actuators

Article

Design and Evaluation of Fault-Tolerant Electro-Mechanical Actuators for Flight Controls of Unmanned Aerial Vehicles

Mohamed A. A. Ismail [1,*], **Simon Wiedemann** [2], **Colin Bosch** [3] **and Christoph Stuckmann** [2]

[1] DLR (German Aerospace Center), Institute of Flight Systems, 38108 Braunschweig, Germany
[2] MACCON GmbH, 81549 Munich, Germany; s.wiedemann@maccon.de (S.W.); c.stuckmann@maccon.de (C.S.)
[3] Institute of Helicopter Technology, Technical University of Munich, 85748 Garching, Germany; colin.bosch@tum.de
* Correspondence: mohamed.ismail@dlr.de; Tel.: +49-531-295-2734

Abstract: Electro-mechanical actuators (EMAs) are a primary actuation technology for unmanned aerial vehicles (UAVs). Intensive research has been conducted for designing and evaluating fault-tolerant EMAs for flight controls of UAVs to ensure their compliance with new airworthiness requirements for safe operation over civilian zones. The state-of-the-art research involves several fault-tolerant architectures for EMAs based on parallel electric motors or a single motor with internal fault-tolerant features. In this study, a fault-tolerant architecture is introduced, comprised of two serial electric motors driven by two isolated controllers and a health monitoring system. The procedures of developing various fault-tolerant features are discussed with a deep focus on designing health monitoring functions and evaluating their influence on the overall actuator stability and availability. This work has been conducted and evaluated based on operational data for ALAADy: a heavy gyrocopter-type UAV at DLR (German Aerospace Center).

Keywords: fault-tolerant electro-mechanical actuator; certified UAVs; model-based fault detection; sensorless load monitoring

Citation: Ismail, M.A.A.; Wiedemann, S.; Bosch, C.; Stuckmann, C. Design and Evaluation of Fault-Tolerant Electro-Mechanical Actuators for Flight Controls of Unmanned Aerial Vehicles. *Actuators* **2021**, *10*, 175. https://doi.org/10.3390/act10080175

Academic Editors: Andrea De Martin, Antonio Carlo Bertolino, Massimo Sorli and Giovanni Jacazio

Received: 24 June 2021
Accepted: 22 July 2021
Published: 25 July 2021

1. Introduction

The outstanding reliability of the manned aircraft is preserved, compared to other transportation systems, thanks to strict certification requirements. On the other side, the average loss rate of unmanned aerial vehicles (UAVs) is currently 10 times worse than the manned category [1]. The fast growth of civilian applications of UAVs encourages civil aviation authorities to set airworthiness certification requirements for heavy UAVs similar to the manned category [2]. Here, the focus is for flight control electro-mechanical actuators (EMAs) that may be within safety-critical onboard systems depending on aircraft design. For specific flight controls layout, e.g., helicopters, the EMA function must not be interrupted after the first failure [2]. In order to satisfy such requirements, fault-tolerant architectures for EMAs are being developed in terms of hardware redundancies, e.g., multiple electric motors, in addition to health monitoring functions for managing fault-tolerant capabilities [2,3]. Evaluating possible hardware redundancies for flight control EMAs has been published in a follow-up study [4], and the selected fault-tolerant architecture is presented in this paper with a comprehensive design for health-monitoring functions.

The objective of developing health monitoring capabilities is to fulfill specific reliability and operating conditions for a specific flight controls layout. Said layout involves flight control redundancies and their failure criticality for a safe landing. Examples of recent research approaches for developing fault-tolerant EMAs can be found in [3–8].

Dalla Vedova et al. [3] presented a model-based diagnosis for EMAs based on a simulated annealing algorithm. The EMA was subjected to a linear chirp signal in order to excite the mechanical structure, and the equivalent response was measured. The chirp signal and measured response were used to identify the parameters of a third-order dynamic model, in particular, the coefficient of friction and a numerical parameter to represent actuator backlash.

Swerdon et al. [5] investigated model-based fault detection for flight control EMAs based on identifying the parameters of a dynamic model. EMA efficiency was monitored through model parameters in order to detect any efficiency loss. EMA efficiency for fault detection has also been considered by Todeschi and Baxerres [6]; in this method, data-based fault detection of the actuator current and torque was used to calculate instantaneous efficiency directly rather than using dynamic models.

Arriola and Thielecke [7] investigated data-based health monitoring functions for parallel active–active flight control EMA. Five monitoring functions were derived from a high-fidelity model of the actuator, including adjustable thresholds that account for certainties for model parameters and operation transients. However, the monitoring functions are mainly optimized for the mechanical faults, while the electrical faults are monitored by direct root-mean-square errors of the electric current controller without incorporating the actual applied load on the motor. In addition, the actuator architecture is complicated as it involves multiple load cells that have cost and reliability challenges.

Rito and Schettini [8] developed a model-based health monitoring system for a fault-tolerant EMA for primary flight control of UAVs. Two model-based position and speed-tracking models are developed based on detecting malfunctions when the actual position and speed feedback deviate from the nominal behavior. The aerodynamic load was fully ignored in these models, which leads to limited efficiency for safety-critical actuator reconfiguration during in-flight conditions.

The challenges for developing reliable fault-tolerant EMAs are significantly related to the availability and the handling of the actuator load data. First, the availability of actuator load measurements is crucial for developing effective health monitoring functions that are less sensitive (i.e., low false diagnosis rates) to typical high transient operating conditions. Prior research includes integration of multiple load sensors [7], ignorance of the load data [8] or conducting the monitoring functions at no-load as a pre-flight test [3].

Second, health monitoring functions were developed as multiple functions of single-input–single-output models to evaluate the actuator health considering either a speed or a load variation. Though, the actual operating regime of the actuator at a certain health condition can be only uniquely defined by both the operating speed and the applied load.

In this study, a fault-tolerant EMA architecture is introduced comprising two serial electric motors driven by two isolated controllers and multiple health monitoring functions. Health monitoring functions are less sensitive to transient aerodynamic load thanks to sensorless load observers. In addition, these observers present a dual analytical redundancy to maintain its full functionality after a single safety-critical failure at one of the actuator lanes. The procedures of developing hardware and software subsystems are discussed with a deep focus on designing fault detection functions and their influence on the overall stability and availability. In this paper, reliability-driven requirements for fault-tolerant features are investigated in Section 2. The implementation of the fault-tolerant features for the electric motor is intensely discussed in Section 3. The health monitoring and reconfiguration functions are developed in Section 4. The overall fault tolerance performance is evaluated in Section 5. The scientific contributions are summarized in Section 6.

2. Reliability-Driven Architecture Design

2.1. Reliability-Driven Requirements

To satisfy the reliability requirements for EMAs in flight controls, an approach in line with SAE ARP4761 [9] is selected. This guideline is a common methodology in aerospace to demonstrate compliance with required reliability and safety levels. It assists in the definition of functional safety requirements in a top-down approach followed by detailed system safety analyses in a bottom-up verification step.

UAVs with an equivalent manned certification basis of CS-VLA are subject to their own airworthiness standards. The European Union Aviation Safety Agency (EASA) published the rulemaking document SC-RPAS.1309 [10], according to which a catastrophic failure condition should not occur more frequently than 10–6 times per flight hour. Using these constraints, we performed an aircraft/system functional hazard assessment (FHA) which was previously published [2]. The analysis illustrated that the most stringent actuation safety requirements induced on the system level could be found in rotorcraft. This led to the selection of the ALAADy Gyrocopter as a use case for the prototype actuator. EMAs performing functions with catastrophic failure conditions require a high level of development independence. Thus, by assuming a secondary system (e.g., a parachute), the EMA criticality can be reduced to 'hazardous', and requirements for independent development of redundant components can be (partially) eliminated. These considerations as well as the aircraft functional layout then lead to a required failure probability for one actuation leg of less than 5 × 10^{-6} per flight hour.

From both quantitative and qualitative perspectives, the EMA must comply with the relevant regulations of SC-RPAS.1309. The architecture finding process introduced in [2] provides a structured approach linking the safety assessment with preliminary design activities. Qualitative and quantitative criticality data for individual failure modes from [11–19] assisted in the preliminary safety assessment. We regard the following results as noteworthy:

- For UAV use cases, a duplex-redundant architecture of the electronic/electrical hardware is sufficient;
- A single mechanical load path is acceptable if mechanical components are designed according to the required service life and failure probabilities.

2.2. Fault-Tolerant Features and Quantitative System Safety Assessment

The actuator architecture, as shown in Figure 1, represents the fault-tolerant architecture of the EMA. Segregation of all electrical and electronic components enables a robust fault-tolerant design. Consequently, there are separate Controller (CON) and Monitoring Units (MON) in separate Actuator Control Units (ACU). Both channels feature independent power supplies and drive independent rotor arrangements. Every channel contains its independent motor and position encoders. The mechanical load path features a Harmonic Drive gearbox and a single output. According to Table 1, the fault-tolerant strategy includes three general EMA operating modes:

For verification of compliance with quantitative reliability targets, SAE ARP4761 [9] suggests using a stochastic Markov Model. Bonivento et al. [20] have used this methodology and illustrated the method's ability to represent different system operating states. A system state change is modeled using failure rates λ [1/h] in this case. Figure 2 illustrates the system's detailed failure behavior for the 'loss of actuation' failure condition. This process is represented by nine different operating states and three operating modes. Each of the six Fail Safe states is equivalent to a 'loss of actuation'. The probability of the system to be in any operating mode at a given point in time t is expressed using the following equation (Equation (1)):

$$P_{NM}(t) + P_{FO}(t) + P_{FS}(t) = 1 \tag{1}$$

In the beginning of the analysis, the system is in the Normal Mode, i.e., P_{NM} (t = 0) = 1, P_{FO} (t = 0) = 0, P_{FS} (t = 0) = 0.

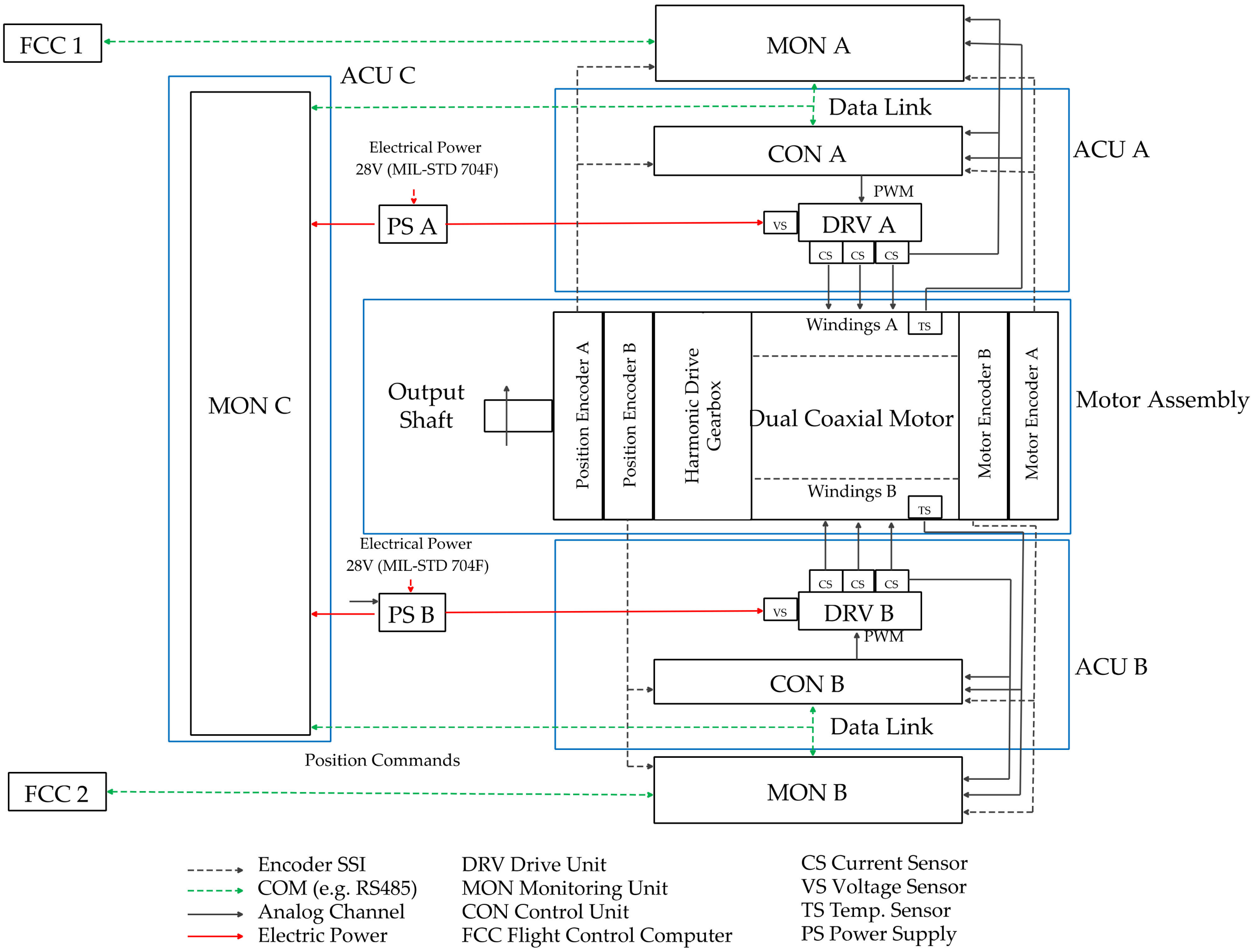

Figure 1. Overall actuation architecture containing two fault-tolerant motor channels as well as a single mechanical path.

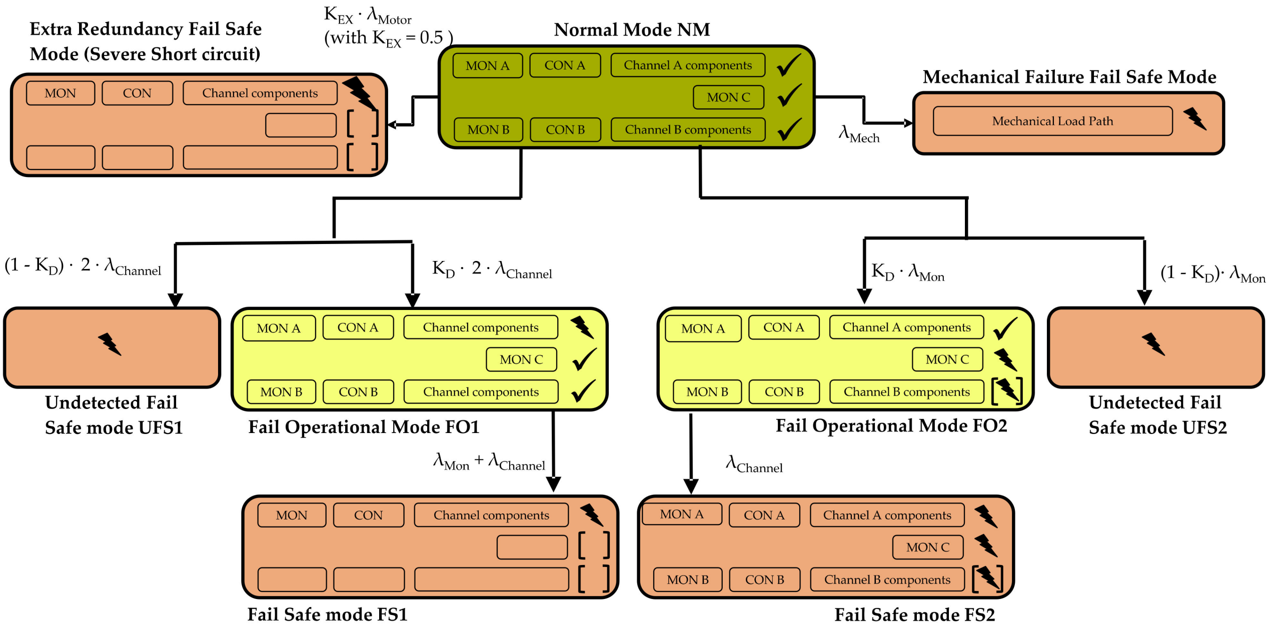
Extra Redundancy Fail Safe Mode (Severe Short circuit)
$K_{EX} \cdot \lambda_{Motor}$ (with $K_{EX} = 0.5$)
Normal Mode NM
MON A
CON A
Channel A components
MON C
MON B
CON B
Channel B components
MON
CON
Channel components
Mechanical Failure Fail Safe Mode
Mechanical Load Path
λ_{Mech}
$(1 - K_D) \cdot 2 \cdot \lambda_{Channel}$
$K_D \cdot 2 \cdot \lambda_{Channel}$
$K_D \cdot \lambda_{Mon}$
$(1 - K_D) \cdot \lambda_{Mon}$
Undetected Fail Safe mode UFS1
Fail Operational Mode FO1
Fail Operational Mode FO2
Undetected Fail Safe mode UFS2
$\lambda_{Mon} + \lambda_{Channel}$
$\lambda_{Channel}$
Fail Safe mode FS1
Fail Safe mode FS2

Figure 2. Stochastic Markov Model with 9 different operating states and 3 operating modes (NM: green, FO: yellow, FS: red).

Table 1. EMA operating modes.

General Operating Mode	Description
Nominal Mode (NM)	All components working properly
Fail Operational (FO)	Faulty channel is switched off, actuator is active with one channel
Fail Safe—(Actuator off) (FS)	EMA is switched off, triggering a secondary system

Entering Fail Operational Modes (FO1 and FO2) is triggered in case of a failure occurs in one or both channels. The respective failure rates are λ_{Channel} and λ_{Mon}. Each channel contains its independent components (controller (CON), Monitoring Unit (MON), windings, power electronics, etc.). For the first failure, the fault detection rate K_D quantifies the ability of fault detection. In the case of failed detection, represented by 1-K_D, the transition to the Fail Safe Mode (UFS1 and UFS2) is assumed to be performed on a UAV level. Modes FS1 and FS2 are triggered if a consecutive failure is detected during the Fail Operational Modes. Any relevant mechanical failure occurring with the failure rate λ_{Mech} is presumed to immediately trigger the Fail Safe Mode. In addition, a common cause of electrical failure could jeopardize the redundant concept. If detected, this also activates the Fail Safe Mode. However, as quantifying these effects requires in-depth field data, we estimate the common cause rate to be $\lambda_{\text{CC,electric}}$ = 0.5 λ_{Motor}, with λ_{Motor} representing the failure rate of the electric motor.

The Markov chain is simulated according to the following equation (Equation (2)), where P_i (P_j) stands for the probability of the system to be in state i(j) and λ_{ij} is the transition rate from state i to state j:

$$\dot{P}_j(t) = \lambda_{ij} \cdot P_i(t) \tag{2}$$

Component failure rates are computed in a bottom-up approach using manufacturer data, mechanical reliability models and the FIDES approach. FIDES provides electronic failure rates based on a multitude of technical and manufacturing aspects [21]. Table 2 illustrates the failure rate methodology:

Table 2. Holistic approach for the component failure rates.

Failure Rate	Components with Highest Influence on Parameter	Used Models	Order of Magnitude
λ_{Mech}	Gearbox, bearing	Manufacturer based service life approaches coupled with 2-parameter Weibull distributions	10^{-6} h^{-1}
λ_{Channel}	ACU boards, motor	FIDES methodology, manufacturer data	10^{-5} h^{-1}
λ_{Mon}	ACU board	FIDES methodology	10^{-5} h^{-1}

Figure 3 shows the results of the Markov analysis as part of a sensitivity study. The chart depicts the estimated overall failure probability of the actuator after t = 1 h, plotted over the variation of previously introduced input parameters. Variation of the respective parameters is based on available minimum, median and maximum values.

The chart illustrates that the channel failure rate is subject to the highest uncertainties since this parameter is influenced by a variety of components. Any component within one channel subject to an increased risk of failure (e.g., due to manufacturing, uncertainty in development and testing, etc.) influences the overall failure probability to a high extent. This result stresses the requirement for high-quality aerospace components to be used coupled with an appropriate level of design assurance. λ_{Mech} and the common cause failure rate have similar effects on the overall reliability. A major impact is caused by the fault detection rate K_D (reference is K_D = 0.96). It presents the highest gradient and an increase to 0.98 could bring the actuator to the level of certification (5 × 10^{-6} 1/h), emphasizing the importance of a well-proven health monitoring system (see Section 4).

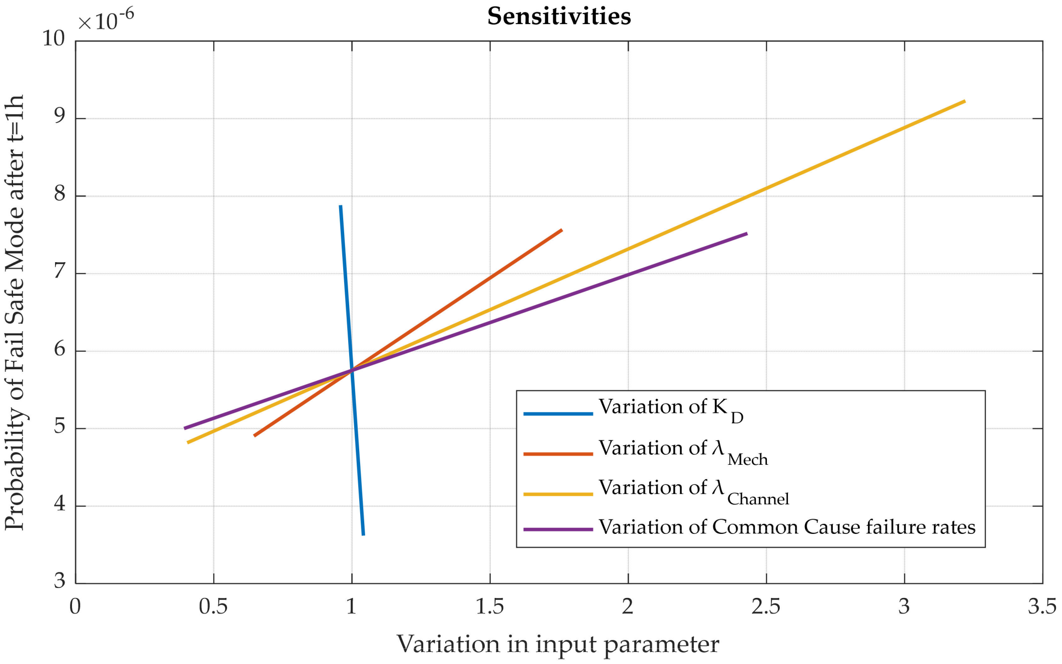

Figure 3. Sensitivity study based on the Markov analysis of the fault-tolerant EMA architecture.

2.3. Qualitative Criticality Assessment and Inputs for Health Monitoring

In addition to the quantitative assessment, qualitative criticality analyses assist in identifying critical failure modes and focus areas of the EMA. This analysis, however, is subject to an increased level of uncertainty, as literature data are limited and available data are oftentimes referring to similar but non-identical EMA architectures. Therefore, the following analysis, illustrated in Figure 4, provides only an approximate data basis.

Figure 4 shows mean EMA criticality data from different sources, including the desired operating modes. All electronic and electrical failures should be dealt with by means of the redundant channel design and should therefore not directly lead to the Fail Safe Mode. One exemption is the 'Motor Shortened Coil' as there might be severe short circuits affecting both redundant branches, as previously discussed. Mechanical failures may directly trigger the Fail Safe Mode.

In an effort to evaluate the behavior of the Health Monitoring System (Section 4), it is essential to closely regard the relevant failure modes from Figure 4 as well as to estimate the system's ability to safely execute the transitions between the operating modes. We therefore concentrate on essential mechanical failure modes and on those failures leading to the Fail Operational Mode. Table 3 provides a list of faults, including their target operation modes, to be investigated in more detail. Detailed descriptions for the injection approaches of the faults in Table 3 are furnished in Section 5.1.

Table 3. List of potential faults and target operation modes.

Fault ID	Condition	Mode
1	Healthy	Nominal Operation
2	Drag torque in Lane B, 20%	
3	Drag torque in Lane B, 40%	Fail Operational
4	Drag torque in Lane B, 60%	
5	Drag torque in Lane B, 80%	
6	Drag torque in Lane B, 100%	
7	Open circuit in Lane B	

Table 3. *Cont.*

Fault ID	Condition	Mode
8	Reduction in armature resistance Lane B, 20%	Nominal Operation
9	Reduction in armature resistance Lane B, 40%	
10	Reduction in armature resistance Lane B, 60%	
11	Reduction in armature resistance Lane B, 80%	
12	Reduction in armature resistance Lane B, 100%	
13	Reduction in magnetic flux Lane B, 20%	
14	Reduction in magnetic flux Lane B, 40%	Fail Operational
15	Reduction in magnetic flux Lane B, 60%	
16	Reduction in magnetic flux Lane B, 80%	
17	Reduction in magnetic flux Lane B, 100%	
18	Disconnection of CON A	
19	Disconnection of CON B	
20	Disconnection of MON A	
21	Disconnection of MON B	
22	Disconnection of MON C	
23	Disconnection of Position Encoder A	
24	Disconnection of Position Encoder B	
25	Disconnection of Motor Encoder A	
26	Disconnection of Motor Encoder B	
27	Increase in the viscous friction of the gear, 200%	Nominal Operation
28	Increase in the viscous friction of the gear, 400%	
29	Increase in the viscous friction of the gear, 600%	
30	Increase in the viscous friction of the gear, 800%	Fail Safe

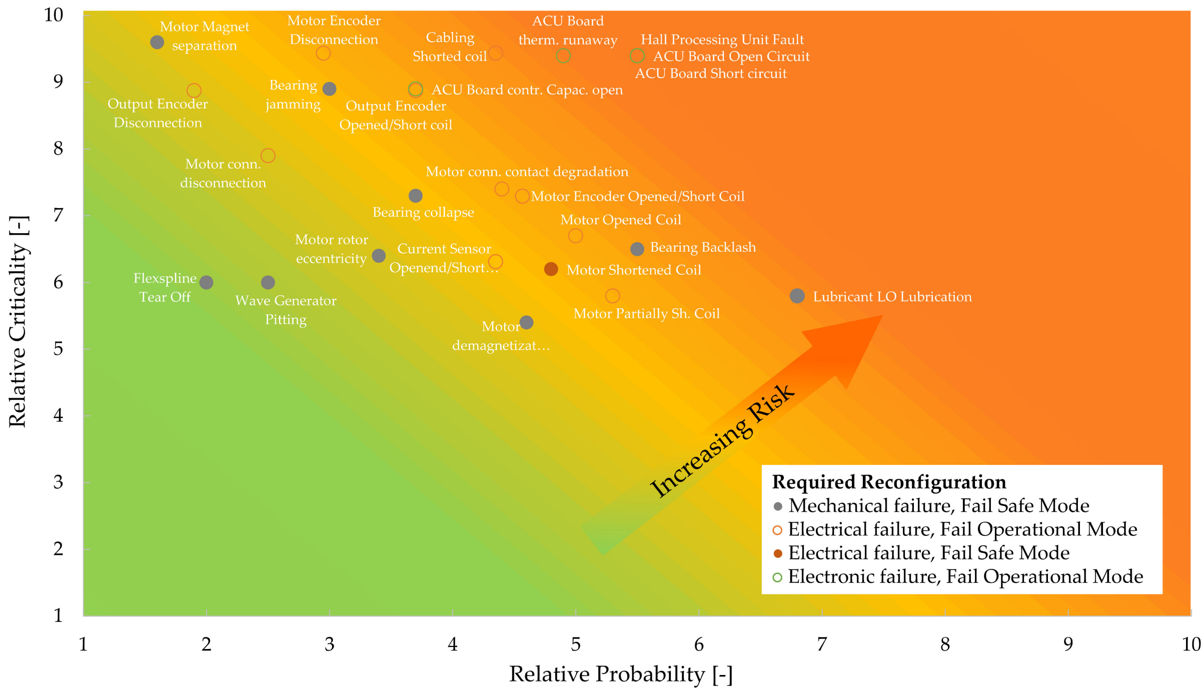

Figure 4. Qualitative risk analysis of different EMA failure modes [11–14].

3. Fault-Tolerant Electrical Motor Design

3.1. Classification of the Failure Scenarios

A frequently held opinion in the area of electric motor design is that the concept of redundant winding systems is already sufficient to design a motor in order to be fail safe in the sense that in the event of a fault occurring, switching over to the redundant system already guarantees undisturbed motor operation. Switching from the main to the redundant system is only a solution if the fault can be switched off permanently in the faulty system and without any further influence on the overall system performance. The motor's internal winding short-circuits are particularly critical, as they cause permanent damping in the fault system and continue to have an influence on the overall system even after switching over to the redundant system. For example, if there is only a cable break in the motor supply lines, the attenuation in the fault system is not critical as long as no internal motor short circuit is caused. This case could arise if the copper strands of the cable come into contact with the motor housing. However, if all cables are protected against dislocation, e.g., by bandaging and proper installation, there will be limited danger of a short circuit. Thus, switching to the redundant winding system is a measure to counteract the fault in a stable manner for further motor operation.

Nevertheless, if overheating occurs in the main winding system as a result of overload operation, there is a risk of important insulating parts melting and a short-circuit can be caused, which can lead to a second-order fault (consequential fault). In most applications, it is argued that, to achieve a second-order fault, a chain reaction with a subsequent fault must be caused. This first-order fault case can be hypothetically considered as controllable by switching to the redundant system. However, the practical case of a chain reaction of coupled faults is the more likely case. The problem is that the malfunctions must be detected very quickly during motor operation in order to prevent a subsequent fault. Moreover, if the first fault has already occurred, it is difficult to detect it by measurement. This would require the monitoring of an overstress on a partial insulation. This requires predictions of the insulation behavior, such as the use of an aging model, which is based on temperature measurements. In addition, this approach would presuppose that it is possible to localize the overheating sufficiently precisely in the first place. In summary, the occurrence of a second-order fault is much more likely when these identification mechanisms are not considered.

Another consideration to be made is the severity of the fault in terms of the system behavior. For this purpose, the following different fault categories are distinguished in Table 4 and Figure 5.

Table 4. Notations for Figure 5.

Note #	Description
1	Phase to Phase SC of two phases of one winding system: wire insulation has to be failed, and furthermore, the phase-to-phase insulation has to be affected.
2	SC internally within the phase: wire insulation has to be failed at two separate positions, resulting in the effect that turn number at one coil becomes unsymmetrical: inter-turn SC.
3	Phase to Phase SC of two phases of the two different winding systems: wire insulation has to be failed, and furthermore, the phase-to-phase separator insulation has to be affected.
4	Phase to ground of one winding system: wire insulation has to be failed, and furthermore, the phase to liner insulation has to be affected.
5	Star point to ground SC for one phase of the one winding system: the insulation tube of the star point has to be failed and has to come in contact with motor grounding.
6	Power cable of one system contacts the motor grounding: the insulation tube of the motor power cable has to develop cracks, and cable has to come in contact with motor grounding.
7	Power cable of one system contacts the power cable of the second winding system: both insulation tubes of the motor power cables of each system have to develop cracks and contact.

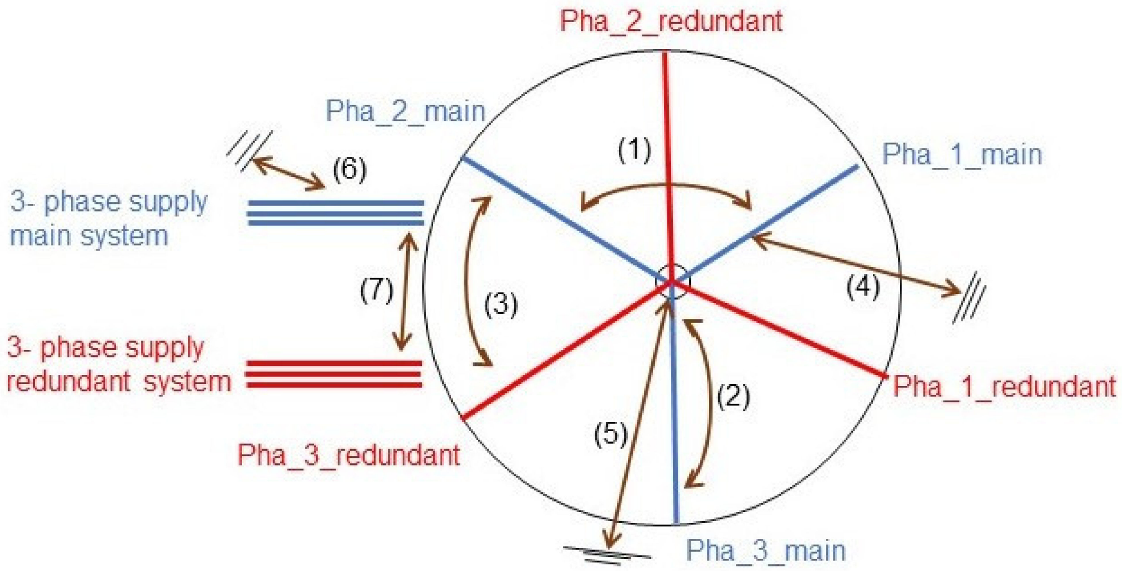

Figure 5. Failure classification of short circuit scenarios for motors with redundant winding systems.

A special influence on the system would be given if permanent damping is caused in the system. The case of such asymmetrical damping is to be listed as particularly critical. Among these, the following types of faults are to be listed [21]:

- A short circuit of two phases of a system;
- A short circuit of one phase of a system;
- Asymmetrical partial short circuits of a system;
- Short circuits between two systems would be listed as particularly critical.

3.2. Consideration of Aging Processes in Winding Systems

Most of the listed SC faults can be avoided if very robust maximum temperature materials are used. All materials should be one to two temperature classes better than the temperature class of the motor design. A general motor lifetime estimation can be obtained by the Arrhenius equation [22,23] as follows (Equation (3)):

$$L = B\, e^{\frac{E}{K*T}}, \tag{3}$$

where L is the lifetime in units of time, B is a constant value for the insulation lifetime at a reference temperature, E is the activation energy of aging reaction (1.05 for insulation class F), K is the Boltzmann constant ($K = 1.38 \times 10^{-23}$ J/K) and T is the absolute temperature in Kelvin. The formula of Equation (3) can be expressed in terms of insulation classes in Equation (4) as follows:

$$L_x = L_0\, 2^{\frac{T_B - T_X}{HIC}}, \tag{4}$$

where L_x is the estimated lifetime at temperature T_x, L_0 is the reference lifetime at rated load, T_B is the maximum allowable temperature for insulation class, T_x is the maximum hotspot temperature for insulation class, HIC = Halving interval (14, 11, 9.3, 8 and 10 for class A, B, F, H and C). Specifically, a design case for temperature class C (maximum permitted hotspot: 220 °C) and a motor utilization (maximum permitted hotspot: 155 °C) is considered in Equation (5).

$$L_x = 20,000\ \mathrm{h} * 2^{\frac{220-155}{10}} > 1.8 \text{ million hours} \tag{5}$$

It can be seen that by using materials that are specified as two times higher than qualified at the full-rated temperature, the theoretically computed motor lifetime can be strongly extended. This relationship underlines that the design of fail-safe motors can be favored by the use of high-temperature materials. The probability of the occurrence of first-order faults and the resulting consequential faults can therefore be significantly reduced.

3.3. Concepts to Achieve Fault Tolerance for Short Circuits

Unbalanced short circuits can be avoided by a special constellation of the winding coil arrangements. Two of them are shown in Figures 6 and 7.

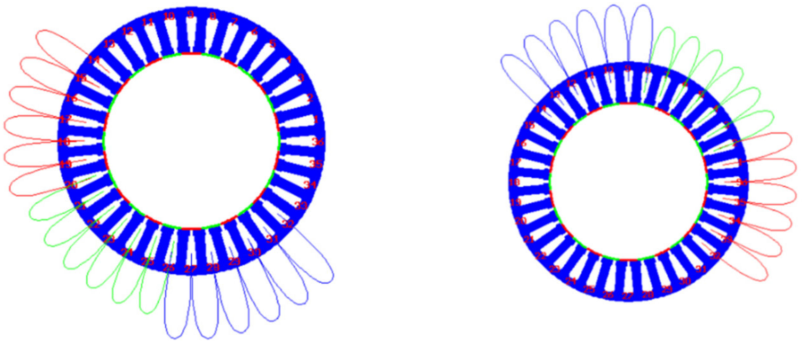

Figure 6. First example of a winding system which allows a geometrical decoupling of the main- and redundant winding system (winding scheme by placing the main-/redundant at each half of the stator: 18 coils main on the left motor half and 18 coils redundant on the right motor part).

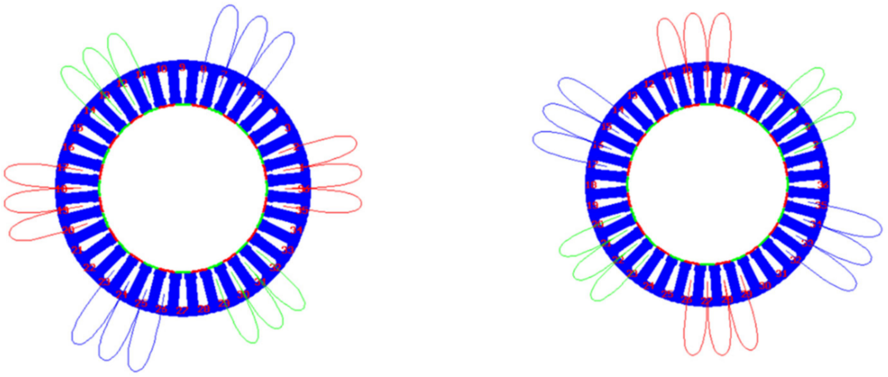

Figure 7. Second example of a winding system that allows a geometrical decoupling of the main- and redundant winding system (winding scheme by placing the main and redundant parts alternately: 3 coils main and 3 coils redundant, always alternating).

In both winding schemes, the main and redundant windings are placed at a certain distance to avoid, with a high probability, the event of the following kind of motor failures:

- The phase-to-phase short circuit is unlikely to occur for both concepts since the windings are obtaining contact only at a very limited position or outside of the motor; both positions can be insulated by an extensive insulation structure.
- The symmetrical SC can be avoided by having an extensive insulation structure in the slot. Both listed failure scenarios, in principle, have to be caused by multiple failures. Therefore, the wire insulation has to fail, and consequently, a heating-up process has to be induced by the effect of melting of the varnish coating isolation of the wire (Figure 8). Therefore, an undetected inter-turn SC has to be presented for a longer period, resulting in failures of more than one wire. To weaken this kind of failure, layer by layer wire turns have to be installed, as shown in Figure 9.

Short circuits between the main and redundant system do not need to be considered for this application since both systems are supplied on different potential power supply levels. Nevertheless, it is generally advisable to ensure that no uncovered faults develop in the system, e.g., by monitoring the potential of the motor star point. It applies for both winding designs that short circuit scenarios can be reduced to the clearly less critical case of an inter-turn short circuit. The trade-offs between both winding constellations are as follows:

(a) Winding scheme one:

This winding scheme places the main/redundant part at each half of the stator circumference of 18 coils on the left motor half and 18 coils redundant on the right motor part. Mostly, the coils of one phase of one system obtain contact. After every sixth slot, alternative phases of one system obtain contact. The main and redundant systems obtain contact at only two positions. This can be considered to be uncritical because the systems are operating on different potentials. The winding factor of this winding architecture is a common range of <0.9.

(b) Winding scheme two:

This winding scheme separates each phase of the main part and redundant part in two geometrically distanced winding systems. The contact in every fourth slot between the main and redundant systems can be considered to be uncritical because the systems are operating on different potentials. The general note on error monitoring must be considered. Only coils of one phase of one system are obtaining contact. The winding factor of this winding architecture is within the common range of >0.9. By using the second winding scheme, the risk of failure cases, which can result in permanent damping scenarios, is highly reduced. Two additional points have to be considered for this. The motor cables have to be routed by assembling them in individual insulation tubs. This assures that phase wires are protected using robust tubes in the area where the cables are obtaining contact with cables of different phases (Figure 8). If constructively possible, the cable should be positioned vertically from the winding ends in order to avoid any overlapping. The risk of internal short circuits of one phase can be minimized by using high-temperature wires with insulation grade III and by using layered windings, as shown in Figure 9. If a second-order failure occurs, only windings with equal turn numbers are obtaining contact with each other. Consequently, the influence is limited since the resulting turns per coil are still in the same range, and therefore, the degree of asymmetry is still low.

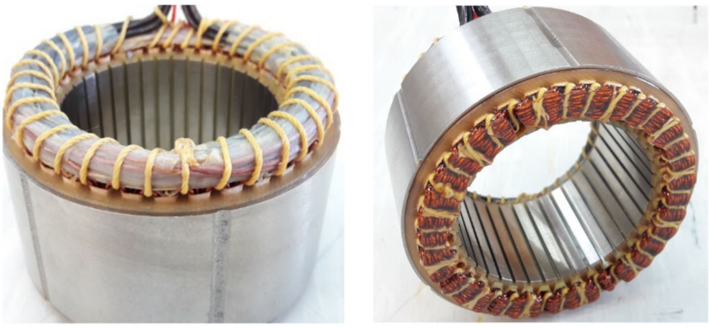

Figure 8. Example of laying the motor cables in individual tubes and assembling them vertically from the winding ends in order to avoid any overlapping.

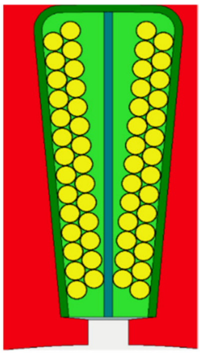

Figure 9. Example of a layered motor winding with 2 parallel wires per winding turn.

3.4. Implementation in the Motor Design

The optimal slot to pole combination was selected based on the definition of the winding system. Hence, the slot number is defined as 36 slots. Using an 8/9 combination (8 rotor poles and 9 stator poles) and using a multiple, e.g., 4, the pole number was defined to 32 (pole pair number 16). The stator outer diameter of 80 mm is very small with regard to the relatively high slot to pole number. A spoke rotor design configuration was chosen in order to foresee as much magnet material as possible as well as to not to be limited by the pole arc magnet dimensional space, which can also be seen in Figures 10 and 11 (ID 9.1).

Another design concept is shown in Figure 11. Digital hall sensors are utilized for estimating the motor currents (ID 10, 11) in order to increase the robustness and compactness of the motor design. To assure a robust failure concept, integration of the hall sensors in close contact with the stator windings, as usually implemented, is not recommended. The maximum temperature of such sensors is usually smaller, and sensors are more prone to become damaged in comparison to the windings, which have a high maximum hotspot temperature. The hall sensors are therefore placed above an auxiliary rotor, which allows a thermal decoupling of the stator winding and the hall sensors, allowing them to be easily maintained. An implementation of the sensors within the stator slots would also decrease the winding slot factor and hence the total mass.

The general mechanical architecture of the actuator and its main components are listed in Table 5 and are shown in Figures 10–13.

Table 5. Notations for Figures 11–13.

Note #	Component
1	Output lever
2	Output position encoder of lane A (rotor + stator)
3	Output position encoder of lane B (rotor + stator)
4	Spline-shaft
5	Spline-hub
6	Connection box of the output encoders
7	Gearbox, gear ratio of 1/50 (Harmonic Drives)
8	Cable tube of the output encoders
9	Motor (stator, main rotor (9.1), passive cooling)
10	Rotor for the digital position hall sensor
11	Digital hall sensor circuit board of lanes A and B (electrically isolated)
12	Motor encoder (rotor + stator)
13	Actuator control unit (ACU) of lanes A and B (two circuit boards)
14	Actuator connectors of lanes A and B (communication and power supply)

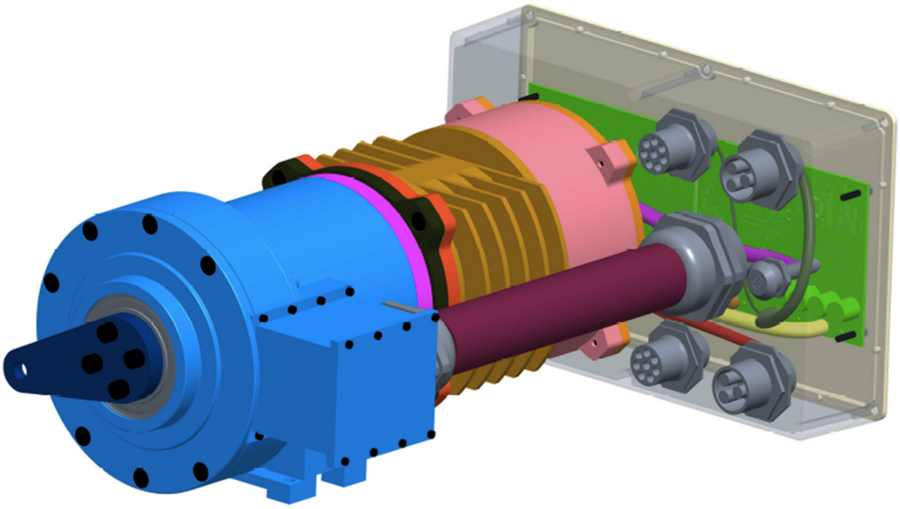

Figure 10. Complete actuator assembly.

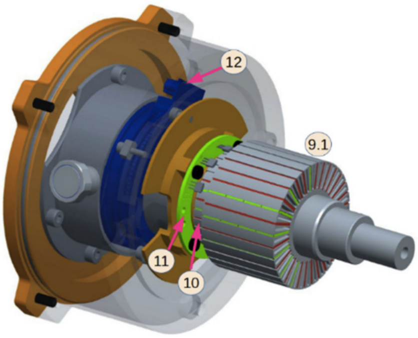

Figure 11. Sensor concept and the main motor rotor.

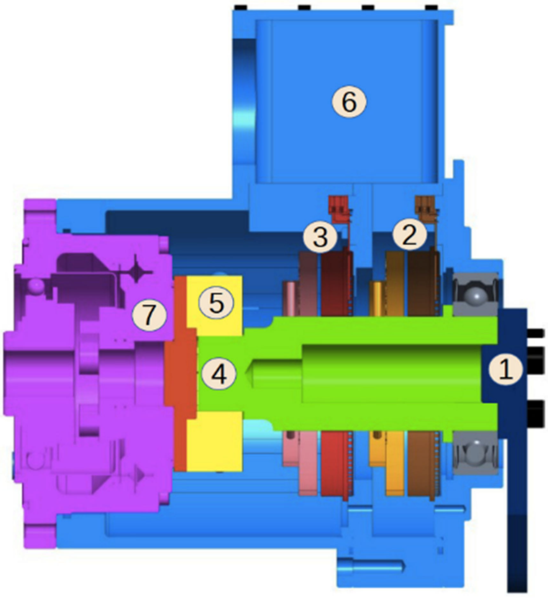

Figure 12. Output parts of the actuator.

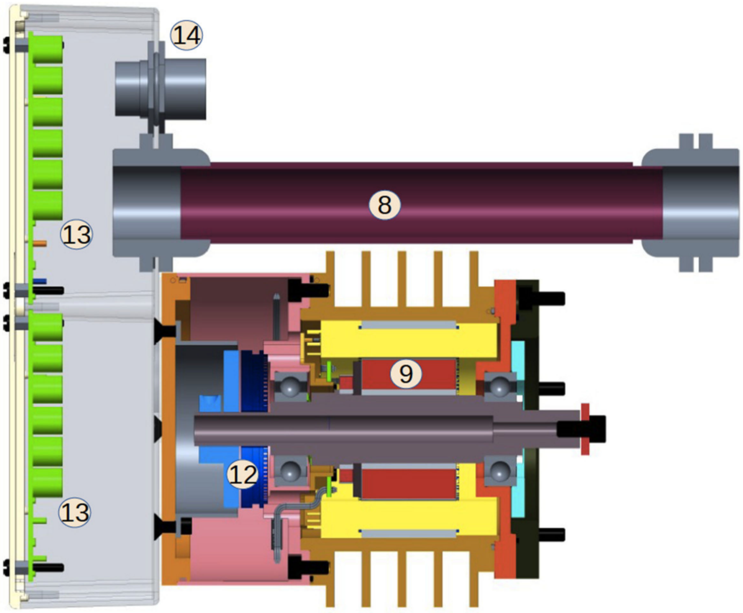

Figure 13. Motor-side parts of the actuator.

3.5. Electronic and Software Architecture

As shown in Figures 1 and 14, each of the lanes A and B includes a drive unit (DRV) and a control unit (CON), together forming the actuator control unit (ACU). The main purpose of the ACU is to control the motor currents in such a way that the output lever follows a commanded reference position given by the FCC and to provide monitoring data for the MONs. Both the DRV and the CON are located on one ACU circuit board, which is shown in Figure 13. The CON mainly represents a safety microcontroller, and the DRV consists of electronic components, including the power MOSFETs of the half bridges which are connected to the motor terminals. Generally, the electronic and software architecture must be as simple as possible to reduce the number of possible failures within the system. Additionally, the source code of the CON unit for the communication and motor control must be as simple and robust as possible.

The proposed solution to fulfill these requirements is shown in Figure 14. The motor is controlled by means of three cascaded loops to control the position, speed and current of the motor. It can be seen that only the position and speed control is implemented in software, whereas the current control is located externally in an ASIC. The advantage of this is a heavily reduced source code since functionalities such as: current measurement, current control including current-limit implementations, hall sensor measurements and its signal conditioning, commutation tables, pulse width modulation (PWM) and fault detections are all undertaken by the external ASIC circuit. The second advantage is that one specific ASIC is normally widely used in different applications, including safety-critical areas such as automotive with quantities of several thousand per year. The usage of an intensively used and proofed ASIC functionality with given failure rates compared to a newly developed system is obvious.

The utilized current control ASIC features the following functionalities, for simplicity divided into input and output related tasks:

Input: reference current from the microcontroller, drive enabled from the FCC and microcontroller, hall signals, power supply, reference direction (DIR)

Output: drive current measurement, digital hall sensor commutation status (TACHO), direction (DIR), health status bits (FF1 and FF2). The health status of the ASIC indicates several faults, which are listed in Table 6.

Table 6. Health status bits (FF1 and FF2).

FF1	FF2	Fault
0	1	Undervoltage
0	0	Overtemperature
0	0	Logic fault
1	0	Short to supply
1	0	Short to supply
1	0	Shorted motor winding

The motor speed is calculated by means of the ASIC TACHO bit and through the rate of change of the output position encoder signal. Additional fault detection relevant signals such as the temperature of the power electronics and motor windings as well as the DC-link voltage and current are processed within the microcontroller and transmitted via the datalink to the MON. Abnormal functionality such as software lock-ups or hardware faults of the microcontroller can be detected by a watchdog to recover back to a healthy state. The information of a watchdog event is also transmitted via the datalink to the MON. Due to the external current control, the functionality of the microcontroller is reduced to the control of the output position lever by means of the position and speed control loop and to the communication of measurement data such as:

- CAN (ARINC 825): communication with MON (see also Figure 14);
- SPI: communication with DAC for the generation of a current reference voltage for the ASIC.

- SCI: reading of the output encoder serial communication protocol;
- ADC: temperature sensor measurement of the power electronics and motor windings, ASIC drive current, DC-link current and voltage;
- GPIOS Input: ASIC fault diagnoses bits (FF1, FF2), TACHO, DIR, external drive enable, GPIOS Output: BRAKE, drive enabled, DIR.

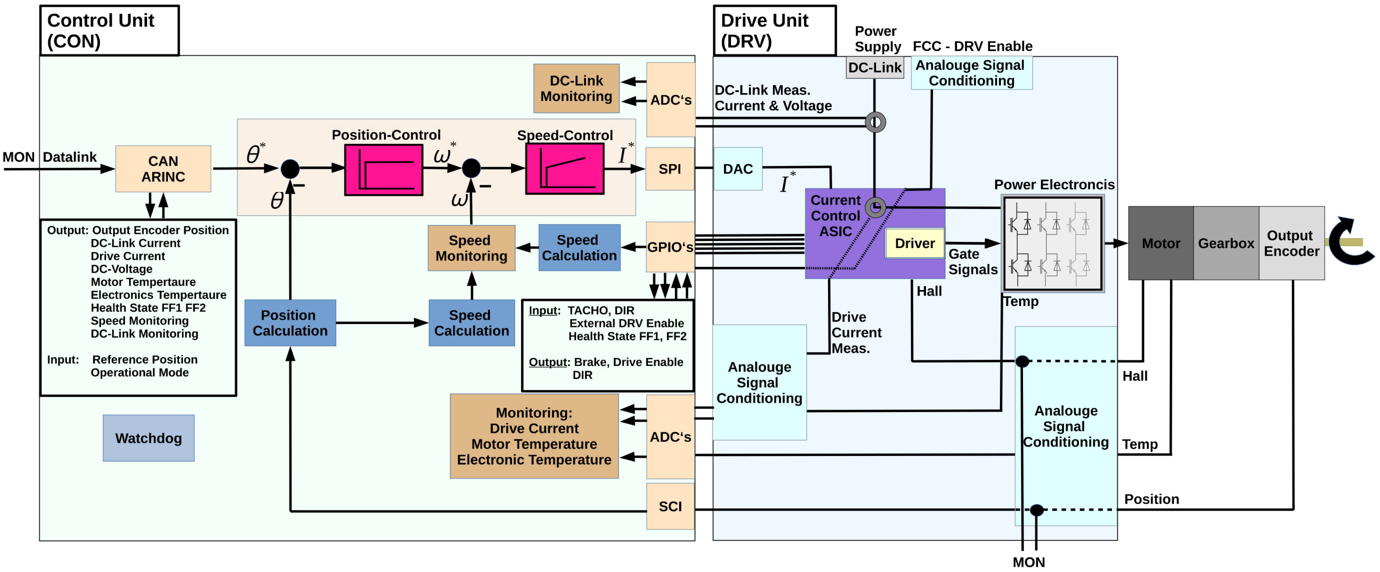

Figure 14. Overview of the electronic and software architecture (one of two identical lanes).

4. Health Monitoring System Design

The health monitoring system consists of three monitoring units: MON A, MON B and MON C, as shown in Figure 15. Both MON A and MON B have identical monitoring functions for their local lanes for detecting inter-lane faults, while MON C is dedicated to detecting cross-lane faults between Lane A and Lane B. An example of a cross-fault is torque fighting between actuation lanes due to sensor or communication faults. The next subsections provide a detailed investigation of the internal monitoring functions of the monitoring units.

4.1. Health-Monitoring Functions

4.1.1. Open Loop Monitors (OLMs)

Open Loop Monitors (OLMs) provide a monitoring function for the position-tracking performance of the actuator output shaft. As shown in Figure 16, an OLM function consists of a simplified single-input–single-output dynamic model, G_p, to represent the nominal position-tracking performance. A position residual, r_θ, between the measured actuator position θ_{mes} and the predicted position $\hat{\theta}$ (estimated by G_p), is calculated as follows (Equation (6)):

$$r_\theta = \theta_{mes} - \hat{\theta}, \tag{6}$$

A fault diagnosis decision by an OLM is based on two processing levels for the position residual r_θ. First, the position residual is compared to a threshold TH_p to only detect significant deviations, i.e., higher than TH_p, between the measured θ_{mes} and the predicted positions $\hat{\theta}$. Second, the position residual magnitude should be checked for its duration above the threshold. The transient operation of the actuator typically involves short spikes that may temporarily exceed TH_p and cause false diagnosis. The minimum duration for a position transient over the threshold, to be identified as a fault, is called the fault latency interval for the position residual FLI_p.

Both TH_p and FLI_p are constant parameters, and they are calculated (i.e., within the design phase) by an iteration method to maximize the fault diagnosis efficiency for numerous simulated fault conditions with transient operating conditions. Here, an OLM is considered for each actuation lane, namely, OLM_A and OLM_B, as shown in Figure 15. OLM_A and OLM_B use the position encoders of Lane A and Lane B, respectively, to independently measure the same output position of the actuator θ_{mes}. This is a reliability concept to maintain fault-tolerant features. The OLM function generates a decision signal, OLM_D, which has a low logic by default, and it is raised to a high logic if an abnormal event is detected.

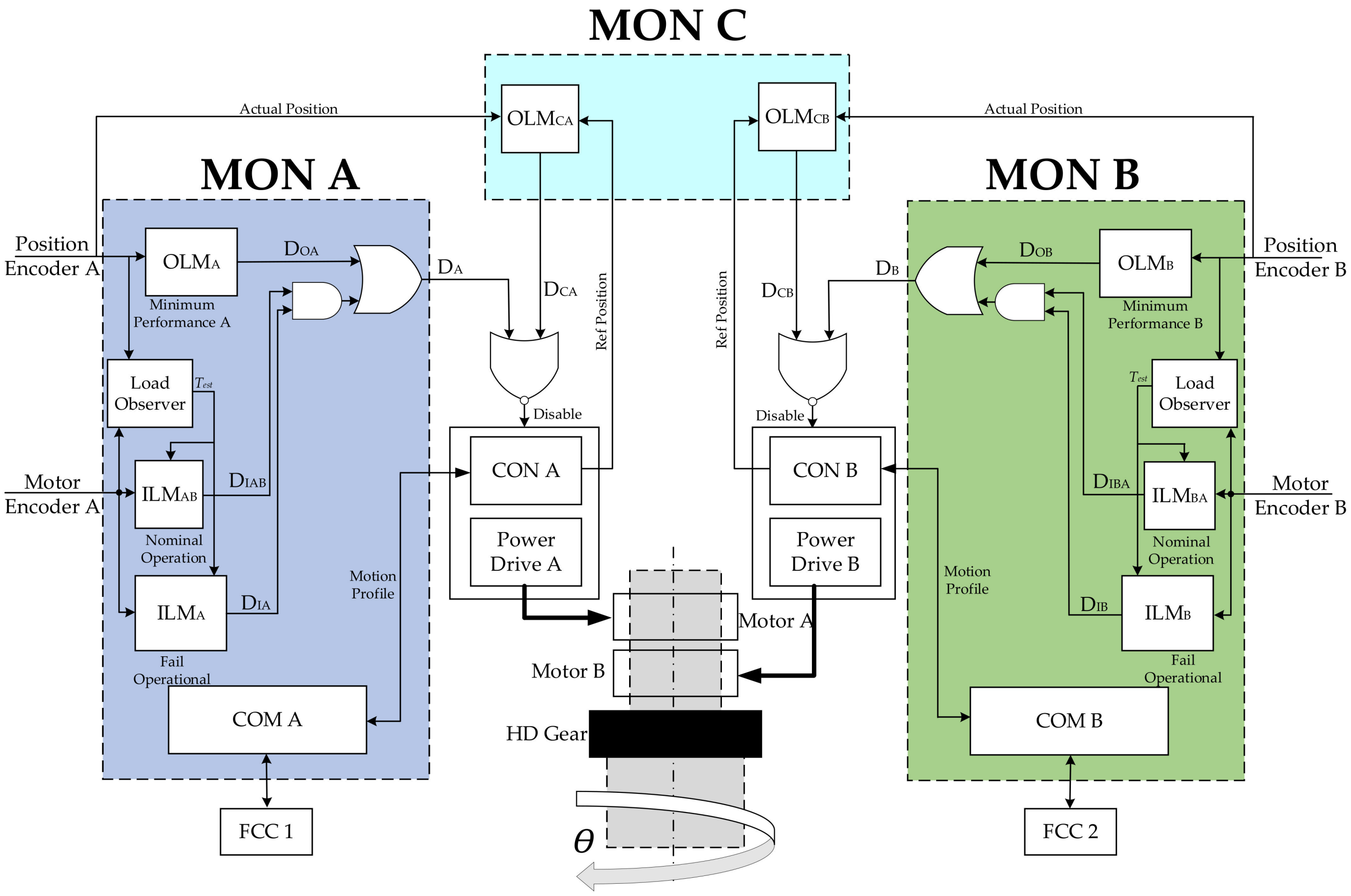

Figure 15. Fault-tolerant actuation architecture comprising three health monitoring units and a dual co-axial motor.

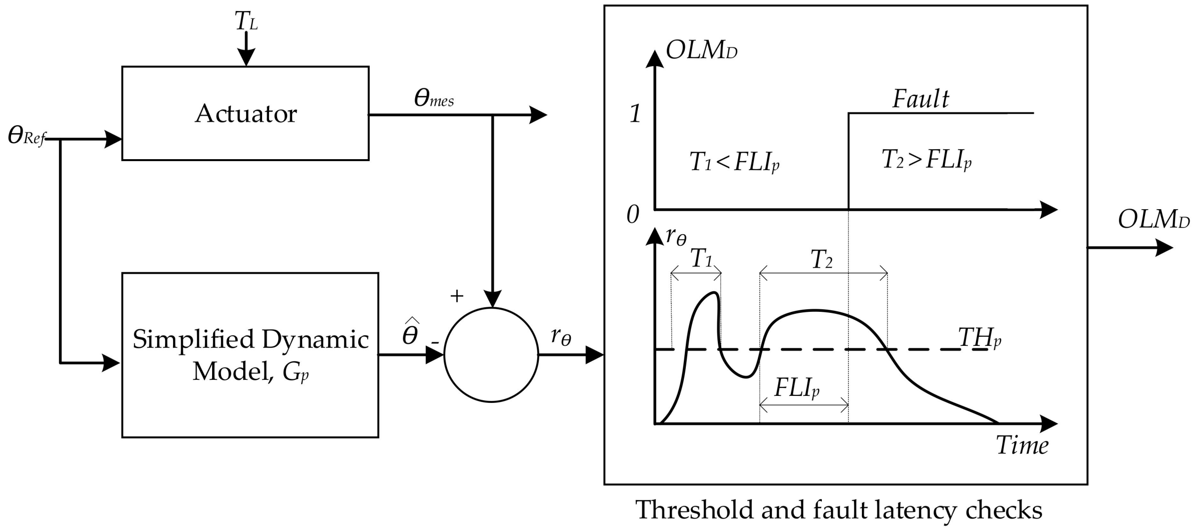

Figure 16. The principle of an OLM function.

4.1.2. Inner Loop Monitors (ILMs)

Inner Loop Monitors (ILMs), also known as the first-order tracking method [8], provide a monitoring function for the speed tracking performance of the individual actuator lanes. Simplified versions of ILMs for EMAs have been previously investigated in [7,8] for detecting electrical and mechanical faults. However, these ILMs are exclusively based on monitoring speed tracking performance without compensating the actuator load. In this paper, enhanced ILMs are investigated by directly incorporating the actuator load into ILMs, as shown in Figure 17. The enhanced ILM consists of a multi-input–single-output dynamic model, G_v, to represent the nominal speed-tracking performance at a load level T_L. A speed residual, r_v, between the measured actuator speed $\dot{\theta}_{mes}$ and the predicted speed $\hat{\dot{\theta}}$ (estimated by G_{vI} and G_{vT}) is calculated as follows (Equation (7)):

$$r_{\dot{\theta}} = \dot{\theta}_{mes} - \hat{\dot{\theta}} \tag{7}$$

Similar to OLMs, a fault diagnosis decision by an ILM is based on two processing levels: the speed threshold, TH_v, and the fault latency interval, FLI_v. Both TH_v and FLI_v are constant parameters, and they are calculated (i.e., within the design phase) by a search method to maximize the fault diagnosis efficiency for numerous simulated fault conditions with realistic transient operating conditions. Here, two ILMs are considered for each actuation lane: ILM_{AB} and ILM_{A} for Lane A and ILM_{BA} and ILM_{B} for Lane B. ILM_{AB} is dedicated to monitoring the nominal operational mode based on a simplified model G_{vAB} where both lanes A and B are operational. ILM_{A} includes a simplified model, G_{vA}, in which only Lane A is operational, i.e., a fail-operational A mode. The objective of using two different ILMs for nominal and fail-operational modes is to generate and monitor two residuals for each operating mode. This strategy aims at increasing health monitoring efficiency and sensitivity. For OLMs, the position tracking performance for nominal and fail-operational modes are almost identical because the OLM's residual does not significantly account for the internal configuration of the actuator, whereas the ILM's residual is directly influenced by the local lane current and hence the ongoing degradation status.

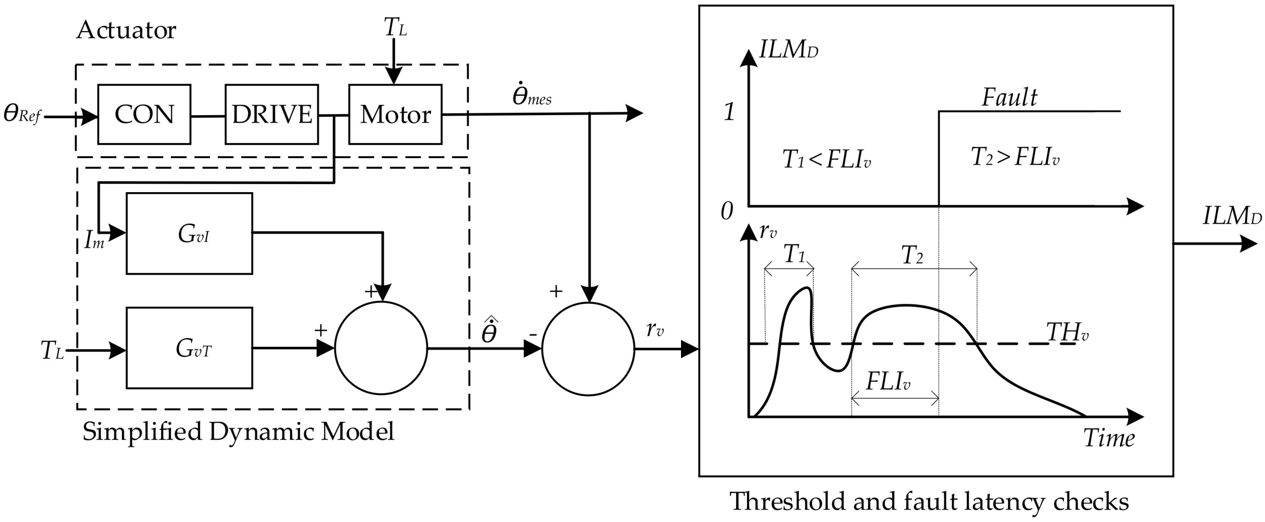

Figure 17. The principle of an enhanced ILM function.

The ILM function generates a decision signal ILM_{D} which has zero logic by default and is raised to one logic if an abnormal event is detected. The determination of G_{vAB} and G_{vA} is based on data-based identification procedures for the actuator during the nominal and the fail-operational modes, and it is discussed in Section 5.2.

4.2. Multiple Model Monitors

The objective of developing multiple model monitors (MMMs) is to generate multiple reference signals for evaluating actuator health. These signals are estimated from multiple models and independent sensors. This approach aims at enhancing the reliability of health monitoring functions and their diagnosing decisions. Here, three MMMs are utilized, namely: MON A, MON B and MON C. Both MON A and MON C are utilized for monitoring local lane faults through an OLM and two ILM functions. While MON C provides backup monitoring for critical cross-lane faults, considering Lane A as an example, the OLM_A provides a monitoring function for the position tracking error, as discussed in Section 4.1.1, using the position encoder for Lane A. Whether the actuator is working on the nominal mode or on the fail-operational model, the position tracking requirements are almost similar so that only one single OLM is used per lane. On the other side, there is a significant performance deviation for the ILM performance if the actuator is working on a nominal or a fail-operational mode, so that it is necessary to develop multiple ILMs for each operational mode. There are two ILMs for Lane A, namely: ILM_A and ILM_AB. Additionally, for Lane B, there are identical ILMs denoted as ILM_B and ILM_BA. Please note that pairs of ILM_A and ILM_B, as well as ILM_AB and ILM_BA, have identical dynamic models, but they are driven by data from independent local lane-level sensors, i.e., redundant position and motor encoders.

As discussed in Section 4.1.2, the efficiency of developing reliable ILM functions is based on incorporating the actuator load measurements to cancel abnormal ILM residuals due to irregular load transients. Here, all ILM functions need actuator load measurements. Using a load sensor has several challenges, such as the expensive costs as two load sensors must be used to prevent single failures in addition to the reduced reliability for increasing actuator complexity.

A load observer function is integrated into MON A and MON B, as shown in Figure 15. The actuator load is monitored using the relatively low torsional stiffness of the Harmonic Drive gear of the actuator output shaft. The torsional deformation of said gear is extracted by subtracting synchronized data from position and motor encoders. This data is then mapped to the actuator load using a dynamic model. The full development and experimental testing of such a load observer concept have been recently published in [24].

The ILM_AB has been identified to model a healthy nominal mode for the actuator in which both lanes are fully operative, while the ILM_A has been identified to model the fail-operational mode for Lane A in which Lane B is fully disconnected. The monitoring functions OLM_A, ILM_A and ILM_AB generate corresponding decision signals D_OA, D_IA and D_IAB, respectively. A decision signal has zero logic by default and it is raised to one logic if an abnormal event is detected. The diagnosis decisions from ILM_A and ILM_AB, D_IA and D_IAB are summed in AND gate to generate the joint ILM diagnosis decision. The overall diagnosis decision, D_A or D_B, for the lane is determined internally by either a decision from the OLM function or the joint ILM decision, as shown in Figure 15.

For MON C, there are only two OLMs, i.e., OLM_CA and OLM_CB, that are based on the position encoder of Lane A and Lane B, respectively. The objective of MON C is to monitor the position-tracking performance of the whole actuator because it is a high-level operational requirement. In addition, MON C performs a self-monitoring function for both MON A and MON B for possible wrong commands or their total loss of functions. Both OLM_CA and OLM_CB receive the actual position directly from local lane encoders. The position reference signal is obtained from direct links to local controllers, as shown in Figure 15. For example, if MON A is defective, i.e., D_A cannot be activated, OLM_CA will still be operative, and it provides a diagnosis decision to switch off Lane A (the control and drive unit of Lane A) by D_CA instead of D_A. A full allocation of the system faults due to a loss of a sensor or a processing unit is listed in Table 7.

Table 7. Multiple model monitors and the diagnosis decision signals.

Diagnosis Decision Signal	D_A	D_B	D_{CA}	D_{CB}
Default, Nominal Operation	0	0	0	0
Loss of position encoder A	1	0	1	0
Loss of position encoder B	0	1	0	1
Loss of motor encoder A	1	0	0	0
Loss of motor encoder B	0	1	0	0
Loss of MON A	0	0	1	0
Loss of MON B	0	0	0	1
Loss of MON C	0	0	0	0
Loss of CON A	1	0	1	0
Loss of CON B	0	1	0	1

4.3. Mode Transition Mangement

The default operating mode of the actuator is the nominal mode in which both Lane A and Lane B are fully operative. In case of a limited tolerable fault, the nominal mode is kept active. Otherwise, a severe fault will lead to a mode transition towards either a fail-operational mode or the Fail Safe mode, as discussed in Section 2. The definition of a limited or a severe fault is tunable by adjusting OLM and ILM parameters (described in Section 5.2) in order to control their diagnosis decision signals. As shown in Figure 15, there are four primary diagnosis signals, namely: D_A, D_B, D_{CA} and D_{CB}. Both D_A and D_B are assigned for Lane A and Lane B, respectively, based on their local ILM and OLM functions, while MON C generates D_{CA} and D_{CB} as redundant diagnosis signals for Lane A and Lane B based on OLMs at MON C. The mode transition management of the actuator based on the primary diagnosis decision signal is listed in Table 8.

Table 8. Mode transition management based on diagnosis decision signals.

Mode/Diagnosis Decision	DA ∪ DCA	$D_B \cup D_{AB}$
Default (Nominal Mode)	0	0
Fail-operational A	1	0
Fail-operational B	0	1
Fail Safe (Actuator off)	1	1

5. Fault-Tolerant Actuation Evaluation

In this section, the health monitoring functions, as developed in Section 4, are tuned and evaluated using a high-fidelity model of the actuator. First, a wide range of physical and sensor faults are considered for determining the optimum parameters for OLMs and ILMs for all lanes. Second, the performance of the tuned monitoring functions is evaluated and discussed.

5.1. Fault Injection Methods

There are two common methods for injecting faults into the actuator model, namely: parameter-based fault injection and performance-based fault injection, as follows:

5.1.1. Parameter-Based Fault Injection

In this method, the faults are modeled by dynamic changes of actuator parameters, e.g., a reduced armature resistance for a short circuit and a reduced magnetic flux parameter for the magnet flux degradation. This method is simple and easy to be executed for some faults. However, there are two significant limitations related to its sensitivity. It is negatively influenced by model uncertainties and dynamic approximations. In addition, it is hard to be evaluated by performance requirements. For example, a 10% reduction in the armature resistance cannot be directly converted to a specific system requirement, e.g., the corresponding power deficiency. Excessive friction faults are considered by the viscus friction parameter of the gear (parameter-based fault injection), which is a common element for both lanes.

5.1.2. Performance-Based Fault Injection

The performance-based fault injection is modeled by applying dynamic changes to the actuator operational variables, e.g., a reduced motor torque to emulate a short circuit fault. The performance-based fault injection also involves a dynamic disconnection (i.e., termination of the output signal during nominal operation) for the lane controllers CON A–B or monitoring units. The principle is based on modeling the faults in terms of adding a disturbance torque to the actuator model to emulate a degradation. The main advantage is that the fault effects can be evaluated directly on the actuator requirements for the torque performance data. Two sets of performance-based and parameter-based faults are considered in Table 9 based on the reliability analysis in Section 2.

The drag torque is an electrical braking torque due to a short-circuit fault. The severity of a drag torque depends on the short circuit location, as explained in Table 4. The drag torque is calculated by multiplying the drag torque gain (20–100%) and the electrical torque of a lane. Then, it is injected as an additive torque loss to the electric torque of the lane.

Table 9. List of potential faults and their injecting methods.

Fault Condition	Injection Method
Drag torque in Lane A or B	Performance-based
Open circuit in Lane A or B	Performance-based
Dynamic disconnection of CON A or B	Performance-based
Dynamic disconnection of MON A, B or C	Performance-based
Reduction in armature resistance Lane A or B	Parameter-based
Reduction in magnetic flux Lane A or B	Parameter-based
Increase in the viscous friction of the gear	Parameter-based

5.2. Monitoring Functions Tuning

5.2.1. Simplified Dynamic Models

Two datasets have been generated from a high-fidelity SIMULINK model for the actuator, including comprehensive control and electrical and mechanical subsystems, and it runs at a 100 kHz sampling rate. The datasets were collected at a 1 kHz sampling rate as a target sampling frequency for the health monitoring system to support their execution in embedded targets, e.g., microcontrollers. The datasets are used to identify the necessarily simplified models for OLMs and ILMs, and they include the reference position, the actual speed, the local lane currents and the applied aerodynamic load. The first dataset is for the nominal operation condition, where both lanes are fully operative. The second dataset is for a fail-operational mode, in which one lane (A or B) is disabled. Data-based system identification methods have been applied, using Captain® Toolbox [25], to find the optimum discrete transfer functions for OLMs and ILMs (described in Figures 16 and 17) as listed in Table 10.

Table 10. Simplified dynamic models for OLMs and ILMs.

Model	Transfer Function
$\boldsymbol{G_p}$	$\frac{0.00097z^{-1}}{1-1.9427z^{-1}+0.9436z^{-2}}$
$\boldsymbol{G_{vIA}}$, $\boldsymbol{G_{vIB}}$	$\frac{0.8154}{1-0.9967z^{-1}}$
$\boldsymbol{G_{vIAB}}$, $\boldsymbol{G_{vIBA}}$	$\frac{1.6466}{1-0.9967z^{-1}}$
$\boldsymbol{G_{vT}}$	$\frac{0.0163z^{-1}}{1-0.9963z^{-1}}$

5.2.2. Fault Latency and Thresholds

The optimum estimation for the fault latency and thresholds for OLMs and ILMs is driven by certain requirements and constraints. The requirements encompass reliable implementation for the fault detection and reconfiguration, according to Table 3. In addition, the monitoring functions must not violate the actuator control stability during and after the actuator reconfiguration process. The faults in Table 3 can be grouped into critical control faults and non-critical control faults. The first group includes faults that directly influence the stability of the actuator control loop—fault IDs: 18,19 and 23–26. The whole actuator becomes unstable if the detection and reconfiguration time for these faults are not fast enough to follow the actuator control loops. The second group involves other faults where their detection and reconfiguration intervals are less significant to the control stability. In order to estimate the optimum fault latency and thresholds, the monitoring functions have been evaluated separately for critical control faults. The stability of the actuator control has been evaluated for wide ranges of thresholds and fault latency intervals for ILMs and OLMs to determine their stability constraint maps, as shown in Figures 18 and 19.

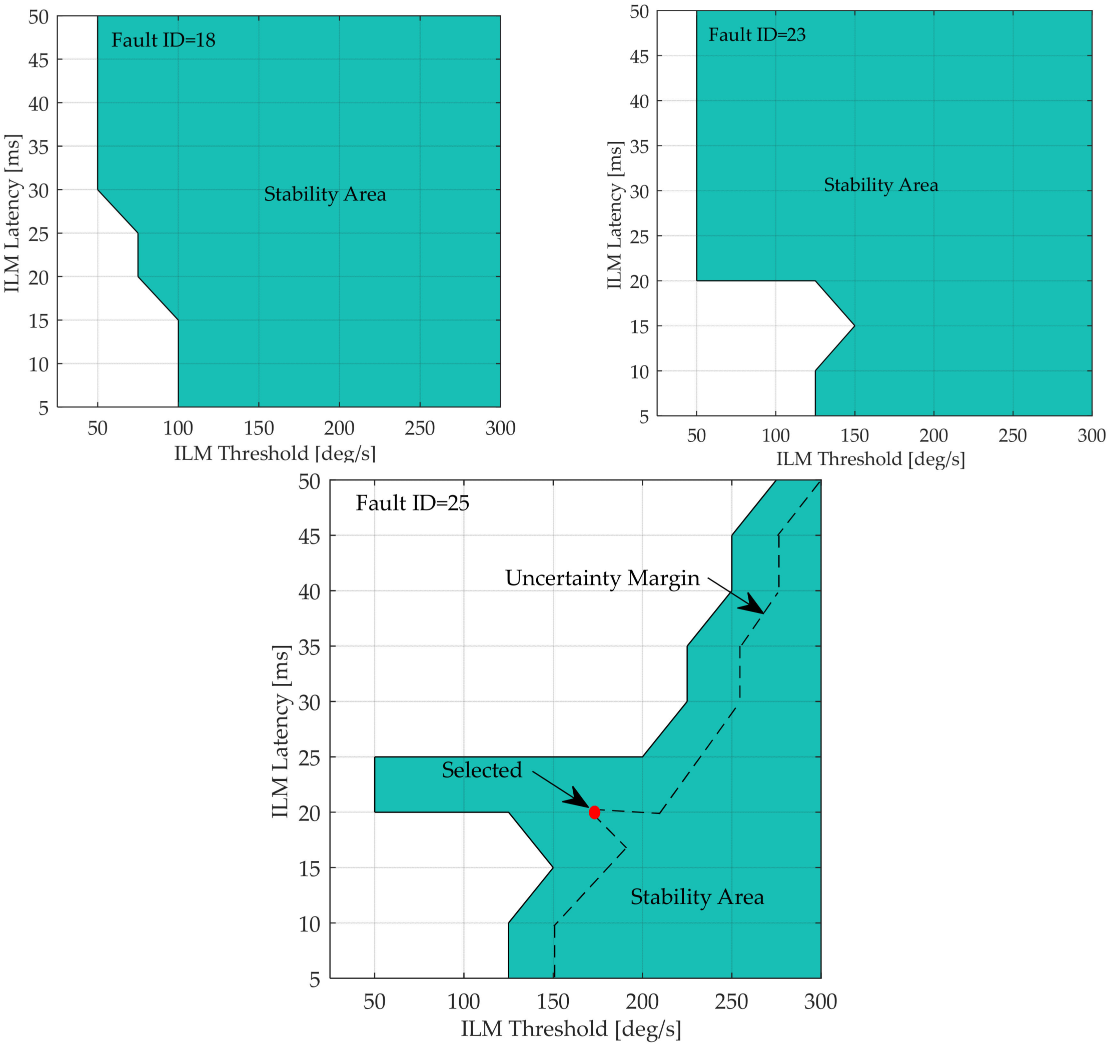

Figure 18. Stability constraint maps for ILM functions for fault ID = 18, 23 and 25.

The first map (Figure 18) is for ILM functions, and it is the same for all ILMs: ILM_{A}, ILM_{AB}, ILM_{B} and ILM_{BA}. On the left side, possible ILM pairs, i.e., threshold and fault latency, to achieve stable control are highlighted by shaded area for fault ID = 18 or 19, which is a loss of a controller. On the right side, stable ILM pairs are for a loss of the position encoders, i.e., fault ID = 23 or 24. On the bottom side, stable ILM pairs are for a loss of the motor encoders, i.e., fault ID = 25 or 26, where the stability area is more constrained compared to fault ID = 18 or 19. The optimum selection of ILM pairs should consider an uncertainty margin to account for the operational transients and simulation approximations. This margin is realized by a threshold level of 160 deg/s and a latency of 20 ms.

The second map (Figure 19) is for OLM functions. For controlling critical faults, the control stability is only influenced by the OLM threshold. Similar to ILM, an uncertainty margin for OLM parameters involve the OLM threshold of 1.5 deg and the same latency of ILM of 20 ms. Parameters for OLMs and ILMs are listed in Table 11.

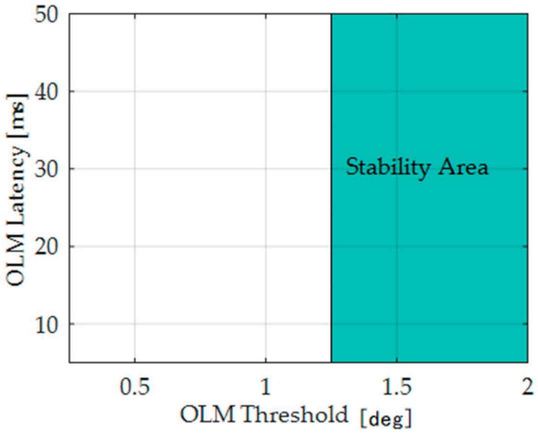

Figure 19. Stability constraint map for OLM functions for fault ID = 18, 23 and 25.

Table 11. Optimum OLM/ILM parameters at sampling rate of 1 kHz.

Parameter	Magnitude	Unit
TH_p	1.5	deg
TH_v	160	deg/s
FLI_p	25	ms
FLI_v	20	ms

5.3. Fault Toleranace Performance

Fault detection and reconfiguration functions have been evaluated for 30 health conditions listed in Table 3. Four detailed case studies will be discussed in this section, in addition to the overall performance for all conditions in Table 3. The first case study is for fault ID = 2, where a 20% drag torque (20% of the electric torque) is applied to Lane B after 0.5 s. As shown in Figure 20, there are no significant errors for both position and speed tracking performance for the actuator after injecting the fault. The reference speed is bounded within the predicted nominal levels that are estimated by ILM_{AB} (Nominal AB) and ILM_{BA} (Nominal BA). The largest nominal margin occurred at 1.2 s, where the external load direction is altered at no movement. Fail-operational A and B indicate the predicted health status by ILM_{A} and ILM_{B}, respectively.

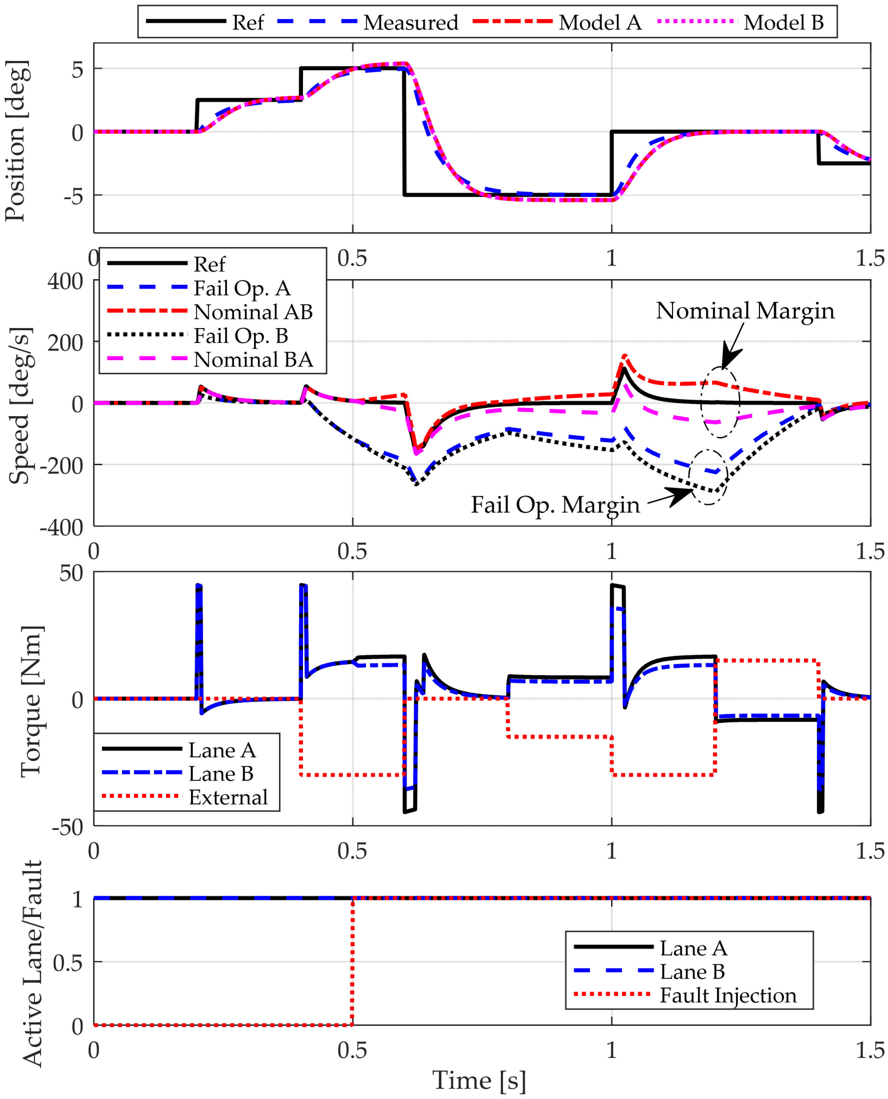

Figure 20. Example of a nominal operation after an operational marginal fault, fault ID = 2 in Table 3.

The second case study is for fault ID = 18, where the controller of Lane A is disconnected after 0.5 s, as shown in Figure 21. The fault has been detected by a diversion from the reference speed to the speed of the fail-operational A (ILM_A). This diversion initiated a mode transition after 0.061 s of injecting the fault. There is no significant deviation for the position tracking error after the fault injection because the actuator reconfiguration maintained that desired position-tracking performance.

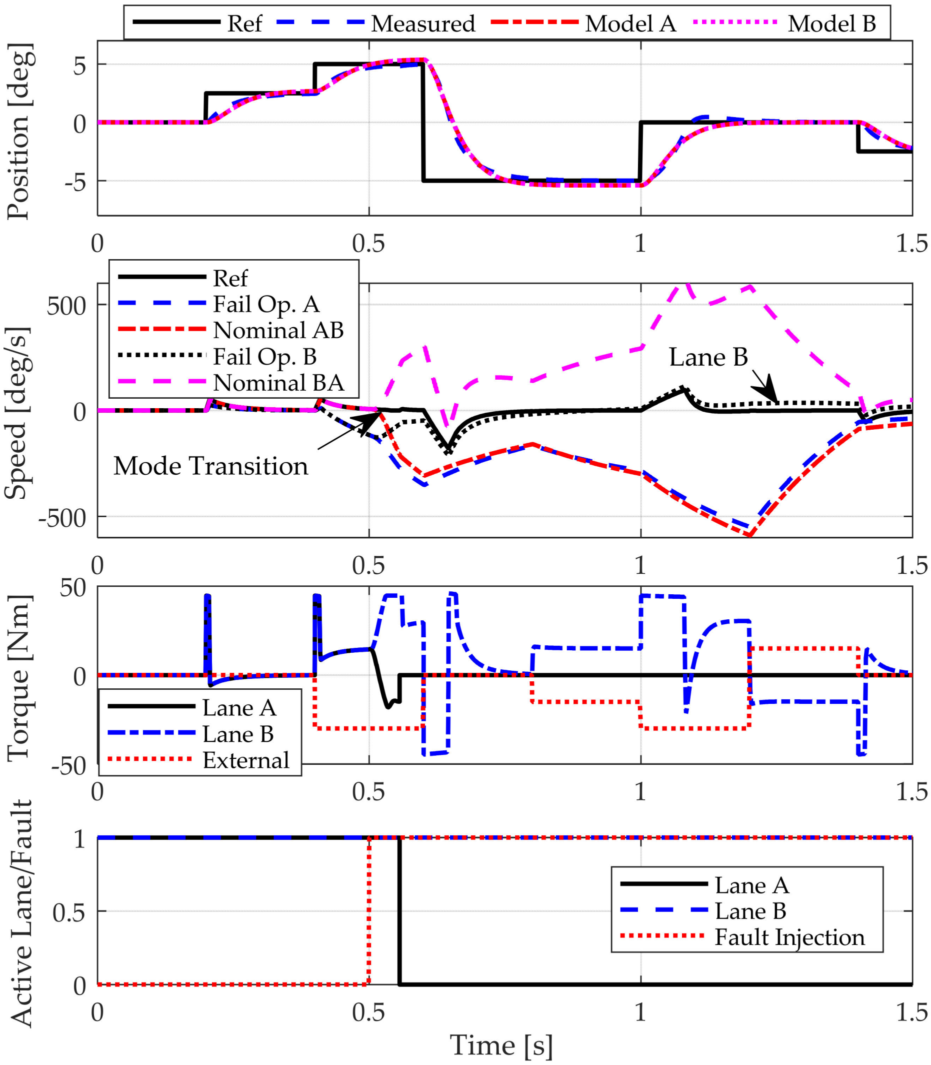

Figure 21. Example of a fail-operational after a local lane fault, fault ID = 18 in Table 3.

The third case study is for fault ID = 16, where 80% reduction of the magnetic flux of Lane B occurred after 0.5 s, as shown in Figure 22. As described in Section 5.1.1, a reduction of the magnetic flux is a parameter-based fault injection by decreasing the magnetic flux parameter in the actuator model. The fault has been detected by a diversion from the reference speed to the speed of fail-operational B (ILM_B). This diversion initiated a mode transition after 0.082 s of injecting the fault. There is no significant deviation for the position tracking error after the fault injection.

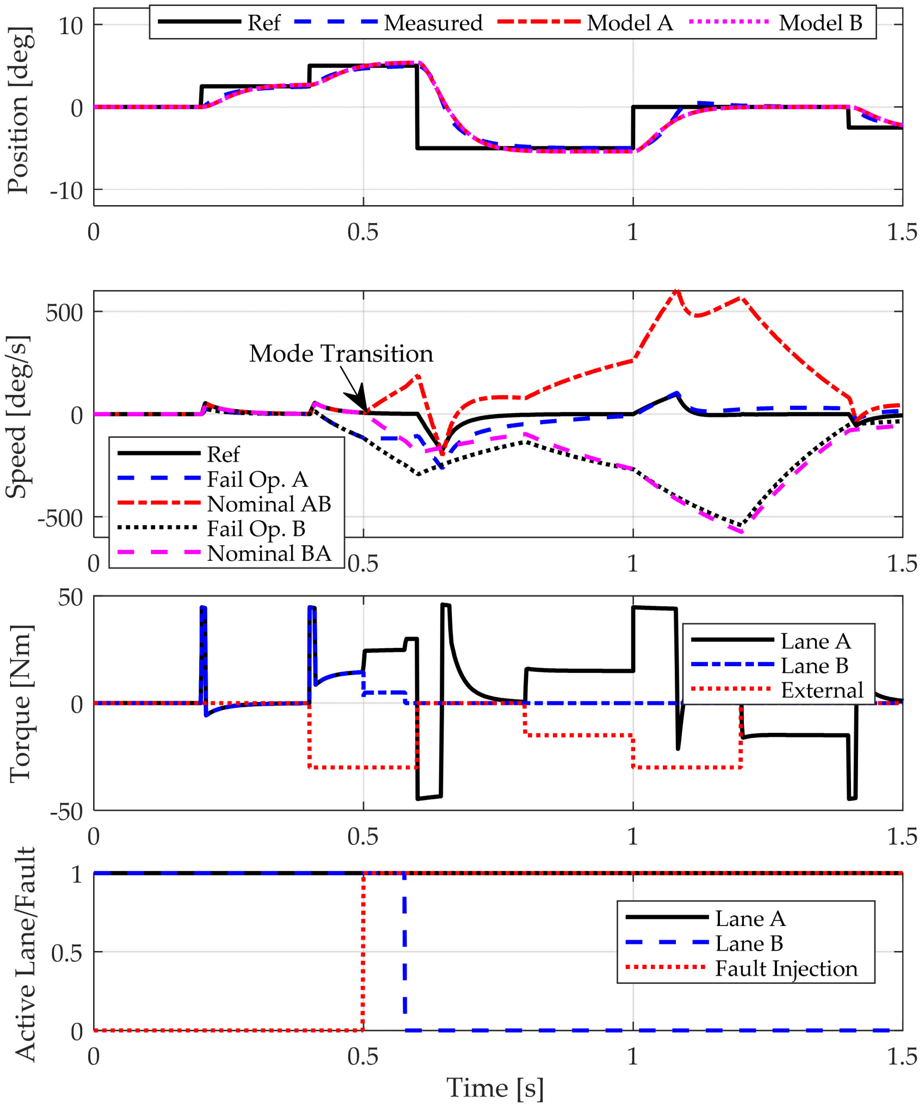

Figure 22. Example of a fail-operational after a local lane fault, fault ID = 16 in Table 3.

The last case study is for fault ID = 30, where there is an increase of 800% for the friction parameter of the gear unit after 0.5 s, as shown in Figure 23. This fault affects both lanes as the gear is a common element. The fault has been detected by a diversion from the reference speed away to none of the fail-operational modes; thus, a fail safe of disconnecting the whole actuator has been activated. There is a fault detection latency of 0.183 s, which does not significantly compromise safe mode transition to failsafe mode.

The overall fault tolerance performance is shown in Figure 24 and Table 12. Based on the estimations in Figure 24, the mode transition interval can be used to generally classify the criticality of the faults. The fault criticality is inversely proportional to the mode transition interval because lower critical faults need an extended duration to trigger the monitoring function than higher critical ones than modes with a higher criticality.

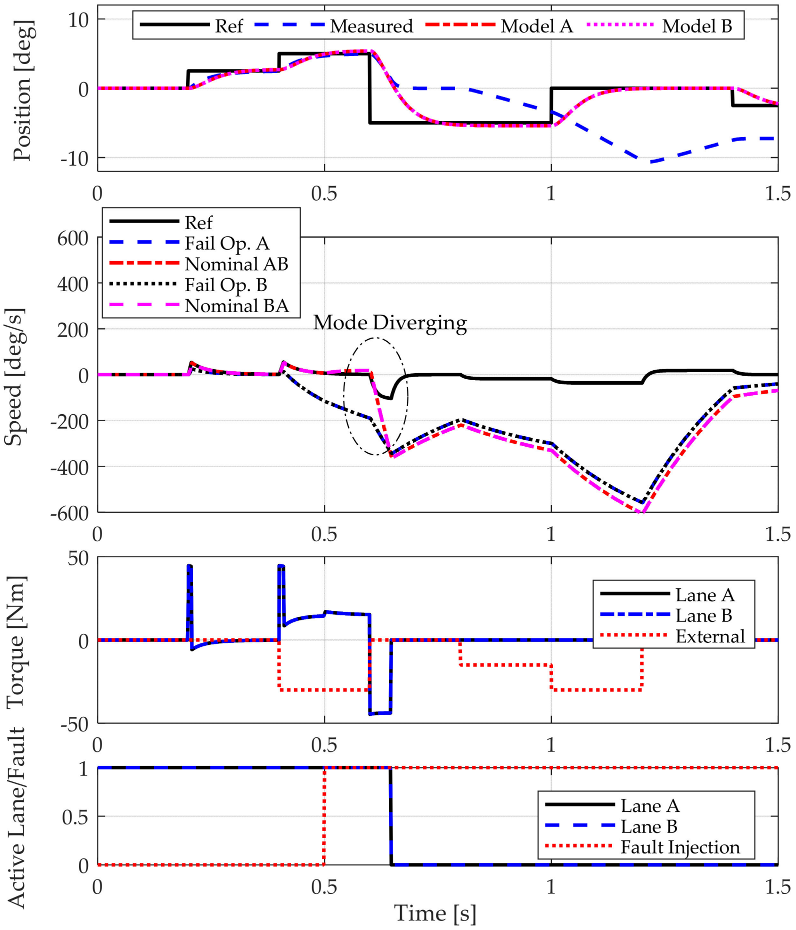

Figure 23. Example of a fail safe after a cross-lane fault, fault ID = 30 in Table 3.

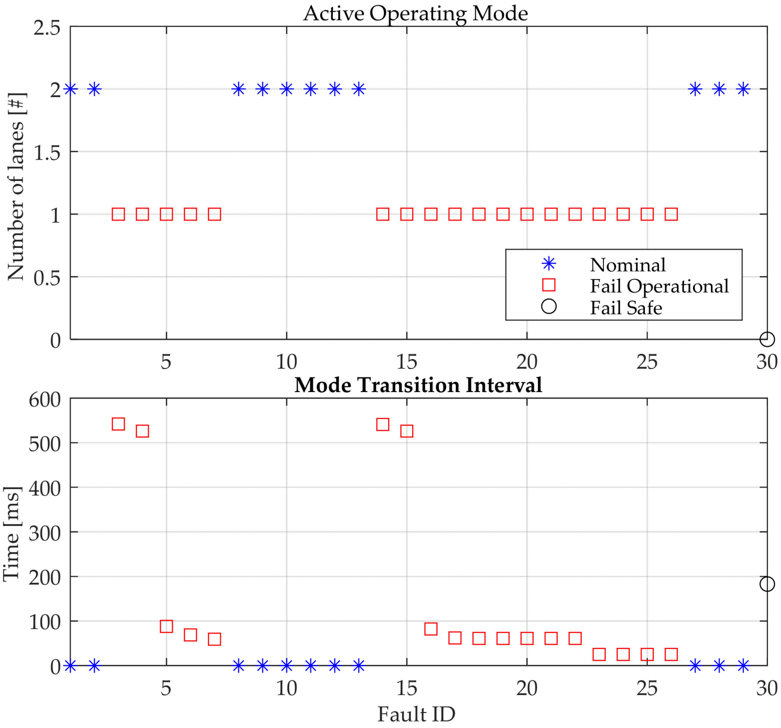

Figure 24. Fault detection and reconfiguration for 30 health conditions in Table 12.

Table 12. Fault detection and reconfiguration for 30 health conditions.

Fault ID	**Condition**	**Reconfiguration**	
		Time (ms)	**Mode**
1	Healthy	0	Nominal Operation
2	Drag torque in Lane B, 20%	0	
3	Drag torque in Lane B, 40%	542	Fail Operational
4	Drag torque in Lane B, 60%	526	
5	Drag torque in Lane B, 80%	88	
6	Drag torque in Lane B, 100%	69	
7	Open circuit in Lane B	59	
8	Reduction in armature resistance Lane B, 20%	0	Nominal Operation
9	Reduction in armature resistance Lane B, 40%	0	
10	Reduction in armature resistance Lane B, 60%	0	
11	Reduction in armature resistance Lane B, 80%	0	
12	Reduction in armature resistance Lane B, 100%	0	
13	Reduction in magnetic flux Lane B, 20%	0	
4	Reduction in magnetic flux Lane B, 40%	541	Fail Operational
15	Reduction in magnetic flux Lane B, 60%	526	
16	Reduction in magnetic flux Lane B, 80%	82	
17	Reduction in magnetic flux Lane B, 100%	62	
18	Disconnection of CON A	61	
19	Disconnection of CON B	61	
20	Disconnection of MON A	61	
21	Disconnection of MON B	61	
22	Disconnection of MON C	61	
23	Disconnection of Position Encoder A	25	
24	Disconnection of Position Encoder B	25	
25	Disconnection of Motor Encoder A	25	
26	Disconnection of Motor Encoder B	25	
27	Increase in the viscous friction of the gear, 200%	0	Nominal Operation
28	Increase in the viscous friction of the gear, 400%	0	
29	Increase in the viscous friction of the gear, 600%	0	
30	Increase in the viscous friction of the gear, 800%	183	Fail Safe

6. Conclusions

The development of a fault-tolerant EMA architecture for future certified UAVs has been discussed for a realistic heavy unmanned gyro-copter. It has been shown that an hourly probability of at least 5×10^{-6} should be reached for certification under EASA SC-RPAS.1309. To show compliance, a Markov analysis coupled with a detailed bottom-up failure rate computation was performed. This analysis showed stringent requirements (minimum 98% fault detection) for the Health Monitoring System. At the same time, high-quality aviation components as well as a state-of-the-art mechanical design should be used to reach the threshold for certification. The fault-tolerant motor design minimizes the discussed motor short circuits by means of the proposed winding design and installation constraints. The design allows a parallel and single operation of the motor by the main and redundant windings and through independent control electronics and sensor units. In addition, the motor encoder is located externally from the stator winding, and electronic components are separated from the motor. This reduces the thermal stress of the sensors and electronic components and reduces the maximum hot spot temperature within the system. The fault-tolerant architecture has been supported by two new health-monitoring concepts, namely, multiple mode monitors and sensorless load observers. The multiple mode monitors are aimed at generating multiple condition indicators for evaluating the actuator health status. These indicators are estimated from multiple health monitoring models and sensors. Not only a single failure but also a deficiency for a monitoring function or a sensor cannot violate the overall health and the actuation function. In addition, the efficiency of evaluating the actuator health during in-flight conditions has been reinforced by utilizing two sensorless load observers. They provide redundant aerodynamic load measurements for tuning health monitoring functions to be less sensitive to load-based false diagnoses. A tuning procedure for health monitoring functions has been investigated to account for the actuator control stability. It has been reported that there are constraints for selecting monitoring functions to keep the actuator in a stable closed-loop control. Such constraints are calculated by iterative parameter-searching simulations for all stability-related faults. The final tuned monitoring functions include a safety boundary for detecting potential faults as well as avoiding violating the control stability requirements. Health monitoring functions have been successfully evaluated for a set of 30 scenarios of physical, performance and sensor faults that are injected into a high-fidelity SIMULINK model, including a fluctuated aerodynamic load.

Author Contributions: Fault-tolerant health monitoring features and fault-detection methods, M.A.A.I.; fault-tolerant electrical design and modeling, S.W. and C.S.; reliability-driven analysis architecture design, C.B. All authors have read and agreed to the published version of the manuscript.

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

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Sadeghzadeh, I.; Zhang, Y. A Review on Fault-Tolerant Control for Unmanned Aerial Vehicles (UAVs). In Proceedings of the 2011 AIAA Infotech@Aerospace Conference, St. Louis, MI, USA, 29–31 March 2011.
2. Bosch, C.; Ismail, M.A.; Wiedemann, S.; Hajek, M. Towards Certifiable Fault-Tolerant Actuation Architectures for UAVs. In *Advances in Condition Monitoring and Structural Health Monitoring*; Lecture Notes in Mechanical Engineering; Springer: Singapore, 2021; pp. 355–364.
3. Dalla Vedova, M.D.L.; Lauria, D.; Maggiore, P.; Pace, L. Linear Electromechanical Actuators affected by Mechanical Backlash: A Fault Identification Method based on Simulated Annealing Algorithm. *WSEAS Trans. Syst.* **2015**, *14*, 268–276.
4. Ismail, M.A.; Bosch, C.; Wiedemann, S.; Bierig, A. Fault-Tolerant Actuation Architectures for Unmanned Aerial Vehicles. In *Advances in Condition Monitoring and Structural Health Monitoring*; Lecture Notes in Mechanical Engineering; Springer: Singapore, 2021; pp. 345–354.
5. Swerdon, G.; Watson, M.; Bharadwaj, S.; Byington, C.S.; Smith, M.; Goebel, K.; Balaban, E. A system engineering approach to electro-mechanical actuator diagnostic and prognostic development. In Proceedings of the Machinery Failure Prevention Technology (MFPT) Conference, Dublin, Ireland, 23–25 June 2009.
6. Todeschi, M.; Baxerres, L. Health monitoring for the flight control EMAs. *IFAC PapersOnLine* **2015**, *48*, 186–193. [CrossRef]
7. Arriola, D.; Thielecke, F. Model-based design and experimental verification of a monitoring concept for an active-active electromechanical aileron actuation system. *Mech. Syst. Signal Process.* **2017**, *94*, 322–345. [CrossRef]
8. Rito, D.; Schettini, F. Health monitoring of electromechanical flight actuators via position-tracking predictive models. *Adv. Mech. Eng.* **2018**, *10*, 1–12.
9. SAE International. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*; ARP4761; SAE International: Warrendale, PA, USA, 1996.

10. European Aviation Safety Agency. *Special Condition—Equipment, Systems, and Installation*; SC-RPAS.1309-01; European Aviation Safety Agency: Cologne, Germany, 2015; Issue 2.
11. Rito, D.; Galatolo, R.; Schettini, F. Self-monitoring electro-mechanical actuator for medium altitude long endurance unmanned aerial vehicle flight controls. *Adv. Mech. Eng.* **2016**, *8*, 1–11.
12. Balaban, E.; Bansal, P.; Stoelting, P.; Saxena, A.; Goebel, K.F.; Curran, S. A diagnostic approach for electro-mechanical actuators in aerospace systems. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2009.
13. Baklouti, A.; Nguyen, N.; Mhenni, F.; Choley, J.-Y.; Mlika, A. Improved Safety Analysis Integration in a Systems Engineering Approach. *Appl. Sci.* **2019**, *9*, 1246. [CrossRef]
14. Xuan, J.; Wang, X.; Lu, D.; Wang, L. Research on the safety assessment of the brushless DC motor based on the gray model. *Adv. Mech. Eng.* **2017**, *9*, 1–15. [CrossRef]
15. Wang, N.; Zhou, Y. Research on Reliability of a Hybrid Three-Redundant Electro-Mechanical Actuator. In Proceedings of the IEEE International Conference on Mechatronics and Automation, Changchun, China, 9–12 August 2009.
16. Bennett, J.W. Fault Tolerant Electromechanical Actuators for Aircraft. Ph.D. Thesis, Newcastle University, Newcastle upon Tyne, UK, 2010.
17. Bodden, D.S.; Clements, N.S.; Schley, B.; Jenney, G. Seeded Failure Testing and Analysis of an Electro-Mechanical Actuator. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 3–10 March 2007.
18. Zhu, S.; Cox, T.; Xu, Z.; Gerada, C.; Li, C. Design Considerations of Fault-Tolerant Electromechanical Actuator Systems for More Electric Aircraft (MEA). In Proceedings of the IEEE Energy Conversion Congress and Exposition (ECCE), Portland, OR, USA, 23–27 September 2018.
19. Department of Defense. *Military Handbook—Reliability Prediction of Electronic Equipment*; MIL-HDBK-217F; US Department of Defense: Washington, DC, USA, 1991.
20. Bonivento, C.; Capiluppi, M.; Marconi, L.; Paoli, A.; Rossi, C. Reliability Evaluation for Fault Diagnosis in Complex Systems. *IFAC Proc. Vol.* **2006**, *39*, 1330–1335. [CrossRef]
21. A Methodology for Components Reliability. Available online: www.fides-reliability.org (accessed on 27 April 2021).
22. Hopper, T.; Anders, M.; Stuckmann, C. Building electric motors for space, with redundancy and high reliability. In Proceedings of the 14th European Space Mechanics and Tribology Symposium (ESMATS), Constance, Germany, 28–30 September 2011.
23. Zhao, K.; Cheng, L.; Zhang, C.; Nie, D.; Cai, W. Induction Motors Lifetime Expectancy Analysis Subject to Regular Voltage Fluctuations. In Proceedings of the IEEE Electrical Power and Energy Conference (EPEC), Saskatoon, SK, Canada, 22–25 October 2017.
24. Ismail, M.A.; Windelberg, J.; Liu, G. Simplified Sensorless Torque Estimation Method for Harmonic Drive Based Electro-Mechanical Actuator. *IEEE Robot. Autom. Lett.* **2021**, *6*, 835–840. [CrossRef]
25. Young, P.C.; Taylor, C.J.; Tych, W.; Pedregal, D.J.; McKenna, P.G. *Captain Toolbox*; Lancaster University: Lancaster, UK, 2010.