right spoilers 3 and 4 command runaway (right wing down) fast.
SP34CRRNWF2	Left spoilers 3 and 4 command runaway (left wing down) fast.
AAOA	Erroneous activation of angle of attack protection.
AHISPD	Erroneous activation of high-speed protection.
ATHPRT	Erroneous activation of pitch attitude protection.
APHIPRT	Erroneous activation of roll attitude protection.
PNL	High gain in pitch normal law.
RNL	High gain in roll normal law.
FAOA	Erroneous sign in angle of attack protection.
FHISPD	Erroneous sign in high-speed protection.

The selected trim points and failures are combined with normal operational manoeuvres to define the conditions for effectiveness tests.

Table 6 lists the flight manoeuvres that are used for effectiveness tests. They represent typical flight manoeuvres during cruise. Additionally, a landing approach is selected. Combining the selected trim points, manoeuvres, and failures results in 857 effectiveness tests.

Table 6: Selected manoeuvres for effectiveness tests.

ID	Description
HF	Hands-free
CLB	1000 ft climb manoeuvre, 2000 ft/min rate of climb
DSNT	1000 ft descent manoeuvre, $-2000\ ft/min$ rate of descent
TURN	Initiate a 90-degree turn with a turn rate of $r = 3\ °/s$
TCLB	Steady turn[3], 1000 ft climb manoeuvre
TDSNT	Steady turn, 1000 ft descent manoeuvre
LND	Landing approach with lateral offset to localiser with pilot model

3.4 Robustness Tests

To investigate the robustness of the IMFs, the normal operation flight manoeuvres defined in Table 6 are combined with external disturbances (severe gusts and turbulence). Additionally, high-gain manoeuvres are defined to push the aircraft into operational limits and to activate FCL protection functions.

Table 7 lists the selected high gain manoeuvres.

Table 7: Selected high gain manoeuvres for robustness tests.

ID	Description
FCLBPS	3000 ft fast climb manoeuvre, $\dot{H} > 5000\ ft/min$ rate of climb, if target altitude is reached high push command.
FDSNTPL	3000 ft fast descent manoeuvre, $\dot{H} < -5000\ ft/min$ rate of descent, if target altitude is reached high pull command.
EDSNT	Emergency descent, full spoiler, thrust 0, $\dot{H} = -6000\ ft/min$ rate of descent.
FTURN	Initiate a 180-degree turn, with turn rate of $\dot{\chi} > 5\ °/s$, high pull-up command allowed, constant altitude ± 500 ft.
TFCLB	fast 3000 ft climb manoeuvre and turn with turn rate of $\dot{\chi} > 5\ °/s$, then level flight.
TFDSNT	fast 3000 ft descent manoeuvre and turn with turn rate of $\dot{\chi} > 5\ °/s$, then level flight.
LNDHG	Landing approach with high lateral offset to localiser with pilot model, high gain pilot.

The selected external disturbances comprise turbulence of three different intensities as well as discrete gusts. The discrete gusts include crosswind gust, downwind gust, upwind gust, and headwind gust. Tailwind gusts are excluded from robustness evaluations due to their negligible impact on IMFs, as demonstrated in reference [9].

The gust intensities are based on CS-25 [12] and SAE AS94900 [13] standards. The CS-25 discrete gust has a probability of occurrence of 1 in 70,000 flight hours. This gust is used to estimate the

[3] Only combined with steady turn trim points, therefore no roll inputs required.

maximum aircraft gust loads. In the context of IMF robustness evaluation, this gust represents the most critical gust encounter during which IMFs shall not trigger a false alarm. Gust intensities based on SAE AS94900 are selected, to investigate gusts with lower intensities and higher probabilities of occurrence, i.e. 1 in 1,000 flight hours.

A total of 1348 robustness tests have been defined, combining the selected trim points, manoeuvres, and external disturbances.

4 Evaluation of Test Results

The 857 effectiveness tests and 1348 robustness tests have been simulated and their results have been evaluated, to investigate if an IM-FCL, consisting of the IMFs listed in Table 4, can effectively detect the effects of FCL development errors, while being robust under foreseeable operational conditions.

An indicator of the effectiveness is the percentage of detection (POD). A POD equal to one represents an effectiveness of 100%. It is calculated by dividing the times the IM-FCL detected a failure, N_{FD}, by the total number of effectiveness tests, N_T, that comprised the specific failure. The detection time, the time that elapses from failure injection until failure detection, is another quality characteristic

$$POD = \frac{N_{FD}}{N_T}.$$

The percentage of false alarms (PFA) is used as an indicator for the robustness. A PFA equal to 0 represents a very robust IMF. It is calculated analogously to the POD, by dividing the times an IMF triggered a false alarm. N_{FA}, by the number of robustness tests

$$PFA = \frac{N_{FA}}{N_T}.$$

4.1 Effectiveness Test Results

The detection times of each IMF are evaluated for each effectiveness test. The IM-FCL detects a failure, if at least one of the IMFs detects a failure. In addition, the tests are grouped for each failure listed in Table 5. The POD of the IM-FCL and individual IMFs is calculated for each failure. Table 8 shows the results of the effectiveness tests.

The first column lists all investigated pseudo failures. The second column lists the POD of the IM-FCL, and the third column lists all IMFs that contributed with a POD higher than 70 %. The individual IMF number is listed in Table 11, see Annex.

In most cases, more than one IMF detect a failure. Especially, command-runaway-like failures (*CRNW*) lead to an exceedance of the limit check thresholds. However, these IMFs (1 to 5) detect the failure significantly later than the command comparison IMFs (22 to 24). It has to be evaluated if such late detections are acceptable or if the associated IMF is dispensable.

Failures that mostly affect control surfaces for the longitudinal motion (i.e., IHC*, ETC*, AAOA, AHISPD, ATHPRT, PNL, FAOA and FHISPD) are detected with high POD by the corresponding limit check IMFs (1, 2, 3 and 4), the Trim Drift Check (21) and the Elevator Command Comparison IMF

(22). The Pitch Angle and Angle of Attack Protection Check (16 and 18) effectively detect a sign error in the angle of attack protection function (FAOA).

The elevator command freeze (ETCOHLD) is detected by IMFs 3, 12, 13, 15 and 21. However, no IMF reaches a POD > 70 %. The trim drift check (21) is the best with a POD of 58 %. Also, several IMFs 6, 8, 12, 15, 16 and 22 detect the erroneous activation of the angle of attack (AAOA) and overspeed protection (AHISPD) – yet, with a POD < 70 %. The Angle of Attack Protection Check (16) and the Roll Rate Hands-free Check (6) detect best with PODs of 66 % and 42 % respectively. The high gain error in the pitch normal law (PNL) causes pilot-involved oscillations (PIO). It is detected by IMFs 2, 8, 12 and 22. The Pitch Rate Sign Check and Load Factor Hands-free Check (12 and 8) contribute with a POD of around 60 % while the other two reach a POD of 50 %.

The Pitch Rate Sign Check (12) is the only IMF that detects the ATHPRT failure. The erroneous activation of the pitch angle protection function, results in a feedforward gain of zero for pitch inputs. That means, any pitch input on the side stick results in an incremental normal load factor demand $\Delta n_z = 0$. Therefore, the aircraft does not react to any pitch inputs. As all test cases are initiated within the normal flight envelope during steady state flight, this failure does not lead to exceedance of any limit. Therefore, neither the limit, hands-free, trim drift nor protection function check can detect this failure. The $\dot{\gamma}$ Controllability Check (15) and the Elevator Command Comparison IMF (22) should be able to detect this failure. However, the first requires pitch-down demands of above 50% of maximum side stick deflection, which are not achieved. And the Elevator Command Comparison IMF (22) would require a lower threshold to detect this failure. A smaller threshold would significantly reduce the robustness of this IMF, further optimization is required to improve detection capabilities.

Table 8: Percentage of detection of investigated failures.

Failure	POD	$IMF_{>70\%}$
IHCRNWSN	100.00%	**21,22**
IHCRNWFN	100.00%	**21,22**
ETCRNWFP	100.00%	**2,3,22**
ETCRNWFN	100.00%	**2,3,4,22**
ETCRNWSP	100.00%	**21,22**
ETCRNWSN	100.00%	**4,21,22**
ETCOHLD	91.67%	-
XICRNWASS	100.00%	**2,3,5,7**
XICRNWASF	100.00%	**2,3,4,5,7,23**
XICRNWASS2	96.67%	**3,5,23**
XICRNWASF2	100.00%	**2,3,4,5,23**
XICHLD	80.00%	**14**
ZECRNWFN	100.00%	**6,9,10,24**
ZECRNWFP	100.00%	**9,10,22,23,24**
ZECRNWSN	100.00%	**9,10,24**
ZECRNWSP	100.00%	**9,10,24**
SP34CRRNWF	100.00%	**23**
SP34CRRNWF2	96.67%	**23**
AAOA	74.51%	-
AHISPD	66.67%	-
ATHPRT	37.50%	-
APHIPRT	80.39%	-
PNL	91.67%	-
RNL	100.00%	**23**
FAOA	100.00%	**3,4,16,18**
FHISPD	100.00%	**1,3**

The failures mostly affecting control surface commands of the lateral motion (XIC*, ZEC*, SP34C*, APHIPRT and RNL) are effectively detected by the IM-FCL. Aileron command runaways are effectively detected by the Pitch and Bank Angle Limit Check (3 and 5), the Bank Angle Hands-free IMF (7) and the Aileron Command Comparison (23). The aileron command freeze (XICHLD) is only effectively detected by the Roll Rate Controllability IMF (14).

Rudder command runaways (ZEC*) are effectively detected by the Side Slip Angle and Lateral Load factor Hands-free IMFs (9 and 10), and the Rudder Command Comparison IMF (24). The latter is

the IMF with the fastest detection. IMFs 9 and 10 are redundant and could be removed from the IM-FCL. The spoiler command runaways (SP34C*) and erroneous gain in the roll normal law (RNL) are detected by the Aileron Command Comparison (23) in over 90 % of the test cases. Only the erroneous activation of the bank angle protection (APHIPRT) requires more than one IMF to achieve a high POD of the IM-FCL.

It is noteworthy that the Overspeed Protection Check (17) does not detect the effects of an error in the overspeed protection function (FHISPD). This IMF, as well as the Roll Rate and Load Factor Sign Check (11 and 13), Bank Angle Protection Check (19), and Aileron Command Sign Check (20) do not significantly contribute to the effectiveness of the IM-FCL. Their specific activation conditions reduce its effectiveness and increases its complexity. They could be removed from the IM-FCL.

The confirmation time added to the hands-free and sign IMFs reduces their effectiveness. Most failures lead to an exit from the normal flight envelope, deactivating the IMF, before the confirmation time allows a detection. Monitoring the FCL output directly, i.e. command comparison IMFs seem to be a better approach.

In summary, the effectiveness tests showed that all failures could be detected by the IM-FCL effectively, with exception of the erroneous activation of the pitch angle protection (ATHPRT). It has to be investigated if the $\dot{\gamma}$ Controllability Check (15) can detect this failure, when pitch-down demands of above 50 % of maximum side stick deflection are applied or if a different concept is required.

The tests also showed that several IMFs are redundant, e.g. Sideslip Angle and Lateral Load Factor Hands-free Check. Redundant IMFs are dispensable for a revised IM-FCL. The Overspeed Protection Check, Roll Rate and Load Factor Sign Check, Bank Angle Protection Check, and Aileron Command Sign Check IMFs did not significantly contribute to IM-FCL effectiveness. They can be removed from a future IM-FCL.

To maintain effectiveness a future IM-FCL should consist of command comparison IMFs (22 to 24), the Trim Drift Check (21), Bank Angle Hands-free Check (7), controllability checks (14 and 15), and limit checks (1 to 5). The latter are often redundant and detect a failure significantly later then other IMFs. However, they act as a monitor of last resort and should not be removed before a better IMF is available. It has to be investigated if protection function checks can supplement the IM-FCL to increase effectiveness in the corners of the flight envelope.

4.2 Robustness Test Results

To evaluate the robustness of the investigated IMFs, acceptable values of PFA are defined based on the probabilities of occurrence of the test conditions. One design goal is to maintain highest rates of availability. It is assumed that state-of-the-art FCS have a probability of loss of NM FCL of $10^{-7}\ 1/fh$. This is the requirement for a good IMF (green). Furthermore, it is assumed that a switch to the direct mode FCL that is announced to the pilots is classified as major. Therefore, false alarms with a probability of occurrence of less than $10^{-5}\ 1/fh$ are considered acceptable (yellow).

The robustness tests are split into four groups, considering their probability of occurrence, see Table 9. The values of Table 9 are a reference for assessing robustness. It is important to note, that the PFA highly depends on the defined robustness tests. Therefore, the PFA and the probability of the test condition have to be combined. For example, the test cases of the group normal operation conditions occur at every flight. Therefore, the PFA must be 0.

Table 9: Robustness tests groups, probabilities of occurrence and threshold for acceptable and good PFA.

Group	Prob. of occurrence	PFA (accept.)	PFA (good)
Normal operation	$1/fh$	0	0
SAE gust	$10^{-3}\ 1/fh$	$10^{-2}\ 1/fh$	$10^{-4}\ 1/fh$
HG manoeuvre	$1/27.000fh$	$\frac{1}{3.7}\ 1/fh$	$\frac{10^{-2}}{3.7}\ 1/fh$
CS-25 gust	$1/70.000fh$	$\frac{1}{1.43}\ 1/fh$	$\frac{10^{-2}}{1.43}\ 1/fh$

Table 10 shows the PFA of the investigated IMFs for the different robustness test groups. The Overspeed, Pitch Angle and Bank Angle Limit Checks (1, 3 and 5), the Bank Angle Hands-free Check (7), Roll Rate Sign Check (11), and the Overspeed and Bank Angle Protection Checks (17 and 19) are robust, as they do not trigger a false alarm at any of the investigated robustness tests.

On the other hand, the Pitch Rate Sign Check (12) and the Angle of Attack Protection Check (16) are the only IMFs that trigger false alarms during normal operations. They require additional development to improve robustness. However, considering their low contribution to the effectiveness of the IM-FCL, the extra effort is of no worth.

The Angle of Attack Limit Check (4), the Load Factor Sign Check (13), and Aileron Command Sign Check (20) triggered false alarms at SAE gust test conditions. Both sign check IMFs do not significantly contribute to IM-FCL effectiveness and could be removed from a revised IM-FCL. IMF 4 triggered false alarms during landing approach in strong turbulence (30 kt mean wind). Its thresholds and design should be tweaked to further improve robustness.

Table 10: PFA of investigated IMFs.

IMF	Normal operation	SAE gust	H. G. Man.	CS-25 gust
1	**0.0%**	**0.0%**	**0.0%**	**0.0%**
2	**0.0%**	**0.0%**	**1.4%**	**0.0%**
3	**0.0%**	**0.0%**	**0.0%**	**0.0%**
4	**0.0%**	**0.4%**	**5.9%**	**21.6%**
5	**0.0%**	**0.0%**	**0.0%**	**0.0%**
6	**0.0%**	**0.0%**	**0.0%**	**22.0%**
7	**0.0%**	**0.0%**	**0.0%**	**0.0%**
8	**0.0%**	**0.0%**	**0.0%**	**22.0%**
9	**0.0%**	**0.0%**	**0.0%**	**14.8%**
10	**0.0%**	**0.0%**	**0.0%**	**12.7%**
11	**0.0%**	**0.0%**	**0.0%**	**0.0%**
12	**15.5%**	**10.8%**	**24.1%**	**12.3%**
13	**0.0%**	**0.2%**	**0.2%**	**0.4%**
14	**0.0%**	**0.0%**	**0.2%**	**1.3%**
15	**0.0%**	**0.0%**	**16.2%**	**0.0%**
16	**1.4%**	**1.1%**	**1.4%**	**7.6%**
17	**0.0%**	**0.0%**	**0.0%**	**0.0%**
18	**0.0%**	**0.0%**	**0.7%**	**1.3%**
19	**0.0%**	**0.0%**	**0.0%**	**0.0%**
20	**0.0%**	**0.6%**	**0.0%**	**0.8%**
21	**0.0%**	**0.0%**	**0.2%**	**0.0%**
22	**0.0%**	**0.0%**	**5.4%**	**3.4%**
23	**0.0%**	**0.0%**	**0.0%**	**7.6%**
24	**0.0%**	**0.0%**	**0.0%**	**16.9%**

The rest of IMFs triggered some false alarms during high gain manoeuvres and/or severe gust encounters (CS-25 gust). While increasing the thresholds of these IMFs can improve robustness, it will certainly reduce the effectiveness of the IM-FCL. An extra function that can detect severe gust encounters can be a solution.

If severe gust encounters cannot be detected with high accuracy and/or increasing the thresholds does not improve robustness, the IM-FCL would trigger false alarms with an unacceptable high probability. In this case, the specific IMFs cannot be used in the IM-FCL, as the availability of the NM FCL would significantly decrease due to the automatic switch between laws.

A warning to the pilot with the option to manually switch to a simpler law may be a different solution. Pilots would know whether a gust is encountered, or an excessive manoeuvre is commanded. Nevertheless, a warning message may speed up the pilot's reaction time when a failure has occurred, and it can increase his confidence in his intuitive judgment that something is wrong.

In summary, the robustness tests showed that the Overspeed, Pitch Angle and Bank Angle Limit Checks, the Bank Angle Hands-free Check, Roll Rate Sign Check, and the Overspeed and Bank Angle Protection Checks are robust. The Pitch Rate Sign Check and the Angle of Attack Protection Check are the only IMFs that trigger false alarms during normal operations. They require additional development to improve robustness. Also, the rest of IMFs, triggered some false alarms during high gain manoeuvre or CS-25 conditions. Its thresholds and design should be tweaked to further improve robustness. An extra function that can detect severe gust encounters can improve the robustness against these conditions.

5 Conclusion and Outlook

This paper shows that the concepts for Independent Monitoring Functions (IMF), as described in [8], is applicable to a different aircraft and that the combination of 24 IMF to an Independent Monitor of Flight Control Laws (IM-FCL) can effectively detect all investigated pseudo failures. One exception is the erroneous activation of the pitch angle protection (ATHPRT). It has to be investigated if the $\dot{\gamma}$ Controllability Check can be improved or if a different IMF is required.

Command runaway like failures are best detected by the comparator concept. Whereas, failures that reduce the manoeuvrability of the aircraft, e.g. XICHLD or AHISPD, are best detected by the controllability check IMFs. Failures that occur at the corners of the flight envelope (FAOA and FHISPD) could only be detected by the limit check IMFs and the Pitch Angle and Angle of Attack Protection IMF.

The Overspeed Protection Check, Roll Rate and Load Factor Sign Check, Bank Angle Protection Check, and Aileron Command Sign Check IMFs do not significantly contribute to the effectiveness of the IM-FCL. An IM-FCL without these functions would remain effective - with reduced complexity.

A simpler but effective IM-FCL should consist of command comparison IMFs, the Trim Drift Check, Bank Angle Hands-free Check, controllability check IMFs, and limit check IMFs. The latter are often redundant and detect a failure significantly later then other IMFs. However, they act as a monitor of last resort and should not be removed before a better IMF is available. It has to be investigated if protection function checks can supplement the IM-FCL to increase effectiveness in the corners of the flight envelope.

The results showed that most IMFs are robust under the investigated tests. The Overspeed, Pitch Angle and Bank Angle Limit Checks, the Bank Angle Hands-free Check, Roll Rate Sign Check, and the Overspeed and Bank Angle Protection Checks, did not trigger false alarms. Whereas the Pitch Rate Sign Check and the Angle of Attack Protection Check are the only IMFs that trigger false alarms during normal operations. This needs improvement.

The rest of IMFs triggered some false alarms during high gain manoeuvres and/or severe gust encounters (CS-25 gust). Increasing the thresholds of these IMFs can improve robustness, but it will certainly reduce the effectiveness of the IM-FCL. A function that can detect severe gust encounters is a better solution. If the robustness cannot be improved, the IM-FCL would trigger false alarms with an

unacceptable probability of $1.43 \cdot 10^{-5}\ 1/fh$ or more. In this case the corresponding IMFs should not be used.

Demonstrating robustness is a challenging task that requires further investigation. The PFA is highly dependent on the defined robustness tests. Therefore, probabilities for each investigated robustness test conditions need to be defined, to calculate the acceptable PFA threshold. Also, automatic switching to a simpler flight control law as a system reaction to IM-FCL alarms requires further investigations. For uncrewed airplanes, it is the only option. However, for piloted aircraft, it may unfavourably decrease the availability of NM FCL.

Acknowledgments

The work presented in this paper was funded by the European Union Aviation Safety Agency as part of the Horizon Europe Programme: Flight Control Laws and Air Data Monitors. (EASA.2021.HVP.28) approved by the European Commission. The authors gratefully acknowledge the support.

References

[1] P. Traverse. Airbus Electrical Flight Controls: A Family of Fault-Tolerant Systems. In *Digital Avionics Handbook.* C. R. Spritzer, U. Ferrel and T. Ferrel. 3rd edition. CRC Press, 2015.

[2] Y. C. Yeh. Triple-triple redundant 777 primary flight computer. In *Proceedings of the 1996 IEEE Aerospace Applications Conference,* Aspen, USA, February 1996.

[3] W. Torres-Pomales. Software Fault Tolerance: A Tutorial. NASA Technical Memorandum TM-2000-210616, NASA, Langley Research Center, Hampton, VI, USA, 2000.

[4] Nancy G. Leveson. *Engineering a Safer World: System Thinking Applied to Safety*. MIT Press, 2011.

[5] European Union Aviation Safety Agency (EASA). Means of Compliance with the Special Condition VTOL. MOC SC-VTOL Issue 2, 2021.

[6] European Union Aviation Safety Agency (EASA). Generic Certification Review Item: Consideration of Common Mode Failures and Errors in Flight Control Functions. Generic CRI D-XXX. Unpublished.

[7] European Union Aviation Safety Agency (EASA). Horizon Europe Project: Flight Control Laws and Air Data Monitors. EASA.2021.HVP.28. Online. Accessed 16.05.2023. https://etendering.ted.europa.eu/cft/cft-display.html?cftId=9764.

[8] D. Hübener, R. Luckner and G. Weber. Concepts for Independent Monitoring of Flight Control Laws. In *Proceedings of the 10th EUCASS – 9th CEAS Aerospace Europe Conference*, Lausanne, Switzerland, July 2023.

[9] D. Hübener, A. Arnold, R. Luckner and G. Weber. Validation Activities for Flight Control Law Monitors. In *Deutscher Luft- und Raumfahrtkongress 2023*, Stuttgart, Deutschland, September 2023.

[10] P. Traverse, I. Lacaze and J. Souyris. Airbus Fly-By-Wire: A Total Approach to Dependability. In *Building the Information Society. IFIP International Federation for Information Processing*, vol 156. R. Jacquart. Springer, 2004.

[11] P.G. Hamel. *In-Flight Simulators and Fly-by-Wire/Light Demonstrators*. Springer Verlag, 2017.

[12] European Union Aviation Safety Agency (EASA). Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes. Standard, CS-25 Amendment 26, December 2020.

[13] SAE Aerospace. Aerospace - Flight Control Systems - Design, Installation and Test of Piloted Military Aircraft, General Specification. Standard, AS94900, July 2007.

Annex

Table 11: Investigated Independent Monitoring Functions.

IMF Name	IMF number
Overspeed Limit Check	1
Load Factor Limit Check	2
Pitch Angle Limit Check	3
Angle of Attack Limit Check	4
Bank Angle Limit Check	5
Roll Rate Hands-free Check	6
Bank Angle Hands-free Check	7
Load Factor Hands-free Check	8
Side Slip Angle Hands-free Check	9
Lateral Load Factor Hands-free Check	10
Roll Rate Sign Check	11
Pitch Rate Sign Check	12
Load Factor Sign Check	13
Roll Rate Controllability Check	14
Flight Path Controllability Check	15
Angle of Attack Protection Check	16
Overspeed Protection Check	17
Pitch Angle Protection Check	18
Bank Angle Protection Check	19
Aileron Command Sign Check	20
Trim Drift Check	21
Elevator Command Comparison	22
Aileron Command Comparison	23
Rudder Command Comparison	24