Technical Note

TN-FMRA-23-007-v01

Title: List of Proposed Flight Control Law Monitors

Project: EASA.2021.HVP.28 “Horizon Europe Project: Flight Control Laws and Air Data Monitors” Lot 1

Work Package: Task 3

Document Ref.: TN-FMRA-23-007

Version: v01

Authors: Dominik Hübener;Bryan Laabs;Guido Weber

Date: 31.08.2023

Summary: This Technical Note defines the proposed monitors for flight control laws. It includes a preliminary discussion on monitoring levels, monitoring concepts and the approach for monitor design, a list of requirements for the proposed monitors and a summary. This Technical Note represents the deliverable D-3.1 of the “Horizon Europe Project: Flight Control Laws and Air Data Monitors” Lot 1 (EASA.2021.HVP.28)” project.

	Prepared	**Reviewed**	**Approved**	**Released**
Name	D. Hübener B. Laabs G. Weber	A. Arnold D. Chernetsov	F. Silvestre P. Schädler	P. Schädler
Date	31.08.2023	31.08.2023	31.08.2023	31.08.2023
Signature	electronic signature	electronic signature	electronic signature	electronic signature

Revision History

Version	Date	Author	Description of Changes
01	31.08.2023	D. Hübener B. Laabs G. Weber	Initial version

Distribution List

Name	Organisation	Copies
G. Weber	Liebherr Aerospace	electronic
P. Schaedler	Liebherr Aerospace	electronic
T. Socher	Liebherr Aerospace	electronic
S. Ziehm	Liebherr Aerospace	electronic
T. Lanz	Liebherr Aerospace	electronic
S. Koebe	Liebherr Aerospace	electronic
E. Dejene	Liebherr Aerospace	electronic
H. Mendes	EASA	electronic
M. Weiler	EASA	electronic
F. Silvestre	TU Berlin	electronic
B. Boche	TU Berlin	electronic
D. Hübener	TU Berlin	electronic
A. Arnold	TU Berlin	electronic

Contents

Abbreviations **4**
Definitions **4**
Symbols **5**
Bibliography **5**
1 Introduction **7**
1.1 Motivation 7
1.2 Report Structure 7
2 Preliminary Discussion **8**
2.1 Assumptions and Design Objectives 8
2.2 Monitoring Levels 9
2.3 Concepts 10
2.3.1 Comparator 10
2.3.2 Plausibility Checks 11
2.4 Approach for Monitor Detail Definition 12
3 List of Proposed Monitors **14**
3.1 Plausibility Checks on Aircraft Level 14
3.1.1 Limit Checks 15
3.1.2 Handsfree Checks 17
3.1.3 Sign Checks 19
3.1.4 Controllability Checks 20
3.2 Plausibility Checks on FCL Level 20
3.2.1 Protection Function Checks 20
3.2.2 Sign Check 22
3.2.3 Pitch Trim Drift Checks 22
3.3 Comparator Checks 23
3.3.1 Elevator Checks 23
3.3.2 Aileron Checks 23
3.3.3 Rudder Checks 23
3.4 Additional Monitor Functions 23
3.4.1 Total Energy Monitor 24
3.4.2 Real-Time Pilot-Induced Oscillation Detection 24
4 Summary **26**

Abbreviations

A/C	Aircraft
AEO	All Engines Operating
AoA	Angle of Attack
ATD	Advanced Technologies Demonstrator
DL	Direct Law
FbW	Fly by Wire
FCS	Flight Control System
FCL	Flight Control Laws
FCL SW	Flight Control Law Software
FHA	Functional Hazard Assessment
FMRA	Fachgebiet Flugmechanik, Flugregelung und Aeroelastizität, TU Berlin
FSEnv	Flight Simulation Environment
IM	Independent Monitor
NL	Normal Law
PIO	Pilot-Induced Oscillations
THS	Trimmable Horizontal Stabilizer
SW	Software

Definitions

Term	Definition/Meaning
Common mode error	An error which affects a number of elements otherwise considered to be independent (ARP4754A § 2.2).
Dependability	An ability to deliver service that can justifiably be trusted in the user environment. It is the ability to avoid service failures that are more frequent and more severe than it is acceptable. Dependability consists of the attributes: availability, reliability, safety, confidentiality, integrity and maintainability [14].
Development error	A mistake in requirements determination, design or implementation. (ED79A/ARP 4754A, §2.2)
Error	With respect to software, a mistake in requirements, design, or code (DO-178C Annex B).
	An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation (AMC 25.1309 paragraph 5.j).
Failure	A loss of function or a malfunction of a system or a part thereof. (ARP4761)
Failure condition	The effect on the aircraft and its occupants both direct and consequential caused or contributed to by one or more failures, considering relevant adverse operational and environmental conditions. A failure condition is classified according to the severity of its effects as defined in advisory material issued by the certification authority (DO-178C Annex B).
Failure mode	The way in which the failure of a system or item occurs (ARP4754A § 2.2).

Term	Definition/Meaning
Fault	A manifestation of an error in an item or system that may lead to a failure (ARP4754A § 2.2).

Symbols

α	Angle of attack
β	Sideslip angle
θ	Pitch angle
Φ	Roll angle
γ	Flight path angle
η	Elevator angle
ξ	Aileron angle
ζ	Rudder angle
n_z	Normal load factor
n_y	Lateral load factor
p	Roll rate
q	Pitch rate
r	Yaw rate
H	Altitude
m	Mass
V_{CAS}	Calibrated airspeed
V_{MO}	Maximum operation speed
V_{NE}	Never exceed speed
V_S	Stall speed
Ma	Mach number
RR_ζ	Rudder pedal input
SS	Sidestick input

Bibliography

[1] “Monitoring of Flight Control Laws,” EASA, https://www.easa.europa.eu/en/research-projects/monitoring-flight-control-laws (accessed Feb. 14th 2023).

[2] *Reliance on Development Assurance Alone When Performing a Complex and Full-Time Critical Function*, Position Paper CAST 24 of Certification Authorities Software Team, 2006.

[3] RTCA: *RTCA DO-178C - Software Considerations in Airborne Systems and Equipment Certification*, 2010.

[4] Torres-Pomales, W.: *Software Fault Tolerance: A Tutorial*, NASA/TM-2000-210616, National Aeronautics and Space Administration, 2000.

[5] Lee, P. A. and Anderson, T.: *Fault Tolerance Principles and Practice,* 2nd edition Springer Verlag, Wien, 1990

[6] Laabs, B.: *User Manual for the VFW614-ATD Flight Simulation Environment*. Technical Note TN-FMRA-23-001, version 1, TU Berlin, Berlin, 2023.

[7] Laabs, B.: *Validation of the VFW614-ATD Flight Simulation Environment*. Technical Note TN-FMRA-23-002, version 1, TU Berlin, Berlin, 2023.
[8] Chernetsov, D., Luckner, R., Laabs, B.: *VFW614-ATD Flight Simulation Environment*. Technical Note TN-FMRA-23-003, version 1, TU Berlin, Berlin, 2023.
[9] Traverse, P., Lacaze, I. and Souyris, J..: *Airbus Fly-by-Wire: A Process Towards Total Dependability*, 25th International Congress of the Aeronautical Sciences, 2006.
[10] Favre, C.: *Fly-by-Wire for commercial aircraft: the Airbus experience,* International Journal of Control*, Vol. 59, No. 1, pp. 139-157,* 1994.
[11] Brockhaus, R., Alles W., and Luckner R.: *Flugregelung*, 3. Auflage, Springer Verlag, Heidelberg, 2011.
[12] *VFW614 Flight Handbook*, Rev. 7 of 01.07.1978.
[13] Heintsch, T., Holzhausen, T.*: Flight Control Laws for the Primary Flight Module in the PFCU*. Technical Note TN-EF-037/96, issue 6, DaimlerChrysler Aerospace Airbus, Hamburg, 2000.
[14] B. Kalpana and S. Uma: *Literature Review on Dependable and Secure Computing*, International Journal of Research in Computer Applications and Robotics, vol. 2, no. 8, pp. 19–25, 2014.
[15] EASA: *CS 25 Amendment 26 – Certification Specification and Acceptable Means of Compliance for Large Aeroplanes*, 2020.
[16] *Engineering data from a representative commercial Liebherr Aerospace GmbH development project,* 2009*.*
[17] Mitchell, D. G., Arencibia, A. J., Munoz, S.: *Real-Time Detection of Pilot-Induced Oscillations*, AIAA Atmospheric Flight Mechanics Conference and Exhibit, Providence, Rhode Island, 2004

1 Introduction

The Horizon Europe Project: “Flight Control Laws and Air Data Monitors” Lot 1 (EASA.2021.HVP.28) investigates the viability of an *Independent Monitor* for Flight Control Law Software (FCL SW) to detect failures caused by FCL errors [1]. This Technical Note represents the delivery D-3.1 for Task 3 of the project.

In Task 3, potential monitors shall be proposed and delivered as a list, additionally their details shall be specified. The monitors can check the aircraft reaction or the FCL output. The advantages of the monitoring levels are discussed, and two concepts for monitoring functions are described. The proposed monitors and their details are captured in a list of requirements that is used to design the proposed monitors and to derive test sequences for monitor validation.

TU Berlin uses the FCL SW that was developed in the VFW614-ATD technology project, in which new technologies for an Electronic Flight Control System were developed and demonstrated. The FCL SW and the desktop flight simulation *FSEnv* of the VFW614-ATD flight dynamics are representative for a modern Fly-by-Wire (FbW) aircraft (A/C). This desktop flight simulation was prepared in Task 1 of the EASA.2021.HVP.28 project and extended by failure injection means. The documentation comprises a user manual [6], a programmer’s guide [8] and a validation report [7].

This document proposes a list of monitoring functions and specifies their details as requirements. The design objectives and approach for monitor detail definition are described. The advantages and disadvantages of each monitoring level are discussed. Monitors can work on aircraft level or FCL SW level. Additionally, a classification for FCL monitor based on failure detection measures is proposed.

1.1 Motivation

In typical flight control architectures, Flight Control Laws are developed based on a single set of requirements and implemented in dissimilar computing lanes. The outputs of the lanes are compared to detect implementation and hardware faults. The comparison of control and monitor lane outputs cannot detect faults that are caused by errors in the FCL requirements or errors in the FCL design. Development assurance is used to mitigate the risk of development errors. However, the certification authorities state in the position paper [2], that “development assurance alone is not necessarily sufficient to establish an acceptable level of safety” and that additional mitigation techniques i.e., fault tolerance, should be applied. An Independent Monitor for the FCL could be a means to achieve fault tolerance against FCL development errors.

1.2 Report Structure

The report is structured as follows:

- Section 2 preliminarily discusses potential monitoring levels and monitor classes based on detection measure, and describes the approach for monitoring detail definition,
- Section 3 contains the details of the proposed monitoring functions,
- Section 4 summarizes the report.

2 Preliminary Discussion

This section lists important assumptions and answers the following two questions that need to be discussed before specific monitoring functions are proposed in Section 3.

1. What monitoring level is suitable to achieve the design objectives of the independent monitor?
2. What detection measures can be applied to detect FCS malfunctions?

2.1 Assumptions and Design Objectives

The following assumptions are made:

- Only failure conditions are considered that may have hazardous or catastrophic consequences.
- Only the Normal Law (NL) of VFW614-ATD FCL SW is investigated for possible failure conditions. The Direct Law (DL) of the FCL SW is assumed to be free of errors due to its simplicity. The DL can be activated as a backup law if the *Independent Monitor* identifies a failure.
- The pilot reaction time is 1 s. It is assumed that the pilot reaction time and the time until the backup FCL is activated is enough to prevent/recover hazardous or catastrophic flight conditions.[1]
- The NL is representative for an Electronic Flight Control System of a modern CS-25 category aircraft. So, in general, the *Independent Monitor* that shall be developed is applicable to any aircraft of this category.
- Loss of sensor signals integrity and its consequences on flight control are not considered. It is assumed that a separate sensor monitoring function exists and signal integrity is given.
- Severe structural damage (e.g., caused by mid-air collisions, surface debris that are dislodged by jet blast, tire explosion in the belly, etc.) and its consequences on flight control are not considered. If the result of structural damage is insufficient control power, it is impossible to control the aircraft any longer. If control power is still sufficient but if the FCL are not robust enough to provide adequate handling qualities, control would still be possible, but the pilot workload may be excessive. So, either a more robust design or an FCL reconfiguration (adaptation) would be required.

The objective of the Independent Monitor is to increase the safety of the FCS while maintaining highest rates of availability. To increase the safety the independent monitor

- shall detect failures, i.e. erroneous function (malfunction), of the FCS caused by FCL development errors, and
- shall be functionally independent from the normal law FCL. This avoids common requirement errors and therefore ensures system integrity.

To maintain availability of the FCS the independent monitor

- shall only detect failure conditions which are potentially classified as hazardous or catastrophic,
- shall be robust under foreseeable operational conditions, and
- shall have a significantly lower level of complexity than normal law FCL.

A simple monitor avoids new development errors that could lead to spurious detection of failures and reduce the availability of the FCS.

[1] This assumption needs to be validated when designing monitoring thresholds. However, the appropriate response to a failure detection is not within the scope of this project and will not be investigated.

2.2 Monitoring Levels

Figure 2-1 shows an example of a sequence of events in which a software error leads to a failure condition at aircraft level. The independent monitor can work on three levels: local (FCL SW-level), intermediate (FCS-level) or global (aircraft-level). Ideally, the independent monitor can detect faults on the FCL-level, to avoid system failures and eventually hazardous failure conditions. However, the design objective is to detect failures that lead to hazardous or catastrophic failure conditions (effect at aircraft level).

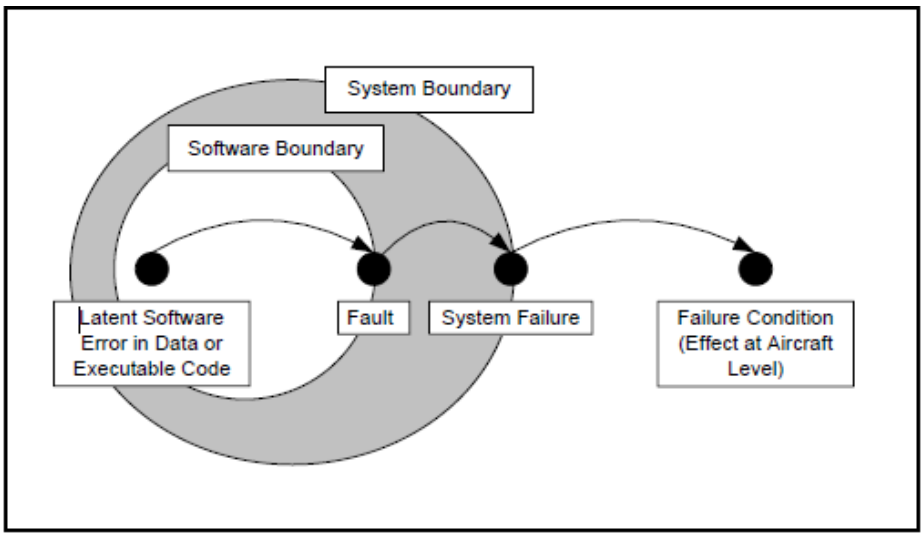

Figure 2-1: Sequence of Events, Software Error Leading to Failure Condition (source: [3]).

The block diagram in Figure 2-2 shows a simplified pilot aircraft control loop and three possible options for FCL monitors (green, blue and orange). The FCL monitoring function can use different information sources e.g., pilot control inputs, FCL outputs, control surface position or aircraft reaction.

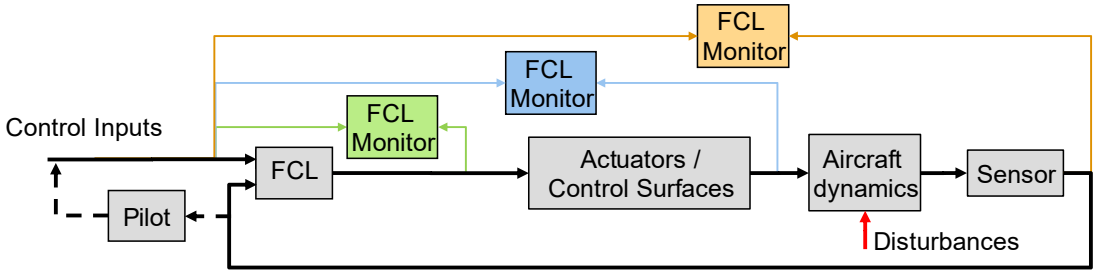

Figure 2-2: Options for an Independent Monitor.

The **green FCL monitor** compares the pilot demand and the FCL output and checks for plausibility. The source for possible faults can be directly delimited to the FCL software. However, it is challenging to achieve functional independence between the monitor and the FCL. The monitor works on the same level as the normal law FCL to be monitored. The effect of an erroneous FCL output has to be extrapolated to the aircraft reaction to determine adequate monitor thresholds.

The **blue FCL monitor** compares the control inputs to the control surface deflections and checks for acceptability. An advantage of this option – compared to the green FCL monitor - is that it checks the actual control surface position that controls the aircraft. However, it is challenging that possible actuator failures and dynamics shall not result in spurious monitor tripping. If the actuator is assumed to be failure free, the control surface position and the FCL output are very similar. Therefore, the same challenges as the green monitor apply to the blue monitor. A monitoring on the intermediate level does not seem to offer any advantages.

The **orange FCL monitor** compares the pilot demand to the aircraft reaction. Monitoring of aircraft parameters allows a direct assessment of the criticality of potential failure conditions.

Achievement of functional independence seems to be feasible on this level. As aircraft response to external disturbances, such as wake vortex encounters or severe gusts, can also be significant, it is challenging to unambiguously distinguish between a potential FCS malfunction and external disturbances.

The independent monitor can monitor on a global level (aircraft) or on a local level (FCL output). Monitoring on an intermediate level does not offer significant advantages. Functional independence and a direct assessment of the criticality of the failure is feasible on the global monitoring level. The local level has the advantage of a direct allocation of the detected fault and a potentially earlier detection, which would give the pilot more time to react to a potentially hazardous failure condition. Therefore, a monitor similar to the orange FCL monitor is preferred. The FCL output may also be monitored for fault localisation and isolation and to detect faults before critical aircraft conditions are reached.

2.3 Concepts

Anderson and Lee have proposed a classification of fault detection measures that can be provided in a computer system [5]. Usually, the detection measures work on a local level (within the software or at its output [4]) and are therefore not suited for the independent monitor. However, two fault detection measures can be applied: *replication checks* and *reasonableness checks*.

Replication checks compare the results of redundant components or systems. A fault is detected when the outputs of the variants differ [4], [5]. This check works on FCL SW-level. Dissimilarity in the high-level requirements of the FCL function (functional independence) is necessary, to avoid common mode errors.

Reasonableness checks are based on a knowledge of the internal design and construction of a system. These checks verify whether the behaviour of the software is acceptable rather than correct, based on predictions on the anticipated system state [4], [5]. Predictions can be derived from aircraft and/or system requirements, but never from high-level requirements of the FCL. This way errors common to the monitor and the FCL can be avoided.

Independent FCL Monitors can be categorized by decision mechanism. A decision mechanism is a function that adjudicates, arbitrates, or otherwise decides on the acceptability of the results obtained by the FCL variants. Two basic concepts are proposed:

- Comparator, and
- Plausibility Check.

2.3.1 Comparator

Comparators are based on the idea of replication checks and work on a local level. As the functionality of the dissimilar alternative may significantly differ from normal law FCL, the outputs may significantly differ as well. A comparator that can tolerate this difference is required. Also, because of the dissimilarity in the high-level requirements of the FCL they may not generate the same output signals. So, it has to be considered that not all FCL outputs can be compared.

Functional dissimilar alternatives can be an existing backup law (e.g. direct law FCL), or a newly designed FCL. A newly developed alternative FCL entails a significant additional effort, increases complexity and the risk to implement new errors. Therefore, the development of a new FCL is not further considered here to mitigate the effects of FCL development errors.

All fly-by-wire aircraft have a backup law, that can be used as an alternative. Advantages are, that no extra resources are required for its development and that the backup law is functionally independent from the normal law FCL. So, it is worthwhile to investigate how the existing alternatives can be used for failure detection. However, operations near the flight envelope limits where mode transition occur, and protection functions are activated may be challenging.

Simulations of an exemplary CS-25 fly-by-wire aircraft have shown, that a comparison of the normal law FCL and the direct law FCL outputs is possible. In the investigated testcases the normal law and direct law FCL simultaneously compute their commands, but only the normal law FCL controls the aircraft. The monitoring thresholds can be reduced if the direct law FCL commands are adjusted to the dynamic pressure.

2.3.2 Plausibility Checks

The concept *Plausibility Check* verifies that the behaviour of the FCL software is acceptable and plausible rather than correct, based on predictions on the anticipated system state. Predictions can be derived from aircraft and/or system requirements. Alternatively, they can be derived from operations, e.g. like a pilot who knows how a FCS should behave. The plausibility check monitor can work on aircraft and FCL level.

Possible Plausibility Checks can be categorized into three groups:

- Limit Checks,
- Behaviour Checks, and
- Command Checks.

Limit Checks check for a violation of (hard) limits that the aircraft is not supposed to exceed. Exceedance of the limit is always a sufficient condition to detect failures. If one (or more) of the limits are exceeded, it is assumed that a failure is present. Those limits are derived from aircraft safety requirements, e.g. α_{max} to avoid stall, $n_{z,max}$ to avoid structural damage, etc. Limit Checks are simple and only compare one aircraft state parameter to its respective limit. Table 1 lists possible examples of limit checks.

Table 1: Examples of Limit Checks.

Limit	Failure when…
α_{max}	$\alpha > \alpha_{max}$
$V_{CAS,max}$	$V_{CAS} > V_{CAS,max}$
$n_{z,max}$	$n_z > n_{z,max}$

The Abnormal Attitude Monitor from AIRBUS aircraft comprises a set of limit checks, that monitor essential flight parameters (static thresholds for pitch attitude, bank angle, angle of attack, calibrated airspeed, and Mach number) [9], [10].

Behaviour Checks check the plausibility of the aircraft reaction under consideration of the pilot demand. They are never a sufficient condition to determine if the FCL is faulty. If undesired aircraft behaviour is detected, the FCL commands need to be checked to determine the cause of the failure. E.g., if the measured load factor is greater than one without the corresponding pilot commands, an undesired aircraft behaviour is detected. However, this could be caused by an external disturbance or other system failures (e.g., actuator runaway). Only if the FCL commands a pitch-up ($\Delta\eta_{cmd} < 0°$)[2] a failure of the FCS caused by a FCL error is probable. Table 2 gives examples of behaviour checks.

Table 2: Examples of Behaviour Checks.

Condition	Failure detected when…	Rationale
Pilot demands pitch-up AND no protection is active.	($n_z \leq 1$ OR $q \leq 0\,^{°}/_{s}$) AND no external disturbance	When pilot demands a pitch-up movement and no protection function is active, the aircraft should pitch up and build up a positive normal load factor.

[2] Note that the axis system defined in [11] is used.

Pilot demands right roll AND no protection is active.	$p \leq 0\,^{\circ}/_{s}$ AND no external disturbance	When pilot demands a right roll movement and no protection function is active, the aircraft should roll to the right $(p > 0\,^{\circ}/_{s})$.

Command Checks comprise checks for acceptability of the FCL commands to the control surfaces that are monitored under consideration of the pilot demand. Predictions on the FCL commands can be derived from aircraft and/or system requirements, but never from FCL requirements. Command Checks have to consider more than one aircraft state parameter to detect failures. Therefore, they are more complex than Limit Checks. Checks of this category can be a sufficient or a necessary condition to detect faults of the FCL. Table 3 gives examples for command checks.

Table 3: Examples of Command Checks.

Condition	Failure detected when….	Rationale
Aircraft at stall protection limit AND no pitch-up demand.	$\Delta\eta_{cmd} < 0°$	When aircraft is near the stall protection limit and pilot does not demand pitch up, the FCL should command a pitch down to decrease α.
Abnormal pitch-down detected (pilot demands pitch-up).	$\Delta\eta_{cmd} > 0°$	When pilot demands a pitch-up movement, but the aircraft does not react as expected because of a FCL pitch-down command. A failure has occurred.

2.4 Approach for Monitor Detail Definition

The development of monitor functions for flight control systems is based on the aircraft level and system level functional hazard assessment (FHA). On aircraft level, certain limits of flight parameters like accelerations, angular rates, or attitude angles are defined with respect to their severity level. These limit values are further broken down to the system level and documented in the system FHA. As a result, failure modes on system level like a control surface transient will have an allocated severity level corresponding to the aircraft reaction caused by the failure mode.

These values represent the performance requirements for system-level monitor functions and are used for implementation verification accordingly. Here, monitor performance has to be balanced versus monitor robustness against nuisance trips. For instance, a monitor threshold too far below the critical threshold or a too short confirmation time will provide good performance e.g., timely detection with a limited transient, but it may lead to unintended monitor trips during failure-free situations.

As stated above, for the FCL monitor only hazardous and catastrophic severity levels are considered. Figure 3 shows the boundaries within the flight envelope that are considered for the detailed validation of the *Independent Monitor*. The blue area indicates the normal (operational) flight envelope. The yellow area indicates the peripheral (permissive) flight envelope, where NL protection functions are active. The VFW614-ATD aircraft can only be operated in this area by pilot effort on the cockpit controls. The orange and red domains indicate critical flight states that are either prevented by protection functions or by the pilot. They should never be reached during fault-free NL operation. The orange domain indicates the monitor detection boundary until when the monitor shall trip to avoid catastrophic or hazardous consequences.

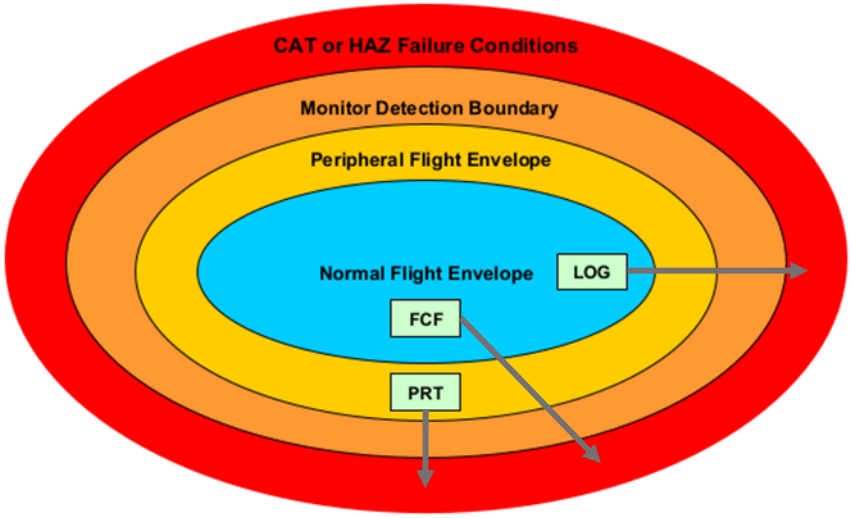

Figure 3: Distribution of Functional Classification over the Flight Envelope.

While some limits, e.g. normal to peripheral flight envelope, are predefined by the design of the FCL, others need to be investigated and defined. Especially the limits of the monitor detection boundary domain will have a great impact on the performance of the monitor. Also, on the ability of the FCS to recover from failures and the availability of the FCS. If the orange domain is set too wide, the availability of the FCS Normal Law is reduced but the ability to recover will probably be increased. However, too narrow limits can increase the availability of the FCS Normal Law but might result in unrecoverable failure conditions.

The limits should be defined based on engineering judgement and simulation results. A thorough validation is necessary to find the best compromise between availability and failure recovery ability. In this project, the validation will not be possible due to limited resources. However, changing the values will not have a significant impact on the monitor design.

For the following monitor specifications, the set of monitoring thresholds is derived from the VFW-614 flight handbook [12], the VFW-614 ATD FCL design, refer to [13], and upset limits defined for a representative, serial production regional jet aircraft, refer to [16].

The upcoming validation activities will use these parameter sets as an initial basis. The validation campaign will address both monitor effectiveness / performance and monitor robustness. As a result, monitor threshold values might require adaptations. Monitor confirmation times and reset or down-count times will also play an important role as a tuneable parameter in the course of the monitor validation phase.

3 List of Proposed Monitors

The objective of the Independent Monitor (IM) is to increase the safety of the FCS while maintaining highest rates of availability. The following design objectives are defined. The IM

- shall detect failures, i.e. erroneous function (malfunction), of the FCS caused by FCL development errors, and
- shall be functionally independent from the normal law FCL, and
- shall have a significantly lower level of complexity than normal law FCL, and
- shall only detect failure conditions which are classified as hazardous or catastrophic, and
- shall be robust under any foreseeable operational condition.

The requirements for the monitoring functions are defined for aircraft level (AL) and FCL SW level (SL), see Subsection 2.2. A total of 24 monitoring functions are proposed. **Table 4** summarizes the proposed monitoring functions.

Table 4: List of proposed monitoring functions.

Function	Parameter	Requirements
Limit Checks	V_{CAS}, n_z, θ, α and ϕ	AL-01 to AL-10
Handsfree Checks	p, ϕ, n_z, β and n_y	AL-11 to AL-16
Sign Checks	p, q, and n_z	AL-17 to AL-19
Controllability Checks	p and q	AL-20 to AL-21
Protection Function Checks	V_{CAS}, α, θ and ϕ	SL-01 to SL-06
Command Sign Check	ξ_{cmd}	SL-07
Pitch Trim Drift Check	THS command	SL-08
Command Comparison	η_{cmd}, ξ_{cmd} and ζ_{cmd}	SL-9 to SL-11

3.1 Plausibility Checks on Aircraft Level

The following threshold values are based on the design of the VFW614 aircraft. For other aircraft these values must be adapted and validated as described in section 2.4.

Table 5 Monitor thresholds depending on flap setting [13].

Configuration [1]	0	1	2	3	4
Flap deflection [°]	-6	1	5	14	35
V_{MO}/V_{FE} [kt]	255.0*	225.0*	220.0*	200.0*	165.0
Neutral elevator deflection η_0 [°]	1.47	1.66	1.80	2.04	3.38
α_{prot}** [°]	10.9	11.36	11.53	10.25	8.18
α_{max}** [°]	12.9	14.4	14.5	13.3	11.2

* V_{MO} reduced to 199 kt if landing gear extended [13].
** α_{prot} and α_{max} are dynamic limits [13]. Reduction of α_{prot} and α_{max} depending on airbrake deflection or Mach number is neglected for initial monitor development.

Table 6: Stall speed V_S in [kt] depending on mass and flap setting [13].

Configuration [1] / Mass [kg]	0	1	2	3	4
11818.0	87.0	77.0	73.0	70.0	66.0
14545.0	96.0	86.0	81.0	78.0	73.0
18182.0	107.0	96.0	91.0	88.0	82.0
20909.0	114.0	103.0	97.0	94.0	87.0

The term *Normal Flight Envelope* refers to the following range of values:

Pitch angle Θ:	$-15° \leq \Theta \leq 30°$
Equivalent airspeed V_{EAS}:	$1.23 \cdot V_s \leq V_{EAS} \leq V_{MO}$
Angle of attack α:	$\alpha \leq \alpha_{prot}$
Bank angle Φ:	$-33° \leq \Phi \leq 33°$
Load factor n_z:	$-1 \leq n_z \leq 2.5$ (configuration = 0), $0 \leq n_z \leq 2$ (configuration > 0)

3.1.1 Limit Checks

AL-01	IM shall trip if the aircraft pitch angle θ exceeds 32°.
Rationale:	High pitch angles can lead to stalls and/or spatial disorientation. Threshold value: $\theta_{max} = 30°$ [13] plus 2° margin.
Inputs	θ
Type	Limit Check

AL-02	IM shall trip if the aircraft pitch angle θ falls below -17°.
Rationale:	Low pitch angles can lead to overspeed conditions and high structural loads. Threshold value: $\theta_{min} = -15°$ [13] minus 2° margin.
Inputs	θ
Type	Limit Check

AL-03	IM shall trip if the aircraft high lift devices are retracted, AND calibrated airspeed V_{CAS} exceeds 295 kt below 21200 ft OR Mach number Ma exceeds 0.66 above 21200 ft.
Rationale:	Overspeed condition can cause structural damage. Threshold value: $V_{NE} = 290$ kt [12] plus 5 kt margin, $M_{NE} = 0.65$ [12] plus 0.01 margin.
Inputs	V_{CAS}, Ma, H and $Flap\ deflection$
Type	Limit Check

AL-04	IM shall trip if the aircraft high lift devices are extended, AND calibrated airspeed exceeds V_{FE} plus 30 kt.
Rationale:	Overspeed condition can cause structural damage. Threshold value: V_{FE} [12] plus 30 kt margin. V_{NE} not defined in [12].
Inputs	V_{CAS} and $Flap\ deflection$
Type	Limit Check

AL-05	IM shall trip if the absolute aircraft bank angle |Φ| exceeds 69°.
Rationale:	High bank angles can lead to stalls and/or spatial disorientation. Threshold value: $\|\Phi_{max}\| = 67°$ [13] plus 2° margin.
Inputs	ϕ
Type	Limit Check

AL-06	IM shall trip if the aircraft high lift devices are retracted, AND normal load factor n_z exceeds 2.55 g.
Rationale:	High normal load factors can cause structural damage. Threshold value: $n_{z,max} = 2.5$ g [13] plus 0.05 g margin.
Inputs	n_z and $Flap\ deflection$
Type	Limit Check

AL-07	IM shall trip if the aircraft high lift devices are retracted, AND normal load factor n_z falls below -1.05 g.
Rationale:	High normal load factors can cause structural damage. Threshold value: $n_{z,min} = -1.0$ g [13] minus 0.05 g margin.
Inputs	n_z and $Flap\ deflection$
Type	Limit Check

AL-08	IM shall trip if the aircraft high lift devices are extended, AND normal load factor n_z exceeds 2.05 g.
Rationale:	High normal load factors can cause structural damage. Threshold value: $n_{z,max} = 2.0$ g [13] plus 0.05 g margin.
Inputs	n_z and $Flap\ deflection$
Type	Limit Check

AL-09	IM shall trip if the aircraft high lift devices are extended, AND normal load factor n_z falls below -0.05 g.
Rationale:	High normal load factors can cause structural damage. Threshold value: $n_{z,min} = 0.0$ g [13] minus 0.05 g margin.
Inputs	n_z and $Flap\ deflection$
Type	Limit Check

AL-10	IM shall trip if the aircraft angle of attack exceeds $\propto_{max}$, OR V_{CAS} falls below $1.12 \cdot V_S$.
Rationale:	High angle of attack or low airspeed can lead to stalls. Threshold value: $\propto_{max}$ and V_S [13].
Inputs	α, V_{CAS}, m and $Flap\ deflection$
Type	Limit Check

3.1.2 Handsfree Checks

AL-11	IM shall trip if absolute roll rate $\lvert p \rvert$ exceeds 6 °/s AND no pilot roll input, AND aircraft 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: $\lvert p \rvert = 6$ °/s equals 50% pilot roll rate demand on the side stick [13] and the upset limit specified in [16].
Inputs	p and SS_ξ
Type	Behaviour Check

AL-12	IM shall trip if absolute bank angle $\lvert\Phi\rvert$ exceeds $35°$ AND no pilot roll input, AND the airspeed is lower than V_{MO}.
Rationale:	Aircraft roll angle should not exceed $33°$ without active pilot roll demand. Threshold value: $\lvert\Phi_{prot}\rvert = 33°$ [13] plus 2° margin.
Inputs	ϕ, SS_{ξ} and V_{MO}
Type	Behaviour Check

AL-13	IM shall trip if normal load factor n_z exceeds 1.6 g, AND no pilot pitch input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft normal load factor should not exceed limit if pilot does not demand a change of the flight path angle. Threshold value: $n_z = 1.6$ g equals 50% positive pilot load factor demand on the side stick [13] and the upset limit specified in [16].
Inputs	n_z and SS_{η}
Type	Behaviour Check

AL-14	IM shall trip if normal load factor n_z falls below 0.4 g, AND no pilot pitch input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft normal load factor should not exceed limit if pilot does not demand a change of the flight path angle. Threshold value: $n_z = 0.4$ g equals 50% negative pilot load factor demand on the side stick [13] and the upset limit specified in [16].
Inputs	n_z and SS_{η}
Type	Behaviour Check

AL-15	IM shall trip if absolute lateral load factor $\lvert n_y\rvert$ exceeds 0.2 g, AND no pilot yaw input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft lateral load factor should not exceed limit if pilot does not demand a change in yaw to avoid structural damage.
Inputs	n_y and RR_{ζ}
Type	Behaviour Check

AL-16	IM shall trip if absolute sideslip angle $\lvert\beta\rvert$ exceeds $5°$, AND no pilot yaw input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft sideslip angle should not exceed limit if pilot does not demand steady sideslip angle to avoid uncontrollable aircraft conditions.
Inputs	β and RR_ζ
Type	Behaviour Check

3.1.3 Sign Checks

AL-17	IM shall trip if roll rate p is positive/(negative), AND pilot gives left/(right) wing down input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft reaction should correspond to pilot demand, if no protection reduces pilot authority.
Inputs	p and SS_ξ
Type	Behaviour Check

AL-18	IM shall trip if pitch rate q is positive/(negative), AND pilot gives pitch down/(up) input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft reaction should correspond to pilot demand, if no protection reduces pilot authority.
Inputs	q and SS_η
Type	Behaviour Check

AL-19	IM shall trip if normal load factor rate $\dot{n}_z$ is positive/(negative), AND pilot gives pitch down/(up) input, AND aircraft operated in normal flight envelope.
Rationale:	Aircraft reaction should correspond to pilot demand/expectation, if no protection reduces pilot authority.
Inputs	n_z and SS_η
Type	Behaviour Check

3.1.4 Controllability Checks

AL-20	IM 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 AEO, AND aircraft operated in normal flight envelope.
Rationale:	Lateral control must be enough 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). Threshold value: 100% pilot roll rate demand on the side stick have to result in an absolute roll rate$\lvert p\rvert \geq 8.5$ °/s [15], AMC 25.147 (d)+(f). Therefore, $\lvert p\rvert = 3.4$ °/s have to be acquired with 40% pilot roll rate demand at 50% roll input on the side stick [13]
Inputs	p and SS_ξ
Type	Behaviour Check

AL-21	IM shall trip if pilot pitch down input exceeds 50%, AND the change in trajectory $\dot{\gamma}$ stays above -2.5 °/s, AND absolute flight path angle is below 10°, AND aircraft operated in normal flight envelope.
Rationale:	Pilot should always have minimum pitch authority to be able to avoid collisions. Threshold value: In horizontal flight, 100% pilot pitch down demand on the side stick have to result in a flight path angle rate $\dot{\gamma} \leq -5.0$ °/s [15], AMC 25.143 (l) (4). Therefore, $\dot{\gamma} = -2.5$ °/s have to be acquired with 50% pitch down input on the side stick [13].
Inputs	γ and SS_η
Type	Behaviour Check

3.2 Plausibility Checks on FCL Level

3.2.1 Protection Function Checks

SL-01	IM shall trip if the bank angle protection is active, AND no pilot roll input, AND the FCL commands aileron deflections that lead towards an increasing absolute bank angle.
Rationale:	Above the protected bank angle limit $\Phi_{prot} = \pm 33$ °, the bank angle protection should generate aileron commands that return the A/C to the normal bank angle range $\Phi \leq \Phi_{prot}$ [13]. This applies also if the stall-protection is active.
Inputs	ξ_{cmd} and SS_ξ
Type	Command Check

SL-02	IM shall trip if the bank angle protection is active, AND overspeed protection is active, AND no pilot roll input, AND the FCL commands aileron deflections that lead towards an increasing absolute bank angle.
Rationale:	In overspeed conditions, the bank angle protection should generate aileron commands that return the A/C to a bank angle of $\Phi = 0°$ (wings level) [13].
Inputs	ξ_{cmd} and SS_{ξ}
Type	Command Check

SL-03	IM 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.
Rationale:	Above the speed limit V_{MO}, the overspeed protection should generate elevator commands (positive load factors) that return the A/C to airspeed range $V_{CAS} \leq V_{MO}$ [13].
Inputs	η_{cmd} and SS_{η}
Type	Command Check

SL-04	IM shall trip if the high AoA protection is active, OR the low-speed protection is active, AND no pilot pitch input, AND the FCL commands elevator deflections that lead towards increasing the AoA.
Rationale:	Above the protected AoA limit α_{prot}, the high AoA/low-speed protection should generate elevator commands (negative load factors) that return the AoA to the range of $\alpha \leq \alpha_{prot}$ [13].
Inputs	η_{cmd} and SS_{η}
Type	Command Check

SL-05	IM shall trip if the high pitch attitude protection is active AND the FCL commands elevator deflections that lead towards increasing the pitch attitude.
Rationale:	Above the protected pitch attitude limit Θ_{max}, the high pitch attitude protection should generate elevator commands (leading to negative load factors) that return the A/C into the protected pitch range $\Theta \leq \Theta_{max}$.
Inputs	η_{cmd} and SS_{η}
Type	Command Check

SL-06	IM shall trip if the low pitch attitude protection is active AND the FCL commands elevator deflections that lead towards decreasing the pitch attitude.
Rationale:	Below the protected pitch attitude limit Θ_{min}, the low pitch attitude protection should generate elevator commands (leading to positive load factors) that return the A/C into the protected pitch range $\Theta \geq \Theta_{min}$.
Inputs	η_{cmd} and SS_{η}
Type	Command Check

3.2.2 Sign Check

SL-07	IM shall trip if the pilot commands right wing down (/left wing down), AND initial aileron commands induce left wing down (/right wing down) roll acceleration, AND aircraft operated in normal flight envelope.
Rationale:	In the normal flight envelope, the initial aileron command after changes of the pilot input should correspond to the pilot demand.
Inputs	ξ_{cmd} and SS_{ξ}
Type	Command Check

3.2.3 Pitch Trim Drift Checks

SL-08	IM 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 operated in normal flight envelope.
Rationale:	The automatic trim function should decrease the elevator hinge moment.
Inputs	η_{cmd} and THS_{cmd}
Type	Command Check

3.3 Comparator Checks

3.3.1 Elevator Checks

SL-09	IM shall trip if the elevator command of normal law η_{cmd} and direct law $\eta_{DL,cmd}$ significantly differ, AND aircraft operated in normal flight envelope.
Rationale:	The flight control law outputs should be similar when considering the effects of dynamic pressure and flight envelope protections are inactive.
Inputs	η_{cmd} and $\eta_{DL,cmd}$
Type	Comparator

3.3.2 Aileron Checks

SL-10	IM shall trip if the aileron commands of normal law ξ_{cmd} and direct law $\xi_{DL,cmd}$ significantly differ, AND aircraft operated in normal flight envelope.
Rationale:	The flight control law outputs should be similar when considering the effects of dynamic pressure and flight envelope protections are inactive.
Inputs	ξ_{cmd} and $\xi_{DL,cmd}$
Type	Comparator

3.3.3 Rudder Checks

SL-11	IM shall trip if the rudder command of normal law ζ_{cmd} and direct law $\zeta_{DL,cmd}$ significantly differ, AND aircraft operated in normal flight envelope.
Rationale:	The flight control law outputs should be similar when considering the effects of dynamic pressure and flight envelope protections are inactive.
Inputs	ζ_{cmd} and $\zeta_{DL,cmd}$
Type	Comparator

3.4 Additional Monitor Functions

This chapter provides a short overview of additional monitor functions that were discussed with respect to their effectiveness, robustness, complexity, and implementation effort. All the discussed monitors can be allocated to the monitor type “plausibility check on aircraft level”.

These additional monitoring functions have shown some theoretical potential but, for the time being, are not further developed due to:

- too high complexity or too difficult robust implementation in a production flight control system

- questionable added value in the light of the monitors described above (which cover certain aspects of the additional monitors)
- exceedance of the scope considered for the FCL monitoring as described in section 2.2

An implementation of the additional monitors in the frame of the LITUB project is therefore not planned, and focus is put on implementation and validation of the monitors specified above.

Accordingly, no dedicated requirements for these monitor functions were developed. However, for completeness, a brief introduction of these potential monitors is given in this section.

3.4.1 Total Energy Monitor

Unintended behaviour of the FCS caused by FCL development errors can potentially lead to an insufficient total energy state of an aircraft. The total energy of an aircraft is an important parameter for the assessment of the criticality of a certain flight state. Besides the absolute total energy value, the balance between potential energy and kinetic energy is of importance, which varies depending on the flight condition and flight task. Total energy and energy reserves also play an important role considering the planned flight trajectory and required manoeuvres.

Accordingly, a potential total energy monitor would check for three aspects:

- the absolute total energy
- the ratio between potential and kinetic energy, and asses it with respect to the current flight condition and applied control inputs
- the total energy and energy reserves versus the planned flight trajectory

In addition to standard input signals used for the FCS, the monitor would require information on the current thrust level, which must be calculated based on thrust lever setting, barometric altitude, and airspeed. To assess the current energy state in relation to the upcoming trajectory changes, the monitor would also require inputs from the flight management system.

Within the first aspect described above (absolute total energy), the kinetic energy is of most relevance for airliners during the major portion of a flight. This is covered already by the aircraft limit checks in subsection 3.1.1. The limit checks specified for monitor A01 and A10, but also functions like the Airbus Alpha Floor function already represent a type of low kinetic energy monitoring and, in the case of Alpha Floor, a low kinetic energy mitigation function. Low potential energy situations are of relevance to airliners during the approach, landing and take-off flight phases and are addressed by state-of-the-art functions like GPWS (ground proximity warning system).

The second aspect of total energy monitoring taking the energy ratio into account is of most relevance for highly manoeuvrable military aircraft, e.g., during highly dynamic manoeuvres in ground proximity and is therefore not considered for this project.

The third aspect would result in a monitor acting one or two levels above the scope for this project (refer to section 2.2), as the outer loops of flight management and trajectory planning would have to be considered. Monitoring on that level is far away from the source of potential errors of interest in this project, i.e., the FCL. Thus, many other factors can contribute to critical states on that level, and tracing to error sources within the FCL would not be feasible.

3.4.2 Real-Time Pilot-Induced Oscillation Detection

Pilot Induced Oscillations (PIO) can potentially result from FCL development errors, including FCL insufficiencies based on wrong or incomplete assumptions. This is the case although there has been extensive research on PIO prevention and prediction during the design phase of aircraft and their flight control systems. That said, it must be assumed that PIO cannot be completely prevented by design in advance and will continue to occur.

To mitigate risks of critical PIO that may lead to catastrophic effects, one approach that has been discussed is real-time PIO detection. The idea is to detect a PIO situation in real-time in its early stage before it has developed into a critical situation, and to provide a warning for the flight crew. The method developed and described in [17] basically detects a developing oscillation in aircraft response and checks for correlating control inputs, including their absolute amplitude / control force, and phase relation to the aircraft response. Research activities described in [17] have

demonstrated the effectiveness of the real-time detection method via post-processing of recorded PIO events, and also via real-time application in desktop simulations.

However, it was found that the robustness of the monitoring algorithm would be lower than classic warning functions, like stall warning or stick shakers. In other words, if a pilot applies pumping control inputs, the monitor checking for the control input amplitude and the phase relation between control inputs and aircraft response could trip, although there is no real PIO situation. Any nuisance trip of the system would significantly lower the confidence of flight crews in the system and added value for flight safety is questionable.

Another open question is how pilots would need to be trained to effectively respond to a generated PIO warning. And again, if a PIO is identified in real-time, there might be many other factors besides FCL errors that can lead to that situation. In turn, a clear traceability to issues within the FCL will be difficult to achieve.

However, in [17], the method is recommended to be applied during the development / validation phase of flight control systems. In a flight test environment, it could be used to identify any operational areas where a system is prone to PIO in real time and enable engineers to validate assumptions made for the FCL development and adapt FCL settings and/or functionality accordingly.

4 Summary

This report proposes a list of independent monitor functions that shall be investigated and validated. The independent monitor can work on three levels: local (FCL SW-level), intermediate (FCS-level) or global (aircraft-level). Monitoring on an intermediate level does not offer significant advantages. Functional independence and a direct assessment of the criticality of the failure is feasible on the global monitoring level. And the local level has the advantage of a direct allocation of the detected fault and a potentially earlier detection, which would give the pilot more time to react to a potentially hazardous failure condition.

The monitoring functions can be classified by decision mechanism. Two basic concepts are proposed:

- Comparators, and
- Plausibility Checks.

Comparators compare the results of redundant (but functional independent) FCL. A fault is detected when the outputs of the variants differ. This check works on FCL SW-level. Plausibility Checks verify that the behaviour of the FCL software is acceptable and plausible rather than correct, based on predictions on the anticipated system state. The plausibility check monitor can work on aircraft and FCL level. Plausibility Checks can be categorized into three groups:

- Limit Checks,
- Behaviour Checks, and
- Command Checks.

Limit Checks check for a violation of (hard) limits that the aircraft is not supposed to exceed. Exceedance of the limit is always a sufficient condition to detect failures. If one (or more) of the limits are exceeded, it is assumed that a failure is present.

Behaviour Checks check the plausibility of the aircraft reaction under consideration of the pilot demand. They are never a sufficient condition to determine if the FCL is faulty. If undesired aircraft behaviour is detected, the FCL commands need to be checked to determine the cause of the failure.

Command Checks comprise checks for acceptability of the FCL commands to the control surfaces that are monitored under consideration of the pilot demand. Command Checks have to consider more than one aircraft state parameter to detect failures. Therefore, they are more complex than Limit Checks. Checks of this category can be a sufficient or a necessary condition to detect faults of the FCL.

A total of 24 independent monitoring functions are proposed. Three functions of the class Comparators and 21 functions of the class Plausibility Checks.

Additional monitor functions are briefly introduced that were investigated but not selected for further development for several reasons, including lack of added value, exceedance of the scope of FCL monitoring, and too high complexity.