



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

LETECKÝ ÚSTAV

INSTITUTE OF AEROSPACE ENGINEERING

**THE INTEGRATED METHOD UTILIZING GRAPH
THEORY AND FUZZY LOGIC FOR SAFETY AND
RELIABILITY ASSESSMENT**

INTEGROVANÁ METODA HODNOCENÍ BEZPEČNOSTI A SPOLEHLIVOSTI PALUBNÍCH
SYSTÉMŮ ZA POUŽITÍ TEORIE GRAFŮ A FUZZY

ZKRÁCENÁ VERZE

PhD Thesis

AUTOR PRÁCE

AUTHOR

Ing. Luboš Janhuba

ŠKOLITEL

SUPERVISOR

doc. Ing. Jiří Hlinka, Ph.D.

BRNO 2018

ABSTRAKT:

Dizertační práce se zabývá návrhem integrované metody hodnocení bezpečnosti a spolehlivosti palubních leteckých systémů za použití teorie grafů a fuzzy logiky. Navržená integrovaná metoda je univerzálně použitelná v oblasti leteckého inženýrství hodnocení bezpečnosti a spolehlivosti, nicméně je primárně navržena pro použití v kategorii v rámci General Aviation a civilních bezpilotních prostředků. Současná podoba hodnocení spolehlivosti je téměř výhradně závislá na úsudku analytika. Použití komerčních softwarových nástrojů pro hodnocení spolehlivosti je extrémně nákladné, přičemž možnost přístupu a úpravy použitých algoritmů je minimální.

Současný prudký vývoj palubních leteckých systémů je spojen s jejich zvyšující se komplexností a sofistikovaností. Integrovaná metoda používá teorii grafů, jako nástroj modelování funkčních závislostí mezi jednotlivými prvky systému. Použití teorie grafu současně umožňuje daný systém analyzovat, hodnotit hustotu vzájemné funkční vazebnosti, identifikovat důsledky případných poruchových stavů. Aplikace fuzzy logiky umožňuje manipulovat s expertní znalostí a stanovit kritičnost daného prvku a systému. Rozšířená kritičnost prvku zohledňuje pravděpodobnost jeho selhání, možnost detekce dané poruchy, závažnost těchto selhání vzhledem k vlivu na alokované funkce. Metoda zároveň obsahuje předběžné hodnocení úrovně odolnosti a zabezpečení systému vůči vnějším vlivům.

ABSTRACT:

Doctoral thesis creates an integrated algorithm for airborne system safety and reliability assessment. In 'general aviation' (mostly up to EASA CS-23) and 'non-military unmanned aerial vehicles industry' - safety and reliability assessment process still rely almost exclusively on human judgment. Current processes of system modelling and assessing are based on analyst understanding of a particular system. That is a difficult and extremely time-consuming process. Commercial computation aids are extremely expensive with restricted or even closed access to the solution algorithms. Together with this problem, the rapid development of modern airborne systems and their increasing complexity elevates the level of interconnection, safety and reliability analyses which have to be continuously evolved and adapted to the extending complexity.

The given integrated method utilizes the graph theory and fuzzy logic in order to develop integrated and partially computerized mean for reliability analysis of sophisticated and highly interconnected airborne systems. Through the use of the graph theory, it is possible to create the model of particular systems and its sub-systems in the form of universal data structure. It is even possible to assess various systems and items interrelations. And it also enables to evaluate particular item position and topology within the system and on the global level. Extended criticality evaluation is conceived as the fuzzy expert system that emulates decision making by a human expert. The integrated method also provides additional mean how to evaluate the system design. Fuzzy robustness assessment evaluates e.g. system diversity rate, redundancy, separation and environmental protection.

KLÍČOVÁ SLOVA:

Letadlo, Systém, Spolehlivost, bezpečnost, letectví, kritičnost, Fuzzy logika, Teorie grafů, Analýza

KEYWORDS:

Aircraft, System, Reliability, Safety, Aviation, Criticality Fuzzy logic, Graph theory, Assessment

MÍSTO ULOŽENÍ PRÁCE

Oddělení pro vědu a výzkum FSI VUT v Brně

Contents

1	INTRODUCTION	6
2	STATE OF THE ART	7
2.1	Doctoral Thesis drivers	7
2.2	Field of Interest	7
2.3	The Aircraft Systems and Architecture	8
2.3.1	<i>General Systems</i>	8
2.3.2	<i>Avionics System</i>	8
2.3.3	<i>UAVs and UAS</i>	9
2.4	Standard Reliability techniques and tools.....	9
2.4.1	<i>System modeling</i>	9
2.5	Criticality evaluation.....	11
2.5.1	<i>Criticality analysis</i>	11
2.5.2	<i>Risk Priority Number</i>	11
2.5.3	<i>Criticality review outcome</i>	11
2.6	Recent development of Safety and reliability methods.....	12
3	DOCTORAL THESIS OBJECTIVES	13
3.1	Main Objectives.....	13
3.2	Additional objectives.....	13
4	SELECTED MEANS	14
4.1	Integrated method architecture	14
4.1.1	<i>Introduction</i>	14
4.1.2	<i>Function hierarchy</i>	15
4.1.3	<i>Main functions</i>	16
4.1.4	<i>Support functions</i>	16
4.1.5	<i>Additional functions</i>	17
4.1.6	<i>Integrated method</i>	17
4.2	System modeling	18
4.2.1	<i>Function based modeling</i>	18
4.2.2	<i>Graph based model benefits</i>	20
4.2.3	<i>Rough tree and recursion algorithm</i>	22
4.2.4	<i>Graph model structure evaluation</i>	23
4.3	Extended criticality.....	25
4.3.1	<i>Severity</i>	26
4.3.2	<i>Occurrence</i>	26
4.3.3	<i>Detectability</i>	27
4.3.4	<i>Node topology parameter</i>	27

4.4	System robustness	27
4.5	Fuzzy evaluation process.....	28
4.5.1	<i>Fuzzification</i>	28
4.5.2	<i>Inference rules</i>	29
4.5.3	<i>De-fuzzification</i>	30
4.6	Integrated method process.....	31
5	MAIN RESULTS.....	32
5.1	Case study definition.....	32
5.2	EVALUATION PROCESS RESULTS	34
5.2.1	<i>Global model parameters results</i>	34
5.2.2	<i>Case study global model evaluation- basic parameters</i>	34
5.2.3	<i>Model structure and topology results</i>	35
5.2.4	<i>Robustness parameters</i>	35
5.2.5	<i>Rough tree evaluation</i>	36
6	CONCLUSION	37
7	ACRONYMS AND ABBREVIATIONS	38
8	REFERENCES	39
9	PUBLICATION.....	40
10	PRODUCTS	40
11	AUTHOR CURRICULUM VITAE	41

1 INTRODUCTION

Nowadays aerospace engineering might be characterized as rapidly growing and diverse. The sky upon our heads is literally occupied by a thousands of airplanes with different shapes, propulsions and weight. It is essential to ensure safe and secure air traffic. Increasing number of airplanes is speeding up the need for means of ensuring its safe flight and landing. Modern airborne systems provide advanced full-scale assistance. In the era of "More Electric Aircraft" flight data, autopilot, warning system, diagnostic system, control of engine, flaps, trims, landing gear might be integrated into the glass cockpits.

This aircraft airborne systems are getting more and more complex and sophisticated. Hence safety and reliability analyses have to continuously evolve and adapt to the extending complexity.

Modern and complex airborne systems first started to appear in the field of general aviation recently. Previously separate components for communication, navigation (global positioning systems) have been integrated into the glass cockpit to provide flight management functions and advanced support for flight crew (e.g. terrain and traffic avoidance, etc.). Recent generation of airborne systems started to appear as automatic and partially autonomous system adding new level of safety to the aircrafts. These systems are becoming standard components also in avionic systems of general aviation aircrafts. Therefore, safety and certification requirements are evolving, getting more detailed and essential.

At the same time, unmanned aerial systems are skyrocketing to the top of current interest. UAS includes e.g. autopilot, communication, warning systems, engine control system, expensive payload and other significant components. Due to that there is a deep necessity to evaluate UASs safety and reliability.

Safety assessment process still relies almost exclusively on human judgment (in lower categories). Recommended practices define processes for system modelling are based on analyst understanding of a particular system. Reviewing of many system components, assemblies, elements function followed by assessing of all failure modes and their resulting effects on the system is at least complicated process. Assessment methods and techniques are integrated into a coherent safety life cycle.

Development of general aviation airborne system, e.g. (Flight control system, Fly-by-wire, engine utility system, etc.) and development of non-conventional highly automated airborne systems is reaching point where it is not possible to avoid computerized support for system analysis (at least in minimal level). Increasing level of complexity elevated the level of interrelation which brings a need to think how to make safety process more transparent, accessible and results comprehensible.

Further airborne systems of light airplanes along with unmanned aerial systems suffer with lack of relevant reliability data. The absence of detailed studies focused on probability of successful performance of an airborne system at any time, makes safety assessment inconclusive. The successful performance of any system depends on the extent to which reliability is designed and built. In the real conditions, even almost identical systems, operating under similar conditions will have different life-time. Therefore, the failure of the sophisticated systems could be described only probabilistically.

It is crucial to understand the patterns and modes of failure related to the particular system, item or element. A huge difference could be noted between the failure's patterns of e.g. mechanical or electrical. The electronic and mechanical systems (the most important in aviation system engineering) deteriorates during usage as a result of elevated temperature changes, mechanical wear, fatigue or a number of other reasons. (Partially [9])

The reliability of component is associated with the system operation and component function. It is almost impossible for general aviation manufacture to provide reliability testing for each component of the system in relevant conditions.

This thesis intends to prepare algorithm for safety and reliability modelling and evaluation of a complex systems (usually) with safety critical function regardless of presence or absence of reliability data. The results implementation methodology to the formal assessment process will be also included into the doctoral thesis.

Doctoral thesis outputs should be an integrated process allowing to estimate item criticality and system reliability (when reliability data are available) using the same data structure along with additional outputs. It is assumed that integrated method usage will be in the field of general aviation and unmanned aerial systems.

2 STATE OF THE ART

2.1 DOCTORAL THESIS DRIVERS

The word complex (complexity) characterizes something, consisting of many elements, where those elements interact with each other in multiple ways. Complexity studies assess, how elements relationship affect a collective behavior of system. For instance, modern modular avionics units (MAU) are connected by Ethernet in particular house. In this architecture, functions are spread across common system modules and the operational functionality of the system is imparted by software [13]. This is the model example of increasing system complexity.

What is the complex system in aerospace?

The most fundamental question is- what is the complex or more precisely sophisticated airborne system? The best way how to get the answer, it is to begin with FAA advisory circular 23.1309-1E definition, where the complex system is defined:

“A system is “complex” when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods.” [1]

To exceed problem with growing interconnection between system components which results in high complexity, it is imperative to find means of system easy and accessible representation in form of data structure.

2.2 FIELD OF INTEREST

Integrated method presented in following chapters of this doctoral thesis should be, after development and debugging process, universally applicable on general systems. Nevertheless, critical reviews, experiences and method adjustment are done especially for airborne systems. The most probable application of suggested method is in general aviation. However, it could be successfully applied on Unmanned Aerial Vehicles as well.

Method, results and outputs should be in a sufficient form for less complicated systems of small aircrafts and most likely for aerial vehicles. These categories do not have well-structured and detailed safety assessment targets and procedures defined in regulation requirements and certification requirement are not so strict and intense in term of formal structure. For safety and reliability assessment of larger aircrafts (like EASA CS-23) it should provide advanced mean of complex system representation, accessible manageable for system engineering department personal.

What is General Aviation?

The term General Aviation is mainly considered as equal to the EASA CS-23 category. It covers airplanes in the normal (limited to non-aerobatic operations), utility (limited operation due CS-23.3), aerobatic and commuter (propeller driven, twin engine, up to 18 passengers, take-off weight of 8618 kg or less) categories.

The airborne systems are certified under EASA CS-23-part F (safety assessment 23.1309), typically with advisory circular FAA AC 23. 1309- 1E (recent). The advisory circulars are not mandatory and do not

constitute a regulation. It is a set of acceptable means for demonstrating compliance with applicable regulation (EASA CS-23).

2.3 THE AIRCRAFT SYSTEMS AND ARCHITECTURE

Aircraft is highly developed piece of modern engineering. It consists of sets of interacting systems working together which enables aircraft to perform its operation. Any system can be described as particular combination of items controlled (or not) by controlling unit that provides particular function. Several systems are formed by collection of sub-systems. These sub-systems work together to perform as single system.

Airborne systems are diverse, airplane is equipped by high integrity system like flight control, real-time gathering and processing like fuel management (mostly airliners, jets or fighters) or simply logical processing systems. They all affect airplane safety in some way. [13]

As it was mentioned above, airborne systems of any modern airplane is getting more complex and sophisticated. Means of safety and reliability has to evolve as well. First step of that kind of evolution is to understand field of interest principles. Basic description of airborne system is following with illustration on

Chyba! Nenalezen zdroj odkazů..

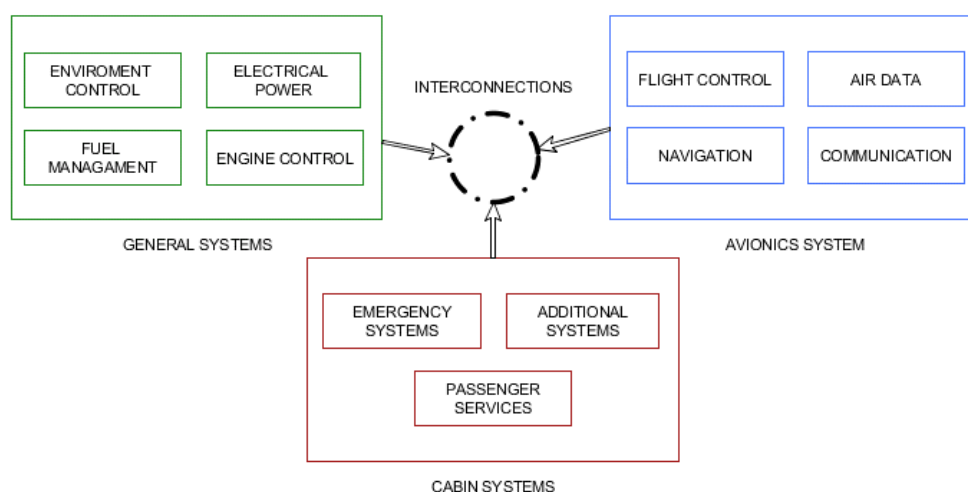


Figure 1 EASA CS-23 Commuter aircraft basic systems example (based on [13])

2.3.1 General Systems

The general systems are essential for airplane to conduct safe flight and landing. Engine control system, electrical power generating and distributing system, flight control, hydraulic system, fire protection, fuel management or environment control are integrated parts of each airplane. These systems are mandatory included in system safety assessment. They are usually combination of mechanical and electrical parts. For instance, safety assessment of electrical system is one of most difficult analysis in SSA process. It is imperative to find equilibrium between analysis deep and clarity. Extensive variability of this system creates necessity of methodical approach to safety and reliability assessment.

2.3.2 Avionics System

Avionics covers cockpit displays (PFDs, MFDs, etc.), navigation system, communications, aircraft management system, warning system, aerometric system (Pitot-static system, airspeed indicators, attitude indicators, etc.). It is most rapidly evolving airborne system.

During last sixty years avionics system architecture evolved. Huge boost of aircraft performance speeds a need for avionics system evolution. To utilize growing improvements, capability and complexity of avionics system hugely grew. Performance, reliability and computation power is increasing together with costs.

Using just standard reliability methods like FMEA the safety and reliability assessment is extremely complicated and expensive. For instance avionics system without glass cockpit of EASA CS-23 Commuter aircraft consist of at least of 28 airborne components (GTNs, Indicators, artificial horizons, etc.), 90 electric components (fuses, relays, switches, etc.) and 10 antennas (communications, GPS, etc). Without computerized aids the assessment process is really complicated with non-coherent outputs.

2.3.3 UAVs and UAS

The common mistake related to the UASs is that UASs reliability is marginal problem. If it crashes, there is no one on board and it is no big deal. This idea is getting more and more outdated. Unmanned aerial vehicles are expensive and provides important operations. Any UASs crash can cause property damages, injures or fatalities to over flown people and property.

In near future UAS will be subject of mandatory safety and reliability assessment. As it was mentioned in this doctoral thesis, UAS are typical example of system which consists of items without available probabilistic data. Integrated method is designed to at least partially overcome lack of reliability data.

2.4 STANDARD RELIABILITY TECHNIQUES AND TOOLS

2.4.1 System modeling

To manipulate and evaluate complex system it is imperative to find a proper way how to represent a system. System modelling is the multidisciplinary study of model usage to system conceptualization. There are numerous means of system modelling. In engineering reliability studies, they are usually specialized for particular purposes.

Reliability Block Diagrams

Reliability block diagrams are assessment methods, which show logical connection between components of a system. The system is described within serial (AND gate) and parallel connections (OR gate). Block diagrams can be used for description of failure condition as well. In that case serial connection represents OR gate, parallel connection AND gate. For example, RBD is not suitable technique for evaluation of avionics system consisting integrated modular parts.

Fault trees

Fault Tree Analysis is a deductive, top-down method based on oriented graphs and Boolean logic. This method was created during development of intercontinental ballistic missile LGM-30 Minuteman in 1960s. Soon, the method was adopted in Boeing and is widely used in aviation.

Fault tree analysis uses probability to assess whether a particular system or architecture will meet the requirements. It starts from consideration of system failure effect, referred to the "Top Event". The analysis proceeds by determining how these can be caused by individual or combined lower level failures or events. The analysis procedure and structure is also described in detail in SAE ARP4761. The Top Event is usually failure condition.

Markov Chains

Markov analysis is associated with failure probability and probability of being returned to an available state invented by Russian mathematician Andrey Markov. It is mostly applied to safety assessment of maintained systems or in combination with fault trees. The one main benefit is relatively easy computerization.

In Markov chains a single component can be in one of two basic states- fail or available. Probability of transition from state available to state fail is called state transition. Every state and transition with probabilities in the existing states are modelled in state-space diagram (example Figure 7). The availability of system can be then solved by using tree diagram. (Partially [13]) Disadvantage of Markov chains is complexity of solution in the case of complex system. System with two components may have 2^n different states. Anyhow aircraft is considered as non-repairable system.

Petri Nets Model

It is a tool for description of relation between events and conditions. Techniques is also known as place/transition net and it is based on directed bipartite graphs, where nodes represent events which may occur. Petri nets were developed by mathematician and computer scientist Carl Adam Petri and presented for the first time in his doctoral thesis. Petri net is directed bipartite graph with degrees. The arc represents places which are previous and/or post conditions for transition with arrow. It is used for graphical notation for stepwise processes which includes choices, iteration and concurrent execution. (Partially [13])

Functional Hazard Assessment

Functional Hazard Assessment identifies potential system failures and the effects of these failures. Failures are tabulated and classified according to their possible effects, and the safety objectives are assigned according to the criteria. [18]

This analysis creates ground work for determination of individual system criticality during first phase of development of an aircraft. The analysis also defines system specification which will be subject of further quantitative analysis. This failure conditions were identified during functional hazard assessment. Development phase of project identified basic requirements and establish preliminary draft of electric system.

Failure Mode and Effect Analysis

FMEA is structured, qualitative method used for identification of failure modes and resulting effects on system operations. It was created within study of military malfunction in 1950s. It is probably recent most used reliability analysis method. The principle of FMEA is to consider each mode of failure of every component of a system and to assert the effects on system operation of each failure mode in turn. [14]

There are three basic FMEA levels- Functional, Design and Process. It can be extended to the qualitative and quantitative analysis by adding criticality level. The analysis procedure and structure is described in detail in SAE ARP4761. In the process of airborne system evaluation is FMEA most important part of analysis. The FMEA analysis describes failure modes of each element considered in safety assessment. FMEA identifies critical elements, functions, which should be analyzed in depth.

Common Cause Analysis

According to the ARP4754A Common Cause Analysis (CCA) establishes and verifies physical, functional separation, isolation and independence between systems and items. CCA techniques are an extension of deductive safety assessment targeted to the detection of dependence between events which would be otherwise treated independently. Generally, CCA analyse independence between systems, functions or items, which may be required to satisfy the safety requirements. There are three basic subparts of the CCA which are used in aviation- Zonal Safety Analysis (ZSA), Particular Risk Analysis (PRA) and Common Mode Analysis (CMA).

2.5 CRITICALITY EVALUATION

Criticality as a term might be explained in field of aviation as a state of being critical to sustain safe flight and landing. It is a descriptive number interconnecting severity of component failure together with its probability of occurrence. In common system safety assessment, it is usually defined in various ways. This doctoral thesis presents two most important.

2.5.1 Criticality analysis

Criticality analysis ranks each potential failure mode identified in the process of FMEA, according to the combined influence of severity classification and its probability of occurrence based upon best available data. Following description is based on Military Standard MIL-STD-1609a [2].

Qualitative approach [2]

It is appropriate when specific failure rate data are not available. Failure modes identified in failure mode and effects analysis are assessed in the terms of probability of occurrence. Individual failure mode probabilities of occurrence should be grouped into distinct, logically defined levels, which establish qualitative failure probability level.

Quantitative approach [2]

Quantitative approach adds failure rate data to the criticality analysis, while the source of this data should be the same as that used in the rest of safety and reliability assessment. The data shall be derived for example from operational data, commercial databases (NPRD-2011C, FMD-97CD, EPRD97-CD, VZAP-95C, etc.) or military handbooks Reliability Prediction (MIL-HDBK-217 Reliability prediction of electronic equipment).

Failure mode criticality number [2]

Criticality number is the portion of the criticality number for the item due to one of its failure modes under particular severity classification.

2.5.2 Risk Priority Number

RPN method adopts linguistic terms to rank the chance of failure mode occurrence (labelled P), the severity of its failure effect (S) and chance of undetected failure (D) using numeric scale 1-10. Technique uses previously prepared "conversion" tables (like Ben-Daya and Raouf 1996, etc.) as bases for the linguistic judgment scales used to estimate the quantities which are used to calculate the RPN value. RPN method can be labelled as quicker and cheaper in comparison with criticality analysis. Nevertheless RPN as quantitative method is essentially based on qualitative assessment and results are only educated guesses at best. [4] This technique is usually applied in automotive industry

2.5.3 Criticality review outcome

To exceed a problem with vaguely defined basis methodology based on fuzzy logic is presented. This methodology has been proposed by several researchers and development groups (Bowles and Pealez 1995, Adbelazis 1999, Braglia and Frosolini 2001, etc.) as a tool for direct manipulation with linguistic terms used in criticality assessment. The linguistic terms in criticality assessment process can be directly handled with some advantages compared to the strictly numerical methods.

2.6 RECENT DEVELOPMENT OF SEFETY AND RELIABILITY METHODS

Shortcomings of existing procedures partially described in previous chapters, especially in relation to the complex safety critical systems where insufficient inputs are available led to research works with intend to overcome these shortcomings. Most relevant works include:

- (A) Method combining various solution techniques for dynamic fault tree analysis. It is specialized for computer systems presented by R. Manian, J.B. Dugan, D. Coppit and J. Sullivan from University of Virginia. It extends the DIF-tree analysis capability to model several different distributions of time of failure, including fixed probabilities, experimental, Weibull and log normal probability distributions. Used approach extends both the binary decision diagram and Markov analytical approaches. [15]
- (B) One way how to overcome Markov method problems (even simple system has a 2^n states) is to use Fuzzy Markov model. It is a technique for analyzing fault tolerant designs under considerable uncertainty, like compilation of component failure rates. It works in conjunction with fuzzy fault trees. It provides alternative to the probability paradigm possibility. Main disadvantage of this methods is still computation complexity. [16] However the concept of adding fuzzy logic as an alternative of probability paradigm strongly influenced doctoral thesis method.
- (C) A method of evaluation of power system using the node-weighted network proposed by Peng Zahng and Qishaung Ma [17], which is based on nature connectivity is one of this doctoral drivers. The electric system modeled by using the no-weighted network is closer to the real system than standard RBD. Application of a basic graph theory principles together with knowledgebase of particular system among others leads to the different treatment of system during design and test phases. However, the presented scope of graph application is insufficient. The possible graph theory applicability is much more lagers. This doctoral thesis intends to use graph theory as essential instrument of system representation.
- (D) The most promising starting point for advanced way how model and evaluate complex airborne system is the technique described in [11]. Suggested reliability technique using a combination of graph theory and Boolean logic provides easy accessible system representation along with qualitative evaluation of the system interconnection and reliability. Technique is described during its integration and extension to the doctoral thesis method.

However, none of abovementioned research studies is alone suitable for application subject of doctoral thesis main interest: Safety assessment of complex safety critical systems with insufficient input data (applicable in large extend also to UAVs and general aviation aircrafts).

Therefore, doctoral thesis presents integrated technique which consist of combination and extension of several diverse approaches and techniques adjusted for safety assessment of airborne systems. As a starting point for integrated method architecture development, critical review revealed possible several approaches related to the other industries. Critical review of state of the art revealed strong need to find a proper way, how model particular system. There was a possibility of graph theory usage. Sinnamon and Andrews study of "New approaches to evaluating fault trees" [12] deals with uses binary decision trees for FTA evaluation. Indian study focused on Systematic failure mode effect analysis using fuzzy linguistic model deals with combination of fuzzy logic and prioritizing failure cases of hydraulics system (element of feeding system) [6]. Usage of fuzzy logic as a tool of handling risk assessment led to fuzzy logic application in airborne criticality evaluation.

3 DOCTORAL THESIS OBJECTIVES

3.1 MAIN OBJECTIVES

Doctoral thesis proposal established set of main and additional objectives for the doctoral thesis. These objectives are implemented to the thesis according to the its structure and logic:

- Airborne systems design critical review in the main field of interest- General aviation.
- Preparation of graph theory as a mean of airborne system representation usable during system safety assessment (focused on complex and non-conventional systems).
- Preparation of graph theory results into a form of solid bases for fuzzy criticality assessment.
- Adjusting of fuzzy criticality assessment for application in various airborne system, where lack of input data prevents assessment using traditional methods. Creation of fuzzification techniques (score tables, scales, etc.), specific fuzzy base rules and appropriate de-fuzzification methods in order to estimate relevant system criticality number.
- Finally, incorporation of graph theory application together with fuzzy criticality assessment study into the integrated algorithm of safety and reliability evaluation.
- Integrated process applicability demonstration in on case study.

3.2 ADITIONAL OBJECTIVES

- Summary of regulation requirements imposed on aircraft equipment (including safety and reliability requirements).
- System robustness additional evaluation (Not included in thesis proposal)

4 SELECTED MEANS

4.1 INTEGRATED METHOD ARCHITECTURE

4.1.1 Introduction

Reliability assessment in the field of modern aviation is long extensively complex process involving analysis of huge number of mutually connected elements of different systems. Each system affects other systems in different way. Easily accessible data structure should make safety and reliability process more effective. Method how represent complex airborne system suggested in this doctoral thesis uses a simple mathematical tool the graph theory. It is natural step to represent system by drawing a graph. A set consisting of points along with lines joining pairs of these points represent particular system and its interconnection. Then it is possible to define each component, subsystem or assembly as a set of interconnected elements.

In standard safety and reliability studies are usually used another special graphs- reliability block diagrams and fault trees. Block diagram is a kind of pseudo graph. It is used for modeling of a system with assumption that system will operate if any sequence of components operates. The fault trees are used to represent important failure modes identified by the functional hazard assessment. However, both techniques (RBD, FTA) require extensive calculation for just one failure mode. Also, there is only a poor correlation between real system and its representation.

Second part of suggested integrated method deals with insufficiency of input reliability data. The criticality assessment could partially substitute input reliability data. In the order to establish solid basis for criticality and robustness evaluation fuzzy logic is included to the method. This technique is practically used in several industry branches (nuclear power plants, different process plants, etc.). Common technique of criticality evaluation (MIL-HDBK Criticality Analysis) used in general aviation is not sufficient for all types of modern systems, especially for non-conventional systems with limited input data.

Standard criticality number used in safety and reliability analysis of airborne system is defined as a relative measure of the consequences a failure mode and its frequency of occurrence according to Military standard MIL-STD-1629A.

Integrated method extends this definition to the wider level (see chapter Extended criticality). It uses term Extended criticality to distinguish between standard criticality and criticality developed in this doctoral thesis.

Generally, system engineering deals with vaguely defined qualitative terms and results. The fuzzy criticality analysis uses linguistic variables to describe the severity, frequency of occurrence, and detectability of the failure. Fuzzy criticality application as integral part of proposed method aims to even extend classical fuzzy criticality assessment to a next level.

Proposed integrated method presents way how to preliminary express system ability to resist ambient influences without adapting its initial stable configuration without full scale Common Cause Analysis by establishing robustness number/ level. Analyst is able to evaluate system inference, protection from external influences (system separation/ segregation, diversity, etc.) using robustness evaluation guidelines.

Function oriented graph modeling, extended criticality evaluation and robustness evaluation form integrated method of safety and reliability assessment. Particular parts of integrated method are based on state of the art critical review, literature study and especially on previous experiences.

4.1.2 Function hierarchy

Aircraft is highly developed, interconnected and sophisticated system. It has to perform dozens of functions at once just to sustain at flight. Modern airplanes combine heterogeneous system with different characteristics and requirements. Flying object has to provide sustainable propulsion, high maneuverability with reliable flight control, precise navigation, continuous communication with air traffic control and many more other. Fuselage, leading edge, pitot-static system has to be protected against ice and rain, fuel system and engines against fire, flight crew and passengers against lack of oxygen, cold and suffocation. Electrical generators must provide DC and AC power for autopilot, indication system, navigation, external lights, etc.

Process of airborne system safety and reliability assessment ordinarily consists of many interrelated but separated processes. Various analyses are proceeded during whole design, starting with basic aircraft level functional assessment. As the aircraft and its systems are evolving from initial requirements to the detailed design, analysis must verify resulting influences on the airplane safety and reliability.

Concept of aircraft safety is based on **Main Safety Objective (MSO)**: The ability to sustain at flight and land safely.

Reliability is the probability that item (in this case aircraft) can perform a required function under given conditions for a given interval. Aircraft's main function is to be able to sustain flight and land safely. Probability is a mathematical tool expressing the likelihood of occurrence of a specific event. Probability estimations are based on engineering and historic data; these data should include some measure of uncertainty. Uncertainty expresses the degree of belief analysts have in their estimates. Uncertainty decreases as the quality of data and understanding of system improve. The initial estimates of failure rates or failure probability might be based on comparison to similar equipment, historical data (heritage), failure rate data from databases or expert elicitation. [19]

Results of every particular analysis supposed to serve as base for following design step forward. As it was mention above, all these analyses mainly relay on human judgement (especially in the field of doctoral thesis field of interest). Results are handled manually in particular steps. Process starts with functions identification, Functional Hazard Assessment (FHA) is proceeded at Aircraft level, then lowers down to the System-level.

This process could be with some limitation generalized. Basically, Aircraft level FHA identifies airplane "higher" functions. These functions are directly interconnected with aircraft's ability to sustain safe flight and proceed landing. Otherwise, System-level FHA explains functions of particular system. How they are bounded to the higher functions.

A complex system functions should be arranged into fixed hierarchy. Functions are than ranked above (or at same level) each other according to their influence on main safety objective. Safety influence is possible to express in form of degree of decisive importance with respect to the crucial outcome in relation to the main safety objective. Functions with direct influence on main safety objective are labeled as Main function (MF). MF implements main safety objective. Functions which are designed to facilitate or support main function are labeled as Support function (SF). Support function could be taken as means to ensure higher functions. Function without relation to the main safety objective or not significantly contributing to the supply function performance are labeled as Additional functions (AF).

Functions hierarchy serves during system modeling as key element. Unlike traditional modeling methods, integrated method uses function- oriented modeling. Event- oriented models usually used in reliability analysis (for instance fault trees) are designed to identify combination of events (usually a failure) causing particular failure and it is possible to estimate probability of this failure. Each model describes combination of events for single case (failure). It does not sufficiently describe complexity or connectivity of system items and functions. Suggested function- oriented modeling adopts graph theory principles to describe system interconnection. Particular system consists of various items. Items are mutually interconnected to ensure particular function; these connections are modeled as direct vertices between parent and child nodes (items) in direction to the function. For example, electric generator provides

electrical power. Electrical power is distributed through sequence of relays and buses to the electrical loads. These loads ensure their particular functions. Using previous example, automatic direction finder (ADF) is one of many aircraft electrical loads. It is a radio- navigation instrument measuring and displaying relative bearing to suitable radio station

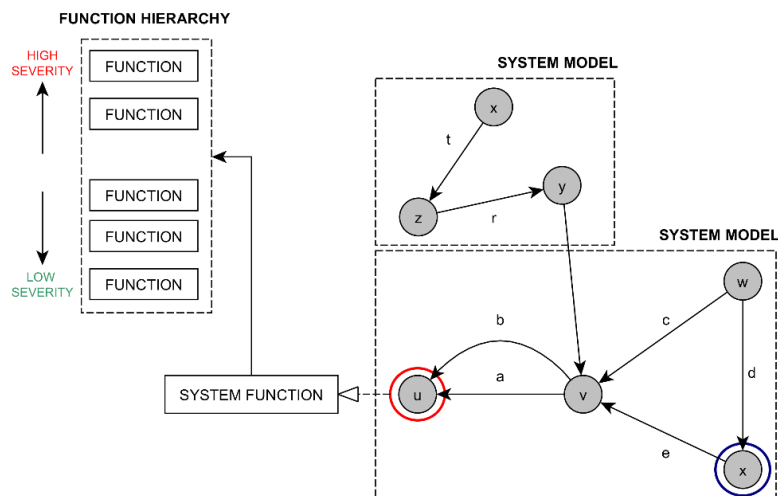


Figure 2 Function- based modelling

4.1.3 Main functions

Aircraft function are divided main and supporting functions. The main functions attain system main safety objective; these functions are labeled as **Main functions (MF)**.

- **Propulsion** - *Loss of propulsion during landing and takeoff phases usually leads to the hazardous or catastrophic situations.*
- **Flight Control**- *Inability to control flight directly jeopardize crew and passenger's safety. During critical flight phases (takeoff, landing, go around), there is high probability of catastrophic outcome. It could lead to serious injury or fatality, loss of structural integrity of wings, tail or fuselage. It could case collision with other aircrafts.*
- **Navigation and Communication**- *Indirect influence on the higher safety objective.*
- **Landing aids**- *Loss of ability to eject landing gear leads to hull loss and possible fatal injury. Inability to use landing aids (ILS, MLS) potentially also leads to the hazardous or catastrophic consequences.*

4.1.4 Support funcitons

Functions providing necessary resources are labeled as Support functions (SF). Its objective is support of main function realization. These functions are auxiliary to main functions.

Using the rational level of abstraction, support functions could be categorized:

- Provide a motion or source of motion (fuel system provides "source of motion" for engine)
- Instrumentation and control of main function (engine control, flight control indication)
- Provide an appropriate operating environment (pressure, temperature, humidity)

4.1.5 Additiional functions

Additional functions do not contribute to performance of main function. Therefore, they are not influencing Main Safety Objective. Essentially, absence of these functions does not affect aircraft operations. For instance, passenger’s entertainment system, on board lighting, etc.

4.1.6 Integrated method

The main idea of integrated method is to establish mean how to combine particular parts of safety and reliability assessment. Function- oriented system model in the form of directed graph serves as a universal platform for the whole assessment process.

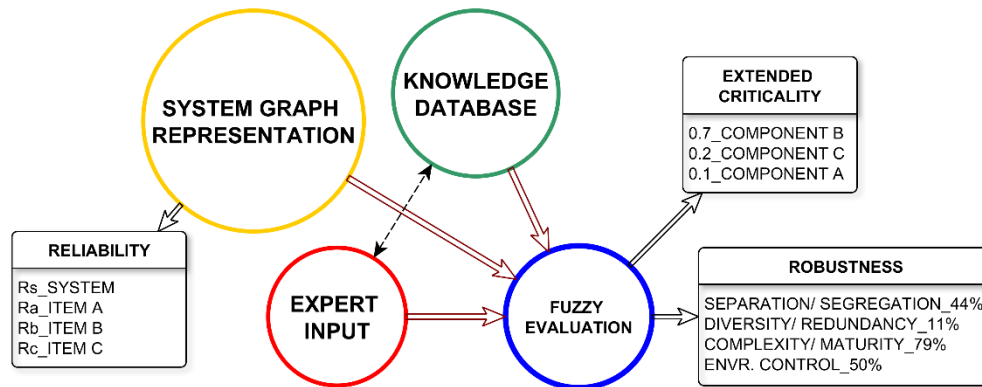


Figure 3 Integrated method architecture

System function and operation are not defined just by items interconnection. System functionality is influenced by huge number of factors. Each item has specific contribution to the function performance. As it is mention above functions are arranged into hierarchy according to their relation to the main safety objective. Criticality level could be defined as “degree of this influence”.

In the doctoral thesis field of interest, system consist of items without appropriate probabilistic data (due to various reasons, see state of the art). System configuration is result of engineering process and it is possible to describe it by expert knowledge. Abstract knowledge consists of vague statements (in the way, it is not possible to express these in precise mathematical definitions). Therefore, criticality by doctoral thesis definition cannot result from exact formula. Integrated method must adopt sort of mean to handle vague definition. Fuzzy logic is adopted to criticality and robustness level estimation. This process is described in deep in chapter Extended criticality.

What are the factors influencing system functionality? Safety and reliability process intents to identify possible failure modes and resulting effects on system functions (in general to the MSO). Specific failure modes have different severity of influence. They occur in with different probability and with deferent possibility of detection. Integration method provides knowledge database which contains preliminary failure classification related to the MF, SF and AF, usually applied remedies and criticality evaluation inputs.

System functionality is also highly influenced by its physical installation. Various systems are deployed through the airplane. Crew cabin is sort of nerve centrum. Controlling mechanisms, system indication is routed from wings, engines, tail and other to dashboard. Connection separation and segregation plays leading role in system protection against ambient influences (temperature, electric short cut, etc.), which could threaten the MSO. Employment of technology with different physical principles potentially increases system diversity. Redundancy build on diverse system rooting could lead to the system safety increase. Diverse redundancy together with essential items (or function) duplication could create even higher system safety (in the case of highly complex systems).

System complexity is important factor influencing system design, emergency procedures and crew training. Maturity and experiences with application of complex system influence system architecture. Complex system maintenance procedures are directly connected to the potential failure detectability. Human interface during design and maintenance is other factor, which must be counted into sum of influences. Process of robustness level evaluation helps to create larger picture of system functions and operations. Integrated method offers guidelines for robustness evaluation. Integrated method intends to establish connection between item failure, common cause failure, function hierarchy, criticality, robustness on the platform of systems model in the form of directed graph. Following chapters explain particular steps of the procedure.

4.2 SYSTEM MODELING

Various systems may be easily represented by a graph. That kind of data structure is highly universal and easy to process. Graph representation finds a usage during whole SSA process. It can be expanded, modified and assigned to a larger unit. During the failure mode effects evaluation phase data serves as a tool for components interconnection investigation. Physical interconnection rate can be easily estimated (described in further chapters). The failure mode consequences classification can be partially automated considering physical interconnection and affected components.

In the case of complex failure modes selected according to the FHA analysis, sub-system or sub-function of the system may be detached from general system data structure. Then its probability of failure or reliability is established.

4.2.1 Function based modeling

Concept of aviation safety is based around most essential objective- the ability to sustain at flight and land safely. Integrated method names this- Main Safety Objective (MSO). Aircraft and its functions is designed, developed and tested to fulfil and ensure the MSO.

These complex airborne system functions could be arranged into fixed hierarchy. Functions are then ranked above (or at same level) each other according to their influence to the MSO. Safety influence is possible to express in form of degree of decisive importance with respect to the crucial outcome in relation to the main safety objective. Functions with direct influence on main safety objective are labeled as Main function (MF). MF implement main safety objective. Functions which are designed to facilitate or support main function are labeled as Support function (SF). Support function could be taken as means to ensure higher functions.

Function without relation to the main safety objective or not significantly contributing to the supply function performance are labeled as Additional functions (AF). Unlike traditional modeling methods, integrated method uses function- oriented modeling. Event- oriented models usually used in reliability analysis (for instance fault trees) are designed to identify combination of events (usually a failure) causing particular failure and it is possible to estimate probability of this failure. Each model describes combination of events for single case (failure). It does not describe complexity or connectivity of system items and functions.

Suggested function- oriented modeling adopts graph theory principles to describe system interconnection. System items are mutually interconnected to ensure particular function; these connections are modeled as directed vertices between parent and child nodes (items) in direction to the function. For example, electric generator provides electrical power, then it is distributed through sequence of relays and buses to the electrical loads. Function oriented model allows to describe interconnection between various system (electrical, avionics, etc.) in relation to the particular function.

In standard safety and reliability studies are usually used another special graph- reliability block diagrams and fault trees. Block diagram is a kind of pseudo graph. It is used for modeling of a system with assumption

that system will operate if any sequence of components operates. The fault trees are used to represent important failure modes identified by the functional hazard assessment. However, both techniques (RBD, FTA) require extensive calculation for just one failure mode. Also, there is only a poor correlation between real system and its representation.

System consists of various items and their interconnection in order to assure provide intended functionality. Unlike design scheme, function based modelling represents sequence of function provided by items. Item is represented by node (vertices). For each node, there are various basic attributes- like type, system participation, zone, occurrence, detectability, severity and criticality. Function interaction is represented by edge. For each edge, there are also various basic attributes type, system participation, occurrence and zone. Set of attributes could be extended or reduced for particular application.

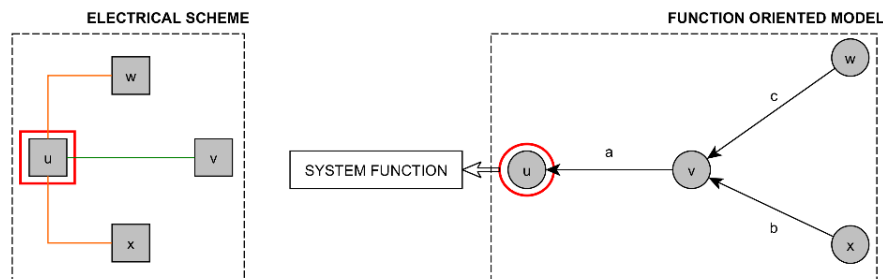


Figure 4 Function based modelling example

Example in Figure 4 describes fundamental difference between physical interconnection provided by drawing or schemes and function model. In example item **u** represents engine. Items **w**, **x** represents two channels of electric supply from airborne batteries or cross-feed (alternate generator). Item **v** represents changeover switch (flight crew selected one or other way to start the engine based on a given scenario). Physically, items **w**, **v** and **x** are not connected. However, their functions are fundamentally connected. Function based modelling is in this doctoral thesis based on so called function propagation. Items functions are interconnected to the chain in order to provide function.

It is based on so called function propagation. Items functions are interconnected to the chain in order to provide function. For instance, generator provides electrical energy. Energy is transferred through the sequence of wires, relays and buses to particular loads. Through chain of functions is the intended high function provided. Functionality of particular item is influenced by controlling mechanism (generator control unit or logic relay).

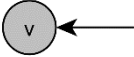
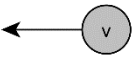
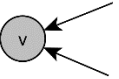
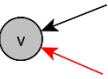
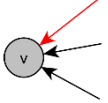
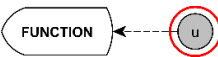
<i>Node- edge relation</i>	<i>Description</i>
	Item functionality is conditioned by function of preceding item in the direct line of function.
	Item functionality conditions function of succeeding item in the direct line of function.
	Item functionality is conditioned by at least one of preceding items. Edge type is identical. <i>Note. In the case of failure propagation, it is basically AND gate.</i>
	Item functionality is conditioned by function of two preceding items in the direct line of function. There are two types of inputs (therefore there is no redundancy). For instance, red one is electric power and black data sensing. <i>Note. In the case of failure propagation, it is basically OR gate.</i>
	Item functionality is conditioned by function at least one of redundant preceding item and the function of other one.
	It represents final (A/E) – acting item- providing the function itself) node in direct line of function. Node is excluded from graph topology evaluation.

Table 1 Node- edge relation

Items are usually associated with several functions on system or local level. However, multiple of them is associated with many more function on the global level. Model analysis is conducted on these two separate levels. Some network parameters are influenced by this division, other not.

Operational modes

Function oriented model should be developed for various operational modes. These modes reflect system configuration in particular situation. Operational modes selection is based on expert knowledge of analysis and system designers:

- Standard function
- Engine start/ Engine cross-start
- One engine or generator failure
- Multiple engine or generator failure
- Electromagnetic interferences
- Hydraulic system failure
- Fuel distribution malfunction
- Primary flight control means malfunction

4.2.2 Graph based model benefits

System data structure in the form of graph allows to easily assess particular items, systems or function interconnection. This ability is highly useful for analysis itself, it could be applied during initial design phase of project or final formal evaluation. Data structure is accessible and modifiable. Analyst is able to model system in various operational modes and configurations. Interconnections of items allows to combine items function in order to provide intended high function. These interconnections influence particular items functionality, diffuse failure effects through the systems. Typically, it is subject of strongly structured and formal types of analysis like FMEA. Function based modeling (and storing in the form clusters of nodes and edges) serves as effective mean of identifying mutual influence.

Predecessors

Predecessors are defined a set of nodes (vertices) coming before a given node in a directed path. This trivial attribute of graph is actually quite useful and illustrative.

The figure on the left shows example of set nodes preceding a given node. The node represents **R MAIN** electrical bus of case study. It is quite obvious, that **R MAIN** functionality (ability to provide electrical power to its loads) is conditional to functionality of various items. Electrical power is supplied from right generator or battery or through the bus-tie interconnection from left generator. Drive of generators is provided by engines. Generators are governed by controlling unit **RCU**, **LCU** respectively.

Successors

The other side of a coin is successor. It is set of nodes coming after a given node in direct path. Continuing using the same example, the case study **R MAIN** is used in the Figure 25 (a) as initial to whom other succeeds. Electric power is supplied to left axillary bus (**AVION LAX**), directly to the elevator trim fuse and possible to the main bus from right main bus. Than the electrical power is distributes though various buses and fuses to loading items. These items provide particular function. Combination of support function provides intended high function resulting in Main Function.

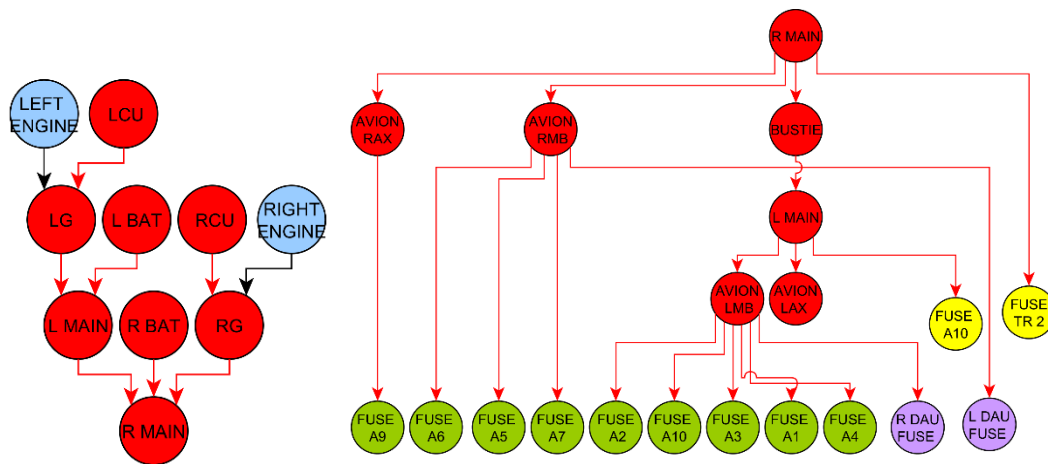


Figure 5 Predecessors (left) Successors (right)

Item-function relations

Function modeling serves in this case as powerful mean to analyze particular failure mode. Further, Integrated method includes (beside other things function) item extended criticality evaluation (see Chapter 5). As it is stated above Items contributing to the function performance carries share of function criticality. It is based on various factors- detectability, occurrence, node topology parameter and severity of failure consequence. Severity is based on item level of contribution to function(s) provision. Function base modeling provides item interconnection to the system function through the predecessor/ successor sequence.

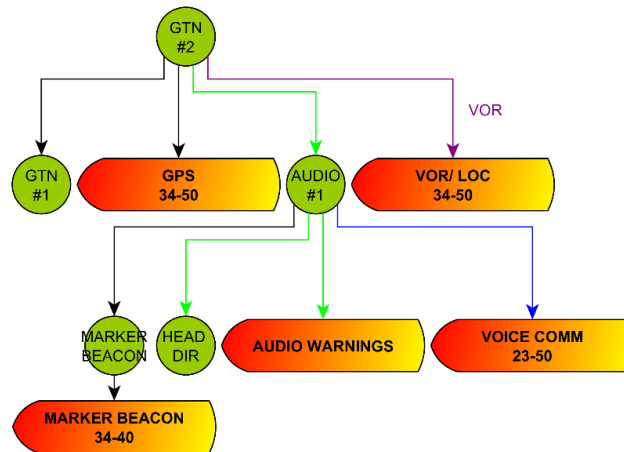


Figure 6 Case study GTN #2 succeeding function

In combination with knowledge database (Full doctoral thesis **Appendix A**), integrated method provides items relation to the function and their(s) preliminary classification. Knowledge database also provides preliminary severity membership volume for fuzzy criticality assessment. This input represents expert knowledge (analyst is able to adjust this volume to better correlation with evaluated system).

4.2.3 Rough tree and recursion algorithm

A tree in graph theory is a connected graph with no cycles, so it is acyclic. Trees are important to the structural understanding of graph and to the algorithmic of information processing, and they play a central role in the design and analysis of connected networks. [10]

From the system engineering point of view, trees are already essential part of particular failure mode analysis. Fault tree analysis proceeds by determining how failure can be caused by individual or combined lower level failures or events. Creating FTAs is difficult deductive process. It involves deep understating of system functions, mutual interconnection. Function base modeling presented in this doctoral thesis covers all of it. Through the local system model it is possible to obtain mutual influence of items toward particular items, failure propagation toward assessed failure mode.

Recursive algorithm

By using system model in the form of graph based data structure it is possible to create a rough fault tree. The term rough implies that fault tree has to be inspected before it could be incorporated in the formal analysis. Integrated method contains simple recursive algorithm designed to evaluate particular failure (due to function based modeling).

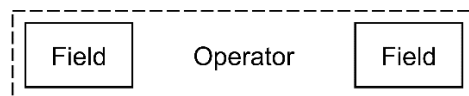


Figure 7 Recursive algorithm block- Field-operator-field

Recursion process is a procedure which goes through the data structure step by step. A step involves re-calling of the procedure itself. A procedure is established as a set of steps defined by a set of rules. To run a procedure means that to perform a step and follow the given rules.

Process could be described by using the linguistic terms. Process asks to a given node- what is the failure probability that system is not working to the given item level? This probability depends on a given node failure rate and failure rate of preceding nodes combination. When inputs to node are of the same type- it corresponds with FTA gate AND (input A and B have to fail) and when inputs are of different type- it corresponds with FTA gate OR (input A or B have to fail).

When a node is terminal, it depends only on its own failure rate. Recursive process is possible to define by two parameters- Base case (Rule terminating the recursive process) and Set of rules (It drives a case toward the base case).

Failure mode evaluation starts with Given function- than it goes “back” through the system model using the set of rules express in doctoral thesis by Recursive algorithm block. It uses local tree data structure. Block uses tree data structure. It provides a way how to evaluates relation between nodes. This relation depends is expressed by a given operator. The left field of recursive algorithm block (Figure 7) is for **assessed** node and the right filed is for **preceding** node or set of nodes. Operator depends on type of inputs.

Operator OR is applied when there is a Single input (Failure of both nodes results in failure up to given level), Multiple inputs of different type (Failure of any nodes results in failure up to given level) or if a node is defined as OR gate for preceding nodes.

Operator AND is applied when there is a Multiple inputs of same type (There has to be failure of all input nodes) or a node is defined as AND gate for preceding items.

In the case there are multiple inputs right filed (of the recursive algorithm block) is filled by lower level recursive algorithm block. In the case there are multiple inputs right filed (of the recursive algorithm block) is filled by lower level recursive algorithm block

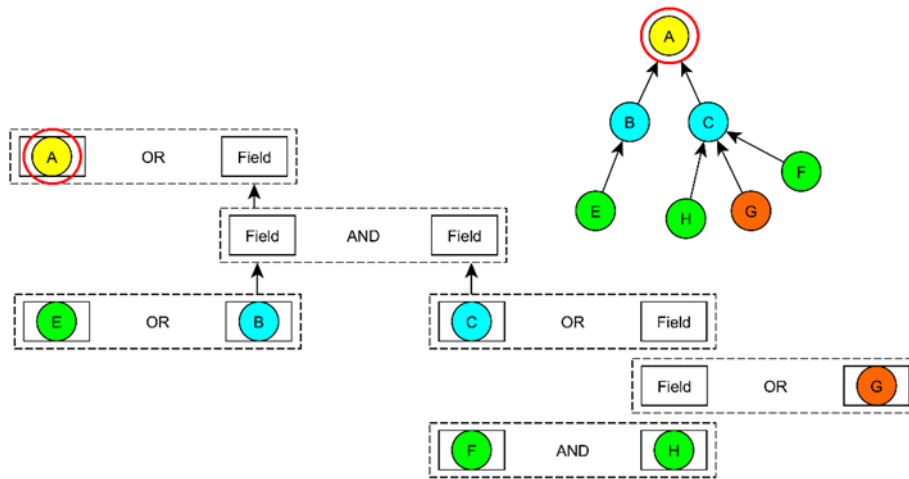


Figure 8 Recursive algorithm block- complex inputs example

4.2.4 Graph model structure evaluation

Betweenness centrality

BC of a node n is computed in the process as:

$$C_B(n) = \sum_{s \neq n \neq t} \left(\frac{\sigma_{st}(n)}{\sigma_{st}} \right) \text{ Equation 1}$$

Where s, t are nodes in the graph different from n . σ_{st} denotes number of shortest path from s to t . $\sigma_{st}(n)$ is the number of paths from s to t that n lies on. BC is computed only for graphs that do not contain multiple edges. The betweenness value for each node n is normalized by dividing by the number of node pairs excluding n : $(N - 1)(N - 2)/2$ where N is the total number of nodes in the connected component that n belongs to. Thus, the betweenness centrality of each node is a number between 0 and 1. [21] The betweenness centrality of a node reflects the amount of control that this node exerts over the interactions of other nodes in the network. [22]

Closeness centrality

CC of a node n is defined as the reciprocal of the average shortest path length. It is defined as:

$$C_{BC}(n) = \frac{1}{avg(L(n, m))}$$

Where, $L(n, m)$ is the length of the shortest path between two nodes n and m . The CC of each node is number between 0,1 [23]. Unlike betweenness centrality, closeness centrality is a measure of how particular function are tied together through the function of particular item or items. Closeness centrality ranking determines node importance due to function concentration.

Subgraph Centrality [25]

Method for characterizing nodes in network according to the number or closed walks starting and ending at the node. Close walks are appropriately weighted such that their influence on the centrality decreases as the order of the walk increases. These closed walks are directly related to the subgraphs of network. Subgraph centrality of the node is i as the sum of closed walks of different lengths in the network starting and ending at node i . The contribution of these closed walks decreases as the length of the walks increases. That is, shorter closed walks have more influence on the centrality of node than longer closed walks.

Subgraph centrality of the vertex i as the sum of close walks of different lengths in the network starting and ending at vertex i .

$$C_S = \sum_{k=0}^{\infty} \frac{\mu_k(i)}{k!} \text{ Equation 2}$$

$$\mu_k(i) = (A^k)_{ii} \text{ Equation 3}$$

Number of closed walks of length k starting and ending on edge i in the network is given by local spectrum moment $\mu_k(i)$, which are simply defined as the i th diagonal entry of the k th power of the adjacency matrix A .

Detailed description of subgraph centrality is provided in ESTRADA E., RODRÍGUEZ- VELÁZQUEZ J., Subgraph centrality in complex networks, Physical Review E 71, 056103, 2005 [25]

Centroid value

The centroid value is complex centrality index. It is computed by focusing the calculus on couples of nodes (v, w) and systematically counting the nodes that are closer (in the term of shortest paths) to v or w . The calculus proceeds by comparing the node distance from other nodes with the distance of all other nodes from the others, such that a high centroid value indicates that a node v is much closer to other nodes. Thus, the centroid value provides a centrality index always weighted with the values of all other nodes in the graph. Indeed, the node with the highest centroid value is also the node with the highest number of neighbors (not only first) if compared with all other nodes. In other terms, a node v with the highest centroid value is the node with the highest number of neighbors separated by the shortest path to v . The centroid value suggests that a **specific node has a central position within a graph region characterized by a high density of interacting nodes**. Also here, **high and low values are more meaningful when compared to the average centrality value** of the graph G calculated by averaging the centrality values of all nodes in the graph. [24]

$$C_{cen}(v) = \min(f(v, w): w \in V(v)) \text{ Equation 4}$$

Where: $f(v, w) = \gamma_v(w) - \gamma_w(wv)$ and $\gamma_v(w)$ is the number of vertex closer to v than w .

How to interpret Centroid value in airborne system application?

Particular sub-system or item is functionally capable to influence other system and modules. Thus, item with high centroid value, compared to the average centroid value of the network, will be possibly involved coordinating the functionality of other highly connected items. A network with a very high average centroid value is more likely influencing functional units or modules. It is useful to compare centroid value to other means detecting dense regions in graph. [Inspired by 24]

4.3 EXTENDED CRITICALITY

System safety and reliability assessment system is standardly derived from certain attribute- probability that item (or system) could perform required function (probabilistic reliability). The concept of reliability as a probability means that any attempt to quantify it must involve the use of statistical methods. Engineers try to ensure one hundred percent reliability, but experience tells us it is not always possible. Therefore, reliability statistics are usually concerned with probability values which are very high (or very low: probability that a failure occurs, which is 1- reliability). Quantifying such numbers brings increased uncertainty, since it needs more corresponding information. Other sources of uncertainty are introduced because reliability is often about people who make and people who use the product, and because of the widely varying environments in which typical products might operate. [14]

The significant degree of uncertainty is brought to reliability assessment by its definition. In the case of general aviation airborne system degree of uncertainty rises because of non- relevant reliability data or its absence. As it was mentioned in doctoral thesis introduction, the absence of detailed studies focused on probability of successful performance of an airborne system at any time, makes safety assessment inconclusive. The successful performance of any system depends on the extent to which reliability is designed and built. In the real conditions, even almost identical system, operating under similar conditions will have different life-time. Therefore, the failure of a sophisticated systems, e.g. the airborne systems are described only probabilistically. As it was mentioned above, integrated method intent to adopt descriptive attributes in order to evaluate system. Extended criticality and robustness numbers are built on expert knowledge (designers, maintenance personal, flight crew).

To handle expert knowledge gained based on critical review as linguistic terms integrated methods uses fuzzy logic. Fuzzy criticality assessment was used and published (for example [3], [4], [5], [6]) before by several researchers and development groups. However, doctoral thesis aims to extend this concept as integral piece of larger method and adjusted for airborne system safety and reliability assessment application.

Extended criticality evaluation concept is way how to overcome these problems. Criticality by MIL-STD-1629A definition is a relative measure of failure mode its frequency of occurrence. Then criticality analysis is a procedure by which each potential failure mode is ranked according to the combined influences (by MIL-STD-1629A [2] definition severity and probability of occurrence).

Extended criticality level (and number) is generally descriptive attribute of item (sub-system) contribution to system (aircraft, high level function) state of being critical to **MSO** (sustain safe flight and landing). This doctoral thesis intends to extend criticality level concept by combining different influences based on precise critical review.

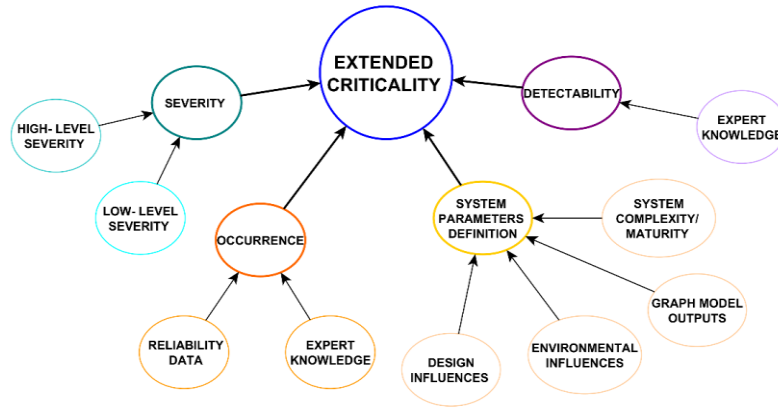


Figure 9 Combined influences on the extended criticality

Several aspects influence item criticality. These influences are projected in to set of inputs. There are four inputs in to the fuzzy criticality evaluation (see Figure 46). Severity, occurrence, detectability and system topology are those inputs. Following chapters describes in the process of extended criticality evaluation, process of fuzzification, fuzzy inference and de-fuzzification.

4.3.1 Severity

Severity is defined by the MIL-STD-1629A as the consequences of a failure mode. It considers the worst potential consequences of a failure, determined by the degree of injury, property damage, that could ultimately occur. In system architecture definition of an aircraft, main, support and additional functions were established. Failure mode consequences are possible to express by **High-level severity (HLS)** established according to its relation to **MF, SF, AF** and **MSO**.

Function severity (FS) is related to the airplane function high and low critical functions (MF, SF). Severity distribution to the separated levels allows precisely describe failure mode consequences for separated system and airplane itself.

As at it was mentioned multiple times, system items are interconnected in order to provide a given function. Therefore, item could be associated with various functions. Item severity of potential failure depends on its allocated functions, their severity respectively (FS). Appendix A provides function severity for several systems. Term High-level severity (HLS) is in integrated method related to the item. Process of function severity is described in previous sub-chapter. Item HLS strongly depends on system configuration. Item function could be designed as redundant or could be backed up by auxiliary system or configuration.

4.3.2 Occurrence

Reliability is the probability of successful performance of a system in any time. The successful performance of any system depends on the extent to which reliability is designed and build in to it. In practice, it is observed that even seemingly identical system, operating in under similar conditions, fail in different times. [9]

As stated earlier, in the field of doctoral thesis interest (VLA, LSA, UAV, etc.) it is not possible provide relevant reliability data. Yet, precise reliability analysis should determine the possibility and probability of particular failure mode. There is a need to somehow establish at least probability of failure mode occurrence and probability of failure mode detectability. These influences contribution to the item extended criticality has to be taken under consideration. Occurrence levels are used as strong inputs to the fuzzy criticality assessment representing (precisely- available data or linguistically based on expert knowledge) probability of occurrence.

4.3.3 Detectability

Probability of failure mode detection is crucial factor influencing item or system criticality. It is extremely difficult and highly expensive to establish precise probability of failure mode detection using the reliability and maintainability testing.

Nevertheless, there is a possibility to establish change of failure mode detection using the expert knowledge expressed in form of linguistic terms and score tables. Doctoral thesis adopting different criteria for item failure mode detectability reflecting various type of systems. Chapter 5.5.1. Detectability defines score tables for particular types of systems. Resulting scores are taken into a fuzzification process. Doctoral thesis established detectability levels- **Latent**, **low** detectability, **moderate** detectability and **very high** detectability. These levels are defined by score range. Worst case scenario- latent failure level equals FAA AC23.1309-1E definition- A failure is latent until it is made known to the flight crew or maintenance personnel.

4.3.4 Node topology parameter

Node topology parameter (NTP) serves as one of the inputs to the fuzzy criticality assessment described in following chapters. It express node interconnections in the system. NPT reflects node influence on local and global level. It is based on previously defined and describe parameters- betweenness centrality, subgraph centrality and centroid volume which reflect node position in the network. To determine relative importance is used Metfessel allocation. In this case analyst has to quantitatively evaluate importance of parameters based on their influence on network (airplane systems).

4.4 SYSTEM ROBUSTNESS

Integrated method has to implement expert system parameters definition into a process of system evaluation. Every particular system has its own characteristics. System items should be separated avoiding common cause failure. In case of essential system (related to the function severity) required redundancy has to be ensured.

Item maturity, process of design, complexity and previous experiences with item usage in similar condition has to be taken under consideration. System and its items have to meet environmental and software technical condition necessary for aviation application. Environmental requirements ensure that item is not vulnerable against changing temperature, humidity, attitude, inflected vibration, voltage spikes and many more.

Integrated method developed in doctoral thesis is partially designed as sort of expert system. Expert knowledge is handled in the form of linguistic terms. International standard IEC 61508 [53] published by the International Electro- Technical Commission contains questionnaire covering basic system parameters definition- Separation/ Segregation, Diversity/ redundancy, Complexity/ design/ maturity, Assessment, Environmental control/ testing. This standard is design as basic functionality safety standard applicable to all kinds of industry. It is called Functional Safety of Electrical/Electronics/Programmable Electronic Safety-related Systems.

For doctoral thesis purposes IEC 61508 questionnaire is significantly modified for airborne system application (it is partially inspired by [26]). Each system parameters category (Separation/ Segregation, Diversity, Redundancy, etc.) is adjusted for basic types of system- mechanically based, electrically based, electronically based, hydraulics. Evaluation of questionnaire answers is newly designed for aviation application. Answer evaluation uses fuzzy logic to express expert knowledge (using fuzzy four fuzzy sets- No, Rather no, Rather no and Yes). Output of system parameter evaluation is robustness numbers for particular category. This numbers express property of system being strong and resistant in design.

Term robustness should be taken with a reserve. It could be defined as “the ability of system to resist change without adapting its initial stable configuration”. Although aircraft and its systems could adapt to the emergency situations applying emergency procedures and remedies, it should be designed as robust and reliable as is reasonable practicable. Robustness number allows to evaluate level of system (and aircraft) separation/ diversity/ redundancy/ complexity/ maturity/ environmental.

Robustness numbers provides an additional and advisory means how to describe evaluate system. These data could be stored for further processing. In future it is possible to compare scores between system of similar applications. It is possible, that questionnaire will be modified in order to elevate its correlation with reality.

4.5 FUZZY EVALUATION PROCESS

It is a process of evaluating inputs to and output through fuzzy sets. The most used inference technique is Mamdani. Developed by Professor Ebrahim Mamdani of London university in 1975. Process consist of four steps- fuzzification process (particular inputs used in integrated method are presented above), rule evaluation, aggregation of rule outputs and de-fuzzification.

Crisp inputs (expressing expert knowledge and assessment) are numerical volumes of discourse. Each type of input has special range of the discourse. Crisp inputs are fuzzified against the appropriate fuzzy set. These inputs fuzzified against the appropriate particular linguistic fuzzy sets. Fuzzy rules consist of antecedent (expressed IF) and consequent (implication, expressed THAN). Antecedent part could consist of multiple parts, which are expressed in the configuration of fuzzy operators (AND, OR).

Fuzzified inputs are applied to the antecedents of the fuzzy rule base to obtain single that represents the result of rule antecedents. Resulting number is applied in consequent part of fuzzy rule. Fuzzy rule base contains number of particular rules. Therefore, process of aggregation is used. It is a process of unification of the outputs of all rules. Each rule (clipped and scaled) consequents are combined into a single fuzzy set. Resulting number has to defuzzified to obtain a crisp number expressing output (critically, robustness). It is a process of aggregation of fuzzy set into this single crisp output. Based on [20]

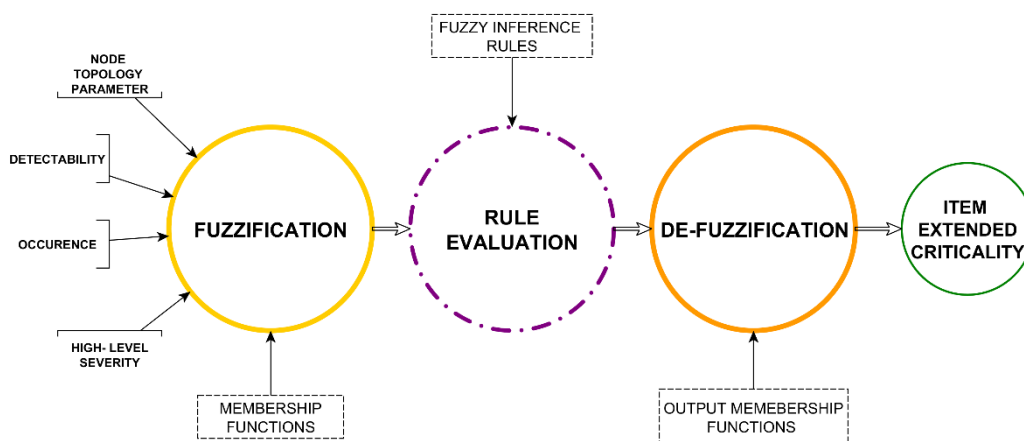


Figure 10 Fuzzy inference process

4.5.1 Fuzzification

It is done because of simple reorganization that number of the quantities which are considered to be a crisp and deterministic, but they are not deterministic at all. Because they carry considerable uncertainty. If the form of uncertainty happens to arise because of imprecision, ambiguity, or vagueness, then the variable is probably fuzzy and can be represented by a membership function. [8] Fuzzification process includes the Node topology parameter, High-level severity, Occurrence, Detectability inputs to into their

fuzzy representation which can then be matched with the premises of the rules in the rule base. Fuzzification is done in order to transform crisps into a membership degree. It should express how inputs belong into linguistic terms used in the rules.

4.5.2 Inference rules

It is a platform for abstracting information based on linguistic terms (expert's judgment) the fuzzy rules base is used. Interaction between various failure modes and effects are represented in the form of fuzzy rules. "If-then" rules describe the riskiness of the system for each combination of input variables and they are easily implemented.

It presents the way of thinking, that then we know something (hypothesis, premises) then it is possible to infer or derive to the conclusion (consequent fact). Fuzzy base rule concept is most effective in the case of complex system modelling, when the system is observed by people because it makes use of linguistic variables can be naturally represented by fuzzy sets and logical connectives of these sets. Rules are based on natural language representations and models, which are themselves based on fuzzy sets and fuzzy logic. [7]

The fuzzy level of understanding and describing a complex system is expressed in the form of a set of restrictions on the output based on certain conditions of the input. Restrictions are generally modelled by fuzzy sets and relations. Restriction statements are connected by linguistic connectives such as "and, or, or else." [7] Extended criticality fuzzy rule base rules respect relationship between classes, probabilities, severity of failure established in FAA AC23.1309-1E [1]

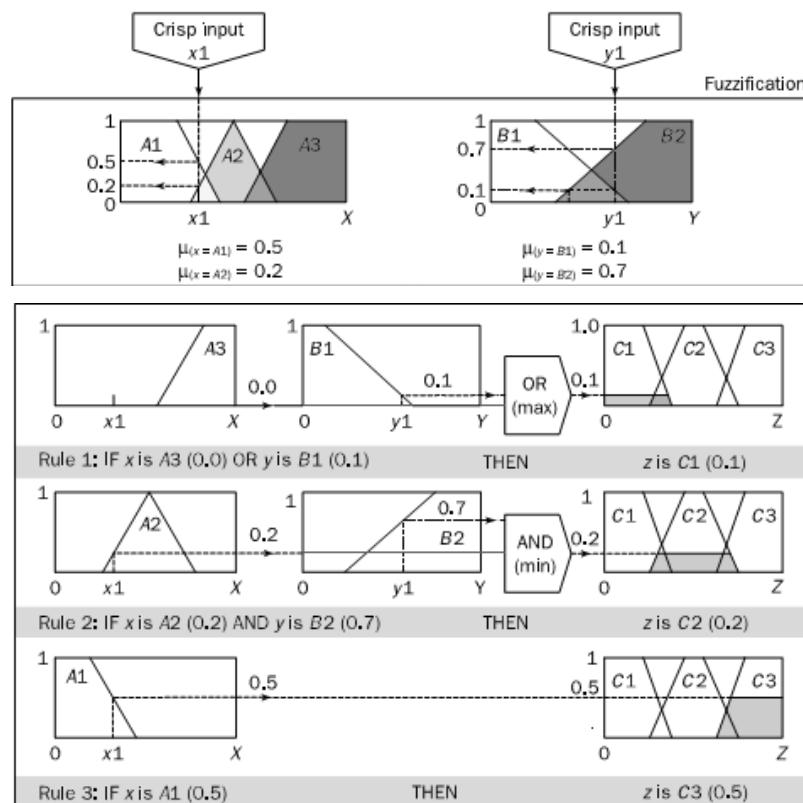


Figure 11 Fuzzy logic rule application [20]

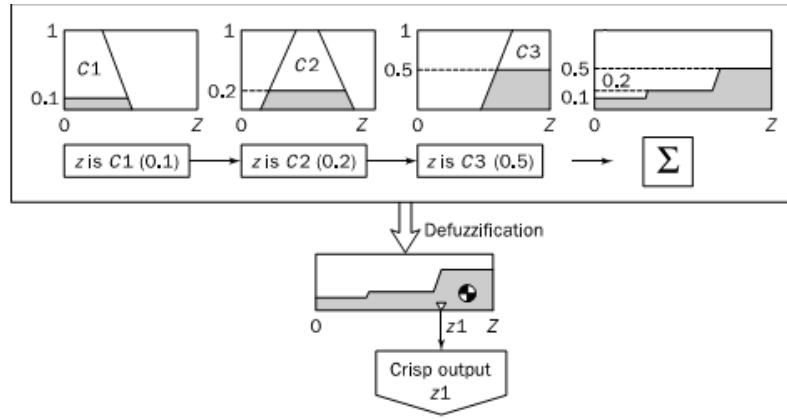


Figure 12 Fuzzy logic rules aggregation and de-fuzzification [20]

4.5.3 De-fuzzification

De-fuzzification is done in the order to gain the fuzzy process single scalar quantity output. It processes to obtain crisp ranking from fuzzy conclusion set. Ranking represents the extended criticality level of the failure mode for potential corrective or remedial action. The de-fuzzification process requires, decipher the meaning of the fuzzy conclusion and their membership and resolve conflict between results. Doctoral thesis will find proper de-fuzzification method. Then it will prepare way how to process gained criticality. FCA will be part of larger safety and reliability evaluation process.

It is used centroid technique, probably the most used defuzzification technique. It finds where vertical line would slice the aggregate set into two equal masses. Mathematically this center of gravity (COG) can be expressed as follow.

$$COG = \frac{\int_a^b \mu_x(x)xdx}{\int_a^b \mu_x(x)dx} \text{ Equation 5}$$

In theory, the COG is calculated over a continuum of points in aggregate output membership function. It is possible to obtain COG by calculating it over a sample of points. [20]

4.6 INTEGRATED METHOD PROCESS

I. System Definition

- Type (ATA 100 coding)
Electrical, Hydraulic, Navigation, etc.
- Allocated function (Using **Appendix A**)
Preliminary classification based on knowledge database, Limit HLS
- Robustness parameters
Separation/ Segregation, Diversity/ Redundancy, Complexity/ Design/ Maturity/ Experience, Procedures/ Maintenance/ Human Interface, Environmental Control

II. Items

- List of items
- System interconnections and allocated function (**Graph model**)
- Item potential failure modes (Using **Appendix A**)
- Item occurrence level
- Item detectability
- Item **HLS** (Relation to the allocated function)

III. System model

- Allocated function failure modes and preliminary failure rates
- Centrality, Topology
- Item **NTP**

IV. Fuzzification process

- Items extended criticality
- System robustness and particular parameters

V. Reports

- List of most critical items
- System parameters
- System model accessible for further evaluation
- Pseudo FMEA structured results

5 MAIN RESULTS

5.1 CASE STUDY DEFINITION

As a case study was chosen Institute of Aerospace Engineering VUT 486-DX4. It is a testing platform used for maintenance, safety and reliability analysis and advanced airborne diagnostic methods development application. It was developed on BUT Institute of Aerospace Engineering. The testing platform is used in several doctoral theses to demonstrate effectiveness of particular system engineering technique. Twin engine airplane is designed as EASA CS-23 Commuter Class IV.

Each system has been selected to demonstrated particular type of airborne system. Avionics system is the most complex system. It consists of various types of items (aero-metrical, electronics, air pressure, etc.). It is directly connected to the several main function. Avionics system provides navigation, communication, information about aircraft horizontal and vertical orientation. Flight crew workload is highly related to the system functionality.

Pitot- static system provides static and dynamics pressure to the significant avionics indicators which provide information about airspeed, altitude and vertical speed. It consists of pressure tubes, inputs, tubes and mechanical valves. Elevator trim system controls trailing edge of a control surface in order to stabilize aircraft in a desired attitude. Potential failures like disengagement could result in flutter occurrence with catastrophic or hazardous outcome. System represents electromechanical system. Source of tab motion is provided by actuator and then transferred through mechanical block into a tab movement.

Engine indication system provides indication of present state of a given engine. It consists of dozens of sensors (temperature, pressure, etc.). Its functionality strongly depends on data acquisition unit functionality which process sensors inputs and provides indication. It is a typical example how function could be clustered by main processing unit.

Electrical system serves as airborne source of electrical power. Its functionally directly influence other system functions. It is basically backbone of any larger airplane.

Case study systems:

- **Electrical system-** It consist of 15 nodes and 17 edges. It is convectional twin engine electrical system with two generators and two airborne batteries. Electrical power is distributed thought two main buses. Those buses could be mutually connected by BUSTIE contactor. (see figure on the right)
- **Avionics system-** It consist of 39 nodes and 40 edges. There are 11 multi edges pairs (that indicates complex interaction). Main items of avionics system are GTN 1/2.
- **Elevator trim system-** It consist of 13 nodes and 14 edges. It is designed as electro-mechanical system. Sources of trim movement are actuators connected to trim by mechanical levers.
- **Engine indication system-** It consist of 26 nodes and 28 edges. It is designed to collect measured engine parameters in order to indicated its status provide cautions and warnings.
- **Pitot- static system-** It consist of 6 nodes and 8 edges. System is design to provide static and dynamic pressure to the avionics system.

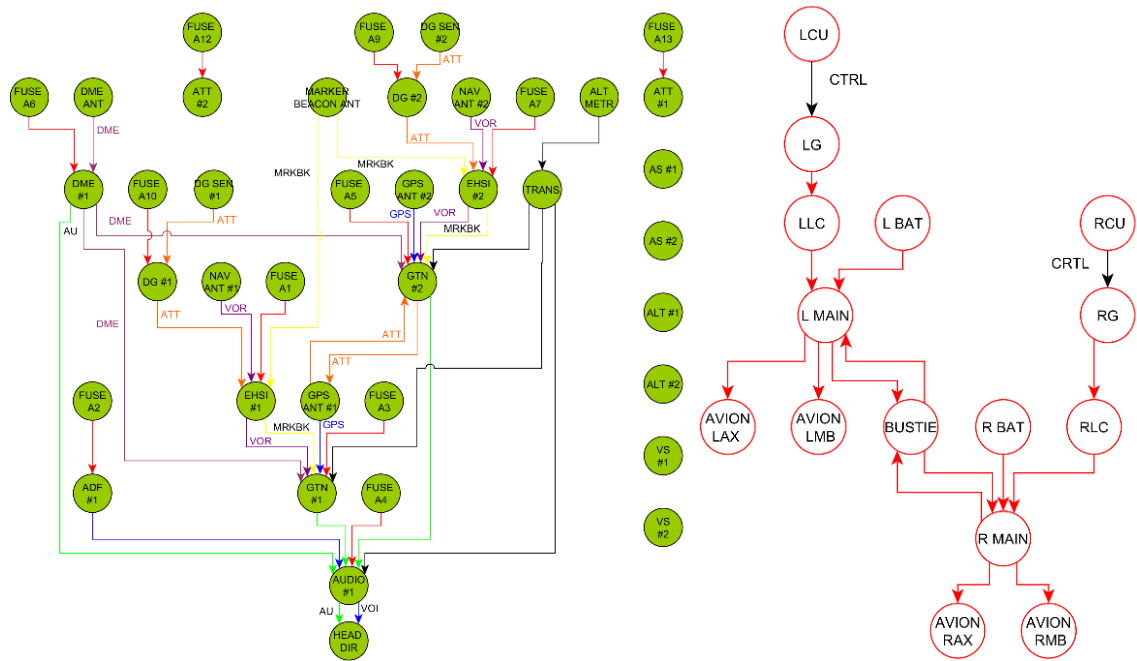


Figure 13 Case study- Avionics system (left), Electrical system (right)

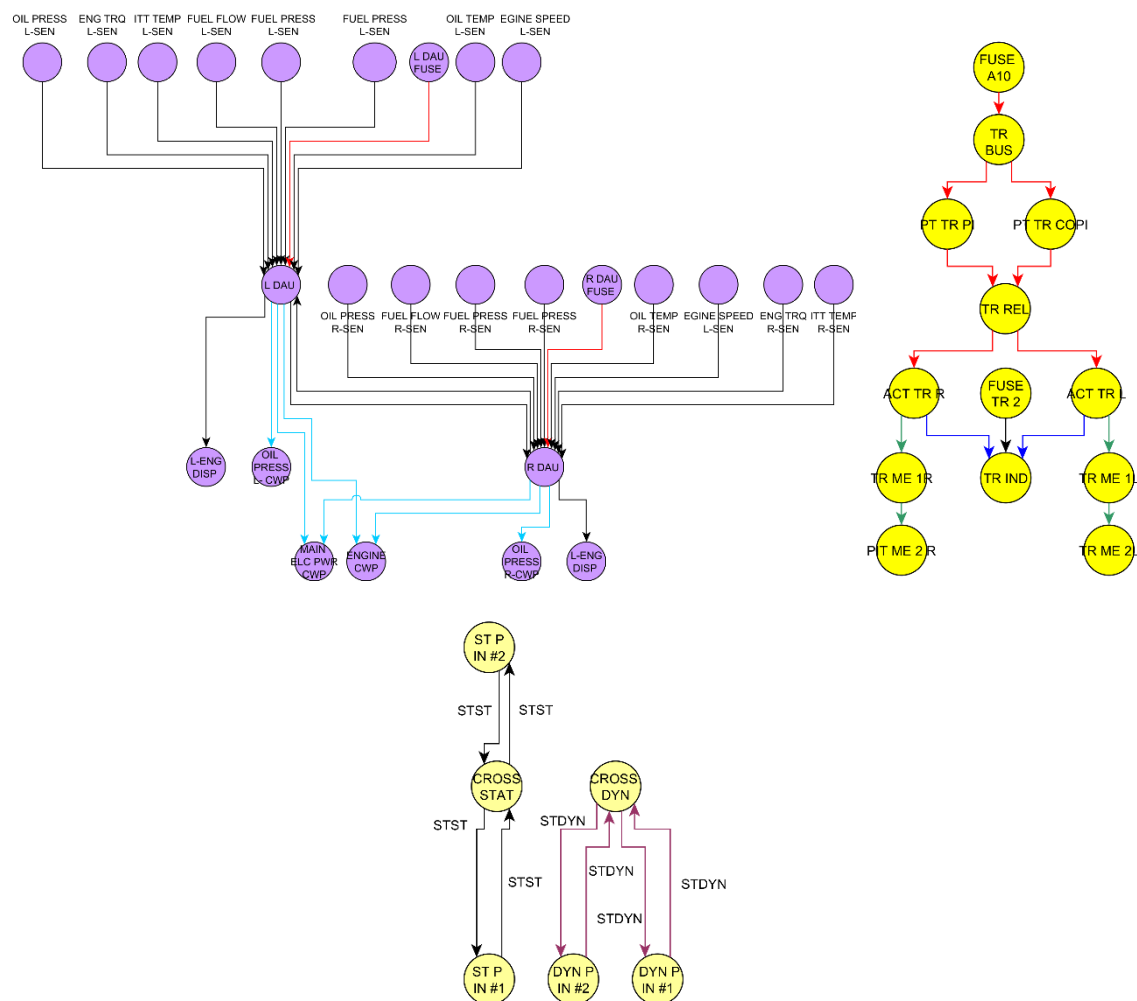


Figure 14 Case study- Engine indication system (left), Elevator system (right), Pitot-static (bottom)

5.2 EVALUATION PROCESS RESULTS

This chapter summarizes case study evaluation results. Case study consist of five selected systems. Results show integrated method potentials despite the fact that these systems are simplified and restricted.

Results provide detailed description of system interconnection, identify important items and weak parts of systems. Results would be quite useful for formal safety and reliability assessment.

5.2.1 Global model parameters results

Case study consists of 102 items, 132 interconnections in order to provide 25 functions. Systems are evaluated only in flight mode (due to scale limitation). Systems are physically located in 11 zones (from cockpit, though fuselage to horizontal stabilizer, including engine units and wings).

<i>Number of nodes</i>	102	<i>Diameter</i>	12
<i>Number of edges</i>	132	<i>Multi edges node pairs</i>	11
<i>Average number of neighbors</i>	2,37	<i>Shortest paths</i>	1193 (11%)
<i>Clustering coefficient</i>	0,015	<i>Zones</i>	110, 220, 230, 310, 331, 341, 410, 510, 610, 720, 730

Table 2 Case study global model evaluation- basic parameters

5.2.2 Case study global model evaluation- basic parameters

Extended criticality evaluation identified as most important item (in given set of systems) FUSE A10 and TR REL. These items directly influence both elevator trims functionality. Generally, fuse has failure rate suitable for MAJOR consequences (EASA CS-23, class IV) and relatively low likelihood of failure detection. As most critical items of electrical system are identified LLC and RLC contactors. These items connect generator with electrical network. There is no direct indication of LLC and RLC malfunction (in case study design). As most critical items of avionics system are identified EHSI units which are associated with high severity function (Attitude information FS=10 in IFR conditions).

<i>Most critical items (Global)</i>	#	<i>Name</i>	<i>WNTP</i>	<i>HLS</i>	<i>Occurrence</i>	<i>Detectability</i>	<i>Extended criticality</i>
	1	FUSE A10 (TRIM)	40,90	7,50	2,38E-06	7,0	5,000815662
	2	TR REL (TRIM)	40,90	7,50	1,86E-06	5,5	5,000815662
	3	LLC (ELEC)	36,97	3,50	1,06E-04	6,0	5,000815662
	4	RLC (ELEC)	36,94	3,50	1,06E-04	6,0	5,000815662
	5	EHSI #2 (AVIO)	18,32	4,50	3,00E-04	3,5	4,375413348
	6	EHSI #1 (AVIO)	18,00	4,50	3,00E-04	3,5	4,350370057
	7	TR BUS (TRIM)	42,15	7,50	2,50E-07	6,5	4,311464805
	8	L MAIN (ELEC)	56,80	3,00	2,50E-07	6,5	4,252264671

Table 3 Case study global model evaluation results- extended criticality list

DAU units are quite logically identified as most critical items of engine indication system. These units cluster system functionality (collecting and processing of engine parameters). However, they are associated only with low severity function (mainly MINOR). Most critical items (based on extend criticality) of Pitot-static system are identified CROSS STAT/ DYN valves (not on this list) and sixteenth and seventeen globally.

5.2.3 Model structure and topology results

Table 49 shows importance lists based on two model centrality parameters. On the left side are stated most important items on the local level. It is based on subgraph centrality which favours local importance of interconnection over global. DAU units are identified as most important. Integrated avionics units (GTNs) are logically identified as important. They are associated with multiple functions (densely interconnected with other items).

Name	#	Local importance (SubG)	#	Name	Global importance (BC)
R DAU (ENGIND)	1	24,95	1	L MAIN (ELEC)	0,0436
L DAU (ENGIND)	2	24,77	2	R MAIN (ELEC)	0,0365
GTN #1 (AVIO)	3	16,21	3	BUSTIE (ELEC)	0,0238
GTN #2 (AVIO)	4	16,19	4	AVION LMB (ELEC)	0,0226
AUDIO #1 (AVIO)	5	15,92	5	AVION RMB (ELEC)	0,0186
DME #1 (AVIO)	6	10,69	6	R DAU (ENGIND)	0,0181
AVION LMB (ELEC)	7	9,67	7	L DAU (ENGIND)	0,0181
TRANS (AVIO)	8	9,37	8	LLC (ELEC)	0,0160

Table 4 Case study global model evaluation results- node interconnection

Right side of same table shows most important items based on global importance. It is based on betweenness centrality. As most important items are identified L MAIN and R MAIN buses. Through these buses is electrical power distributed to particular buses (AVION LMB/ RMB) and to the loads. BUSTIE contactor is identified as third most important item. It interconnects both main buses in the case of one generator failure (or distribution sequence to it). Electrical system is dominant in this importance list. It is logical, electrical system is connected to majority of airborne systems.

5.2.4 Robustness parameters

Case study systems were evaluated by using robustness fuzzy assessment. Questionnaire answers express expert judgement. It provides additional information about system designed. Complete answers are stated in Appendix C.

System	Separation/ segregation	Diversity/ redundancy	Complexity/ design/ maturity/ experience	Environmental control/ testing
Elevator trim	Score. 0,775 Level. HIGH	Score. 0,0967 Level. LOW	Score. 0,0967 Level. LOW	Score. 0,653 Level. HIGH
Electrical	Score. 0,773 Level. VERY	Score. 0,5 Level. MEDIUM	Score. 0,495 Level. MEDIUM	Score. 0,715 Level. HIGH
Avionics	Score. 0,901 Level. VERY HIGH	Score. 0,633 Level. HIGH	Score. 0,903 Level. VERY HIGH	Score. 0,743 Level. HIGH
Pitot-static	Score. 0,5 Level. MEDIUM	Score. 0,35 Level. MEDIUM	Score. 0,0967 Level. LOW	Score. 0,686 Level. HIGH
Engine indication	Score. 0,686 Level. HIGH	Score. 0,0983 Level. LOW	Score. 0,5 Level. MEDIUM	Score. 0,659 Level. HIGH

Table 5 Case study- system robustness parameter

As a most complex system is identified avionics system with various cross connection between avionics units. However, avionics system is designed as separated, system is also partially designed as redundant and diverse.

5.2.5 Rough tree evaluation

Function in graph theory based on models are evaluated through the recursive algorithm logic. It provides initial information for formal failure mode evaluation. Results indicates that PITCH TRIM L/R are outside allowable probability limit for failure mode with MAJOR consequences (EASA CS-23, class IV).

<i>Function</i>	<i>Failure mode</i>	<i>Classification</i>	<i>Probability</i>	<i>Result</i>
PITCH TRIM L 27-30a	<i>Loss of function/ Jam</i>	MAJOR	$2,45.10^{-5}$	OUTSIDE RANGE
PITCH TRIM R 27-30b	<i>Loss of function/ Jam</i>	MAJOR	$2,45.10^{-5}$	OUTSIDE RANGE
PITCH TRIM IND 27-30c	<i>Loss of function</i>	MINOR	$2,41.10^{-6}$	IN RANGE
AUTOMATIC DIRECTION FINDER 34-50	<i>Loss of function</i>	MINOR	$1,94.10^{-5}$	IN RANGE
AIRSPPEED INDICATION 34-10	<i>Loss of function</i>	IFR/ HAZARDOUS	$6,59.10^{-9}$	IN RANGE
VERTICAL SPEED 34-10	<i>Loss of function</i>	MINOR	$1,08.10^{-8}$	IN RANGE
ALTITUDE INDICATION 34-10	<i>Loss of function</i>	IFR/ CATASTROPHIC	$6,92.10^{-10}$	IN RANGE
GPS 34-50	<i>Loss of function</i>	MINOR	$2,54.10^{-9}$	IN RANGE
VOR/LOC 34-10	<i>Loss of function</i>	MINOR	$1,36.10^{-7}$	IN RANGE
ATTITUDE INFORMATION 34-20	<i>Loss of function</i>	IFR/ CATASTROPHIC	$1,41.10^{-18}$	IN RANGE

Table 6 Case study rough tree evaluation

These rough trees are prepared only for loss of function failure modes. Failure modes are evaluated in relation with most severe classification (in the IFR conditions in the case of altitude indication, airspeed indication and attitude indication).

6 CONCLUSION

Doctoral thesis outcome

Doctoral thesis establishes integrated method for safety and reliability assessment of airborne systems within the scope of general algorithm. It utilizes function based modeling, Graph theory and Fuzzy logic in order to create advanced and complexed mean of airborne system analysis.

Combination of function oriented modeling and graph theory usage allows modeling the airborne systems in the form of accessible data structure. This model contains functions allocated to the given system and items interconnected in order to provide these functions. Global modeling enables to assess various systems and items interrelations. Graph theory application enables to evaluate particular item position and topology on the system and global level.

Doctoral thesis extends standard definition of criticality by adding new attributes to evaluated item. Extended criticality as a relative measure is based on item failure mode consequences, its frequency, likelihood of failure detection and overall influence on other items. Fuzzy evaluation is applied as mean of expert judgement processing. It allows to evaluate system even in the case of lack of relevant quantitative input data. Integrated method also provides additional mean how to evaluate system design. Fuzzy robustness assessment evaluates e.g. system diversity rate, redundancy, separation, environmental protection. Method processes expert judgment in the form of questionnaire and use fuzzy logic to obtain resulting robustness levels.

Doctoral thesis further provides extensive knowledgebase for each particular step of integrated method process. Appendix A provides severity classification knowledge base for selected airborne systems. Appendix B gives a review of basic item reliability data. Appendix C contains case study evaluation results and Appendix D robustness questionnaire.

Integrated method is successfully tested on the case study. For a case study was chosen the testing platform VUT 468-DX4. Its design is based on experience gained during multiple past projects and it provides clear idea of integrated method application.

Conclusion

Doctoral thesis fulfils its main objectives/ goals. Some intended means of integrated method had to be adjusted due to development process and results. However, in general integrated method is applicable and useful as it was intended in the proposal. In addition to the proposal, the doctoral thesis provides fuzzy robustness evaluation.

Future perspectives

Several perspectives for future development and improvements of integrated method designed in this doctoral thesis might be identified. Doctoral thesis established main idea- combination of function based modeling, graph theory application and fuzzy criticality and robustness evaluation. Currently the basic algorithm is created. However, process is atomized into separated parts (processed with different programs). In future, the process will be developed in to the form of standalone program with advanced front-end. Main attention might be given to the recursive algorithm proper coding. Doctoral thesis has established main idea of the algorithm. However, the algorithm should be properly coded in possible follow-up projects.

Future application of integrated method might result into the partial adjustments in order to enhance its applicability and the result consistence. The results of the integrated method should be stored because they will provide necessary feedback.

7 ACRONYMS AND ABBREVIATIONS

A/I	Acting items
AFM	Airplane Flight Manual
ARP	Aerospace Recommended Practice
ATA	Air Transport Association
ATC	Air Traffic Control
BC	Betweenness Centrality
CA	Criticality Analysis
CC	Closeness Centrality
CCA	Common Cause Analysis
CMA	Common Mode Analysis
COG	Center of Gravity
CS	Certification Requirements
DAU	Data Acquisition Unit
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FCA	Fuzzy Criticality Assessment
FCOM	Flight Operating Manual
FHA	Functional Hazard Assessment
FMEA	Failure Mode and Effect Analysis
FS	Function Severity
FTA	Fault Tree Analysis
GA	General Aviation
HLS	High- level severity
IFR	Instrument Flight Rules
IMC	Instrument meteorological conditions
LAX	Left Auxiliary bus
LCU	Left Control Unit
LG	Left Generator
LLC	Left Line Contactor
LMB	Left Main Bus (avionics)
MAU	Modern Avionics Unit
MF	Main function
MM	Mitigation mean
MSO	Main Safety Objective
MTBF	Mean Time Before Failure
NTP	Node topology parameter
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RAX	Right Auxiliary bus
RBD	Reliability Block Diagram
RCU	Right Control Unit
RG	Right Generator
RLC	Right Line Contactor
RMB	Right Main Bus (avionics)
RTCA	Radio Technical Commission for Aeronautics
SF	Support function
SSA	System Safety Assessment
SubG	Subgraph Centrality
UAS	Unmanned Aerial Systems
UAV	Unmanned Aerial Vehicles
VFR	Visible Flight Rules

8 REFERENCES

- [1] Advisory Circular FAA AC 23.1309-1E *System Safety Analysis and Assessment for Part 23 Airplanes*, Federal Aviation Administration, Washington D.C., 2011
- [2] MIL-STD-1629A *Military Standard Procedures for performing a failure mod, effect and criticality analysis*, Department of Defense Washington, DC USA, 1977
- [3] BOWLES, J.B. and PELAEZ, C.E., *Fuzzy logic prioritization of failures in a system failure mode, effect, and criticality analysis*, Reliability Engineering and System Safety, Vol.50, pp. 203-13
- [4] BRAGLIA, M. and FROSOLINI, M., *Fuzzy criticality assessment model for failure mode and effect analysis*, International Journal of Quality & Reliability Management, Vol.20 Iss 4, pp. 503-524
- [5] ROSS, T.J., *Fuzzy logic with Engineering Application*, McGraw-Hill, New York, N.Y., 1995
- [6] Rajiv Kumar Sharma Dinesh Kumar Pradeep Kumar, *Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling*, International Journal of Quality & Reliability Management, Vol. 22 Iss pp. 986-1004, 2001
- [7] NOVÁK, V., PERFILIEVA, I. and MOČKOŘ, J.: *Mathematical principles of fuzzy logic*, Dodrecht: Kluwer Academic
- [8] ROSS, T.J. *Fuzzy logic with engineering applications*. 2nd ed. Hoboken, NJ: John Wiley, c2004, xxi, 628 p. ISBN 0470860758-.
- [9] RAO, Singiresu S. *Reliability-based design*. New York: McGraw-Hill, c1992. ISBN 0-07-051192-6.
- [10] GROSS, J. L., YELLEN, J., ZHANG, P.; *Handbook of Graph Theory*, Taylor & Francis Group, LLC, 2014
- [11] THANG. J., *Mechanical system reliability analysis using combination of graph theory and Boolean logic*, Reliability Engineering and System Safety 72 (2001) 21-30
- [12] SHANNMON R.M., ANDREWS J.D., *New approaches to evaluating fault tree*, Reliability Engineering and System Safety 58 (1997) 89-96
- [13] MOIR, I., SEABRIDGE A., *Aircraft systems: mechanical, electrical, and avionics subsystems integration*. Bury St. Edmonds, U.K.: Professional Engineering Publishing, 2001, xxii, 344 p. ISBN 1563475065.
- [14] O'CONNOR, P.D., *Practical reliability engineering*. 4th ed. Chichester: John Wiley & Sons, 2002, 513 s. ISBN 0-470-84463-9.
- [15] MAINAN R., DUGAN J.B., COPPIT D., SULLIVAN K.J., *Combining Various Solution Techniques for Dynamic Fault Tree Analysis of Computer System*, High-Assurance Systems Engineering Symposium, 1998. Proceedings. Third IEEE International
- [16] LEUSCHEN, M. L.; WALKER, I. D.; CAVALLARO, J. R. *Robot reliability through fuzzy Markov models*. In: Reliability and Maintainability Symposium, 1998. Proceedings, Annual. IEEE, 1998. p. 209-214.
- [17] ZHNAG P., MA Q., *A Method of Evaluating Reliability of More-Electric-Aircraft Power System Using Node-Weight Network*, Advanced Materials Research Vols. 516-517 (2012) pp 1288-1291
- [18] MOIR, I. *Civil avionics systems*, 2003, Chichester: John Wiley, 2006, 395 p. ISBN 1 86058 342 3.
- [19] NASA System Safety Handbook vol2.: Aviliable from:
<https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150015500.pdf> [17. 8. 2018]
- [20] NEGNEVITSKY, Michael. *Artificial intelligence: a guide to intelligent systems*. 2nd ed. New York: Addison-Wesley, 2005. ISBN 0321204662.
- [21] Brandes, U.: *A faster algorithm for betweenness centrality*. J Math Sociol 25 (2001) 163-177
- [22] YOON J., Blumer, A., Lee, K.: *An algorithm for modularity analysis of directed and weighted biological networks based on edge-betweenness centrality*. Bioinformatics, 22 (2006) 3106-8
- [23] Newman, M.E.J.: *A measure of betweenness centrality based on random walks*. arXiv (2003) cond-mat/0309045

- [24] SCARDONI G., TOSADORI G., LAUDANNA C., FABBRI F., FAIZAAAN M., *CentiScaPe: Network centralities for Cytoscape*, Available from: <https://f1000research.com/articles/3-139/v2>
- [25] ESTRADA E., RODRÍGUEZ- VELÁZQUEZ J., *Subgraph centrality in complex networks*, Physical Review E 71, 056103, 2005
- [26] ZAKUCIA, J. *Metódy posudzovania spoľahlivosti zložitých elektronických systémov pre kozmické aplikácie*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2015. 120 s. Vedoucí dizertační práce doc. Ing. Jiří Hlinka, Ph.D.
- [27] IEC 61508-6: *Functional safety of electrical/ electronic/ programmable electronic safety-related systems* – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

9 PUBLICATION

- [PA1] JANHUBA, L.; NAVRÁTIL, J. METHODS FOR SAFETY AND RELIABILITY EVALUATION OF GENERAL AVIATION AIRCRAFT ELECTRIC SYSTEM. In Sborník příspěvků Mezinárodní Masarykovi konference pro doktorandy a mladé vědecké pracovníky 2014. Hradec Králové: MAGNANIMITAS. 2014. 2014. p. 1-11. ISBN: 978-80-87952-07-8.
- [PA2] JANHUBA, L. Standard and Future- Potential Methods for Safety and Reliability Assessment Illustrated by an Airborne Electric System Example. AVIATION, 2016, vol. 19, no. 4, p. 180-186. ISSN: 1648-7788.
- [PA3] KOŠTIAL, R.; JANHUBA, L.; HLINKA, J. INTELLIGENT SCHEDULED MAINTENANCE METHODOLOGY FOR GENERAL AVIATION STRUCTURES BASED ON MSG-3 AND MULTIPLE- CRITERIA DECISION MAKING ANALYSIS. In Engineering Mechanics 2017. Engineering mechanics 2014. 1. Praha: ACAD SCI CZECH REPUBLIC, INST THERMOMECHANICS, DOLEJSKOVA 5, PRAGUE 8, 182 00, CZECH REPUBLIC, 2017. p. 498-501. ISBN: 978-80-214-5497-2. ISSN: 1805-8248.
- [PA4] Aircraft Leading Edges Minor Damages Detection Based on Thermographic Survey of Electrical Anti-Icing System, READ 2018 Conference **/PENDING/**
- [PA5] Integrated Method utilizing Graph Theory and Fuzzy Logic for Safety and Reliability Assessment of Airborne Systems, READ 2018 Conference **/PENDING/**

10 PRODUCTS

- [TA1] KOŠTIAL, R.; BENCALÍK, K.; HLINKA, J.; JANHUBA, L.; TŘETINA, K. Rám pro zkoušení elektrických aktuátorů; funkční vzorek; 2013
- [TA2] HLINKA, J.; JANHUBA, L.: Shock-box; Zkušební zařízení pro zkoušení odolnosti vybavení letadel vůči provozním rázům. Zkušebna Leteckého ústavu, VUT-FSI v Brně, Technická 2, 616 69 Brno Česká republika. (funkční vzorek)

11 CURRICULUM VITAE

Name

Luboš Janhuba

Personal data

Date of birth: 2. 6. 1985
Palace of birth: Hradec Králové
Citizenship: Czech Republic
Nationality: Czech
Marital status: Freelance
Email: janhuba@fme.vutbr.cz

Education

2011 – recent Institute of Aerospace Engineering Faculty of Mechanical Engineering, Brno
University of Technology Technická 2, 616 69 Brno
Specialization: Machines and Equipment – Doctoral study

2008 – 2011 Institute of Aerospace Engineering Faculty of Mechanical Engineering, Brno
University of Technology Technická 2, 616 69 Brno
Specialization: Aircraft Design- Master study

2004 – 2008 Faculty of Mechanical Engineering, Brno University of Technology
Technická 2, 616 69 Brno
Specialization: Mechanical engineering – Bachelor study

2000 – 2004 SPŠ, SOŠ s SOU Hradec Králové

Language skills

English

Employment

2012-recent Institute of Aerospace Engineering Faculty of Mechanical Engineering, Brno
University of Technology

2016 The College of Central Europe (Lecturer- Basic physics)

Internship

2009-2010 Erasmus program- Universitat Politècnica de Catalunya, Barcelona-
Terrassa

Research activities

2014-2016 Pokročilá konstrukce kompozitní náběžné hrany letounu, zahájení:
01.01.2014, ukončení: 31.12.2016

2012-2013 Rozvoj metod zkoušení a diagnostiky moderních palubních soustav letadel,
zahájení: 01.01.2012, ukončení: 31.12.2013

Conference and seminars

2017 Conference Engineering Mechanics 2017, Svratka, paper

2016 READ 2016 conference, paper

2014 READ 2014 conference, paper