VALIDATION ACTIVITIES FOR FLIGHT CONTROL LAW MONITORS

D. Hübener, A. Arnold, R. Luckner
Technische Universität Berlin, Institut für Luft und Raumfahrttechnik, 10587 BERLIN, Germany

G. Weber, Liebherr-Aerospace Lindenberg GmbH, 88161 LINDENBERG, Germany

Abstract

Electronic flight control systems are safety-critical and complex systems requiring highest levels of integrity and availability. This is why the development process for the embedded flight control laws has to ensure rigorous validation and verification. However, the complete absence of development errors cannot be guaranteed. Usually, there is one requirement set from which flight control laws software is developed. Accordingly, undetected errors in the flight control law requirements represent a potential single point of failure. Means to mitigate the effects of such errors are addressed by a current project on the investigation of flight control law monitors that the European Union Aviation Safety Agency has launched in 2022. One possible approach is to develop independent flight control law monitoring functions. This paper proposes potential *Independent Monitoring Functions* and validates their feasibility using a simulation environment with a flight mechanical model and flight control laws for manual flight of a commercial aircraft.

ACRONYMS

DM	Direct Mode
EASA	European Union Aviation Safety Agency
FCL	Flight Control Laws
FCS	Flight Control Systems
HF	hands-free
IM-FCL	Independent Monitor for FCL
IMFs	Independent Monitoring Functions
NM	Normal Mode
TP	Trim Point

1 INTRODUCTION

Electronic flight control systems are safety-critical and complex systems requiring 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 are implemented in dissimilar computing lanes and the outputs of the lanes are compared to detect faults. References [1],[2],[3] describe flight control 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 control and monitor lane approach assures fail-passive behaviour if the lanes disagree.

However, nearly all serious 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]. Therefore, the FCL development 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 "*[f]ull 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 [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.

The primary objective for such an independent monitor for FCL (IM-FCL) is to mitigate the effects of common mode development errors. The IM-FCL should detect a failure before it becomes hazardous, but it must not cause false alarms, and it must be functionally independent from the FCL that it monitors. That means, new functions and new requirements have to be defined. 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.

Two monitoring concepts have been developed and are subject of the validation activities described here. The objective is to assess the feasibility of those concepts. The first concept compares the output of the nominal FCL mode to the output of a simplified FCL to detect failures. The second concept relates the flight state to the pilot commands and determines whether the FCL output is acceptable for continued safe flight - but not necessarily correct.

As with any system monitor, there are two basic criteria for monitor validation. The first criterion is monitoring effectiveness: does the monitor detect the effects of FCL development errors before they lead to critical conditions? The second one is monitoring robustness within the full operational flight envelope: is the monitor robust against false alarms in failure-free situations?

The monitor validation uses a simulation environment, consisting of the flight mechanical model of a regional jet and its state-of-the-art flight control laws for manual flight. Means for failure insertion have been developed to stimulate FCL failures. The effectiveness and robustness of the FCL monitors have been evaluated for different flight

doi: 10.25967/610300

phases, flight manoeuvres, flight conditions (including wind) and failure conditions.

This paper summarizes the investigated concepts for IM-FCL that are described in [8]. The validation method is explained, including a short description of the flight simulation environment, the test conditions, and the test cases. Selected validation test results are discussed. The paper concludes with a summary and outlook on future validation activities.

2 CONCEPTS FOR MONITORING FUNCTIONS

Reference [8] describes principles and concepts for independent monitoring of FCL. Multiple Independent Monitoring Functions (IMFs) form an IM-FCL. 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*[1].

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, and works on the FCL level. Therefore, it can directly allocate a detected failure to the FCL. In addition, the detection occurs potentially earlier than with monitors that are working on aircraft level, as the latter only can react upon aircraft response [8].

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. The Plausibility Check can monitor on aircraft or FCL level. Monitoring on aircraft level allows a direct assessment of the criticality of the failure and it inherently provides functional independence between the monitor and the FCL [8]. Possible Plausibility Checks can be categorized into three groups:

- *Limit Checks*,
- *Behaviour Checks, or*
- *Command Checks* (not used in this paper).

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. *Command Checks* comprise checks for acceptability of the FCL commands to the control surfaces that are monitored under consideration of the pilot demand. Refer to [8] for a detailed description of these concepts.

2.1 Comparator

Three Independent Monitoring Functions (IMFs) based on the Comparator concept are proposed. The NM FCL computes the commands that control the aircraft, the IMFs use for comparison the DM FCL that simultaneously compute control surface deflections. NM FCL commands depend on the dynamic pressure to compensate changing effectiveness of the aerodynamic control surfaces by gain scheduling. The DM has fixed gains for most of the flight envelope and relies on the pilot to adapt his commands to the flight conditions. To achieve comparable command signals, the DM FCL commands are scaled by using the dynamic pressure ratio $\bar{q}_{ref}/\bar{q}$. For example, the elevator command $\eta_{cmd,DM}$ is scaled by:

$$\eta_{cmd,DM\ sc} = \frac{\bar{q}_{ref}}{\bar{q}}\eta_{cmd,DM} \tag{1}$$

The IMFs compare the NM and the DM elevator, aileron and rudder commands respectively. The requirement and rationale listed in TAB 1 is an example for an elevator comparator check. Requirements for the aileron and rudder command comparison are defined in a similar way.

TAB 1: Requirement for elevator command comparison function.

Requirement	The IMF shall trip, if the elevator command of normal law η_{cmd} and direct law $\eta_{cmd,DM\ SC}$ significantly differ, AND if the aircraft is operated in normal flight envelope.
Rationale	The NM and DM FCL outputs should be similar when considering the effects of dynamic pressure and flight envelope protections are inactive.
Type	Comparator

The condition "aircraft is operated in normal flight envelope" refers to the protected values of the pitch angle, airspeed, angle of attack, bank angle and load factor. This condition is checked to ensure that the NM protection functions are not active, as their activation would drastically change the NM commands and a comparison with DM commands would not be viable.

TAB 2 list the thresholds of the comparator IMFs at the three investigated trim points defined in TAB 9.

TAB 2: Thresholds for comparator IMFs.

Limit TP	$\Delta\eta_{cmd}$	$\Delta\xi_{cmd}$	$\Delta\zeta_{cmd}$
09	1.1°	8.0°	1.4°
23	1.2°	9.0°	3.1°
01	9.0°	9.0°	6.0°

2.2 Plausibility Check

Twelve monitoring functions for the Plausibility Check concept are proposed, consisting of:

- limit checks (5), and
- behaviour checks:
  - hands-free checks (3), and
  - sign checks (4) (not evaluated in this paper).

Hands-free checks monitor the aircraft reaction during hands-free operation only, that is when no pilot inputs are

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

applied. Sign checks monitor the aircraft reaction during pilot inputs. Examples for the requirements of the proposed monitoring functions are listed in TAB 3 to TAB 5.

TAB 3 gives an example for a limit check of the bank angle. Requirements for airspeed, angle of attack, pitch angle and load factor limit checks are defined in the same way, using the values of TAB 6.

TAB 3: Requirement for maximum bank angle limit check.

Requirement	IM shall trip if the absolute aircraft bank angle |Φ| exceeds 70°.
Rationale	A high bank angle can lead to stalls and/or spatial disorientation.
Type	Limit Check

Requirements for the bank angle and load factor hands-free checks are defined analogously using the values listed in TAB 7.

TAB 4 gives an example of a hands-free check. This function checks that the roll rate does not exceed a predefined limit without pilot inputs. Requirements for the bank angle and load factor hands-free checks are defined analogously using the values listed in TAB 7.

TAB 4: Requirement for roll rate hands-free check.

Requirement	The IMF shall trip if the absolute value of the roll rate $\|p\|$ exceeds 6 °/s, AND if no pilot roll input, AND if the aircraft is operated in normal flight envelope.
Rationale	Aircraft roll rate should not exceed limit if pilot does not demand a change in bank angle. Threshold value: $\|p\| = 6$ °/s
Type	Behaviour Check

TAB 5 gives an example of a sign check for the roll rate. Requirements for pitch rate, yaw rate and load factor sign checks are defined analogously. Sign check IMFs are not further considered in this paper.

TAB 6 and TAB 7 list thresholds for hazardous failure conditions at the investigated trim points. With the exception for the angle of sideslip β, the threshold values originate from functional hazard assessments on aircraft and on system level. The threshold values for β are based on engineering judgement. The threshold values defined in TAB 7 are valid for hands-free operation only, i.e. no pilot inputs.

TAB 5: Requirement for roll rate sign check.

Requirement	The IMF shall trip, if roll rate p is positive/(negative), AND if the pilot gives left/(right) wing down input, AND if the aircraft is operated in normal flight envelope.
Rationale	Aircraft reaction should correspond to pilot demand, if no protection function reduces pilot authority.
Type	Behaviour Check

TAB 6: Thresholds for hazardous failure conditions.

Limit TP	$\boldsymbol{\Theta}$	$\boldsymbol{\alpha}$	$\boldsymbol{n_z}$	$\boldsymbol{V_{CAS}}$ **or** $\boldsymbol{Ma}$
09	$\Theta < -15°$ $30° < \Theta$	$9.1° < \alpha$	$n_z < -1.0\,\mathrm{g}$ $2.55\,\mathrm{g} < n_z$	$332\,\mathrm{kt} < V_{CAS}$
23		$10.0° < \alpha$		$0.845 < Ma$
01		$14.9° < \alpha$		$181\,\mathrm{kt} < V_{CAS}$

TAB 7: Thresholds for hazardous failure conditions during hands-free operation.

Limit TP	$\boldsymbol{n_z}$	$\boldsymbol{p}$	$\boldsymbol{\beta}$	$\boldsymbol{\Phi}$
09	$n_z < 0.4\,\mathrm{g}$ $1.6\,\mathrm{g} < n_z$	$\|p\| > 6\frac{°}{s}$	$5° < \beta$	$35° < \|\Phi\|$
23			$10° < \beta$	
01			$16° < \beta$	

3 VALIDATION OF MONITORING FUNCTIONS

The validation activities for the selected FCL monitors that are implemented according to the described concepts are now summarized. TAB 8 lists the investigated monitoring functions. Three monitoring functions based on the Comparator concept and eight monitoring functions based on the Plausibility Check concept are investigated and compared for both monitoring effectiveness and robustness. The objective of the validation is to demonstrate the feasibility of the monitoring functions.

TAB 8: List of proposed monitoring functions.

Concept	Function	Monitored Parameter
Comparison	Command Comparison	η_{cmd}, ξ_{cmd} and ζ_{cmd}
Plausibility	Limit Checks	V_{CAS}, n_z, Θ, α and Φ
	Hands-free Checks	p, Φ, and n_z

3.1 Simulation Environment

The validation activities use a simulation environment consisting of an aircraft flight mechanical model of a representative regional jet aircraft, and a set of Normal Mode and Direct Mode (back-up) FCL for manual flight. Both the aircraft model and the FCL originate from a commercial development project. The aircraft model has been validated by flight tests, and the FCL used in the simulations are developed and qualified with Design Assurance Level A according to [9]. Thus, the simulation environment provides a highly representative platform for the FCL monitor validation activities.

3.2 Validation Approach

The objective of the validation tests is to assess the feasibility of the proposed IMFs. As the comparison and hands-free IMFs are limited to operations within the normal flight envelope, i.e. when no NM protection functions are active, only test cases in the normal operational flight envelope will be investigated. However, failures or disturbances may lead to a departure from the normal operational flight envelope.

Three trim points (TP) are selected. They represent three flight phases: cruise (TP09), loitering (TP23), and approach (TP01). TP09 is a cruise condition at high altitudes and high airspeeds. TP23 is a flight condition between descent phases at medium altitude and low speed in clean configuration. TP01 represents a low-speed approach, near the angle of attack protection limit, with landing gear down and flaps fully deflected. TAB 9 lists the key parameters of the investigated trim points.

TAB 9: Investigated trim points (TP).

TP	Altitude	Flaps	Landing Gear	V_{CAS}	$\theta = \alpha$
09	30,568 ft	0°	*up*	303 kt	1.45°
23	13,122 ft	0°	*up*	230 kt	3.42°
01	666 ft	*full*	*down*	135 kt	7.64°

The effects of FCL development errors on the FCL output can vary significantly. However, first simulations showed that the initial effect is often similar to a command runaway. For example, an erroneous activation of the high angle of attack protection can lead to an unwanted and significant pitch command.

The validation activities focus on runaway-like failures that lead to hazardous or catastrophic failure conditions. The failure is injected by replacing the FCL output with a runaway signal. The investigated test cases represent failures that occur during hands-free operation of the aircraft, when no pilot inputs are applied. Sign check monitoring functions require a pilot input to check for a plausible direction of aircraft response. Those functions are not considered here.

3.3 Test Cases

The test cases used for the IMF validation are grouped into two categories, *effectiveness* test cases and *robustness* test cases. Effectiveness test cases check for the timely detection of unsafe conditions as described in [8]. Robustness test cases check for spurious detections under failure-free operating conditions including operational manoeuvres and external disturbances. The IMF is robust under these conditions, if it does not trigger. In all investigated test cases the manoeuvre, disturbance or failure starts at $t = 2.0\ s$.

3.3.1 Effectiveness Test Cases

The objective of the IM-FCL is to detect failures that lead to conditions classified as hazardous or catastrophic [8]. To assess the effectiveness of the monitors, test cases of runaway-like failures with limited amplitude and rate have been defined, so that the aircraft just exceeds at least one of the defined thresholds of TAB 6 and/or TAB 7. This allows an assessment of the sensitivity of the IMFs. Runaways with smaller amplitudes are assumed to have no hazardous consequences. They do not need to be detected, while runaways with larger amplitudes will always be hazardous or catastrophic. Two types of runaways are investigated: fast runaways and slow runaways. Thirty-three failures on all control surface commands and directions are defined, see TAB 10.

TAB 10: Runaway test cases for effectiveness tests.

Test Case	Description
FAIL100 to FAIL104	Elevator command runaway. Maximum rate and limited amplitude.
FAIL105 to FAIL108	Slow elevator command runaway. Limited rate and limited amplitude.
FAIL200 to FAIL202	Asymmetric aileron command runaway (left wing down). Maximum rate and limited amplitude.
FAIL203 to FAIL205	Slow asymmetric aileron command runaway (left wing down). Limited rate and amplitude.
FAIL210 and FAIL211	Symmetric negative aileron runaway (lift dump).
FAIL300 to FAIL302	Positive rudder command runaway (nose to the left). Maximum rate and limited amplitude.
FAIL303 and FAIL304	Slow positive rudder command runaway (nose to the left). Limited rate and amplitude.
FAIL400 and FAIL401	Trimmable horizontal stabilizer runaway. Maximum rate and limited amplitude.
FAIL402	Slow trimmable horizontal stabilizer runaway (pitch down). Limited rate and limited amplitude.
FAIL500 to FAIL502	Asymmetric spoiler command runaway (left wing down). Maximum rate and limited amplitude
FAIL503 to FAIL505	Slow asymmetric spoiler command runaway (left wing down). Limited rate and amplitude.
FAIL510 and FAIL511	Symmetric flight spoiler runaway (lift dump).

3.3.2 Robustness Test Cases

To assess the robustness of the monitors, five test cases consisting of operational manoeuvres and test inputs, as well as five test cases of severe wind conditions are defined. TAB 11 summarizes the simulated robustness test cases.

TAB 11: Robustness test cases (with gust gradient H).

Test Case	Description
MON100	Level flight. Right roll to 20° bank angle and hold for 40 s. Left roll to level flight.
MON200	Level flight. Initiate climb with $1000\ \mathrm{ft/min}$.
MON300	Level flight. Initiate descent with $-1000\ \mathrm{ft/min}$.
MON004	Sinusoidal pitch inputs.
MON005	Sinusoidal roll inputs.
DIS10	Discrete crosswind gust from the left according to CS 25.341 [10] with $H = 107\ \mathrm{m}$.
DIS20 / DIS30	Discrete down-/upwind gust according to CS 25.341 [10] with $H = 107\ \mathrm{m}$.
DIS40 / DIS50	Discrete tail-/headwind gust according to CS 25.341 [10] with $H = 107\ \mathrm{m}$.

The investigated discrete 1-cosine gusts are defined in [10]. They have a probability of occurrence of

$$P = \frac{1}{70000}\ \mathrm{fh} \approx 1.43 \cdot 10^{-5}\ \mathrm{fh}. \qquad (2)$$

The design gust velocities in true airspeed are for cruise flight $17.5\ m/s$ (TP09), for loitering $15.24\ m/s$ (TP23) and for approach $14.54\ m/s$ (TP01).

3.4 Test Results

3.4.1 Effectiveness Test Results

The effectiveness of an IMF is assessed by the failure detection time, which is the time from failure occurrence until its detection. To better understand the evaluation test results and the determination of failure detection times, two test cases, are described in detail – one for the longitudinal and one for the lateral motion. For all other tests, only the failure detection times are discussed.

FIG 3-1 and FIG 3-2 show the time histories for test case FAIL100, an elevator command runaway with maximum rate, at the cruise trim point TP09. Only the longitudinal motion is excited. The pitch angle Θ, angle of attack α and pitch rate q are depicted in the diagram at the top. The normal load factor n_z and the critical n_z (hands-free) limit, defined in TAB 7, are shown in the second plot. The third plot depicts the calibrated airspeed V_{CAS} and Mach number Ma. Two IMFs flags are displayed in the bottom diagram: the comparison of elevator commands (η_{comp}), and the n_z hands-free check ($n_{z,HF}$).

The fast elevator command runaway leads to a pitch down, a reduction of the normal load factor to $n_z = 0.4\ \mathrm{g}$, and an increase of the calibrated airspeed (acceleration). The comparison function for the elevator command detects the failure that occurs at $t = 2.0\ \mathrm{s}$, almost immediately (after $0.02\ \mathrm{s}$). That is $2.21\ \mathrm{s}$ before the critical n_z (hands-free) limit is exceeded, see triggering of the n_z hands-free IMF ($n_{z,HF}$). This confirms that monitoring at FCL level has the benefit of early failure detections. An early failure detection allows the FCS to react or at least warn the pilot. This increases the chances of avoiding or quickly recovering from potentially hazardous or catastrophic failure conditions.

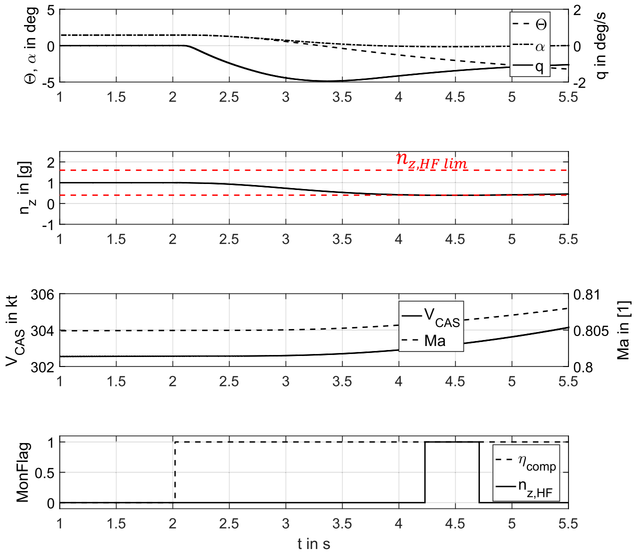

FIG 3-1: Reaction of the aircraft and monitoring flags for test case FAIL100 at TP09.

FIG 3-2 shows the elevator commands of the NM and DM FCL. The top diagram shows the time histories of the elevator commands of the NM and DM FCL. The difference between elevator commands calculated according to equation (1) and the comparison threshold is depicted in the middle plot. The monitoring flag of the comparison function for the elevator command is shown in the bottom time history.

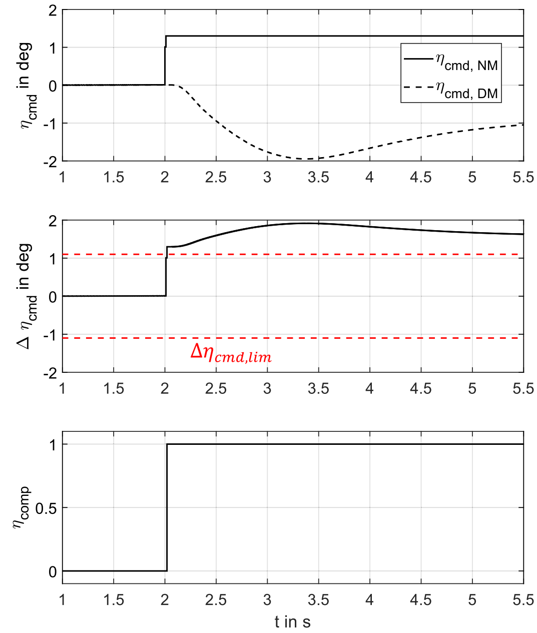

FIG 3-2: Comparison of elevator FCL commands for test case FAIL100 at TP09.

The $1.3°$ runaway of the NM elevator command at $t = 2.0\ \mathrm{s}$ with maximum rate of $100\ °/\mathrm{s}$ is similar to a step input. It leads to an immediate exceedance of the comparison threshold for the elevator command. The pitch damper of the DM FCL computes elevator commands opposite to the erroneous NM elevator command, further increasing the difference between elevator commands. The computed difference of the FCL elevator commands $\Delta\eta_{cmd}$ clearly exceeds the monitoring threshold. This may be an indication, that the comparison function threshold for the elevator commands is set too low.

FIG 3-3 shows the reaction of the aircraft and four monitoring functions to a slow rudder command runaway (FAIL303) at the cruise trim point. The top diagram shows the time histories of the bank angle (Φ) and roll rate (p) with their critical limits defined in TAB 7. The second plot shows the angle of sideslip (β), its critical limit and the yaw rate (r). The NM FCL right and left aileron commands (ξ_{RHcmd} and ξ_{LHcmd}) and their saturation limit are depicted in the third diagram. The bottom plot shows monitoring flags of the lateral motion.

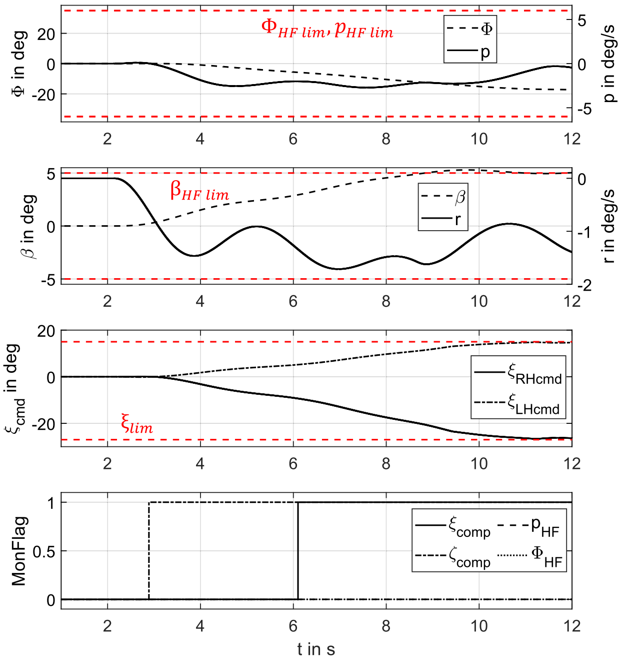

FIG 3-3: Reaction of aircraft and monitoring flags for test case FAIL303 at TP09.

The rudder command runaway increases the angle of sideslip and induces a left roll that the NM FCL try to counteract with corresponding aileron commands. The NM FCL aileron commands stop the left roll and the critical limit for the roll rate (p) is never exceeded. However, the limit of the angle of sideslip is exceeded after $6.0\ s$ (at $t \approx 8.0\ s$). The first IMF that detects the failure is the comparison of the rudder command function ζ_{comp} after $0.9\ s$ (at $t =\ 2.9\ s$). Next, the comparison function for the aileron command ξ_{comp} triggers after $4.1\ s$, as the NM FCL tries to counteract the faulty rudder command. For this test case, none of the IMFs that are based on plausibility checks detects the failure, as the limits of the bank angle and roll rate are not exceeded. The saturation of the aileron commands shows that this failure reduces the remaining roll authority and therefore, it is safety critical. A monitor for the angle of sideslip, which was not designed, could be an option.

TAB 12 lists the detection times of the elevator command comparison function η_{comp} and the load factor hands-free function $n_{z,HF}$ for effectiveness test cases affecting the longitudinal motion. The first detection is highlighted in **bold**. Both IMFs detect all failures. In some test cases, absolute limits of n_z, Θ or α were exceeded, triggering the corresponding limit check. For clarity, those detection times are not listed in TAB 12, as the detection always occurs after the elevator command comparison and n_z hands-free function have detected failures.

TAB 12: Failure detection times of effectiveness test cases of the longitudinal motion.

TP	TC ID	$n_{z,HF}$	η_{comp}
09	**FAIL100**	2.23 s	**0.02 s**
	FAIL101	5.56 s	**1.11 s**
	FAIL105	5.09 s	**1.52 s**
	FAIL106	2.86 s	**0.92 s**
	FAIL210	1.58 s	**0.7 s**
	FAIL211	4.02 s	**1.47 s**
	FAIL400	2.40 s	**1.62 s**
	FAIL401	2.91 s	**1.61 s**
	FAIL402	21.57 s	**4.39 s**
	FAIL510	1.65 s	**0.79 s**
	FAIL511	6.95 s	**2.99 s**
23	**FAIL102**	2.22 s	**0.03 s**
	FAIL103	2.00 s	**0.03 s**
	FAIL107	4.04 s	**1.55 s**
	FAIL108	4.25 s	**1.67 s**
	FAIL401	5.24 s	**0.25 s**
01	**FAIL104**	3.55 s	**0.1 s**

The elevator command comparison function is always the first of the two IMFs to detect a failure, triggering 0.86 s (FAIL510) to 17.18 s (FAIL402) before the $n_{z,HF}$ IMF detects a failure. It also detects failures that do not affect the elevator command directly. Those failures are runaways of the trimmable horizontal stabilizer (FAIL400 to FAIL402) as well as symmetric failures of ailerons (FAIL210, FAIL211), and spoilers (FAIL510 and FAIL511). In these cases, the NM FCL tries to compensate the effects of the erroneous control surface command with elevator commands. Then, η_{comp} IMF triggers as the difference between NM and DM commands exceeds the limit. While in those cases, the elevator command is not erroneous, the difference between the NM and DM FCL elevator commands is an indication for an abnormal situation caused by FCL failure. It should be mentioned that the aileron command comparison function ξ_{comp} also detected the symmetric aileron command runaways (FAIL210 and FAIL211). The load factor hands-free function $n_{z,HF}$ is effective as it detected all failures in the pitch axis, however, significantly later than η_{comp}.

TAB 13 lists the detection times of four monitoring functions for effectiveness test cases affecting the lateral motion. The comparison function for the aileron command ξ_{comp} detects all aileron failures (FAIL200 – FAIL207) as well as all other failures in the investigated test cases affecting the lateral motion. The rudder command comparison only detects failures that directly affect the rudder command (FAIL300 to FAIL304). A dedicated monitoring of rudder commands may not be required, as the aileron comparison IMF can detect these failures.

The roll rate hands-free function p_{HF} detects a failure in all test cases except (FAIL303, FAIL304, FAIL504, FAIL202 and FAIL205). In those test cases, the critical limit of the roll rate $|p|_{lim} = 6\,°/s$ is not exceeded, see FIG 3-3. The bank angle hands-free function Φ_{HF} only detects failures in some test cases and always after the p_{HF} or ξ_{comp} monitoring functions have triggered.

TAB 13: Failure detection times of effectiveness test cases of the lateral motion.

TP	TC ID	p_{HF}	Φ_{HF}	ξ_{comp}	ζ_{comp}
09	**FAIL200**	1.78 s	-	**0.52 s**	-
	FAIL203	6.56 s	9.09 s	**5.06 s**	-
	FAIL300	1.43 s	-	1.86 s	**0.02 s**
	FAIL303	-	-	4.1 s	**0.89 s**
	FAIL500	**0.55 s**	-	1.31 s	-
	FAIL503	13.75 s	14.49 s	**5.1 s**	-
23	**FAIL201**	1.44 s	-	**0.5 s**	-
	FAIL204	7.42 s	9.28 s	**5.96 s**	-
	FAIL301	1.73 s	-	1.48 s	**0.04 s**
	FAIL304	-	-	5.32 s	**1.94 s**
	FAIL501	0.85 s	-	**0.69 s**	-
	FAIL504	-	28.91 s	**7.59 s**	-
01	**FAIL202**	-	-	**0.09 s**	-
	FAIL205	-	-	**7.27 s**	-
	FAIL302	3.18 s	-	1.45 s	**0.06 s**
	FAIL304	14.00 s	-	**3.71 s**	4.65 s
	FAIL502	0.75 s		**0.41 s**	-
	FAIL505	9.67 s	11.28 s	**2.78 s**	-

The effectiveness test cases have shown that the comparison function for the elevator command and aileron command have good effectiveness and early detection capabilities. They can detect failures of all control surface commands. Therefore, a dedicated monitor may be not necessarily required for all control surface commands. In most test cases, the comparison IMFs detect a failure before critical limits are exceeded.

The hands-free IMF p_{HF} detected most of the investigated failures, showing good effectiveness. The IMF p_{HF} could not detect slow rudder runaways (FAIL303 and FAIL304) as well as some aileron and spoiler runaways (FAIL202, FAIL205 and FAIL504). Although IMF Φ_{HF} detected the spoiler runaway, the detection time of nearly 28 s seems to be too large.

Dedicated IMFs, for each safety-critical parameter listed in TAB 6 and TAB 7 are required to improve the effectiveness of the plausibility IMFs.

3.4.2 Robustness Test Results

The robustness tests investigate the IMF during manoeuvres and in external disturbances, i.e. discrete gusts. All tests occur in failure-free conditions, where the IMF must not trigger. The objective is to analyse whether the IMF cause false detections.

FIG 3-4 shows the reaction of the aircraft and monitoring functions during a $40\ s$ steady state, slip-free turn with 20° bank angle (MON100) at the cruise trim point. For this test case no unintended monitor triggering happened.

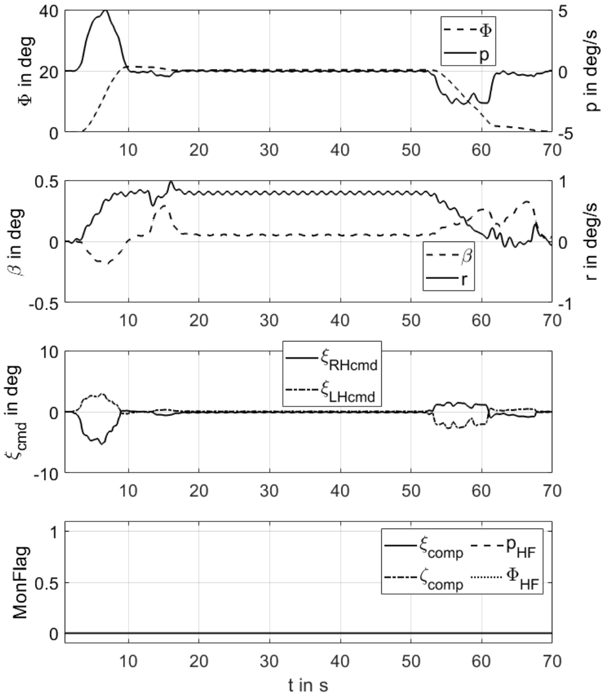

FIG 3-4: Reaction of aircraft and monitoring flags for test case MON100 at TP09.

Some false detections occurred during encounters of extremely strong discrete (design) gusts. FIG 3-5 and FIG 3-6 show examples. The aircraft reaction to an upwind gust (DIS30) during cruise in FIG 3-5 shows that this gust leads to a severe pitch reaction (top diagram) and to a short exceedance of the n_z limit defined in TAB 7 at $t = 2.9\ s$ (second diagram). Speed variations are small (third diagram). Although the gust causes a safety-critical aircraft reaction as the n_z limit is clearly exceeded, the FCL is failure free.

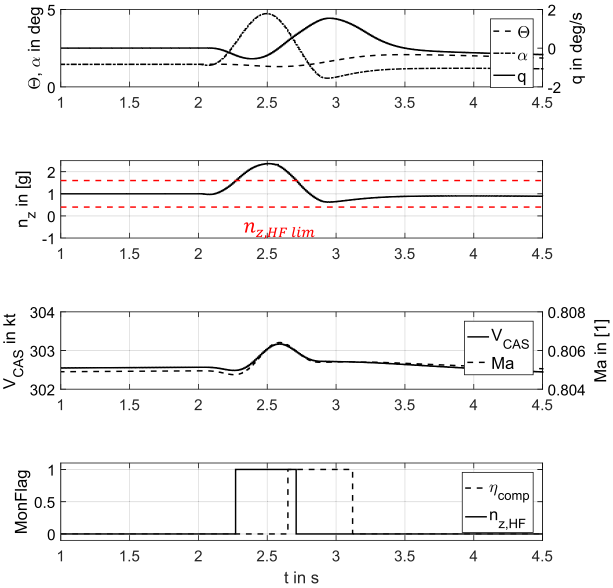

FIG 3-5: Reaction of aircraft and monitoring flags for test case DIS30 at TP09.

The test shows that external disturbances can have a significant impact on the aircraft reaction. The difference between NM and DM FCL commands becomes large as the NM FCL compensate the disturbance, whereas the reaction of the DM with its pitch damper is significantly smaller. These two aspects have to be considered when designing IMFs. The false detections of the $n_{\mathrm{z,HF}}$ and the η_{comp} functions (bottom diagram) can be avoided, for example by adding a confirmation time and/or by increasing the monitoring thresholds. However, the additional confirmation time would affect the early detection capabilities of the monitoring functions. A better solution to avoid false detections would be a function that detects external disturbances and provides this information to the IMF.

FIG 3-6 shows the reaction of the aircraft to the design crosswind gust from the left (DIS10) at the approach trim point TP01. The p_{HF} IMF (hands-free) triggers as the roll rate reaches its critical limit $|p|_{lim} = 6\,°/\mathrm{s}$ at $t = 4.7\ \mathrm{s}$ (top diagram). Even before, at $t = 2.88\ \mathrm{s}$, the aileron command comparison ξ_{comp} falsely triggers, as the crosswind gust drives the NM aileron command into saturation. In this case, increasing the comparison threshold does not make sense. A detection of the crosswind disturbance can be a better solution.

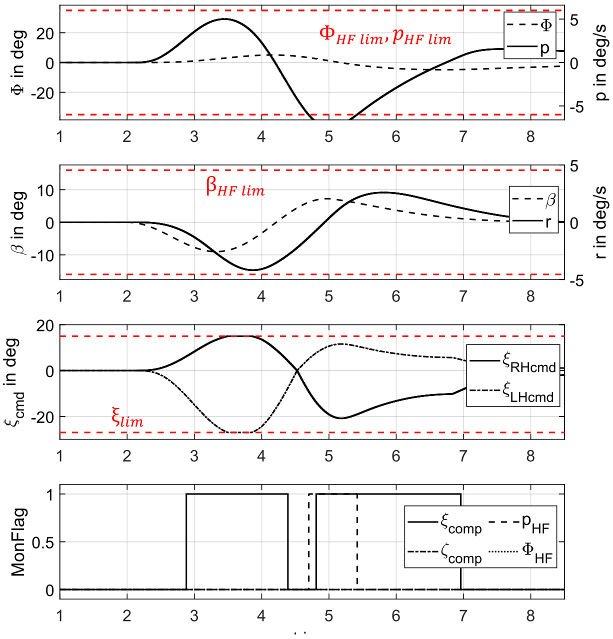

FIG 3-6: Reaction of aircraft and monitoring flags for test case DIS10 at TP01.

TAB 14 lists the false detection times of the robustness test cases at the cruise trim point TP09. IMFs that are not listed did not trigger false alarms. Therefore, those functions are robust for the investigated test cases.

Disturbances affecting the longitudinal motion (DIS20 to DIS50) caused false detections of the n_z hands-free IMF and the elevator command comparison function η_{comp}. An exception is the discrete tailwind gust (DIS40). The aileron command comparison function ξ_{comp} triggered during an upwind gust (DIS30) as the activation of the load alleviation function leads to an exceedance of the comparator thresholds. The roll rate hands-free function p_{HF} triggered during the discrete crosswind gust (DIS10) and the airspeed limit function was triggered - for a short period only - during a discrete headwind gust (DIS50) as the overspeed limit was exceeded. This transient false detection can also be avoided by a function that detects the gust disturbance.

TAB 14: Failed robustness test cases at TP09.

TC ID	$n_{z,HF}$	p_{HF}	η_{comp}	ξ_{comp}	V_{lim}
DIS10	-	**2.54 s**	-	-	-
DIS20	**2.29 s**	-	3.4 s	-	-
DIS30	**2.27 s**	-	2.65 s	2.46 s	-
DIS40	-	-	-	-	-
DIS50	3.72 s	-	3.14 s	-	**2.49 s**

TAB 15 and TAB 16 list the false detection times of the failed robustness test cases at the loitering and approach trim points. At the loitering trim point TP23, only the n_z hands-free function and the aileron command comparison function trigger false alarms. Again, the activation of the load alleviation function is the reason that the aileron command comparison function triggers. Allowing large comparison thresholds for symmetrical aileron commands or deactivating the comparison when the load alleviation is active can improve the robustness of the aileron command comparison IMF.

TAB 15: Failed robustness test cases at TP23.

TC ID	$n_{z,HF}$	ξ_{comp}
DIS10	-	-
DIS20	**2.54 s**	-
DIS30	**2.48 s**	2.78 s
DIS40	-	-
DIS50	-	-

At the approach trim point TP01, the roll rate hands-free function and aileron command comparison function trigger a false alarm during the crosswind gust and the elevator command comparison function triggers during the upwind gust.

TAB 16: Failed robustness test cases at TP01.

TC ID	p_{HF}	η_{comp}	ξ_{comp}
DIS10	4.7 s	-	**2.88 s**
DIS20	-	-	-
DIS30	-	**5.81 s**	-
DIS40	-	-	-
DIS50	-	-	-

In summary, the robustness tests showed no false detections during typical operational manoeuvres or test inputs (MON004 to MON300). More aggressive manoeuvres should be investigated next. Disturbances pose a challenge to the IMF. The tailwind gust is the only (disturbance) test case without false detections. The tests show, that the robustness of the IMFs need improvement. The IMF ξ_{comp} had false detections at all trim points. The IMF η_{comp} falsely triggered in strong up-, down- and headwind gusts. The implemented IMFs did not have a confirmation time. Introducing and tuning of confirmation times could lower the false detection cases. Additionally, tweaking the thresholds of the limit IMFs could contribute. However, significant improvement is only expected if information on the disturbances is provided to the IMFs. Additionally, the ξ_{comp} IMF needs information on the commands of the load alleviation function.

4 CONCLUSIONS

Two concepts for Independent Monitoring of FCL (IM-FCL) from Ref. [8] were investigated to validate the feasibility of the IM-FCL approach: (i) the Comparator Concept that verifies the correct functionality of the FCL by comparing the outputs of two available flight control laws that are functionally independent; (ii) the Plausibility Concept that uses pilot commands to predict aircraft behaviour. Both concepts verify that the FCL outputs are plausible and, in a range, where they do not cause hazardous flight conditions rather than correct. The Comparator monitors on FCL level, the Plausibility Check works on aircraft and FCL level. Checks on FCL level are preferable as they can detect safety-critical failures earlier and before they lead to a hazardous flight condition.

The feasibility of the FCL monitoring concepts regarding their effectiveness (correct and timely failure detection) and robustness (no false detections) was investigated in a representative flight simulation environment with failure-injection capabilities. Independent Monitor functions comprising comparators, hands-free and limit checks were assessed during different flight phases, flight manoeuvres, flight conditions (including gusts) with and without FCL failures. In conclusion, independent monitoring of FCL seems to be feasible. However, significant effort is still required to ultimately prove the efficiency and robustness of an Independent Monitor.

The flight simulation results show that the three Comparator IMFs η_{comp}, ξ_{comp} and ζ_{comp} are effective. Since the elevator and aileron command comparison functions also detect failures of other control surface commands, it can be considered whether this capability can be used to make dedicated monitoring of certain control surface commands unnecessary, e.g. rudder commands. While this capability could reduce the number of required IMFs, it has to be investigated how this aspect influences fault detection and isolation capabilities that may be necessary in a future system.

The elevator command comparison function η_{comp} always detects failures of symmetric control surface commands before the hands-free IMF $n_{z,HF}$, showing a good monitoring effectiveness at all three trim points. In most cases of asymmetric failures, the aileron command comparison function ξ_{comp} detects failures of roll control surfaces earlier than the hands-free IMF p_{HF}. Exceptions are one slow rudder command runaway (TP09/FAIL300) and one asymmetric spoiler command failure (TP09/FAIL500). The rudder command comparison IMF ζ_{comp} detects nearly all rudder runaways first. The only exception is case TP01/FAIL304 where the IMF ξ_{comp} triggers first. This indicates that the detection thresholds should be better balanced for low airspeed (low dynamic pressure).

The hands-free IMF $n_{z,HF}$ detects all symmetric failures. IMF p_{HF} detects most of the investigated asymmetric failures. It did not detect two aileron runaways at low airspeed (TP01/FAIL202 and 205), one asymmetric spoiler failure (TP23/FAIL504) and two slow rudder runaways (TP09/FAIL303 and TP23/FAIL304), for which other IMFs are certainly better suited. To improve the effectiveness of the Plausibility Check IMFs, dedicated monitoring functions for each safety critical parameter listed in TAB 6 and TAB 7 should be considered.

In terms of overall robustness against false alarms, the Comparator IMFs and the Plausibility Check IMFs perform excellent during standard manoeuvres (no false detections). More aggressive manoeuvres should be investigated next. Extreme disturbances, like design gusts, pose a challenge to the IMFs since both concepts give false alarms in such conditions. Introducing and tuning confirmation times and tweaking the thresholds of the IMFs can improve the robustness. However, at low airspeeds, where Normal Law FCL compensate severe disturbances with large control surface deflections up to the stop, deflection thresholds would become excessive - and too large for sensible monitoring.

The robustness and effectiveness of the aileron command comparison IMF ξ_{comp}, can be further increased, if the activation status of the n_z load alleviation function is provided to the IMF. However, significant improvement in robustness is only expected if information on the disturbances is provided to the IMFs. Means to distinguish between a reaction caused by FCL commands and a reaction that is caused by external disturbances are currently investigated.

The next phase of the monitor validation will investigate effectiveness and robustness at more aggressive manoeuvres and further test conditions (variation of mass and centre of gravity, closer to and in the protections, and other failure conditions e.g., erroneous gain). More plausibility IMFs, including sign and command checks, which were not addressed here, will be designed and investigated. The efficiency of plausibility and comparator IMFs will be compared and increased by providing more information to the IMF, especially on disturbances and on other active flight control functions like load alleviation.

ACKNOWLEDGEMENTS

The work presented in this paper was funded by the Federal Ministry for Economic Affairs and Climate Action (BMWK) as part of its Federal Aviation Research Programme (LUFO VI-1) on the basis of a decision by the German Bundestag within the scope of the joint research project MODULAR (grant number 20Y1910A) and TU Berlin’s partner project MODULAR-TUB (grant number 20Y1910C). The authors gratefully acknowledge the support.

5 REFERENCES

[1] Traverse, P., Lacaze, I., Souyris, J. 2006. Airbus Fly-by-Wire: A Process Toward Total Dependability. In *Proceedings of the 25th International Congress of the Aeronautical Sciences.*

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

[3] Torres-Pomales, W. 2000. Software Fault Tolerance: A Tutorial. NASA Technical Memorandum TM-2000-210616.

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

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

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

[7] EASA. 2021. 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] Hübener, D., Luckner, R., Weber, G. 2023. Concepts for Independent Monitoring of Flight Control Laws. In *Proceedings of the 10TH EUCASS – 9TH CEAS Aerospace Europe Conference 2023.*

[9] SAE Aerospace. 2010. Aerospace Recommended Practice: Guidelines for Development of Civil Aircraft and Systems. SAE ARP4754A. Society of Automotive Engineers

[10] EASA. 2020. Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes. CS-25 Amendment 26. European Union Aviation Safety Agency