aerospace

MDPI

Article

A Decentralized Voting and Monitoring Flight Control Actuation System for eVTOL Aircraft

Ruichen He [1,2], Florian Holzapfel [2], Johannes Bröcker [2], Yi Lai [2] and Shuguang Zhang [1,2,*]

[1] School of Transportation Science and Engineering, Beihang University, Beijing 100191, China; heruichen@buaa.edu.cn or ruichen.he@tum.de
[2] Institute of Flight System Dynamics, Technical University of Munich, 85748 Garching, Germany; florian.holzapfel@tum.de (F.H.); johannes.broecker@tum.de (J.B.); yi.lai@tum.de (Y.L.)
* Correspondence: gnahz@buaa.edu.cn or shuguang.zhang@tum.de; Tel.: +86-137-0114-4375

Abstract: The emergence of eVTOL (electrical Vertical Takeoff and Landing) aircraft necessitates the development of safe and efficient systems to meet stringent certification and operational requirements. The primary state-of-the-art technology for flight control actuation in eVTOL aircraft is electro-mechanical actuators (EMAs), which heavily rely on multiple redundancies of critical components to achieve fault tolerance. However, challenges persist in terms of insufficient reliability, immaturity, and a lack of a measurable evaluation method. This research addresses these issues by elucidating the design requirements for EMAs in eVTOL aircraft and proposing a systematic design and evaluation approach for EMA architecture. A key enhancement involves the incorporation of decentralized voting and monitoring (VoDeMo) mechanisms within the Electronic Control Units (ECUs) to improve the overall safety of the EMA. The paper introduces an innovative triple-dual redundant architecture for aircraft control effectors, comprising three dissimilar lanes of ECUs and two similar redundant parallel channels of power electronics and motors. The design is synergistically supported by a comprehensive evaluation that incorporates quantifiable Model-Based Safety Assessment (MBSA), utilizing both physical simulation and logical safety models. Hardware-In-the-Loop (HIL) tests are conducted on a constructed prototype to validate the proposed architecture.

Keywords: electro-mechanical actuator; model-based safety assessment; fault-tolerant architecture; voting and monitoring; eVTOL certification

Citation: He, R.; Holzapfel, F.; Bröcker, J.; Lai, Y.; Zhang, S. A Decentralized Voting and Monitoring Flight Control Actuation System for eVTOL Aircraft. *Aerospace* **2024**, *11*, 195. https://doi.org/10.3390/aerospace11030195

Academic Editor: Piotr Lichota

Received: 1 February 2024
Revised: 26 February 2024
Accepted: 27 February 2024
Published: 29 February 2024

1. Introduction

Electrical Vertical Takeoff and Landing (eVTOL) aircraft represent the forefront of aviation innovation, promising to redefine urban mobility and address the contemporary challenges of congestion, transportation inefficiency, and environmental concerns. This emerging urban air mobility (UAM) sector has attracted a wide array of entrepreneurs. However, some may not possess the necessary experience or resources for developing sophisticated civil aerial systems [1,2]. Despite this influx, stringent certification standards have not wavered [3]. The effective integration of eVTOL aircraft into urban spaces necessitates advanced flight control systems (FCS), particularly in the actuation domain, that prioritize both safety and efficiency. This becomes especially vital when considering the intricacies involved in vertical takeoffs, in-flight stability, and landings in densely populated areas [4,5].

In recent decades, the advent of more/all-electric aircraft (MEA/AEA) has prompted a transition from traditional hydraulic actuation systems to their electrical counterparts. The electro-mechanical actuator (EMA) is gaining popularity in aerospace applications, particularly in commercial transport aircraft [6], because it offers numerous benefits: it is fault-tolerant, more reliable, and leads to significant weight and volume reductions. Additionally, an EMA solely relies on electric power and streamlines transmission processes,

is more cost-effective, easier to maintain, and demonstrates enhanced efficiency, precision, and dynamic characteristics [7]. For taking advantage of these benefits, eVTOL aircraft, which are a subset of AEA, extensively utilize EMAs not only for flight controls but also for Lift–Thrust Units (LTUs), tilting mechanisms, and landing gears. Consequently, any kind of malfunction of the EMAs could become a safety-critical issue for this type of aircraft, and it ranks as one of the most prevalent degradation scenarios [8,9]. As state-of-the-art actuation technology, the greatest challenges in the development of EMA stem from the need for advanced fault-tolerant designs, redundancy management of intricate electronics, and efficient evaluation methods.

Certification standards for eVTOL aircraft demand exceptional safety measures for their actuating systems [3,10]. As eVTOL applications continue to evolve, meeting the rigorous safety and failure probability benchmarks set by SC-VTOL.2300 "Flight control systems" [3], SC-VTOL.2510 "Equipment, systems, and installations" [3], and MOC-4 SC-VTOL.2300 "Common Mode Failures and Errors in Fly by Wire Flight Control Functions" [10] is paramount. Consequently, there is a growing imperative for the development of novel system architectures in the EMAs tailored specifically for eVTOL aircraft.

Since the 1970s, research dedicated to fault-tolerant design within aerospace systems has surged, predominantly covering two principal domains: analytical redundancy and the design of redundant system architectures [11,12]. System architecture is an integration of redundant hardware and software components, health monitoring functions, and decision voting mechanisms to enhance dependability; such designs often result in increased weight, size, power consumption, and overall system complexity. The paradigm of the Boeing 777 Primary Flight Computer (PFC) [13] uses a decentralized output signal monitoring and voting mechanism in each of the triple-redundant PFC channels to compare inputs from multiple sources to determine the most likely correct action, which significantly enhances reliability by reducing single points of failure and common mode failure (CMF). Safe architecture design for flight control systems is becoming a popular topic in the area of eVTOL [14]. Fault-tolerant architectures designed for EMA applications have been extensively studied, with a primary emphasis on hardware redundancies, i.e., duplicating mechanical elements and the actuator control electronics (ACE). Qiao et al. classified the design of EMAs into three distinct types based on the levels of redundancies, and comprehensively analyzed the advantages and disadvantages of each type [7]. Ismail et al. evaluated several flight control EMA architectures [15], and further developed the optimal one. Improving the reliability and efficiency of the system architecture of EMAs remains a challenge. Additionally, the establishment of an effective evaluation method is also a pivotal concern in both scientific research and engineering practice.

For safety evaluation, Model-Based Safety Assessment (MBSA) has emerged as an invaluable tool in the development and assessment of such complex systems, allowing for rigorous system-level testing and validation prior to physical implementation [16]. Within the aviation industry, certification authorities take SAE ARP4754B [17] and SAE ARP4761A [18] as the guiding materials for ensuring and demonstrating the safety of aviation systems. MBSA provides visualization for the effects of events via fault injection; it can be used to assess independent features or CMFs. The frame activities of MBSA are described as nominal system modeling, formalizing derived safety requirements, fault modeling, composing system and fault models, and formal safety analysis [19]. State-of-the-art research has already implemented the novel techniques regarding the development of EMA [20,21]. In this research, we use MBSA in combination with the Hardware-In-the-Loop (HIL) test to demonstrate the safety and fault-tolerant performance of the designed EMA architecture.

The remainder of this paper is organized as follows. Section 2 outlines the architecture design approach of EMA for eVTOL. Section 3 details the design and design process of the proposed VoDeMo EMA architecture. Section 4 covers the evaluation and validation of the designed architecture, including establishing models and test prototypes, followed by

an assessment of potential failures with corresponding simulation and test results. Lastly, Section 5 draws conclusions and discusses potential future works building on this research.

2. Outline of EMA on eVTOL Aircraft

2.1. EMA for eVTOL Flight Control

Studies have proven that powered-by-wire EMAs benefit flight control by having high power density and energy efficiency, fast dynamic response, and high reliability. Thus, despite variations, all eVTOLs rely on EMAs for most of the control actuation. Control surfaces, including primary controls and some secondary controls, are essential not only in cruise flight but also during transition and hover phases. Lift–Thrust Units (LTUs) in eVTOLs serve multi-functional roles, generating thrust, lift, and aiding in steering, requiring precise control due to vibrations. Tilting mechanisms are safety-critical for facilitating the transition between vertical and horizontal flight. Landing gears with degrees of freedom, including extension/retraction, steering, and braking, are crucial for safe operations in confined spaces. Additionally, EMAs in some eVTOLs perform extra functions, such as deploying parachutes and operating doors, contributing to overall system versatility.

2.2. Design Requirements and Principles

Safety Requirements

Certification of eVTOLs necessitates stringent measures to ensure safety.

The SC-VTOL.2510(a) [3] mandates that a single failure must not lead to a catastrophic failure condition, which should be evaluated by a functional hazard analysis (FHA) at the aircraft level. Furthermore, any catastrophic failure condition must be classified as extremely improbable.

The MOC 4 VTOL.2300 [10] suggests adhering to ARP4754B [17], DO-254 [22], and AMC 20-115D [23] guidelines to curtail the risk of CMFs during the developmental phase.

Traditionally, one method to reduce the impact of CMFs is by employing dissimilar components at the system level; this often meant procuring components from multiple manufacturers. For instance, an eVTOL design comprising 50% of its actuators from one supplier and the rest from another would, in the event of a CMF, stand to lose half its actuation capabilities. This approach might fall short in ensuring desired reliability and could also infringe upon weight limitations. Consequently, novel solutions are sought after.

The strategy of VoDeMo is introducing intrinsic dissimilarity within the EMA itself, guaranteeing that control mechanisms remain fail-operational, thus mitigating possible failure conditions.

Functional Separation

EVTOL aircraft are equipped with numerous Battery Management Systems (BMSs), and electrical power of high and low voltage is allocated to the EMAs' motor drives and ACEs, respectively. In the case of the aircraft losing one or more of the BMSs, the EMAs should retain partial functionality. Within the VoDeMo framework, each of the motor drive channels receives power from an independent power supply (e.g., 48Vdc). Conversely, every digital processor draws power from two parallel low-voltage power sources (e.g., 3Vdc).

Within the ACE, in order to prevent non-equal control, although there can be more than one dissimilar processor executing the same control algorithm, their roles should be differentiated. In VoDeMo concept, a Digital Simple voter is placed between the triple-redundant ACE and the dual motor drive channels. The voter operates on a majority-decision principle, ensuring only one ACE lane transmits command to the motor drive channels at a time; meanwhile, the others function as monitors. A more in-depth exploration of this mechanism is reserved for the subsequent section.

Component Separation

The design of the EMA architecture should ensure that each redundant component is isolated. The separation and isolation consider both physical and electrical aspects.

The VoDeMo framework emphasizes the segregation of its low-power digital computation modules, high-power analog elements, and mechanical components. This clear delineation not only streamlines the structure and interfaces among components but also significantly mitigates risks associated with common cause and cascading failures. For instance, without this separation, the heat and vibration generated by the motors can endanger other circuit boards and connections. Moreover, a short circuit in one channel's power electronics could compromise the motor driver. In a worst-case scenario, the unchecked surge from such a short circuit might jeopardize the ACEs and motors, potentially leading to a fire, which could compromise the entire EMA and endanger the aircraft's safety. Thus, this component separation serves as a protective barrier against failure propagation.

Structural Impact on the Aircraft

The VoDeMo framework's design confronts significant challenges in terms of weight, size, and integration. Compared to traditional small airplanes and rotorcraft, eVTOL aircraft typically feature a greater number of actuators and novel EMA applications, such as tilting mechanisms. Consequently, it is imperative for the EMAs to be lightweight to maximize payload capacity and efficiency, and their compactness is crucial for seamless integration within the aircraft's confined airframe space.

2.3. Design Methodology

In light of these requirements, fault-tolerant architecture design (FTAD) of the actuating system is imperative. This can be approached either from an overarching aircraft level or at the granularity of the actuator system level. At the aircraft level, the FTAD is realized through control reconfigurations managed by the FCCs. When FCCs detect a fault, they seamlessly switch between control laws, either passivating or deactivating the faulty actuator, and capitalizing on the availability of multiple actuators. While this approach safeguards the aircraft's operational safety despite a compromised actuator, diminished aircraft controllability resulting from such failures remains a notable concern. On the other hand, the actuator level FTAD concentrates on enhancing actuator reliability. Ismal et al. investigated the off-the-shelf technologies, identifying six types of state-of-the-art architecture designs [24].

This research focuses on FTAD within the actuator system; the main rationales and features include the following:

Redundancy: The bedrock of this approach is system redundancy. The FTAD of EMA might include dual motors, integrated through gearbox, electric clutches, or directly to the output shaft. Dual-winding single motors are also prevalent. Multiple processors facilitate decentralized control and monitoring, allowing the system to detect and bypass erroneous commands. While hardware redundancy is common, some designs also utilize software redundancy for control and monitoring. Redundancies are always incorporated in position sensors to mitigate their insufficient reliability. Additionally, the FCC commands can be duplicated. To manage inconsistencies in FCC commands, sensor readings, and control values, fusing/voting algorithms are developed to determine the most likely correct value, or to take corrective action upon detecting any malfunctions.

Operating Configurations: EMAs with dual motors can operate in three modes: active/active, active/passive, or active/no-load. In the active/active configuration, both channels function simultaneously. In active/passive, one channel is operating while the other remains in a dormant force-free state. The active/no-load configuration has one driving channel, with the other being disconnected via an electric clutch. In both the latter configurations, if the active channel encounters a failure or receives a specific command, there is a switchover to the standby channel. Yet, these configurations have drawbacks like deadweight and possibly failing in activating either of the two channels. Hence, for higher efficiency and reliability, most existing aircraft EMAs adopt the active/active configuration.

Fail-Safe Modes: The active/active configuration can experience force fighting between the two channels. Significant discrepancies, especially during faults, can induce

undue vibrations. To counteract this, a fail-safe mode is essential, either by passivating the malfunctioning channel or disengaging it from the output mechanism.

3. VoDeMo EMA Architecture Design

The VoDeMo design follows the approach in SAE ARP4754B, and a detailed model-based design process has been presented in [25]. The produced blueprint is a triple-lane, dual-channel redundant architecture of EMA, as shown in Figure 1.

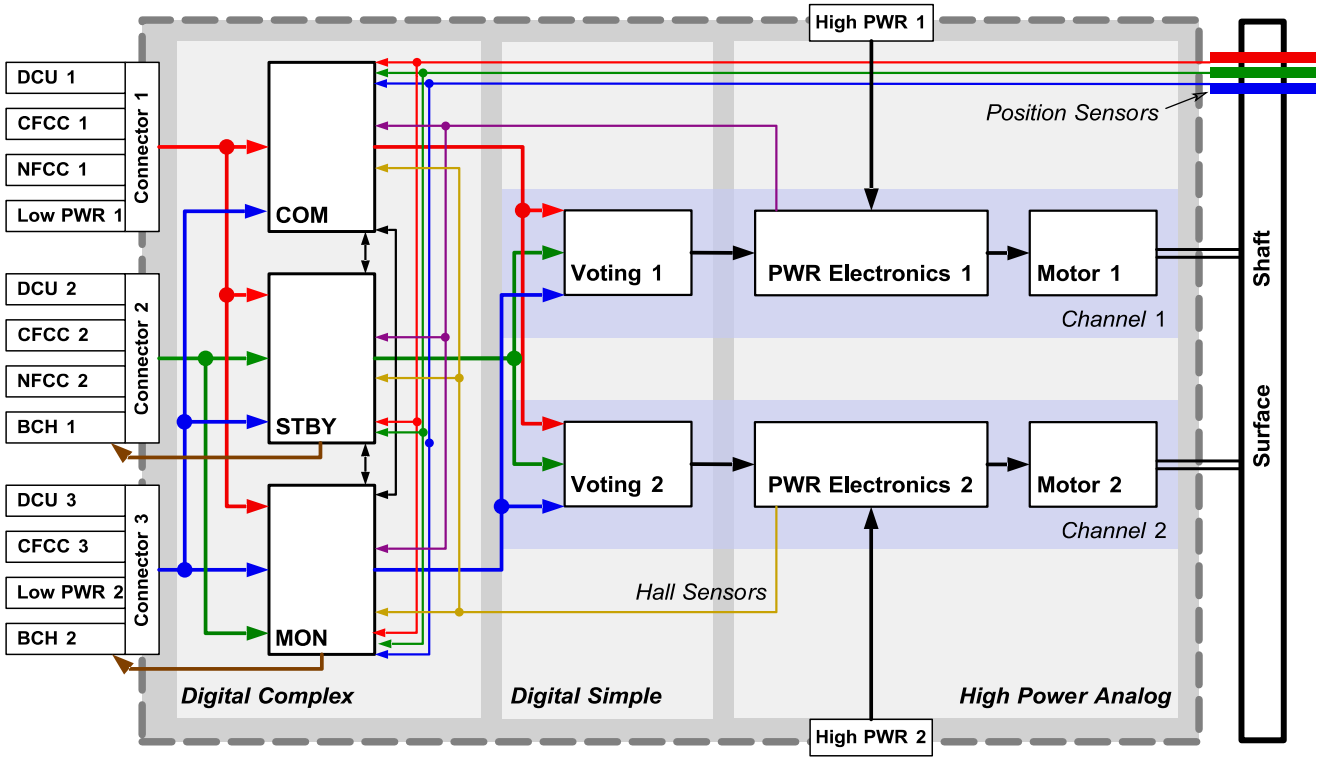

Figure 1. VoDeMo architecture schematic.

3.1. Overview

The essential components of an EMA encompass the following:

Actuator Control Electronics (ACE): the ACE is essentially a micro-controller. It decodes input signals originating from the flight control computers (FCCs), integrates feedback from position sensors, and subsequently relays commands to the power electronics.

Power Electronics: Within this segment, there is a motor driver that interprets command signals from the ACE, amplifying these through voltage pulse width modulation (PWM) to produce motor currents. Moreover, an inverter, utilizing MOSFETs, transitions DC current to AC current, subsequently powering the motor.

Mechanical Assembly: At the heart of the EMA is the electric motor, which efficiently transmutes electrical energy into rotational motion. For the purposes of this study, three-phase brushless DC motors are the chosen type. This assembly also includes various transmission mechanisms, such as gear and screw jacks, which facilitate the actuation process.

Position Sensors: Integral to the system, position sensors on the output shaft provide real-time feedback on the position, enabling the ACE to make informed decisions and adjustments.

The VoDeMo EMA system physically consists of four primary subsystems: a low-power Digital Complex, a Digital Simple, a High-Power Analog, and a mechanical output

shaft, typically manifested as a control surface. The Digital Complex and the Digital Simple form the ACE in the VoDeMo framework.

The VoDeMo system's interfaces encompass data buses and a low-power supply, distributed and harnessed over three connectors. As the EFCS of eVTOL is designed with the capability of providing different levels of automation, the VoDeMo's connectors are designed to interface with two Nominal FCCs (NFCCs), three Critical FCCs (CFCCs), and three Data Concentrate Units (DCUs). The NFCCs execute the primary control law, conforming to the high-standard Simplified Vehicle Operation (SVO), which necessitates real-time feedback on actuator positions. This feedback is relayed from the Digital Complex through dedicated backchannels. In contrast, in a downgraded FBW scenario, the CFCCs are responsible for the secondary control law. Meanwhile, DCUs serve as a contingency measure, managing direct control to the control effectors.

3.2. Digital Complex

Engineering practice and experiments in aerospace field have proved the necessity of dissimilarity in program risk reduction, and triple redundancy for hardware in all computing systems is an outcome of the design evolution of the fly-by-wire (FBW) concept. Consequently, the Digital Complex of VoDeMo is designed consisting of three microprocessors from three different producers. The three concurrent computing lanes, namely the Command Lane (COM), Standby Lane (STBY), and Monitor Lane (MON), operate simultaneously but with degrading priority; COM holds the highest priority, while MON has the lowest.

Figure 2 illustrates the schematic of the COM lane's functional architecture, which is shared among the other two lanes. The three physically independent and dissimilar lanes in Digital Complex commonly serve the following functions:

Monitoring FCC Inputs: Each lane monitors the signal sources from connected data buses and selects the valid and active reference position command for the control loops. The source selection is based on Algorithm 1.

Algorithm 1: FCC Input Monitoring

input : Input validity check $Vflag_{\text{CMD\_Prm}}$, $Vflag_{\text{CMD\_Scd}}$, $Vflag_{\text{CMD\_Dir}}$,
Input updating check $Uflag_{\text{CMD\_Prm}}$, $Uflag_{\text{CMD\_Scd}}$, $Uflag_{\text{CMD\_Dir}}$,
Command inputs $POS_{\text{CMD\_Prm}}$, $POS_{\text{CMD\_Scd}}$, $POS_{\text{CMD\_Dir}}$

output: Decision of signal source selection POS_{ref},
Control validity check $Vflag_{\text{current}}$

initialization;
if $Vflag_{\text{CMD\_Prm}} == \text{true}$ *and* $Uflag_{\text{CMD\_Prm}} == \text{true}$ **then**
  $Vflag_{\text{current}} = \text{true}$;
  $POS_{\text{ref}} = POS_{\text{CMD\_Prm}}$;
  return $Vflag_{\text{current}}$, POS_{ref}
else if $Vflag_{\text{CMD\_Scd}} == \text{true}$ *and* $Uflag_{\text{CMD\_Scd}} == \text{true}$ **then**
  $Vflag_{\text{current}} = \text{true}$;
  $POS_{\text{ref}} = POS_{\text{CMD\_Scd}}$;
  return $Vflag_{\text{current}}$, POS_{ref}
else if $Vflag_{\text{CMD\_Dir}} == \text{true}$ *and* $Uflag_{\text{CMD\_Dir}} == \text{true}$ **then**
  $Vflag_{\text{current}} = \text{true}$;
  $POS_{\text{ref}} = POS_{\text{CMD\_Dir}}$;
  return $Vflag_{\text{current}}$, POS_{ref}
else
  $Vflag_{\text{current}} = \text{false}$;
  $POS_{\text{ref}} = \text{Default}$;
end

This algorithm shows that the control lane primarily adheres to the control law under nominal conditions. However, in cases where the signal validity or activation is compromised, the control transitions to a secondary law. If even the secondary law cannot be employed due to signal failure, the system reverts to direct law. In extreme scenarios, the control system will be deactivated.

Fusing Sensor Feedback Signals: Each lane receives data from multiple dissimilar position sensors and hall sensors. The sensors may operate at different rates. Furthermore, variations may arise due to inherent sensor biases and covariances, even in the absence of fault. Additionally, there could be faulty measurements. To ensure a consistent measurement data stream for integration into the control loops, the Digital Complex has the responsibility of consolidating and processing these signals. In this context, an Extended Kalman Filter (EKF) is employed as a solution to address these challenges. The state vector for time instant k is defined as $\boldsymbol{x}_k = \begin{bmatrix} \alpha_k & \omega_k \end{bmatrix}^\top$, where α is angular position and ω is the rotational velocity.

The process noise vector $\boldsymbol{w}_k = w_k$ is introduced to account for variations in angular rate arising from transient motor torque, airflow-induced disturbances, and friction on the control effector, mitigating uncertainty in the system.

The discrete-time state transition equation of the system can be written as

$$\begin{aligned} \boldsymbol{x}_k = \begin{bmatrix} \alpha_k \\ \omega_k \end{bmatrix} &= \begin{bmatrix} \alpha_{k-1} + \dfrac{(\omega_k + \omega_{k-1})}{2}\Delta t \\ \hat{\omega}_{k-1} + w_k \end{bmatrix} \\ &= \begin{bmatrix} \alpha_{k-1} + \omega_{k-1}\Delta t + w_k \dfrac{\Delta t}{2} \\ \hat{\omega}_{k-1} + w_k \end{bmatrix}, \end{aligned} \tag{1}$$

The measurement vector $\boldsymbol{z}$ is defined as

$$\boldsymbol{z}_k = \begin{bmatrix} z_{\text{pos}} \\ z_{\text{hall}} \end{bmatrix} = \begin{bmatrix} \alpha_k + v_{\text{pos},k} \\ \omega_k + v_{\text{hall},k} \end{bmatrix}, \tag{2}$$

where z_{pos} and z_{hall} are the position and rotational velocity measured by the position and Hall sensors, respectively, $v_{\text{pos},k}$ and $v_{\text{hall},k}$ are the measurement noises.

These two equations can be reformulated in a linear state-space form as

$$\boldsymbol{x}_k = \begin{bmatrix} 1 & \Delta\, t \\ 0 & 1 \end{bmatrix} \boldsymbol{x}_{k-1} + \begin{bmatrix} \dfrac{\Delta t}{2} \\ 1 \end{bmatrix} \boldsymbol{w}_{k-1}, \tag{3}$$

$$\boldsymbol{z}_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \boldsymbol{x}_k + \begin{bmatrix} v_{\text{pos},k} \\ v_{\text{hall},k} \end{bmatrix}. \tag{4}$$

With the state transition and measurements functions, further applying the linear EKF [26], data fusion can be performed.

The EKF also monitors the residuals of the measurements in case, when some of them exceed a predefined threshold, the corresponding sensor(s) will be regarded as faulty. Then, the Digital Complex isolates the failed one and utilizes the remaining data.

Implementing Control Loops: The Digital Complex executes a position control loop as well as a speed control loop. Detailed consideration has been presented in [25].

Cross-lane Communication and Synchronization: The introduction of distributed dissimilar microprocessors within the Digital Complex introduces asynchronous behavior, stemming from the absence of a shared time reference, and variations in compilers. These factors significantly elevate the risk of generating inconsistent commands. To address this issue, we incorporate cross-lane communication and synchronization mechanisms to mitigate these challenges.

The cost-effective cross-lane synchronization method is presented in [27]. The method is based on message exchange algorithms and does not require any additional hardware support.

Cross-lane Monitoring: With the Digital Complex, cross-lane communication enables each microprocessor to monitor its control value by comparing it with the control values from the other two lanes. Taking the COM lane as an instance in Figure 2, the monitor algorithms, after inspecting the updating flags, calculate the real-time norm difference of command values between the COM lane and the other two lanes. This calculated difference is then compared to a predefined threshold. The outputs are two binary equality discretes (BEDs), denoted as "$C == S$" and "$C == M$"; if "$C == S$" is evaluated as "true", it signifies that "$||C - S|| < \varepsilon$", "ε" represents the threshold.

Each lane independently generates two BEDs that cross-check with the other two lanes. These six BEDs are transmitted to the Digital Simple via GPIOs for a decisionmaking voting process, which will be detailed in the following description of the Digital Simple.

Backchannel: The Digital Complex delivers vital feedback to external components, such as the Flight Control Computers (FCCs), which encompasses the real-time information on both the control effector's position and rotational rate. This comprehensive methodology reinforces the resilience and accuracy of the EFCS.

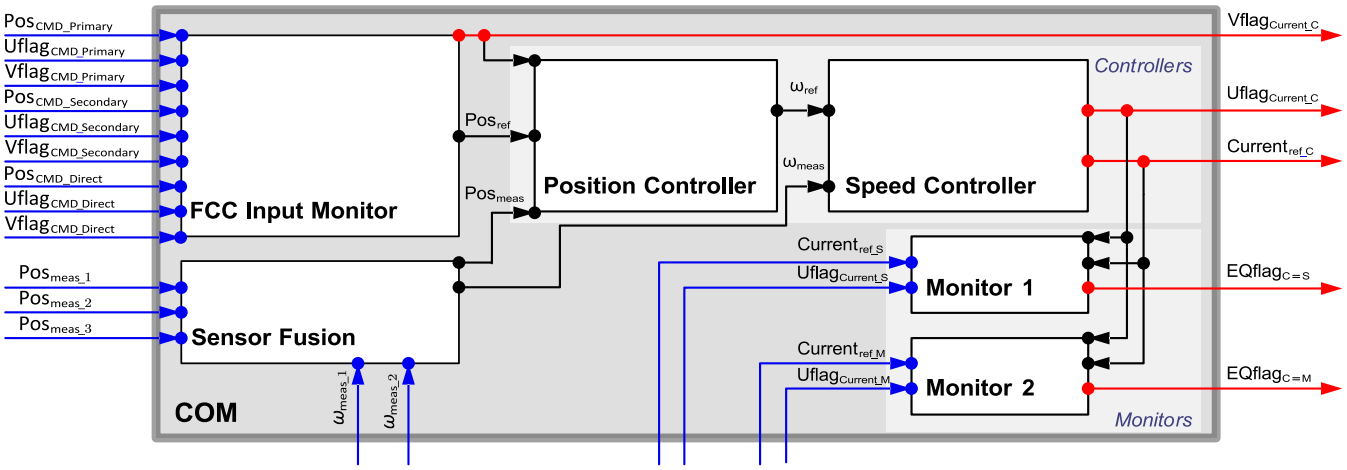

Figure 2. COM lane of the Digital Complex.

3.3. Digital Simple

The Digital Simple is implemented on a Programmable Logic Device (PLD) board, as illustrated in Figure 3. Control commands from both the COM and STBY lanes within the Digital Complex are conveyed via two RS422 buses, while the BEDs are connected through General-Purpose Input/Output (GPIO) interfaces.

The voting logic embedded in the Digital Simple ensures that a command, whether it is COM or STBY, is selected only when there is concurrence with at least one other command of the same value. This equality is double-verified by monitors in both lanes. Moreover, in the event that all three commands are identical in a nominal scenario, the COM command takes precedence over the STBY command. The MON does not transmit any signal in any circumstance. Should there be a lack of consensus among the three commands, the switch within the PLD transitions to a "Passive" mode, which corresponds to a predefined hard-coded message for the respective element.

The vitality of individual lanes is regularly verified through the transmission of a validity flag or heartbeat encoded within control command messages, labeled as CoK, SoK, and MoK. These signals are also routed to the Digital Simple component. In the event that only one or no lane remains operational, the system transitions into the passive mode.

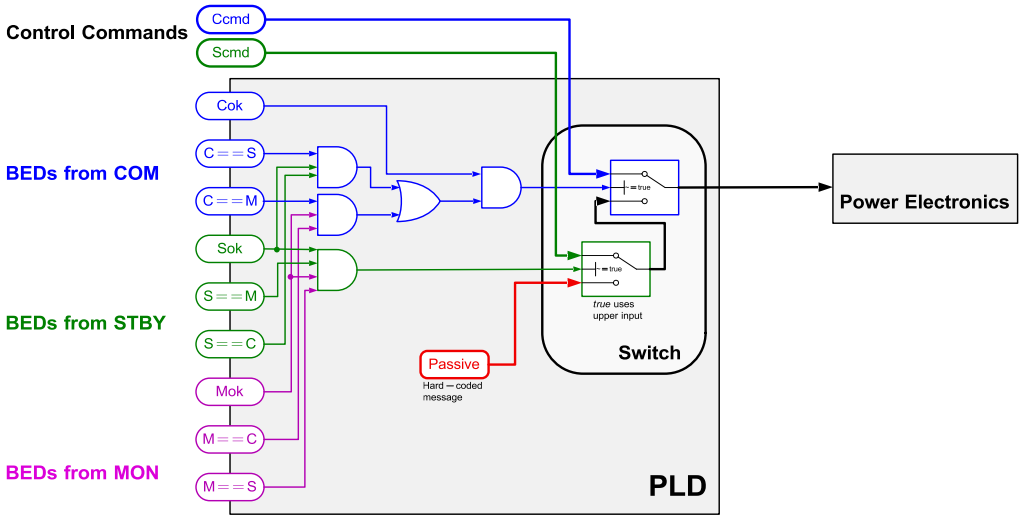

Figure 3. Digital Simple.

3.4. High-Power Analog

The High-Power Analog mainly consists of two power electronics and two motors, which form into two independent channels. Within each power electronic, there is an application-specified integrated circuit (ASIC) mainly implemented with current controller, a PWM generator, and a power inverter. Detailed description and modelling approach have been presented in [25].

The two motors drive a mutual shaft directly; in that way, the torques from the two channels of High-Power Analog are consolidated.

4. Evaluation

The VoDeMo system was meticulously designed with a consistent integration of safety evaluation throughout its development. The evaluation was aided by a safety model, a simulation model, and HIL test.

4.1. Preliminary Safety Assessment Based on Abstract Architecture Model

In the early design phase, we devised an MBSA method to identify dependencies and failure propagation within a proposed architecture. This method allows us to generate safety artifacts, e.g., minimum cut sets (MCSs), for a quantifiable evaluation. This method is adaptable to diverse intricate safety-critical systems.

The safety model that underpins the MBSA is deterministic, formal, and modular; it abstracts the architecture outlined in Figure 1, encapsulating the lowest level of design decisions. An illustration of this abstraction process is presented in Figure 4, demonstrating the transformation of a hardware component into a node within the safety model.

Within the abstract architecture model, each node signifies a system component, encompassing inputs/outputs, power sources, source selection logic, behavioral/reconfiguration logic, failure logic, and propagation logic. Moreover, the data flow and connections are discretized into specific datasets, including boolean, enumerated, or structured data types. This modeling methodology enhances the lucid representation of status transmission within the system, elucidating algorithmic dependencies and potential routes for failure propagation.

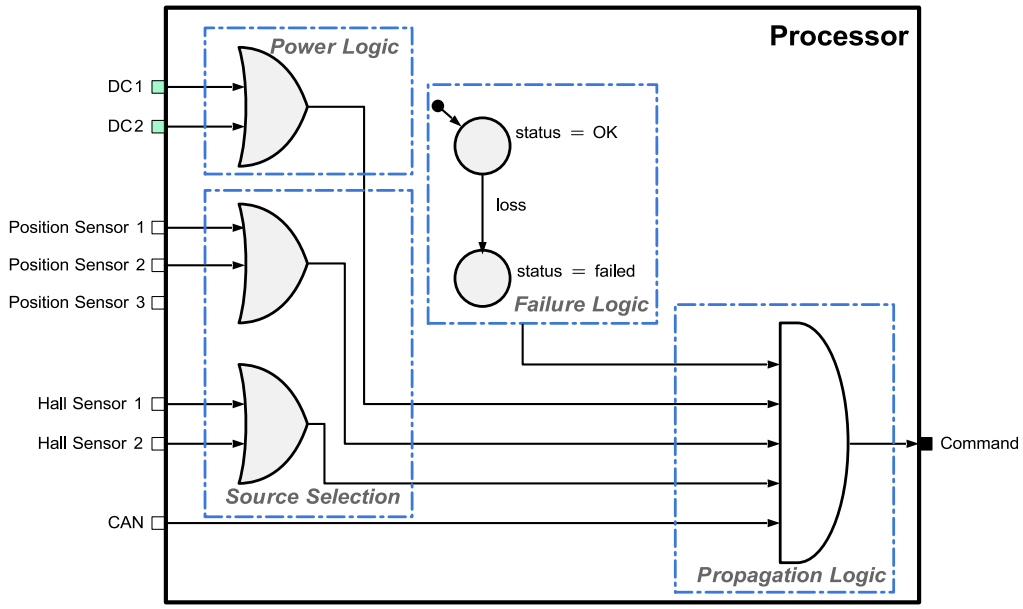

Figure 4. Example of a node in the safety model.

In the FHA of VoDeMo, the hazardous condition is defined as the 'loss of controllability by the EMA'. The primary safety objective of the architecture design is to prevent any individual failure modes or events that could lead to this occurrence. Integration of the *ExCuSe* tool [28] with the safety model facilitates the systematic common cause analysis (CCA) of the top event aligned with the safety objective. The result is the automatic generation of an MCS tree, as illustrated in Figure 5. Each MCS within the tree encompasses several basic events, where each basic event corresponds to a component losing its intended functionality. When all basic events within an MCS happen simultaneously, the top event is triggered, and the primary safety objective is compromised.

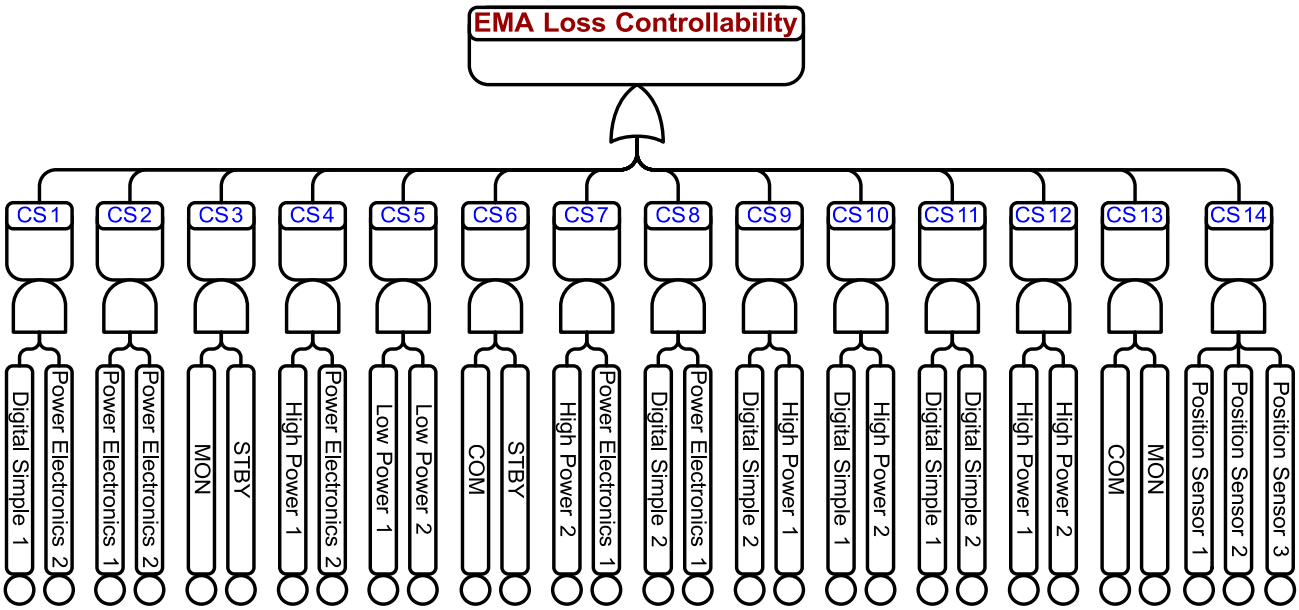

Figure 5. Minimum cut sets.

From Figure 5, it is evident that there are fourteen MCSs leading to the top safety event—loss of the controllability of the EMA. These including thirteen two-order MCSs and one three-order MCS. This demonstrates that no single point of failure can compromise the system. Furthermore, the proposed method significantly streamlines the workload and dif-

ficulty associated with architecture design concerning common cause failures (CCFs) since it clearly resolves dependencies and failure propagation. Based on this, the architecture design places emphasis on ensuring independence between each component associated with every MCS. This is achieved by introducing dissimilarities for redundant hardware, applying installation rules, and implementing physical segregation measures, such as structural barriers.

With the generated fault tree with MCSs, the system failure rate can be worked out. A few methods are compared hereinafter:

The characterization of component faults has been modeled using exponential distributions. In order to expedite the estimation of system failure probability, constant failure rates have been assigned to each specific type of component, as outlined in Table 1.

Table 1. Failure rates of components (per flight hour) [29].

Component Type	Failure Rate/fh
Digital Complex	5×10^{-4}
Digital Simple	1×10^{-5}
Power Electronics	1×10^{-4}
High Power Input	1×10^{-5}
Low Power Input	1×10^{-5}
Position Sensor	1×10^{-3}

Assuming all basic events are independent, then the failure rate of each MCS_i is

$$P(MCS_i) = \prod_{j=1}^{m} P_{ij} \tag{5}$$

here, P_{ij} is the failure rate of event j, assuming there are m basic events within MCS_i.

The exact probability of the overall system failure can be found based on calculation according to the *inclusion–exclusion principle* [30]; the function is

$$P_{sys} = \sum_{i=1}^{n} P(MCS_i) - \sum_{i,w:i<w}^{n} P(MCS_i \cap MCS_w) + \cdots + (-1)^{n-1} P\left(\bigcap_{i=1}^{n} MCS_i\right) \tag{6}$$

where n is the quantity of MCSs. P_{sys} is the probability of the system failure.

Inclusion–exclusion is the most precise method. Nevertheless, the application of this approach becomes notably time-consuming as the quantity of MCSs increases. Consequently, various alternative approximation methods are adopted to compute the probability of the top-level event based on the MCSs:

Rare events approximation:

$$P_{sys} = P\left(\bigcup_{i=1}^{n} MCS_i\right) \leqslant \sum_{i=1}^{n} P(MCS_i) \tag{7}$$

Esary–Proschan upper bound:

$$P_{sys} \leqslant 1 - \prod_{i=1}^{n} (1 - P(MCS_i)) \tag{8}$$

Recursive inclusion–exclusion:

$$P_{sys} \geqslant p_A + p_B - p_A p_B, p_A = P(MCS_1), p_B = \begin{cases} P(MCS_2) & \cdots \ n = 2 \\ P\left(\bigcup_{i=2}^{n} MCS_i\right) & \cdots \ n > 2 \end{cases} \tag{9}$$

The transient failure probability calculated by the four aforementioned methods in functions 6–9 are displayed in Figure 6. The Esary–Proschan upper bound and recursive inclusion–exclusion methods are theoretically equivalent; however, numerically, the latter

may exhibit greater stability. In cases where the MCSs are pairwise-independent, meaning no two MCSs share common events, both techniques yield exact results. Examination of the curves in Figure 6 and results presented in Table 2 reveals that, for mission time within 1000 h, all four methods yield precise probabilities with minimal discrepancies, and, for flight hours up to 1000, there is minimal disparity between the exact probability and the approximated results. Rare Events Approximation emerges as the simplest and most efficient method, delivering satisfactory precision.

Table 2. VoDeMo failure rate and failure probability.

Methods	Failure Rate/fh	Failure Probability (4 h)
Rare Events Approximation	$7.6512238567 \times 10^{-7}$	$3.0678917175 \times 10^{-6}$
Esary–Proschan Upper Bound	$7.6512238567 \times 10^{-7}$	$3.0678917175 \times 10^{-6}$
Recursive Inclusion–Exclusion	$7.6512238567 \times 10^{-7}$	$3.0678917175 \times 10^{-6}$
Exact Inclusion–Exclusion	$7.6512238567 \times 10^{-7}$	$3.0678917175 \times 10^{-6}$

Assuming the longest continuous mission time for eVTOL flight is 4 h, from Figure 6, we can determine the VoDeMo EMA system failure rate per flight hour and its failure probability over a full 4-h mission; see Table 2. The result shows a desirable reliability for certification under EASA SC-VTOL-01 Subpart F [3].

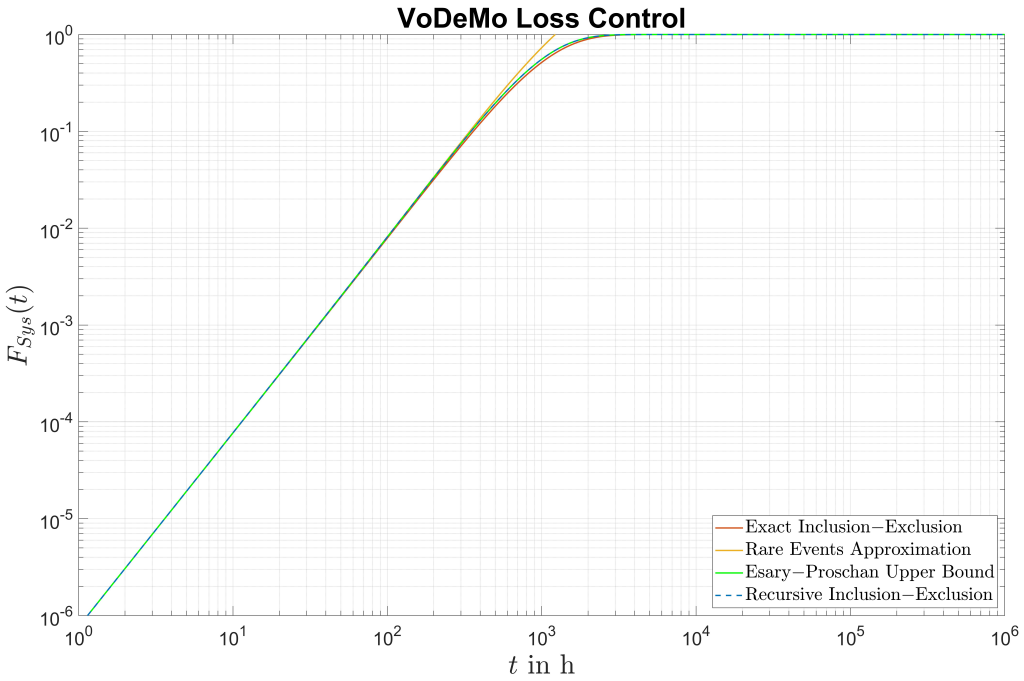

Figure 6. Failure probability transient evaluation with four methods.

4.2. Qualitative Safety Validation with Simulation Model and HIL Test

In order to validate the architecture design and the preliminary analysis, a combination of MBSA and HIL tests is incorporated utilizing the simulation model detailed in [25] and the Actuator Test Bench at the Institute of Flight System Dynamics, Technical University of Munich, as described in [31]. The initial stage of the validation approach involves a systematic exploration of potential failure modes, followed by fault modeling and testing based on the identified failure list to analyze their effects. This method allows for a thorough understanding and mitigation of potential issues in the design of EMAs; it facilitates trial and error during the early design phase and continues to be valuable in the subsequent design validation.

EMAs often operate under harsh environments, including high air pressure, low temperature, elevated humidity, and intricate signal interference. Consequently, various failures may occur in each component of EMAs. The categorization of failure modes in widely used electronic hardware is addressed by various standards, such as MIL-HDBK-338B (US Department of Defense, 1998) [32]. Schallert, C. proposed a comprehensive classification system encompassing failure modes in electrical, mechanical, hydraulic, power, and control systems, among others. In his work, he delineates four levels of hardware statuses; see Table 3 [33]. Mode 0 signifies normal function, while modes 1 and 2 denote distinct losses of functionality, distinguished by the disappearance of flow variables and potential variables, respectively. Additionally, mode 3 encompasses failures resulting from inadvertent activation.

In accordance with this approach, we can systematically enumerate the failure modes of the VoDeMo EMA system for further testing; see Table 4.

Table 3. General component failure modes definition.

Mode	Description	Effect
0	normal function	-
1	loss of function (flow var.)	de-energized, no active motion
2	loss of function (pot. var.)	de-energized, jam or overload
3	inadvertent function	uncommanded motion

Figures 7 and 8 denote the schematic and setup of the VoDeMo test bench. Within the test prototype, the Laboratory PC (Lab PC) directs the FCC to transmit commands to the VoDeMo Digital Complex processors. Upon receiving these commands, the VoDeMo independently computes the desired current command three times across its three distinct processors. Subsequently, the results undergo a voting process, and the final current command is dispatched to the motor control boards. These motor control boards, in turn, generate the desired three-phase DC output for their respective Brushless Direct-Current (BLDC) motors. These motors are interconnected on the shaft of the load motor. The Lab PC can instruct the load motor to generate a specified wind profile applied to the shaft. Three rotary sensors attached to the shaft measure its position and relay this information back to the VoDeMo processors. Additionally, the VoDeMo maintains a debug communication channel with the Lab PC for logging purposes.

Table 4. Overview of VoDeMo system failure modes.

Component	Mode			
	0	**1**	**2**	**3**
Bus	Healthy	Loss connection	Interrupted	False but valid signal (delay, drift, intermittent. . .)
Processor	Healthy	Lost	Faulty output	Asynchronous computation
Power electronic	Healthy	Open circuit	Short circuit	PWM frequency reduction Asynchronous computation
Motor	Healthy	Open circuit	Short circuit	Stator resistance reduction Magnetic flux reduction
Shaft	Healthy	Disconnection	Jam	Friction increment, Disturbance
Sensor	Healthy	Lost	Blocked	Precision degraded (biased, delayed, etc.)

Appendix A presents the detailed outcomes of the qualitative Failure Modes and Effects Analysis (FMEA) conducted to ascertain the capability of the VoDeMo architecture in addressing potential failures. The objective of the FMEA is to validate the system's capacity

to manage all conceivable failures, ensuring no insufficient redundancy or unaccounted failure propagation, and, in the event of a highly severe and rare probability occurrence, the system will seamlessly transition into a passive or fail-safe mode instead of undergoing any unpredictable behavior.

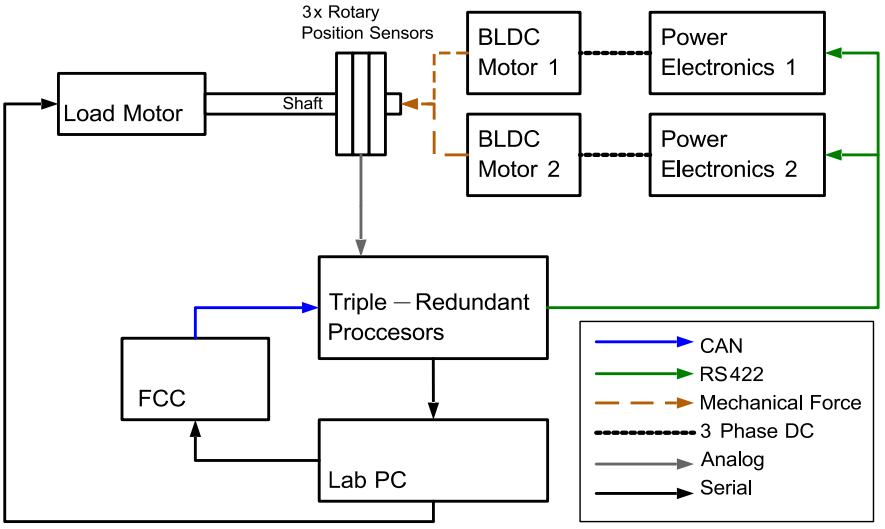

Figure 7. VoDeMo test bench schematic.

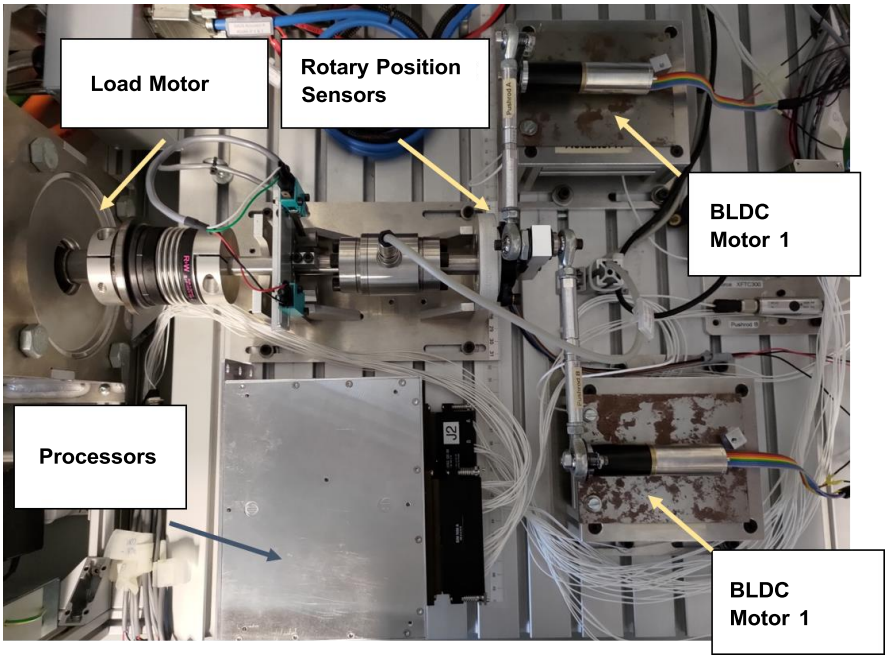

Figure 8. VoDeMo test bench setup.

Test results illustrating two typical failure modes are depicted in Figures 9 and 10, serving as illustrative examples. The first three subplots in each figure show the dynamic response of the overall EMA system in both the healthy condition (blue dashed curve) and the faulted condition (red curve) following a given command (green curve). The last subplot in each figure displays the resolved torques on the two channels in the faulted condition (magenta and cyan curves) compared to the blue dashed curve showing that the torques are equal on the two channels in healthy condition.

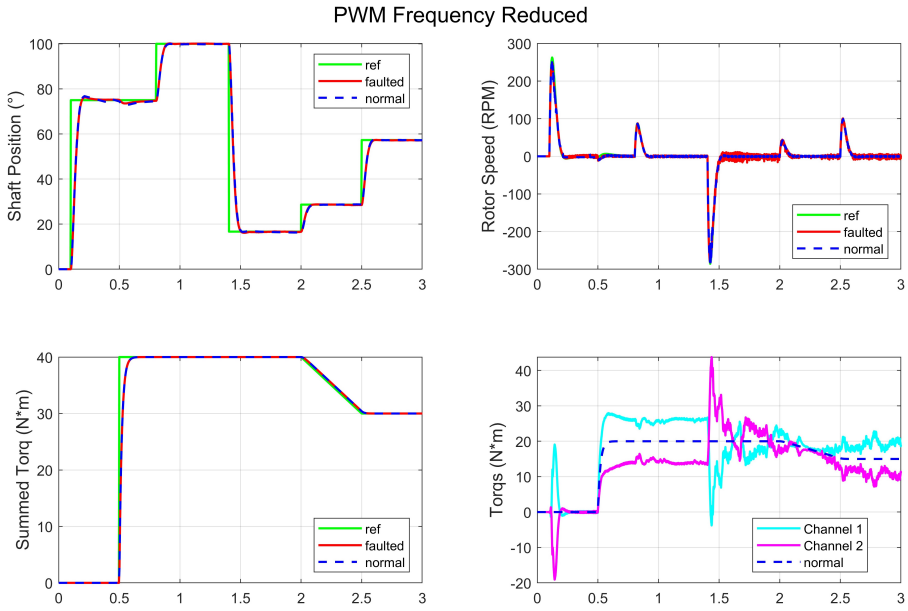

Figure 9. System control response when channel 1 PWM frequency reduced by 10%.

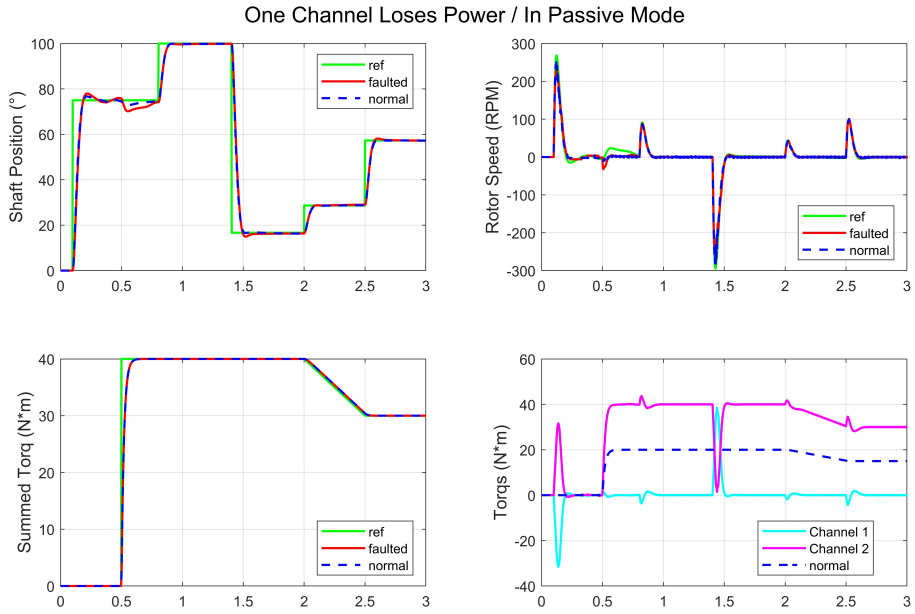

Figure 10. System control response when channel 1 in passive mode.

One common failure mode is the reduction in Pulse Width Modulation (PWM) frequency. This reduction typically occurs due to aging within the switching circuit of the electronic speed controller (ESC), leading to decreased efficiency and increased internal temperature of the motor winding. In a dual-redundant architecture, we intentionally reduce the PWM switching frequency by 10% in the ESC of Channel 1, as shown in the fourth picture in Figure 9. This reduction results in observable asynchrony between the healthy and faulted channels, causing unbalanced loads. However, as depicted in the first three plots of Figure 9, the overall system maintains normal control dynamics related to position, speed, and torque response. This indicates that the architecture can effectively mitigate this failure mode in terms of control dynamics. Nonetheless, the unbalanced loads on the two driving channels still pose a potential risk of mechanical damage to the motor.

In the event of triggering passive mode in one channel, the power electronics deactivate, causing the motor to enter a floating state. As depicted in Figure 10, Channel 1 is switched to passive mode by cutting off the power. From subplot four, it is evident that this

intentional disconnection ensures that no adverse effects are imposed on the operational channel, allowing the EMA system to remain partially operative. In the first three subplots, the position and speed responses in the faulted condition generally follow the command, with a notable deviation observed when there is a transient increase in torque, indicating degraded controllability.

5. Conclusions

In conclusion, this research presents a novel solution for the design and evaluation of an EMA architecture for eVTOL aircraft, with a focus on addressing the challenges posed by emerging eVTOL technology and certification requirements. The architecture design aims to enhance fault tolerance and safety through decentralized voting and monitoring mechanisms within the ECU, functional separation, physical segregation between subsystems and components, and planned degradation configurations. It employs a triple-dual redundant approach with dissimilar lanes of ECUs and redundant parallel channels of power electronics and motors. This design is further buttressed by a preliminary and quantifiable safety evaluation; a failure rate of 7.65×10^{-7} per flight hour is reached for certification under EASA SC-VTOL Subpart F. Moreover, an FMEA is implemented for validation. All failure scenarios, including 20 failure modes and 41 causes leading to these failure modes, have been resolved and examined through simulation and HIL tests. The outcomes demonstrate the efficacy and robustness of the VoDeMo architecture in handling all potential failures and the comprehensiveness in safety precautions.

The VoDeMo architecture solution and development approach can be extended to Lift–Thrust Units on eVTOL aircraft and control effectors on other types of aircraft. Future research will delve deeper into analyzing the impact of Common Cause Failures (CCFs) on system architecture and designing measures to address them effectively.

Author Contributions: Conceptualization, F.H., R.H., J.B., Y.L. and S.Z.; methodology, R.H. and Y.L.; software, R.H. and Y.L.; validation, R.H. and Y.L.; formal analysis, R.H.; investigation, F.H., R.H. and J.B.; writing—original draft preparation, R.H.; writing—review and editing, R.H., S.Z., F.H., J.B. and Y.L.; supervision, S.Z. and F.H.; project administration, J.B.; funding acquisition, F.H. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is funded by the Bundesministerium für Wirtschaft und Klimaschutz as part of the ZIM funding program.

Supported by:

on the basis of a decision
by the German Bundestag

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors are grateful for the support from Volz Servos GmbH & Co. KG (Offenbach, Germany) and AEE AEE GmbH (Weßling, Germany).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

The FMEA table of the VoDeMo architecture is shown in Table A1.

Table A1. FMEA table of VoDeMo architecture.

Functions	Failure Modes	Causes	Effects	Current Corrections
Position and Speed Control Loop	COM Lost	COM destroyed	No COM transmit to Digital Simple "C==S" and "C==M" taken as false	STBY control
		COM PWR disconnected	No COM transmit to Digital Simple "C==S" and "C==M" taken as false	STBY control
		PWR supplies destroyed	The EMA system loses power	Passive
		Failure on RS422 from COM	No COM signal to Digital Simple "C==S" and "C==M" taken as false	STBY control
	STBY Lost	STBY destroyed	No STBY transmit to Digital Simple "S==C" and "S==M" taken as false	COM control
		STBY PWR disconnected	No STBY transmit to Digital Simple "S==C" and "S==M" taken as false	COM control
		PWR supplies destroyed	The EMA system loses power	Passive
		Failure on RS422 from STBY	No STBY signal to Digital Simple "S==C" and "S==M" taken as false	COM control
	MON Lost	MON destroyed	"S==C" and "S==M" taken as false	COM control
		MON PWR disconnected	"M==C" and "M==S" taken as false	COM control
		PWR supplies destroyed	The EMA system loses power	Passive
	Lost COM and STBY	COM and STBY destroyed	No COM and STBY transmit to Digital Simple "C==S","C==M","S==C", and "S==M" taken as false	Passive
		COM and STBY PWR disconnected	No COM and STBY transmit to Digital Simple "C==S","C==M","S==C", and "S==M" taken as false	Passive
		PWR supplies destroyed	The EMA system loses power	Passive
		Failure on two RS422s	No COM and STBY signal to Digital Simple "C==S","C==M","S==C", and "S==M" taken as false	Passive

Table A1. Cont.

Functions	Failure Modes	Causes	Effects	Current Corrections
Position and Speed Control Loop	Lost COM and MON	COM and MON destroyed	No COM and MON transmit to Digital Simple "C==S","C==M","M==C", and "M==S" taken as false	Passive
		COM and MON PWR disconnected	No COM and MON transmit to Digital Simple "C==S","C==M","M==C", and "M==S" taken as false	Passive
		PWR supplies destroyed	The EMA system loses power	Passive
	Lost STBY and MON	STBY and MON destroyed	No STBY and MON transmit to Digital Simple "S==C","S==M","M==C", and "M==S" taken as false	Passive
		STBY and MON PWR disconnected	No STBY and MON transmit to Digital Simple "S==C","S==M","M==C", and "M==S" taken as false	Passive
		PWR supplies destroyed	The EMA system loses power	Passive
	Inconsistentoutputs	COM Latency/bias/noise/fault	"C==S" and "C==M" taken as false	STBY control
		STBY Latency/bias/noise/fault	"S==C" and "S==M" taken as false	COM control
		MON Latency/bias/noise/fault	"M==C" and "M==C" taken as false	COM control
Control signalvotings	Lost voting 1	PLD 1 destroyed	No control signal to CH1	CH1 Passive All load on CH2
	Lost voting 2	PLD 2 destroyed	No control signal to CH2	CH2 Passive All load on CH1
	Lost voting 1 and 2	PLD 1 and 2 destroyed	No control signal to CH1 and 2	CH1 and 2 Passive

Table A1. Cont.

Functions	Failure Modes	Causes	Effects	Current Corrections
Motor drive	Lost Channel 1	H-PWR 1 destroyed\open circuit	No torque generated on CH1	CH1 Passive All load on CH2
		Open circuit on Motor 1	No torque generated on CH1	CH1 Passive All load on CH2
	Lost Channel 2	H-PWR 2 destroyed\open circuit	No torque generated on CH2	CH2 Passive All torque on CH1
		Open circuit on Motor 2	No torque generated on CH2	CH2 Passive All load on CH1
	Lost Channel 1 and 2	H-PWR 1 and 2 destroyed\open circuit	No torque generated on CH1 and 2	CH1 and 2 Passive
		Open circuit on Motor 1 and 2	No torque generated on CH1 and 2	CH1 and 2 Passive
	Unequal outputs	Asyncronous current control	Power surge/force fighting	Normal control Forces quickly merge
		PWM frequency reduced	Power surge/force fighting	Normal control
Mechanicalactuation	Friction on motor 1	Motor1 jammed/bad lubrication	Force fighting/temperature rises	Normal control Higher load on Motor 2
	Friction on motor 2	Motor 2 jammed/bad lubrication	Force fighting/temperature rises	Normal control Higher load on Motor 1
	Friction on shaft	Shaft jammed/bad lubrication	Load increased/temperature rises	Normal control
Position feedback	Lost one sensor	Failure on one sensor	Lost one position measurement	Fuse rest two MEAs
	Lost two sensors	Failure on two sensors	Lost two position measurements	Feedback remain MEA
	Lost three sensors	Failure on all sensors	Lost all position measurements	Passive

CH = channel; PWR = power; H-PWR = high power; MEA = measurement.

References

1. McKinsey & Company. *Study on the Societal Acceptance of Urban Air Mobility in Europe*; Technical Report; European Union Aviation Safety Agency: Cologne, Germany, 2021.
2. McKinsey & Company. *Urban Air Mobility Survey Evaluation Report*; Technical Report; European Union Aviation Safety Agency: Cologne, Germany, 2021.
3. European Union Aviation Safety Agency. *Special Condition for Small-Category VTOL Aircraft*, 1st ed.; European Union Aviation Safety Agency: Cologne, Germany, 2023.
4. Lu, Z.; Hong, H.; Diepolder, J.; Holzapfel, F. Maneuverability Set Estimation and Trajectory Feasibility Evaluation for eVTOL Aircraft. *J. Guid. Control. Dyn.* **2023**, *46*, 1184–1196. [CrossRef]
5. Lu, Z.; Li, H.; He, R.; Holzapfel, F. Energy-Efficient Incremental Control Allocation for Transition Flight via Quadratic Programming. In Proceedings of the 2022 International Conference on Guidance, Navigation and Control, Tianjin, China, 5–7 August 2022; pp. 4940–4951.
6. Nelson, T. *787 Systems and Performance*; The Boeing Company: Arlington, VA, USA, 2005.
7. Qiao, G.; Liu, G.; Shi, Z.; Wang, Y.; Ma, S.; Lim, T.C. A review of electromechanical actuators for More/All Electric aircraft systems. *Proc. Inst. Mech. Eng. Part C J. Mech. Eng. Sci.* **2018**, *232*, 4128–4151. [CrossRef]
8. Thompson, E.L.; Taye, A.G.; Guo, W.; Wei, P.; Quinones, M.; Ahmed, I.; Biswas, G.; Quattrociocchi, J.; Carr, S.; Topcu, U.; et al. A survey of eVTOL aircraft and AAM operation hazards. In Proceedings of the AIAA AVIATION 2022 Forum, Chicago, IL, USA & Virtual, 27 June–1 July 2022; p. 3539.
9. Wasson, K.; Neogi, N.; Graydon, M.; Maddalon, J.; Miner, P.; McCormick, G.F. *Functional Hazard Assessment for the eVTOL Aircraft Supporting Urban Air Mobility (UAM) Applications: Exploratory Demonstrations*; Technical Report; NASA: Washington, DC, USA, 2022.
10. European Union Aviation Safety Agency. *Proposed Means of Compliance with the Special Condition VTOL*, 4th ed.; European Union Aviation Safety Agency: Cologne, Germany, 2023.
11. McGough, J.; Moses, K.; Platt, W.; Reynolds, G.; Strole, J. *Digital Flight Control System Redundancy Study*; US Air Force Flight Dynamics Laboratory (AFFDL): Wright-Patterson Air Force Base, OH, USA, 1974.
12. Bosch, J.; Kuehl, W. Reconfigurable redundancy management for aircraft flight control. *J. Aircr.* **1977**, *14*, 966–971. [CrossRef]
13. Yeh, Y.C. Triple-triple redundant 777 primary flight computer. In Proceedings of the 1996 IEEE Aerospace Applications Conference. Proceedings, Aspen, CO, USA, 10 February 1996; Volume 1, pp. 293–307.
14. Ning, C.; Zhang, H.; Weng, H.; Ma, R. *Safe Architecture Design of Flight Control System for eVTOL*; Technical Report, SAE Technical Paper; SAE International: Warrendale, PA, USA, 2023.
15. Ismail, M.; Wiedemann, S. Design and evaluation of fault-tolerant electro-mechanical actuators for flight controls of unmanned aerial vehicles. *Actuators* **2021**, *10*, 175. [CrossRef]
16. Murray, C. Automakers opting for model-based design. *Des. News* **2010**, *5* ,11.
17. Landi, A.; Nicholson, M. ARP4754B/ED-79A-guidelines for development of civil aircraft and systems-enhancements, novelties and key topics. *Sae Int. J. Aerosp.* **2023**, *4*, 871–879. [CrossRef]
18. SAE. ARP4761A-Guidelines and methods for conducting the safety assessment process on airborne systems and equipments. In *USA: The Engineering Society for Advancing Mobility Land Sea Air and Space*; SAE International: Warrendale, PA, USA, 2023.
19. Joshi, A.; Miller, S.P.; Whalen, M. A proposal for model-based safety analysis. In Proceedings of the 24th Digital Avionics Systems Conference, Washington, DC, USA, 30 October–3 November 2005; Volume 2, pp. 2–13.
20. Gorospe, G.E., Jr.; Kulkarni, C.S.; Hogge, E.; Hsu, A. A study of the degradation of electronic speed controllers for brushless dc motors. In Proceedings of the Asia Pacific Conference of the Prognostics and Health Management Society 2017, Jeju, Republic of Korea, 12–15 July 2017.
21. Moseler, O. Application of model-based fault detection to a brushless DC motor. *IEEE Trans. Ind. Electron.* **2000**, *47*, 1015–1020. [CrossRef]
22. Fulton, R. *RTCA DO-254/EUROCAE ED-80 Digital Avionics Handbook*; CRC Press: Boca Raton, FL, USA, 2017; pp. 217–236.
23. European Union Aviation Safety Agency. AMC 20-115D Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178. In *Easy Access Rules for Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances*; European Union Aviation Safety Agency: Cologne, Germany, 2021.
24. Ismail, M.; Bosch, C. Fault-tolerant actuation architectures for unmanned aerial vehicles. In *Advances in Condition Monitoring and Structural Health Monitoring*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 345–354.
25. He, R.; Hofsäß, H.; Zhang, S.; Holzapfel, F. Model-Based Design and Evaluation Approach of Redundant Electro-Mechanical Actuator Control Architecture for eVTOL. In Proceedings of the International Conference on Guidance, Navigation and Control, Tianjin, China, 5–7 August 2022; pp. 974–983.
26. Crassidis, J.L.; Junkins, J.L. *Optimal Estimation of Dynamic Systems*, 2nd ed.; Chapman & Hall/CRC Applied Mathematics and Nonlinear Science Series; CRC Press: Boca Raton, FL, USA, 2012.
27. Mokhamad, K.; Holzapfel, F. A Cost-Effective Synchronization Method for Distributed Flight Control Computers. *IEEE Trans. Aerosp. Electron. Syst.* **2024** .
28. Rhein, J. ExCuSe—A Method for the Model-Based Safety Assessment of Simulink and Stateflow Models. In Proceedings of the MATLAB Expo 2018, Munich, Germany, 26 June 2018.

29. The United States Department of Defense. *MIL-HDBK-217F N2. Reliability Prediction of Electronic Equipment*; The United States Department of Defense: Arlington, VA, USA, 1995.
30. Mazur, D.R. *Combinatorics: A Guided Tour*; American Mathematical Society: Providence, RI, USA, 2022; Volume 55.
31. Actuator Test Bench. Available online: https://www.fsd.ed.tum.de/infrastructure/gnc-subsystems/ (accessed on 26 February 2024).
32. The United States Department of Defense. *MIL-HDBK-338B Military Handbook Electronic Reliability Design Handbook*; The United States Department of Defense: Arlington, VA, USA, 1998.
33. Schallert, C. Integrated Safety and Reliability Analysis Methods for Aircraft System Development Using Multi-Domain Object-Oriented Models. Ph.D. Thesis, Technische Universität Berlin, Berlin, Germany, 2016.