Technical Note

TN-FMRA-23-005-v01

Title: List of Potential Errors in Flight Control Laws

Failure Classification for Development of an Independent FCL Monitor

Project:	EASA.2021.HVP.28 “Horizon Europe Project: Flight Control Laws and Air Data Monitors” Lot 1
Work Package:	Task 2
Document Ref.:	TN-FMRA-23-005
Version:	v01
Authors:	Dmitry Chernetsov, Bryan Laabs
Date:	08.05.2023

Summary:

This Technical Note defines the failure classification method for the flight control laws. It includes background information from the analysis of aircraft accidents, the short description and listing of the VFW614-ATD FCL functions, the assumptions for the failure classification, the description of the defined failure classes as well as simulation examples and a conclusion. The proposed failure classification method identifies significant failure signatures at the output of the FCL that are relevant for Independent Monitor validation.

This Technical Note represents the deliverable D-2.1 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. Chernetsov B. Laabs	A. Arnold D. Hübener	F. Silvestre	F. Silvestre
Date	08.05.2023	08.05.2023	08.05.2023	08.05.2023
Signature		A. Arnold Hübener		

Revision History

Version	Date	Author	Description of Changes
1	08.05.2023	B. Laabs, D. Chernetsov	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
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

A/C	Aircraft
AoA	Angle of Attack
ATD	Advanced Technologies Demonstrator
CG	Centre of Gravity
DL	Direct Law
EFCS	Electronic Flight Control System
FbW	Fly by Wire
FCF	Flight Control Functions
FCS	Flight Control System
FCL	Flight Control Laws
FCL SW	Flight Control Law Software
FMRA	Fachgebiet Flugmechanik, Flugregelung und Aeroelastizität, TU Berlin
FSEnv	Flight Simulation Environment
MAC	Mean Aerodynamic Chord
MRA	Minimum Reception Altitude
LOG	(Mode) Logic
NL	Normal Law
PRT	Protection Function
THS	Trimmable Horizontal Stabilizer
SW	Software
VNE	Never Exceed Speed

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 [16].
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)

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

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`

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] BEA: *Report: Serious incident on 24 May 2011 during descent to Kuala Lumpur Airport (Malaysia) to the Dassault Falcon 7X registered HB-JFN operated by Jet Link AG, 2016*

[4] ANSV: *Final Report: Accident occurred to the Agusta Westland AW-609 aircraft registration marks N609AG, in Tronzano Vercellese (VC), on the 30th of October, 2015*

[5] NTSB: *Aviation Investigation Final Report: Accident Bell 525 at Italy, Texas on July, 6th, 2016*

[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] Heintsch, T., Holzhausen, T.: *Flight Control Laws for the Primary Flight Module in the PFCU.* Bremen, 2000.

[10] Heintsch, T., Holzhausen, T.: *Direct Laws for the Primary Flight Module in the PFCU.* Hamburg, 2000.

[11] Hübener, D. *Independent Monitoring of Flight Control Laws - Principles and Concepts*, Technische Universität Berlin, Technical Note, TN-FMRA-23-004-v1, Berlin, 2023.

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

[13] Manpuria P. S.: Entwicklung eines Steuergesetzes zur manuellen Steuerung des Abfangvorganges eines Flugzeugs mit elektrischer Flugsteuerung, Bachelor Thesis, TU Berlin, 2015.

[14] Annex List - Annual Safety Recommendations Review 2018, EASA, 31/07/2019 https://www.easa.europa.eu/en/downloads/101381/en

[15] [SAE International: *SAE ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, 1996.

[16] 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.

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 [1]. This Technical Note represents the delivery D-2.1 for Task 2 of the project.

In Task 2, potential FCL errors shall be identified, classified and delivered as a list. Due to the complexity of the FCL and the high number of functions, an exhaustive list with all possible errors is not the focus in the context of this project. Instead, failures of the FCS that are caused by FCL development errors are identified and categorized. For validation of the *Independent Monitor*, representative cases from each category will be simulated in flight scenarios that have the most adverse impact on flight safety.

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. The documentation comprises a user manual [6], a programmer’s guide [8] and a validation report [7].

This document proposes a classification of potential FCL failures based on engineering knowledge and the functions that are implemented by the VFW614-ATD FCL SW. Assumptions are postulated to reduce the amount of possible failure classes and to make the validation campaign for the *Independent Monitors* feasible. The classification depends on both the function that is affected by the error and the failure characteristics that are caused by errors in FCL functions. Exemplary failures for the VFW614-ATD FCL are given for each class of the proposed classification. For these failure examples, simulations are conducted to show that the outcome of the failures are similar independently of the source of the error in FCL SW.

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[1]. However, the certification authorities state 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 in the position paper [2]. An *Independent Monitor* for the FCL could be a means to achieve fault tolerance against FCL requirement and design errors.

Publicly available information (reports on in-service events, incident and accident reports) during airline operations of CS-25/FAR Part 25 aircraft have been analysed in the MODULAR[2] project. Additionally, a serious incident of a Falcon 7X business jet on a transfer flight, [3], and two accidents named by EASA, an accident of a Leonardo AW609 tilt rotor, [4], and an accident of a Bell 525 helicopter, [5], both during test flights, are analysed in Appendix A.1. In all examples from routine airline flights, no single FCL requirement error was the cause for the accident or incident [11]. As the number of potential examples is low, an alternative approach is selected to define and classify potential FCL failures.

1.2 Report Structure

The report is structured as follows:

---

[1] Here, it is assumed that the FCL software is correctly implemented as all implementation errors should be detected in the software verification and validation process or be tolerated by dissimilar software implementation.

[2] LuFo VI-1 project funding reference: 20Y1910C

- Section 2 describes the failure classification method, and contains background information, VWF614-ATD FCL functions overview, assumptions, description of failure classes,
- Section 3 contains failure examples,
- Section 4 summarizes the conclusions,
- Appendix A.1 contains analysis of accidents that EASA has proposed,
- Appendix A.2 describes the general signature of typical actuator failures,
- Appendix A-3 describes the designation of flight phases,
- Appendix A-4 contains an analysis of simulation examples for selected failures,
- Appendix A-5 contains the FSEnv signal mapping to variables in simulation plots.

2 FCL Failure Classification Method

The design of an independent monitor requires to define the potential failures that the monitor shall detect. Publicly available information, i.e., reports on in-service events, incident and accident reports during airline operations of CS-25/FAR Part 25 aircraft, have been analysed in the MODULAR project [11].

Additionally, EASA named an accident of a Leonardo AW609 tilt rotor [4], and an accident of a Bell 525 helicopter [5], both during test flights. Both accidents and a serious incident of a Falcon 7X business jet on a transfer flight [3], are analysed in Appendix A.1. In all examples from routine airline flights, no single FCL requirement error was the cause for the accident.

On the other hand, Leveson states in [12] that nearly all serious technogenic accidents in which SW was involved can be traced to requirement flaws. She identified three cases, in which the SW requirement was correctly implemented but where the SW is still responsible for unsafe behaviour:

1. Incorrect (unsafe) requirement, when the SW is correctly implemented, but the specified behaviour is unsafe from a system point of view.
2. Incomplete requirements, when requirements do not specify some required behaviour for system safety, and
3. Unintended (and unsafe) behaviour of the SW, when the SW has unintended (and unsafe) behaviour beyond what is specified in the requirements.

As the number of potential accident and incident examples is low and the relevant literature gives only rough concepts, an alternative approach is selected to identify and classify failures that are caused by FCL development errors.

The failure classification approach that is described in this document does not identify specific examples of FCL development errors. Instead, effects of FCL errors and the resulting erroneous FCL commands that can have hazardous or catastrophic consequences are determined. These FCL failures are categorized. For validation of the *Independent Monitor*, representative scenarios from each category will be simulated in flight scenarios, where they may have the most adverse impact on flight safety.

2.1 Assumptions

For the proposed FCL failure classification approach, it is irrelevant where in the development process the error was introduced. The error that leads to a system failure, which is affecting the aircraft dynamic response or its dynamic characteristics (A/C level), may result from an error in the FCL requirements or in the FCL design. Therefore, the resulting failures are classified and not the underlying errors.

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 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.

2.2 VFW614-ATD Flight Control Functions

Based on the functional overview of the VFW614-ATD FCL, an initial classification method is developed. The VFW614-ATD FCL were developed in the VFW614-ATD technology project, in which new technologies for an Electronic Flight Control System were developed and demonstrated. The FCL were flight-tested in the years 1999 to 2000. The aircraft was only flown manually. The FCL SW incorporates Direct Law (DL) and Normal Law (NL). The FCL SW commands control surface deflections that are computed from the pilot inputs for the cockpit devices (side stick, pedals, pitch trim hand-wheel, rudder trim switch, speed brake and flap handle). The side stick is used for pitch and roll commands, the pedals are used for yaw commands.

The NL provides the following functions:

- Pitch control by load factor (n_z) demand with turn compensation up to 33° bank angle,
- Roll control by roll rate command / bank angle hold,
- Yaw control by rudder command with yaw damper and turn coordination,
- Protections against excessive load factor, angle of attack, pitch attitude, bank angle, airspeed / Mach number,
- Flare Law that was not included in FCL, the pilot had to switch to Direct Law for landing. However, TU Berlin integrated a flare law that operates similar as the Airbus A320 flare law, see [13].

Figure 2-1 depicts the activity of the different modes of operation of the FCL for a complete mission. Take-off and landing mode are short switching phases between ground and flight mode. In these switching phases, the control surface commands of the flight control functions (FCF) in ground mode and flight mode are blended within 5 seconds. In these phases, only the stall protection (high AoA protection) is available while all other protections are passivated. All other protections such as pitch attitude protection, load factor protection and bank angle protection are only active during flight mode.

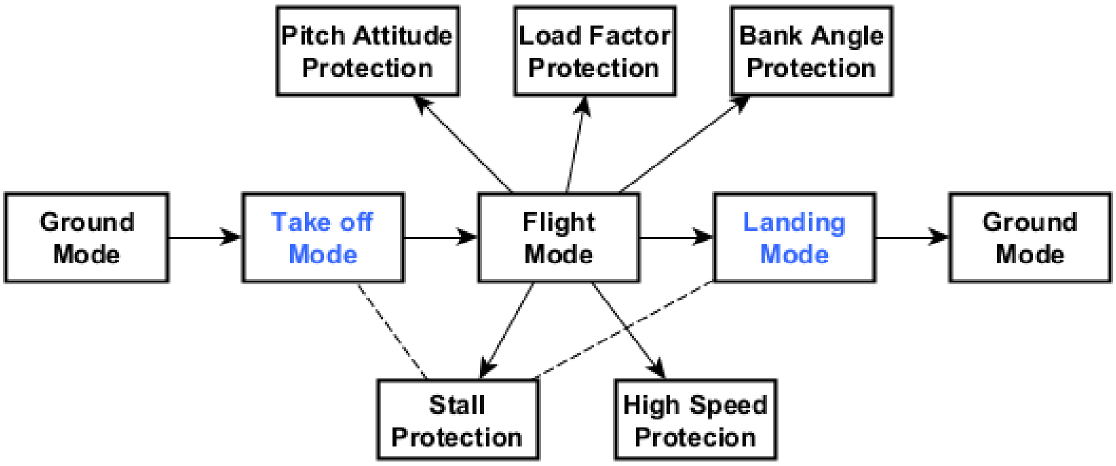

Figure 2-1: Flight Control Law Modes (Landing Mode was implemented by TU Berlin)

The FCL are designed for:

- a CG range 20-28% MAC (reduced CG range of the VFW614-ATD),
- V_{MO} of 255 kt and M_{MO} of 0.56 [-] (max operating speeds of the VFW614).

Table 2-1 shows a functional breakdown of the FCL SW for the Normal Law, that is considered for the failure classification approach.

Table 2-1: Functional Breakdown of ATD FCL SW for the Normal Law

ATD FCL Normal Law Functions
Normal Law Mode Logic Functions (LOG)
• Normal Law Modes (Ground Mode, Flight Mode)
• Protection Activation
Control & Stability / Flight Control Functions (FCF)
• Pitch Normal Law
• Roll Normal Law
• Yaw Normal Law
Protection Functions (PRT)
• Load Factor Protection
• High Speed Protection
• Pitch Attitude Protection
• High AoA Protection
• Bank Angle Protection

2.3 Failure Classes

Based on engineering experience and analysis of the functional structure of the NL that is given in Table 2-1, two methods for failure classification are proposed:

- Classification method based on the type of a function (mode logic, normal flight control function, envelope protection function),
- Classification method that considers the dependency of a failure on the input signals of the FCL SW
  - Input-independent failures: failures in the FCL functions that affect the output independently from input signals (active class),
  - Input-dependent failures: failures in the FCL functions that affect the output in dependence of input signal (reactive class).

2.3.1 Classification Method Based on the Type of a Function

The functional classification distinguishes three function types:

- **Failures in the mode logic (LOG):**
  Erroneous behaviour in primary control functions (pitch, roll, yaw) that is caused by erroneous switching of the modes of operation of NL (Ground Mode, Flight Mode) or by an erroneous activation of a protection function.
- **Failures in the flight control functions (FCF):**
  Erroneous behaviour in primary flight control functions (pitch, roll, yaw) within the limits of the normal flight envelope (see Figure 2-2), where the protection functions are not active.
- **Failures in envelope protection functions (PRT):**
  Erroneous behaviour in primary control functions (pitch, roll, yaw) when a protection function is active and the respective activation conditions are correct.

Figure 2-2 shows the distribution of the functional classification over the flight envelope that is considered for further work in the project to limit the scope of failure cases that shall be investigated for the validation of the *Independent Monitor*. Additionally, all functional failures are primarily considered during the cruise flight phase. The definition of flight phases is given in appendix A.3.

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 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.

All considered functional failures result in a departure from the safe flight envelope. The rectangles indicate the failure starting point in the flight envelope.

The FCF failures are only originated from the normal flight envelope.

The LOG failures are only originated from the normal flight envelope to investigate failure conditions that are caused by erroneous activation of the protections or erroneous mode activation. Failures that are caused by non-activation of protections in the yellow domain are not considered. In these cases, the pilot is responsible for preventing the A/C from reaching the limits of the peripheral flight envelope and returning the A/C to the normal flight envelope. Therefore, the non-activation of a protection function in itself is not hazardous or catastrophic.

The PRT failures are considered from the yellow domain only where the protection functions are correctly activated but are erroneous.

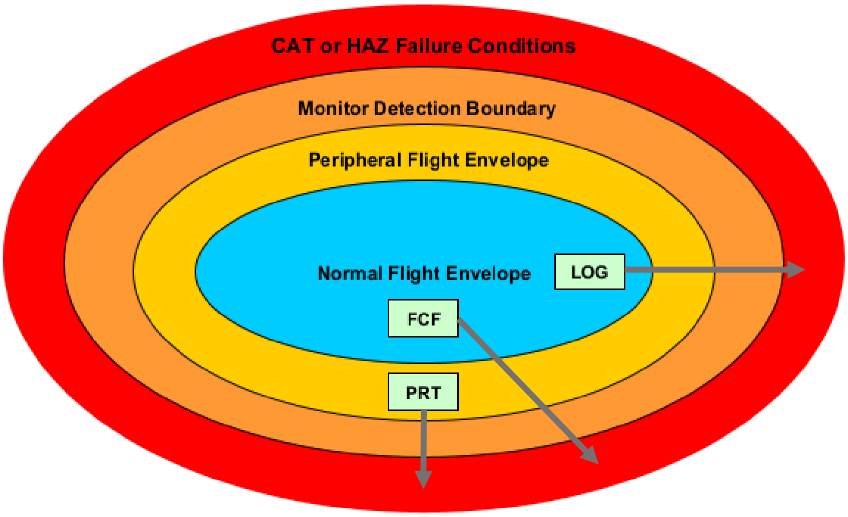

Figure 2-2: Distribution of Functional Classification over the Flight Envelope

2.3.2 Classification Method that Considers the Dependency of a Failure on the Input Signals of the FCL SW

The failures can be classified based on the dependency of the outcome of a failure on the input signals of the FCL SW:

- **active class**
  It comprises 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 (see section A.2).
- **reactive class**
  It comprises 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.

2.3.3 Combination of Classifications Methods

The classes of both methods are combined as designated in Table 2-2. Potential failures that are caused by errors in the VFW614-ATD FCL SW were assigned to the categories that are defined above. Representative examples for each defined subclass are described for the active class (A) in section 3.1 and for the reactive class (R) in section 3.2.

Table 2-2: Combination of Failure Classes

Functional Classes	**Active (A)**	**Reactive (R)**
FCF	A-FCF	R-FCF
LOG	A-LOG	R-LOG
PRT	A-PRT	R-PRT

3 FCL Failure Examples

3.1 Examples of Active FCL Failures

3.1.1 A-FCF

Failure ID	A-FCF-01
Failure Description	Erroneous computation of the elevator command (load factor control)
Category	A-FCF
Outcome	Erroneous elevator command
Potential Consequences	• A/C stalls • Exceedance of maximum structural loads • Ground contact • Hard landing • Reduced pitch control authority

Failure ID	A-FCF-02
Failure Description	Erroneous computation of the aileron command (roll control)
Category	A-FCF
Outcome	Erroneous aileron command
Potential Consequences	• Exceedance of maximum structural loads • Exceedance of maximum roll rate and bank angle • Reduced roll control authority

Failure ID	A-FCF-03
Failure Description	Erroneous computation of the rudder command (yaw control)
Category	A-FCF
Outcome	Erroneous rudder command
Potential Consequences	• Exceedance of maximum structural loads • Exceedance of maximum sideslip angle • Reduced yaw control authority

Failure ID	A-FCF-04
Failure Description	Erroneous pitch trim command computation
Category	A-FCF
Outcome	Erroneous THS command that • First reduces elevator pitch authority and then • Cannot be countered by the elevator The erroneous THS command may build up either slowly (over minutes) or fast (within seconds).
Potential Consequences	• A/C stalls (THS command erroneously nose-up) • Overspeed conditions with exceedance of maximum structural loads during recovery • Exceedance of VNE (THS command erroneously nose-down) • Reduced pitch control authority

3.1.2 A-LOG

Failure ID	A-LOG-01
Failure Description	Erroneous activation of the high AoA protection
Category	A-LOG
Outcome	• Erroneous nose-down elevator command • Erroneous nose-up elevator command if the AoA protection activates at low AoA values below the protection limit
Potential Consequences	• Ground contact if activated at low altitudes during approach • Exceedance of maximum structural loads when activated in at low AoA values below the protection limit • Reduced pitch control authority

Failure ID	A-LOG-02
Failure Description	Erroneous activation of the ground mode in flight
Category	A-LOG
Outcome	• Erroneous elevator command • Loss of auto trim function • Loss of yaw damper function • Loss of turn coordination function
Potential Consequences	• A/C stalls • Exceedance of maximum structural loads, i.e. if the mode change is not annunciated, because all protections are passivated in ground mode

Failure ID	A-LOG-03
Failure Description	Erroneous activation of the ground spoiler function in flight
Category	A-LOG
Outcome	• Extension of the ground spoilers in flight
Potential Consequences	• Exceedance of maximum structural loads • Excessive sink rates

3.1.3 A-PRT

Failure ID	A-PRT-01
Failure Description	Erroneous high-speed protection
Category	A-PRT
Outcome	• Erroneous elevator command
Potential Consequences	• Exceedance of VNE • Exceedance of maximum structural loads • Reduced pitch control authority

Failure ID	A-PRT-02
Failure Description	Erroneous high AoA protection
Category	A-PRT
Outcome	• Erroneous elevator command
Potential Consequences	• Exceedance of maximum structural loads • A/C stalls • Ground contact • Hard landing • Reduced pitch control authority

3.2 Examples of Reactive (R) FCL Failures

The reactive class (R) includes failures that cause an erroneous behaviour that is dependent on the input signals. Therefore, this class includes all failure conditions that are related to unstable control-loops.

3.2.1 R-FCF

Failure ID	R-FCF-01
Failure Description	Erroneous load factor control function
Category	R-FCF
Outcome	• Erroneous short period motion characteristics • Reduced damping
Potential Consequences	• Pilot-induced oscillations • Reduced accuracy of the glideslope tracking during approach • Hard landing • Exceedance of maximum structural loads • Reduced pitch control authority

Failure ID	R-FCF-02
Failure Description	Unstable load factor control
Category	R-FCF
Outcome	• Erroneous elevator command with increasing amplitude (either oscillatory or aperiodic)
Potential Consequences	• A/C stalls • Exceedance of maximum structural loads • Loss of pitch control authority

Failure ID	R-FCF-03
Failure Description	Erroneous computation of the roll model (roll control function)
Category	R-FCF
Outcome	• Erroneous roll motion characteristics (too slow, too agile) • Reduced damping
Potential Consequences	• Exceedance of maximum roll rate or bank angle • Pilot-induced oscillations during fast roll manoeuvres • Reduced manoeuvrability potentially leads to ground contact of the wing tips during approach • Reduced roll control authority

Failure ID	R-FCF-04
Failure Description	Unstable roll control
Category	R-FCF
Outcome	• Erroneous aileron command with increasing amplitude (either oscillatory or aperiodic)
Potential Consequences	• Exceedance of maximum roll rate or bank angle • Exceedance of maximum side slip angle • Exceedance of maximum structural loads • Loss of roll control authority

Failure ID	R-FCF-05
Failure Description	Erroneous yaw damper function
Category	R-FCF
Outcome	• Erroneous Dutch roll characteristics • Reduced damping • Potentially unstable Dutch roll, i.e. during climb/descent
Potential Consequences	• Exceedance of critical structural loads, if pilots try to control the A/C heading by pedal inputs that excite the Dutch roll • Reduced accuracy of the localizer tracking during approach may lead to touchdown out of the touchdown zone

3.2.2 R-LOG

Failure ID	R-LOG-01
Failure Description	Erroneous activation and deactivation of the high AoA protection
Category	R-LOG
Outcome	Alternating activation and deactivation of the high AoA protection at a high frequency
Potential Consequences	• Hard landing • Oscillations in the pitch motion reduce the accuracy of the glideslope tracking during approach • Reduced pitch control authority

Failure ID	R-LOG-02
Failure Description	Erroneous activation and deactivation of the bank angle protection
Category	R-LOG
Outcome	Alternating activation and deactivation of the bank angle protection at a high frequency
Potential Consequences	• Hard landing • Reduced accuracy of the localizer tracking during approach may lead to touchdown out of the touchdown zone • Excitation of aircraft aeroelastic modes • Reduced roll control authority

3.2.3 R-PRT

Failure ID	R-RPT-01
Failure Description	Erroneous high AoA protection
Category	R-PRT
Outcome	• Erroneous AoA control function (too slow, too agile) • Reduced damping
Potential Consequences	• Exceedance of maximum AoA • A/C stalls • Exceedance of critical structural loads • Reduced pitch control authority

Failure ID	R-RPT-02
Failure Description	Erroneous bank angle protection function
Category	R-FCF
Outcome	• Erroneous bank angle command – bank angle hold function (too slow, too agile) • Reduced damping
Potential Consequences	• Exceedance of critical structural loads, if pilots try to control the A/C heading by pedal inputs that excite the Dutch roll • Reduced accuracy of the localizer tracking during approach may lead to touchdown out of the touchdown zone • Reduced roll control authority

Within the Normal Law of the VFW614-ATD FCL, the high-speed protection and the pitch attitude protection are situated on the command path of the FCL. The load factor demand of the pilot is superposed by commands from either the high-speed protection or the pitch attitude protection. The superposed load factor command is limited by the load factor protection. Therefore, failures that are caused by errors in these protection functions do not modify the closed-loop transfer behaviour of the load-factor control function and are consequently classified as active failures.

4 Conclusion

This report proposes a general failure classification instead of a list of specific FCL errors that shall be investigated during validation of the *Independent Monitor*. For the class that considers the dependency of the failures on the FCL SW inputs, investigation of exemplary failure conditions revealed that

- active failures in the FCL lead to actuator-like failures (i.e. runaway), the example simulations described in A.4 confirm this statement,
- reactive failures potentially cause PIOs or dangerous flight conditions that may occur because of the error itself, the crew’s reaction or the current state of flight.

The functional failure classes are considered subclasses of the active and the reactive failure classes. For validation of the *Independent Monitor*, failures shall be investigated in different flight envelope domains depending on its class as proposed in Figure 2-2. In particular, failures that are caused by errors in PRT are similar to failures of the FCF itself but have to be exclusively investigated in the peripheral flight envelope.

The methods for simulation of active and reactive failures differ significantly. Active failures can be triggered by insertion of simple errors into the software. As their effect on the flight controls is similar to actuator-like failures (i.e. runaway), a simplified simulation of these failures by direct manipulation of the FCL output for pitch, roll and yaw control axes is recommended. Although all investigated active failures result in a runaway-like signature on the FCL outputs (see Appendix A.4), it is recommended to additionally investigate oscillatory control surface commands, because their occurrence is possible.

For validation of the *Independent Monitor,* it shall be investigated at which amplitudes, rates or frequencies a runaway or an oscillation of each control surface potentially causes hazardous consequences, e.g. by exceedance of critical structural loads. The selected amplitudes and rates shall be lower or equal than the specified FCL output limits that are usually lower than the mechanical limit of the respective control surface.

To trigger reactive failures, additional methods such as pilot models, pilot experiments, manipulation of FCL SW input signals and enforcement of less-damped control loops shall be used in simulation depending on the defined failure conditions for the specific A/C. Additional manipulation of FCL source code can be necessary.

A Appendix

A.1 Analysis of an Incident and Two Accident Reports proposed by EASA

EASA provided reports of two accidents that are analysed in order to find examples for development errors of the Flight Control Law Software. These accidents are summarised in the following.

A.1.1 Serious Incident of a Falcon 7X Business Jet on a Transfer Flight, [3]

A serious incident occurred during descent to Kuala Lumpur Airport (Malaysia) to the Dassault Falcon 7X (registered HB-JFN) operated by Jet Link AG on May 24th, 2011. An erroneous nose-up command of the trimmable horizontal stabilizer (THS) caused excessive load factors, altitude and airspeed deviations as well as abnormal pitch attitudes. The same soldering defect that caused the THS runaway also disabled the monitor of the THS. Eventually, a temperature monitoring tripped when it detected excessive temperatures because the THS motor continued to operate although the THS had reached its limit. This caused a switch to the redundant correct electronic control that commanded a nose-down movement of the THS until it returned to a trimmed pitch condition.

The safety investigation report [3] concludes:

> *A soldering defect on the pin of a Horizontal Stabilizer Electronic Control Unit (HSECU) component caused the unit to generate incorrect nose-up commands to the motor controlling the trimmable Horizontal Stabilizer (THS) and to transmit to systems in charge of the monitoring of its functioning values indicating a change in the opposite direction to that in which the motor was actually moving. This single defect caused simultaneous failures on the THS control and monitoring channels that were not detected by any of the aircraft systems and were enough to cause THS runaway under normal law*.

The original FMEA did not unambiguously identify this failure condition and did not classify it as hazardous. The safety investigation report does not relate the cause of the incident to an FCL development error.

Nevertheless, the incident provides an example for the limitations of the safety assessment and certification process applied during the development of the aircraft. The architecture of the THS control system allowed a single manufacturing defect to cause a safety-critical failure condition.

The FCL did not command a THS movement. The uncommanded erroneous THS movement should have been detected. However, this failure cannot be attributed to an FCL development error.

Instead, the reason for the THS failure should be searched in deficiencies in the Failure Mode and Effect Analysis as well as in the Common Mode Analysis (CMA) as the BEA recommended to EASA, FAA, SAE and EUROCAE in [3],

- "… *evaluate and propose alternative or additional methods to the FMEA for electronic equipment and software.*"
- "… *develop means or methods that make it possible to consolidate, during safety analyses, checks on the independence of system control and the monitoring of said system.*"

EASA confirms this by its response in [14]: "*the Agency is applying since 2012 a "generic" Certification Review Item "Common Mode Failures and Errors in Flight Control Functions" to enforce the CMA early in the development process and provide specific guidance to the applicant in order to ensure that common mode failures and errors, including related mitigation means, are duly considered in Flight Control Functions."*

A.1.2 Accident of a Leonardo AW609 Tilt Rotor During a Test Flight, [4]

An accident occurred during a planned test flight of the AugustaWestland AW609 experimental tiltrotor-aircraft on 30th of October, 2015. While performing a high-speed descent, the aircraft entered an uncontrolled flying condition, due to a series of lateral-directional oscillations, that were amplified by the pilots attempts to stabilize the aircraft. Then suffered structural breakup followed by in-flight fire and finally impacted the ground.

The safety investigation report [4] concludes:

> *[…] the aerodynamics of the aircraft and the specific test flight conditions in a high speed dive are factors that have created a condition in which the aircraft has developed latero-directional oscillations, subsequently amplified. […] the pilot roll input was counter phase but the control laws [, i.e. turn compensation function,] resulted in an in-phase amplification of the yaw oscillations, making them divergent until the proprotors contacted the respective wings, causing great structural damage followed by an in-flight break-up of the aircraft with subsequent fire.*
>
> *The project simulator […] demonstrated not being able to faithfully reproduce the dynamics occurred during [the accident] flight […]. Therefore, [it] was not really able to properly carry out the role of test bench for the control laws and risk reduction.*

The aerodynamics at the high-speed dive condition were unknown. Therefore, the specification of the FCL was incomplete and did not specify a required behaviour for system safety at this specific flight condition. The turn compensation function, required for normal operations, had unsafe behaviour at the specific flight condition, leading to an amplification of the oscillations when the pilot tried to counteract them.

The accident is a good example for an incorrect (unsafe) requirement or incomplete specification. However, almost no information on FCL development errors can be deduced from the accident report. Only the effects of the FCL development error are described. The resulting failure condition can be classified as R-FCF failure.

A.1.3 Accident of a Bell 525 Helicopter during a Test Flight [5]

An accident occurred during a planned test flight of an experimental research and development Bell 525 helicopter on 6th of July, 2016. During a single engine failure flight test at high airspeed, the helicopter rotor rotation speed decay was arrested but not restored, inducing unexpected cabin vibrations. These vibrations were amplified by a biomechanical and attitude heading reference system feedback, resulting in an in-flight breakup and total loss of the aircraft.

The safety investigation report [5] concludes that the probable causes were:

> *A severe vibration of the helicopter that led to the crew's inability to maintain sufficient rotor rotation speed (Nr), leading to excessive main rotor blade flapping, subsequent main rotor blade contact with the tail boom, and the resultant in-flight breakup. Contributing to the severity and sustainment of the vibration, which was not predicted during development, were (1) the collective biomechanical feedback and (2) the attitude and heading reference system [(AHRS)] response, both of which occurred due to the lack of protections in the flight control laws against the sustainment and growth of adverse feedback loops when the 6-hertz airframe vibration initiated. Contributing to the crew's inability to maintain sufficient Nr in the severe vibration environment were (1) the lack of an automated safeguard in the modified one-engine-inoperative software used during flight testing to exit at a critical Nr threshold and (2) the lack of distinct and unambiguous cues for low Nr.*

In this accident a biomechanical and AHRS feedback caused an unanticipated amplification of the main rotor scissors mode, resulting in the main rotor severing the tail boom and finally in-flight breakup.

The accident is a good example for an incomplete specification of FCL. However, almost no information on FCL development errors can be deduced from the accident report. Only the effects of the FCL development error are described. The resulting failure condition can be classified as an R-FCF failure.

A.2 Actuator Failure Conditions

A.2.1 Unlimited Runaway

The unlimited runaway failure condition (also called hard over) is a failure condition when the control surface deflects in one specific direction up to the maximum or minimum deflection angle (end position). It extends to the mechanical limit with the maximum deflection rate.

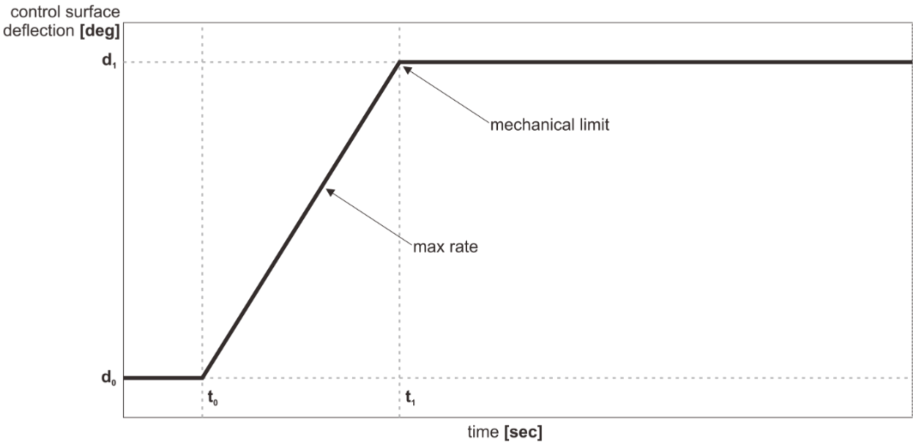

Figure 4-1: Illustration of failure condition: unlimited runaway

The unlimited runaway failure condition begins at t_0. The deflection for this condition starts at d_0, which is a commanded or trimmed condition according to the flight phase condition and stops at d_1, which is the maximum control surface deflection and identified as the mechanical limit for the control surface. The maximum control surface deflection can be in the positive or negative direction. The control surface deflects from d_0 to d_1 with the maximum available rate depending on actuator characteristics and the aerodynamic hinge moment of the control surface.

A.2.2 Transient Runaway

The transient runaway failure condition is a failure condition when the control surface deflects uncontrolled in one specific direction up to a specific deflection angle below the mechanical limit. The failure is then detected, the failed control element is isolated, the control element may float before it is controlled appropriately again. Figure 4-2 illustrates this failure condition.

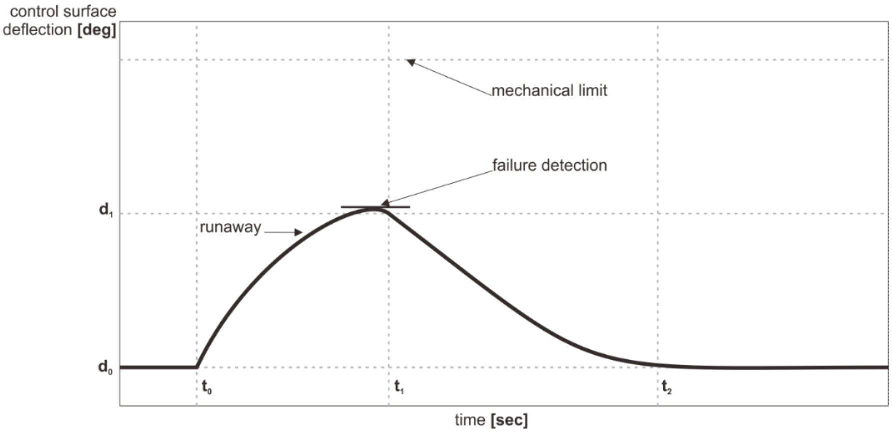

Figure 4-2: Illustration of failure condition: transient runaway

The transient runaway failure condition begins at t_0. When the control surface has reached the deflection d_1 at t_1, the control surface moves towards the deflection d_0 that is commanded by the EFCS. It is assumed that the deflection d_1 is smaller than the limit for excessive local structural loads. The time t_1 is when the failure has been detected, and the correct control is retrieved. At t_2 the control surface has reached the commanded deflection again.

A.2.3 Offset

An offset failure condition is a failure conditions when the control surface is deflected with an offset value relative to correct command. Figure 4-3 illustrates the offset failure condition.

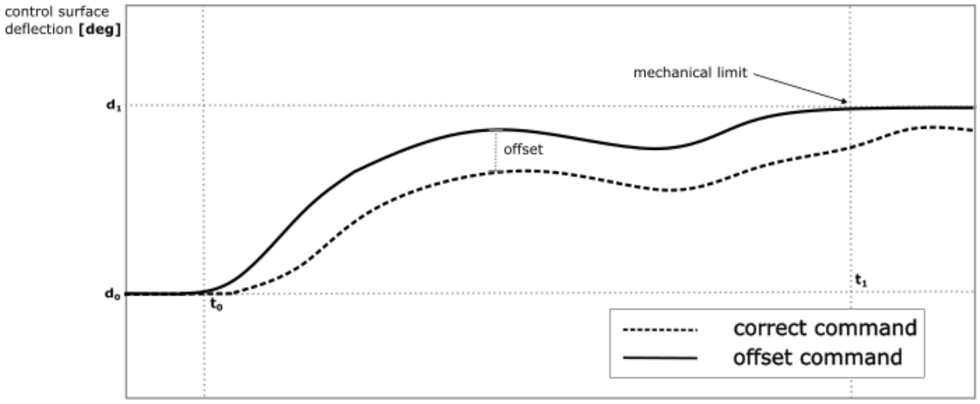

Figure 4-3: Illustration of failure condition: Offset

The offset failure condition begins at t_0 when an offset value occurs. This offset can reduce the margin to the deflection limit. At t_1 the mechanical limit d_1 is reached and the control authority is reduced.

A.2.4 Overlaid Oscillation

An overlaid oscillation is added to the commanded deflection. The describing parameters for the overlaid oscillation are the amplitude and the frequency. Figure 4-4 illustrates this failure condition.

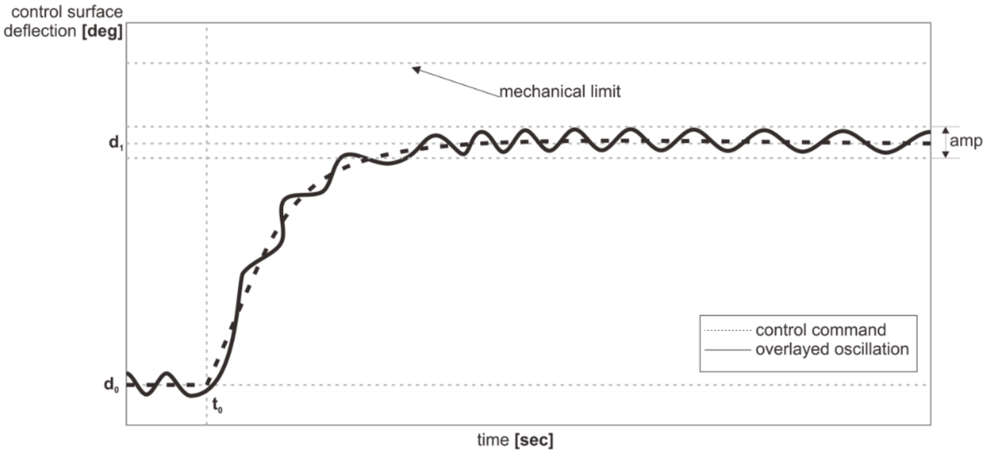

Figure 4-4: Illustration of failure condition: overlaid oscillation

Assumptions for this failure condition:

- Amplitude: < 10% of full control surface deflection value. Frequency: 0.1 – 10 Hz
- The critical natural frequencies of the aircraft structure are within the range of 2 – 6 Hz.

A complete assessment by flight simulation requires a flexible aircraft dynamical model to supplement the FMM by a model of the aeroelastic dynamics.

A.2.5 Jamming

The jamming failure condition is a failure condition when the control surface becomes inoperative and stops at a certain deflection angle.

Figure 4-5 illustrates this failure condition.

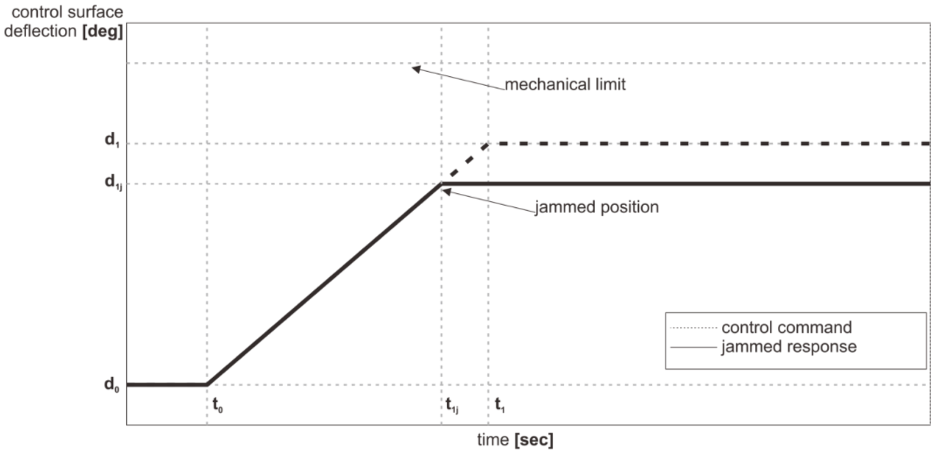

Figure 4-5: Illustration of failure condition: jamming

The control command starts at t_0, and shall reach the commanded control surface deflection d_1 at t_1. At time t_{1j} it jams at position d_{1j}.

A.2.6 Floating

The control surface deflects freely, driven by external forces acting on it (e.g., aerodynamic forces). Figure 4-6 illustrates this failure condition.

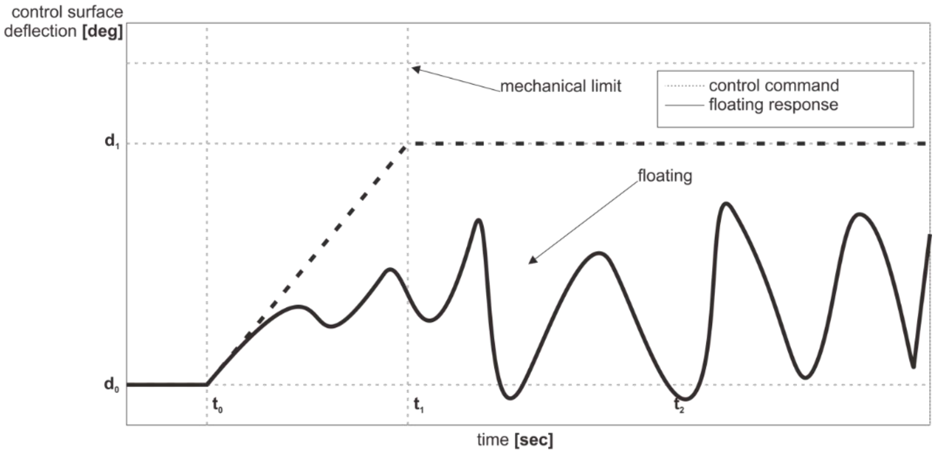

Figure 4-6: Illustration of failure condition: floating

A.3 Flight Phase Classification

The analysis and hazard assessment are performed for flight phase groups that pose similar risks to the aircraft. Based on the similarity of the flight conditions, the flight phases are classified as follows:

1. Ground and near ground (**GNG**): Altitude is < 15 ft (4.6 m),
2. Low altitude (**LA**): Altitude is between 15 feet (4.6 m) and MRA,
3. Standard Mission (**SM**): Altitude is > Minimum Reception Altitude (MRA),
    a. Climb (CLB): Altitude is > MRA and during the climb,
    b. Transit (TRA): Altitude is > MRA, and during transit,
    c. Cruise (CRS): Altitude is > MRA, and during cruise,
    d. Descent (DES): Altitude is > MRA, and during descend,
    e. Holding (HLD): Altitude is > MRA, and during holding,
    f. Landing (LND): Altitude is > MRA and during landing.

4. **ALL** stands for all flight phases.

Table 4-1 lists all defined flight phases.

Table 4-1: Flight Phase Definition

Flight Phase Definition		Description
N/A		Pre-Flight (Service/Planning)
		Pre-Flight (Service/Planning)
		Pre-Flight (Tow to runway)
		Pre-Flight (Start-Up Engines)
		Post-Flight (Shut-Down Engines
		Post-Flight (Tow to Hangar)
		Post-Flight (Shut-Down Systems)
GNG		Take-Off (Roll)
		Take-Off Climb (to T/O Rejection Point)
		Take-Off (Rejected Take-Off)
LA		Initial Climb to MRA
SM	CLB	Flight (Climb)
	TRA	Flight (Transit)
	CRS	Flight (Cruise)
	DES	Flight (Descent)
	HLD	Flight (Holding)
	LND	Landing (Final Approach to MRA)
LA		Landing (Final Approach)
GNG		Landing (Roll-Out)
		Landing (Go-Around)

A.4 Simulation examples of active failures

To investigate the characteristics of active failures, several exemplary errors are included in the FCL SW. A mechanism to systematically include errors in the FCL SW is not yet developed and the means may change in the future. Table 4-2 lists the conducted simulations and the corresponding failure that is defined in 3.1. The errors are directly incorporated into the FORTRAN source code of the FCL SW by simple means such as

- inverting signs of signals or gains,
- manipulating threshold values of mode switches,
- inverting or manipulating limit values,
- manipulating combinatory logic,
- adding offsets to signals.

A simulation that is conducted in the desktop flight simulation *FSEnv* is uniquely identified by its trim point identifier (TPid) and its test scenario identifier (TSid) [6]. The corresponding time histories are generated by the tool TUBPlot [6] with the signal identifier definitions that are listed in A.5.

In all simulations

- the FCL are initialized into the Direct Law,
- the erroneous Normal Law is activated after 1 second,
- the A/C is initialized in a trimmed state of flight,
- no pilot inputs are required to trigger the failure,
- environmental conditions are constant and do not influence the failure characteristics.

Investigation of the time histories for the errors #1 through #6 reveals that

- each failure directly influences the elevator deflections (`ETRH, ETLH`) after activation of the erroneous function of the Normal Law without any pitch axis input by the pilot (`SSPICPT`),
- the failures arising from error #1 and #3 result in a runaway of the elevator and #1 results in the worst-case-scenario with a load-factor n_z up to -4 g that exceeds the structural load limits of the A/C,
- the failures arising from error #2, #4 and #5 result in an initial runaway of the elevator that is overlain by the reaction of the AoA-protection after around 1 s. However, for error #4 and #5 the initial runaway results in a load-factor n_z of more than 4 g that exceeds the structural load limits of the A/C,
- the error #6 manifests itself after the high-speed protection gets active after 20 s (`HISPDPROT`), the initial reaction is a positive elevator deflection without any pitch axis input by the pilot. The positive elevator deflection results in a pitch-down response of the A/C and consequently in a further increasing airspeed above VNE after 25 s.

Table 4-2 Exemplary simulations of active failures

Error ID	TPid	TSid	Failure	Error source in FCL SW	Time History
1	325	851	A-FCF-01	Limitation of the elevator command	LINK
2	325	852	A-FCF-01	Computation of n_z demand from stick input	LINK
3	325	853	A-FCF-01	Limitation of the superposed n_z demand	LINK
4	325	854	A-FCF-01	Turn compensation	LINK
5	523	855	A-LOG-01	Combinatory logic for activation of the AoA protection	LINK
6	934	856	A-PRT-01	Computation of n_z demand of the high-speed protection	LINK

The investigation of simulation examples confirms the initial assumption that active failures manifest themselves by a runaway-like signature at the control surface deflection commands and consequently at the control surface deflections. Depending on the error source, the type of error and the flight condition, the runaway-like signature varies in amplitude or rate and can result in catastrophic or hazardous consequences. The runaway may be overlain by a reaction of other functions of the FCL SW, e.g. a protection function. However, over all investigated examples, an initial runaway of a control surface is present.

During investigation of the active failure characteristics, no oscillations were observed. However, it seems possible that an active failure can manifest itself by an oscillatory signature at the control surface deflection commands.

A.5 Mapping from *FSEnv* signals to TUBPlot signal alias list

Value name	Unit	alias	computed	Bus
`p_f_rads`	rad/s	PR		bu_x_y
`q_f_rads`	rad/s	QR		bu_x_y
`r_f_rads`	rad/s	RR		bu_x_y
`r8time`	s	r8time		r8time
`n_x`	g	NXFRAW		bu_x_y
`n_x_corr`	g	NXF	n_x*(-1)	bu_x_y
`n_y`	g	NYFRAW		bu_x_y
`n_y_corr`	g	NYF	n_y*(-1)	bu_x_y
`n_z`	g	NZFRAW		bu_x_y
`n_z_corr`	g	NZF	n_z*(-1)	bu_x_y
`alpha_aero_rad`	rad	AL		bu_Umg
`beta_aero_rad`	rad	BE		bu_Umg
`Phi_rad`	rad	PH		bu_x_y
`Theta_rad`	rad	TH		bu_x_y
`Psi_rad`	rad	PS		bu_x_y
`Hoehe_m`	m	HMSL		bu_x_y
`gamma_rad`	rad	GA		bu_x_y
`chi_rad`	rad	CH		bu_x_y
`V_aero_ms`	m/s	VTAS		bu_Umg
`V_K_ms`	m/s	VK		bu_x_y
`CAS_kts`	kt	VCAS		bu_Sens
`Baro_Altitude_ft`	ft	HBAR		bu_Sens
`u_Wind_g_ms`	m/s	UWG		bu_Umg
`v_Wind_g_ms`	m/s	VWG		bu_Umg
`w_Wind_g_ms`	m/s	WWG		bu_Umg
`u_Wind_f_ms`	m/s	UWF		bu_Umg
`v_Wind_f_ms`	m/s	VWF		bu_Umg
`w_Wind_f_ms`	m/s	WWF		bu_Umg
`Druck_stat_Nm2`	Pa	PSTAT		bu_Umg
`Staudruck_Nm2`	Pa	PTOT		bu_Umg
`Pos_Nord_rad`	rad	LAT		bu_x_y
`Pos_Ost_rad`	rad	LON		bu_x_y
`Machzahl`	-	MA		bu_Umg
`Pos_Trimmung_HR_rad`	rad	IH		bu_Sub

Value name	Unit	alias	computed	Bus
Pos_Hoehenruder_1_rad	rad	ETLH		bu_Sub
Pos_Hoehenruder_4_rad	rad	ETRH		bu_Sub
SSPI_CPT	-	SSPICPT		bu_Pilot
SSPI_FO	-	SSPIFO		bu_Pilot
PED	-	PED		bu_Pilot
Pos_Seitenruder_1_rad	rad	ZE		bu_Sub
SSRO_CPT	-	SSROCPT		bu_Pilot
SSRO_FO	-	SSROFO		bu_Pilot
Pos_Querruder_1_rad	rad	XIIL		bu_Sub
Pos_Querruder_6_rad	rad	XIIR		bu_Sub
N1_TW1	%	N1L		bu_TW
N2_TW1	%	N2L		bu_TW
N1_TW2	%	N1R		bu_TW
N2_TW2	%	N2R		bu_TW
Schubhebel_TW1_rad	rad	RTLPL		bu_Pilot
Schubhebel_TW2_rad	rad	RTLPR		bu_Pilot
Schub_TW1_N	N	FN1		bu_TW
Schub_TW2_N	N	FN2		bu_TW
Pos_Klappen_1_rad	rad	FLGR		bu_Sub
Konfiguration	-	FLSLCD		bu_Pilot
Pos_Spoiler_2_rad	rad	SPIL		bu_Sub
Pos_Spoiler_15_rad	rad	SPIR		bu_Sub
Pos_Spoiler_1_rad	rad	SPEL		bu_Sub
Pos_Spoiler_16_rad	rad	SPER		bu_Sub
HGND	m	HRA		bu_x_y
Distance_RWY_Origin_m	-	DFLA		bu_ILS
Glideslope_Dev_dot	-	GDEV		bu_ILS
Localizer_Dev_dot	-	LDEV		bu_ILS
Localizer_Reception	-	LSIGNL		bu_ILS
Glideslope_Reception	-	GSIGNL		bu_ILS
WGS	°	WGS		WGS
PSIL	°	PSIL		PSIL
ELLHFAIL	-	ELLHFAIL		ELLHFAIL
ELRHFAIL	-	ELRHFAIL		ELRHFAIL
Position_FW	-	LG		bu_FW
w_Kg_ms	m/s	VKG3RAW		bu_x_y
w_Kg_ms_corr	m/s	VKG3	w_Kg_ms*(-1)	bu_x_y
L116P10NV1	-	HISPDPROT		bu_Regler
L120P1NV04	-	LOSPDPROT		bu_Regler
L117NV01	-	HITHPROT		bu_Regler

Value name	Unit	alias	computed	Bus
L117NV02	-	LOTHPROT		bu_Regler
L117NV03	-	THPROT		bu_Regler
L215NV01	-	PHPROT		bu_Regler
LNORMAL	-	LNORMAL		bu_Regler
IHC_DL	°	IHC_DL		bu_ATD_PFCL_debug
ETC_DL	°	ETC_DL		bu_ATD_PFCL_debug
IHC_NL	°	IHC_NL		bu_ATD_PFCL_debug
ETC_NL	°	ETC_NL		bu_ATD_PFCL_debug
XICRH_DL	°	XICRH_DL		bu_ATD_PFCL_debug
XICLH_DL	°	XICLH_DL		bu_ATD_PFCL_debug
XICRH_NL	°	XICRH_NL		bu_ATD_PFCL_debug
XICLH_NL	°	XICLH_NL		bu_ATD_PFCL_debug
ZEC_DL	°	ZEC_DL		bu_ATD_PFCL_debug
ZEC_NL	°	ZEC_NL		bu_ATD_PFCL_debug
dETC	°	dETC		bu_ATD_PFCL_debug
dXICR	°	dXICR		bu_ATD_PFCL_debug
dZEC	°	dZEC		bu_ATD_PFCL_debug
dETCstar	°	dETCstar		bu_ATD_PFCL_debug
dXICRstar	°	dXICRstar		bu_ATD_PFCL_debug
dZECstar	°	dZECstar		bu_ATD_PFCL_debug