SAFETY CRITICAL DESIGN OF FLIGHT CONTROL SYSTEM ARCHITECTURES - POTENTIAL SAFETY ASPECTS FOR A TRIPLE SPLIT AILERON FOR THE PROJECT WISDOM

S. Lübbe*, O. Bertram*
* German Aerospace Center (DLR), Institute of Flight Systems, Lilienthalplatz 7, Braunschweig, Germany

Abstract

As part of the WISDOM (Wing Integrated Systems Demonstration On Mechatronic Rig) project the German Aerospace Center (**DLR**) - in cooperation with Liebherr Aerospace, FFT Produktionssysteme, TU Berlin and Diehl Aerospace - is developing a demonstrator test rig for future control surface actuation systems. The control surface actuation system is intended as a potential part of future flight control systems. The conceptual design of the underlying flight control system architecture is performed according to design processes for safety critical systems to support the concepts viability for potential real life application. The flight control system is assumed to fulfil traditional flight control functions in addition to innovative gust load alleviation and flutter suppression functions using a set of three ailerons per wing.

The aircraft used as conceptual baseline is an A320-like low to mid-range commercial passenger aircraft. The design focus lies on realising the necessary reliability of the considered flight control functions while accommodating project specific technology innovations within the flight control system.

The analysis processes are based on ARP4761. A potentially viable architecture concept has been identified that incorporates a triplex electrical power supply and simplex control surface actuation. Central challenges and requirements towards a multitude of components and peripheral systems could be identified. These will be presented and discussed after presenting the design process and the resulting architecture. The paper is comprised of four sections. The first introduces central concepts and definitions necessary, such as safety processes and considered actuation technologies. The second addresses the detailed aircraft configuration, the control surface layout, functional allocation and description of the relevant flight control functions. The third section describes the applied design and analysis workflow. Established methods from ARP4761 have been adapted to be used within a model-based systems engineering (MBSE) model and enable side-by-side consideration of system design and safety analysis in a shared model.The fourth and final section presents and discusses the results of the performed design process. These include the resulting flight control system architecture, identified central technology requirements for and a collection of technological challenges that arose from the safety analyses and design iterations.

Keywords
Flight Control System; Safety Analysis; System Design

INTRODUCTION

The German Aerospace Center (**DLR**) - in cooperation with Liebherr Aerospace (**LLI**), FFT Produktionssysteme (**FFT**), Technical University Berlin (**TUB**) and Diehl Aerospace - is developing a demonstrator test rig for future control surface actuation systems as part of the WISDOM (Wing Integrated Systems Demonstration On Mechatronic Rig) project [1]. The flight control system (FCS) is needed as an enabler for sustainable aviation aircraft by potentially allowing for lighter and more efficient aircraft. The presented control surface actuation system is intended as a potential part of future flight control systems. To ensure the concepts viability for potential real life application, the conceptual design of the underlying flight control system architecture is performed according to design processes for safety critical systems, based on Aerospace Recommended Practices (**ARP**) [2, 3]. The flight control system is assumed to fulfil innovative gust load alleviation and flutter suppression functions and roll control using a set of three ailerons per wing. Gust load alleviation and flutter suppression functions are expected to be necessary for the realisation of future high aspect ratio wings and more elastic wing designs [4]. The aircraft used as conceptual baseline for this is an A320-like low- to mid-range commercial passenger aircraft [5]. The design focus for the flight control system lies on potentially achieving the necessary reliability of the considered flight control functions while accommodating project specific technology innovations within the flight control system. Among these are new actuator technologies, supply system configurations and control allocation concepts. The central concern in the initial stages is the overall viability of the actuation concepts, based on

doi: 10.25967/610292

their specific power supply requirements and resulting safety implications. Another goal of the project is to explore the general viability of simplex actuation for the ailerons, which is especially challenging in regards to safety critical flight control applications.
Current flight control systems for commercial aircraft usually employ at least duplex supply of all primary control surfaces [6–8]. These are traditionally supplied hydraulically. Novel aircraft programs, such as the Airbus A380 and Airbus A350, have introduced partial electrification of flight control actuators [7]. Alterations of the applied actuator technology have a huge impact on resulting overall system architecture, especially in regards to the power supply systems and overall safety related requirements. Similar effects are to be expected from extension of function allocation of the system. Because of this, realistic concepts for the system's architecture have to be analysed in parallel to the system design using safety critical analysis processes. The conceptual flight control system architecture in the WISDOM project was achieved by analysing preliminary system architecture concepts for their safety attributes in early stages. The analysis processes are based on ARP4761 methods [2, 3] with adaptions for the application in early concept stages. These especially enable fast disqualification of non-viable architecture candidates for the flight control system and supply system architectures.
A potentially viable architecture concept has been identified that incorporates a triplex electrical power supply and simplex control surface actuation. Central challenges and requirements towards a multitude of components and peripheral systems could be identified. These will be presented and discussed after presenting the design process and the resulting architecture.

1. CENTRAL CONCEPTS AND DEFINITIONS

This section introduces the major topics of the paper. The system of interest is described, as are applying regulations, the relevant design processes, and safety assessments for the design of commercial aircraft.

1.1. Flight Control System

Flight control systems (**FCS**) are a central part of most aircraft, especially larger aircraft. The FCS is generally responsible for realising the pilots control outputs through dedicated control surfaces. From a certain size of aircraft the controls are typically not realisable without aided control action, which requires actuator support to the pilots input signals [9–12]. In modern commercial aircraft, power for control surface actuation is provided through hydraulic power supply or in some cases electrical power supply [13]. FCS is classically further divided into primary and secondary flight control [9, 11, 12].
Primary flight control is responsible for controlling the aerodynamic aircraft states, mainly state and attitude of roll, pitch and yaw angles. In commercial aircraft, primary flight control uses at least ailerons, elevators and rudders. Secondary flight control is mainly concerned with the aircraft's aerodynamic configuration, for example altering the wings effective angle of attack or surface area, resulting in different lift and drag coefficients. It employs high lift devices on the main wings' leading edge and trailing edge. Spoilers on the wings can be used for both primary and secondary flight control [9–11].
Fly-by-wire technology, transferring the pilots commands electrically, enables the FCS to additionally fulfil more sophisticated control functions [12, 13]. This means, that the modern FCS is able to realise flight state commands, such as desired roll rates, instead of only control surface positions, using Flight Control Computers (**FCC**). Airbus aircraft for example accept both, control surface positions and roll/pitch/yaw rates from the pilots, depending on the chosen operation mode.
Another important categorising term in the context of flight control is power-by-wire. Fly-by-wire is marked by using electrical signal transmission in flight control, power-by-wire extends on it by also transmitting the necessary actuation power electrically. This offers advantages in power metering strategies and power supply reconfiguration potential [14].

1.2. Flight control system architectures in contemporary research

FCS have seen a multitude of significant changes over the last century. The last major changes in regards to commercial transport aircraft have been the introduction of fly-by-wire, followed by the partial implementation of power-by-wire in primary flight control for Airbus's A380 and A350. Since then, novel system architectures have mostly been part of academic work or scaled flight demonstrators. Some examples for which will be given to improve the context of the project.
In his research [15] designed a duplex arrangement of electro-mechanical actuators (**EMA**) for primary flight control. The safe design of electro-mechanical actuation for multi-degree of freedom motion of flaps was presented by Christmann [16]. In Bennett [17] their concept for electrical actuation of flaps for a commercial aircraft's inner high lift system is presented. All mentioned examples have in common that known aircraft and control surface layouts were used as the baseline, substituting existing actuators with the analysed technology.
Works in the field of power supply transition range from strictly state-of-the-art aircraft, to novel function design and new control surface layouts. Design of a FCS with optimised power and information distribution based on the control surface layout of the A340 was done by Bauer [18]. Optimisation of power consumption under safety constraints for existing control surface layout with different degrees of electrification of flight control actuators was demonstrated by Postnikov [19]. An Automatic generation of safety evaluation for a novel control surface layout using mixes of hydraulic and electrical power supply was demonstrated in Bornholdt [20], applying the presented method both to a state-of-the-art aircraft and a control surface layout with highly distributed control surfaces. General design rules for FCS and multifunctional FCS were stated based on existing aircraft data to set up the design of potentially new aircraft in Lampl [21].

This is done for the example of an existing aircraft with augmented functionality and control surface layout.

1.3. Gust Load Alleviation and Flutter Suppression

Another important field of research related to flight control involves the functional augmentation of FCS to implement active load control. Active load control is meant to provide additional protection of the aircraft's structure during flight. This is motivated by the overall goal of aerodynamically optimising the aircraft, its mass and lift-to-drag ratio, which in turn necessitate lighter and more flexible wing structures [4]. Research mainly covers control design [22–26], as well as aerodynamic simulation and optimisation [27–29]. Control design for gust load alleviation is additionally developed as feed-forward control, using LIDAR-based technology [22, 24, 30]. Flutter suppression is described in it's own specialised field of controller design, for example in [31, 32].
The common attribute of all referenced research is the usage of control surface deflections in flight as reaction to certain encounters with the aim of reducing the loads encountered by the aircraft's structure.

1.4. Actuation technologies in FCS

Generally, powered FCS can be supplied by either hydraulic or electrical power supply. For primary flight control in particular, there are three different actuator technologies that are currently in use. Each are presented briefly together with their implied requirements to the overall system. A potential technological advancement for control technologies related to the actuation of the FCS is also introduced.

Electro-Hydraulic Servo-Actuator

The first generation of actuators enabling fly-by-wire in commercial aircraft were electro-hydraulic servo-actuators (**EHSA**). These hydraulically powered actuators are controlled electronically and supplied by a constant pressure hydraulic network. An analogue input signal is translated into a fed-back control surface position. EHSAs contain multiple stages of valves to realise the necessary operation modes for primary flight control [7, 13].

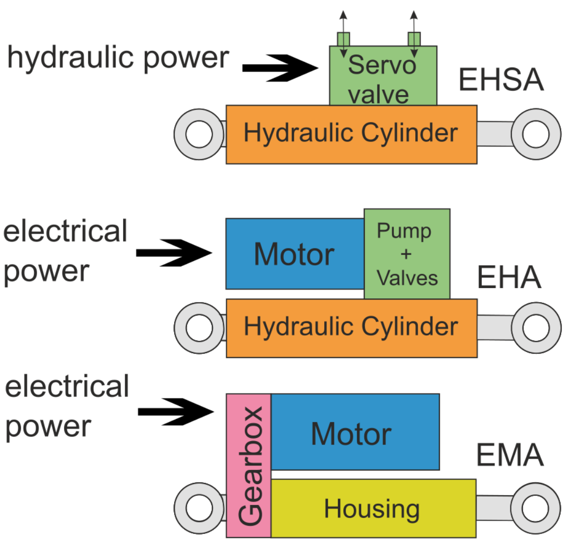


FIG 1. Schematic comparison of EHSA, EHA and EMA

Electro-Hydrostatic Actuator

Electro-hydrostatic actuators (**EHA**) are part of the first generation of power-by-wire flight control actuators. Electrically driven pumps supply a local hydraulic circuit that provides the necessary pressure to drive a hydraulic cylinder. The most established variation of EHA controls the control surface position via its motor speed. Non-nominal operation modes, such as passive or locked, are realised using pre-stage valves [7, 13, 33].

Electro-Mechanical Actuator

An electro-mechanical actuator (**EMA**) generally consists of a motor, some type of gear to translate rotary into linear movement and an electronics unit that meters the necessary power and currents. A variety of translation methods between rotary and linear movement exist, the most common being a leadscrew mechanism [33]. Application specific variations in aviation exist. They employ for example de-coupling for actuator passivisation or break mechanisms for actuator locking.

Remote Electronic Unit

Remote electronic units (**REU**) are distributed control units attached to actuator packages developed by LLI. They implement local control loops for the actuator and can contain various sensors. They are able to perform the necessary digital-to-analogue interface between actuator and FCC and are able to prospectively run even more sophisticated control loops [24]. REUs for flight control applications employ dual channel dissimilar electronic hardware, allowing them to realise separated command and monitoring (con-mon) lanes and thus fail-safe behaviour. REUs can be used for all three actuator types introduced in this section.

1.5. Certification Specifications and ARP4754A

For commercial aircraft, a major factor for the design of every system is certification. To be operated in civil airspace, aircraft have to meet strict requirements in regards to their performance, structural integrity, design documentation, operator handling and safety. For industry this is documented in form of regulations set by civil aviation authorities, such as the European Union Aviation Safety Agency (**EASA**) and Federal Aviation Administration (**FAA**) [34–36]. The CS-25 [35] extensively describes requirements to certifiable aircraft across domains. It applies to winged aircraft for commercial use with passenger numbers of 19 or more or an empty weight over 5700kg. Requirements to the aircraft's system design methodology, overall documentation and safety analyses are further described in de-facto standards published by the Society of Automotive Engineers (**SAE**). The ARP4754A [3]

acts as the main guideline for design and certification of commercial aircraft.
ARP4754A, among others, describes the recommended design steps, organisational requirements and necessary system description. It organises design and analysis process and their chronological order, required in- and outputs, and interrelations. The detailed description of the safety assessment of system and aircraft is done within the ARP4761.

1.6. Safety Assessment and Processes

ARP4761 [2] describes the safety assessment in regards to the processes, their interactions and order, and the recommended analysis and assessment methods. As mentioned earlier, it is embedded within the system engineering processes outlined by ARP4754A [3], that describes the whole design processes from conceptual stage up until entry into service. Both reference each other and build the baseline for the design and certification of commercial aircraft and their aircraft systems. To further describe and handle the complexity of the system design, the aircraft is conceptually organised into

- Aircraft Level,
- System Level,
- Subsystem Level and
- Component Level.

The division and allocation of functions between aircraft systems is part of the particular design and may vary.
Different stages of the design process usually concentrate on specific system levels.

Aircraft FHA and System FHA

Functional Hazard Assessment (**FHA**) analyses either aircraft functions or system functions of a specific system. The considered functions can be further broken down into more detailed functions while remaining on either level. FHA describes a systematic approach for analysing each function for potential failure behaviour, such as loss of functions or inadvertent function activity, and their effect on the aircraft. The effect on the aircraft is considered extensively for every flight phase and additionally with respect to whether the considered failure is known to the operators or not [2].
FHAs are usually performed along and inside their table based documentation, but can also be integrated into a model, as described in [37]. To perform a FHA a collection of intended functions and, at least, initial general assumptions on how they will be achieved are necessary. FHAs need to be constantly updated throughout the development, to track changes in the amount of functions and their behavioural descriptions [2]. FHA results also serve as the starting point and interface to Preliminary Aircraft Safety Assessment (**PASA**) and Preliminary System Safety Assessment (**PSSA**).

Probabilistic Reliability Calculation Methods

In the context of the ARP4761 and this work three different methods for the calculation of probabilities are usually employed:

- Fault Tree Analysis (**FTA**)
- Reliability Block Diagrams (**RBD**)
- Markov Analysis.

All of which can be used to model probabilities of events depending on exposure time and failure rate. More detailed descriptions of the specific methods can be found in [2].

Preliminary Aircraft Safety Assessment

Preliminary Aircraft Safety Assessment (**PASA**) is a systematic examination of proposed aircraft systems architectures, that determines how failures can lead to the functional hazards identified by the Aircraft [3]. PASA also enables to describe potential effects of combinations of events described in the Aircraft FHA. It is an additional term that was introduced in the amendment A of ARP4754 to more generally describe and augment early stage Aircraft FTA in ARP4761. It encourages the usage of other analysis methods and reduces ambiguity in the naming of processes.

Preliminary System Safety Assessment

Preliminary System Safety Assessment (**PSSA**) is the analogous process to the PASA on system level [2, 3]. Proposed system architectures are analysed for their reliability and conformity to requirements and assumptions from the System FHA. Usually employed methods to conduct PSSAs are FTAs, RBDs or Markov Analyses. All relevant failure conditions for the system under analysis have to be examined. To achieve this, detailed descriptions of the proposed system architectures are necessary. These include the descriptions and amounts of components, their interconnections and the required behaviour of the system under analysis. PSSA outputs the budgets and requirements for following design iterations [2].

2. AIRCRAFT AND SYSTEMS' ARCHITECTURE

This section introduces the underlying aircraft design for the project that is considered to be the application case for the FCS and the hardware in the loop test bed. The central idea within the project necessitates a holistic analysis and synergy of the involved disciplines in order to achieve technical relevance of the realised tests and technology concepts. For this, controller design, aircraft design and system architecture design have to be illuminated.

2.1. Aircraft description

The aircraft design used in the project was created by DLR based on a design for a potential successor to the A320 [5]. The control surface layout is unchanged, except for the triple aileron split on both sides. This results in three ailerons, each with 50% length of the original A320 aileron, resulting in an overall increased aileron length of 150% compared to the A320. The aircraft is designed for short to medium range missions.

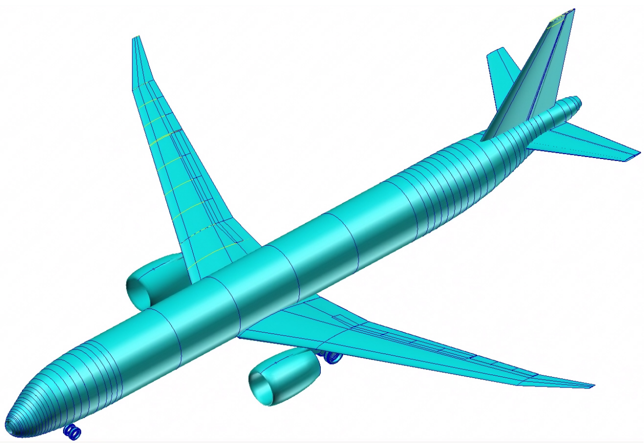


FIG 2. CPACS based description of the D2AE aircraft configuration

The wing design aims at higher lift-to-drag-ratio compared to the A320, which necessitates active load alleviation functions. These are realised through the FCS in particular by implementing active flutter suppression and gust load load alleviation.
The implementation of these functions potentially impacts the FCS, Electrical Power System, Hydraulic System and Navigation System. All other aircraft systems are assumed to correspond to the state-of-the-art as seen in the A320.

2.2. Flight Control System Aspirations

There are several dominant ambitions in the development of future FCS. Most of these are driven by overall design goals of the aircraft. The most relevant in this context are the desired electrification of aircraft systems, increasing digitalisation of control components, and active alleviation of wing loads through flight control system. For the considered FCS in the project context, this translates to the preference of using EMA or EHA for actuation of the ailerons, instead of EHSA.
All of these actuators can be equipped with a REU, that implements a local control loop and communicates digitally with the central FCCs. This local control loop could also implement a fast super-positioned flutter suppression on top of the control surface position control [24]. Each of these aspirations is an open challenge, especially from the perspective of aircraft safety. The design of a FCS architecture that is able to host all of them for the presented designed aircraft configuration has to be systematic and rigorous. Another consideration that is considered for the presented aircraft design is the potential implementation of simplex actuated ailerons.

2.2.1. Initial Assumption of Flight Control Design

For the analysis of the FCS's behaviour the basics of the desired controller design have to be known. For both active gust load alleviation and active flutter suppression we assume an active control action, that is superpositioned upon the normal law commands of the flight control for the ailerons. The new controllers will either have limited local quasi-autonomous authority or be integrated in the existing flight control laws. The Active gust load alleviation will counter loads caused by gust encounters, by temporarily decreasing the wings lift through aileron deflections. The Flutter Suppression is assumed to dampen and eliminate oscillations in flutter cases through complex aileron deflections. Both functions will use the FCCs, all aileron actuators and a to be determined set of sensory units. For the flutter suppression especially an increased amount of sensors is necessary to provide the controller input. The developed control approach uses local inertial data distributed throughout the wings.
The designed controllers will have to be synchronised into the final model.

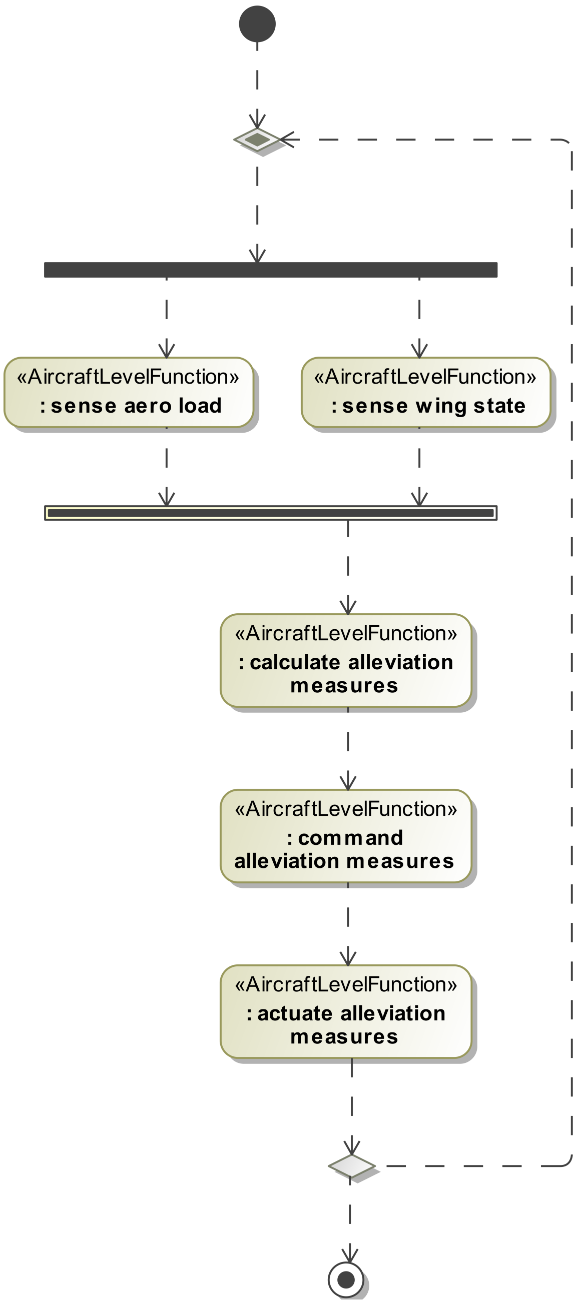


FIG 3. Schematics of load alleviation control process

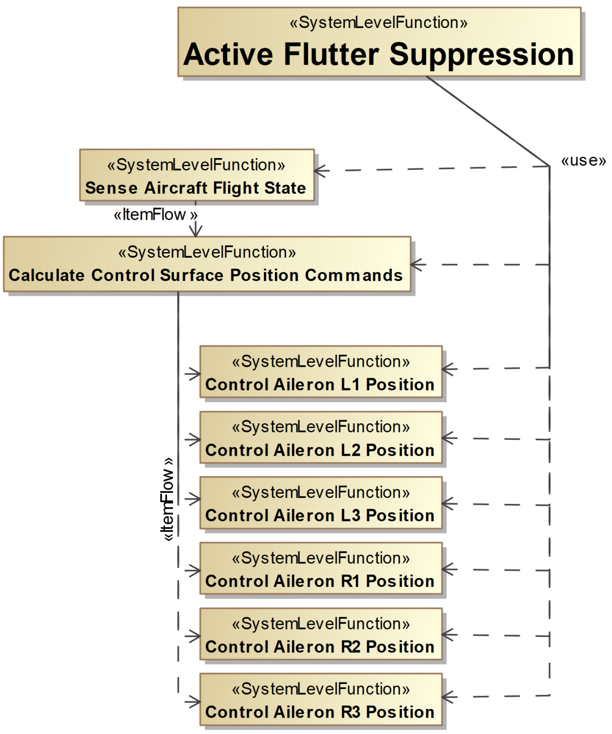


FIG 4. Assumption of functional description of flutter suppression

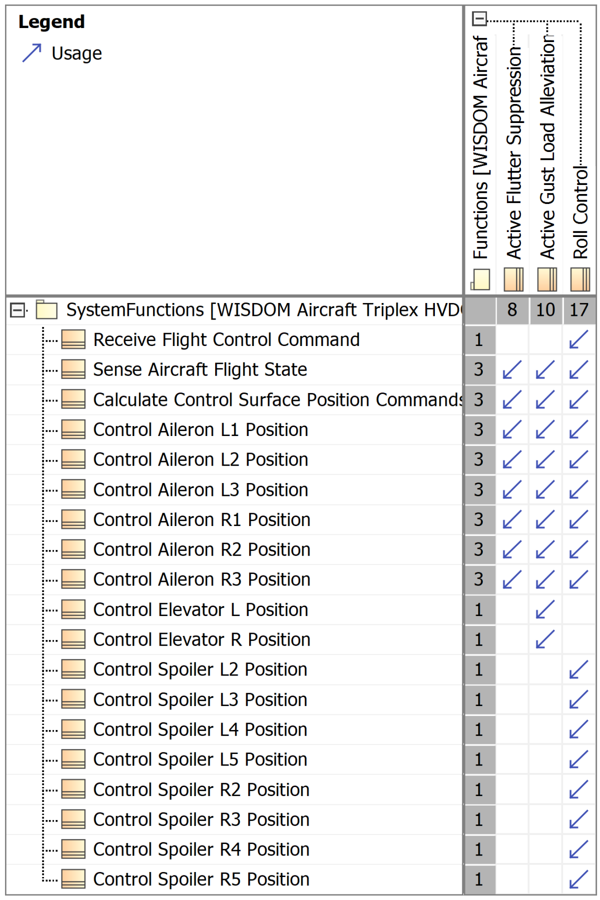


FIG 5. Usage of FCS system functions for relevant control functions

3. DESIGN WORKFLOW

A reduced set of safety assessments was performed early on to generate a first iteration of requirements in respect to the desired new flight control functions. The main goal in this was to achieve a realistic concept for our flight control system architecture and identify unsafe concepts early on. This was done in particular for the functions

- aileron position control
- gust load alleviation
- flutter suppression

in the form of a preliminary functional hazard analysis, followed by an RBD based analysis of actuation concepts. The chosen functions are judged to be the most relevant for their novelty and potential impact. Gust load alleviation and flutter suppression are both additional functions and impacted by the changed control surface layout and actuator technology. Aileron position control will be used for both and potentially be impacted by the altered control and actuation technology.

The performed workflow closely resembles the design process outlined by ARP4754A, but with the addition of preliminary assessments to consider the desired system additions to achieve a viable starting point for the more detailed design (see Figure 6). The applied workflow therefore consists of the steps

- initial Safety Assessment,
- System Architecture Generation,
- Fast Architecture Safety Evaluation,
- Feasability Evaluation and Architecture Selection.

Out of these System Architecture Generation and Fast Architecture Safety Evaluation are executed in parallel, evaluating architecture candidates and increasing the redundancy when disqualifying architectures for following candidates.

3.1. Initial Safety Assessments

The initial safety assessment was conducted in form of a preliminary Aircraft FHA analysing the mentioned functions. The control aileron function was additionally considered to potentially exhibit specific failure modes of "free floating" and "jam", which had to be further specified, depending on flight phase, motion range, and severity. For both new functions it was concluded that

- the loss of 33% of the perspective functions may at most be classified as major and
- the loss of 66% of the perspective functions may at most be classified as hazardous,

to be potentially implemented at all. These conclusions were forwarded as a restriction towards the structural design and control design of the aircraft. For the "free floating" and "jam" failure events several rationals and assumptions had to be defined. Within the analysis it was concluded that these would be especially impacting in regards to the choice of actuators, since EHA/EHSA and EMA show different behaviour under failure. Jam events for EMA are significantly more present for their potential occurrence in rotary mechanical transmission components [38]. In contrast, failure modes that lead to passivisation and, ultimately, potential floating behaviour

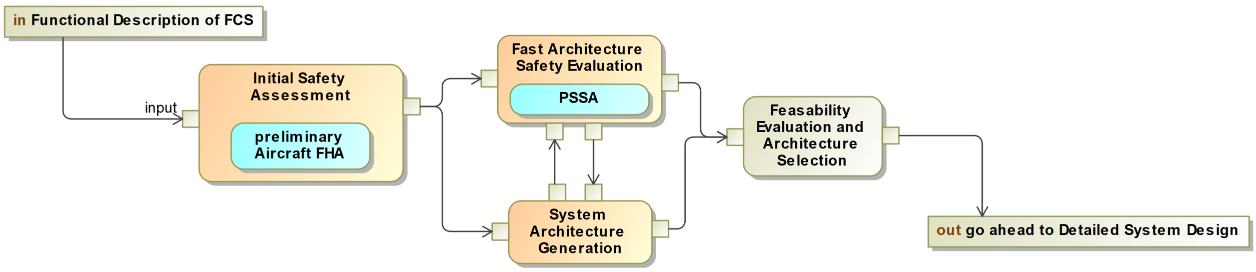


FIG 6. Visualisation of design workflow (turquoise fields indicate ARP4761 adapted applications)

are more likely for EHA and EHSA. The conclusions of the initial Aircraft FHA will be presented in section 4.

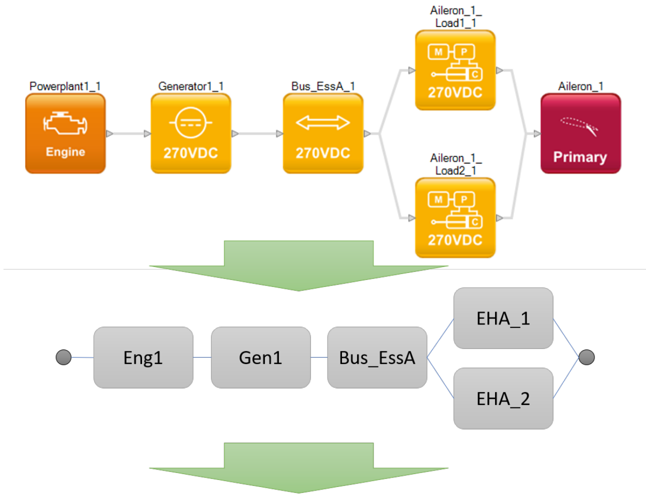
3.2. System Architecture Generation

Different architectures were considered for the FCS. All of them are summarised in Table 2. The three different actuator types were combined with allocations of the respective necessary power supply system in rising redundancy from simplex up to triplex. Additionally, the electrically supplied actuators were also considered with a duplex power supply. Every increase of power redundancy naturally leads to an increase in potential variations of architectures that have to be examined.
To restrict the amount of considered architectures, the scope has been limited to candidates with loads distributed equally and symmetrically to the different busses.

3.3. Fast Architecture Safety Evaluation

The generation of potential system architectures for the FCS and respective power supply were carried out in parallel to a fast evaluation of the expected reliability for the considered functions. The applied analysis method is closely based on the PSSA process and generates RBDs for considered architecture variations. Reliability estimates were calculated for component failure rates taken from literature and checked against the reliability requirements. Each of the proposed architectures is analysed for their potential of partial loss of function and total loss of function separately. They are checked against the assumed failure rate allowances from the initial Aircraft FHA for the relevant functions. This is done using reliability diagrams and a fast heuristic search that examines cut sets up to the fourth degree.
The RBDs are built based on system architecture graphs defined by the arrangement of power supplies, power converters and actuators and their interconnections.
The generated cut sets are used to calculate failure probabilities per flight hour. The probability of a single minimal cut of degree n over time is approximated using Equation 1, where t represents the exposure time, and λ_i the failure rate of a single component.

$$P_{mincut}(t) = \prod_{i=1}^{n} (\lambda_i \cdot t) \tag{1}$$



$$P_{fail} = (P_{fail,Eng1} \vee P_{fail,Gen1} \vee P_{fail,BussEssA} \vee (P_{fail,EHA1} \wedge P_{fail,EHA2}))$$

FIG 7. Architecture to RBD to cutset workflow

The combined probability of all relevant minimal cuts for a single failure case is approximated using Equation 2.

$$P_{failure}(t) \approx \sum_{j=1}^{m} P_{mincut,j}(t) \tag{2}$$

The failure rates for the considered component types are summarised in Table 1 and based, where available, on service data. With this, a minimum achievable failure rate can be estimated, that is used to disqualify non-viable architecture candidates.
The remaining architecture candidates can be further extended and analysed for different arrangements of FCCs. This further increases confidence in the chosen architectures.
The described processes are performed iteratively and interactively. Their interactions are schematically visualised in Figure 6.

Architecture Modelling and Tools

The aircraft and it's systems were modelled using SysML (Systems Modelling Language) in Cameo Systems Modeller. The more detailed description of the FCS and power supply was further specified in a synchronised model within Pacelab SysArc. The safety analyses and design iterations were performed within the models.

Component	failure rate	source
generator	$1.3 \cdot 10^{-5} \frac{1}{FH}$	[38]
engine/APU	$5 \cdot 10^{-5} \frac{1}{FH}$	assumption
hydraulic circuit	$1 \cdot 10^{-4} \frac{1}{FH}$	[13]
electrical bus	$1 \cdot 10^{-7} \frac{1}{FH}$	[38]
EHA	$1 \cdot 10^{-5} \frac{1}{FH}$	[38]
EMA	$1 \cdot 10^{-5} \frac{1}{FH}$	[38]
EHSA	$1 \cdot 10^{-5} \frac{1}{FH}$	[38]

TAB 1. used failure rate data, based on [13, 38]

This enables a traceable and connected design and analysis of the system architecture, functional description, and safety attributes. For further explanations refer to [37, 39, 40].

4. DESIGN RESULTS

Following the described design procedure lead to two potential FCS architectures in respect to the aileron actuation and related FCC allocation. They have an immediate impact on the necessary supply architecture up to the engines and emergency power supply. The generated architecture has been extended to include the remaining, unchanged FCS actuators and control surfaces for primary and secondary flight control, such as elevator and flap actuation.
Additionally, some of the rejected architectures will be illuminated further. They provide valuable insight into specific technological challenges and safety-related weakspots, and represent central learnings of the analysis.

4.1. Preliminary Aircraft FHA

Figure 8 showcases the results from both Aircraft FHA and System FHA in the early design stage of the project. The scope is restricted to functional hazards with major or higher criticality. It has to be highlighted that for all considered functions the predominant failure cases leading to catastrophic results are malfunctions. In contrast, while the loss of the load alleviation is still expected to be potentially catastrophic, the isolated loss of any single aileron must not have a higher criticality than major.
The flutter suppression function was especially influential for the following architecture studies, since both roll control and gust load alleviation have additional functional redundancies.

4.2. Resulting FCS Architecture

A potentially viable FCS architecture has been identified, that employs simplex actuation of the ailerons using EMA with local REU-based position control loops. The EMA power supplies of each actuator have been identified as potential common cause, which requires a system design with three segregated power supply busses. These power busses are also used to supply the other FCS actuators. Figure 9 visualises the preliminary assumption of the system components' location within the aircraft and the necessary cabling. Connections to avionic components and the cockpit are not included. Figure 10 schematically shows the resulting system architecture for primary flight control, spoilers are omitted for clarity. Component connections between FCS components internally and towards the electrical supply busses are shown.
The allocation of the busses has further potential to be optimised for a more equalised load distribution. However, this is out of the scope of the presented analysis.
The failure rate of the resulting FCS architecture, when considering 21 cuts of second degree and 43 cuts of third degree, is estimated at about $\lambda_{LA,loss} \approx 6.23 \cdot 10^{-10} \frac{1}{FH}$

Actuator	power supply redundancy (Hyd ; Elec)	failure rate for loss of function $[\frac{1}{FH}]$	Is viable
EHSA	(1 ; 0)	$> 1 \cdot 10^{-4}$	no
EHSA	(2 ; 0)	$> 1 \cdot 10^{-4}$	no
EHSA	(3 ; 0)	$> 1 \cdot 10^{-8}$	no
EHA[1]	(0 ; 1)	$\sim 1 \cdot 10^{-4}$	no
EHA[1]	(0 ; 2)	$> 1 \cdot 10^{-7}$	no
EHA[1]	(0 ; 3)	$\sim 1 \cdot 10^{-10}$	yes
EHA[2]	(0 ; 2)	$\sim 1 \cdot 10^{-10}$	yes
EHA[2]	(0 ; 3)	$\sim 1 \cdot 10^{-10}$	yes
EMA[1]	(0 ; 1)	$\sim 1 \cdot 10^{-4}$	no
EMA[1]	(0 ; 2)	$> 1 \cdot 10^{-7}$	no
EMA[1]	(0 ; 3)	$\sim 1 \cdot 10^{-10}$	yes
EMA[2]	(0 ; 2)	$\sim 1 \cdot 10^{-10}$	yes
EMA[2]	(0 ; 3)	$\sim 1 \cdot 10^{-10}$	yes

TAB 2. Failure rates for loss of flutter suppression of different FCS and power supply architectures

4.3. Rejected FCS Architectures

As an additional benefit, the analyses of the different potential design concepts have brought a detailed insight into the safety related weaknesses of disqualified concepts. These contain significant information for following design iterations. The most influential ones for each candidate are summarised for future considerations. The consideration of simplex power supply architectures will be omitted at this point, since they offer obvious single points of failure.

Hydraulic Supply - Simplex Actuation

Hydraulically supplied simplex actuation of the ailerons causes two major concerns.
(1.)The loss of any hydraulic supply automatically causes a loss of 33% of available ailerons. For hydraulic supplies the failure rate of $\lambda_{hyd,sup} \approx 1 \cdot 10^{-4} \frac{1}{FH}$ makes this unviable for the desired FCS functional extent, in which the loss of any aileron is considered major.

[1]simplex supplied
[2]duplex supplied

Legend

↗ Criticality Classification

Element	Classifcations	Catastrophic	Hazardous	Major
AFHA-1 Active Load Alleviation		8	4	
AFHA-1-1 Active Flutter Control		4	2	
WIS3E-AFHA-1.1-2 Active Flutter Suppression suffers <Fails to operate function> during any flight phase	1	↗		
WIS3E-AFHA-1.1-3 Active Flutter Suppression suffers <Operates function inadvertend> during any flight phase	1	↗		
WIS3E-AFHA-1.1-4 Active Flutter Suppression suffers <Operates function incorrect> during any flight phase	1	↗		
WIS3E-AFHA-1.1-6 Active Flutter Suppression suffers <Unsym. partial loss of function> during any flight phase	1		↗	
WIS3E-AFHA-1.1-7 Active Flutter Suppression suffers <Total loss of function> during any flight phase	1	↗		
WIS3E-AFHA-1.1-8 Active Flutter Suppression suffers <Unable to stop function> during any flight phase	1		↗	
AFHA-1.2 Active Gust Load Alleviation		4	2	
WIS3E-AFHA-1.2-2 Active Gust Load Alleviation suffers <Fails to operate function> during any flight phase	1	↗		
WIS3E-AFHA-1.2-3 Active Gust Load Alleviation suffers <Operates function inadvertend> during any flight phase	1	↗		
WIS3E-AFHA-1.2-4 Active Gust Load Alleviation suffers <Operates function incorrect> during any flight phase	1	↗		
WIS3E-AFHA-1.2-6 Active Gust Load Alleviation suffers <Unsym. partial loss of function> during any flight phase	1		↗	
WIS3E-AFHA-1.2-7 Active Gust Load Alleviation suffers <Total loss of function> during any flight phase	1	↗		
WIS3E-AFHA-1.2-8 Active Gust Load Alleviation suffers <Unable to stop function> during any flight phase	1		↗	
Control Aileron L1 Position		5	6	1
WIS-AFHA-2-51 Control Aileron L1 Position suffers <Operates function inadvertend> during Climb	1	↗		
WIS-AFHA-2-52 Control Aileron L1 Position suffers <Operates function incorrect> during Climb	1		↗	
WIS-AFHA-2-58 Control Aileron L1 Position suffers <Operates function inadvertend> during Cruise	1	↗		
WIS-AFHA-2-59 Control Aileron L1 Position suffers <Operates function incorrect> during Cruise	1		↗	
WIS-AFHA-2-65 Control Aileron L1 Position suffers <Operates function inadvertend> during Descent	1	↗		
WIS-AFHA-2-66 Control Aileron L1 Position suffers <Operates function incorrect> during Descent	1		↗	
WIS-AFHA-2-72 Control Aileron L1 Position suffers <Operates function inadvertend> during Landing	1	↗		
WIS-AFHA-2-73 Control Aileron L1 Position suffers <Operates function incorrect> during Landing	1		↗	
WIS-AFHA-2-79 Control Aileron L1 Position suffers <Operates function inadvertend> during Take-off	1	↗		
WIS-AFHA-2-80 Control Aileron L1 Position suffers <Operates function incorrect> during Take-off	1		↗	
WIS-AFHA-2-94 Control Aileron L1 Position suffers <Jam of Control Surface> during any flight phase	1			↗
WIS-AFHA-2-95 Control Aileron L1 Position suffers <Free Floating of Control Surface> during All Flightphases	1		↗	
Control Aileron L2 Position		5	6	1
Control Aileron L3 Position		5	6	1
Control Aileron R1 Position		5	6	1
Control Aileron R2 Position		5	6	1
Control Aileron R3 Position		5	6	1

FIG 8. Result Summary of initial Aircraft and System FHA

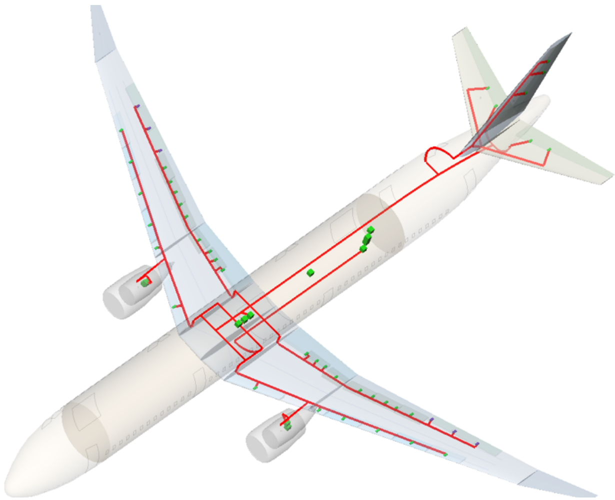


FIG 9. 3D view of the aircraft with preliminary positioning of actuators and power distribution

(2.) Even at triplex supply of the actuators, a total loss of the load alleviation functions, marked by the loss of two ailerons of one wing, has a probability $\lambda_{LA,loss} \approx 1 \cdot 10^{-7} \frac{1}{FH}$.
A simplex actuation with EHSAs was therefore deemed to be not feasible for the aspired FCS.

Hydraulic Supply - Duplex Actuation

Duplex Actuation with hydraulics was also analysed and did not disqualify from a reliability point of view. Assuming a triplex supply of the actuators, the set safety goals could potentially be met. On project level it was decided to reject the architecture in favour of potential simplex actuation. Additionally, the overall ambition of reducing the amount of used hydraulics in the aircraft are in direct opposition to this architecture candidate.

Electrical Duplex Supply - Simplex Actuation

Another promising potential design was the duplex supply of power-by-wire actuators, which did theoretically showcase sufficient behaviour. From a technical standpoint it requires the duplex supply of every aileron actuator. This in turn requires adaptions, so that the supplied actuators do not close the supply busses and potentially cause common mode failures. The architecture was therefore rejected as too ambitious and in favour of the architecture with a more redundant power supply.

4.4. Technological Requirements and Challenges

From the resulting architecture design several technical requirements for the system components of the FCS could be identified. Most of these stem from the safety critical nature of the application, some present open challenges that will have to be further addressed as the system design progresses and matures.

Gust Load Alleviation and Flutter Suppression Controller Performance

The new control functions for load alleviation through the FCS have to be designed in such a way that
- the loss of any single aileron does not cause a loss of performance for either function and
- the loss of two ailerons on a single wing does not constitute a total loss of function.

This means that the controller design has to be performed with a reduced set of ailerons in mind to set the nominal performance. Benefits of the availability of all ailerons for the control design may not be included in the nominal performance considered for structural design.

REU Command Input

The simplex actuation also implies a required high availability of the necessary control inputs. For the REUs as local controllers this means that they have to be able to receive a dual channel control input, out of which one channel is sufficient in case of failure. Also the REU has to realise its own autonomous integrity check, to prevent an incorrect operation of the control surface.

n-to-n Actuator to FCC Communication

REUs and FCCs connected to the same communication bus have to be able to communicate all necessary data in both directions. This is necessary to employ the local control loops to close the larger flight control loops and to check and adapt to the actuators states. It is also necessary to eliminate the FCCs as potential single points of failure for the loss of multiple connected REUs. Additionally, this communication has to be fast enough to close the flight control loops.

Stable Floating Behaviour of Loose Aileron

One of the central requirements from the initial stages on is that any incident, where a single aileron experiences the floating failure mode, will not lead to a catastrophic event, meaning a loss of the aircraft. This was introduced as an initial assumption that has to be carried on to the structural design to ensure the behaviour of the control surfaces in an unactuated state.

Legend: ↗ Connector

		aileron L1 Actuator	aileron L2 Actuator	aileron L3 Actuator	aileron R1 Actuator	aileron R2 Actuator	aileron R3 Actuator	elevator L Actuator A	elevator L Actuator B	elevator R Actuator A	elevator R Actuator B	rudder Actuator A	rudder Actuator B	rudder Actuator C	PRIM 1	PRIM 2	PRIM 3	SEC 1	SEC 2	SEC 3	flight Control Data Bus 1	flight Control Data Bus 2	flight Control Data Bus 3
Electrical System		1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2
essential HVDC Bus A	4	/			/						/	/											
essential HVDC Bus B	4		/			/			/				/										
essential HVDC Bus C	5			/			/	/		/				/									
essential LVDC Bus A	9														/	/	/	/	/	/	/	/	/
essential LVDC Bus B	9														/	/	/	/	/	/	/	/	/
Flight Control System		2	2	2	2	2	2	1	1	1	1	2	2	2	6	6	6	5	5	5	1	1	1
PRIM 1	6															/	/	/	/	/	/		
PRIM 2	6														/		/	/	/	/		/	
PRIM 3	6														/	/		/	/	/			/
SEC 1	5														/	/	/		/	/			
SEC 2	5														/	/	/	/		/			
SEC 3	5														/	/	/	/	/				
flight Control Data Bus 1	9	/	/		/	/			/	/		/		/	/								
flight Control Data Bus 2	8	/		/	/		/				/	/	/			/							
flight Control Data Bus 3	8		/	/		/	/	/					/	/			/						

FIG 10. Primary FCS Architecture with power supply and FCC allocation

5. SUMMARY & OUTLOOK

This paper presented an overview of applied design workflow and challenges in regards to FCS faced in the project WISDOM. Technological aspirations and problems were outlined. The applied process for the generation of a safe system architecture with the aspired functional extent and control surface layout was described and performed. The process involves an early application of ARP4761 safety assessments to enable a fast architecture safety evaluation. The central task in this is to find safety flaws in proposed and potential system architectures based on the initial functional description of a novel aircraft. The architecture design has disqualified various potential architectures for the simplex actuation of a triple split aileron. In the process, viable potential candidates were identified. Each of these candidates presents a set of technological challenges and requirements. The used design workflow facilitated an effective early focus to viable system architectures and an early estimate of the concepts realisability under safety critical considerations. This is especially important to cover design implications of the introduced new FCS functions. This enables The resulting system architecture for the actuation and control of the ailerons was presented. It contains one EMA per aileron and a three channel electrical HVDC power supply. The central requirements for the actuation system from the aircraft safety perspective especially were presented and outlined. Resulting controller performance requirements and structure requirements were identified.

ACKNOWLEDGEMENTS

This work was funded by the federal ministry for economic affairs and climate action (*Bundesamt für Wirtschaft und Klimaschutz*) of the German government based on a resolution of the Bundestag. The project WISDOM (20Y2105A) is part of the Federal Aeronautical Research Program (LuFo VI-2).

Contact address:

sascha.luebbe@dlr.de

References

[1] H. Schumann, S. M. Lübbe, T. Klimmek, and D. Quero Martin. Prüfstand für multifunktionale flugsteuerungssysteme zur lastminderung und flatterunterdrückung bei verkehrsflugzeugen. In *not yet published*, 2023.

[2] SAE International. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (ARP4761), 1996. DOI: 10.4271/ARP4761.

[3] SAE International. Guidelines for development of civil aircraft and systems (ARP4754A), 2010. DOI: 10.4271/ARP4754A.

[4] M. D. Krengel, M. Hepperle, and A. Huebner. Aeroservoelastic wing sizing using a physics-based approach in conceptual aircraft design. In *AIAA Aviation 2019 Forum*, Reston, Virginia, 06172019. American Institute of Aeronautics and Astronautics. ISBN: 978-1-62410-589-0. DOI: 10.2514/6.2019-3368.

[5] T. Klimmek, M. Schulze, and S. Wöhler. Development of a short medium range aircraft configuration for aeroelastic investigations using cpacs-mona. In *Deutscher Luft- und Raumfahrtkongress 2022*, September 2022.

[6] SAE International. Aircraft flight control systems descriptions, 2016. DOI: 10.4271/AIR4094A.

[7] SAE International. Description of actuation systems for aircraft with fly-by-wire flight control systems, 2012. DOI: 10.4271/AIR4253B.

[8] J.-C. Maré. Review and analysis of the reasons delaying the entry into service of power-by-wire actuators for high-power safety-critical applications. *Actuators*, 10(9):233, 2021. DOI: 10.3390/act10090233.

[9] R. Pratt. *Flight control systems*, volume v. 184 of *Progress in astronautics and aeronautics*. American Institute of Aeronautics and Astronautics, Herts, U.K and Reston, Va, 2000. ISBN: 9781600864360.

[10] M. V. Cook. *Flight Dynamics Principles: A Linear Systems Approach to Aircraft Stability and Control*. Elsevier Aerospace Engineering. Elsevier Science & Technology, Kidlington, 2nd ed. edition, 2007. ISBN: 9780080550367.

[11] R. Brockhaus, W. Alles, and R. Luckner. *Flugregelung*. Springer, Berlin and Heidelberg, 3., neu bearb. aufl. edition, 2011. ISBN: 9783642014420.

[12] I. Moir, A. Seabridge, and M. Jukes. *Civil avionics systems*. Aerospace series. Wiley, Chichester, 2. ed. edition, 2013. ISBN: 978-1-118-34180-3.

[13] J.-C. Maré. *Aerospace Actuators 1*. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2016. ISBN: 9781119307662. DOI: 10.1002/9781119307662.

[14] J.-C. Maré. *Aerospace Actuators 3*. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2018. ISBN: 9781119505433. DOI: 10.1002/9781119505433.

[15] D. Arriola and F. Thielecke. Design of fault-tolerant control functions for a primary flight control system with electromechanical actuators. In *2015 IEEE AUTOTESTCON*, pages 393–402. IEEE, 02.11.2015 - 05.11.2015. ISBN: 978-1-4799-8190-8. DOI: 10.1109/AUTEST.2015.7356523.

[16] M. Christmann, S. Seemann, and P. Jänker. Innovative approaches to electromechanical flight control actuators and systems. 2021.

[17] J. W. Bennett, B. C. Mecrow, A. G. Jack, and D. J. Atkinson. A prototype electrical actuator for aircraft flaps. *IEEE Transactions on Industry Applications*, 46(3):915–921, 2010. ISSN: 0093-9994. DOI: 10.1109/TIA.2010.2046278.

[18] C. Bauer, K. Lagadec, C. Bès, and M. Mongeau. Flight control system architecture optimization for fly-by-wire airliners. *Journal of Guidance, Control, and Dynamics*, 30(4):1023–1029, 2007. ISSN: 0731-5090. DOI: 10.2514/1.26311.

[19] S. E. Postnikov, A. A. Trofimov, and S. V. Baikov. Architecture options estimate for the near-medium-haul aircraft control system by the reliability, mass and power consumption criteria. *Aerospace Systems*, 2(1):33–40, 2019. ISSN: 2523-3947. DOI: 10.1007/s42401-018-0017-9.

[20] R. Bornholdt and F. Thielecke. Optimization of the power allocation for flight control systems. In *SAE Technical Paper Series*, SAE Technical Paper Series. SAE International400 Commonwealth Drive, Warrendale, PA, United States, 2014. DOI: 10.4271/2014-01-2188.

[21] T. Lampl, R. Königsberger, and M. Hornung. Design and evaluation of distributed electric drive architectures for high-lift control systems. In *DLRK 2017*. 2017.

[22] H. Fournier, P. Massioni, M. Tu Pham, L. Bako, R. Vernay, and M. Colombo. Robust gust load alleviation of flexible aircraft equipped with lidar. *Journal of Guidance, Control, and Dynamics*, 45(1):58–72, 2022. ISSN: 0731-5090. DOI: 10.2514/1.G006084.

[23] M. Pusch, A. Knoblach, and T. Kier. Integrated optimization of control surface layout for gust load alleviation. *CEAS Aeronautical Journal*, 10(4):1059–1069, 2019. ISSN: 1869-5582. DOI: 10.1007/s13272-019-00367-4.

[24] C. Wallace, S. Schulz, N. Fezans, T. Kier, and G. Weber. Evaluation environment for cascaded and partly decentralized multi-rate load alleviation controllers. 2022.

[25] Wolf R. Krueger, Johannes K. S. Dillinger, Yasser M. Meddaikar, Jannis Lübker, Martin Tang, Tobias Meier, M. Böswald, Keith Soal, Manuel Pusch, and Thiemo Kier. Design and wind tunnel test of an actively controlled flexible wing. 2019.

[26] N. Fezans, H.-D. Joos, and C. Deiler. Gust load alleviation for a long-range aircraft with and without anticipation. *CEAS Aeronautical Journal*, 10(4):1033–1057, 2019. ISSN: 1869-5582. DOI: 10.1007/s13272-019-00362-9.

[27] L. Klug, R. Radespiel, J. Ullah, F. Seel, T. Lutz, J. Wild, R. Heinrich, and T. Streit. Actuator concepts for active gust alleviation on transport aircraft at transonic speeds. In *AIAA Scitech 2020 Forum*, Reston, Virginia, 01062020. American Institute of Aeronautics and Astronautics. ISBN: 978-1-62410-595-1. DOI: 10.2514/6.2020-0271.

[28] J. Ullah, T. Lutz, L. Klug, R. Radespiel, and J. Wild. Active gust load alleviation by combined actuation of trailing edge and leading edge flap at transonic speeds. In *AIAA Scitech 2021 Forum*, Reston, Virginia, 01112021. American Institute of Aeronautics and Astronautics. ISBN: 978-1-62410-609-5. DOI: 10.2514/6.2021-1831.

[29] M. Hillebrand, J. Müller, and T. Lutz. Active gust alleviation on a high aspect ratio wing based on high fidelity cfd simulations. In *AIAA AVIATION 2023 Forum*, page 4347, 2023.

[30] C. Schneider, C. Wallace, N. Fezans, and T. Kier. Distributed active load control system. In *Towards Sustainable Aviation Summit 2022 (TSAS 2022)*. 2022.

[31] J. Theis, H. Pfifer, and P. Seiler. Robust modal damping control for active flutter suppression. *Journal of Guidance, Control, and Dynamics*, 43(6):1056–1068, 2020. ISSN: 0731-5090. DOI: 10.2514/1.G004846.

[32] R. Vepa and J. R. Kwon. Synthesis of an active flutter suppression system in the transonic domain using a computational model. *The Aeronautical Journal*, 125(1293):2002–2020, 2021. ISSN: 0001-9240. DOI: 10.1017/aer.2021.38.

[33] J.-C. Maré. *Aerospace Actuators 2*. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2017. ISBN: 9781119332442. DOI: 10.1002/9781119332442.

[34] E. Torenbeek. *Advanced aircraft design: Conceptual design, analysis, and optimization of subsonic civil airplanes*. Aerospace Series. Wiley, Chichester, 2013. ISBN: 9781118568088.

[35] EASA. Certification specifications and acceptable means of compliance for large aeroplanes (cs-25), 2022.

[36] FAA. Part 25 - airworthiness standards: Transport category airplanes: 14 cfr part 25.

[37] M. Schäfer, A. Berres, and O. Bertram. Integrated model-based design and functional hazard assessment with sysml on the example of a shock control bump system. *CEAS Aeronautical Journal*, 2022. ISSN: 1869-5582. DOI: 10.1007/s13272-022-00631-0.

[38] *Nonelectronic parts reliability data 2016*. Reliability databook series. Quanterion Solutions Incorporated, Utica, NY, 2015. ISBN: 1-933904-76-3.

[39] S. M. Lübbe, M. Schäfer, and O. Bertram. Coupling of model-based systems engineering and safety analysis in conceptual aircraft system design. In *33rd Congress of the International Council of the Aeronautical Sciences, ICAS 2022*, volume 2, pages 1484–1495, 2022.

[40] S. M. Lübbe, M. Schäfer, V. Voth, A. Berres, and O. Bertram. Interconnections in model-based safety analysis and systems design on the example of a fuel cell thermal management system for commercial aircraft. In *AIAA AVIATION 2023 Forum*, Reston, Virginia, 2023. American Institute of Aeronautics and Astronautics. ISBN: 978-1-62410-704-7. DOI: 10.2514/6.2023-4196.