Special Issue Article

Advances in
Mechanical
Engineering

Advances in Mechanical Engineering
2016, Vol. 8(5) 1–11
© The Author(s) 2016
DOI: 10.1177/1687814016644576
aime.sagepub.com
SAGE

Self-monitoring electro-mechanical actuator for medium altitude long endurance unmanned aerial vehicle flight controls

Gianpietro Di Rito, Roberto Galatolo and Francesco Schettini

Abstract

This article deals with the reliability analysis and architecture definition of a fault-tolerant electro-mechanical actuator system for unmanned aerial vehicle applications. Starting from the basic layout of the flight control system of a medium altitude long endurance unmanned aerial vehicle, the attention is focused on the fault mode analysis of the single electro-mechanical actuator system, with the purpose of pointing out the effects of architectural choices on the system reliability. The electro-mechanical actuator system, developed to be a self-monitoring equipment, has three operating modes: normal, fail-operative and fail-safe. Reliability and safety budgets are quantitatively evaluated via fault tree analysis using typical failure rates of system components, and the most critical paths are identified and discussed.

Keywords

Fault-tolerant systems, electro-mechanical actuator, criticality analysis, fault tree analysis

Date received: 29 October 2015; accepted: 21 March 2016

Academic Editor: Nam-Ho Kim

Introduction

Electrically powered actuators are nowadays the reference technology for unmanned aerial vehicle (UAV) flight controls, and their applicability is quite proved in terms of performances.[1–4] Electro-mechanical solutions allow to attain load, speed and dynamic response objectives,[5] but several concerns are still open in terms of reliability. In particular, the use of electro-mechanical actuators (implying less maintainability constraints, thanks to the elimination of hydraulic fluids) requires a cautious approach to safety issues, mainly for a lack of statistical database about components' fault modes.[6] An effective counteraction is provided by redundant architectures managed by health-monitoring electronics, in order to obtain fail-operative and/or fail-safe actuators.[7–10] With reference to a basic electro-mechanical actuator system (EMAS), composed of a control electronics, a power electronics, an electrical motor and a gear reducer, several strategies can be used to reach this goal. Mechanical redundancies can be employed in torque summing or velocity summing architectures.[9,10] Electric redundancies can operate in multiple lanes for both control and power electronics.[7,11] The choice about the number and the type of redundancies depends on the target reliability allocated to the actuator which, in turn, depends on the whole flight control system (FCS) architecture and its overall reliability. For example, the split of control surfaces into independent sub-surfaces, each one actuated by a

Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Pisa, Italy

Corresponding author:
Gianpietro Di Rito, Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Sez. Aerospaziale, Via Caruso 8, Pisa I-56122, Italy.
Email: g.dirito@dia.unipi.it

Table 1. UAV safety objectives for flight on non-segregated airspace: comparison between Italian and US military regulations.

Hazard risk index	STANAG 4671:2009[17] (150 kgf ≤ MTOW ≤ 20,000 kgf)	AER(EP).P-6[18] (MTOW ≥ 4000 kgf)	Catastrophic	Hazardous	Major	Minor	No safety effect
Frequent	$p > 10^{-3}$ pFH	$p > 10^{-1}$ pFH	🟥 Unacceptable	🟥	🟥	🟥	🟩
Probable	$p < 10^{-3}$ pFH	$p < 10^{-1}$ pFH	🟥	🟥	🟥	🟩	🟩
Remote	$p < 10^{-4}$ pFH	$p < 10^{-3}$ pFH	🟥	🟥	🟩	🟩	🟩
Extremely remote	$p < 10^{-5}$ pFH	$p < 10^{-5}$ pFH	🟥	🟩	🟩 Acceptable	🟩	🟩
Extremely improbable	$p < 10^{-6}$ pFH	$p < 10^{-6}$ pFH	🟩	🟩	🟩	🟩	🟩

MTOW: maximum take-off weight.

single EMAS, makes the total loss of control (LOC) of the actuators less critical. System health monitoring with fault detection and isolation is also a key issue in order to make the EMAS operative in case of partial failure, or fail-safe in case of total LOC.[12,13] Reliability analysis plays a fundamental role in this context, by identifying failure modes criticality and providing quantitative system failure rate evaluation.[14–16]

In this article, the reliability analysis has been carried out through the following steps. First of all, the cumulative probability for a catastrophic failure condition is defined, according to applicable airworthiness certification regulations for a medium altitude long endurance (MALE) UAV.[17,18] The FCS layout is then chosen, in terms of number of control surfaces, each one actuated by a single EMAS. The possible FCS failure modes are analysed by a functional hazard assessment (FHA) to find the most critical condition and to derive the failure rate budget for a single EMAS. A possible EMAS architecture is therefore defined, in terms of number and type of internal redundancies. Finally, a fault tree analysis (FTA) is performed to evaluate the system failure rate and to compare it with the target budget. The most critical paths of the FTA are identified and discussed, by highlighting the EMAS components that are more relevant for the reliability level. A list of EMAS monitors capable of managing system redundancies and providing satisfactory failure coverage is finally given.

Safety budget allocation for UAV EMAS

Certification references

The design of an actuator for modern primary flight controls (i.e. implementing automatic and/or autonomous functions) is strongly affected by the safety requirements imposed at aircraft level by the airworthiness regulations. This issue is overemphasised in case of UAV applications, also for the lack of a unified certification reference. The NATO airworthiness certification regulation STANAG 4671:2009[17] is applicable to UAVs having maximum take-off weight (MTOW) in the range 150–20,000 kgf flying above non-segregated airspace, and its paragraph 1309 states that the cumulative probability of occurrence of catastrophic failure conditions shall be lower than 10^{-6} per flight hour. The Italian Ministry of Defence technical directive AER(EP)-P.6[18] also provides guidelines for the safety objectives of Italian Army UAV weighting more than 4000 kgf (Table 1). In particular, the cumulative probabilities of failures with catastrophic and hazardous effects are equal to those recommended by STANAG 4671, while the requirements are more relaxed for failures impacting on UAV reliability (i.e. with major or minor effects).

The reliability requirements of safety-critical equipments derive from those at UAV-level (Table 1), and also depend on UAV architecture, that is, on the number of failure conditions determining an event with safety/reliability effects. For the preliminary design phases, the AER(EP)-P.6 document (used in this work as reference for the EMAS architecture definition) suggests to assume 100 catastrophic failure conditions, and to consequently scale all other objectives. This means that the probability of occurrence of a single catastrophic failure condition shall be budgeted at 10^{-8} per flight hour.

Flight control actuation system layout and EMAS failure rate budgeting

The work has been carried out with reference to the layout of the FCS of a MALE UAV developed by Alenia Aermacchi (see Figure 1). Provided that each surface is moved by a dedicated EMAS, the flight control functions are implemented as follows:

- *Roll control*: performed by four ailerons, two per wing;
- *Pitch control*: performed by three elevators on the horizontal tail;
- *Yaw control*: performed by two rudders, one per each of the two vertical tails.

Table 2. Failure rate budgeting for the flight control EMAS.

FHA outcomes			EMAS failure rate budgeting	
Failure mode	Failed surfaces	Effects	Reliability constraint from AER(EP)-P.6	Requirement for λ_{EMAS}
Partial loss of aileron surface	1	Major	$4\ \lambda_{EMAS} < 10^{-5}$ pFH	$<2.50 \times 10^{-6}$ pFH
	2, on different wings	Major	$4\ \lambda_{EMAS}^{2} < 10^{-5}$ pFH	$<1.58 \times 10^{-3}$ pFH
	2, on the same wing	Hazardous	$2\ \lambda_{EMAS}^{2} < 10^{-7}$ pFH	$<2.24 \times 10^{-4}$ pFH
Total loss of aileron surface	**1**	**Hazardous**	$\mathbf{4\ \lambda_{EMAS} < 10^{-7}}$ **pFH**	$\mathbf{<2.50 \times 10^{-8}}$ **pFH**
	2	Catastrophic	$6\ \lambda_{EMAS}^{2} < 10^{-8}$ pFH	$<4.08 \times 10^{-5}$ pFH
Partial loss of elevator surface	1	Minor	$3\ \lambda_{EMAS} < 10^{-3}$ pFH	$<3.33 \times 10^{-4}$ pFH
	2	Major	$3\ \lambda_{EMAS}^{2} < 10^{-5}$ pFH	$<1.83 \times 10^{-3}$ pFH
	3	Hazardous	$\lambda_{EMAS}^{3} < 10^{-7}$ pFH	$<4.64 \times 10^{-3}$ pFH
Total loss of elevator surface	1	Hazardous	$3\ \lambda_{EMAS} < 10^{-7}$ pFH	$<3.33 \times 10^{-8}$ pFH
	2	Catastrophic	$3\ \lambda_{EMAS}^{2} < 10^{-8}$ pFH	$<5.77 \times 10^{-5}$ pFH
	3	Catastrophic	$\lambda_{EMAS}^{3} < 10^{-8}$ pFH	$<2.15 \times 10^{-3}$ pFH
Partial loss of rudder surface	1	Major	$2\ \lambda_{EMAS} < 10^{-5}$ pFH	$<5 \times 10^{-6}$ pFH
	2	Hazardous	$\lambda_{EMAS}^{2} < 10^{-7}$ pFH	$<3.16 \times 10^{-4}$ pFH
Total loss of rudder surface	1	Hazardous	$2\ \lambda_{EMAS} < 10^{-7}$ pFH	$<5 \times 10^{-8}$ pFH
	2	Catastrophic	$\lambda_{EMAS}^{2} < 10^{-8}$ pFH	$<10^{-4}$ pFH

EMAS: electro-mechanical actuator system; FHA: functional hazard assessment.
Partial loss is intended as a condition of performance degradation, but the surface motion is still safe.
Total loss is intended as a condition that causes a surface jam or unsafe motion.
Bold characters indicate the most stringent case for the maximum allowable EMAS failure rate requirement.

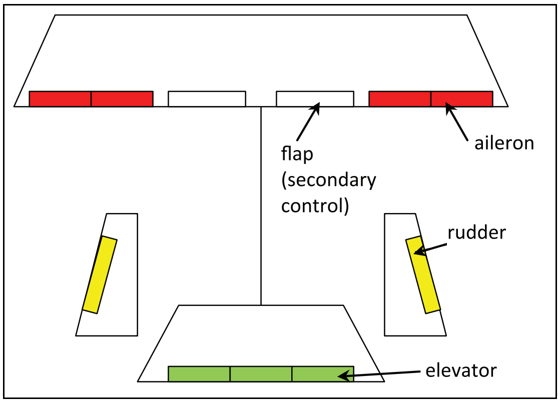


Figure 1. Flight control surfaces of the reference MALE UAV.

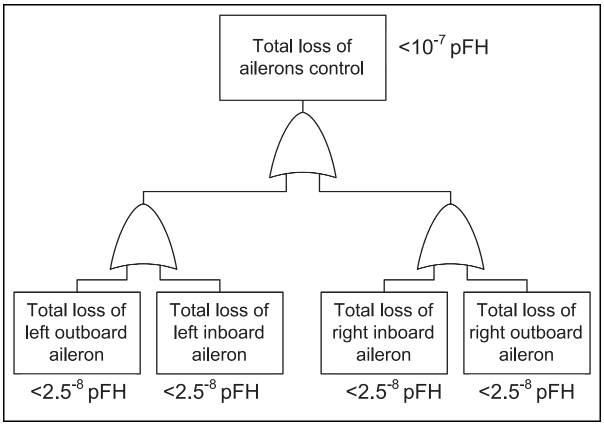

Total loss of ailerons control
$<10^{-7}$ pFH
Total loss of left outboard aileron
Total loss of left inboard aileron
Total loss of right inboard aileron
Total loss of right outboard aileron
$<2.5^{-8}$ pFH
$<2.5^{-8}$ pFH
$<2.5^{-8}$ pFH
$<2.5^{-8}$ pFH

Figure 2. Example pf EMAS failure rate budgeting.

An excerpt of the preliminary FHA of the UAV FCS is given in Table 2, together with the evaluation of the derived EMAS failure rate requirement (λ_{EMAS}), once that the AER(EP)-P.6 safety/reliability constraints are applied. The calculation is made under the assumption that the EMAS is only affected by random faults (i.e. infant mortality and wear-out effects are neglected), so that its failure probability density is exponential.[19] The results demonstrate that the roll control function is the most critical one (Figure 2), and that the dimensioning criterion for EMAS failure rate is related to the total loss of 1 out of 4 ailerons.

EMAS architecture definition

High computational resources are needed to perform the closed-loop control of EMAS, especially for current and speed loops. For this reason, these functions cannot be performed by the flight control computers (FCC), but they must be implemented by dedicated electronics. The control electronics can be integrated with the actuator, obtaining the so-called smart actuators, or separately installed into actuator control units (ACU). The latter approach has been used for the proposed EMAS, mainly to overcome installation problems:

smart actuators have larger dimensions, which in some cases are not compatible with the airfoil thickness.

Functional requirements

In the reference application, the FCS has three FCCs handling the air data and inertial sensor signals. The FCCs exchange their data in order to process a common set of feedbacks and provide the EMAS with consistent operating mode and set-point commands. The operating mode and the set-point commands are the inputs which enable the EMAS to perform its two main functions: equipment health-monitoring and surface control.

Equipment health-monitoring function. With this function, the EMAS provides information to the FCCs about the health state of its parts and components. These feedbacks allow the FCCs to define the EMAS operating mode, which can be

- *Normal*;
- *Fail-operative*, corresponding to the 'system reconfiguration' mode, in which one or more faults to EMAS components have occurred, and they have been detected, isolated and (if applicable) compensated, so that the system maintains its performances to a satisfactory level;
- *Fail-safe*, corresponding to the 'system recovery' mode, in which one or more faults to EMAS components have occurred, and they have been detected and isolated, and the system is configured to react to loads and environment without lowering the safety of the whole aircraft.

Surface control function. With this function, the EMAS provides motion control of the aerodynamic surface. In *normal* and *fail-operative* modes, this is obtained by a closed-loop control of the surface rotation, which assures static and dynamic performances (high accuracy and resolution, low hysteresis, adequate motion bandwidth and dynamic stiffness, while in *fail-safe* mode the function only implies that the actuator operates without lowering the aircraft safety.

The health-monitoring algorithms, executed at high rate both before and during flight (via Power-Up Built-In-Test and Continuous Built-In-Test, respectively), are performed within the ACU. In case of a detected failure, the ACU has the authority to set the EMAS in *fail-operative* or *fail-safe* mode, communicating to the FCC the health state. In case of lack of communication, the FCC has the authority to command the EMAS transition to the *fail-safe* mode.

Concerning the closed-loop control, it is digitally achieved within the ACU computing processor by three nested loops on EMAS position, motor speed and motor current. The loops run at different frequencies to guarantee adequate stability margins. Preliminary design studies provide evidence of the possibility of obtaining an EMAS position bandwidth of 7 Hz, by setting the sampling rate of current and speed loops at 10 kHz and the position loop at 500 Hz.

In the *fail-safe* mode, the proposed EMAS is designed to provide the surface with damping, in order to avoid catastrophic effects (e.g. flutter instability). This damping action is provided, once the motor is isolated from the electrical supply, by imposing the short circuit on its phases and by dissipating the regenerated currents on a bank resistor.

Qualitative CA of a simplex EMAS

In order to identify the most critical fault modes affecting the EMAS and to justify the proposed design solutions, a qualitative criticality analysis (CA)[19] is reported here with reference to a simplex rotary EMAS composed of the following:

- A simplex digital ACU, performing closed-loop controls on motor currents, speed and position;
- A three-phase permanent magnet synchronous motor;
- A mechanical transmission from the motor to the aerodynamic surface;
- Three current sensors (one per phase);
- A resolver for the motor control;
- A rotary variable differential transformer (RVDT) transducer for the rotation sensing.

The CA is developed following the approach used in Balaban et al.,[6] by defining three groups of failure modes, depending on the component/assembly in which the fault occurs:

- Electronic failures
- Electrical failures
- Mechanical/structural failures

As shown from Tables 3 to 5, each component/assembly fault mode is analysed, by defining the possible fault causes and providing an estimation of the following:

- Fault probability of occurrence (FPO) during the operating time interval, defined selecting one of the following five levels:[19]
  - Frequent (Level A)
  - Reasonably probable (Level B)

Table 3. Qualitative criticality analysis of a simplex EMAS (electronic components' failures).

Component/assembly	Fault mode	Fault mode ref.	Fault cause	FPO	FSC
Power supply module	Open circuit	EC01	Wire crack	D	I
	Short circuit	EC02	Wire chafing Insulation degradation	D	I
	Thermal runway	EC03	Component dielectric breakdown	D	I
	Controller capacitor open/short circuit	EC04	Component dielectric breakdown	D	I
Power Electronics (MOSFET with related circuitry)	e.g. MOSFET open/ short circuit	EC05	Various	C	I
Control Electronics (CPU, etc.)	e.g. CPU failure	EC06	Various	C	I

FPO: fault probability of occurrence; FSC: fault severity category; MOSFET: metal-oxide semiconductor field-effect transistor.

Table 4. Qualitative criticality analysis of a simplex EMAS (mechanical components' failures).

Component/assembly	Fault mode	Fault mode ref.	Fault cause	FPO	FSC
Surface link	Backlash	ME01	Wear of components	C	III
	Jamming	ME02	Wear of components	E	I
	Structural failure	ME03	Warping or load misalignment	E	I
Bearings	Backlash	ME04	Wear of components	C	III
	Jamming	ME05	Recirculating elements block Wear of components	E	I
	Collapse	ME06	Warping or load misalignment	E	I
Output lever	Structural failure	ME07	Crack	E	I
Gearbox	Backlash	ME08	Wear of components	C	III
	Jamming	ME09	Wear of components	E	I
	Collapse	ME10	Crack	E	I
Seals	Leakage	ME11 ME12	Wear Crack	D	III
Lubricant	Loss of lubrication	ME13 ME14	Contamination Chemical breakdown	C	III

FPO: fault probability of occurrence; FSC: fault severity category.

  - Occasional (Level C)
  - Remote (Level D)
  - Extremely remote (Level E)
- Fault severity category (FSC) evaluated at EMAS level, defined selecting one of the following four categories:[19]
  - System loss (Category I)
  - System function loss (Category II)
  - System function degradation (Category III)
  - Unscheduled system repair or maintenance (Category IV)

The CA results have been then reported in the criticality matrix shown in Figure 3. The criticality matrix, synthetically comparing the fault modes in terms of severity and probability of occurrence, provides a tool for assigning corrective action priorities. In particular, the further along the diagonal line from the origin the fault mode is recorded, the greater the criticality and the more urgent the need for implementing corrective action. It is worth noting that the criticality matrix of the simplex EMAS has no fault modes classified as Category II, since the system has only one function and there is no difference between Category I and Category II. It can be noted that for a simplex EMAS, several corrective actions should be necessary to have chance of being safety compliant.

Proposed self-monitoring solution

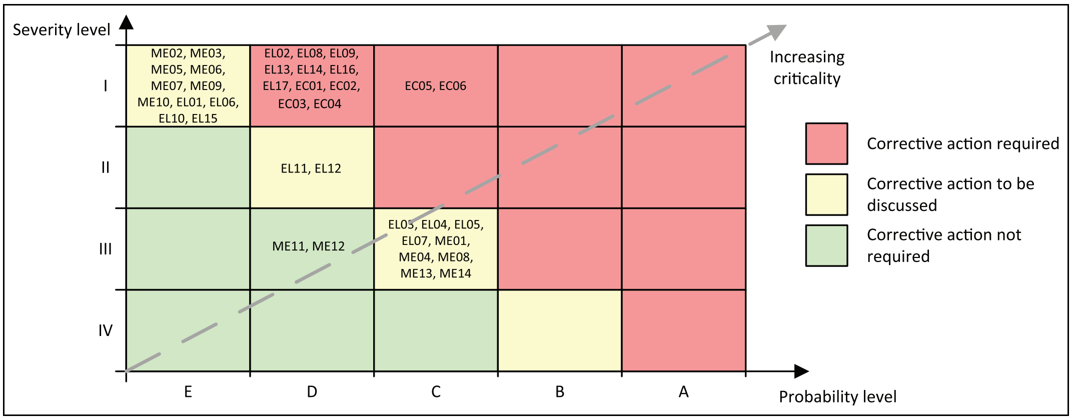
As depicted in Figures 4 and 5, the proposed EMAS is composed of the following:

- The ACU, including
  - two independent computing sections, implementing health-monitoring (MON lane) and closed-loop control (CON lane);
  - a power section modulating the motor coil currents, with three full H-bridges, each one dedicated to a coil, so that the motor is driven with isolated phases;

Table 5. Qualitative criticality analysis of a simplex EMAS (electrical components' failures).

Component/assembly	Fault mode	Fault mode ref.	Fault cause	FPO	FSC
Motor connectors	Disconnection	EL01	Disconnection	E	I
	Contact degradation	EL02	Intermittent connection	D	I
Motor coil	Opened coil	EL03	Wire crack	C	III
	Shorted coil	EL04	Wire chafing Insulation degradation	C	III
	Partially shorted coil	EL05	Wire chafing Insulation degradation	C	III
Motor rotor	Magnet separation	EL06	Bond degradation	E	I
	Magnet demagnetisation	EL07	Thermal runway	C	III
Resolver	Opened coil	EL08	Wire crack	D	I
	Shorted coil	EL09	Wire chafing Insulation degradation	D	I
	Disconnection	EL10	Disconnection	E	I
Current sensors	Opened coil	EL11	Wire crack	D	II
	Shorted coil	EL12	Wire chafing Insulation degradation	D	II
RVDT	Opened coil	EL13	Wire crack	D	I
	Shorted coil	EL14	Wire chafing Insulation degradation	D	I
	Disconnection	EL15	Disconnection	E	I
Wiring	Opened coil	EL16	Wire crack	D	I
	Shorted coil	EL17	Wire chafing Insulation degradation	D	I

FPO: fault probability of occurrence; FSC: fault severity category; RVDT: rotary variable differential transformer.



Severity level	E	D	C	B	A
I	ME02, ME03, ME05, ME06, ME07, ME09, ME10, EL01, EL06, EL10, EL15	EL02, EL08, EL09, EL13, EL14, EL16, EL17, EC01, EC02, EC03, EC04	EC05, EC06		
II		EL11, EL12			
III		ME11, ME12	EL03, EL04, EL05, EL07, ME01, ME04, ME08, ME13, ME14		
IV					

Figure 3. Criticality matrix for a simplex EMAS.

  - a cross-lane data link (CLDL), for the data exchange between the lanes;
  - a supply voltage sensor (SVS);
  - a temperature sensor (TS), measuring the ACU operating temperature;
  - three current sensors (CSa1, CSb1, CSc1), used for closed-loop controls;
  - three current sensors (CSa2, CSb2, CSc2), used for monitoring algorithms;
  - three voltage sensors (VSa, VSb, VSc) used for monitoring algorithms;
  - a resolver (R) for the motor shaft rotation, used for closed-loop control;
  - a transducer (RVDT1) of actuator rotation, used for closed-loop control;
  - a transducer (RVDT2) of actuator rotation, used for monitoring algorithms.
- The EMA, including
  - three-phase permanent magnet synchronous motor with sinusoidal modulation;
  - a two-stage gearbox for the mechanical power transmission.

The ACU CON lane, based on digital signal processor (DSP) technology, is able to manage both the EMAS sensor interfaces and the pulse width

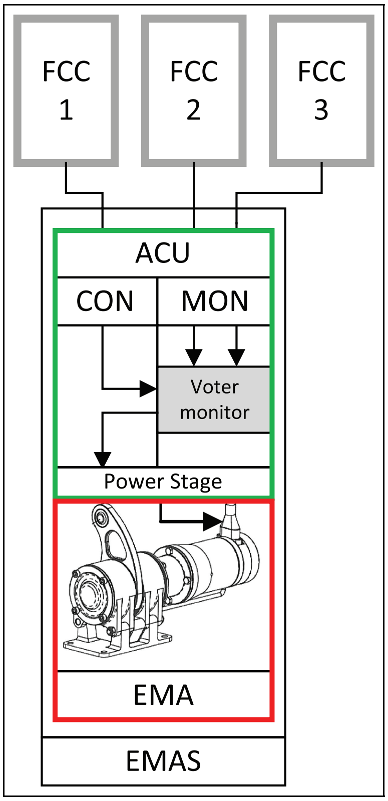


Figure 4. Interface between the EMAS and the FCCs.

modulation (PWM) drive of the motor phases. The MON lane is based on an Advanced RISC Machines (ARM) processor, selected to implement hardware dissimilarity with the ACU CON Lane. The ARM processor has reduced computing performances if compared with the DSP, but it integrates two processors in lock-step configuration to improve the processor error detection (e.g. bus errors and memory errors).

EMAS health-monitoring algorithms

The three basic activities performed by the EMAS monitoring algorithms are as follows:

- *Fault detection*: the operation of distinguishing between normal and failed behaviour, carried out by monitoring, processing and testing system measurements;
- *Fault isolation*: the process of determining the failed component/subsystem that is responsible for abnormal behaviour after a failure has been detected;
- *Fault compensation*: the process of responding to the failure to recover some level of system performance.

The following monitor algorithms have been defined to detect the fault modes analysed during the reliability analysis (a detailed description of the above-mentioned monitor functions is out of the scope of this work):

1. *Outer loop monitor*, which predicts, by means of a model, an expected EMAS response to inputs, in order to detect overall system malfunctions;

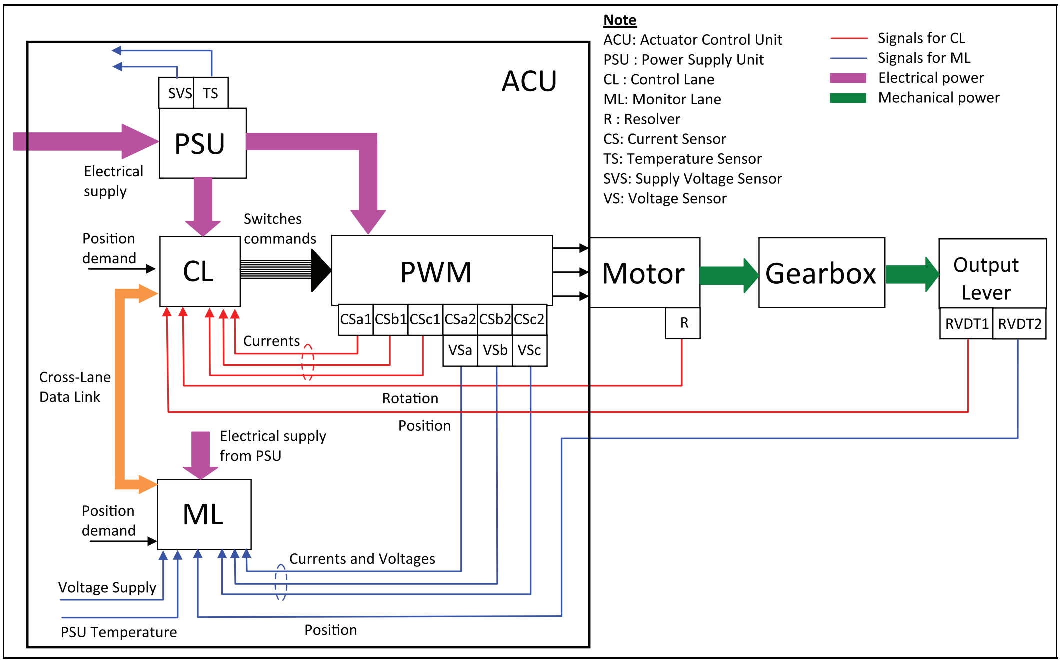


Figure 5. Self-monitoring EMAS architecture.

2. *Current monitor*, which performs a check of the current levels in the motor coils, to detect opened coils and to protect from over-currents;
3. *Cross-lane current monitor*, which performs a comparison between the motor currents measured by the CON and the MON lanes, to detect sensor faults;
4. *In-lane monitors* on RVDTs and resolver, which perform checks of the status of the sensors, to detect component fault;
5. *Cross-lane position monitor*, which performs a comparison between the positions measured by the CON and the MON lanes, in order to detect transducer faults;
6. *Voltage supply monitor*, which performs a check of the voltage supply level, in order to detect a voltage supply breakdown or a voltage sensor fault;
7. *PSU temperature monitor*, which performs a check of the PSU temperature level, in order to detect an abnormal heating of the PSU or a TS fault;
8. *In-lane CPU monitors* (watchdog) for both CON and MON lanes;
9. *Cross-lane voltage demand monitor*, which performs a comparison between the voltage demand for PWM calculated by the CON and the MON lanes, to detect CPU and I/O faults;

It is worth noting that combinations of these algorithms can be implemented for health-state definition at specific mission phases (power-up, pre-flight, etc.).

Effects of the architectural choices on the safety compliance

The safety concerns related to the application (Figure 3) are overcome by the proposed self-monitoring architecture. In particular,

- the system reconfiguration covers the following faults (thanks to the phase-isolating electronics, the control loops are reconfigured and the motor works without performance degradation with only two coils):
  - Electrical failures to the motor coils (EL03, EL04 and EL05, classified as C.III) and to the current sensors (EL11 and EL12, classified as D.II);
  - The power electronics failures (EC05, classified as C.I)
- the system recovery covers the following faults:
  - Control electronics failure (EC06, classified as C.I);
  - Resolver electrical failures (EL08 and EL09, classified as D.I);
  - RVDT electrical failures (EL13 and EL14, classified as D.I);
  - Wiring failures (EL16 and EL17, classified as D.I);
  - Power supply failures (EC01, EC02, EC03 and EC04, classified as D.I);
  - Magnet faults (EL06, classified as E.I, and EL07, classified as C.III);
  - Resolver and RVDT disconnections (EL10 and EL15, classified as E.I).

All other EMAS faults can be covered via maintenance programme (e.g. all the jamming and structural failures) or by specific design solutions (e.g. standard rugged connectors).

Figures 6 and 7 show the FTA related to the total loss of the surface control (i.e. total loss of the EMAS), with reference to the simplex EMAS and to the self-

Table 6. EMAS components failure rate data at 55°C in AUC environment.[20–23]

Component/assembly	Fault mode ref.	Failure rate ($\times 10^{-6}$ pFH)
Power supply module	EC01	0.030
	EC02	0.030
	EC03	0.030
	EC04	0.030
Power electronics	EC05	0.922
Control electronics	EC06	0.820
Fail-safe electronics[a]	EC07	25.546
Surface link	ME02	0.001
	ME03	0.001
Bearings	ME05	0.001
	ME06	0.001
Output lever	ME07	0.001
Gearbox	ME09	3×10^{-4}
	ME10	3×10^{-4}
Motor connectors	EL01	0.004
	EL02	0.380
Motor coil	EL03	1.14
	EL04	1.14
	EL05	1.14
Motor rotor	EL06	10^{-4}
Resolver	EL08	0.162
	EL09	0.162
	EL10	0.003
Current sensors	EL11	0.156
	EL12	0.156
RVDT	EL13	0.270
	EL14	0.270
	EL15	0.005
Cabling	EL16	0.547
	El17	0.547

RVDT: rotary variable differential transformer.
[a] Additional electronics (switch assembly) for the self-monitoring solution.

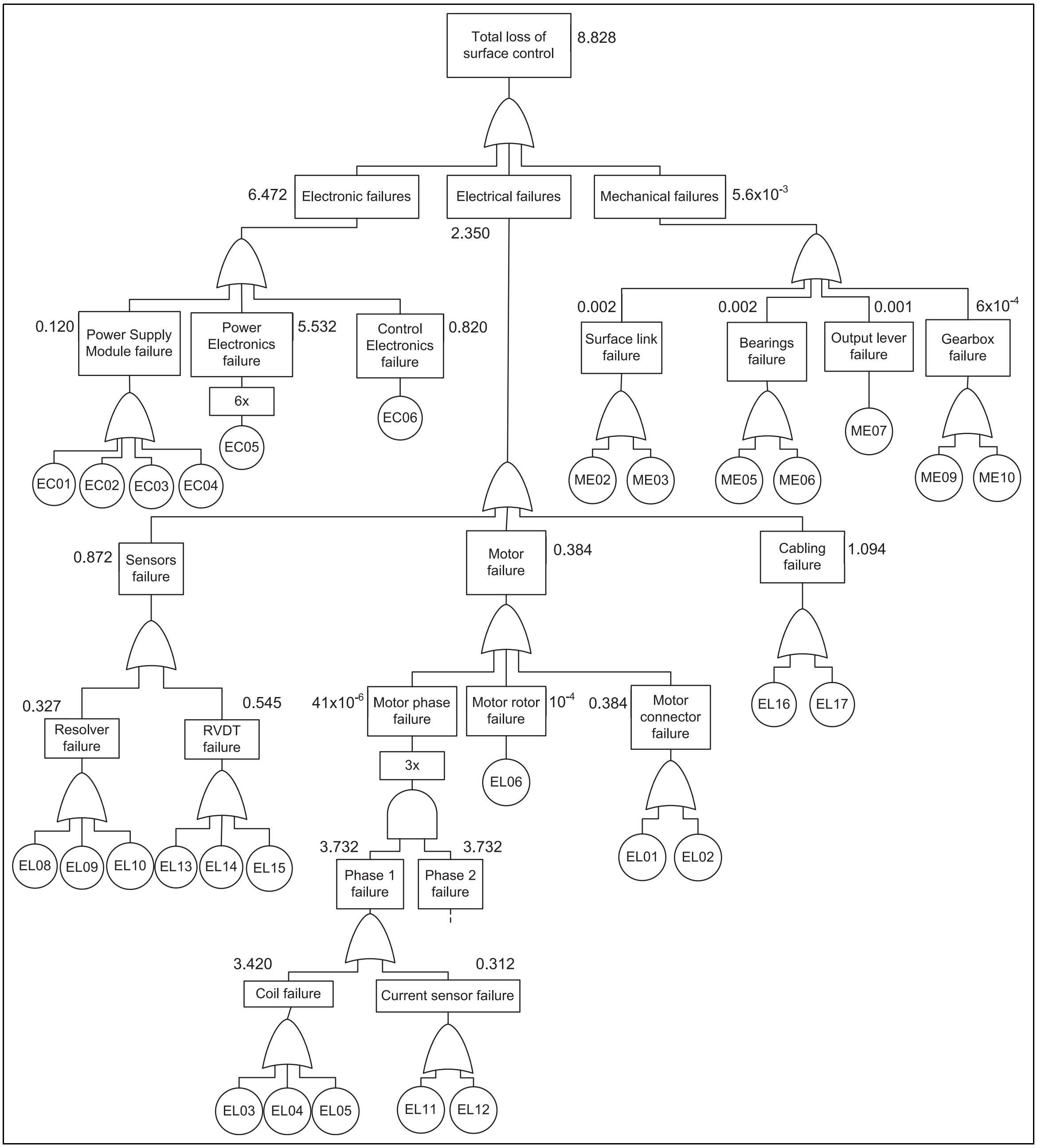


Figure 6. FTA related to the total loss of the simplex EMAS (failure rates × 10^{-6} pFH).

monitoring solution. The failure rate data used in the FTA have been obtained from the literature[20–23] by assuming 55°C operating temperature and airborne uninhabited cargo (AUC) environment (Table 6).

The simplex solution has a 8.828×10^{-6} pFH probability of total loss of surface control (Figure 6), so it is completely inadequate for the application, due to the failure rates of the electronic and electrical sections (6.472×10^{-6} and 2.35×10^{-6} pFH, respectively). On the other hand, the self-monitoring solution (Figure 7), with a 5.75×10^{-9} pFH probability of total loss of surface control, is safety compliant (Table 2). The FTA highlights that this result has been obtained by adding the fail-safe electronics, which, in case of electronic or electrical failures identified by the health-monitoring algorithms, allows to isolate the motor from the electrical supply and to impose the short circuit on its phases (for aerodynamic surface damping). This design thus implies that the EMAS safety level is essentially driven by the mechanical failures, characterised by 5.6×10^{-9} pFH probability of occurrence.

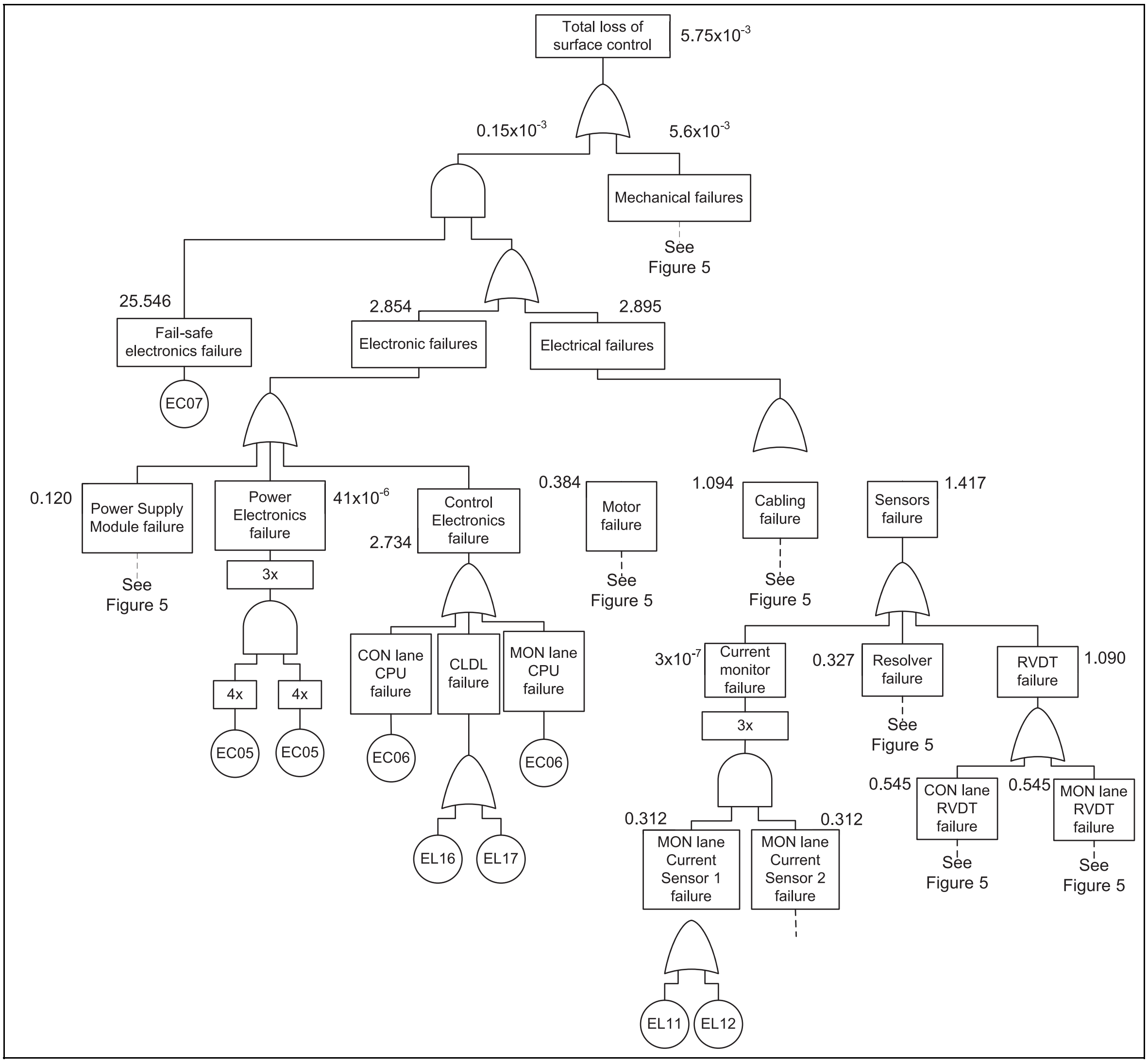


Figure 7. FTA related to the total loss of the self-monitoring EMAS (failure rates $\times 10^{-6}$ pFH).

Conclusion

The architectural design of a fault-tolerant EMAS for MALE UAV's is discussed. Starting from a survey on available airworthiness certification references in case of flight on non-segregated airspace, the safety objectives at EMAS level are defined, and a qualitative CA is performed on a simplex EMAS, to identify the fault modes and causes and to classify their probability of occurrence and severity level. The proposed architecture overcomes the safety concerns of the simplex solution by using redundant components managed by a health-monitoring electronics. The EMAS actually includes two independent computing sections, implementing monitor and closed-loop control functions, and a phase-isolating power electronics. Thus, the actuator has three operating modes: *normal, fail-operative* (in which the EMAS is capable of operating with two out of three motor coils) and *fail-safe* (in which the motor phases are shorted and the regenerated currents create a damping torque on the control surface). To verify the effectiveness of the architectural choices, a quantitative evaluation of the probability of total loss of the surface control is performed via FTA on both the simplex and the self-monitoring solutions. The analysis highlights that the failure rate of the simplex solution (8.828×10^{-6} pFH) is inadequate for the application due to the high failure probability of the electronic and electrical sections. On the other hand, the proposed self-monitoring solution demonstrates to be safety compliant with a failure rate (5.75×10^{-9} pFH) that is essentially driven by the mechanical failures.

Acknowledgements

The authors wish to thank Dr Paolo Serena Guinzio and Dr Germana Vinelli of Alenia Aermacchi for their support to the activity.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research developed in this article was financially supported by Alenia Aermacchi (Research Contract no. 11-0426, 6th September 2011).

References

1. Howse M. All electric aircraft. *IEE Power Engineer* 2003; 17: 35–37.
2. Botten SL, Whitley CR and King AD. Flight control actuation technology for next-generation all-electric aircraft. *Technol Rev J* 2000; 8: 55–68.
3. Rosero JA, Ortega JA, Aldabas E, et al. Moving towards a more electric aircraft. *IEEE Aero El Sys Mag* 2007; 22: 3–9.
4. Navarro R. *Performance of an electro-hydrostatic actuator on the F-18 systems research aircraft*. NASA/TM-97-206224, October, 1997. Edwards, CA: Dryden Flight Research Center.
5. Di Rito G, Galatolo R and Denti E. Object-oriented modelling of flight control actuation systems for power absorption assessment. In: *Proceedings of the 27th congress of the International Council of Aeronautical Sciences (ICAS)*, Nice, 19–24 September 2010, http://www.proceedings.com/09889.html
6. Balaban E, Bansal P, Stoelting P, et al. A diagnostic approach for electro-mechanical actuators in aerospace systems. In: *Proceedings of the 2009 IEEE aerospace conference*, Big Sky, MT, 7–14 March 2009, pp.1–13. New York: IEEE.
7. Garcia A, Cusidò I, Rosero JA, et al. Reliable electromechanical actuators in aircraft. *IEEE Aero El Sys Mag* 2008; 23: 19–25.
8. Mentjes F. Electrically driven general systems for UAV's. In: *UAV design processes/design criteria for structures*. Meeting Proceedings RTO-MP-AVT-145, Paper 3.1, Florence, 15–16 April 2007, pp.3.1-1–3.1-10. Neuilly-sur-Seine, France: RTO.
9. Fawaz YA. Fundamental design concepts in multi-lane smart electromechanical actuators. *Smart Mater Struct* 2005; 14: 1227–1238.
10. Arriola D and Thielecke F. Design of fault-tolerant control functions for a primary flight control system with electromechanical actuators. In: *Proceedings of the international conference AUTOTESTCON 2015*, National Harbor, MD, 2–5 November 2015, pp.393–402. New York: IEEE.
11. Rottach M, Gerada C and Wheeler PW. Design optimisation of a fault-tolerant PM motor drive for an aerospace actuation application. In: *Proceedings of 7th IET international conference on power electronics, machines and drives*, Manchester, 8–10 April 2014. New York: IEEE.
12. Brown D, Georgoulas G, Bae H, et al. Particle filter based anomaly detection for aircraft actuator systems. In: *Proceedings of the 2009 IEEE aerospace conference*, Big Sky, MT, 7–14 March 2009, pp.1–13. New York: IEEE.
13. Ossmann D and Van der Linden FLJ. Advanced sensor fault detection and isolation for electro-mechanical flight actuators. In: *Proceedings of the NASA/ESA conference on adaptive hardware and systems*, Montreal, QC, Canada, 15–18 June 2015, pp.1–8. New York: IEEE.
14. Cao Y, Wang J, Xie R, et al. Fault tree analysis of electro-mechanical actuators. In: *Proceedings of the 34th Chinese control conference*, Hangzhou, China, 28–30 July 2015, pp.6392–6396. New York: IEEE.
15. Bennouna O and Langlois N. Development of a fault tolerant control for aircraft electromechanical actuators. In: *Proceedings of the conference on electrical systems for aircraft, railway and ship propulsion (ESARS)*, Bologna, 16–18 October 2012, pp.83–87. New York: IEEE.
16. Wang N and Zhou Y. Research on reliability of a hybrid three-redundant electro-mechanical actuator. In: *Proceedings of the international conference on mechatronics and automation*, Changchun, China, 9–12 August 2009, pp.1066–1070. New York: IEEE.
17. STANAG 4671:2009. Standardization agreement – unmanned aerial vehicles systems airworthiness requirements (USAR): NATO standardization agency (Edition 1).
18. AER(EP)-P.6. *Istruzioni per la compilazione dei capitolati tecnici per aeromobili militari*. Roma: Ministero della Difesa – Direzione Generale degli Armamenti Aeronautici.
19. O'Connor PDT. *Practical reliability engineering*. 2nd ed. New York: John Wiley & Sons, 1985.
20. *Reliability prediction of electronic equipment*. MIL-HDBK-217F Notice 2, 28 February 1995. Washington, DC: US Department of Defense.
21. *Reliability prediction MIL-HBK 217F subsidiary specification*. ANSI/VITA 51.1-2008 (R2013), 16 October 2013. Washington, DC: American National Standards Institute.
22. *Electronic reliability design handbook*. MIL-HDBK-338B, 1 October 1998. Washington, DC: US Department of Defense.
23. *Non-electronic parts reliability data (NPRD-2011)*. Washington, DC: Reliability Information Analysis Center (RiAC), US Department of Defense (RiAC Automated Databook software).