Technical Note	This project has received funding from the European Union's Horizon Europe Programme
TN-FMRA-24-003-v01	LIEBHERR

Title: Assessment of Required Effort for Implementation

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

Work Package: Task 6

Document Ref.: TN-FMRA-24-003

Version: v01

Author: G. Weber

Date: 10.09.2024

Summary: This Technical Note assesses the implementation effort of the proposed independent monitoring functions. The different investigated monitor types are compared in a qualitative way regarding the effort of the individual development steps. A summary table with a three level implementation effort scale for each monitor type is presented.

This Technical Note represents the deliverable D-6.1 of the “Horizon Europe Project: Flight Control Laws and Air Data Monitors” Lot 1 (EASA.2021.HVP.28)” project.

	Prepared	**Reviewed**	**Approved**	**Released**
Name	G. Weber	E. Dejene D. Hübener	P. Schädler	P. Schädler
Date	10.09.2024	10.09.2024	10.09.2024	10.09.2024
Signature	electronic signature	electronic signature	electronic signature	electronic signature

Revision History

Version	Date	Author	Description of Changes
01	10.09.2024	G. Weber	Initial version

Distribution List

Name	Organisation	Copies
G. Weber	Liebherr-Aerospace	electronic
P. Schaedler	Liebherr-Aerospace	electronic
T. Socher	Liebherr-Aerospace	electronic
E. Dejene	Liebherr-Aerospace	electronic
T. Lanz	Liebherr-Aerospace	electronic
S. Koebe	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

Contents

Abbreviations **4**

Definitions **5**

Symbols **6**

Bibliography **7**

Typographical Conventions **7**

1 Introduction **8**

1.1 Motivation 8

1.2 Report Structure 8

2 Approach to Independent Monitor Implementation Effort Assessment **9**

2.1 Independent Monitor Development Steps 9

2.1.1 Analysis of Considered Failure Modes and Effects 9

2.1.2 IMF System Requirements Capture 9

2.1.3 IMF Design and Preparation of Closed-Loop Simulation 10

2.1.4 Monitor Validation 10

2.1.5 High-level SW Requirements Capture 10

2.1.6 SW-Design and Implementation 10

2.1.7 Monitor Verification (HW/SW, unit level, system level, closed loop) 10

3 Qualitative comparison of different IMF types **11**

Abbreviations

Acronym	Description
A/C	Aircraft
C	Source Code Manipulation
CAT	Catastrophic Flight Condition
CG	Centre of Gravity
DL	Direct Law
FAR	False Alarm Rate
FCF	Flight Control Function
FCL	Flight Control Laws
FMRA	Fachgebiet Flugmechanik, Flugregelung und Aeroelastizität, TU Berlin
FSEnv	Flight Simulation Environment
HAZ	Hazardous Flight Condition
HIR	Hit Rate
LOG	Flight Control Law Logics
IMF	Independent Monitor Function
NL	Normal Law
PFA	Probability of False Alarms
POD	Probability of Detection
PRT	Protection Function
SG	Signal Generator
SW	Software
THS	Trimmable Horizontal Stabilizer
TP	Trim Point
TS	Test Scenario

Definitions

Term	Definition/Meaning
Failure	A loss of function or a malfunction of a system or a part thereof. (ARP4761).
Active Failure	Failures where FCL function acts erroneously and independent from the input signals and cannot be influenced e.g., by the pilot commands. However, the outcome of the failure may vary in amplitude or its time response depending on the input signals. One typical signature of failures of this class is a runaway, which is an actuator-like failure [1].
Reactive Failure	Failures where FCL function reacts erroneously on inputs and is highly dependent on at least one input signal e.g. a command of the flight crew or from the measured signals of the flight condition itself. This class includes failures that increase the A/C’s PIO tendency, reduce the damping of flight dynamic modes or deteriorate the A/C’s handling qualities in other ways [1].
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).
Trim Point	An initial aircraft state which contains calculated dynamic aircraft parameters for desired flight envelope point. The trim routine and trim conditions are described in reference [2].
Test Scenario	Test Scenario comprises test inputs during simulation execution. It includes pilot inputs and initiation of FCL failures. A test scenario is a MATLAB script that specifies required deviations from the default test scenario.
Test Program	Generic term that includes all activities for testing to evaluate the monitor effectiveness and robustness.
False Positive	The FCL-Monitor triggers a false alarm during failure-free operation. This criterion is used for effectiveness tests and robustness tests.
False Negative	The FCL-Monitor does not detect a failure caused by a FCL development error. This criterion is used for effectiveness tests.
True Positive	The FCL-Monitor detects a failure caused by a FCL development error. This criterion is used for effectiveness tests.
True Negative	The FCL-Monitor does not trigger an alarm during failure-free operation. This criterion is used for robustness tests.

Symbols

Symbol	Meaning
α	Angle of attack
α_{max}	Maximum angle of attack
β	Sideslip angle
θ	Pitch angle
Φ	Roll angle
η_F	Flap deflection angle
n_z	Normal load factor
n_y	Lateral load factor
H	Altitude
H_{msl}	Height above mean sea level
m	Mass
N_E	Total number of Effectiveness Simulations
N_R	Total number of Robustness Simulations
N_{TP}	Number of True Positive Simulations
N_{FP}	Number of False Positive Simulations
N_{FN}	Number of False Negative Simulations
N_{TN}	Number of True Negative Simulations
t_f	Point of time when failure occurs
t_r	Latest monitor reaction time
t_g	Time when A/C is recoverable with a significant increase in pilot workload
V_{CAS}	Calibrated airspeed
V_{TAS}	True Air Speed
$V_{FCL,min}$	FCL low speed protection boundary
$V_{FCL,max}$	FCL maximum speed protection boundary
V_{FE}	Maximum flap extended speed
V_w	Wind speed
V_{MO}	Maximum operation speed
V_{NE}	Never exceed speed
V_D	Dive speed
V_S	Stall speed
Ma	Mach number

Bibliography

[1] D. Chernetsov und B. Laabs, „List of Potential Errors in Flight Control Laws, Failure Classification for Development of an Independent FCL Monitor," Berlin, 2023.

[2] D. Chernetsov und R. Luckner, „VFW614-ATD Flight Simultion Environment Technical Manual," 2023.

[3] EASA, „Monitoring of Flight Control Laws," 2023. [Online]. Available: https://www.easa.europa.eu/en/research-projects/monitoring-flight-control-laws. [Zugriff am 14 Februar 2023].

[4] B. Laabs, „User Manual for the VFW614-ATD Flight Simulation Environment," TU Berlin, Berlin, 2023.

[5] B.Laabs, „Validation of the VFW614-ATD Flight Simulation Environment," Berlin, 2023.

[6] D. Hübener, B. Laabs und G. Weber, „List of Proposed Flight Control Law Monitors," Berlin, 2023.

[7] D. Hübener, „Evaluation Results of the Effectiveness Tests," Berlin, 2024.

[8] D. Hübener, „Evaluation Results of the Robustness Tests," Berlin, 2024.

Typographical Conventions

Following typographical conventions are used in this document:

Item	Convention to use	Example
Example Code	`Monospace Consolas` font	`A=5`
Folder name	*Arial* font, italics	*folder*
File name	***Arial*** font, bold, italics	***filename***
New terms	*Arial* font, italics	*Test Case*
variable	`Monospace Consolas` font	`variable`
bus signal	`Monospace Consolas` font, underlined	`bus signal`

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 FCL failures [3]. This Technical Note is a part of the delivery D-6.1 of the “EASA Horizon Flight Control Law Monitors In Task 6, a qualitative assessment of the proposed Independent Monitor Functions (IMFs) is performed in respect to the required efforts and constraints for their implementation, and the most suitable IMFs are identified taking into account the trade-offs between performance and the required effort for their implementation.

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 Environment (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 [4], a programmer’s guide [2] and a validation report [5].

This document describes the results of the implementation effort assessment for the IMFs that were implemented according to reference [6] and checked for their effectiveness and robustness as documented in references [7] and [8]. It comprises the effort assessment approach, and the summary of the implementation effort rating for each IMF.

1.1 Motivation

The objective of the Independent Monitor is to increase the safety of the FCS while maintaining highest rates of availability. It needs to be designed with thresholds and confirmation times set not so high as to not trigger when needed (effectiveness), and not so low as to lead to false alarms during failure-free operations (robustness).

The evaluation of the simulation results and implementation effort allows an identification of the most promising IMFs.

For future commercial development and certification purposes, a more extensive analysis over the complete flight envelope (e.g., with help of Monte Carlo simulations) might be required. However, this is out of scope in this project.

1.2 Report Structure

This report is structured as follows:

- Section 2 summarizes the approach for the implementation effort evaluation of independent monitors. Some general considerations are given, including a short introduction on the development steps, followed by a description of the implementation effort rating scale.
- Section 3 provides an overview on the IMF types with their associated implementation effort rating.

2 Approach to Independent Monitor Implementation Effort Assessment

The implementation effort for the IMFs developed and investigated in this project is one important criterion for the overall feasibility assessment of IMFs, in addition to the IMF effectiveness and robustness.

The objective of this implementation effort assessment is to provide a qualitative comparison for the different types of IMFs between each other rather than to compare the implementation effort of a flight control system without IMFs to a flight control system with IMFs. However, the latter aspect will be subject to further discussions complementing results obtained in this project.

The structured development steps for the IMFs are similar to the development steps necessary for classic monitoring functions, while strong focus should be out on thorough validation of the IMFs regarding effectiveness and robustness. All of these steps are more or less depending on the particular IMF design. The next section provides a summary of the development steps with short explanations.

It has to be noted that the real implementation effort for such IMFs will largely depend on the development toolchain and approaches used (e.g. model-based development approaches acc. DO-331), the flight control system work shares between the airframer and suppliers (e.g. flight control functionalities developed fully in-house at airframer or shared between airframer and supplier) as well as on the experience and know-how of the particular airframer. In the end, also driven by the novelty of the IMF approach, a detailed and representative implementation effort assessment can be obtained by airframers in the scope of a commercial development project.

Accordingly, for this project it was decided to apply a very simple, qualitative implementation effort rating scale which can only give a rough hint on the level of implementation effort required for the different considered IMFs. The rating scale consists of three implementation effort levels: low, medium and high implementation effort. A low implementation effort, when compared to the other IMFs is classified as *good*. A high implementation effort when compared to the other IMFs is classified as *bad*. Everything in between (medium) is considered *acceptable*. The implementation effort assessment takes into account the development steps introduced in the following section and focuses on the criteria: IMF algorithm complexity, validation and verification effort and expected IMF tuning effort.

2.1 Independent Monitor Development Steps

This section provides a short summary of the development steps required for implementing the IMFs.

2.1.1 Analysis of Considered Failure Modes and Effects

As described in reference [6], an analysis of the different failure modes (resulting from FCL development errors) considered within the FCL and their effects at the FCL outputs has to be conducted. This represents a “white box” approach, with knowledge of the internal FCL functionality and structure being necessary. Alternatively, a “black box” approach could be followed, with definitions of the FCL output failure signatures not taking into account the internal functions. It is expected that for a real development project, a combination of both approaches would be followed.

This development step is independent from the IMF type chosen for mitigation.

2.1.2 IMF System Requirements Capture

A set of system-level requirements for the IMFs has to be developed. The requirements should include the failure effects to be mitigated and the monitor reaction, as well as the system reconfiguration.

These requirements should not include any particular monitor design, thus these efforts are considered mostly independent from the particular IMFs.

2.1.3 IMF Design and Preparation of Closed-Loop Simulation

Suitable IMF designs in response to the requirements are developed in this phase. This includes the definition of IMF inputs, outputs, its internal structure, thresholds and confirmation times and conditions for its activation. In addition, the setup for the monitor validation including the considered flight conditions, system states and external conditions are defined and prepared in a simulation environment.

This development step is specific for the different types of IMFs.

2.1.4 Monitor Validation

This development step is key for the successful implementation of the IMF, as it addresses the validation of the IMF effectiveness and robustness in a simulation environment. In an iterative way, the monitor design and/or its internal settings can be adapted based on the validation results. The difficulty here is to define a sufficient level of coverage especially for the robustness validation test cases. Pilot-in-the-loop trials are recommended, too, for sound assessment of the monitor reaction and system reconfiguration. In the end of this phase, the IMF structure and settings are fixed and flown down to high-level SW requirements. A set of test cases defined in this phase could be used for later verification activities.

This development step is specific for the particular IMF. However, the effort is mostly driven by the number and complexity of validation test cases, which is considered similar between the different IMFs.

2.1.5 High-level SW Requirements Capture

Within this development step, the high-level SW requirements for the particular IMFs are developed. Alternatively, an executable model could be developed that would serve for later SW implementation.

This development step is specific for the particular IMF.

2.1.6 SW-Design and Implementation

Within this development step, the SW-design is derived based on the SW high-level requirements. Code will be written based on the SW design. Alternatively, the model mentioned above could be used for SW implementation / code generation.

This development step is specific for the particular IMF.

2.1.7 Monitor Verification (HW/SW, unit level, system level, closed loop)

In the course of this development step, the implementation of the IMFs is checked with the real system or its components in the loop. These activities could be conducted on different levels, like unit level, system level, and most important closed-loop aircraft and flight control system level, including pilot-in-the-loop trials. As stated above, the verification activities should include repetitions of the validation test cases in order to make sure the implementation meets the expectations obtained during the validation. An essential part of the verification activities should be conducted in a representative flight simulation environment as it is also used for validation of the aircraft and system level FHAs. This development step, together with the validation activities is considered to represent the majority of development effort for IMFs in general.

This development step is specific for the particular IMF. However, the effort is mostly driven by the number and complexity of validation test cases, which is considered similar between the different IMFs.

3 Qualitative comparison of different IMF types

Table 3-1 provides a summary of all investigated IMF types with a rough estimation of their implementation effort according to the rating scale explained above.

Table 3-1: Implementation effort of different IMF types.

IMF type	Implementation Effort	Comment
Limit Checks	**Low**	Simple algorithm, V+V activities easy to set up, low effort for tuning activities expected
Hands-free Checks	**Medium**	Simple algorithm, V+V activities easy to set up, medium effort for tuning activities expected
Sign Checks	**Medium**	More complex algorithm, V+V activities set up require more effort, medium effort for tuning activities expected
Controllability Checks	**Medium**	More complex algorithm, V+V activities set up require more effort, medium effort for tuning activities expected
Protection Function Checks	**High**	More complex algorithm, V+V activities set up require more effort, high effort for tuning activities expected
Command Sign Check	**High**	More complex algorithm, V+V activities set up require more effort, high effort for tuning activities expected
Pitch Trim Drift Check	**Medium**	More complex algorithm, V+V activities set up require more effort, medium effort for tuning activities expected
Command Comparison	**Medium**	Simple algorithm, V+V activities set up require more effort, medium effort for tuning activities expected