Towards Certifiable Fault-Tolerant Actuation Architectures for UAVs

C. Bosch, M. A. A. Ismail, S. Wiedemann, and M. Hajek

Abstract There is an increasing demand for integrating unmanned aerial vehicles (UAVs) into civilian airspaces. Consequently, onboard systems should be evaluated for possible threats to human life. This paper discusses future certification requirements for flight control actuators. A scheme is proposed for evaluating reliability requirements for flight control electro-mechanical actuators (EMAs) considering different flight control configurations. This work is part of the TEMA-UAV project, which aims at developing certifiable fault-tolerant actuation for future UAVs.

Keywords Electro-mechanical actuators · Airworthy certification · Fault-tolerant architectures

1 Introduction

Unmanned aerial vehicles (UAVs) are mainly used in leisure products and in military applications. However, due to the continuous technological advancements of electro-mechanical actuators (EMAs), power electronics and controllers [1], as well as their availability at lower costs, a recent study [2] predicts increased demand for UAVs in the next 30 years. Future UAV operation scenarios include not only government authority missions, such as border security, maritime surveillance, and military actions, but also their use for delivery purposes, medical supply, fire-fighting, and agriculture. However, the increasing interest in medium-sized UAVs demands

C. Bosch (✉) · M. Hajek
Institute of Helicopter Technology, Technical University of Munich, Arcisstraße 21, 80333 Munich, Germany
e-mail: Colin.Bosch@tum.de

M. A. A. Ismail
Institute of Flight Systems, DLR (German Aerospace Center), Lilienthalplatz 7, 38108 Brunswick, Germany

S. Wiedemann
MACCON Elektroniksysteme GmbH, Aschauer Str. 21, 81549 Munich, Germany

L. Gelman et al. (eds.), *Advances in Condition Monitoring and Structural Health Monitoring*, Lecture Notes in Mechanical Engineering,
https://doi.org/10.1007/978-981-15-9199-0_33

new certification requirements, including their onboard systems and utilised actuation architectures. This paper focuses on future flight control EMAs and proposes a scheme to evaluate reliability requirements of such a system in consideration of different flight control configurations.

2 UAV Safety Requirements Review

2.1 European Aviation Safety Agency Civil Rulemaking and SC-RPAS.1309

Currently, aviation authorities focus on creating a regulatory basis for UAV safety and certification. Resulting from this dynamic rulemaking, systems manufacturers are often required to anticipate aspects of certification before applicable regulations have been published. Following several review phases, the European Aviation Safety Agency (EASA) recently published regulations (EU) 2019/947 [3] and 2019/945 [4] describing top-level safety targets for manufacturers and operators, considering three different UAV risk categories: *open* (takeoff weight < 25 kg), *specific* and *certified*. The *open* category aims at low-risk operations and is not the focus of this discussion. The other categories represent two different approaches to UAV certification:

1. Operations within the *specific* category demand an operational risk assessment in which the operator assesses the mission risk or shows conformity with *standard scenarios*. Due to geographical or temporal UAV operation, we regard this as a mission-based certification [3, 4].
2. A certification similar to that needed for manned aviation might be required for the *certified* category. UAVs being operated over assemblies of people and exceeding a characteristic dimension of 3 m are subject to this category [4]. While EASA has not published Certification Specifications for UAVs yet, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) proposed CS-LURS (rotorcraft) [5] and CS-LUAS (fixed-wing) [6], both providing regulations for UAVs lighter than 750 kg. Furthermore, the Schiebel S-100 UAV, which has a takeoff weight of 200 kg, was given *special conditions* based on CS-LURS as a certification basis [7].

For type certification, aircraft development should follow a top-down approach, which is extensively described in guidelines ARP4754 (system development) [8] and ARP4761 (safety assessment) [9]. The first step consists of a structured investigation of potential functional failure conditions on aircraft level, also referred to as functional hazard assessment (FHA). It requires information about criticalities and their accepted quantitative probabilities. Both CS-LURS and CS-LUAS reference AMC RPAS.1309. In 2015, EASA proposed *Special Conditions* SC-RPAS.1309-01 for UAVs lighter than 750 kg [10]. As depicted in Table 1, higher probabilities are acceptable than in manned aviation [8]. In addition, SC-RPAS.1309 accepts a loss of

Table 1 Acceptable UAV risk for SC-RPAS.1309 [10]

Failure condition classification	NSE	MIN	MAJ	HAZ	CAT
Allowable quantitative probabilities [h^{-1}]	–	10^{-3}	10^{-4}	10^{-5}	10^{-6}
Design assurance level (DAL)	–	D	C	C	B

NSE No safety effect, MIN Minor, MAJ Major, HAZ Hazardous, CAT Catastrophic

Table 2 Acceptable UAV risk according to STANAG 4671 [11]

Failure condition classification	NSE	MIN	MAJ	HAZ	CAT
Allowable quantitative probabilities [h^{-1}]	–	10^{-3}	10^{-4}	10^{-5}	10^{-6}

vehicle as hazardous "where it can be reasonably expected that multiple fatalities will not occur" [10]. The specified design assurance levels (DALs) also show a reduction compared to manned aviation [8, 10].

2.2 Military Regulations

Military certification of UAVs often follows STANAG 4671. This standard provides airworthiness requirements for UAVs with takeoff weights between 150 and 20,000 kg. Table 2 denotes accepted probabilities [11].

2.3 Consequences for TEMA-UAV Requirements

Sections 2.1 and 2.2 show that

- UAVs exceeding characteristic dimensions of 3 m are likely to be subject to a structured type certification process following new EASA regulations.
- STANAG 4671 and SC-RPAS.1309 represent very similar safety and probability requirements.

The Use Cases considered for TEMA-UAV (see Sect. 4) are in the same size range as the Schiebel S-100 aircraft. Both the S-100 planned EASA certification efforts and the Use Cases' dimensions (>3 m) undermine the decision to plan for a regular type certification. We regard this as a worst-case scenario in case the operator's concept of operations is not eligible for the *specific* category.

3 A Scheme for Evaluating Flight Control Actuation Architectures

Certification requirements are usually described in terms of high-level safety constraints. A transition to low-level reliability constraints is achievable by evaluating possible functional deficiencies for a given flight control architecture. We propose a scheme for evaluating these requirements for flight control EMAs, as shown in Fig. 1. The top-level stage is related to safety objectives that are defined by certification regulations for UAVs flying in non-segregated airspace. This FHA process, as already mentioned in Sect. 2, requires respective UAV criticality and occurrence information (e.g. [10, 11]) on a design-independent level.

For a UAV use case, we define a flight controls layout comprising the number of control surfaces for primary flight control. Applying safety requirements to flight control levels requires a specific flight controls layout. For example, a total loss of the pitch control has a catastrophic effect on UAV level. The accepted probability of failure may increase if the flight controls layout for the pitch function consists of duplex actuation channels. The outcomes of FHA involve qualitative and quantitative conditions for a candidate fault tolerant control (FTC) architecture. The qualitative conditions ensure that no single point of failure can conflict with safety-critical

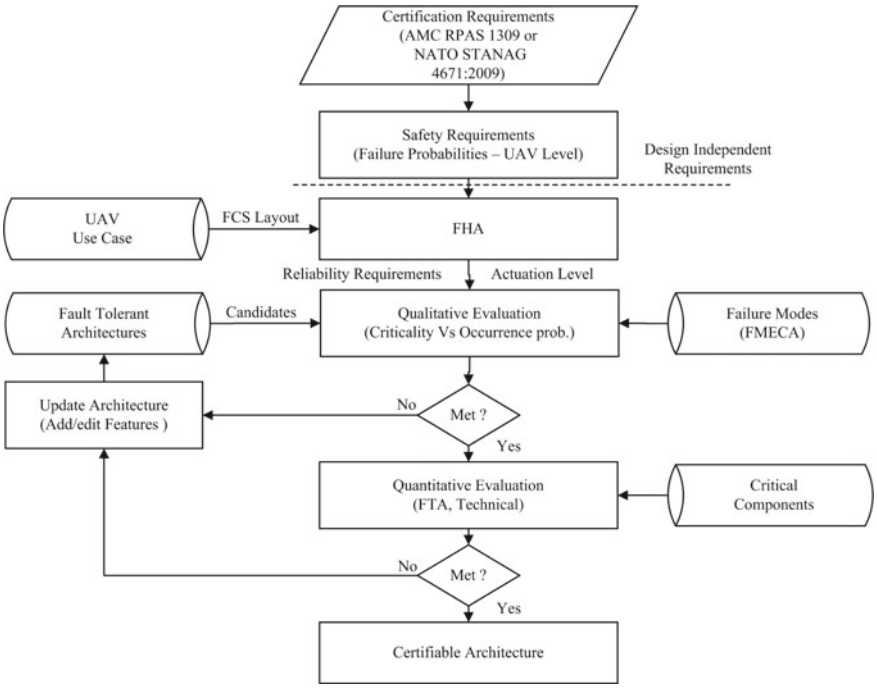

Fig. 1 A scheme for evaluating flight control actuation architectures

actuation functions. The quantitative conditions define the required failure rates for a candidate FTC architecture to be consistent with certification regulations.

For UAV design, we discuss a candidate FTC architecture fulfilling necessary functional and operational requirements, such as flight control computers, actuators, and fault-tolerant features. In order to point out potential failure modes for fault detection and reconfiguration methods for a candidate FTC architecture, qualitative conditions from the FHA are evaluated by failure modes, effects and criticality analysis (FMECA). Failures can be mitigated by FTC features, (e.g. redundancy) or by maintenance inspections. Quantitative conditions from FHA are evaluated by fault tree analysis (FTA) to ensure that all safety-critical failure modes have a probability of occurrence lower than the threshold determined by the FHA. To be considered certifiable, it could be necessary to update candidate FTC architectures by adding or editing FTC features.

4 Use Case Analysis

Di Rito, Galatolo and Schettini performed an aircraft FHA for a fixed wing configuration [12]. By extending their methodology for different aircraft configurations, we can analyze design-specific actuation system criticalities. For that purpose, we regard several UAV use cases to derive respective safety requirements for the system level. Figure 2 illustrates the integration of different use cases in the ARP development processes.

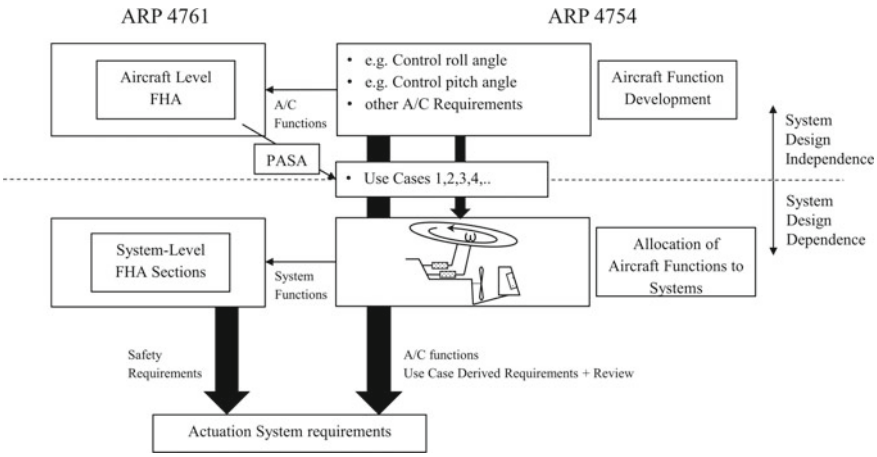

Fig. 2 Use case evaluation in accordance with ARP development and safety processes [8]

Table 3 Example of a simplified fixed-wing FHA (RMT: Remote)

FHA function	Failure cond.	Possible failure effect	Class./Pr.
Control roll	Loss of roll	May result in uncontrollable flight state	CAT/10^{-6} h^{-1}
	Erroneous roll	Erratic roll inputs result in uncontrollable flight state	CAT/10^{-6} h^{-1}
	Partial err. roll	Limited control might help fly to a safe crash site	HAZ/10^{-5} h^{-1}
Control pitch	Loss of pitch	May result in uncontrollable flight state	CAT/10^{-6} h^{-1}
	Erroneous pitch	Erratic pitch inputs result in uncontrollable flight state	CAT/10^{-6} h^{-1}
	Partial err. pitch	Limited control might help fly to a safe crash site	HAZ/10^{-5} h^{-1}
Control yaw	Loss of yaw	In crosswinds, the workload on the RMT crew increases	MAJ/10^{-4} h^{-1}
	Erroneous yaw	Erratic yaw inputs result in uncontrollable flight state	CAT/10^{-6} h^{-1}
	Partial err. yaw	Limited yaw control may help fly to a safe crash site	HAZ/10^{-5} h^{-1}

4.1 Aircraft FHA

Top-level failure conditions are dealt with in an aircraft FHA [9], in which we consider different aircraft configurations while neglecting the specific flight control layout. We regard three separate FHAs (fixed-wing, rotorcraft and gyrocopter). For every function, respective failure conditions are assessed for their criticality. Table 3 depicts a simplified example for a fixed-wing UAV.

4.2 Use Case Definition

According to the *Unmanned Vehicles Handbook*, fixed-wing UAVs had the biggest share (≈65–70%) of production and development UAVs in the year 2008, followed by rotorcraft configurations with a share of ≈20% [13]. To represent this, we examine three fixed-wing flight control architectures and one rotorcraft application. Following previous work by Bierig et al., a generic gyrocopter architecture is also included in this analysis [14]. Figure 3 depicts Use Cases 1–5. The fixed wing Use Cases (1–3) differ in the number of respective control surfaces for roll, pitch and yaw and were derived from existing UAV examples. Use Case 4 features a classic main/tail rotor configuration, while Use Case 5 describes a gyrocopter flight control architecture.

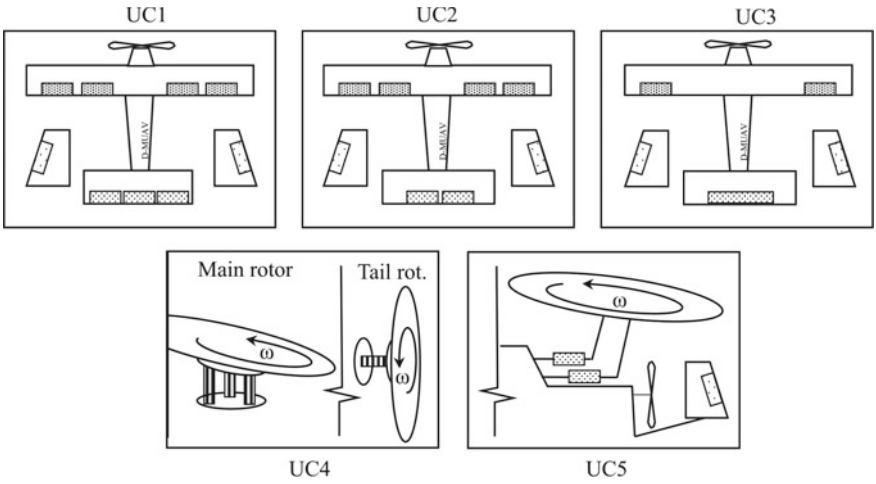

Fig. 3 Use Cases 1–5 (control surfaces and actuation legs are marked as dotted rectangles)

4.3 Derivation of Safety Requirements/Preliminary Aircraft Safety Assessment (PASA)

Following the use case definition, we can derive quantitative and qualitative requirements. For this analysis, several assumptions are required. For Use Cases 1–3 we propose:

- One actuation leg per control surface
- For pitch and roll: the FHA failure condition *erroneous* is applicable if at least 50% of control surfaces of the respective axis have failed. If less than 50% of surfaces have failed, we assume a *partial erroneous* state. The failure condition *loss* is assessed as catastrophic on aircraft level, but this does not need to be discussed here because surfaces would need to fail in a specific way (free floating), which induces less strict reliability requirements for the system level.
- For yaw: the FHA failure condition *erroneous* is applicable, if more than 50% of control surfaces have failed. If ≤50% of surfaces have failed, we assume a *partial erroneous* state.

In the following analysis, we use Boolean logic to develop the actuation level required probabilities (λ_{ACT}) necessary to meet the top-level target. Table 4 shows an example for Use Case 2. For reasons of clarity, only most critical failures are shown.

For Use Case 4 we assume:

- Any failure of the tail rotor actuation is considered *erroneous* and *loss* on aircraft level.

Table 4 Preliminary aircraft safety assessment/actuation requirements derived from aircraft FHA (Use Case 2)

FHA function	FHA failure condition	Failed surfaces	Actuation requirement equation
Control roll	Erroneous roll	2 of 4 ailerons	$6 \cdot \lambda_{ACT}^2 \leq 10^{-6}h^{-1}$
	Partial erroneous roll	1 of 4 ailerons	$4 \cdot \lambda_{ACT} \leq 10^{-5}h^{-1}$
Control pitch	Erroneous pitch	1 of 2 elevators	$2 \cdot \lambda_{ACT} \leq 10^{-6}h^{-1}$
	Partial erroneous pitch	_____	_____
Control yaw	Erroneous yaw	2 of 2 rudders	$\lambda_{ACT}^2 \leq 10^{-6}h^{-1}$
	Partial erroneous yaw	1 of 2 rudders	$2 \cdot \lambda_{ACT} \leq 10^{-5}h^{-1}$

– If at least one of the swashplate actuation legs fails, both top-level failure conditions *erroneous* and *loss* are triggered.

For use case 5:

– If one of both actuation legs fails, both top-level failure conditions *erroneous* and *loss* are triggered.
– Any failure of the rudder actuation leg is considered *erroneous* and *loss* on aircraft level.

4.4 PASA Results

Figure 4 illustrates specific actuation requirements for previously defined use cases for critical failure conditions. The strictest requirements can be found in the swashplate actuation of Use Case 4 and the rotor disk actuation of the gyrocopter application, while average budgeted failure rates are slightly higher in fixed-wing applications. For Use Cases 1–3, a reduced number of control surfaces increases the failure rate budget per surface if the same respective aircraft FHA failure condition is triggered.

4.5 Consequences for TEMA-UAV

For the development of a prototype actuator, which is part of TEMA-UAV, we selected the rotor disk actuation of Use Case 5 for the following reasons. Firstly, there is a relatively low failure budget for the rotor disk actuation. Secondly, knowhow from other DLR projects and the possibility for prototype testing at DLR are crucial [14]. A design-specific system FHA for this use case is depicted in Table 5.

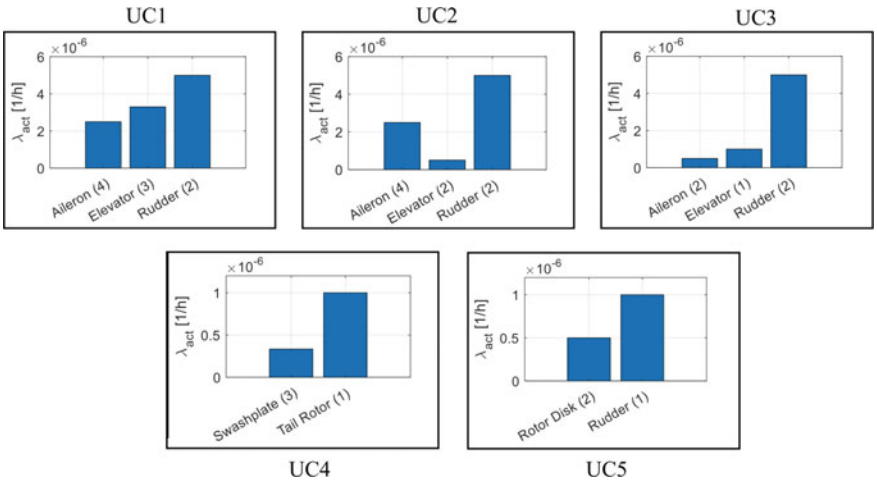

Fig. 4 Failure rate requirement for one actuation leg λ_{ACT} for Use Cases 1–5 (number of legs in brackets)

Table 5 System FHA excerpt for one actuation leg of the rotor disk (Use Case 5)

Function	Failure condition	Failure effect	Class./$\lambda_{ACT,req}$
Command actuation leg	Erroneous actuation	Erratic roll/pitch inputs cannot be compensated	CAT/5•10^{-7} h^{-1}
	Loss of actuation	Lost control of flight attitude	CAT/5•10^{-7} h^{-1}

As part of the actuation requirements specification, the system FHA creates the basis for the subsequent preliminary system safety assessment (PSSA) to investigate different actuator architectures.

5 Conclusion

Although certification specifications have not been published yet, the probabilities and DALs discussed in Sect. 2 represent the most important safety requirements for aircraft level. For UAVs exceeding a size of 3 m, we recommend concentrating on a full type certification. The use case analyses illustrated the strong dependency between aircraft failure conditions and qualitative and quantitative safety requirements on actuation level, which depend on the system design. The analyses also emphasized that the actuation legs of fixed-wing configurations might have a less strict probability requirement than those of rotorcraft configurations. In a rotorcraft or gyrocopter UAV, every described actuation leg is needed for safe continuation of flight. In this work, actuation requirements are insensitive to specific reliability data.

However, at a later stage, knowledge about component failures will be required to assess specific architectures, which can fulfill the budget determined in this paper.

Acknowledgements This work is supported by the TEMA-UAV project through the German National Aerospace Research Program (Lufo V-3).

References

1. Ismail MAA, Bosch C, Wiedemann S, Windelberg J (2019, under publication) Fault tolerant actuation architectures for UAVs. In: WCCM 2019, Singapore, 2–5 December 2019
2. European Drones Outlook Study—Unlocking the value for Europe (2016) SESAR, Brussels, November
3. Commission Implementation Regulation (EU) 2019/947, EASA, Brussels, 24 May 2019
4. Commission Delegated Regulation (EU) 2019/945, EASA, Brussels, 12 March 2019
5. Certification Specification for Light Unmanned Rotorcraft Systems (CS-LURS), JARUS, 30 October 2013
6. Recommendations for Certification Specification for Light Unmanned Aeroplane Systrems (CS-LUAS), JARUS, November 2016
7. Special Condition for EASA Type Certification Base – Camcopter S-100c RPAS, EASA, 09 July 2016
8. Guidelines for Development of Civil Aircraft and Systems, SAE ARP4754, November 1996
9. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE ARP4761, December 1996
10. Special Condition—Equipment, Systems, and Installation, SC-RPAS.1309-01, 24 July 2015
11. Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR), STANAG 4671, September 2009
12. Di Rito G, Galatolo R, Schettini F (2016) Self-monitoring electro-mechanical actuator for medium altitude long endurance unmanned aerial vehicle flight controls. Adv Mech Eng 8(5):1–11
13. Donaldson P, Lake D (2008) Unmanned aircraft – in production/unmanned aircraft—in development. In: Unmanned vehicles handbook, United Kingdom, Shephard, pp 13–84
14. Bierig A et al (2018) Design considerations and test of the flight control actuators for a demonstrator for an unmanned freight transportation aircraft. In: R3ASC 2018, Toulouse