Eksploatacja i Niezawodnosc – Maintenance and Reliability
Volume 23 (2021), Issue 1
journal homepage: http://www.ein.org.pl

Article citation info:
Hlinka J, Kostial R, Horpatzka M. Application of enhanced methods for safety assessment of FADEC. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2021; 23 (1): 63–73, http://dx.doi.org/10.17531/ein.2021.1.7.

Indexed by:
Web of Science Group

Application of enhanced methods for safety assessment of FADEC

Jiri Hlinka[a], Rostislav Kostial[a] , Michaela Horpatzka[a]

[a]Institute of Aerospace Engineering, Brno University of Technology, Technicka 2896/2 616 69 Brno Czech Republic

Highlights

- Safety assessment for FADECs in early development phases.
- A unified concept of criticality levels respecting FADEC use in different types of aircraft.
- Combination of Item and Functional FMEA used to reduce time-effort for safety assessment.
- New failure effect classification used to link effects to different aircraft categories.

Abstract

The paper deals with safety and reliability assessment as an integral part of the development process for modern aviation products with potentially critical functions. Focus is on digital engine control units, their development process and tools offering potential savings in otherwise time demanding and expensive safety assessment processes. The paper shows application of several approaches, which together form an innovative way for safety assessment of aerospace products (otherwise strictly limited by regulation procedures). It is focused on practical ways towards reduction of development costs during safety assessment, which do not compromise its comprehensiveness. Described approaches are based on experience from development of numerous aerospace products in last nearly 20 years. As an addition, possibility to further enhance the proposed innovative effect classification by application of FMECA was shown. Possible methods for quantitative assessment using Fuzzy logic and/or multiple-criteria decision analysis were discussed.

Keywords

Full Authority Digital Engine Control (FADEC), aircraft, safety assessment, reliability.

1. Introduction

Recent fast development in digital technologies in many fields enables replacement of "old-fashioned" analogue or even mechanical control systems by state of the art digital control solutions with many advantages. In aerospace, this process was slowed-down by the fact that replacement of control functions which are safety critical is a demanding and expensive process. Therefore, some aerospace applications still use abovementioned obsolete technologies. Especially in the area of small aircraft with limited resources for development and certification, this issue prevents faster development.

To tackle this issue, new effective approaches need to be developed. The paper deals with research of new approaches to effectively develop complex electronic systems for general aviation aircraft, in particular to ensure effective safety assessment for FADEC (Full Authority Digital Engine Control) under development.

2. Full Authority Digital Engine Control in General Aviation

Full authority digital engine control has been in wider use for large transport aircraft since the 1980´s. Existing FADECs for large transport or military aircraft have a relatively "narrow" definition of application. In contrary, FADEC considered in this paper is for the general aviation field, where the range of applications can be wide. At the same time, limited resources for development of new solutions in general aviation caused that FADEC technology is still not present in many engine types in current service.

General aviation category includes a variety of applications from small aircraft used for fun flying, through agricultural aircraft, up to aircraft used for transport of passengers. These applications may significantly differ with size/design of the aircraft (and requirements on safety), but also with type of flights performed by particular aircraft.

Although being initially designed for turbine engines, recently FADEC becomes increasingly popular for use among smaller aircraft with piston engines as well.

In this area, manufacturers of piston engines like Continental and Lycoming are increasingly using this technology for their engines. Lycoming uses its iE2 FADEC technology (TO-450, TIO-540-NXT, TSIO-550, TEO-540-A1A engines). Continental uses its PowerLink FADEC (IO-240, IO-360, IO-550, IOF-240, IOF-550, TSIOF-550 engines). Main advantages of FADEC in this area include simplicity of the engine control (pilot can focus more on situational awareness and less on the aircraft control), better diagnostics of problems, and improved performance and efficiency. Similar attention is given to FADECs for diesel reciprocating engines for aviation use. As claimed by Cox [12], prices of FADECs for this application were between $2500 and $7500.

E-mail addresses: J. Hlinka - hlinka@fme.vutbr.cz, R. Kostial - kostial@fme.vutbr.cz, M. Horpatzka - michaela.horpatzka@vutbr.cz

Also today´s small turbine engines in general aviation are often equipped with FADEC in all or some configuration options. As an example, Rolls-Royce M250 turboshaft engine developed from Allison Model 250 (produced and continuously improved from the 1960s) features dual-channel FADEC in the latest series. The engine is used for example in MD 530F from 2016 or in Bell 407GXi from 2018 [26].

Pratt and Whitney has two variants of PT6 engine with electronic control. PT6C is a medium-class helicopter turboshaft engine with dual-channel FADEC with hydro-mechanical backup, used in AW139 [30]. The latest PT6E offers a dual-channel integrated electronic propeller and the engine control system also with single-lever power control. Single-lever power control (for both engine and propeller) reduces pilot workload. In 2019 PT6E was announced as the power plant for Pilatus PC-12 NGX [29].

Czech company PBS Velka Bites developed small turbine engines. FADEC is a standard equipment of models TJ100 and TJ150. Model TJ100 is aimed at light sport aircraft, gliders, UAVs and micro jets, while bigger TJ150 was designed directly for unmanned applications [1].

The paper deals with FADEC for small turbine engines for general aviation. All works are part of a wider research project done in cooperation with UNIS company. Research is dedicated to advanced technology of modular control and diagnostics systems for small turbine engines with thrust around 1500 N and small turboprop engines with power around 180kW. Such engine size has a wide range of aircraft applications and flight profiles. This may include for example UAS (unmanned aerial systems), small sport aircraft (2 or 4 seaters), or auxiliary power for gliders, see Tab. 1. Each application has specific performance demands, engine operation duration, or frequency of power level changes.

3. System Safety Assessment Process in Aerospace

Although safety assessment is an integral part of design and certification of new equipment for aerospace use, current common methods have significant space for improvement. Regulation requirements (both FAA 14 CFR, and EASA CS) prescribe during development/design safety assessment combination of standard methods like FHA (Functional Hazard Assessment), FMEA/FMECA (Failure Modes, Effects/and Criticality Analysis), FTA (Fault Tree Analysis), RBD (Reliability Block Diagrams). Recommended practices for aerospace are summarized in SAE APR 4761 [14]. Critical review of prediction techniques is the subject of several papers, for example [27], [35]. However, for the development of complex product, like FADEC, also new sophisticated methods can be applied.

FHA is a systematic, comprehensive

examination of functions to identify and classify conditions of those functions according to their severity [14]. FHA is usually used as a preliminary analysis during the early design phase, when exact components of the system are not yet known. Since it evaluates functions of the system and effects of their loss, it helps to find critical systems/parts already in early design phases.

FMEA is a qualitative method of analysis that involves the study of possible failure modes and faults in sub items, and their effects at various indenture levels [17]. For aerospace use it provides a systematic, bottom up method of identifying the failure modes of systems, components or functions and determining the effect on the aircraft. It is a key method to prove the requirement "no catastrophic event should result from the failure of a single component". Typically is used Functional or Item (Piece parts) FMEA [14].

Both FHA and FMEA are qualitative assessment methods. For quantitative assessment are used FTA, RBD or Markov analysis. These are top-down methods which proceed down through more detailed levels of design. After qualitative analysis, when failure condi-

Table 1. Possible range of use for general aviation FADEC (intended use and limitations)

Auxiliary Propulsion	
Single Engine Aircraft **Glider**	a) Engine is not used for **critical phases** of flight (take off, landing etc.) b) Electrical power is not generated by engine. Independent source (battery) is used. c) Independent fuel cut offs. d) Regulation **CS-22 +CRI + CS-23, CS-E**
Primary Propulsion	
Single Engine Aircraft	a) Electrical power backup (batteries) for at least 30 minutes flight in case of generator failure. b) Independent fuel cut offs. c) Aircraft without anti-icing system are limited to IMC without icing. d) Regulation **CS-23, CS-E** (CS-VLA, CS-LSA, L-2)
Multi Engine Aircraft	a) Electrical power backup (batteries) for at least 30 minutes flight in case of generators failure. b) Independent fuel cut offs. c) Each engine is controlled by independent own FADEC unit. d) Aircraft without anti-icing system are limited to IMC without icing. e) Regulation **CS-23, CS-E**
UAV/UAS Primary Propulsion	
Single Engine Aircraft	a) Electrical power backup (batteries) for at least 30 minutes flight in case of generator failure (including remote control, and communication with operator.) b) Independent remotely controlled fuel cut offs. c) Aircraft without anti-icing system are limited to IMC without icing. d) Regulation **STANAG 4671, CS-LUAS**
Multi Engine Aircraft	a) Electrical power backup (batteries) for at least 30 minutes flight in case of generators failure (including remote control, and communication with operator.) b) Independent remotely controlled fuel cut offs. c) Each engine is controlled by independent own FADEC unit. d) Aircraft without anti-icing system are limited to IMC without icing. e) Regulation **STANAG 4671, CS-LUAS**

tions are identified, quantitative analysis can be applied to find what single failure or combinations of failures exist at lower levels that might cause each failure condition [14].

In addition, for software development in the aerospace industry, recommendations of RTCA DO-178 [11] are applied. More information on safety assessment of software for aerospace use can be found in a number of papers. For example, in [33] is an overview of the RTCA DO-178C and its impacts on Certification of Safety-Critical avionic systems. Another overview and certification of the safety critical computer systems using RTCA DO-178 is presented in [19]. More practical use of RTCA DO-178 for condition monitoring system is presented in [13].

Although new progressive methods offering some advantages can be found in several research works (for example [20]), aerospace industry relies on above-described well proven methods which are also established in aerospace regulation requirements. Therefore, the work presented in the paper is based on FHA and FMEA. In addition, the paper focuses on new ways to reduce time effort and costs for safety assessment using these methods, which are acceptable for the aerospace certification process. In fact, modifications proposed in the paper are so extensive, that they form an innovative approach to both FHA and FMEA which was not to such extent applied in aviation before. For example, presented enhanced FHA uses a totally new definition of criticality levels allowing rapid application of results on different aircraft classes (with different applications and failure effects). Proposed hybrid FMEA approach (although may be seen in similar applications for other industrial sectors), in this paper is interlinked to classification from enhanced FHA (for greater flexibility for different aircraft types), and optimized for aerospace application (respecting its typical segmentation/functional zoning). Since the aerospace industry is facing escalation of development costs with every new aircraft generation (additional development costs related to more strict requirements and more complex systems), reduction of effort and costs in every aspect of the development process is extremely important.

3.1. System Safety Assessment of FADEC

For safety assessments of FADEC are usually used methods, which allow simulation - for example Markov analysis (Markov chains) which was used for prototypes of FADEC for JAS 39 Gripen [15], or where the Markov process [24] and Monte Carlo simulation [25] based time limited dispatch analysis for FADEC was used. Another option is an analysis based on Bayesian networks. Research [21] used improved BN analysis for commercial aircrafts FADEC. Simulations require detailed model of the FADEC system and thus are suitable for later design phases, where the system structure is mostly established and it is assumed there will be no more major changes. Since the detailed modelling of complex systems is time consuming, there are efforts to simplify these models or methods [9].

However in the described case, the assessment was done for the FADEC in pre-prototype and prototype phase of development, where many parts were subject to change. Therefore putting an effort into creation of a detailed system model was impractical.

To adapt to early design conditions, adjustment was done to the traditional safety assessment methods especially FHA and FMEA to minimize the need to rework analysis every time the change occurs. For quantitative analysis FTA (Fault Tree Analysis) was used, which is not described in detail in the paper since its standard form described in SAE ARP 4761 [14] was used. The use of FTA in combination with Markov analysis for FADEC reliability assessment is described in detail in [22] for example. System safety for FADEC from a software perspective was addressed in [28].

4. Enhanced safety assessment concept for complex electronic systems

Current general safety assessment process for aviation in a simple form is shown on Fig. 1. This scheme was derived from recommendations of EASA CS AMC 25.1309 (Acceptable Means of Compliance) System design and analysis [3].

The team of authors was from the beginning facing strict submission of FADEC with a wide range of use, see Tab. 1. Similar needs can be expected for different engine control units producers in a given power range. To enable efficient and precise safety assessment of such complex electronic system, some new techniques were adopted.

These include:

- Functions criticality level analysis – a unified concept of criticality levels respecting FADEC use in different types of aircraft, see chapter 4.1;
- Enhanced FHA – used to identify critical functions of FADEC, see chapter 4.2;
- Hybrid Block FMEA – used to reduce time-effort for safety assessment, see chapter 4.3;
- Two-phase failure effect classification – used to link FADEC failure effects to different aircraft categories (applications), see chapter 4.3.1.

These techniques can be applied on any complex electronic system (in general). For aviation, in addition, all safety assessment techniques must comply with main airworthiness requirements for aircraft design and certification, typically EASA CS-23 [7] or FAA 14 CFR Part 23 [2] (for aircraft with fixed wing and propulsion unit), EASA CS-22 [6] (for gliders with auxiliary power unit), or other similar requirements. Depending on the country of origin, also Chinese or Russian equivalent airworthiness requirements can be applied. However, most of the regulation requirements link to the same industrial standards and practices. For example, CS-23 and 14 CFR Part 23 requirements link to safety assessment procedures described in ASTM F3230-17 [31]. Detailed guidelines for safety assessment including a list of assessment methods are also available in SAE ARP 4761 [14]. A list of basic assessment methods is shortly mentioned in chapter 3, further information on safety assessment procedures is for example in [26]. The paper is focused on practical ways towards reduction of develop-

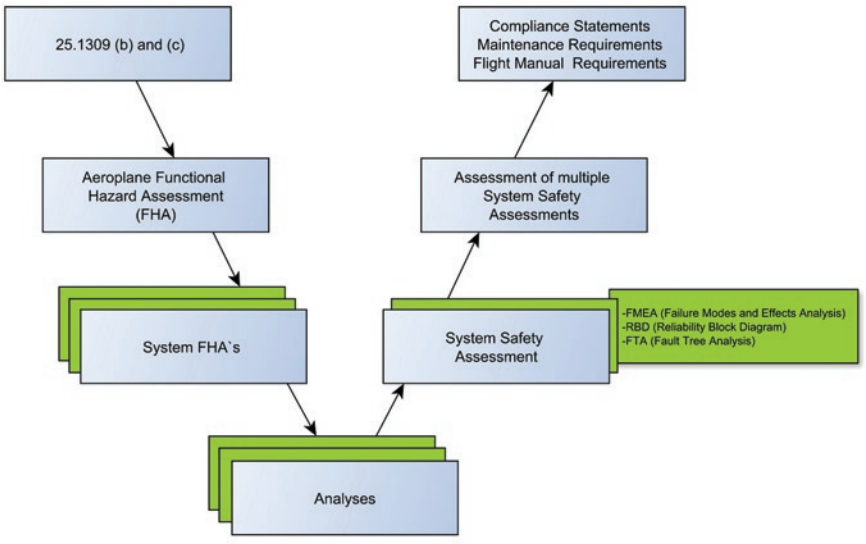

Fig. 1. Current general safety assessment process for aviation

Table 2. Functions criticality level

Functions Criticality level	Description
Essential	Functionality of particular part of the system or the system itself is directly influenced by a function behaviour. It essentially provides intended function of the system or part of the system (Thrust control, fuel flow control etc.)
Moderate	The function indirectly influences essential functions. However, moderate function does not provide intended function itself (Overspeed protection, Turbine temperatures, Oil pressure etc.).
Marginal	Functions that supports essential or moderate functions in the proposed envelope.
Insignificant	Functions without influence on essential or moderate functions.

ment costs during safety assessment, which do not compromise its comprehensiveness.

4.1. Functions Criticality Level Analysis

As can be seen from Tab. 1, FADEC for general aviation engine can perform a wide variety of missions. In addition, it can also have a wide range of critical functions, i.e. engine control, electric power generation control, etc. Therefore, it is necessary to decompose all FADEC functions and link them to categories. New applied method divides all FADEC functions into four categories, see Tab. 2. These functions are linked to Enhanced FHA analysis and complement the Failure Classification.

4.2. Enhanced FHA

Every FADEC function is analysed using FHA (Functional Hazard Assessment). The main goal of FHA results is to provide a list of potentially risky functions (and shortcomings), which should be further analysed, and/or corrective action should be taken (design change, added redundancy, etc.). Standard FHA is generally used for one specific application. This may be a problem if intended use of the product is for different specifications (CS-22, CS-23) or applications (manned/ unmanned). Enhanced FHA uniquely solved this problem, since it was developed to effectively cover all intended applications of analysed product. Enhanced FHA shown in Fig. 2 for the first time ever identifies effects for all FADEC applications in the single table.

According to aviation regulation requirements, all functions with HAZARDOUS or CATASTROPHIC consequences have to be further analysed using a prescribed set of analysis methods. Also functions from categories ESSENTIAL or MODERATE (according to Tab. 2) should have detailed safety assessment. These steps were done as normal engineering procedure out of the scope of the paper.

See chapter 5.2 for more details on example FADEC results.

4.3. Hybrid Block FMEA

Classic safety assessment process defined in SAE ARP4761 recognizes Part FMEA or Functional FMEA. Since developed FADEC was a complex electronic device, with a significant number of electronic parts, standard part FMEA would be time consuming. On the other hand, functional FMEA would not respect fully hardware "block composition" of FADEC. Therefore, "hybrid FMEA" was proposed and applied, combining advantages of both, part and functional FMEA. Goal of the application of hybrid method was to reduce the number of analysed components, and ability to quickly integrate design changes into safety assessment.

Decomposition of analysed FADEC led to functional blocks. Each block is a set of components performing defined functions. Two block types can be recognized:

- Simple block – performs single function (i.e. temperature measurement, el. current filtration, …)

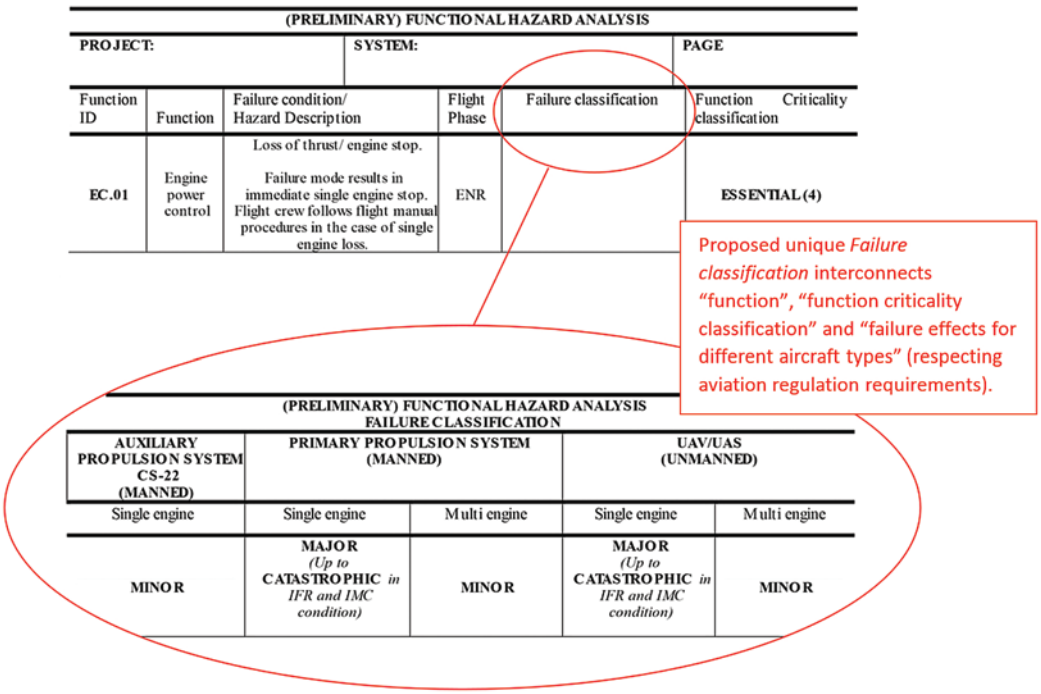

Fig. 2. Example FHA applied on the FADEC

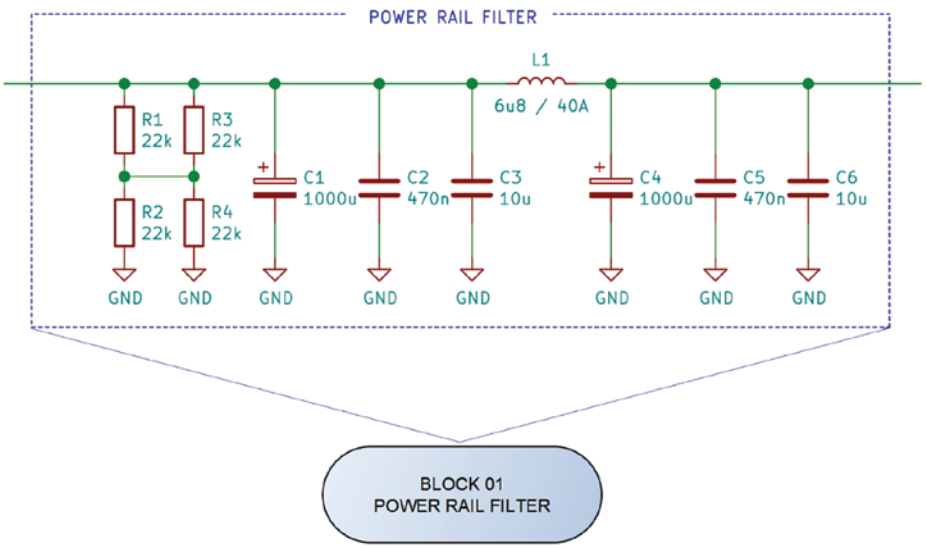

Fig. 3. Example of simple filter block for el. energy filtration

- Node block – performs more than one function (i.e. MCU-Micro Controller Unit with sensors data processing and fuel flow control).

Each function must be analysed in FMEA for Node blocks. Fig. 3 shows an example of a functional block (composed of filters in the circuit of integrated electric power generator) which consist of capacitors (C1, C2 etc.) resistors (R1, R2 etc.) and coils (L1) with connections to ground (GND).

4.3.1. Two-phase failure effect classification for FMEA

Same failures can have different effects on different aircraft types/ categories. Shown methodology takes this fact into account, it has two-phase process.

Phase One: Failure effect classification on a system level

Phase one classifies failure effects on FADEC system itself. Every safety assessment classification is done just for FADEC system, no effect on aircraft or engine is considered. Goal of the Phase One is to predict critical elements of FADEC (without link to particular application). Therefore, different assessment classification is used compared to aviation standards [3], see Tab. 3.

Phase Two: Failure effect classification on an airplane level

Based on previous long-time experience with safety assessment of different types of engine control systems, we can state that failures of engine control system components can lead only to a limited number of failure effects on the airplane level. Tab. 4 demonstrates several different MCU (Main Control Unit) failures with the same effect on the aircraft.

Above mentioned failure effects are summarized and classified for different aircraft. An example of "Hybrid Block FMEA" with two-phase failure effect classification is shown on Tab. 5 and Tab. 6.

4.4. Extension to Hybrid Block FMECA

To further enhance proposed innovative effect classification, it is possible to use FMECA (Failure Modes, Effects and Criticality Analysis) instead of FMEA. This will move proposed solution towards quantitative assessment, adding also criticality level (for example in the form of CN – Criticality number). Authors did consider this extension for future enhancement of the presented method. Many models for criticality definition exist, including models based on risk matrix,

Table 3. FADEC system criticality level

FADEC Criticality Level	Description
Safety - Critical	Failures which directly affect the system ability to perform primary and/ or essential functions. System can no longer perform its primary functions. Emergency shutdown or switch to backup system required.
Serious	Failures which directly affect the system ability to perform primary and/ or essential functions. System is able perform its primary functions for limited amount of time, before shutdown or switching to backup system.
Degraded	Failures which can affect performance of the system. Primary functions are preserved with limited performance for an unlimited time.
Not Critical	Failures without an effect on primary or essential functions.

Table 4. Example of different failures with same effects on aircraft

BLOCk/ Failure Effect	Effect on System	Effect on Aircraft / Failure Class
Power Rail Filter/ Short	In case of a failure, ECU (Electronic Control Unit) overvoltage protection is activated. In worst case scenario, ECU is switched-off and back-up system is used for engine control. Crew has visual indication on activation of back-up system.	Airplane continues in flight using back-up system for engine control. Some features are deactivated, i.e. overspeed protection, automatic engine start, etc. ECU cannot be re-activated during flight. Failure Class: **FAILURE.2**
Control Microprocessor/ Analog to Digital Converter failure	In case of a failure, analogue segment of MCU (Microprocessor) and analogue inputs fail, resulting in ECU emergency shut down and use of back-up system for engine control. Crew has visual indication on activation of back-up system.	
Overspeed Protection/ Loss of Sensing	In case of a failure, MCU has no information on turbine rpm. This results in ECU emergency shut down and use of back-up system for engine control. Crew has visual indication on activation of back-up system. Crew is able to monitor turbine rpm using on-board instruments (indication is independent on overspeed protection).	

Table 5. Example of FMEA format

Failure mode and effect analysis (FMEA)							
Project:	**System:**	**NO. DW:**		**Page:**			
Block ID	Function	Failure Mode	Failure description	Failure effects			Note
				Flight phase **See. Table 7**	Effects on system	Effects on aircraft	
Block 1	Power-Rail filter provides el. filtration and connectivity to aircraft on-board electrical grid.	Short circuit	Short circuit on one or more of the block items.	APR	In case of a failure, ECU overvoltage protection is activated. In worst case scenario, ECU is switched-off and back-up system is used for engine control. **CLASS: Critical**	In case of failure, the aircraft continue in flight on back-up system. Some functions are deactivated (overspeed protection, automated start etc.). ECU cannot be reactivated during the flight. **CLASS: Failure.02**	-

Table 6. List of failures and classification on aircraft

List of failures - Failure mode and effect analysis (FMEA)			
Project:	**System:**	**Failure No.:** FAILURE.01	**FAILURE DESCRIPTION:** In case of failure, the engine losses thrust due to the emergency shutdown. **Change in aircraft behaviour Master warning – red light and sound (except: jet engine glider)**
Plane Category	Flight phase **See. Table 7**	Failure Classification	Note
Jet engine Glider	**STD**	-	-
	TOF, APR, ICL, LND	-	Engine is not used for critical phases of flight
	ENR	Max. **MINOR**	Failure can limit the flight range or lead to controlled landing to the terrain.
Ultralight plane (Max. 400 kg)	**STD (START)**	-	-
	TOF, APR, ICL, LND	**MAJOR**	Flight crew follows flight emergency procedures for loss of thrust. Forced emergency landing. .
	ENR	**MINOR**	Flight crew follows flight emergency procedures for loss of thrust. Can lead to emergency landing to the terrain.
Single engine CS-23 plane (Max. 8618 kg)	**STD**	-	-
	TOF, APR, ICL, LND	**HAZARDOUS** to **CATASTROPHIC**	Potentially leads to the catastrophic result in the case of improper (or limit) take off, initial climb, approach and landing. Extensive crew workload (in limited time) could impair ability to perform task.
	ENR	**MAJOR** to **CATASTROPHIC**	Failure mode results in forced emergency landing according to the flight manual emergency procedures. It potentially leads to the catastrophic results in IMC conditions.
Multi engine CS-23 plane (Max. 8618 kg)	**STD (START)**	-	-
	TOF, APR, ICL, LND	**MAJOR** to **HAZARDOUS**	Failure mode results in immediate single engine stop and significant crew workload. Flight crew follows flight manual procedures in the case of single engine loss. Flight crew uses fully functional engine and flight controls to eliminate negative effects of loss of engine control. Potentially hazardous condition in case of inappropriate reaction to asymmetrical thrust.
	ENR	**MINOR**	Failure mode results in immediate single engine stop. Flight crew follows flight manual procedures in the case of single engine loss.

Table 7. ICAO flight phases [10]

ICAO FLIGHT PHASES		
Phase	**Abbreviation**	**Description**
STANDING	**STD**	Prior to pushback or taxi, or after arrival, at the gate, ramp, or parking area, while the aircraft is stationary.
TAXI	**TXI**	The aircraft is moving on the aerodrome surface under its own power prior to take off or after landing.
TAKEOFF	**TOF**	From the application of take off power, through rotation and to an altitude of 35 feet above runway elevation.
INITIAL CLIMB	**ICL**	From the end of the Take-off sub-phase to the first prescribed power reduction, or until reaching 1,000 feet above runway elevation or the VFR pattern, whichever comes first.
EN ROUTE	**ENR**	Instrument Flight Rules (IFR): From completion of Initial Climb through cruise altitude and completion of controlled descent to the Initial Approach Fix (IAF). Visual Flight Rules (VFR): From completion of Initial Climb through cruise and controlled descent to the VFR pattern altitude or 1,000 feet above runway elevation, whichever comes first
MANEUVERING	**MNV**	Low altitude/aerobatic flight operations.
APPROACH	**APR**	Instrument Flight Rules (IFR): From the Initial Approach Fix (IAF) to the beginning of the landing flare. Visual Flight Rules (VFR): From the point of VFR pattern entry, or 1,000 feet above the runway elevation, to the beginning of the landing flare.
LANDING	**LDG**	From the beginning of the landing flare until aircraft exits the landing runway, comes to a stop on the runway, or when power is applied for take off in the case of a touch-and-go landing.
EMERGENCY DESCENT	**EMG**	A controlled descent during any airborne phase in response to a perceived emergency situation.
UNCONTROLED DESCENT	**UND**	A descent during any airborne phase in which the aircraft does not sustain controlled flight.

which are most widely used in aerospace. Several selected models for CN definition are listed below.

4.4.1. CN based on criticality factors ([16])

$$C_{KR} = \{\pi_1, \pi_2, \pi_3 \ldots \pi_N\}^{\frac{1}{N}} \tag{1}$$

where factors $\pi_{(1\ldots N)}$ are weighting factors that express influences on failure effects. These factors can for example represent influence of:

- failure classes,
- effect of the part failure on the system,
- failure probability of one part in a set of all analysed parts,
- ease of failure detection,
- speed of response on failure.

All these factors are based on expert judgement which leads to certain subjectivity of assessment. Therefore this method is suitable primarily for assessments, where there is no reliable source of information on failure probability.

4.4.2. CN defined using generic base failure rate with influencing factors ([16])

$$C_{KRi} = \sum_{1}^{N} \left(\beta \cdot \alpha \cdot K_E \cdot K_A \cdot \lambda_G \cdot t \cdot 10^6 \right)_i \tag{2}$$

where:

- C_{KRi} criticality factor of the part,
- i ID number of the part,
- N total number of parts,
- β conditional probability that the failure will lead to a critical failure of the system,
- α relative ratio between failure rate of the given type to total failure rate for given part,
- λ_G failure rate of a part with influence of all possible failure modes. The usual form is: failure rate/10^6,
- t operating time that each part accumulates during whole operating time of the system,
- K_E corrective factor, incorporates effects of different operating conditions against conditions, for which was λ_G determined,
- K_A corrective factor, incorporates effects of different operating loads against loads, for which was λ_G determined.

Failure mode (modal) criticality number ([32])

$$C_m = \left(\beta \cdot \alpha \cdot \lambda_p \cdot t \right) \tag{3}$$

where:

- C_m Failure mode criticality number
- β Conditional probability of the current failure mode's failure effect
- α Failure mode ratio
- λ_p Item failure rate
- t duration of applicable mission phase (expressed in hours or operating cycles)

4.4.4. Risk priority number (RPN) method in FMECA

RPN method reviews the risk level of failure modes using assessment of *probability of failure mode occurrence* (O), *effects severity* (S) and the *probability of detecting the failure* (D). It ranks O,S and D on 1 – 10 [34]. Risk assessment is calculated by multiplying the ranking values of O, S and D [5].

Although in aerospace mode occurrence (O) can usually be defined with high degree of confidence (thanks to the previous experience and operational data), effects severity (S) and probability of detecting the failure (D) may sometimes involve high degree of subjective judge-

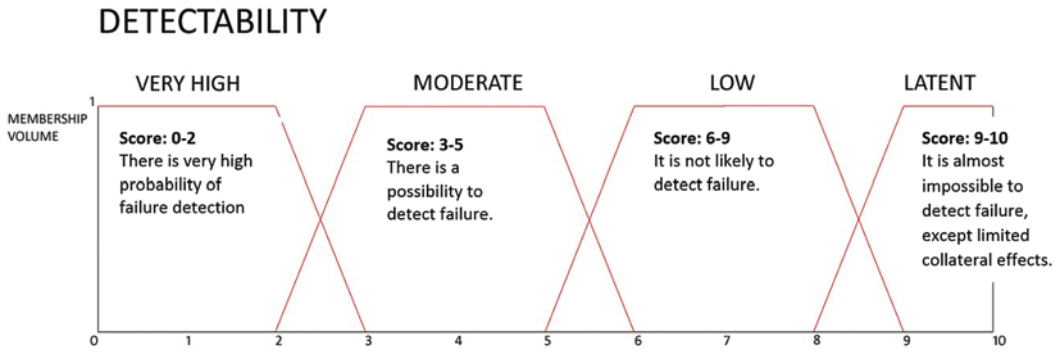

Fig. 4. Fuzzy membership function for liguistic variable- detecablity [18]

Table 8. Detectability scoring table, ref. [18] with highlighted capacitor C1 failure modes (green – short, blue – value change, red – open)

	Direct detectability *(indication)*			**Indirect detectability** *(results of non-function)*			**Pre- flight inspection/ procedures**		**Score**	
Direct detectability: *Failure is indicated. Flight crew is able to respond to the failure effects and proceed according to the flight manual*	**YES** *(multiple levels)*	**YES** *(single level)*	**NO**	**YES**	**Partially**	**NO**	**YES**	**NO**		
Indirect detectability: *Failure is indirectly indicated to the crew by its collateral effects. Flight crew is able to identify occurring failure without significant workload.*	x			x			x		1	HIGH
		x		x			x		2	
		x			x		x		3	
		x			x			x	4	
		x				x	x		5	
			x	x			x		6	
Pre-flight inspection test: Item malfunction is possible to detect during pre- flight test, according to the flight manual.			x		x		x		7	
			x			x	x		8	
			x		x			x	9	
			x			x		x	10	LATENT

ment. To reduce this significant shortage, which is not only linked to RPN method (but also other mentioned methods), Fuzzy logic may further be applied as a supporting tool. This can be especially meaningful in case of probability of detecting the failure (D). An alternative approach on optimization of parameters is for example in [34].

Although a number of papers can be found, where RPM is criticized for some shortcomings, which were summarized by Liu in [23], it is most suitable method for Fuzzy logic application (and reduction of degree of subjective judgement). Most significant shortcomings usually mentioned include RPN values and their varying sensitivity to small changes, or that parameters O, S and D are equally weighted.

Choice of specific criticality analysis method primarily depends on available input information and secondarily on specific conditions and goals of the analysis. For example case described in the paper, most suitable seems to be RPN method, which will be considered in further text. Authors do consider extension of methods presented in Chapter 4 towards partially quantitative assessment using FMECA with application of Fuzzy logic or Multiple-criteria decision analysis. Chapters 4.5 and 4.6 are showing potential of this extension, and should be considered as an introduction to future work.

4.4.5. Fuzzy extended criticality inputs

To evaluate a given item *probability of detecting failure* (D), for example scoring Tab. 8 can be used (based on [18]). Detectability scoring interval is $\langle 0,10 \rangle$. Lower score corresponds with higher probability of failure detection. High score corresponds with lower probability of failure detection resulting in a latent failure. Detectability fuzzy membership is established in Fig. 4. The trapezoidal membership function is used.

Tab. 9 shows an example component from simple filter block shown on Fig. 3. In this case the component is ceramic capacitor C1, and its failure modes detectability. As can be seen, there is no direct possibility to detect any of the three failures modes shown. Short circuit can be detected based on collateral effects (activation of overload protection and automatic switch to HBM mode), and during pre-flight inspection. Change in operational parameters is practically undetectable and latent until more capacitors degrade, or until another failure mode occurs. Open circuit of the capacitor can cause filtration degradation which can influence some of very sensitive parts of the system. The detectability of the failure is very complicated.

Fuzzy interface process

As can be seen in Fig. 5, input values O, S, and D are starting point for Fuzzy inference process. Fuzzy procedures described many times in the literature can be applied. The most used inference technique is Mamdani, developed by Professor Ebrahim Mamdani of London University in 1975. Detailed description of fuzzy inference process is out of the scope of the paper. It uses several process steps, including

Fuzzification, Rule evaluation (using Fuzzy interference rules) and De-fuzzification.

The last step, De-fuzzification, is done in the order to gain the fuzzy process single scalar quantity output. Ranking represents the extended criticality level of the failure mode.

Table 9. Detecability list of C1 capacitor failure modes

DETECABLITY LIST OF C1 CAPACITOR FAILURE MODES		
Short circuit	6	LATENT
Open circuit	9	LATENT
Value Change	10	LATENT

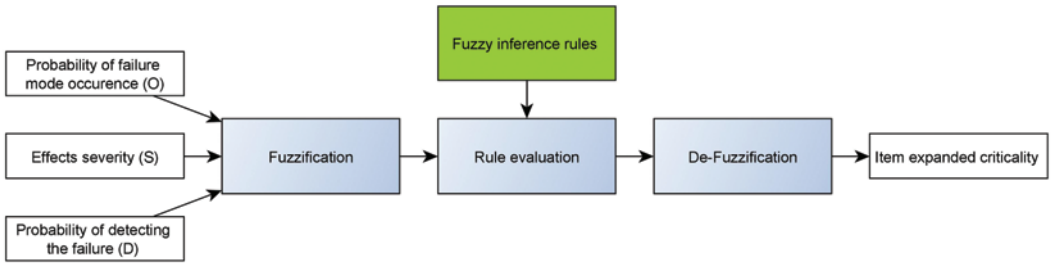

Fig. 5. Fuzzy inference process

The last step, De-fuzzification, is done in the order to gain the fuzzy process single scalar quantity output. Ranking represents the extended criticality level of the failure mode. For De-fuzzification, probably the most used defuzzification technique is centroid technique. It finds where vertical line would slice the aggregate set on final Fuzzy scoring into two equal masses. Mathematically this center of gravity (COG) can be expressed as follow:

$$COG = \frac{\int_a^b \mu_x(x)xdx}{\int_a^b \mu_x(x)dx} \tag{4}$$

where μ_x is membership function on final scoring.

Risk assessment methodology using fuzzification for RPN methodology was discussed in ref. [8]

4.4.6. Multiple-criteria decision analysis

Second method considered for future evaluation of criticality is multiple-criteria decision analysis. If applied during FADEC prototype design, it has an advantage of different weighting for O, S, and D criteria. It also has small sensitivity for changes of non-critical criteria. On the other hand, it is sensitive for changes of critical criteria used for decision making. There was some work which uses multiple-criteria decision before, for example [4], where was used TOPSIS method maritime risk evaluation.

Authors plan to make comprehensive evaluation of both methods on the case of one functional FADEC block. Method with best results will be than recommended for application on whole FADEC.

5. Result and discussion - Enhanced safety assessment concept applied on FADEC

5.1. Analysed system description

All methods described in chapter 4 were applied to the engine digital control unit for small turbine engine with 1500 N thrust and integrated electric generator. Control unit was composed of 4 main modules with the total 1168 components. Control unit general composition is shown on Fig. 6.

5.2. System analysis results

For the particular FADEC system, enhanced FHA was performed (as described in chapter 4.2) for aircraft categories presented in Tab. 1. The goal was to identify effects resulting from the failure of the analysed function. In total 21 functions were defined and analysed covering complete FADEC functionality with respect to higher aircraft levels. In total 6 critical functions were selected for more detailed analysis. In addition, for less critical functions, corrective actions were proposed (often new procedures for flight manual).

System components were divided into functional blocks, complete FADEC was divided into 78 functional blocks. Blocks were analysed using hybrid block FMEA with Failure Effect Classification. Total of

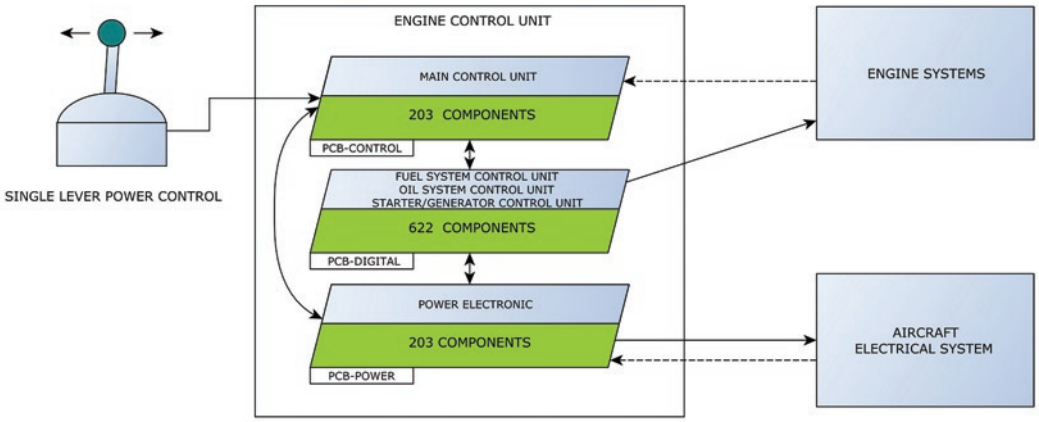

Fig. 6. General composition / scheme of analysed FADEC

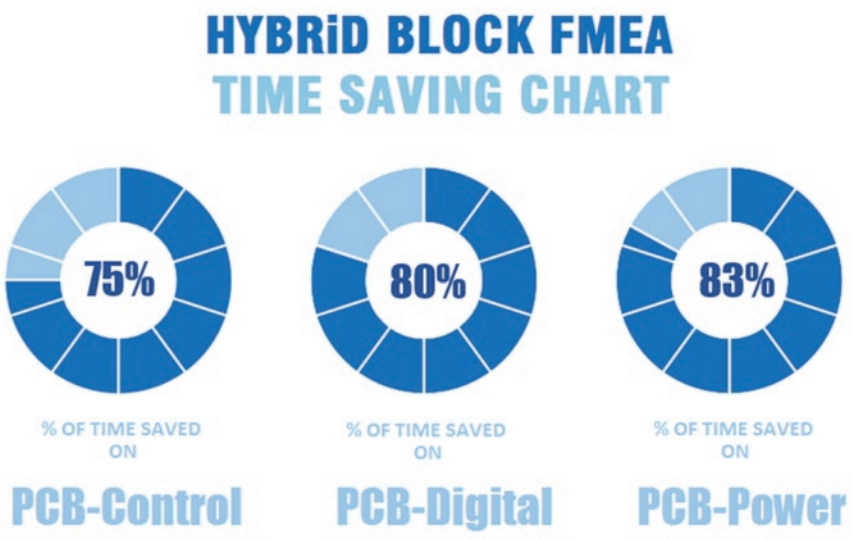

Fig.7. Time savings received by application of presented methods

Table 10. Comparison between part FMEA and Hybrid block FMEA

PCB	Parts	Functional blocks	DuratioN - Hours Part FMEA (10 min per part)	Duration - Hours HYBRiD BLOCK FMEA (30 min per BLOCK)	% of time (Hybrid FMEA/ Part FMEA)
PCB-1	203	**17**	2030 h	**510 h**	**25%**
PCB-2	622	**41**	6220 h	**1230 h**	**20%**
PCB-3	343	**20**	3430 h	**600 h**	**17%**

7 main effects on aircraft level (effects with significant impact on the function of the whole aircraft and safety of flight) were identified.

During the FADEC development countless minor changes were made, such as replacements of some elements, or changes in the power supply or filtration parts of FADEC. Thanks to the use of Enhanced safety assessment and especially the Hybrid block FMEA, it was not necessary to analyse these minor changes at the level of individual components. Only failure rates for the given block were corrected and so the FMEA evaluation did not change.

There were a few major changes during the development which had influence on FADEC functions or number and layout of PCBs (Printed Circuit Boards). These changes had to be revised in Hybrid block FMEA but for blocks affected by design changes only.

If we consider minimum time necessary for single part analysis in part FMEA to be in average 10 min (taking into account great number of repeating parts, which speed-up the assessment process), and compare it with average 30 min for the analysis of a single block in hybrid block FMEA, we can estimate time savings for safety assessment of FADEC like device, see Tab. 10 and Fig 7.

Calculated times are based on long-time experience from aerospace safety assessment process (item analysis time, influence of connection into the system and effects on other system items/elements are considered). The concept of safety assessment has been proven to be suitable for safety assessment in early phases of FADEC development. It can be assumed that methods mentioned in this paper will be suitable for other complex electronic systems.

6. Conclusion

More strict regulation requirements and more complex aircraft systems are the main reason for increasing development costs for recent aerospace projects. Reduction of development effort and costs in every aspect of the development process is therefore extremely important. At the same time, it is not possible to omit any function on the aircraft and its detailed analysis. Unique solutions presented in the paper were strictly driven by a requirement to ensure the same extent of analysed functions as traditional methods, without possibility to omit any important information (i.e, function or component failure). Structure and outputs were continuously compared with previous works on other aviation products. At the same time, developed solutions enable quick adoption of safety assessment on different aircraft types (different FADEC applications) without the need to repeat a complete set of analyses from the beginning for each aircraft type. Thanks to a combination of specially defined function criticality levels with enhanced FHA, any future application in different aircraft category can be quickly analysed without demanding modifications of complete safety assessment.

Enhanced safety assessment done on an example FADEC confirmed, that small design changes inside blocks (with small/no functional effects) do not require comprehensive and time demanding revision of complete safety assessment (as in case of classic Part FMEA application). Small design change applied in this example design was, among others, integration of filtration capacitors. At the same time, reliability of major hardware blocks is available.

Larger design modifications (like change of number of PCBs) require major revision of safety assessment. However, this revision can be easily applied only to modified blocks. Functional blocks proved useful also for later fault tree analysis.

At every moment of performed works, comparison was done to monitor, if new method analyses all functions / component failures like in the case of traditional methods prescribed by regulation requirements, tracking if comprehensiveness and reliability correctness of the process is ensured. There was no evidence of any shortcoming as a result of developed procedures.

As an addition, possibility to further enhance the proposed innovative effect classification by application of FMECA was shown. Possible methods for quantitative assessment using Fuzzy logic and/or

multiple-criteria decision analysis were discussed. Authors do consider this extension for future enhancement of the presented method.

Acknowledgement

Work published in the paper was funded by the Ministry of Industry and Trade of the Czech Republic within the TRIO program, through the research project FV20043 Advanced Technology of Modular Control and Diagnostics Systems for Aircraft Engines.

References

1. Aircraft Engines. Aircraft Engines - PBS. [https://www.pbs.cz/en/our-business/aerospace/aircraftgines].
2. Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes. FAA 14 CFR Part 23
3. AMC 25.1309 System design and analysis. EASA CS-25 Amendment 21. 2018.
4. Başhan V, Demirel H, Gul M. An FMEA-based TOPSIS approach under single valued neutrosophic sets for maritime risk evaluation: the case of ship navigation safety. Soft Comput 2020, https://doi.org/10.1007/s00500-020-05108-y
5. Bluvband Z, Grabov P. Failure Analysis of FMEA. 2009 Annual Reliability and Maintainability Symposium 2009; 344-347, https://doi.org/10.1109/RAMS.2009.4914700.
6. Certification Specification for Sailplanes and Powered Sailplanes. EASA CS-22 Amendment 2, 2009.
7. Certification Specification for Normal-Category Aeroplanes. EASA CS-23 Amendment 5, 2017.
8. Chang K H, Cheng C H. A risk assessment methodology using intuitionistic fuzzy set in FMEA. International Journal of Systems Science 2010; 41; 1457-1471, https://doi.org/10.1080/00207720903353633.
9. Chen B, Li C, Li Y, Wang A. Reliability analysis method of an aircraft engine FADEC system. 8th International Conference on Reliability, Maintainability and Safety 2009; 8: 289-292, https://doi.org/10.1109/ICRMS.2009.5270188.
10. Data Definition Standard - English- Attribute Values. ICAO ECCAIRS Aviation 1.3.0.12. 2013.
11. DO-178C Software Considerations in Airborne Systems and Equipment Certification. RTCA
12. FADEC Comes Of Age. [https://www.planeandpilotmag.com/article/fadec-comes-of-age/?start=1].
13. Gerdes M, Galar D, Scholz D. Decision trees and the effects of feature extraction parameters for robust sensor network design. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2017; 19 (1): 31-42, https://doi.org/10.17531/ein.2017.1.5.
14. Guidelines and methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE ARP 4761, 1996.
15. Hjelmgren K, Svensson S, Hannius O. Reliability analysis of a single-engine aircraft FADEC. International Symposium on Product Quality and Integrity; 1998 Jan 19-22; Anaheim., https://ieeexplore.ieee.org/document/653811/references#references.
16. Holub R, Vintr Z. Spolehlivost letadlove techniky (Dependability of aircraft). Brno University of Technology, electronic textbook, 2001.
17. IEC 60050-192:2015 International Electrotechnical Vocabulary (IEV) - Part 192: Dependability. International Electrotechnical Commission.
18. Janhuba L. The Integrated Method Utilizing Graph Theory and Fuzzy Logic for Safety and Reliability Assessment of Airborne Systems. Brno University of Technology; 2018, https://doi.org/10.13164/conf.read.2018.4.
19. Kornecki A, Zalewski J. Software certification for safety-critical systems: A status report. 2008 International Multiconference on Computer Science and Information Technology Wisia, 2008, https://doi.org/10.1109/IMCSIT.2008.4747314.
20. Li J, Wang Z, Ren Y, Yang D, Lv X. A novel reliability estimation method of multi-state system based on structure learning algorithm. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2020; 22 (1): 170-178, https://doi.org/10.17531/ein.2020.1.20.
21. Li N, Lu Z, Zhou J. Reliability assessment based on Bayesian networks for full authority digital engine control systems. 11th International Conference on Reliability, Maintainability and Safety (ICRMS) 2016; 11, https://doi.org/10.1109/ICRMS.2016.8050158.
22. Liang H, Zhang S, Wei Z, Shao N. System Safety Analysis of a Full Authority Digital Engine Control System. International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC) 2017, https://doi.org/10.1109/SDPC.2017.109.
23. Liu H C. FMEA using uncertainty theories and MCDM methods. FMEA Using Uncertainty Theories and MCDM Methods. Springer, 2016; 13-27, https://doi.org/10.1007/978-981-10-1466-6_2.
24. Lu Z, Liang X, Zuo M J. Markov process based time limited dispatch analysis with constraints of both dispatch reliability and average safety levels. Reliability Engineering & System Safety 2017, 167: 84 - 94, https://doi.org/10.1016/j.ress.2017.05.031.
25. Lu Z, Zhuo J, Li X. Monte Carlo simulation based time limited dispatch analysis with the constraint of dispatch reliability for electronic engine control systems. Aerospace Science and Technology 2018, 72: 397 - 408, https://doi.org/10.1016/j.ast.2017.11.023.
26. M250 turboshaft - RollsRoyce. [https://www.rolls-royce.com/products-and-services/civil-aerospace/helicopters/m250-turboshaft.aspx#/].
27. Pandian G, Das D, Li Ch, Zio E, Pecht M. A critique of reliability prediction techniques for avionics applications. Chinese Journal of Aeronautics 2018; 31(1): 10-20, https://doi.org/10.1016/j.cja.2017.11.004.
28. Prabhu S S, Kapil H, Lakshmaiah S H. Safety Critical Embedded Software: Significance and Approach to Reliability. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, https://doi.org/10.1109/ICACCI.2018.8554566.
29. PT6 E-Series Engine - Pratt & Whitney. [https://www.pwc.ca/en/products-and-services/products/helicopter-engines/pt6c].
30. PT6C - Pratt and Whitney. [https://www.pwc.ca/en/products-and-services/products/helicopter-engines/pt6c].
31. Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft. ASTM F3230-17. 2017.
32. TM 5-698-4, Failure Modes, Effects and Criticality Analyses (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities. Department of the Army. 2006, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=83559.
33. Youn W K, Hong S B, Oh K R, Ahn O S. Software certification of safety-critical avionic systems: DO-178C and its impacts. IEEE Aerospace and Electronic Systems Magazine 2015; 30(4):4-13, https://doi.org/10.1109/MAES.2014.140109.
34. Yu M N, Yu Z H, Jian H L, Xiao J Z. The optimization of RPN criticality analysis method in FMECA. 2009 International Conference on Apperceiving Computing and Intelligence Analysis 2009; 166-170, https://ieeexplore.ieee.org/document/5361125.
35. Zeng Z, Kang R, Chen Y. Using PoF models to predict system reliability considering failure collaboration, Chinese Journal of Aeronautics 2016; 29(5): 1294-1301, https://doi.org/10.1016/j.cja.2016.08.014.
36. Zio E, Fan M, Zeng Z, Kang R. Application of reliability technologies in civil aviation: Lessons learnt and perspectives. Chinese Journal of Aeronautics 2019; 32(1): 143-158, https://doi.org/10.1016/j.cja.2018.05.014.