



BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF MECHANICAL ENGINEERING

FAKULTA STROJNÍHO INŽENÝRSTVÍ

INSTITUTE OF AEROSPACE ENGINEERING

LETECKÝ ÚSTAV

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 LOGIKY

DOCTORAL THESIS

DIZERTAČNÍ PRÁCE

AUTHOR

AUTOR PRÁCE

Ing. Luboš Janhuba

SUPERVISOR

ŠKOLITEL

doc. Ing. Jiří Hlinka, Ph.D.

BRNO 2018

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.

KEYWORDS

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

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 hodnocení bezpečnosti a spolehlivosti, nicméně je primárně navržena pro použití v oblasti 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. Kritičnost prvku zohledňuje pravděpodobnost jeho selhání, možnost detekce dané poruchy, závažnost těchto selhání vzhledem k vlivu na alokované funkce.

KLÍČOVÁ SLOVA

Letadlo, Systém, Spolehlivost, Bezpečnost, letectví, Kritičnost, Fuzzy logika, Teorie grafů, Analýza

JANHUBA, L. The Integrated Method Utilizing Graph Theory and Fuzzy Logic for Safety and Reliability Assessment. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2018. 233 p. Supervised by doc. Ing. Jiří Hlinka, Ph.D.

DECLARATION

I declare that the presented thesis is the result of my own work under the guidance of my supervisor and I cited all literature and electronic sources what I used during the research.

In Brno, 29. srpna 2018

ACKNOWLEDGEMENT

At first I would like to express my thanks to Jiří Hlinka, Rostislav Košťál, Tomáš Létal, Luboš Janhuba senior and Martin Janhuba who directly helped me in completing my doctoral thesis.

I am also grateful to Milan Kundera, Karl Ove Knausgard, Yuval Noah Harari, Guillaume Apollinaire, Nick Cave, Mark Rothko, Pablo Picasso, Caravaggio, George Carlin, Karel Kryl, Václav Havel, Voltaire, Fjodor Michajlovič Dostojevskij, Polly Jean Harvey, Arcade Fire, Tom Waits, Nirvana, Franz Kafka, Jan Patočka, Milada Horáková, Rick Sanchez, Harriet Beecher Stowe, Výsadkové skupiny- Anthropoid, Silver A, Silver B, Out distance (except K. Č.), Bioscop, Bivouac, Steel, Tin, Intransitive (except V. K.), entire second and third wave, Giordano Bruno, Vasilij Alexandrovič Archipov, Johannes Gutenberg, Madame Bovary, Dean Moriarty, Dulcinea del Toboso, Amélie Poulain, HGW, František Fajtl, Pavel Tigrid, John Yossarian, Rosalind Franklin, Stanley Kubrick, Arnold J. Rimmer, Profesor Avenarius.

Divadlo Vosto5, divadlo Sklep, Jesse Owens, Věra Čáslavská, Josef Balabán, Josef Mašín, Václav Morávek, Emil Zátopek, Pink Floyd, Czechoslovak Squadron RAD and other fighters, František Kupka, Carl Orff, Jacques le fataliste et son maître, Estragon and Vladimír, Moreno a Pulpus, Charta 77, Jean-Luc Picard, Children of men

Josef K., Winston Smith, Jan Palach, Člověk v tísni, George Orwell, Jan Balabán, Sabina, Médecins Sans Frontières, Joseph Heller, Doktor Škréta, Margaret Heafield, Gerty Cori, Anna Coleman Ladd, Adalbert Kolínský, Eliška Kutnohorská, John Oliver, Ilia, Tamina, Joan Miró, Lotfi Zadeh, Respekt, Gene Roddenberry, Rosa Louise McCauley Park, Albert Mayer, Československé legie, Marie Moravcová, Eso Rimmer, TGM, Magnificent Eight 1968, Arnošt Lustig, Karel Seiner, Jimmy Dixon, Zapadlí vlastenci, Albert Schatz a Selman Abraham Waksman, Jiří Kratochvíl and my entire family.

Contents

Chapter 1	11
Introduction.....	11
Main Objectives.....	13
Additional Objectives	13
Chapter 2	14
State of the Art	14
2.1 Doctoral Thesis Drivers.....	14
2.2 Field of Interest	14
2.3 General Requirements	15
2.3.1 Certification Requirements	15
2.3.2 EASA CS-23 Certification Base	16
2.4 The Aircraft Systems and Architecture.....	17
2.4.1 General Systems	17
2.4.2 Avionics System	18
2.4.3 UAVs and UAS.....	18
2.5 Standard Reliability Techniques and Tools.....	19
2.5.1 System Modeling	19
2.5.2 Standard Safety and Reliability Assessment Tools	22
2.6 Criticality evaluation.....	24
2.6.1 Criticality analysis	24
2.6.2 Risk Priority Number	25
2.6.3 Outcome	26
2.7 Recent Development of Safety Assessment Methods	26
Chapter 3	28
Integrated Method Architecture	28
3.1 Introduction.....	28
3.2 Function Hierarchy	29
3.3 Aircraft Main Function	32
3.4 Aircraft Support Function.....	34
3.5 Aircraft Additional Functions.....	34
3.6 Failure identification and indication.....	36

3.7	Failure mitigation means.....	36
3.8	Flight crew response	37
3.9	Method Architecture.....	39
Chapter 4	42
	System Modeling.....	42
4.1	Introduction.....	42
4.2	Model Processing	43
4.3	Modeling Principles	44
4.3.1	Function propagation principle	45
4.3.2	Global and local models	46
4.3.3	Interconnection layering	46
4.4	A Graph Theory Basics.....	49
4.4.1	Basic definitions.....	49
4.4.2	Graph handling in doctoral thesis	52
4.5	Basic graph attributes.....	53
4.6	The Rough Tree and Recursion algorithm	56
4.6.1	Recursive algorithm.....	56
4.6.2	Recursion example	58
4.6.3	Rough tree failure rate estimation.....	59
4.7	Graph model structure and topology.....	60
4.7.1	Fundamentals of graph	60
4.7.2	Network Position	61
4.8	Model Parameters.....	65
4.9	Evaluation process and outputs	67
4.9.1	Evaluation process outputs	67
4.9.2	Weight of function.....	69
4.9.3	Node topology parameter	70
Chapter 5	72
	Extended Criticality and Robustness	72
5.1	Introduction.....	72
5.2	Extended Criticality Evaluation.....	73
5.2.1	Severity definition	74
5.2.2	Occurrence definition.....	78
5.2.3	Detectability definition.....	79

5.2.4	Topology parameter definition	80
5.3	Robustness and System parameters	80
5.4	Integrated Method Knowledgebase.....	83
5.4.1	Classification Knowledge Base	83
5.4.2	Basic Items Reliability Data Overview	84
5.4.3	Robustness parameters questionnaire	84
5.5	Fuzzy Extended criticality Inputs	85
5.5.1	Detectability input.....	85
5.5.2	Node topology	87
5.5.3	High-level severity input.....	88
5.5.4	Occurrence input.....	89
5.6	Robustness and Parameters inputs.....	91
5.7	Fuzzy Extended criticality Outputs	92
5.7.1	Extended criticality output.....	92
5.7.2	Robustness number output.....	93
5.8	Fuzzy Inference.....	95
5.8.1	Fuzzification.....	95
5.8.2	Defuzzification	102
5.9	Fuzzy evaluation outputs.....	103
Chapter 6	104
	Integrated method process	104
6.1	Process.....	104
Chapter 7	105
	A Case study	105
7.1	Primary Case Study Definition	105
7.2	Primary Case Study Systems.....	106
7.2.1	Electrical System.....	106
7.2.2	Avionics system	107
7.2.3	Elevator trim system.....	109
7.2.4	Pitot-static system	110
7.2.5	Engine indication system.....	111
7.3	Evaluation process results.....	112
7.3.1	Global model parameters results.....	112
7.3.2	Extended criticality results	113

7.3.3	Model structure and topology results.....	114
7.3.4	Robustness parameters results	115
7.3.5	Rough tree evaluation results	116
	Conclusion	117
	Bibliography.....	119
	Acronyms and Abbreviations	123
	List of figures	125
	List of tables	127
	Appendices	129

CHAPTER 1

INTRODUCTION

Nowadays aerospace engineering might be characterize 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.

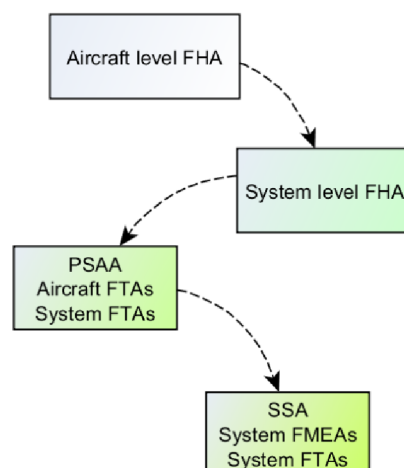


Figure 1 Simplified ARP 4761 process

Safety assessment process still relays 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 system components, assemblies, elements function followed by

assessing of all failure modes and their resulting effects on the system is at least sophisticated and perplexing process. Assessment methods and techniques are integrated into a coherent safety life cycle (Figure 1).

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, creates 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 lifetime. 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 [13])

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 reliability data or absence. The results of methodology implementation 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) while using the same data structure along with additional outputs. It is assumed that integrated method usage will be in the range of general aviation and unmanned aerial systems.

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.

ADDITIONAL OBJECTIVES

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

CHAPTER 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 the 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 [18]. This is the model example of increasing system complexity.

What is the complex system in aerospace engineering?

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 AC 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 GENERAL REQUIREMENTS

2.3.1 Certification Requirements

Doctoral deals with various airborne systems of airplanes. Special attention is given to the unmanned aerial vehicles and systems. At first it is necessary to define certifications bases for each of those classes and listed basic requirements.

Table 1 General description of relevant regulation requirements

<i>Category</i>	<i>Definition</i>	<i>Regulation (European Union/ Czech Republic)</i>
CS-25 Class	Turbine powered Large Airplanes.	EASA CS-25 AC 25.1309-1A
CS-23 Class	Airplanes with excluding the pilot seat(s), of nine or fewer and a maximum certificated take off weight of 5670 kg or less	EASA CS-23 AC 23.1309-1E
CS-E	Requirements for engine design and testing	EASA CS-E
Very light	Weight less than 750kg; Stall speed no more than 83 km.hr ⁻¹	EASA CS-VLA
Light sport	Weight less than 600 kg; Stall speed no more than 83 km.hr ⁻¹	EASA CS-LSA
Ultra-light	Weight less than 300kg for single seat Weight less than 450kg for two seats Weight less than 472,5kg for two seats and aircraft with parachute rescue system	EASA Basic Regulation 216/2008
UAS, UAV	Unmanned aerial vehicles (depends on particular state regulation)	Doplňěk X (CAA regulation- Czech Republic)

2.3.2 EASA CS-23 Certification Base

In the case of absence of proper certification base and recommendations, it is imperative to use Regulations requirements of closest upper class, EASA CS-23.1309 and advisory circular FAA AC 23.1309-1E (most recent at the time).

The advisory circulars are sets of acceptable means for demonstrating compliance with applicable regulation (EASA CS-23/ CS-25). They are not mandatory and do not constitute a regulation. A simply stated, ACs establish definitions of classification of failure conditions, relationship between probabilities, severities of failure conditions. Further, ACs describes safety assessment objective, which is to ensure an acceptable safety level for equipment and system installed on the airplane. [1]

According to the ACs instruction analyst classifies consequences of each failure conditions and chooses appropriate combinations of the assessment methods.

FAA AC 23.1309-1E failure conditions classifications:

- (1) **NO SAFETY EFFECT**- *no probability*
- (2) **MINOR**- *may be probable*
- (3) **MAJOR**- *must be no more than remote*
- (4) **HAZARDOUS**- *must be extremely remote*
- (5) **CATASTROPHIC**- *must to be extremely improbable*

Advisory circulars are based on related industrial documents such as SAE ARP 4754A (Guidelines for Development of Civil Aircraft and Systems), SAE ARP 4761 (Guidelines for Development Conduction the Safety Assessment Process on Civil Airborne Systems an Equipment) and RTCA documents (RTCA/DO-160, RTCA/DO-178B, RTCA/DO-254).

As it was stated, all those documents serve as support for demonstration of compliance with applicable regulation. It is up to each analyst to choses appropriate assessment procedures, methods and evaluation means.

2.4 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. [18]

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 Figure 2.

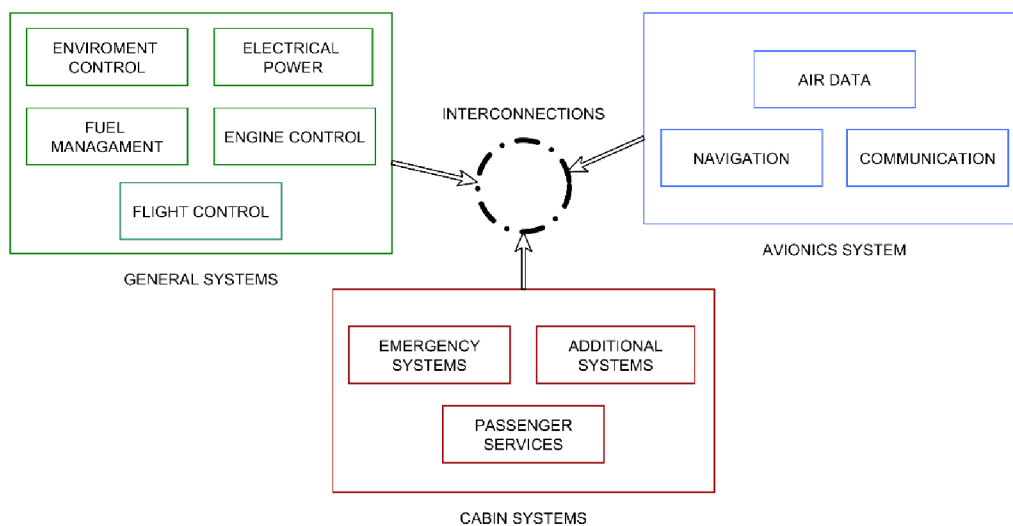


Figure 2 EASA CS-23 Commuter aircraft basic systems example (based on [18])

2.4.1 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.

2.4.2 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.

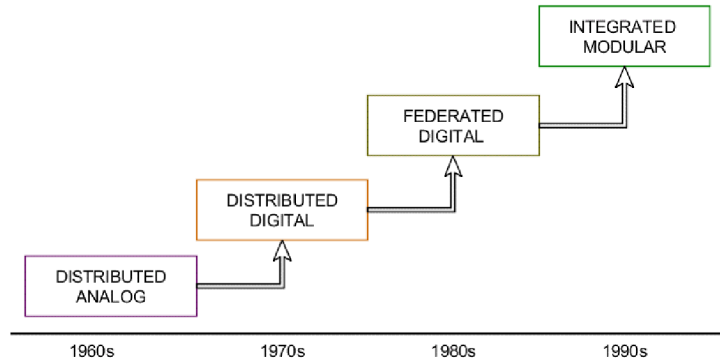


Figure 3 Avionic system evolution (based on [18])

During last sixty years avionics system architecture evolved (Figure 3). Huge boost of aircraft performance speeds a need for avionics system evolution. To utilize growing improvements, capability and complexity of avionic 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 a 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.

2.4.3 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.

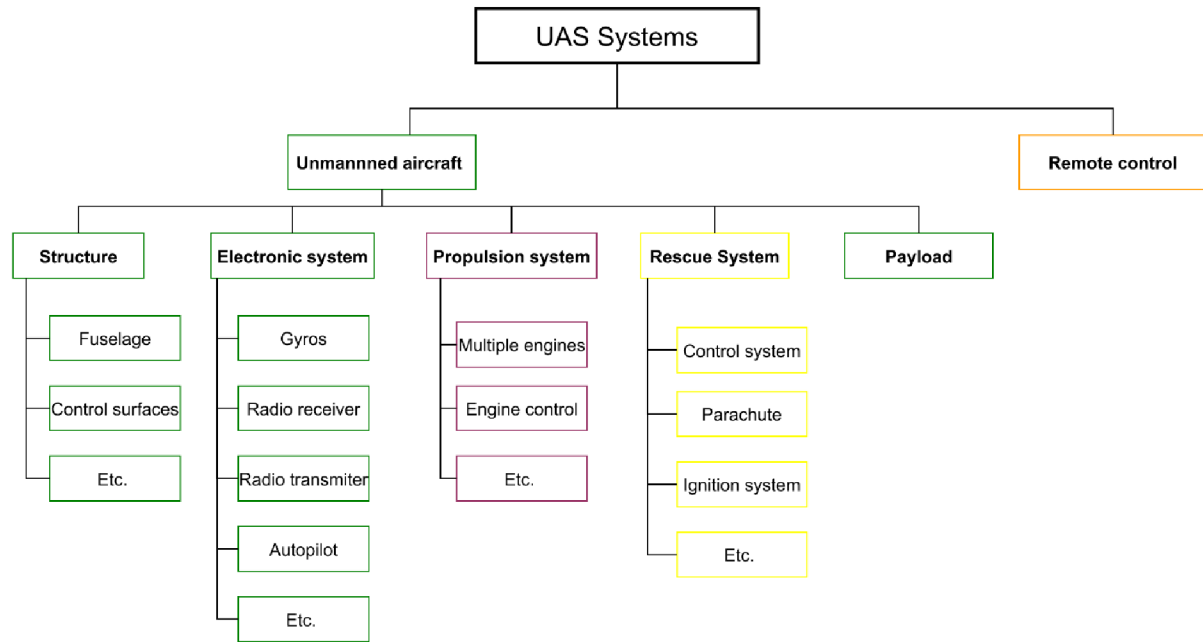


Figure 4 UAV system example

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.

2.5 STANDARD RELIABILITY TECHNIQUES AND TOOLS

2.5.1 System Modeling

To manipulate and evaluate complex system it is imperative to find a proper way how to represent a system. System modelling is a multidisciplinary study of model usage to system conceptualization. There are numerous means of system modeling. 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.

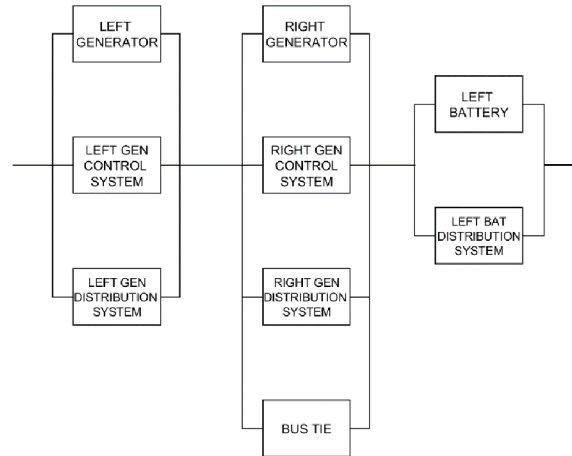


Figure 5 Failure of one main bus supply block diagram

Block diagram on Figure 5 represents failure of one main bus supply of modern aircraft system. RBD analysis are highly useful in analysis of *traditional* system consists of separate elements. 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. Its starts from consideration of system failure effect, referred to the “Top Event”. The analysis proceeds by determining how these failures 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.

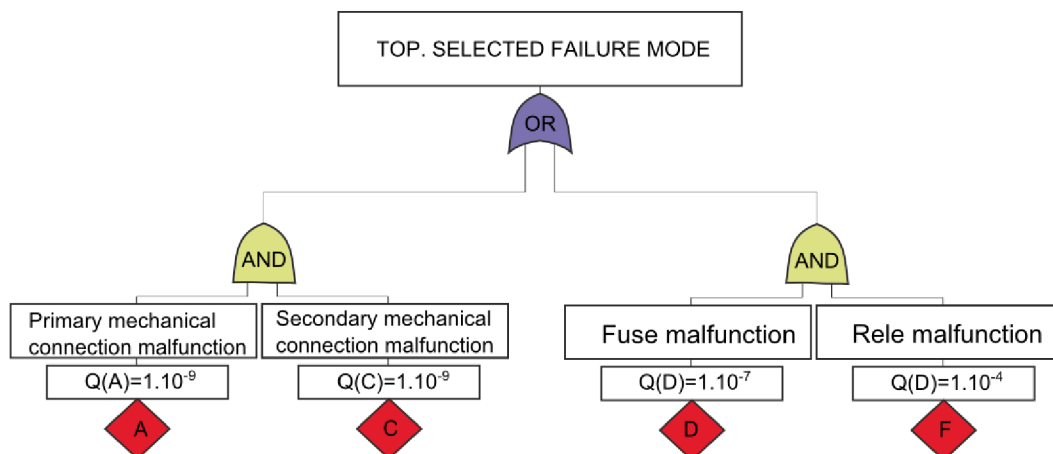


Figure 6 Fault Tree Example

The Figure 6 shows example of top event representation (Loss of ability to change position of elevator trim). In the lower layer two examples of an AND gates are showed (output TOP event occurs only if

all inputs occur). On the higher layer is example of an OR gate is showed (output occurs if any input occurs).

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 tree analyses. 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 than solved by using tree diagram. (Partially[18])

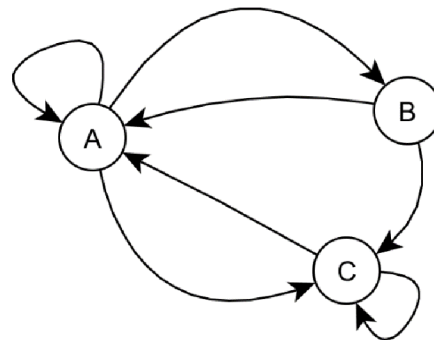


Figure 7 Markov Chain Example

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. Technique 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.

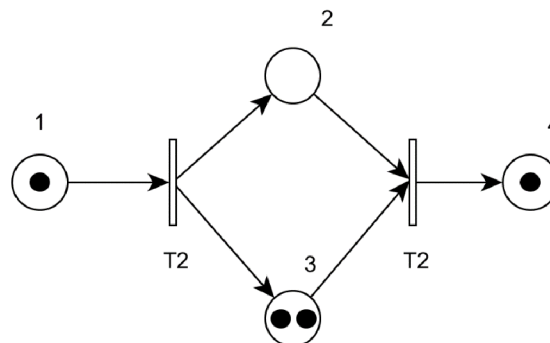


Figure 8 Petri Net Example

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 chases, iteration and concurrent execution. (Partially [18])

2.5.2 Standard Safety and Reliability Assessment Tools

This chapter gives a brief overview of reliability tools, which are used during safety assessment of complex system. Assessment process starts with identifications of system requirements, design specifications and functional principles. Following methods are stated according to their use in safety assessment.

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. [24]

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 assertion the effects on system operation of each failure mode in turn. [19]

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 analyze 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).

- Zonal Safety analysis: It consists of consideration of installation aspects of individual systems and components and the mutual influence between several systems/components installed in close proximity on the aircraft. [3]
- Particular Risk Analysis: Its task is to assess the aircraft design for external threats that may compromise continued safe flight and landing (ARP4761 Particular Risk Assessment). [3]
- Common Mode Analysis: It contributes to the verification that independent principles have been applied when necessary. Considerations should be given to the independence of functions and their respective monitors. [3]

CCA is needed, when it is necessary to prove, that several components can fail (or just became unavailable) due to the particular cause of failure, which causes the condition for multiple components to be affected by the same cause. [25]

2.6 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.

2.6.1 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. This technique is usually applied in aviation industry. Following description is based on Military Standard MIL-STD-1609a [3].

Qualitative approach [3]

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 [3]

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 [3]

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

$$C_m = \beta \cdot \alpha \cdot \lambda_p \cdot t \quad \text{Equation 1 [3]}$$

Where:

C_m	Criticality number for failure mode
β	Conditional probability of mission loss
α	Failure mode ration
λ_p	Part failure rate
t	Duration of applicable mission phase usually express in hours or number of operating cycles (based on analyst judgment)

Failure effect probability (β)

It is a conditional probability that the failure effects will result in the identified criticality classification result in the identified criticality classification, given that the failure mode occurs representing an analyst judgment.

Failure mode ration α

A part of failure rate λ_p related to the particular failure mode under considerations should be evaluated and noted. It is a probability expressed as a decimal fraction that the part or item will fail in the identified mode. Sum of the all failure modes rations for that part or item will equal one. In the case, that failure data are not available, the α values will represent analyst’s judgment based upon analysis of the item or part function.

Item criticality numbers [3]

An item criticality number is number of system failures of **specific type** expected due to failures modes. The specific type of system failure is expressed by the severity classification for the item failure mode. For a particular severity classification and mission phase, item criticality number is the sum of failure mode criticality numbers C_m .

$$C_r = \sum_n^j (\beta \cdot \alpha \cdot \lambda_p \cdot t)_n \quad \text{Equation 2 [3]}$$

Where:

$$n = 1,2,3 \dots j$$

C_r Criticality number for the item

n The failure modes in the items that fall under a particular criticality classification

j Last failure mode in the item under the criticality classification

2.6.2 Risk Priority Number

RPN method adopts linguistic terms to rank the chance of failure mode occurrence (labeled 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.

$$RPN = P \cdot S \cdot D \quad \text{Equation 3 [6]}$$

RPN method can be labeled as quicker and cheaper in comparison with criticality analysis. Nerveless RPN as quantitative method is essentially based on qualitative assessment and results are only educated guesses at best. [6] This technique is usually applied in automotive industry

2.6.3 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.

2.7 RECENT DEVELOPMENT OF SAFETY ASSESSMENT 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. [21]
- /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. [22] 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 [23], 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 larger. 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 [16]. 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 even in the case of insufficient input data.

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" [17] 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) [8]. Usage of fuzzy logic as a tool of handling risk assessment led to fuzzy logic application in airborne criticality evaluation.

Function- oriented Risk model for Engineering System presented in the paper by Weijing Zhou and Huairong Shen [32] served as inspiration for function oriented modelling used in integrated method (described in following chapter).

CHAPTER 3

INTEGRATED METHOD ARCHITECTURE

3.1 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.

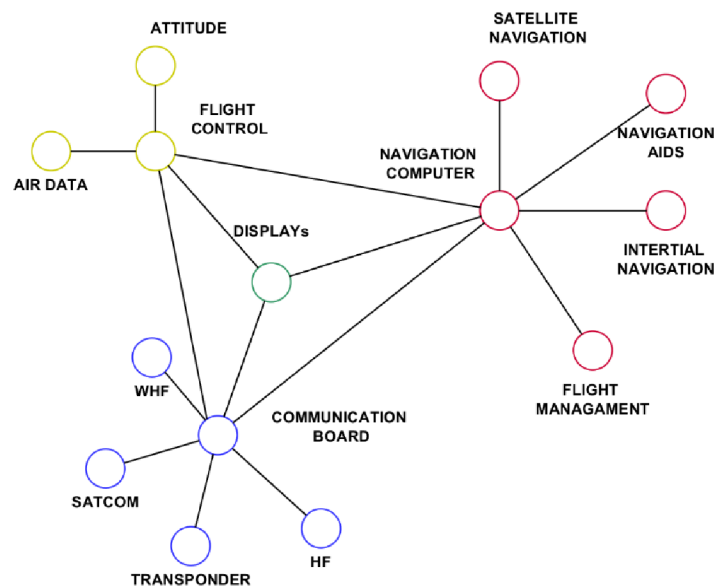


Figure 9 Avionics system example in the form of graph

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 5). 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.

3.2 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. [26]

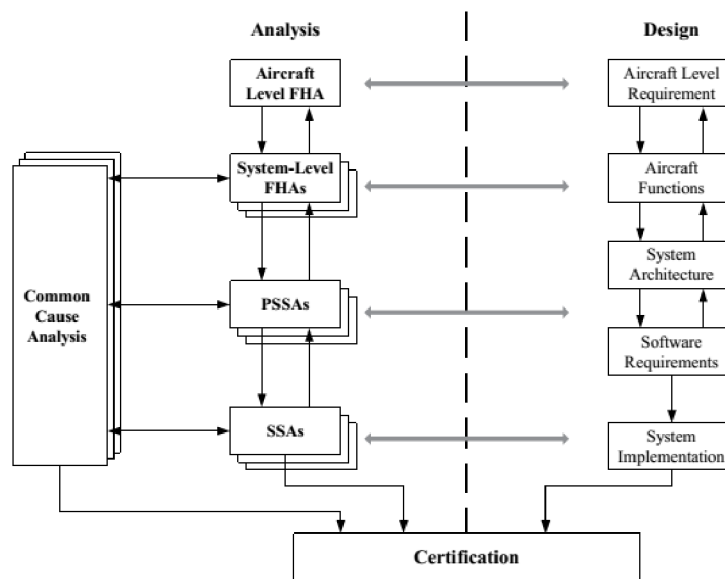


Figure 10 Simplified portrayal of safety process [18]

Figure 10 illustrates simplified process of safety assessment used during aircraft design. It shows, how system design evolves in cooperation with reliability analysis. Process of aircraft evolution starts with aircraft level requirements, then this evolution leads to the system architecture, which in turn define potential software requirements and implementation. Various types of analysis are conducted during that process.

Results of every particular analysis supposed to serve as base for following design step forward. As it was mention above, all these analyses mainly rely 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 then 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. Functions division is simply illustrated in Figure 11.

Function without relation to the main safety objective or not significantly contributing to the supply function performance are labeled as **Additional functions (AF)**.

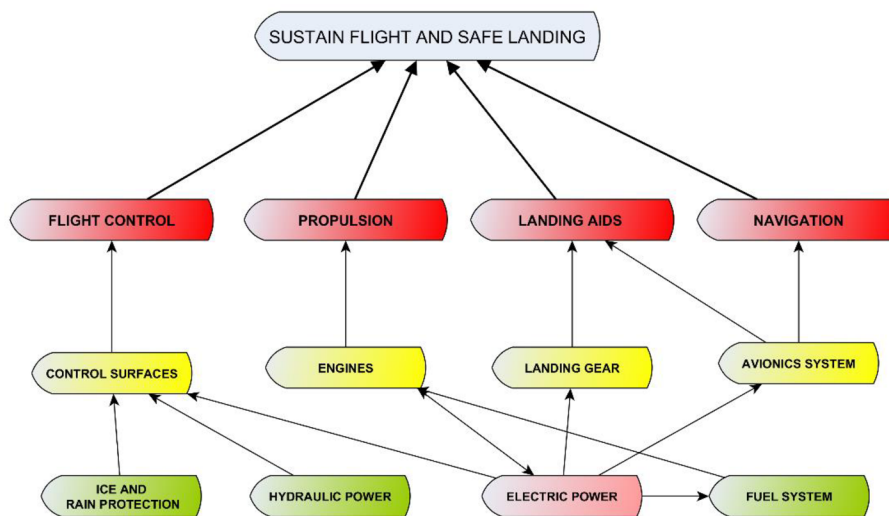


Figure 11 Functions hierarchy- illustration

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.

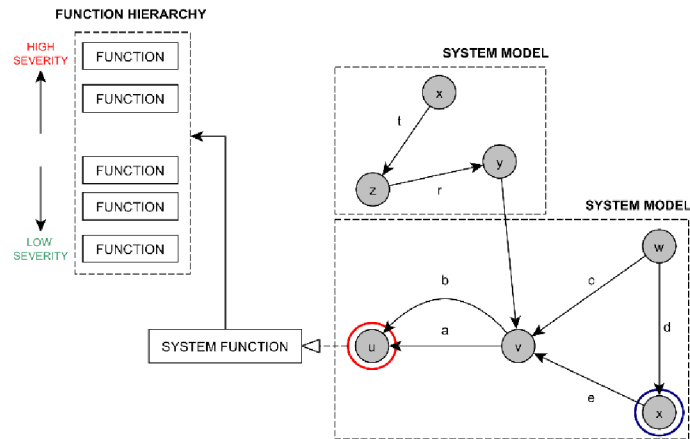


Figure 12 Function- based modeling

Function oriented model allows to describe interconnection between various systems (electrical, avionics) in relation to the particular function. Modeling principles and integrated method architecture are described in deep in following chapters.

3.3 AIRCRAFT MAIN FUNCTION

Aircraft functions are divided into main and supporting functions. Functions which directly influence system main safety objective are labeled as **Main functions (MF)**. What are the main functions? It is possible to abstracts essence of aircraft main function definition (with some amount of reserve). Object movement through the atmosphere (flight) is achieved by generating sufficient aerodynamic lift. Aerodynamic lift is air flowing past surface of wing, tail and fuselage. To achieve it, there must be object has to have sufficient propulsive thrust. Flying object has to be equipped by some kind of flight control system. When it is orderly flying, it has to be navigated through the air to reach intended destination. Crew must be able to communicate with air traffic control (ATC). Every flight has to be ended by safe landing.

This trivial thought experiment illustrates the logic of function division into a hierarchy. Main functions definition is summarizes in Table 2.

Table 2 Aircraft main functions

MAIN FUNCTIONS	
PROPULSION	Loss of propulsion during landing and takeoff phases usually leads to the hazardous or catastrophic situations. Result: Direct influence on the higher safety objective fulfillment.
FLIGHT CONTROL	Inability to control flight directly jeopardize crew and passenger's safety. During all flight phases there is high probability of hazardous or catastrophic outcome in the case of significant failure. It could lead to serious injury or fatality, loss of structural integrity of wings, tail or fuselage. It could case collision with other aircrafts. Result: Indirect influence on the highest safety objective.
NAVIGATION AND COMMUNICATION	Result: Indirect influence on the higher safety objective.
LANDING AIDS	Loss of ability to extend landing gears leads to hull loss and possible fatal injury. Inability to use landing aids (ILS, MLS) potentially also leads to the hazardous or catastrophic consequences. Result: Direct influence to the higher safety objective (more precisely safe landing)

Aircraft as object of reliability study consists of various sub-systems, which cooperate together to achieve system goals. Equally support functions cooperate together as a mean to ensure main functions.

Safety criticality definition

It is essential to define synergy between integrated method definitions (Main function, support function). Functions are performed by item or items cooperation. Items contributing to the function performance carries share of function criticality. Term safety-critical (item/ sub-system/ system) is defined by Military handbook MIL-STD 882E [26]. It states, that safety critical item is *a hardware or software item that has been determined through analysis to potentially contribute to a hazard with Catastrophic or Critical mishap potential, or that may be implemented to mitigate a hazard with Catastrophic or Critical mishap.*

Item level of contribution to the main function performance determines level of safety criticality. Process of criticality evaluation is described in deep in following chapters.

3.4 AIRCRAFT SUPPORT FUNCTION

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:

- (1) **Provide a motion or source of motion** (fuel system provides “source of motion” for engine, hydraulic power)
- (2) **Instrumentation and control of main function** (engine control, flight control indication)
- (3) **Provide an appropriate operating environment** (pressure, temperature, humidity)

Note. Based on [32]

3.5 AIRCRAFT ADDITIONAL 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.

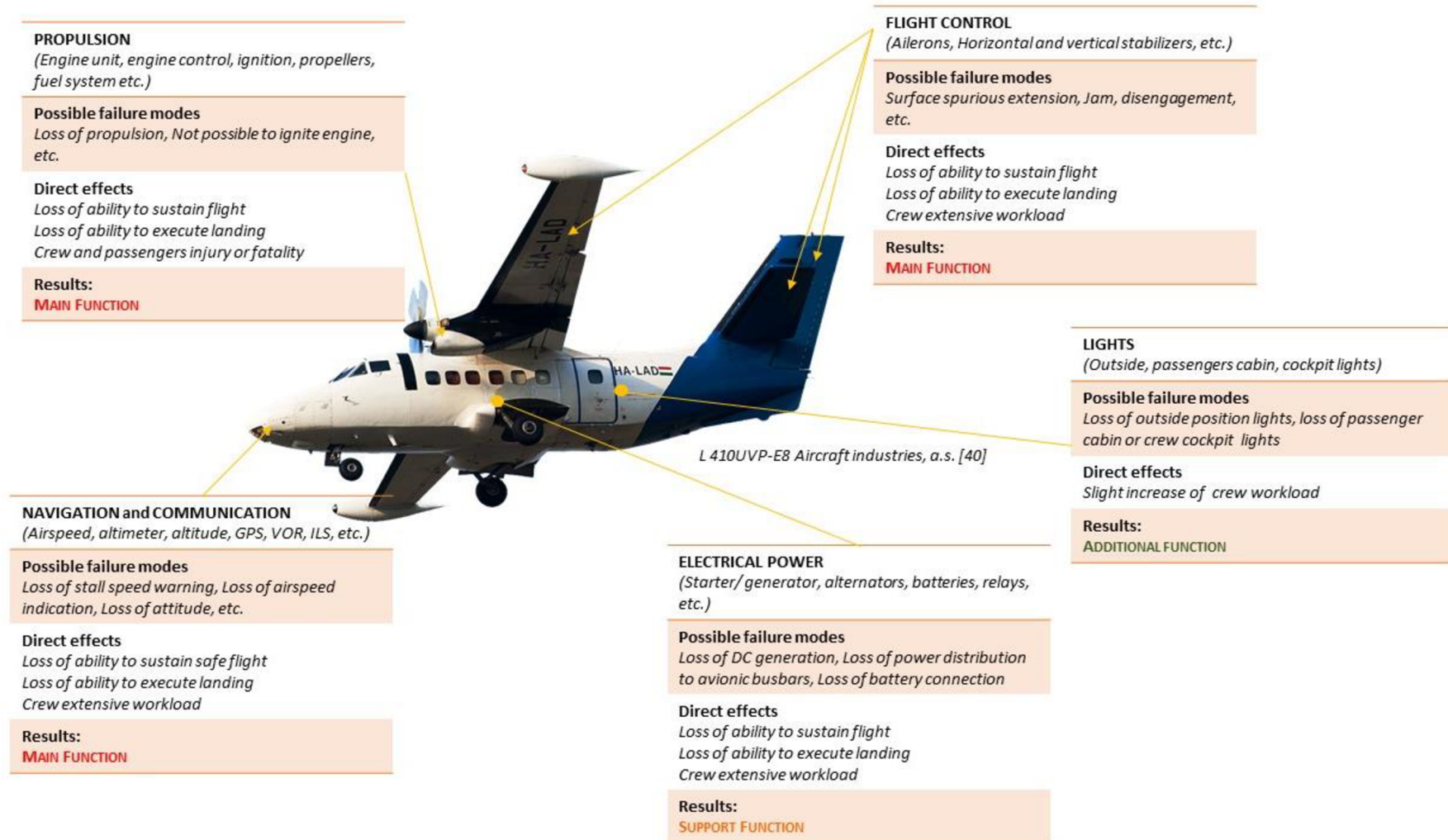


Figure 13 Aircraft function examples

3.6 FAILURE IDENTIFICATION AND INDICATION

System Indication [1]

If warning, caution or advisory lights are installed in the cockpit, they must, unless otherwise approved by the Agency, be –

- A. **Warning** - Red, for warning lights (lights indicating a hazard which may require immediate corrective action)
- B. **Caution** - Red, for warning lights (lights indicating a hazard which may require immediate corrective action)
- C. **Safe operation**- Red, for warning lights (lights indicating a hazard which may require immediate corrective action)
- D. Any other colour, including white, for lights not described in sub-paragraphs (a) to (c), provided the colour differs sufficiently from the colours prescribed in sub-paragraphs (a) to (c) to avoid possible confusion

3.7 FAILURE MITIGATION MEANS

When determining the mitigation means and the resulting severity of a Failure Condition, the following may be considered (based on [42]):

- MM0.** Additional function or system
Other systems could take over (at least partially) function of system in failure.
- MM1.** Fault isolation and reconfiguration
System is able to change configuration in order to sustain functional. Typical examples are electrical system consisting of multiple generators and batteries, fuel system or propulsion. Configurable nature of system allows eradicate failure mode consequence with only minimal loss of functionality.
- MM2.** Redundancy (e.g. heading information may be provided by an independent integrated standby and/or a magnetic direction indicator)
System is designed as redundant- particular functions have backup by separated items. For instance, avionics system.
- MM3.** Availability of, level of, and type of alerting provided to the flight crew
Multi-level indication means- note, caution, warning (see previous definition)
- MM4.** The flight phase and the aircraft configuration
There is different severity in various flight phases- some functions are not required. Aircraft configuration could influence resulting severity.
- MM5.** The duration of the condition
Time period effects flight crew response and severity of failure.
- MM6.** The aircraft motion cues that may be used by the flight crew for recognition
Collateral effects indicate flight crew occurring failure. It strongly depends on nature of failure.

- MM7.** Expected flight crew corrective action on detection of the failure, and/or operational procedures (*Pre-identified failure mode*)
Flight manual should contain emergency procedures in the case of occurring failure.
- MM8.** Ability of the flight crew to control the airplane after a loss of primary attitude display on one side in some flight phases
Cockpit is designed to controllable after one side failure.
- MM9.** For multiple failures (e.g. primary and standby) the non-simultaneity of the failures
- MM10.** Protections from other systems (flight envelope protection, augmentation systems) (included in robustness)

Note: Means to assure continued performance of any system design mitigation means should be identified.

The safety assessment should include the rationale and coverage of the Display System protection and monitoring philosophies employed. The safety assessment should include an appropriate evaluation of each of the identified Display System Failure Conditions and an analysis of the exposure to common mode/cause or cascade failures in accordance with AMC/ ACJ 25.1309. Additionally, the safety assessment should include justification and description of any functional partitioning schemes employed to reduce the effect/likelihood of failures of integrated components or functions. [42]

3.8 FLIGHT CREW RESPONSE

Terminology definitions

- Airplane Flight Manual (AFM)- Document that contains information (operating limitations, operating procedures, performance information, etc.) necessary to operate the airplane at the level of safety established by the airplane's certification basis. [43]
- Flight Operating Manual (FCOM)- A document developed by a manufacturer that describes, in detail, the characteristics and operation of the airplane or its systems.

Procedures

A procedure is a step-by-step method used to accomplish a specific task.

- A. **Emergency-** A procedure requiring immediate flight crew action to protect the airplane and occupants from serious harm.
- B. **Abnormal or Non-normal situation-** A procedure requiring immediate flight crew action to protect the airplane and occupants from serious harm.
- C. **Normal-** A procedure associated with systems that are functioning in their usual manner.

Emergency Procedures

The emergency procedures can be included either in a dedicated section of the AFM or in the non-normal procedures section. In either case, this section should include the procedures for handling any situation that is in a category similar to the following [43]:

- /a/ Engine failure with severe damage or separation.
- /b/ Multiple engine failure
- /c/ Fire in flight
- /d/ Smoke control. At least the following should be clearly stated in the AFM:
After conducting the fire or smoke procedures, land at the nearest suitable airport, unless it is visually verified that the fire has been extinguished.
- /e/ Rapid decompression.
- /f/ Emergency descent.
- /g/ Uncommanded reverser deployment in flight.
- /h/ Crash landing or ditching.
- /i/ Emergency evacuation.

3.9 METHOD ARCHITECTURE

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.

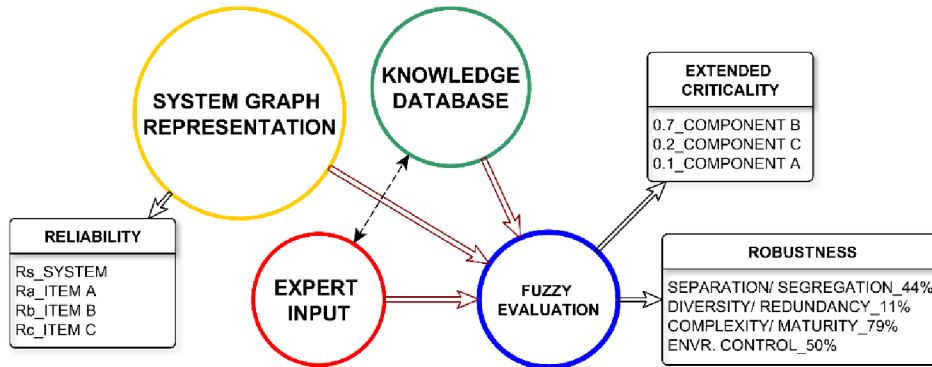


Figure 14 Integrated method architecture

General idea is that, analyst decompose aircraft into systems, and subsystems consisting of items. Each system structure is designed to provide specific function or multiple functions. Items are connected by various types of interconnection e.g. (mechanical, electrical supply, electrical control, data, indication) to achieve intended function.

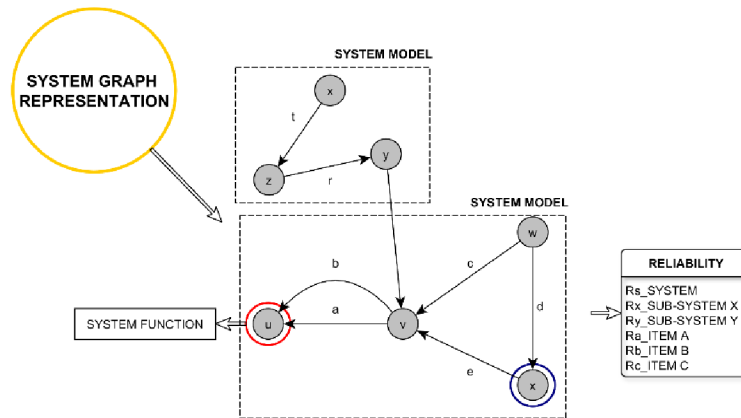


Figure 15 System modeling

Integrated method algorithm of failure mode detaching allows to model *rough failure tree* for specific function failure. One of main advantages of function- oriented model is usable in many ways and easily accessible.

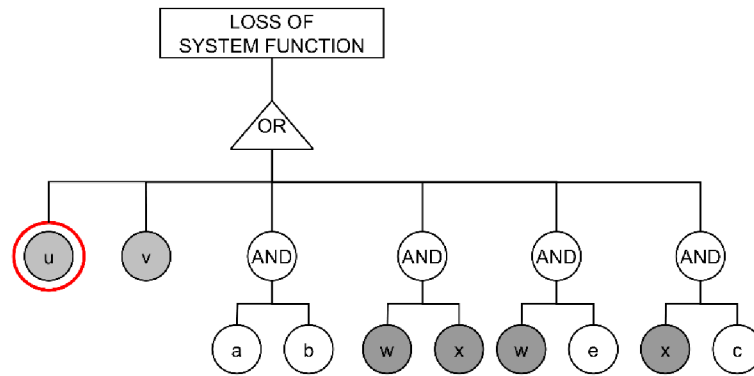


Figure 16 Rough failure tree “System Example-Loss of function”

Each item has a specific attribute (for instance failure rate, probability of failure detection, physical location- zone, severity of failure, rate of interconnection with other items). System functions and operation are not defined just by item interconnections. System functionality is influenced by huge number of factors. Each item has specific contribution to the function performance. As it is mentioned above functions are arranged into hierarchy according to their relation to the main safety objective. Extended criticality level could be defined as “degree of this influence”.

System as a unit is also evaluated. Robustness evaluation asses how system is protected against ambient influences, level of redundancy and diversity and environmental testing.

In the doctoral thesis field of interest, system sometimes consists 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 (it is not possible to express these in precise mathematical definitions).

Therefore, extended criticality by doctoral thesis definition cannot result from exact formula. Integrated method must adopt means how to handle vague definition. Fuzzy logic is adopted to extended criticality and robustness level estimation. This process is described in deep in *Chapter 5 System Criticality and Robustness*.

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 (precisely defined in *Chapter 5*) and with deferent possibility of **detection**. Integration method provides knowledge database (**Appendix A**) which contains preliminary failure classification related to the **MF**, **SF** and **AF**, usually applied remedies and extended criticality evaluation inputs.

System functionality is also highly influenced by its physical installation. Various systems are deployed through the airplane. Cockpit is sort of nerve centrum. Controlling mechanisms, system indication is routed from wings, engines, tail and many 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 functions) duplication could create even higher system safety (in the case of highly complex systems).

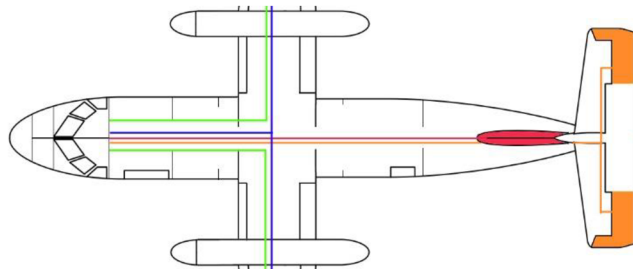


Figure 17 System installation routing example

System **complexity** is an 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. This process is described in deep in *Chapter 5*. Integrated method offers guidelines for robustness evaluation (**Appendix D**).

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.

CHAPTER 4

SYSTEM MODELING

4.1 INTRODUCTION

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 servers as a tool for components interconnection investigation. Physical interconnection rate can be easy estimated (describe 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.

Figure 18 illustrates a graph theory application example. Figure show largely simplified model of flight control mechanism. It is just a part of larger system representation. Engine movement is transformed into electrical energy and then transferred to the actuator. It demonstrates clarity and simplicity of graph representation.

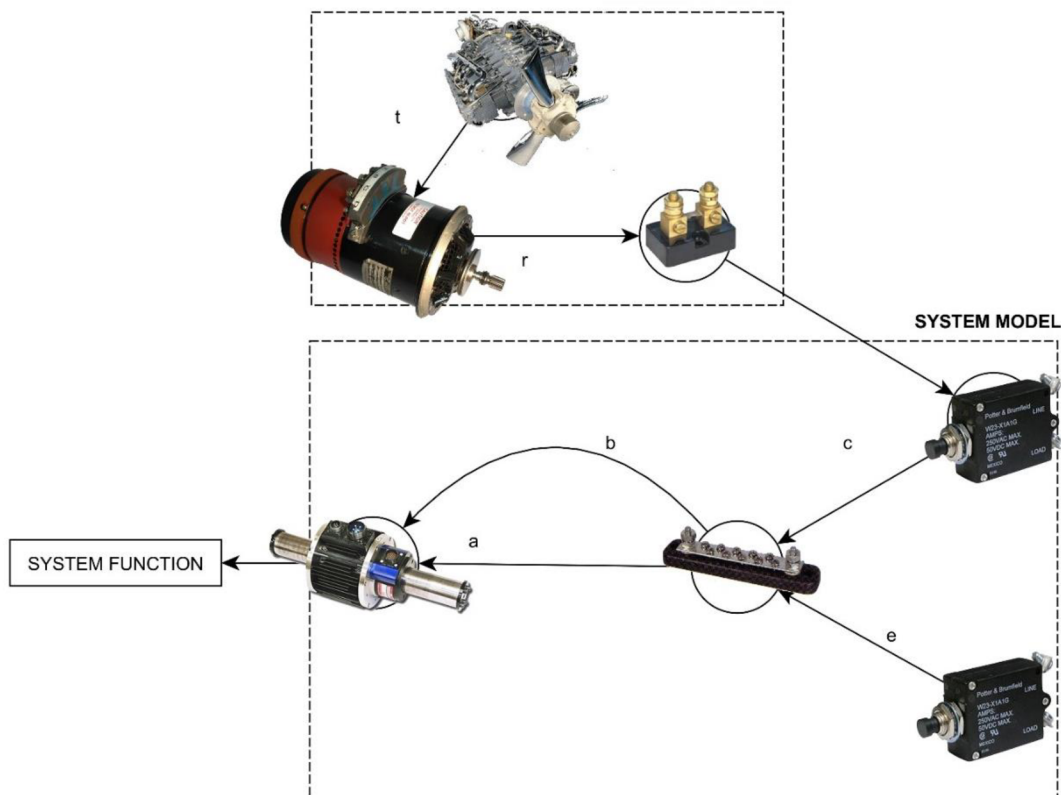


Figure 18 Simplified trim system model example

A graph representation is main part of integrated method. Whole process and graph theory contribution to the other parts is discussed in following chapters.

4.2 MODEL PROCESSING

System representation in the form of graph should serve as a universal data structure for subsequent manipulation and assessing. Using the common tools for graph creation general-purpose diagramming programs and open source programming languages it is possible to establish accessible parametric model of particular airborne system.

It is very easy to find a parallel to data structure. In modern computer aids for 3-D interactive application (Dassault Systèmes CATIA, Autodesk Inventor, etc.) is particular model or assembly described by a tree. A tree represents lines, curves, surfaces, components and its parameters (dimensions, material, density, etc.) in form of a graph as well. Tree elements may be modified, re-connected or implemented into another model.

A graph representation is one of the most universal data structures. Further trough computerization it is possible to properly adjust algorithm for real application integrating knowledge and experiences collected during the critical review, case study and potential real test applications.

Through the top-down layering of graph representation, the system and its functions (from essential to non-significant to the system safety) may modeled. Computerization brings huge potential for method development, its usability, tabulated or graphical results and adaptability.

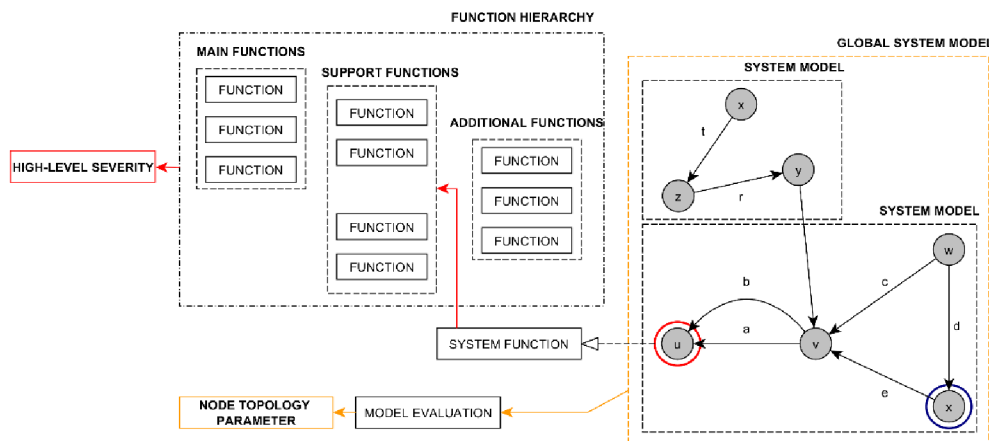


Figure 19 Graph theory application

4.3 MODELING PRINCIPLES

Applied **function oriented** approach basically models system functions. Unlike design scheme, function base modeling represents sequence of functions provided by items. Item is represented by a **node** (vertices). For each node, there are various basic attributes like type, system participation, zone, occurrence, detectability, severity and criticality. These attributes will be described in deep in following chapters. Interconnection is represented by an **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.

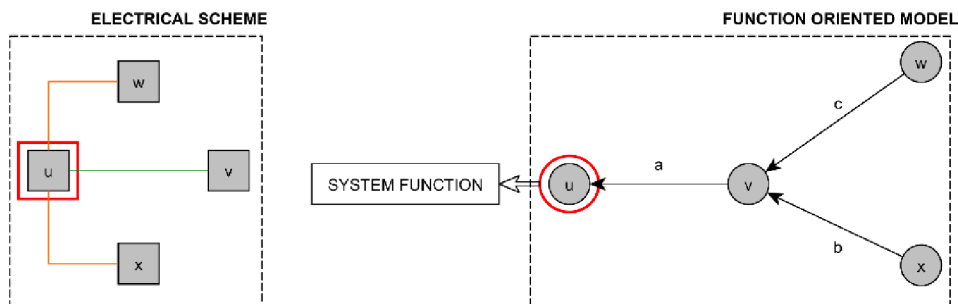


Figure 20 Function based modelling example

Example in Figure 20 describes fundamental difference between physical interconnection provided by drawing or scheme 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.

4.3.1 Function propagation principle

Function based modeling is (in this doctoral thesis) 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* though 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).

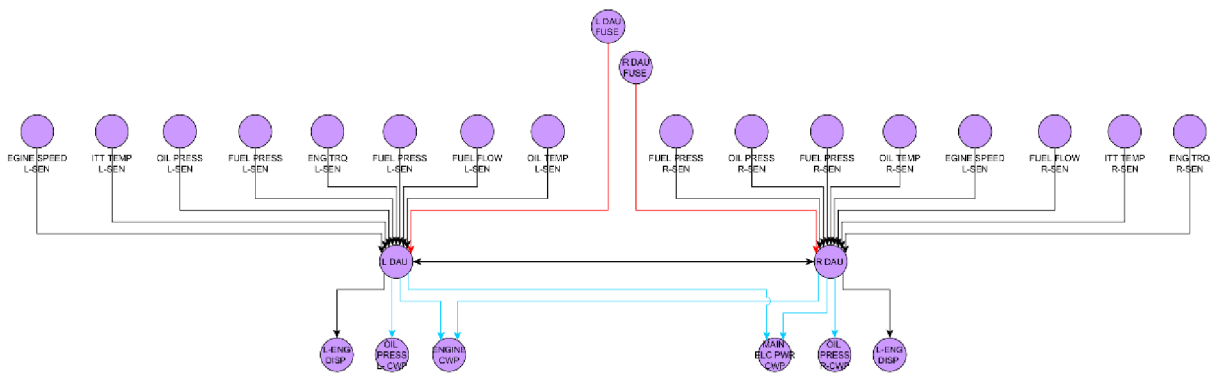


Figure 21 Case study engine indication model

Table 3 presents list of possible node-edge relation. It describes their nature and gives visual example.

Table 3 Node- edge relation explanation

Node- edge relation	Description
	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/I) – acting item- providing the function itself) node in direct line of function. Node is excluded from graph topology evaluation.

4.3.2 Global and local models

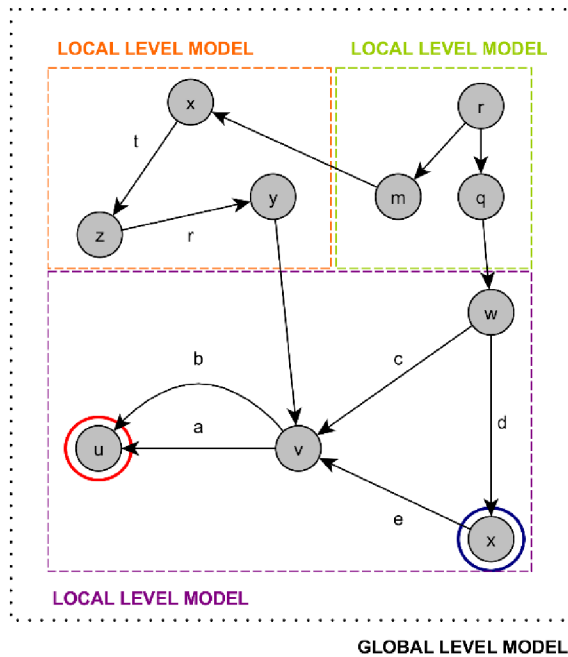


Figure 22 Global and local model

One of the key elements of integrated method architecture is to identify interconnection between items on the wide level. To adopt outlook of global level.

Items are usually associated with several functions on system or **local level**. However, multiple of them are 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.

As example see Figure 21, L DAU fuse is on the local (system level) only connected to the L DAU unit. Logically, fuse is just safety mechanism, how to protect electrical system from shortcut. On the global (airplane) level, L DAU fuse is connected to the electrical bus.

Item functionality could have much larger influence to **MSO** on the wider global level. Function based modelling significantly assists in the process of interconnection identification.

4.3.3 Interconnection layering

In the chapter 4.3.1 Function propagation principle, types of items interconnection had been already discussed. It is essential to distinguish between particular types of connections in order to organized model to precise **operational mode**- complex system like avionics or electrical could be reconfigured for different modes like engine start or generator loss.

There is a huge physical difference between mechanical, electrical, signaling or data interconnection in the detectability of failure, occurrence of failure, etc. As it is mentioned many times in this doctoral thesis, model is interconnected in order to provide particular function. Interconnections themselves contribute to providing this functions.

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.

Operational modes examples:

- a) Standard function
- b) Engine start/ Engine cross-start
- c) One engine or generator failure
- d) Multiple engine or generator failure
- e) Hydraulic system failure
- f) Fuel distribution malfunction
- g) Primary flight control means malfunction

Doctoral thesis case study is restricted to flight mode operational mode.

Nature of interconnections

Items could be associated with multiple functions. Otherwise, edge is usually associated with specific function. Functions are provided by sequence of items functionality. Type of function could be labeled in the model to clearly identify node and edge allocation.

Figure 23 shows case study avionics system with labeled various types of interconnection.

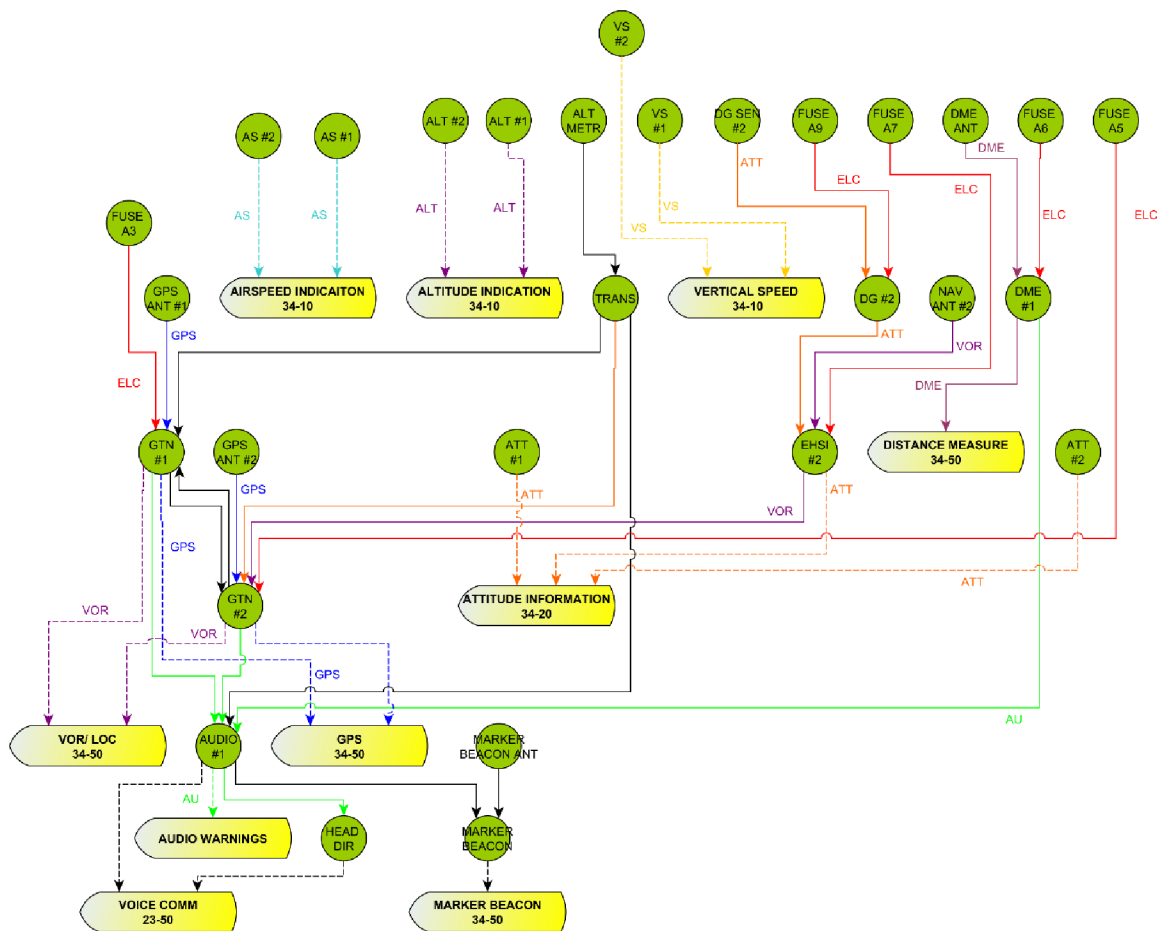


Figure 23 Case study avionics system with various types of interconnection illustration

Interconnection significance

Influence of all nodes and edges is not equal. It is based on their function allocation, detectability, occurrence, etc. System model could be filtered in order to analyze only *significant* function sequences based on NO SAFETY EFFECT, MINOR, MAJOR, HAZARDOUS, CATASTROPHIC classification (see

2.3.2 EASA CS-23 Certification Base). It is quite useful during formal and structured safety and reliability analysis.

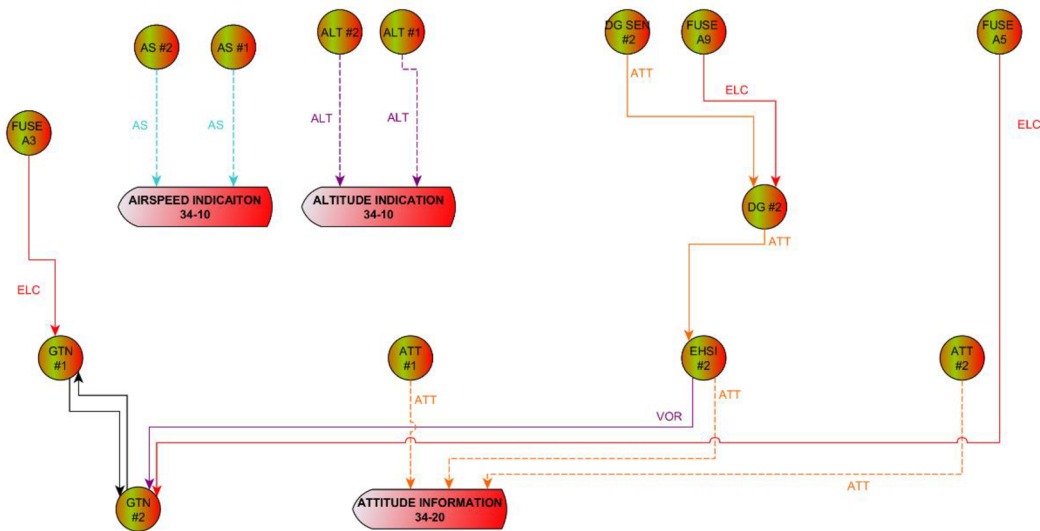


Figure 24 Case study avionics filtered for HAZARDOUS associated nodes and edges (restricted for illustration)

4.4 A GRAPH THEORY BASICS

In last fifty years, a graph theory is getting more and more interest. Any mathematical object involving points and connections between them may be called a graph. If all the connections are unidirectional, it is called a digraph. [15]

Graph theory could be used to model any types of physical interconnection between elements. Airborne systems decomposed into subsystems consist of physical items. These items could be considered as a vertices and mutual interconnection as edges. This pair is a key element of graph theory.

4.4.1 Basic definitions

Graph [15]

A graph is a pair $G = (V, E)$ which consists of two sets V and E .

Where:

- The elements of V are called **nodes (vertices)**.
- The elements of E are called **edges**.
- Each edge has a set of one or two vertices associated to it, which are called **endpoints**.
And edge is said to **join** its endpoints.

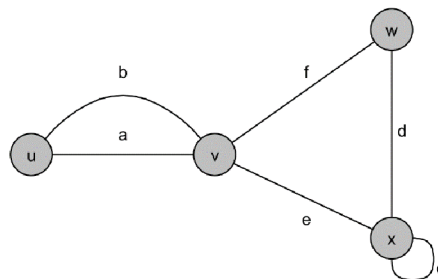


Figure 25 $V = (u, v, w, x); E = (a, b, c, d, e, f)$

Directed graph [15]

A directed graph (or digraph) is a pair $G = (V, E)$ which consists of two sets V and E .

Where:

- The elements of V are called **vertices (nodes)**.
- The elements of E are ordered pairs, called **arcs** (or **directed edges/ arrows**)

An arc $e = (x, y)$ is directed from x to y . Simply stated y can be called the head and x the tail. An orientation of graph is reached by assigning a direction to each edge. Any directed constructed this way is *oriented graph*. A directed is an oriented graph if and only if it has none self-loops nor 2-cycles.

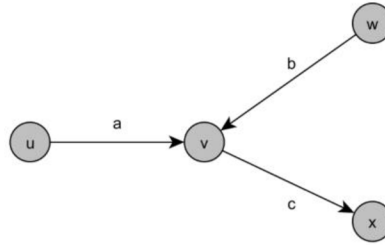


Figure 26 Oriented graph example

Graphs could be easily mathematically represented by several ways. Most common is graph representation by adjacency matrix. An **adjacency matrix** for simple graph G example, where vertices are in order $v_1, v_2, v_3 \dots v_n$ is $n \times n$ matrix A_G .

Where:

$$A_G(i, j) = \begin{cases} 1 & \text{if there is edge from } v_i \text{ to } v_j \\ 0 & \text{other than that} \end{cases}$$

Equations 1

Adjacency matrix for graph example.

$$A_G = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Equations 2

It is also possible to represent graph by incidence matrix. For simple graph example G , it is a matrix I

$$I(v, e) = \begin{cases} -1 & \text{if edge } e \text{ is directed to vertex } v \\ 1 & \text{if edge } e \text{ is directed from vertex } v \\ 0 & \text{other than that} \end{cases}$$

Equations 3

$$I[v, e] = \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

Equations 4

Furthermore, there is a possibility to use adjacency list. It is used for mathematical representation of graph $G = (V, E)$. Adjacency list is an array L of $|V|$ lists (one of each vertex). Pointer L_i is linked to a list containing all vertices j adjacent to i .

$$v_1 = \{v_2\}$$

$$v_2 = \{v_1, v_3, v_3, v_4\}$$

$$v_3 = \{v_3, v_4\}$$

$$v_4 = \{v_2, v_3\}$$

Equations 5

For practical purposes, it is necessary to extended simple graph (where two vertices are connected by just one edge) by using multigraphs (two vertices can be connected by number of edges and loops also). Multigraphs allows to model a system with parallel connection between items.

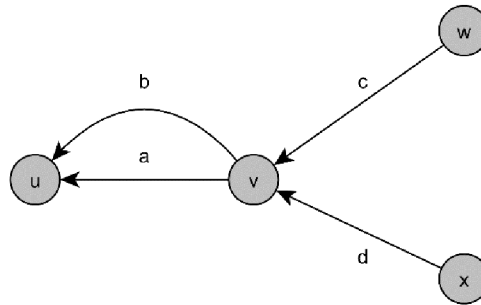


Figure 27 Multi-graph example

$$I[v, e] = \begin{pmatrix} 0000 \\ 2000 \\ 0100 \\ 0100 \end{pmatrix}$$

Equations 6

Subgraph

A subgraph of graph example G is a graph Q, where $V_Q \subset V_H$ and $E_Q \subset E_H$. Induced subgraph of graph example G with set of vertices $v_1 = \{w_1, \dots, w_k\}$ denoted W, has W vertex-set and it contains every edge of graph G whose endpoints are in W. [15]

$$V(G(W)) = W \text{ and } E(G(W)) = \{e \in E(G) | \text{the endpoints of edge } e \text{ are in } W\}$$

Equations 7 Subgraph definition [15]

Graph theory fundamentals are intentionally left out. These principles and rules are for example described in Handbook of Graph Theory [15].

Shortest-path Problem and Dijkstra's algorithm

It is one of the most basic and essential problem in graph theory. Path between two nodes, whereas the sum of the weight of particular edges is minimal possible. Most frequent usage of problem solution is in road navigation, communications, etc.

There is a plenty of important algorithms for problem solving. One of them is Dijkstra's algorithm developed by computer scientist Edsger W. Dijkstra in 1956.

It allows finding shortest path form given initial node to the final node assuming there is numerical edge length (witch can represent various quantities related to the graph usage, for instance failure rate in reliability assessment). The **distance** between two nodes in a graph is length of a shortest path from initial to final node

The shortest path is a tree rooted at initial node, contacting all nodes that are reachable from initial node. Figure 28 illustrates shortest path tree, where length of edges is described by $a < b$; $c = e = d$.

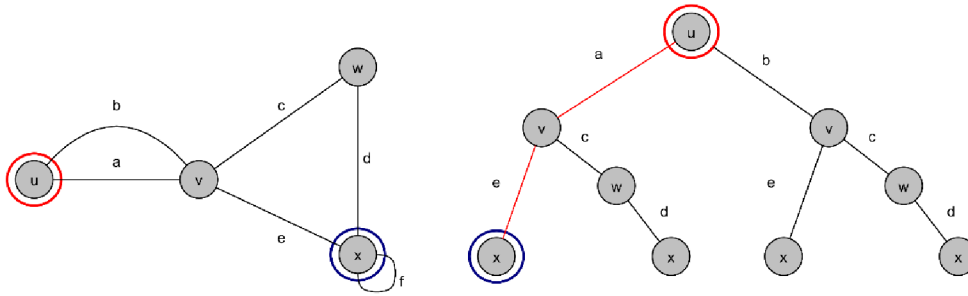


Figure 28 Shortest path tree for graph example

Nowadays there is lot versions of Dijkstra’s algorithm adjusted to the particular situations. Solution made by using Dijkstra’s algorithm could be enormously time consuming. Therefore, it effective to implement priority queues (for instance binary heap) for short path problem solution in the case of complex system.

4.4.2 Graph handling in doctoral thesis

Presented definitions and principles serves as very essential base for further system graph (or network) modeling, processing and evaluating. This doctoral thesis is focused on creating integrated method of safety and reliability assessment of airborne system. Graph theory is applied as a modelling platform. It also provides means how to describe model and evaluated its structure.

Graph theory is extensively applied on various engineering and scientific problems. Biology is one of most interesting example of graph theory application. It is used for visualizing molecular interaction and biological pathways. Graph theory application is inspired from biology application, uses graph (network) structure description parts, not estimation and probabilities. Doctoral thesis adopts several biology based means and principles for instance [49], [34], [37], [38], [52].

Therefore, it is possible to use already existing open-source software to model, process and evaluate system instead of painfully creating new and potentially bugged codes.

Model itself is created in graph modelling and editing program on xml format platform. Each node has a set of created attributes (see 4.2 Model Processing). Edges has a similar set of attributes. These attributes will described in full in following chapters (Chapter 5).



Figure 29 Processing platform [Cytoscape. org]

Model processing and evaluation is done in open source Cytoscape 3. Cytoscape is an open source software platform for visualizing networks. Although Cytoscape was originally designed for biological research, now it is a general platform for complex network analysis and visualization. Cytoscape core distribution provides a basic set of features for data integration, analysis, and visualization. Additional features are available as Apps (formerly called Plugins). Apps are available for network and molecular profiling analyses, new layouts, additional file format support, scripting, and connection with

databases. They may be developed by anyone using the Cytoscape open API based on Java™ technology and App community development is encouraged. [Cytoscape.org]

4.5 BASIC GRAPH ATTRIBUTES

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 (“cluster”) 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

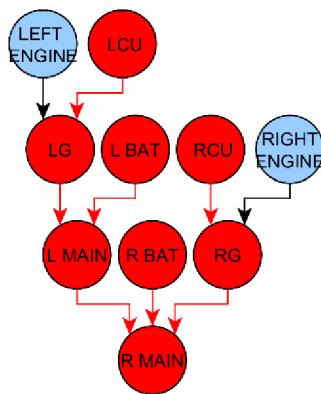


Figure 30 Case study R MAIN bus predecessor example

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 (defined in 7.2.1 Electrical System). 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.

Logically, system function is influence by many other factors (like control unit setting, engine regimes, operation modes). However, presented mean is highly useful for the analysis purposes or system study itself.

Successors

The other side of a coin is a 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 31 (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 the particular loads. These items provide particular function. Combination of support function provides intended high function resulting in Main Function.

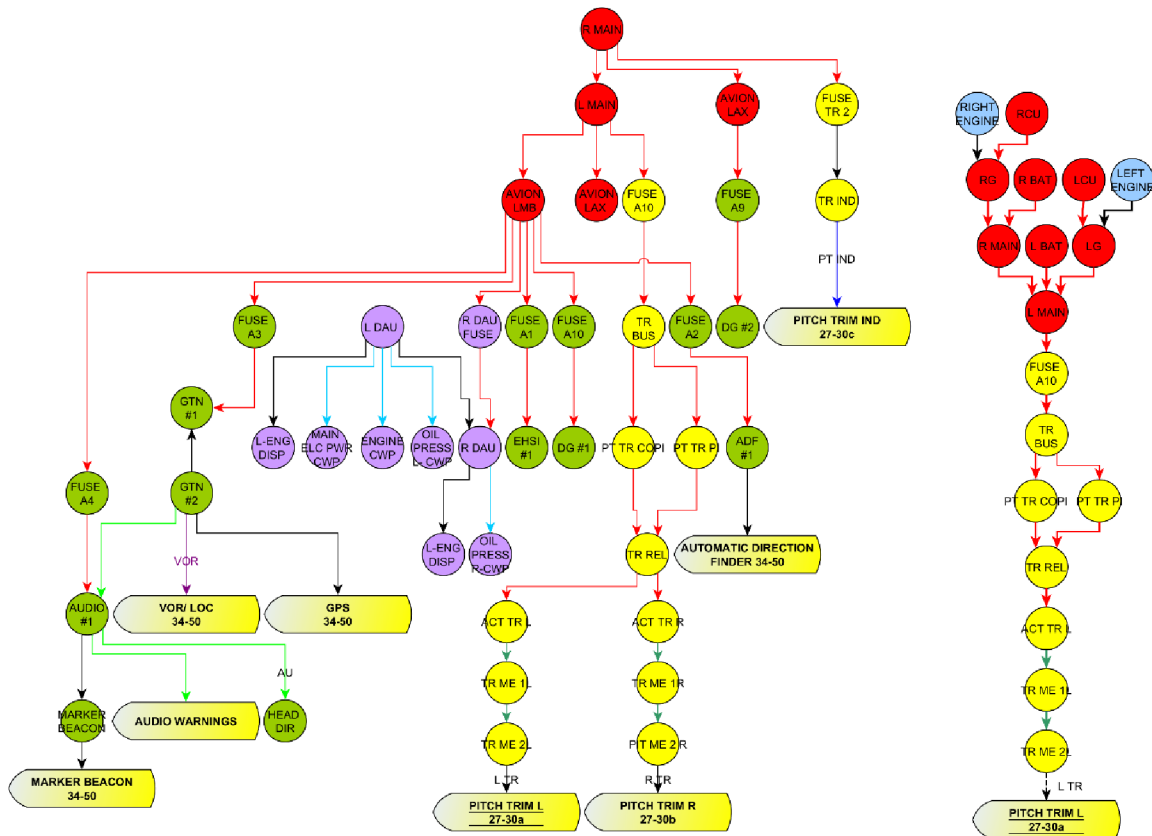


Figure 31 (a) Case study R MAIN bus successors example (restricted for illustration purposes) (b) Pitch trim sequence

Item-function relations

Function modeling serves in this case as a 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- one of them is 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.

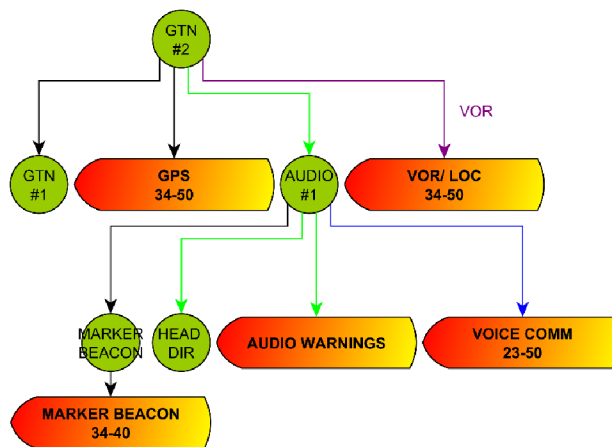


Figure 32 Case study GTN #2 succeeding function

In combination with knowledge database (**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).

Table 4 Case study GTN #2 functions severity preliminary classification (restricted for illustration purposes)

<i>Function</i>	<i>Flight phase</i>	<i>Preliminary classification/ membership volume</i>
34-50 Dependent Position Determining- <i>Global positioning system- loss of function.</i>	ALL (except LDG)	MINOR FS 2
	LDG	HAZARDOUS FS 7,5
34-50 Dependent Position Determining - VHF omnidirectional range- <i>loss of function</i>	ALL	MINOR FS 2
23- 50 Audio Integrating- <i>loss of function</i>	ALL	HAZARDOUS FS 7,25
23- 40 Instrument landing system- <i>loss of function.</i>	APR, LDG	MAJOR FS 6 IFR/IMC/ CATASTROPHIC FS 10

4.6 THE 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. [15]

From the system engineering point of view, trees are already essential part of particular failure mode analysis. Fault trees analysis proceeds by determining how failure can be caused by individual or combined lower level failures or events (described in 2.5.2 Standard Safety and Reliability Assessment Tools). Creating FTAs is difficult deductive process. It involves deep understating of system functions and mutual interconnection. Function based 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.

4.6.1 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 incorporate in the formal analysis. Integrated method contains simple **recursive algorithm** designed to evaluate particular failure (due to function based modeling).

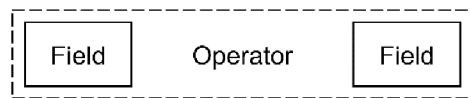


Figure 33 Recursive algorithm block- Field-operator-field

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 set of rules. To run a procedure means that to perform a step and follow the given rules.

Process could be described by using a 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).

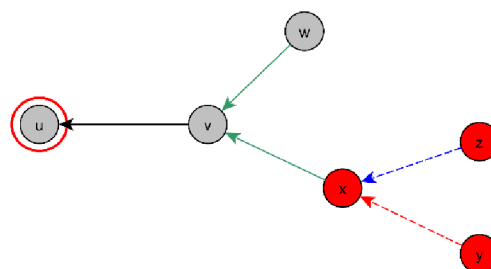


Figure 34 System example- partially in failure

When a node is terminal, probability of failure depends only on its own failure rate. Recursive process is possible to define by two parameters:

- **Base case-** Rule terminating the recursive process
- **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.

Recursive algorithm block

Block uses tree data structure. It provides a way how to evaluates relation between nodes. This relation dependency is expressed by a given *operator*.

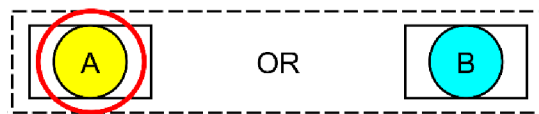


Figure 35 Recursive algorithm block- single input example

In the Figure 35, the left *field* is for **assessed** node and the right *field* is for **preceding** node or set of nodes. *Operator* depends on type of inputs.

Table 5 Recursion operators application

Operator	Inputs	Description
OR	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.
	Any	A node is defined as OR gate for preceding items.
AND	Multiple inputs of same type	There has to be failure of all input nodes.
	Any	A node is defined as AND gate for preceding items.

If there are multiple inputs, right *field* (of the recursive algorithm block) is filled by lower level recursive algorithm block (see Figure 36).

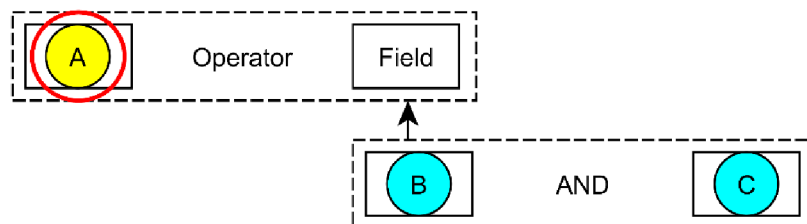


Figure 36 Recursive algorithm block- multiple input of same type example

This procedure continues until right field is occupied by a terminal node. It means that algorithm reached to the point where a given node failure rate express probability of failure on a given level (when the node is terminal).

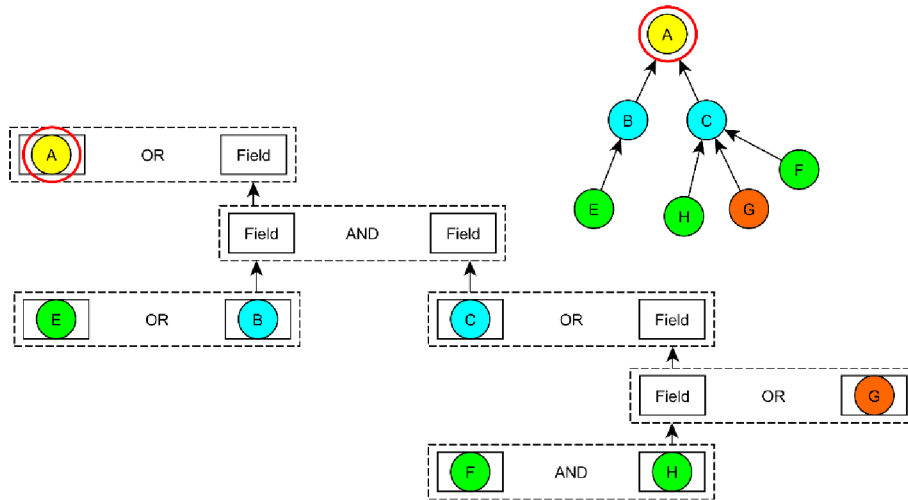


Figure 37 Recursive algorithm block-complex inputs example

4.6.2 Recursion example

In the Figure 38, system example (slightly adjusted for illustrative purposes) used through the doctoral thesis is evaluated by recursive algorithm. Direct edges connecting nodes **w** and **x** with node **v** are defined as same type (for instance electric wires). Directed edges connecting nodes **z** and **y** with node **x** are defined as different type.

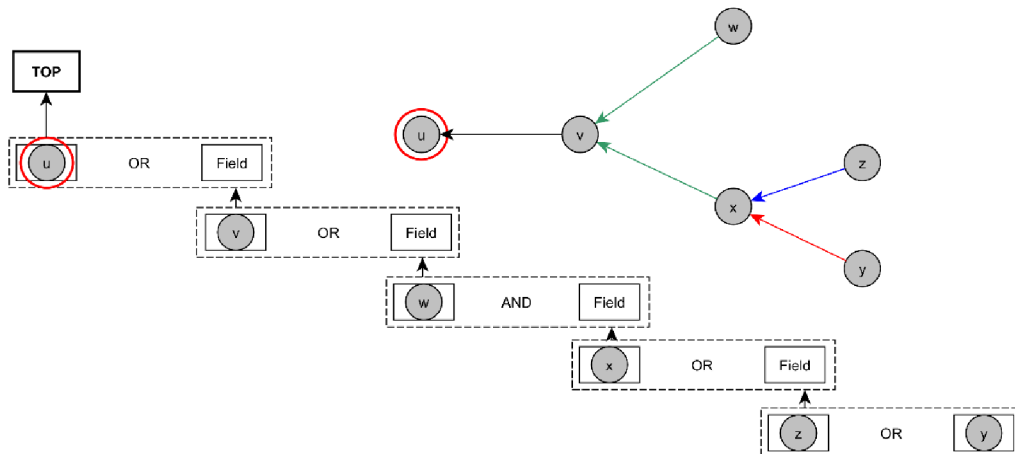


Figure 38 Recursive algorithm logic applied on system model example

Example illustrates how recursive algorithm is propagated through the system model from initial node to the terminal. Each node could have several failure modes which could result or at least contribute to the system failure. Knowledge base B (**Appendix B**) gives a limited summary of various items failure rates and failure modes. It is up analyst to select which failure modes are relevant to the particular failure mode.

Figure 39 (on the left side) shows rough tree resulting from system example evaluation. This failure mode probability could be estimated by using FTA direct technique described in following chapter. The right side of same figure shows rough tree after OR gate aggregation.

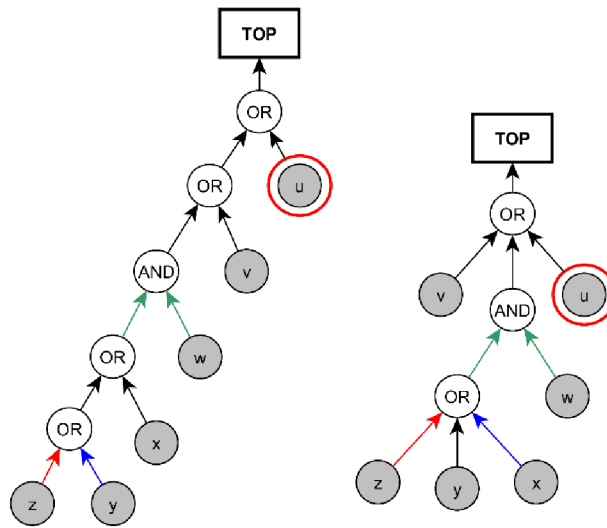


Figure 39 Recursive algorithm out before (left) and after OR gates aggregation (right).

4.6.3 Rough tree failure rate estimation

Using the recursion algorithm, it is possible to obtain rough fault tree (explained above). It is possible to estimate failure rate of this rough tree by using FTA direct technique.

Table 6 FTA direct technique estimation [14]

AND GATE	OR GATE
$P(G) = \prod_{i=1}^{i=s} P(A_i)$	$P(G) = 1 - \prod_{i=1}^{i=s} [1 - P(A_i)]$

4.7 GRAPH MODEL STRUCTURE AND TOPOLOGY

There are a lot of potentially useful algorithms and tools. System model structure could be evaluated through various parameter. These parameters describe model topology, node position and importance. It provides a bigger picture of node (or edge) interrelations.

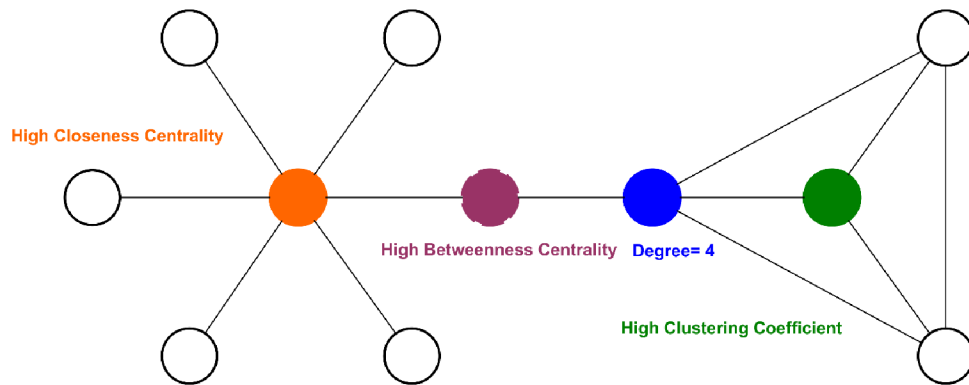


Figure 40 Centrality, degree and clustering coefficient definition

Graph model processing results in several types of importance lists. These lists are based on selected node parameter. For instance, centrality measure indicated how densely is node is linked with other node in a given system or on global level. Node in and out degree give an information how is node functionality related to preceding node and how influences subsequent nodes.

4.7.1 Fundamentals of graph

Indegree and Outdegree

The **indegree** of a vertex v in a graph G is the number of arcs directed to v . The **outdegree** of vertex v is the number of arcs directed to from v . Each self-loop at v counts one towards the indegree of v and one toward the out degree. [15]

In directed graph, the sum of the indegrees and the outdegrees both equal the number of edges. [15]

A walk

A walk in a graph G is an alternating sequence of a vertices and edges, $W = v_0, e_1, v_1, e_2, \dots, e_n, v_n$. Such that for $j=1, \dots, n$, the vertices v_{j-1} and v_j are endpoints of the edges e_j . If, moreover, the edge e_j is directed from v_{j-1} to v_j , the W is a directed walk. The initial vertex is v_0 , final (or terminal) vertex is v_n . The internal vertex is a vertex that is neither initial nor final. [15]

Distance and connectivity [15]

The **directed distance** from a vertex u to a vertex v in a directed graph is the length of shortest directed walk from u to v .

- A graph is connected if between pair of vertices l s walk.
- A directed graph is **(weakly) connected** if its underlying graph is connected
- A directed graph is **strongly connected** if from each vertex to each other vertex is a directed walk
- The **eccentricity** of a vertex v in a connected graph is its distance to a vertex farthest from v
- The **radius** of a connected graph is its minimum eccentricity
- The **diameter** of a connected graph is its maximum eccentricity

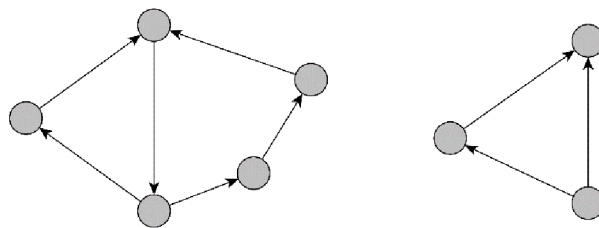


Figure 41 A strongly connected (left) and weakly (right) connected directed graph

Network (model) diameter

It is the largest distance between two nodes. If the network is disconnected, it is maximum of all diameters of its connected components.

4.7.2 Network Position

Centrality

It is a structural (geometrically related) property of network. For these network measures, centrality refers to the geometric center or the level of importance. [35]

Betweenness centrality (BC)

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

$$C_B(n) = \sum_{s \neq n \neq t} \left(\frac{\sigma_{st}(n)}{\sigma_{st}} \right) \quad \text{Equation 4}$$

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. [33]

The BC of a node reflects the amount of control that this node exerts over the interactions of other nodes in the network. [34]

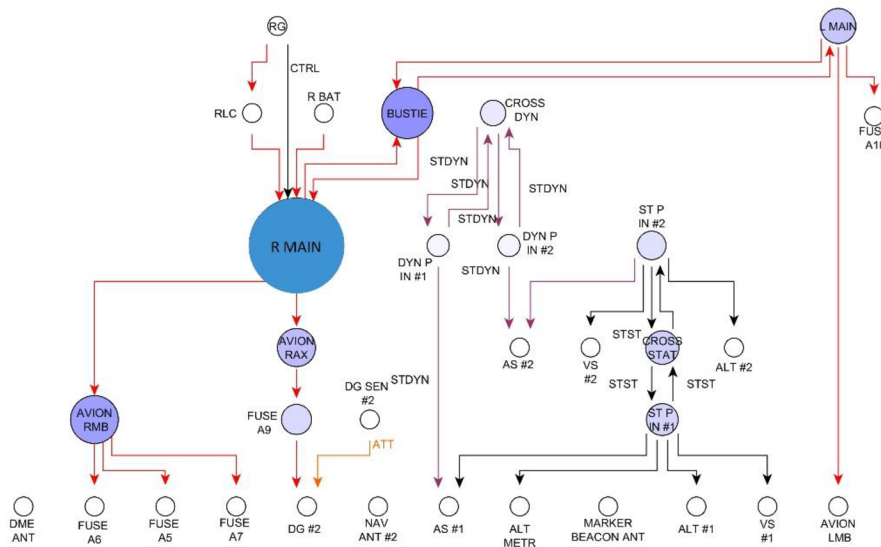


Figure 42 Example system betweenness centrality illustration (BC correspond to the edge size)

This measure identifies and favors nodes that join separated systems (electrical with avionics, electrical with engine control, etc.), dense subnetworks respectively, rather than nodes inside particular system. Betweenness centrality ranking determine item importance on the wider (global level).

Closeness centrality (CC)

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

$$C_{BC}(n) = \frac{1}{avg(L(n,m))} \quad \text{Equation 5 [35]}$$

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 [35].

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.

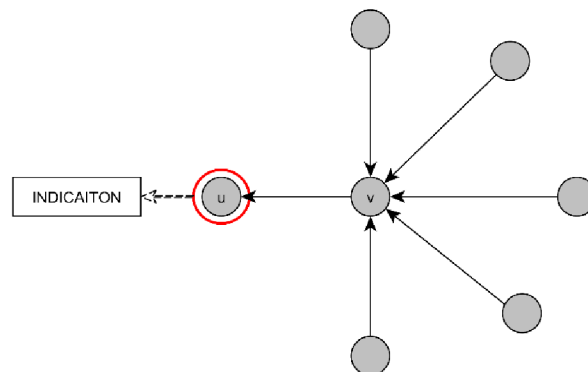


Figure 43 Closeness centrality example

Edge betweenness

This attribute stores the edge betweenness of each edge normalized by dividing by $(M-1)(M-2)$, where M is the number of edges in the connected component that the edge belongs to. The edge betweenness of $e = (v, w)$ is defined as the number of shortest paths between two nodes s and t that go through e divided by the total number of shortest paths that go from s to t . [36]

Subgraph Centrality (SubG) [38]

Method for characterizing nodes in network according to the number of 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 i is 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 .

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

Equation 6 [38]

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 \mathbf{A}

$$\mu_k(i) = (\mathbf{A}^k)_{ii}$$

Equation 7 [38]

Detailed description of subgraph centrality is provided in ESTRADA E., RODRÍGUEZ- VELÁZQUEZ J., Subgraph centrality in complex networks, Physical Review E 71, 056103, 2005 [38]

This centrality measure was tested on several artificial regular graphs and compared to other centrality measures.

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. [37]

$$C_{cen}(v) = \min(f(v, w): w \in V(v)) \quad \text{Equation 8 [37]}$$

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 37]

Local patterns and Clustering

Express likelihood of items mutual influence on their functions. It is expressed by clustering coefficient of a node is C_n defined as

$$C_N(v) = \frac{2 \cdot e_n}{(k_n \cdot (k_n - 1))}$$

Equation 9 [37]

Where k_n is the number of neighbors of node n and e_n is number of connected pairs between all neighbors of n . Clustering coefficient is a ration N/M , where N is the number of edges between the neighbors of n , and M is the maximum number of edges that could possibly exist between the neighbors of n . The clustering coefficient of a node is always number between 0 and 1.

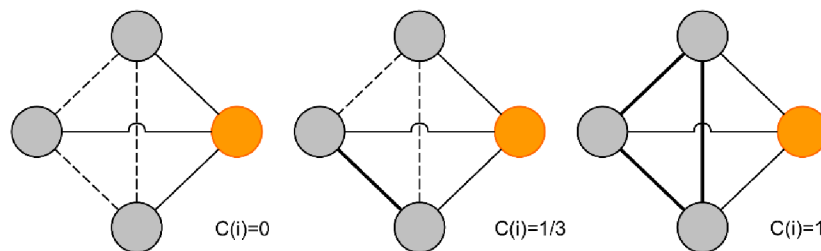


Figure 44 Clustering coefficient

Network clustering could serve as a sort of additional control mechanism. If it is applied on the system network.

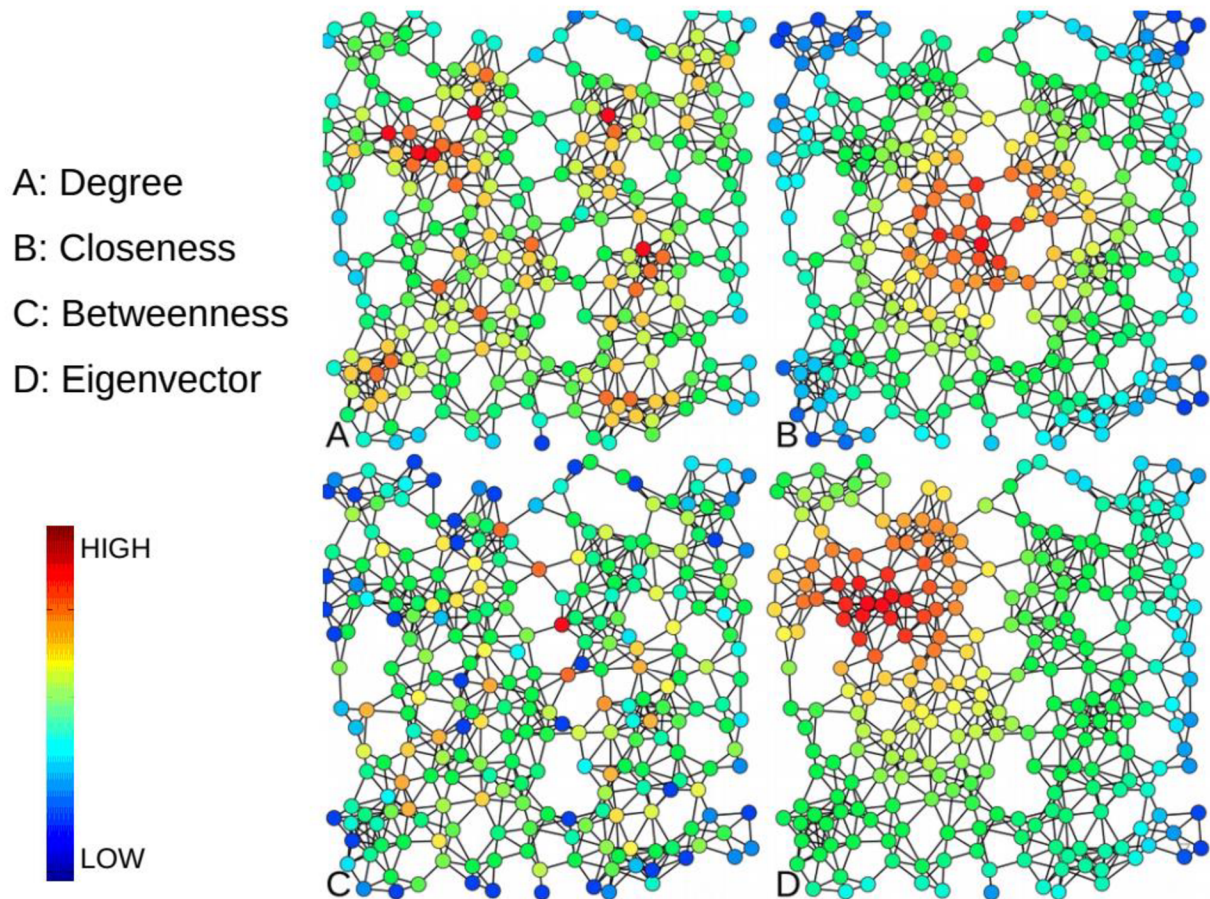


Figure 45 Graph centralities illustration [49]

4.8 MODEL PARAMETERS

System model (consisting of nodes and edges) could be evaluated as whole or by particular nodes. It gives additional information about model structure and topology. Following chapters show difference between different systems.

Global parameters show, that model clustering coefficient reflect, how particular node cluster together, how dense the network is. It partially reflects system complexity. Avionics system clustering coefficient is similar to the global network. Elevator trim model is structured as acyclic graph- a tree. There are no multi-edge nodes pairs- it is single purpose system designed to trim the elevator. This information could be stored for further comparison. A database with different applications will be established for following development of integrated method.

Table 7 Case study model parameters (global)

GLOBAL			
<i>Clustering coefficient</i>	0,015	<i>Number of nodes</i>	102
		<i>Number of edges</i>	132
<i>Diameter</i>	12	<i>Multi edges node pairs</i>	11
<i>Shortest path</i>	1193 (11%)	<i>Average number of neighbors</i>	2,37

Table 8 Case study model parameters (avionics)

AVIONICS			
<i>Clustering coefficient</i>	0,012	<i>Number of nodes</i>	39
		<i>Number of edges</i>	40
<i>Diameter</i>	5	<i>Multi edges node pairs</i>	4
<i>Shortest path</i>	130 (8%)	<i>Average number of neighbors</i>	1,846

Table 9 Case study model parameters (elevator trim)

ELEVATOR TRIM			
<i>Clustering coefficient</i>	0,0	<i>Number of nodes</i>	13
		<i>Number of edges</i>	14
<i>Diameter</i>	6	<i>Multi edges node pairs</i>	0
<i>Shortest path</i>	53 (33%)	<i>Average number of neighbors</i>	2,154

4.9 EVALUATION PROCESS AND OUTPUTS

The main goal of graph model processing is to identify important nodes (and possibly edges) of a system. The node importance is established on various bases. Node influence on connecting multiple system (function cross-connection). Particular nodes cluster various functions of items in order to provide particular function. Engine data acquisition unit is a typical example of it. Dozens of sensors measure various engine parameters. These data are collect in these units in order to establish engine functionality.

Evaluation process results in **node topology parameter** (NTP), which is one of the inputs to the fuzzy criticality evaluation. It also provides **several important node lists** to the analyst. These lists could be extremely useful during formal safety and reliability assessment.

4.9.1 Evaluation process outputs

Evaluation process is demonstrated on case study systems set (see Chapter 7Chapter). Application on this set of systems proved usage of graph theory based measures. At the Table 8 partial results are presented. List shows most important nodes sorted due to their betweenness centrality parameter. This parameter represents node importance as connector of various sub-systems clusters and system (on the global) level. The most important node is in this case is L MAIN electric bus. It is a logical result. Electrical system is taken as example of node importance overlap on global level. L MAIN bus supplies essential parts of avionics system as well as elevator trim system. Difference between left and right main buses importance is partially result of case study restriction (for instance elevator control, flaps, ailerons are left out due to case study simplification). On the third spot is BUSTIE contactor. The contactor interconnects both main buses in the case of generator (or distribution sequence) failure. Avionics buses (AVION LMB/ RMB) and line contactors (LLC/ RLC) as a key parts of distribution sequence are pointed out.

Data acquisition units are first items on the list other than electrical system members. These units collect engine parameters, process them and display to the flight crew. They also process and transmits notification information, warning and caution indication. Be aware that these result do not reflect importance of particular function.

Table 10 Case study evaluation process output

System	Node name	In-degree	Out-degree	Centralities				Centroid volume	#
				BC	#	SubG	#		
ELCSYS	L MAIN	3	4	0,0441	1	6,61	9	54	11
ELCSYS	R MAIN	3	4	0,0383	2	6,42	11	54	11
ELCSYS	BUSTIE	2	2	0,0250	3	2,79	35	54	11
ELCSYS	AVION LMB	1	7	0,0220	5	9,63	6	23	14
ELCSYS	AVION RMB	1	5	0,0204	6	6,61	10	22	15
EIND	L DAU	10	5	0,0181	7	24,86	1	8	39
EIND	R DAU	10	5	0,0181	8	24,78	2	8	39
ELCSYS	LLC	1	1	0,0163	9	2,59	42	55	7
ELCSYS	RLC	1	1	0,0163	10	2,57	45	55	7
TRIM	FUSE A10	1	1	0,0129	11	2,59	43	11	19

As last item on the list is elevator trim fuse. This item interconnects elevator trim to the electrical network and protect it in the case of shortcut. High volume of betweenness centrality is logical.

Table 11 Case study evaluation process output 2

System	Node name	In-degree	Out-degree	Centralities				Centroid volume	#
				BC	#	SubG	#		
EIND	L DAU	10	5	0,0181	6	24,86	1	8	39
EIND	R DAU	10	5	0,0181	6	24,78	2	8	39
AVIO	AUDIO #1	6	2	0,0046	20	13,76	3	1	77
AVIO	GTN #2	7	2	0,0067	15	12,25	5	4	61
AVIO	GTN #1	6	1	0,0016	36	10,83	6	2	74
ELCSYS	AVION LMB	1	7	0,0220	4	9,63	7	23	14
AVIO	DME #1	2	3	0,0024	27	9,11	8	5	54
AVIO	TRANS	1	3	0,0020	28	7,87	9	5	54
ELCSYS	L MAIN	3	4	0,0441	1	6,61	10	54	11
ELCSYS	AVION RMB	1	5	0,0204	5	6,61	11	8	39

Next table shows evaluation process output from the different point of view (Table 11). Nodes are sorted by their subgraph centrality parameters. Subgraph centrality prefers local node importance. Typical examples of local importance are processing and controlling components. Case study evaluation identified as most locally important items DAU units, audio panel, GTNs, etc. These outputs are quite intuitive. Node local importance in this context means high subgraph centrality parameter. This parameter represents node closed walks, that start and ends in a given node. Contribution (to the subgraph centrality) of these closed walks decreases as the length of the walks increases. Results show

that DAU unit in-degree is ten and out-degree is five. For the case study model it is unprecedented. Even GTNs has lower in and out degree ratio (partially due to model limitation and simplification). It indicates high level of function clustering. Function related to these items are hugely depends on their functionality. Temperature and pressure sensors are relatively simple components (and usually designed as multi-redundant). Provided information could be at least partially subtitled by reaming inputs in the case of failure. However, these inputs have to be processed and presented to the flight crew. Pressing units are logically the most important nodes at the system (local) function sequence.

All these parameters expand and complete (at the possible level) analyst understanding of a given system and airplane level relations. It is not possible to stated which parameter is generally most important. It depends on particular application. Analyst could choose the dominant parameter (or adjust its preference) for node topology parameter establishing. Nevertheless, importance list main usage is to put substantial nodes to the spotlight for further evaluation and possible re-design.

4.9.2 Weight of function

In previous subchapters, node local and global importance is evaluated based on graph model interconnections. However, this evaluation does not include function allocated to the particular node (and their severity). Particular function has a position in the function hierarchy (3.2 Function Hierarchy) based on its relation the main function and severity of failure consequences. Particular nodes and edges have different weight of severity.

Position parameters of a node are weighted by allocated function to the node. Weight is related to the amount of function severity (logically subjective measure).

Table 12 Case study evaluation process output and allocated functions

System	Node name	Allocated functions					
		EL4	x	x	x	x	x
ELCSYS	L MAIN	EL4	x	x	x	x	x
ELCSYS	R MAIN	EL4	x	x	x	x	x
ELCSYS	BUSTIE	EL4	x	x	x	x	x
ELCSYS	AVION LMB	EL4	x	x	x	x	x
ELCSYS	AVION RMB	EL4	x	x	x	x	x
EIND	L DAU	L EI5	L EI2	L EI7	L EI3	L EI6	L EI1
EIND	R DAU	R EI5	R EI3	R EI6	R EI1	R EI4	R EI7
ELCSYS	LLC	EL4	x	x	x	x	x
ELCSYS	RLC	EL4	x	x	x	x	x
TRIM	FUSE A10	ET1	ET2	x	x	x	x

Severity input is defined in following chapter (5.2.1) as an input to the fuzzy criticality evaluation. Each node and edge has an allocated function in the graph model. Function has specific identification code. Table 12 shows allocated function to case study the most important nodes base on betweenness centrality. Case study definition, complete importance lists and allocated function are described in the chapter (Chapter 7).

Selected graph position parameter is multiplied by aggregated severity (see 5.2.1). These adjusted measures could be used during system analysis (and possible re-design) or used as basis for node topology parameter instead of regular position parameters.

Table 13 Case study evaluation process output- weighted

System	Node name	In-degree	Out-degree	Centralities				Centroid volume	#
				BC	#	Weighted SubG*	#		
E.IND	R DAU	10	5	0,0181	6	93,55	1	8	39
E.IND	L DAU	10	5	0,0181	6	92,90	2	8	39
AVIO	GTN #1	7	2	0,0032	23	77,00	3	3	70
AVIO	GTN #2	7	2	0,0038	20	76,90	4	3	70
AVIO	TRANS	1	3	0,0016	34	37,47	5	4	59
TRIM	TR REL	2	2	0,0105	14	32,74	6	7	43
AVIO	AUDIO #1	6	2	0,0046	19	31,84	7	1	77
ELCSYS	AVION LMB	1	7	0,0226	4	29,00	8	24	14
AVIO	EHSI #1	4	2	0,0022	27	26,05	9	4	59
AVIO	EHSI #2	4	2	0,0026	24	25,87	10	4	59

Weighted evaluation process results show that locally most important nodes are DAU. Its subgraph centrality is even after weighting process still dominant.

4.9.3 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 interconnection 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 model. 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).

In the set of parameters, not all elements of the set P_{ai} have the same relative importance in relation to the particular problem under consideration. This relative significance or importance is simply referred to as a weight parameter W_i . The analyst evaluates the it parameter with value b_i , if it lies in the scale, e.g., $b_i < 0, 100 >$. The more important the parameter is, the higher its score is. While the scoring method requires the user to provide quantitative evaluation of indicators, it also allows for a more differentiated expression of subjective preferences than in, e.g., the ranking method. [39]

$$W_i = \frac{b_i}{\sum_{P_{ai}} b_{Pa}}, i = 1, 2, \dots, n$$

Equation 10 [39]

Where W_i weight assigned to each parameter, b_i is the number of assigned points, n is the number of all considered parameters, b_{pa} parameter, i index of the parameter, b_{pa} —the total number of points assigned to all parameters. The resulted weights, determined from expert assessments. [39]

Node parameters- betweenness centrality, subgraph centrality and centroid volume processed using described Metfessel allocation. Resulting node topology parameter is computed by following equation.

$$NTP_i = p_{BC} \cdot BC_i + p_{SubG} \cdot SC_i + p_{CV} \cdot CV_i$$

Equation 11

Where, p_{BC} is between preference, BC_i node processed betweenness centrality, p_{SubG} processed subgraph centrality, SC_i node centrality, p_{CV} centroid volume preference and CV_i processed node centroid volume.

Table 14 Case study importance list based on NTP and weighted NTP

System	Node name	NTP	System	Node name	NTP Weighted
E.IND	R DAU	65,29	E.IND	R DAU	68,60
E.IND	L DAU	64,94	E.IND	L DAU	68,25
ELCSYS	L MAIN	62,15	ELCSYS	L MAIN	56,80
ELCSYS	R MAIN	56,93	ELCSYS	R MAIN	51,64
ELCSYS	AVION LMB	43,51	AVIO	GTN #2	46,71
ELCSYS	BUSTIE	40,81	AVIO	GTN #1	46,06
AVIO	GTN #2	36,14	TRIM	TR BUS	42,15
AVIO	GTN #1	35,74	TRIM	TR REL	40,90
ELCSYS	LLC	35,47	TRIM	FUSE A10	40,90
ELCSYS	RLC	35,44	ELCSYS	AVION LMB	38,41
Preferences: $p_{BC} = 0,3$ $p_{SubG} = 0,5$ $p_{CV} = 0,2$					

Final output from graph theory based model processing is NTP importance list. Table 14 show two types of importance list. Un-weighted topology parameter results show, that most important items a L DAU a R DAU units followed by various electrical buses, contactor and GTNs. Calculation configuration prefers local importance over the global. Calculation configuration is adjustable to particular application and analyst judgment. For case study evaluation weighted NTP is chosen (on the left side of previous figure. In this case GTNs are most important items. These results at best correspond with analyst judgment in this particular application.

As it was mentioned in previous sub-chapters many times NTP is used in following chapters as input contributing to the particular node criticality.

CHAPTER 5

EXTENDED CRITICALITY AND ROBUSTNESS

5.1 INTRODUCTION

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. [19]

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 [5], [6], [7], [8]) before by several researchers and development groups. However, doctoral thesis aims to extend this concept as integral peace of larger method and adjusted for airborne system safety and reliability assessment application.

This concept fits into presented integrated method, it uses system model in the form of graph and its outputs resulting from Graph theory application. Figure 46 illustrates combined influences on the item/ sub-system criticality.

5.2 EXTENDED CRITICALITY EVALUATION

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 [3] definition severity and probability of occurrence).

Extended criticality level (and number) is generally descriptive attribute of item (sub-system) contribution to system (airplane, 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.

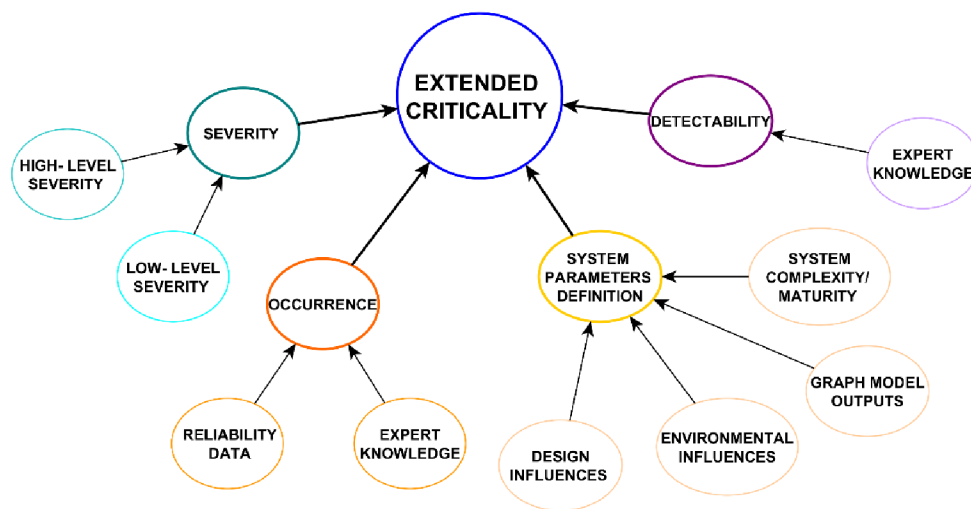


Figure 46 Combined influences on the extended criticality

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.

5.2.1 Severity definition

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 aircraft function high and low critical functions (**MF, SF, AF**). Severity distribution to the separated levels allows precisely describe failure mode consequences for separated system and airplane itself.

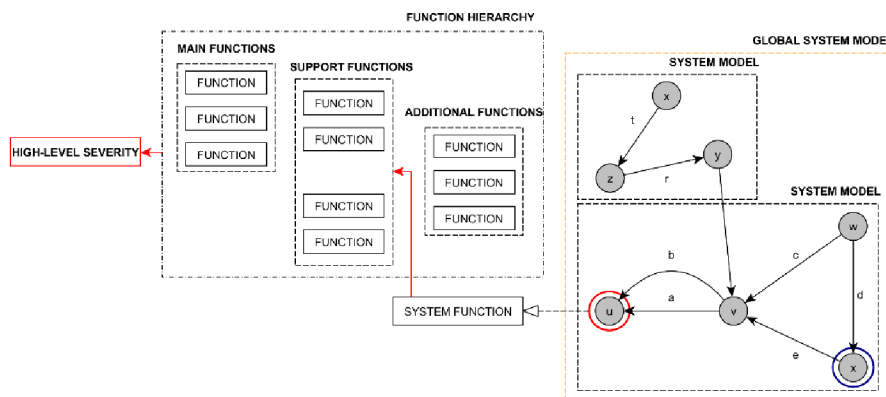


Figure 47 High-level severity evaluation process

Function severity is based on evaluation of failure effect on three main aspects- Airplane (functional capabilities), flight crew (ability to operate airplane) and passengers (comfort, physical distress and injuries). This evaluation is derived from FAA AC23.1309-14 advisory circular [1].

Table 15 Function severity

FUNCTION SEVERITY EVALUATION			Related classification
Effect level	Base membership volume	Description	
NO EFFECTS (N/E)	0	There is no significant effect any of all three aspects.	NO SAFETY EFFECT
SLIGHT EFFECTS (SLIGHT)	1	Only a slight effect on all three aspects.	MINOR
SIGNIFICANT EFFECTS (SIGN)	4	There is a significant effect on all three aspects.	MAJOR
LARGE EFFECTS (LARGE)	7	There is a large effect on all three aspects.	HAZARDOUS
CATASTROPHIC (CAT)	10	There is a catastrophic effect on all three aspects.	CATASTROPHIC

All main aspect of failure (airplane, crew, passengers) direct effects have to be evaluated and classified separately. These classifications are then aggregated in order to obtain resulting Function severity. Highest level of effect classification (N/E, SLIGHT, SIGN, LARG, CAT) sets base membership volume. Each aspect classification in the same level adds 1 point. Each aspect level classification in the closest lower level adds 0,5 point. Lowest aspect classification adds 0,25.

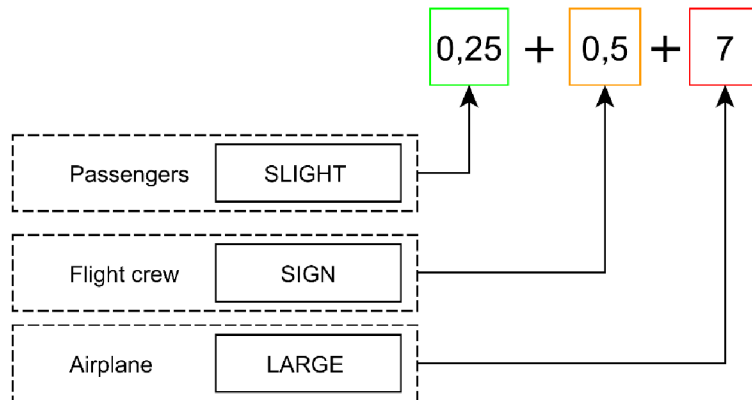


Figure 48 Function severity failure effects aggregation example

Figure 48 shows example of system failure effect aggregation. Highest aspect of failure consequences is on airplane (LARGE), function severity membership base then equals to **FS=7**. Closest lower consequences aspect classification is on flight crew (SIGN), **FS=7,5**. The lowest aspect classification is on passengers (SLIGHT), therefore **FS=7,75**.

Integrated method provides functions preliminary classification and membership volume of airborne systems failures in **Appendix A**. Systems are coded according to the ATA 100 numbering system which is a common referencing standard for commercial aircraft documentation.

Item High-level severity

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.

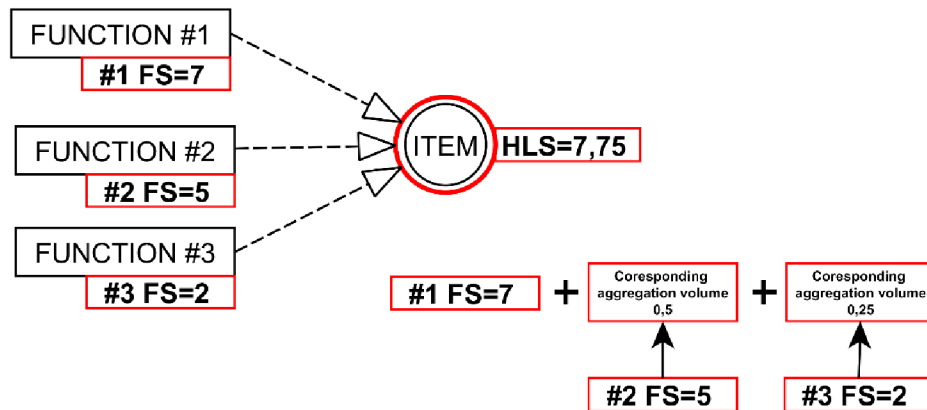


Figure 49 Item HLS and FS

Severity aggregation process starts with function with highest severity allocated to the item. To this severity is added aggregation volume of other function. Appropriate aggregation volume is taken from Table 16.

Table 16 HLS aggregation volumes

Severity level	Function severity	Aggregation volume
NEGLIGIBLE	0	0
LOW	1-3	0,25
MEDIUM	3-6	0,5
HIGH	6-8	0,75
VERY HIGH	9-10	1

High level severity is classified as NEGLIGIBLE, LOW, MEDIUM, HIGH and VERY HIGHT. These classifications are related to the formal classification MINOR, MAJOR, HAZARDOUS and CATASTROPHIC required by authority (see 2.3.2 Certification bases). For each item, it is derived from is allocated functions and their severity.

These classifications are not linearly distributed. There is essential difference between MAJOR and HAZARDOUS and especially between HAZARDOUS and CATASTRPOPHIC. Aggregation process is a measure how to ensure distinction between these classifications.

In the Figure 50, adjusted system example present distinction between is HLS and FS. Nodes w and x are associated with FUNCTION #1. This function has FS=5. However, HLS for both items equals to 5. These nodes have redundant function.

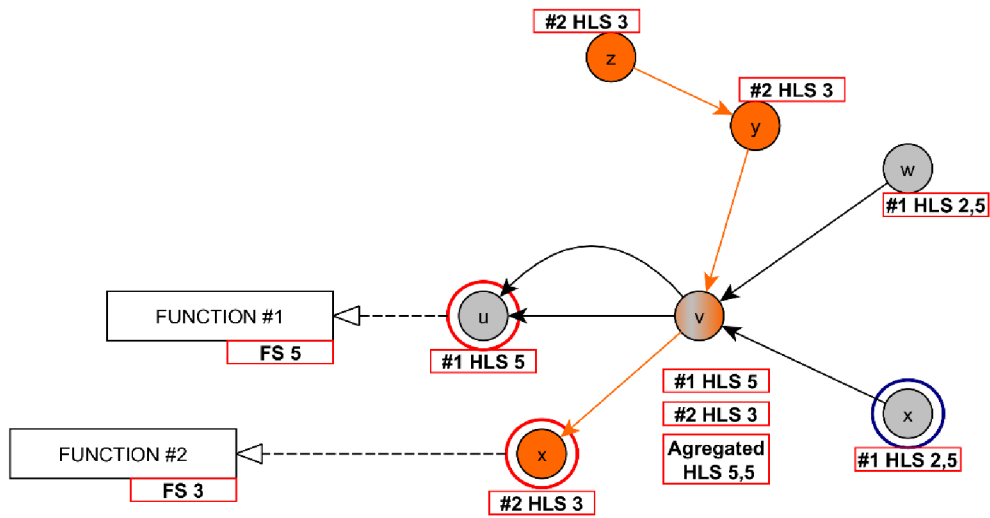


Figure 50 Item High-level severity aggregation

Node v is associated with functions #1, #2. Its HLS=5,5 according to the aggregation processed described above.

Corrective measures

A few corrective measures are applied on the process of HLS aggregation in order to achieve higher level of correlation with reality.

Table 17 Cumulated severity corrective measures

ID	Definition	Example
1	If the function of a given item is redundant to another item or items. HLS is for all of them divided by the amount of redundant items.	Case study elevator trim could be controlled by two separated items- PT TR PI a PT TR COPI.
2	Cumulated severity could not be higher than classification of allocated highest function.	Case study DAU units have seven MINOR allocated function. Classification of one engine failure is MAJOR. Resulting cumulated severity is $HLS_{DAU} = 5$
3	Item function serves as auxiliary measure in the case of previous common failure or failures. It is designed as	Case study CROSS STAT/ DYN valves are designed to interconnect both channels of static pressure air/ dynamic pressure. Adjusted HLS is applied (HLS/2)

5.2.2 Occurrence definition

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. [13]

As stated earlier, in the field of doctoral thesis interest (mainly UAVs and light weight aircrafts) it is not possible to 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.

Probability of occurrence

Probability of failure mode occurrence is most essential complementary measure to quantify system reliability- ability to perform its function. Presented integrated method uses two ways how to express probability of occurrence- **quantitative** (relevant reliability data are available) and **qualitative** using the linguistic term to established occurrence level.

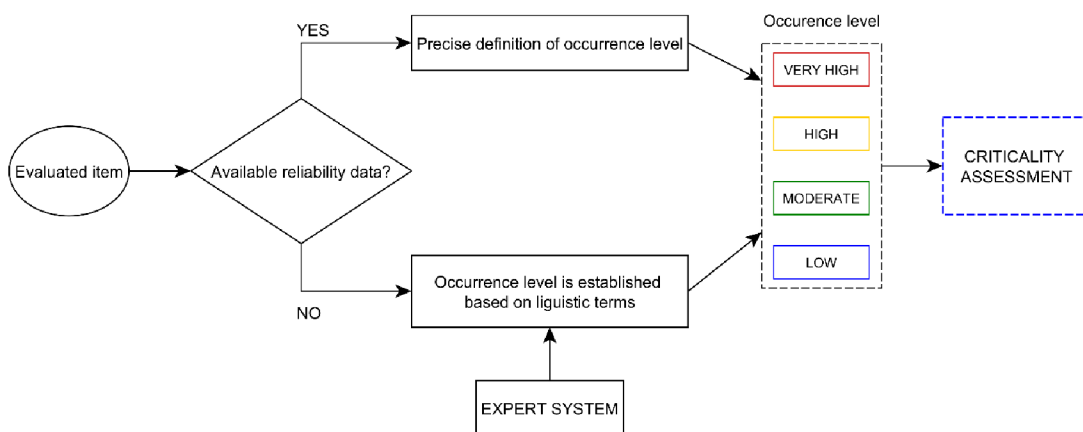


Figure 51 Occurrence levels

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. Input parameter handling is described in chapter 5.2.2 Occurrence.

Critical review summarizing basic items for specific type of system is attached as **Appendix C**. It is sort of guide for occurrence score definition. These reliability data are taken from various commercial reliability databases, representing typical items of particular system.

5.2.3 Detectability definition

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.

Table 18 Detectability criteria definition

Direct detectability <i>(indication)</i>	Failure of evaluated system is indicated to the crew. Flight crew is able to respond to the failure effects and proceed according to the flight manual.
YES <i>(Multiple levels)</i>	Multilevel crew alerting system- alert, caution, warning.
YES <i>(Single level)</i>	Loss of function indication.
NO	There is no direct indication to the crew.
Indirect detectability <i>(results of non-function)</i>	Failure is indirectly indicated to the crew by its collateral effects. Flight crew is able to derive occurring failure without significant workload.
YES	Fulfill indirect detectability definition.
Partially	It is possible to reasonably assume that there is at least partial indirect detectability of occurring failure.
NO	Does not fulfil detectability definition.
External pre-flight test	Item malfunction is possible to detect during standard external pre- flight test. Flight crew execute pre- flight maintenance outside the aircraft according to the flight manual.
YES	Fulfill indirect detectability definition.
NO	Does not fulfil detectability definition.
Internal pre-flight test	Item malfunction is possible to detect during standard external pre- flight test. Flight crew execute pre- flight procedures inside the aircraft according to the flight manual.
YES	Fulfill indirect detectability definition.
NO	Does not fulfil detectability definition.

Detectability levels are defined as score intervals. Resulting detectability level is part of integrated method outputs.

5.2.4 Topology parameter definition

It was described in previous chapter (see 4.9.3 Node topology parameter). Node topology parameter express node interconnection 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.

5.3 ROBUSTNESS AND SYSTEM PARAMETERS

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.

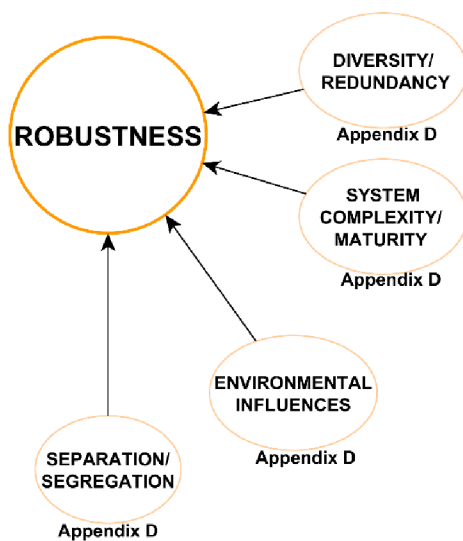


Figure 52 Combined influences on the robustness number

In the case of “lower” airplane classes like it could be necessary to take all these influences as well. 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 [50]). 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.

Questionnaire itself and detailed guidelines is attached as **Appendix D**. Analyst is should be able to use express system parameters and evaluate level of system robustness.

Following tables give an example of used questions. In each column is stated question **relevance (R)**, **partial relevance (P/R)**, **non- relevant (N/R)** for specific type of system. However, question relevance is not mandatory. Its application is up to system expert and analyst.

Separation/ segregation

Table 19 Questionnaire review - separation/ segregation class

QUESTIONS					
Relevance	Electrical	Electronics	Mechanical	Pneumatic	Hydraulic
Separation/ segregation					
Q1: Are all connection (cables, wires, pipes) for the channels routed separately at all positions?	R	R	R	R	R
Q2: Are the logic sub-system channels on separate printed-circuits boards?	R	R	N/R	N/R	N/R

Table 20 Questionnaire review - diversity/ redundancy class

QUESTIONS					
Relevance	Electrical	Electronics	Mechanical	Pneumatic	Hydraulic
Diversity					
Q1: Do the channels employ different technologies (for example, one electronic or programmable electronic and the other relay)?	R	R	N/R	N/R	N/R
Q2: Do the channels employ different electronic technologies (for example, one electronic, the other programmable electronic)?	R	R	N/R	N/R	N/R

Table 21 Questionnaire review example- Environmental class

QUESTIONS					
Relevance	Electrical	Electronics	Mechanical	Pneumatic	Hydraulic
Environmental control					
Q6: Are all signal and power cables separate at all positions?	R	R	R	R	R
Environmental testing					
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	R	R	R	R	R

Resulting answers are weighted and serve as inputs to the fuzzification process. This process is explained in detail in following chapters. Means of questionnaire answers fuzzy evaluation is also explaining in these chapters.

5.4 INTEGRATED METHOD KNOWLEDGEBASE

The knowledge bases are intended to be a source of expert knowledge. It is based on experiences and procedures used on the BUT Institute of Aerospace Engineering gain during participation in several Czech and international projects focused on safety and reliability assessment of airborne systems.

Knowledge bases are mainly useful for General Aviation purposes EASA CS-23 application, nevertheless these data could be used in unnamed aerial system application or light aircraft application. Bases are designed to guidelines for integrated method application (fuzzy criticality evaluation) or standard safety and reliability assessments. Provided information are designed for twin and single engine aircrafts (notified in **Appendix A**).



Figure 53 PA-31-350 Chieftain (left)[46], VUT 100 (right) [45]

5.4.1 Classification Knowledge Base

The airborne systems classification knowledge database is attached as **Appendix A**. It is a structured analysis developed especially for proposed integrated method. Airborne systems are divided into several chapters and sub-chapters according to the ATA 100 (ATA DEFINITIONS OF AIRCRAFT GROUPS, SYSTEMS AND SUB-SYSTEMS). Each failure mode of system is evaluated separately. Assumed effect on three main safety aspects airplane, crew and passengers are classified (based on FAA AC23. 1309-1E), commented and fuzzy membership volume is established. The membership volume of **function severity** (see 5.2.1 Severity) serves as input for definition of system criticality.

Table 22 Classification database structure

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/Function severity	Note
					Airplane	Crew	Passengers		

Chapter selection is based on previous experience with safety and reliability assessment of typical airborne systems. For instance, power-plant is development and certified separately to the aircraft development. Therefore, engine chapters (72) are not included in knowledge database. Otherwise, engine unit integration is essential part of safety and reliability assessment. Engine controls, ignition

chapters (73, 76) are included in the database. Various chapters are intentionally left out, because these types of systems are not usually applied in the field of interest (see Table 23).

Table 23 Classification knowledge database content

CONTENT OF KNOWLEDGE DATABASE A			
22	AUTO FLIGHT	31	INDICATING/ RECORDING SYSTEMS
23	COMMUNICATION	32	LANDING GEAR
24	ELECTRICAL POWER	33	LIGHTS
26	FIRE PROTECTION	34	NAVIGATION
27	FLIGHT CONTROL	46	INFORMATION SYSTEMS
28	FUEL	76	ENGINE CONTROLS
29	HYRAULIC POWER	77	ENGINE INDICATING
30	ICE AND RAIN PROTECTION	80	STARTING

5.4.2 Basic Items Reliability Data Overview

The basic items reliability data overview is attached as **Appendix B**. Selected reliability data are taken from several commercial reliability databases:

- (1) MIL-HDBK-217F NOTICE 2 *Reliability Prediction of Electronic Equipment* [27]
- (2) MIL-HDBK-338B *Electronic Reliability Design Handbook* [28]
- (3) SRC SPIDR *System and Part Integrated Data Resource v.1.0* [29]
- (4) RIAC Databook 3.0.1 *NPRD-2011 C, FMD-97CD, EPRD97-CD, VZAP-95 C* [30]

Database provides **occurrence** membership volume of item for fuzzy criticality assessment.

Table 24 Structure of basic parts reliability database

BASIC PARTS					
<i>Item</i>	<i>Failure mode</i>	<i>Failure rate</i> <i>[hr⁻¹]</i>	<i>Occurrence level</i>	<i>Information source</i>	<i>Note</i>

5.4.3 Robustness parameters questionnaire

As it was mentioned above system parameters definition questionnaire is attached as **Appendix D** to this document. It serves as a mean how to process expert knowledge, allocated functions and relations to the other system. Using this questionnaire, it is possible to evaluate level of system separation/ segregation, diversity/ redundancy and environmental control/ testing.

5.5 FUZZY EXTENDED CRITICALITY INPUTS

5.5.1 Detectability input

Integrated method provides scoring table to evaluate a given item detectability (Table 25). Detectability is described in the chapter 5.2.3 Detectability. Scoring table is based on previous experiences with modern maintenance planning and evaluation MSG-3 and safety and reliability evaluation. Detectability scoring interval is $< 0,10 >$. Lower score corresponds with higher probability of failure detection. High score corresponds with lower probability of failure detection resulting in latent failure.

Table 25 Detectability scoring table

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

Scoring table provides advisory mean how to express detectability. Detectability significantly depends on expert judgment. Scoring table application is not mandatory. It could be adjusted for particular application.

However, detectability is strongly bounded with failure occurrence. This relation is established in fuzzy inference rules. High attention with detectability is advised. Next table provides short example of items and their detectability. Scoring tables are applied in the case study evaluation (Chapter 7).

Table 26 Detectability examples

DETECABILITY LIST OF EXAMPLES	
INTEGRATED AVIONICS SYSTEM, AUTOPILOT	1
DATA ACQUISITION UNIT, ELECTRIC GENERATORS	2
PRESSURE AIR VALVES	6
PRESSURE, TEMPERATURE OR PRESSURE SENSORS	8
STATIC PRESSURE INPUTS	9
RELAY, AIR INLET	10

For the purposes of fuzzy inference process detectability levels are established. Through these levels fuzzy inference rules are expressed. Particular levels are distinguished by their score intervals (see Table 27). Levels are also useful in the process of system evaluation.

Table 27 Detectability levels definition

<i>Detectability level</i>	<i>Description</i>	<i>Score interval</i>
LATENT	It is almost impossible to detected failure except limited collateral effects.	9-10
LOW DETECTABILITY	It is not likely to detect failure.	6-9
MODERATE DETECTABILITY	There is a possibility to detect failure.	3-5
VERY HIGH DETECTABILITY	There is very high probability of failure detection	0-2

Detectability fuzzy membership is established in Figure 54. The trapezoidal membership function is used.

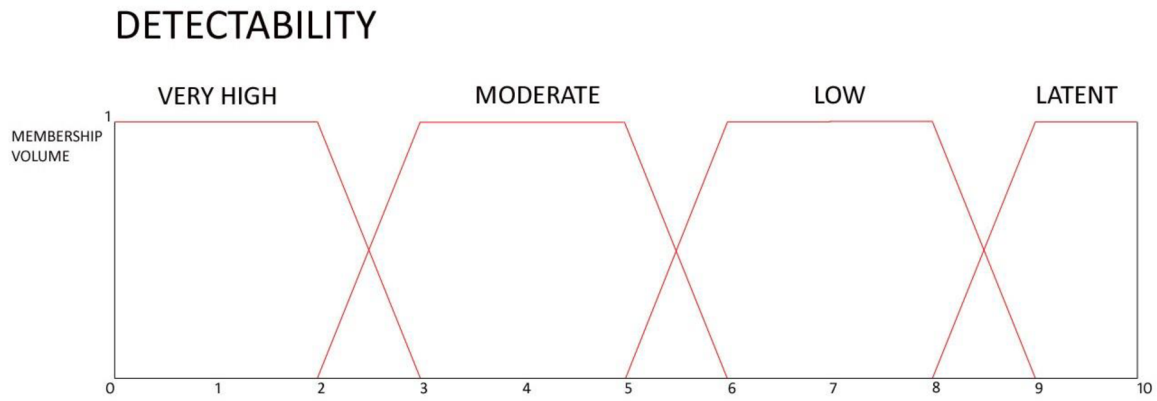


Figure 54 Fuzzy membership function for linguistic variable- detectability

5.5.2 Node topology

Node topology parameter has scoring interval $\langle 0,100 \rangle$. It is based on graph model evaluation. Lower score correspond with item low influence on the system. NTP fuzzy membership is established in the Figure 55. The trapezoidal membership function is used.

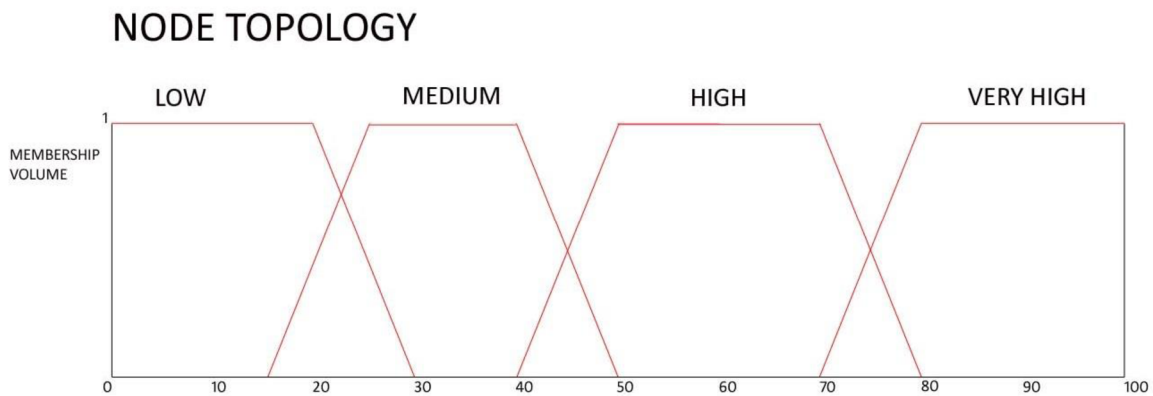


Figure 55 Fuzzy membership function for linguistic variable- node topology

For the purposes of fuzzy inference process node topology parameter levels are established. Through these levels fuzzy inference rules are expressed. Particular levels are distinguished by their score intervals (see Table 28).

Table 28 NTP levels

<i>Topology parameter level</i>	<i>Description</i>	<i>Score interval</i>
VERY HIGH	High level of node interconnection and impact to the system. Item has an exceptionally global function.	80-100
HIGH	High level of node interconnection and impact to the; system. Item has a global function.	50-70
MEDIUM	Medium level of node interconnection and impact to the system. Item has a local function.	25-40
LOW	Low level of node interconnection and impact to the system. Item has a local function.	0-15

5.5.3 High-level severity input

High-level severity is key input of item extended criticality evaluation. HLS could be obtained by two ways. Main way is knowledge base application (**Appendix A**). Knowledge base provides preliminary classification of most important system failures (important at the field of interest). These classifications are based on experience in the field safety and reliability assessment, modern maintenance and pilot experience in BUT Institute of Aerospace Engineering. It could be adjusted for particular application. Secondary way is expert knowledge of analyst and usage of high severity levels and ranks. High level severity levels are derived from EASA CS-23 and FAA AC 23.1309-1E.

Table 29 High- level severity levels

<i>High- level severity</i>	<i>Description</i>	<i>Rank</i>
VERY HIGH	Very high level of severity of failure consequences. It could potentially leads to the fatal injuries of fatalities	9-10
HIGH	Large reduction in functional capabilities or safety margins. Potentially serious or fatal injury. Excessive flight crew workload.	6-8
MEDIUM	Significant reduction in functional capabilities or safety margins. Physical distress. Significant flight crew workload.	3-5
LOW	Slight reduction in functional capabilities or safety margins. Physical discomfort. Slight increase of flight crew workload.	0-2
NEGLIGIBLE	No effect on operational capabilities or safety.	-

High level severity fuzzy membership is established in Figure 56. The trapezoidal membership function is used.

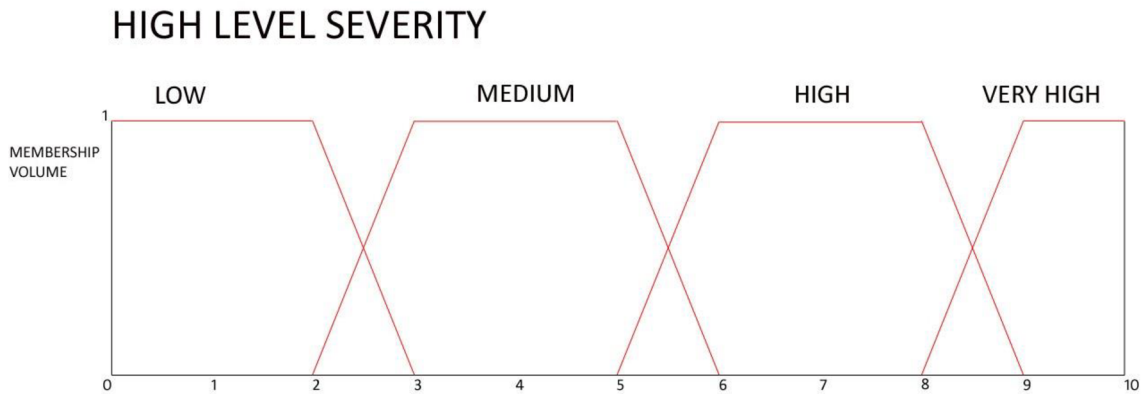


Figure 56 Fuzzy membership function for linguistic variable- high level severity

5.5.4 Occurrence input

Occurrence fuzzy input definition is partially based on allowable probability of failure condition established by **FAA A23.1309-1E** [1] Class IV. It could be possibly adjusted for different class or category.

Failure rate value λ will be used for substitution of failure probability. According to the assumption that average flight time of the airplane is 1 hour, there is no need to multiply value λ by value representing flight time. Therefore, it is possible to use simplified formula:

$$Q = \lambda \cdot \Delta t = \lambda \cdot 1 = \lambda$$

Equation 12

This formula is commonly used simplification. The simplification applies to components with high-level of inherent reliability ($\lambda < 1 \cdot 10^{-3}$). This requirement is fulfilled with the used components.

Probability intervals could be adjusted for different class even for different certification base. It is up to analyst to set up occurrence base.

Table 30 Occurrence definition

OCCURRENCE LEVELS for EASA CS-23 Class IV				
Occurrence level	Description	Probability interval [hr ⁻¹]		Corresponding MTBF
FREQUENT	Failure probability is extremely high (item repeat failures).	1.10⁻⁴	1	> 1 000 hours
REASONABLE PROBABLE	Failure probability is high (item repeat failures).	1.10⁻⁶	1.10⁻²	1 000 - 100 000 hours
OCCASIONAL	Failure is occasional.	1.10⁻⁵	1.10⁻⁶	-
REMOTE	Failure probability is low.	1.10⁻⁷	1.10⁻⁸	-
EXTREMELY UNLIKELY	Failure is almost unlikely.	1.10⁻⁹	0	-

In the case of absence of relevant reliability input data, analyst is able to use Table 30. It describes particular occurrence level and gives a description allowing analyst to established occurrence level. These inputs are not totally precise, however in combination with other fuzzy extended criticality inputs help to establish mean of item evaluation.

Occurrence fuzzy membership is established in Figure 57. The trapezoidal membership function is used.

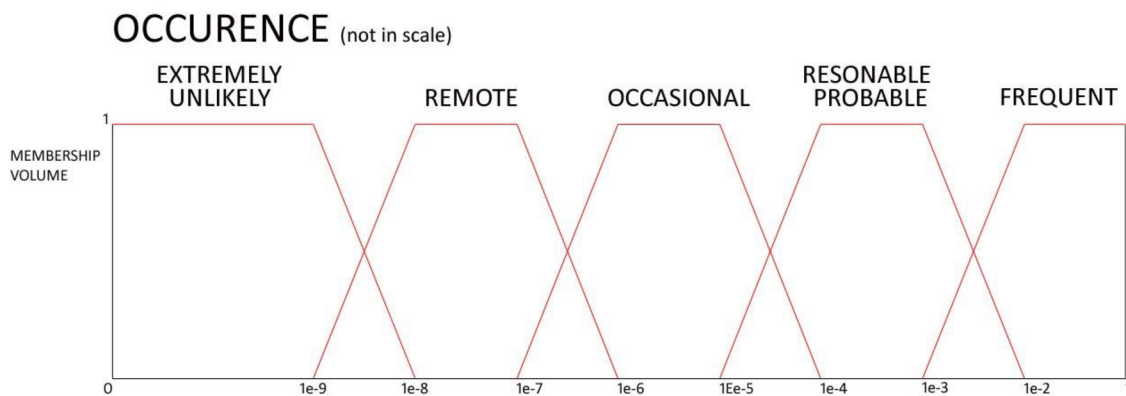


Figure 57 Fuzzy membership function for linguistic variable- occurrence

5.6 ROBUSTNESS AND PARAMETERS INPUTS

System robustness is evaluated from several points of views (see 5.3 Robustness and System parameters). Each of them express different attributes. Evaluation is processed through questionnaire. Fuzzy robustness process is a way how to express expert knowledge. Questionnaire answers serve as inputs to the fuzzy inference process Robustness inputs fuzzy membership are established in Figure 58. The triangular membership function is used.

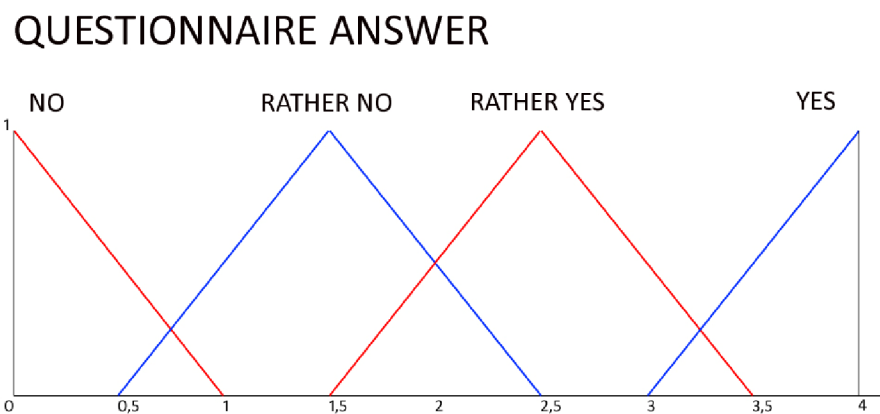


Figure 58 System parameters answer membership function

Expert knowledge could be expressed as linguistic answers (Table 31) or as a crisp number from interval $\langle 0,4 \rangle$.

YES	It does fulfil definition.
R/YES	Rather fulfils definition.
R/NO	Rather not fulfils definition.
NO	It does fulfil definition.

Table 31 Questionnaire answers definition

5.7 FUZZY EXTENDED CRITICALITY OUTPUTS

5.7.1 Extended criticality output

Number resulting from antecedent part of fuzzy rule is then applied on rule consequent. Number resulting from particular fuzzy rule is then aggregated in order to obtain resulting fuzzy criticality number. For consequent of fuzzy criticality is used trapezoidal membership function (see Figure 59).

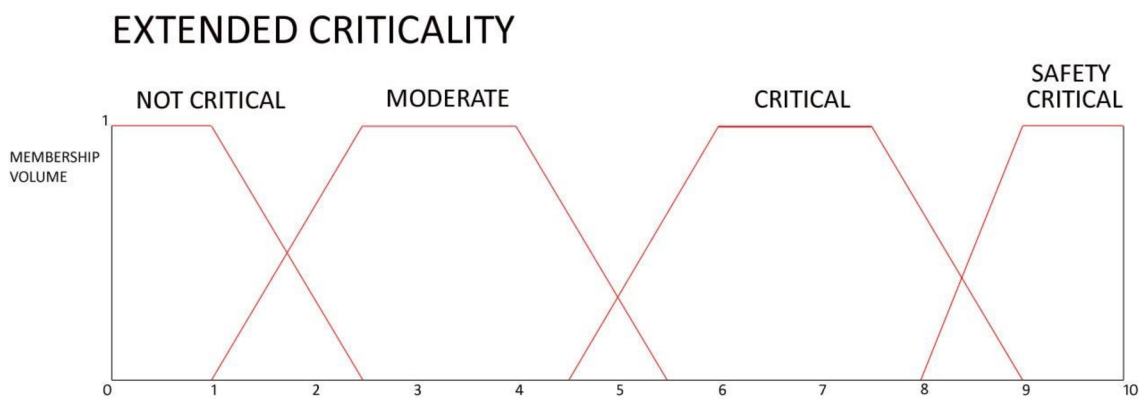


Figure 59 Extended criticality output membership function

Fuzzy criticality evaluation process results in extended criticality number. It gives a relative information about item importance. This information is based on several attributes. Extended criticality number corresponds with particular level (see Table 32).

Table 32 Extended criticality level definition

<i>Extended criticality level</i>	<i>Fuzzy ranking interval</i>	<i>Description</i>
SAFETY- CRITICAL	8,5-10	An item/ subsystem is directly influence MF implementation and threaten MSO execution. It is indispensable to continue control safe flight and landing.
CRITICAL	5,5-7,5	An item/ subsystem influence MF implementation. However, it is not directly critical to the MSO . Low level of occurrence level, high failure detectability reduces extended criticality number.
MODERATE	2,5-4	An item/ subsystem does not influence MF implementation nor MSO execution. It partially influences AF implementation.
NOT CRITICAL	0-1,5	An item/ subsystem does not influence AF , MF implementation nor MSO execution.

5.7.2 Robustness number output

Number resulting from antecedent part of fuzzy rule is then applied on rule consequent. Number resulting from particular fuzzy rule is then aggregated in order to obtain resulting fuzzy robustness number. For consequent of fuzzy criticality is used triangular membership function (see Figure 60).

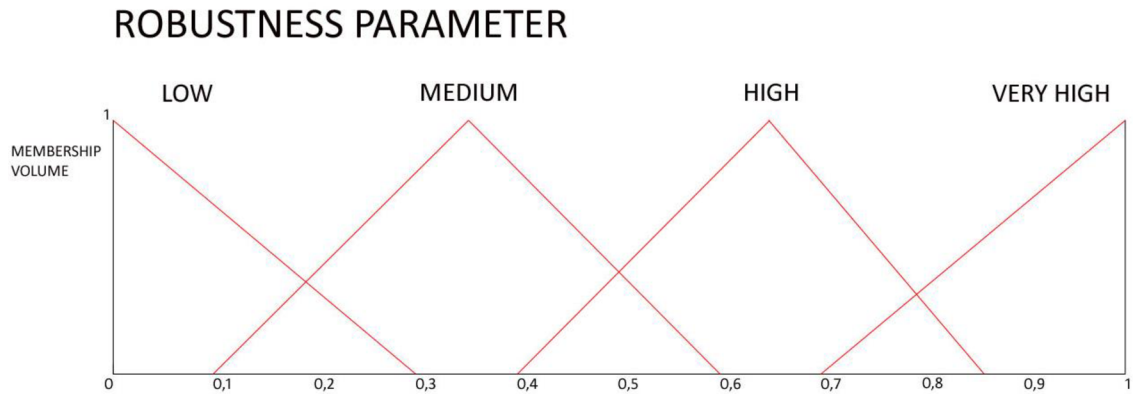


Figure 60 Robustness parameter output membership function

Fuzzy robustness evaluation results in out several robustness number based on evaluated category (for instance Diversity/ Redundancy). It provides additional information about system design. Each category reflects different system attribute. Resulting number corresponds with a particular robustness parameter level (see Table 33).

Table 33 Robustness level definition

<i>Parameter Level</i>	<i>Fuzzy ranking interval</i>	<i>Description</i>
VERTY HIGH	0,7-1	A given parameter of particular system is very high. Except complexity/ design and maturity it corresponds with very high level of system protection. Complexity/ design and maturity: it correlates with very high complex system with low maturity of its items.
HIGH	0,4-0,65-0,85	A given parameter of particular system is high. Except complexity/ design and maturity it corresponds with high level of system protection. Complexity/ design and maturity: it correlates with high complex system with relatively low maturity of its items.
MEDIUM	0,1-0,35-0,6	A given parameter of particular system is medium. Except complexity/ design and maturity it corresponds with medium level of system protection. Complexity/ design and maturity: it correlates with medium complex system with relatively high maturity of its items.
LOW	0-0,3	A given parameter of particular system is low. Except complexity/ design and maturity it corresponds with low level of system protection. Complexity/ design and maturity: it correlates with low complex system or with very high maturity of its items.

5.8 FUZZY INFERENCE

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 [31]

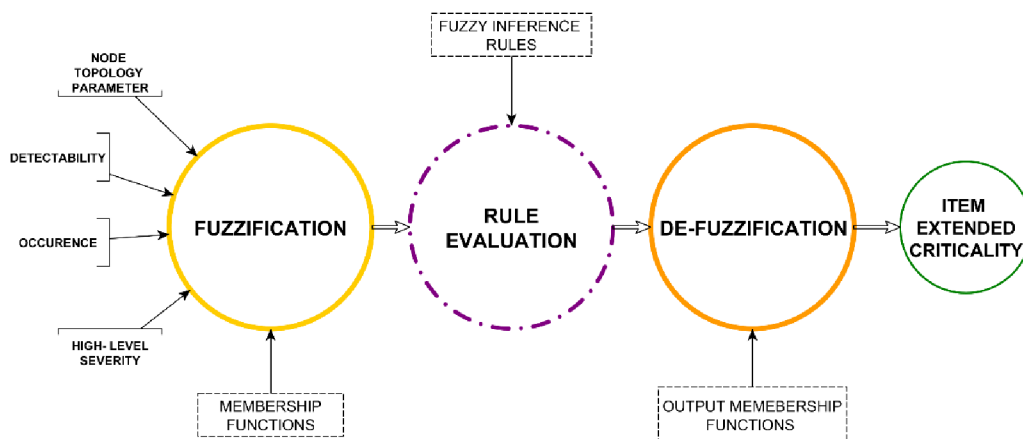


Figure 61 Fuzzy inference process

5.8.1 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. [12]

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 transforms crisps into a membership degree. It should express how inputs belong into linguistic terms used in the rules.

Table 34 Extended criticality inputs fuzzification

EXTENDED CRITICALITY INPUTS	
<p>NODE TOPOLOGY PARAMETER</p>	<p>Node topology express level of item interconnection on the global level.</p> <p>Range of discourse: 0-100</p> <p>Example input</p> <p>Crisp number: 78</p> <p>$\mu_{(x=HIGH)} = 0,25$ $\mu_{(x=VERY HIGH)} = 0,78$</p>
<p>HIGH LEVEL SEVERITY</p>	<p>High-level severity express item severity based on its allocated functions. Analyst assess item's failure (or incorrect function) severity in relation to the MSO (ability to sustain safe flight and landing). Range of discourse: 0-10</p> <p>Example input</p> <p>Crisp number: 5,2</p> <p>$\mu_{(x=MAJOR)} = 0,72$ $\mu_{(x=HAZARDOUS)} = 0,27$</p>
<p>OCCURRENCE</p> <p><i>Note. Figure is not in scale</i></p>	<p>Occurrence express probability of item failure. Precise volume could be substituted by occurrence level based on expert knowledge.</p> <p>Range of discourse: 0-1</p> <p>Example input</p> <p>Crisp number: $\mu = 9.10^{-4}$</p> <p>$\mu_{(x=OCCASIONAL)} = 0,26$ $\mu_{(x=REASONABLE PROBABLE)} = 0,78$</p>
<p>DETECTABILITY</p>	<p>Detectability express likelihood of item failure detection.</p> <p>Range of discourse: 0-10</p> <p>Example input</p> <p>Crisp number: 1,8</p> <p>$\mu_{(x=VERY HIGH)} = 1$</p>

5.7.2 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 modeling, 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. [11]

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 modeled by fuzzy sets and relations. Restriction statements are connected by linguistic connectives such as "and, or, or else." [11] Extended criticality fuzzy rule base rules respect relationship between classes, probabilities, severity of failure established in FAA AC23.1309-1E [1]

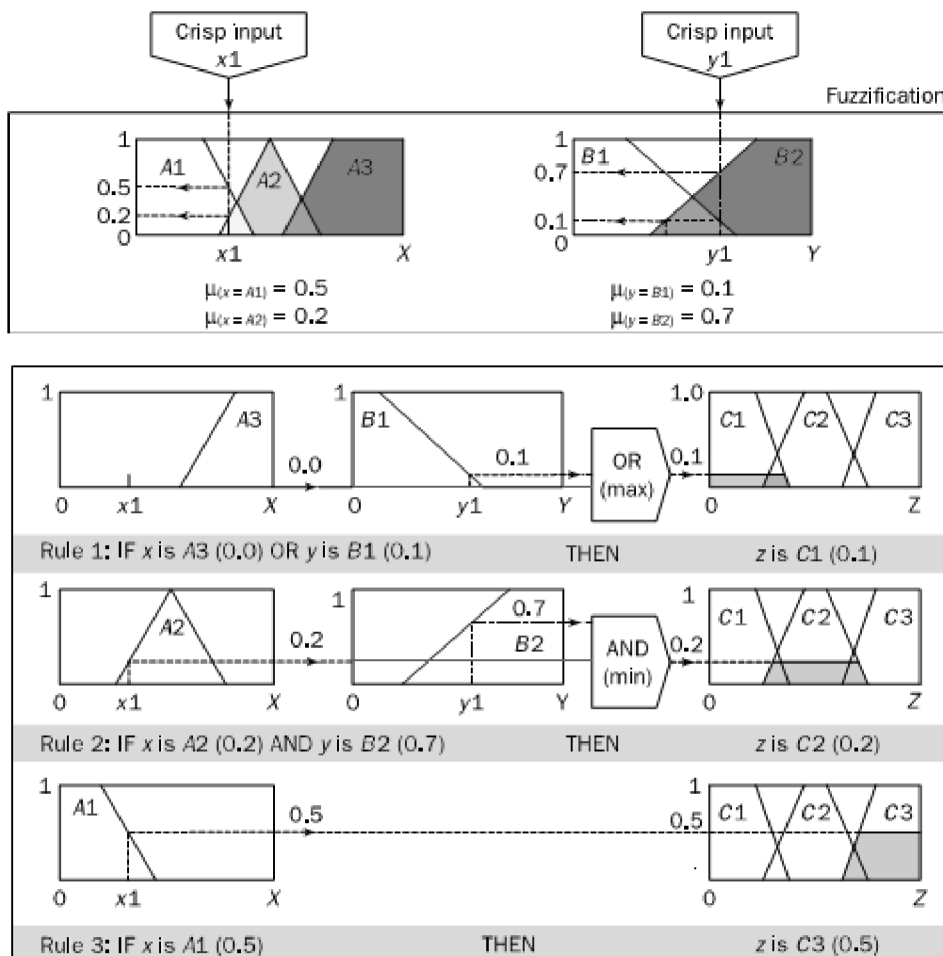


Figure 62 Fuzzy logic rule application [31]

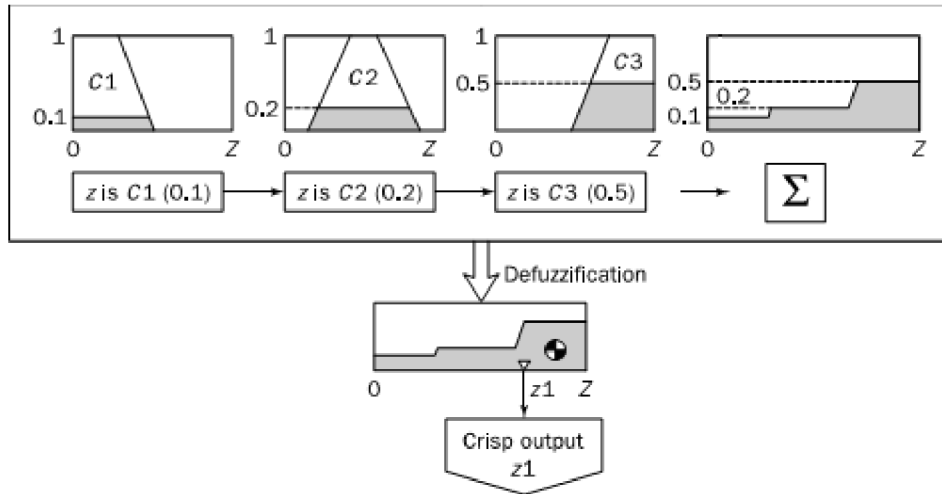


Figure 63 Fuzzy logic rules aggregation and de-fuzzification [31]

First set of fuzzy inference tables is designed for system robustness evaluation- Separation/ segregation, diversity/ redundancy, Complexity/ Design/ Maturity/ Experience, Environmental control. Process of robustness evaluation is described in deep in **Appendix D**.

Table 35 Robustness Inference rule base – separation/ segregation

ROBUSTNESS FUZZY INFERENCE RULES - Separation/ segregation						
Setting		Antecedent				Consequent
#	Operator	Q1	Q2	Q3	Q4	LEVEL OF SEPARATION
1	AND	YES	YES	YES	YES	VERY HIGH
2	OR	YES	-	-	YES	VERY HIGH
3	AND	R/YES	YES	YES	R/YES	VERY HIGH
4	AND	YES	NO	NO	YES	HIGH
5	AND	R/YES	R/NO	R/NO	YES	HIGH
6	AND	R/NO	R/YES	R/YES	R/NO	MEDIUM
7	AND	NO	NO	NO	YES	MEDIUM
8	AND	R/NO	R/NO	R/NO	R/NO	LOW
9	AND	NO	NO	NO	NO	LOW

Table 36 Robustness inference rule base- diversity/ redundancy

ROBUSTNESS FUZZY INFERENCE RULES- Diversity/ Redundancy						
<i>Setting</i>		<i>Antecedent</i>				<i>Consequent</i>
#	<i>Operator</i>	<i>Q1</i>	<i>Q2</i>	<i>Q3</i>	<i>Q4</i>	LEVEL OF REDUNDANCY/ DEVERSITY
1	AND	YES	YES	YES	YES	VERY HIGH
2	AND	YES	YES	-	-	VERY HIGH
3	AND	YES	-	YES	-	VERY HIGH
4	AND	YES	R/YES	R/YES	-	HIGH
5	AND	R/YES	R/NO	YES	YES	HIGH
6	AND	R/YES	R/NO	R/YES	YES	HIGH
7	AND	R/YES	R/NO	R/NO	NO	MEDIUM
8	AND	YES	NO	NO	YES	MEDIUM
9	AND	R/NO	-	YES	N/NO	MEDIUM
10	AND	YES	NO	NO	NO	MEDIUM
11	AND	R/NO	R/NO	R/NO	R/NO	LOW
12	AND	R/NO	NO	NO	NO	LOW
13	AND	R/YES	NO	NO	NO	LOW
14	AND	NO	-	-	-	LOW
15	AND	NO	NO	NO	NO	LOW

Table 37 Robustness inference rule base- Complexity/ Design/ Maturity

ROBUSTNESS FUZZY INFERENCE RULES- Diversity/ Redundancy						
<i>Setting</i>		<i>Antecedent</i>				<i>Consequent</i>
#	<i>Operator</i>	<i>Q1</i>	<i>Q2</i>	<i>Q3</i>	<i>Q4</i>	LEVEL OF COMPLEXITY/ MATURITY/ DESIGN
1	AND	NO	YES	YES	YES	LOW
2	AND	R/NO	YES	YES	R/YES	LOW
3	AND	YES	YES	YES	YES	MEDIUM
4	AND	NO	YES	YES	R/NO	MEDIUM
5	AND	R/NO	YES	R/NO	YES	MEDIUM
6	AND	YES	YES	R/NO	YES	HIGH
7	AND	YES	R/NO	R/NO	YES	HIGH
8	AND	YES	R/NO	R/NO	YES	VERY HIGH
9	AND	YES	NO	NO	NO	VERY HIGH
10	OR	YES	-	-	NO	VERY HIGH

Table 38 Robustness inference rules- Environmental

ROBUSTNESS FUZZY INFERENCE RULES- Environmental								
Setting		Antecedent						Consequent
#	Operator	Q1	Q2	Q3	Q4	Q5	Q6	LEVEL OF ENVIRONMENTAL PROTECTION
1	OR	-	-	-	-	YES	YES	VERY HIGH
2	AND	YES	YES	YES	YES	-	-	VERY HIGH
3	AND	R/YES	YES	YES	YES	-	-	VERY HIGH
4	AND	R/YES	R/YES	R/YES	R/YES	R/YES	R/YES	HIGH
5	AND	YES	YES	YES	YES	R/NO	R/NO	HIGH
6	AND	-	YES	YES	YES	NO	NO	MEDIUM
7	AND	NO	R/YES	R/YES	R/YES	R/YES	NO	MEDIUM
8	AND	NO	R/NO	R/NO	R/YES	YES	NO	MEDIUM
9	AND	R/NO	R/NO	R/NO	R/NO	R/NO	R/NO	LOW
10	AND	-	-	-	-	NO	NO	LOW
11	AND	NO	NO	NO	NO	NO	NO	LOW

Following table presents fuzzy inference rules for item extended criticality evaluation. It handles linguistic variables inputs to the extended criticality evaluation. These inputs (NTP, Occurrence, Detectability, Severity) were defined. Fuzzy rules are applied on doctoral thesis case study (see **Appendix C**).

Table 39 Extended criticality inference rule base

EXTENDED CRITICALITY FUZZY INFERENCE RULES						
Setting		Antecedent				Consequent
#	Operator	Node topology parameter	High- level severity	Occurrence	Detectability	Criticality
Severity base						
1	-	-	V/HIGH	-	-	SAFETY CRITICAL
2	-	-	HIGH	-	-	CRITICAL
3	-	-	MED	-	-	MODERATE
4	-	-	LOW	-	-	N/ CRITICAL
Topology base						
5	-	V/HIGH	-	-	-	SAFETY CRITICAL
6	-	HIGH	-	-	-	CRITICAL
7	-	MEDIUM	-	-	-	MODERATE
8	-	LOW	-	-	-	N/ CRITICAL
Occurrence- detectability base						
9	AND	-	-	E/UNPRO	Not LATENT	N/ CRITICAL
10	AND	-	-	REMOTE	Not LATENT	N/ CRITICAL
11	AND	-	Not LOW	OCCASIONAL	Not LATENT	MODERATE
12	AND	-	Not LOW	R/PROBABLE	V/HIGH	MODERATE
13	AND	-	Not LOW	R/PROBABLE	Not V/HIGH	CRITICAL
14	AND	-	Not LOW	FREQUENT	Not V/HIGH	SAFETY CRITICAL
Combinatory rules						
15	AND	V/HIGH	-	FREQUENT	-	SAFETY CRITICAL
16	AND	HIGH	-	R/PROBABLE	Not V/HIGH	CRITICAL
17	AND	MEDIUM	-	Not FREQUENT	Not LATENT	MODERATE
18	AND	LOW	-	Not FREQUENT	Not LATENT	N/ CRITICAL
19	AND	-	HIGH	E/UNPRO	V/HIGH	MODERATE
20	AND	-	MED	E/UNPRO	Not LATENT	N/ CRITICAL
21	AND	-	MED	REMOTE	Not LATENT	N/ CRITICAL
22	AND	-	MED	OCCASIONAL	V/HIGH	N/ CRITICAL
23	AND	-	MED	OCCASIONAL	HIGH	N/ CRITICAL
24	AND	-	LOW	R/PROBABLE	-	N/ CRITICAL
25	AND	-	LOW	FREQUENT	-	N/ CRITICAL

5.8.2 Defuzzification

De-fuzzification is done in the order to gain the fuzzy process single scalar quantity output. It processes to obtain crisps 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 uses 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.

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

Equations 8 COG Defuzzification technique

Figure 63 shows, that a centroid defuzzification method finds a point representing the center of gravity of the fuzzy set, on particular interval. 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. [31]

Following table shows case study most critical items resulting from fuzzy inference process. Differences between extended criticality are not large. However, extended criticality number is a **relative measure** of item importance. It is based on quantitative volumes and qualitative description of system provides by expert knowledge.

5.9 FUZZY EVALUATION OUTPUTS

As it was described in previous chapters, fuzzy evaluation process results in item extended criticality number and system robustness number for a given category. Robustness number provides additional information about system design. Robustness evaluation is applied on doctoral thesis case study (see **Appendix C**). Table 40 gives an example of robustness numbers for case study avionics system.

Table 40 Robustness parameters- case study example

System	Separation/ segregation	Diversity/ redundancy	Complexity/ design/ maturity/ experience	Environmental control/ testing
Avionics	Score. 0,901 Level VERY HIGH	Score. 0,633 Level. HIGH	Score. 0,903 Level. VERY HIGH	Score. 0,743 Level. HIGH

Resulting extended criticality numbers form extended criticality importance list. It identifies most critical items of a given system and global model. Fuzzy criticality evaluation is applied on doctoral thesis case study (see **Appendix C**). Following table provides illustrative cut-out importance list for case study application (Table 41).

Table 41 Extended criticality- case study selected items

System	Node name	NTP	HLS	Occurrence	Detectability	EXTENDED CRITICALITY
TRIM	TR REL	40,90	7,50	1,86E-06	5,5	5,000815662
TRIM	FUSE A10	40,90	7,50	2,38E-06	7,0	5,000815662
ELCSYS	LLC	36,97	3,50	1,06E-04	6,0	5,000815662
ELCSYS	RLC	36,94	3,50	1,06E-04	6,0	5,000815662
AVIO	EHSI #2	18,32	4,50	3,00E-04	3,5	4,375413348
TRIM	TR BUS	42,15	7,50	2,50E-07	6,5	4,311464805
ELCSYS	L MAIN	56,80	3,00	2,50E-07	6,5	4,252264671
ELCSYS	BUSTIE	18,50	1,50	1,06E-04	6,0	1,945567198
E.IND	OIL TEMP L-SEN	5,10	2,25	1,24E-06	8,0	1,757189542
E.IND	OIL TEMP R-SEN	5,10	2,25	1,24E-06	8,0	1,757189542
AVIO	VS #2	0,90	1,00	1,04E-04	6,0	0,901851852
AVIO	DG SEN #1	1,49	1,00	5,28E-04	2,0	0,901851852

CHAPTER 6

INTEGRATED METHOD PROCESS

6.1 PROCESS

This chapter briefly summarizes integrated method process. Process is divided into four main parts. It starts with system definition, then continues with item definition, system model processing, fuzzy criticality evaluation and ends with outputs reports.

I. System Definition

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

II. Items

- List of items
- System interconnections and allocated function (**Graph model**)
- Item potential failure modes (Using **Appendix A**)
- Item occurrence levels (Using **Appendix B** or commercial reliability database)
- Item detectability
- Item **HLS** (Relation to the allocated function)

III. System model

- Allocated function failure modes and rough trees
- 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

CHAPTER 7

A CASE STUDY

7.1 PRIMARY 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.

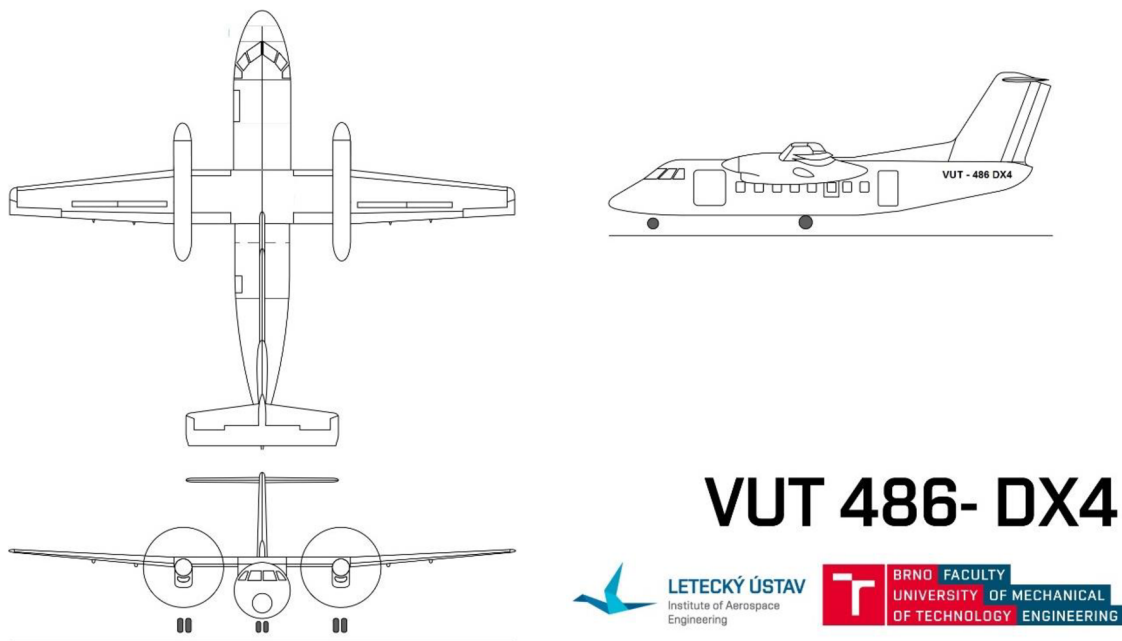


Figure 64 VUT 486- DX4

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.

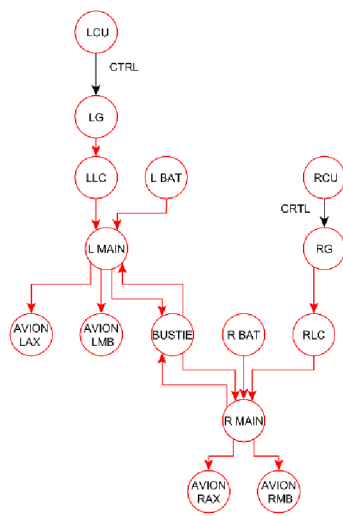
Pitot- static system provides static and dynamics pressure to the significant avionics indicators which provide information about airspeed, altitude and vertical speed. It consists of pressure tubes, inputs, tubes and mechanical valves. Elevator trim system controls trailing edge of a control surface 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 functionality directly influence other system functions. It is basically backbone of any larger airplane.

7.2 PRIMARY CASE STUDY SYSTEMS

7.2.1 Electrical System



Electrical system is designed as two channels with four independent energy sources. Left starter/ generators (**LG**) primary provides electrical energy power for left channel, right channel is supplied by right engine. Generators are connected to the network by contactor **LLC**, **RLC** respectively. Both channels could be tied in the case of emergency situation by **BUSTIE** contactor, which connects left and right main bus (**L MAIN/ R MAIN**). Two batteries (**L BAT/ R BAT**) are connected to the system through main buses. These batteries could fully supply all electrical loads for at least 30 minutes (according to the EASA CS-23 requirements).

Main avionics buses (**AVION LMB/ RMB**) supplies electrical energy to the avionics essential items. Non- essential items are connected to the avionic auxiliary buses (**AVION LAX/ RAX**).

Figure 65 Case study electrical system On board generators (**LG/ RG**) functions are controlled by their control units (**LCU/ RCU**). These units operate generators motion and provide protection in the case of failure.

Electrical system is adjusted for doctoral thesis purposes. It consists of 23 items (average electrical system of this category consists of 100+ items). This is adjustment serves to simplification of case study.

Table 42 Case study electrical system allocated functions

ELECTRICAL SYSTEM ALLOCATED FUNCTIONS (selected for doctoral thesis)	
<i>ATA 100</i>	<i>Preliminary Classification/ Function severity</i>
EL1 L/GENERATOR DRIVE 24-10	MINOR FS 3
EL2 R/GENERATOR DRIVE 24-10	MINOR FS 3
EL3 DC GENERATION (L BATTERY) 24-30	MINOR FS 3
EL4 DC GENERATION (R BATTERY) 24-30	MINOR FS 3
EL5 DC ELECTRICAL DISTRIBUTION 24-60	MINOR FS 3
COMBINATORY DC ELECTRICAL DISTRIBUTION	HAZARDOUS FS 7,85

7.2.2 Avionics system

Avionics system is designed as a hybrid system, consisting of two digital integrated avionics units GPS/ NAV/ Comm/ MFD touchscreens and mechanical and aerometric backup instruments. VUT 486 system is intentionally outdated. This type of hybrid avionics system allows to test doctoral thesis integrated method on various types of items clustered into single system.

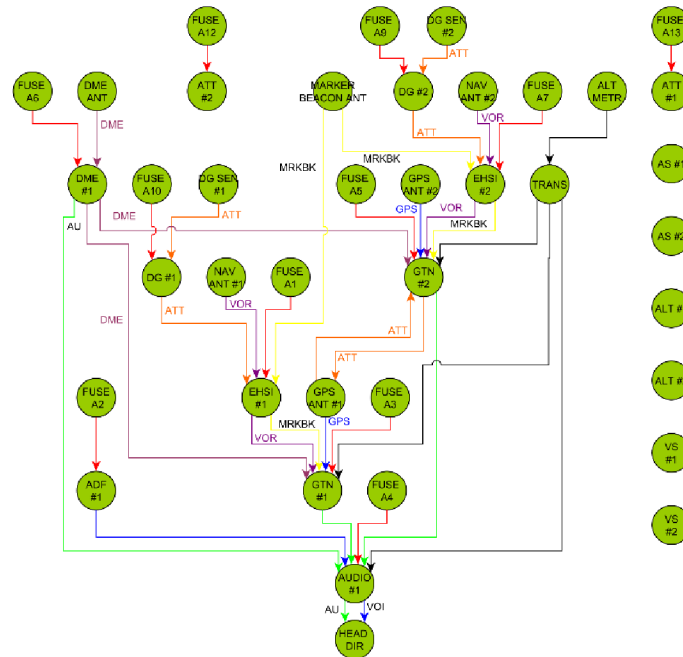


Figure 66 Case study avionics system

System is inspired by similar Czech-made aircrafts in category EASA CS-23, however it is different. Therefore, analysis results do not represent state of any actual avionics system of these aircrafts.

Integrated avionics units (**GTN #1**, **GTN #2**) allow voice communications with ATC and other aircrafts, state ambient weather conditions, displays attitude, turn and slip indication (using the **EHSI #1**, **EHSI #2** and **DG #1**, **DG#2**), landing aids and GPS/ VOR navigation, distance measure.

System is equipped by distance measuring equipment (**DME #1**), automatics direction finder (**ADF #1**). Flight instrument subsystem consist of aerometric items (altimeters **ALT #1/ #2**, airspeed indicator **AS #1/ #2** and vertical speed indicators **AS #1/#2**), backup mechanical attitude indicators (**ATT #1/ #2**).

Table 43 Case study avionics system allocated functions

AVIONICS SYSTEM ALLOCATED FUNCTIONS (selected for doctoral thesis)	
<i>ATA 100</i>	<i>Preliminary Classification/ Function severity</i>
AV1 VERTICAL SPEED 34-10	MINOR FS 2 (<i>Loss of function</i>)
AV2 ALTITUDE INDICATION 34-10	HAZARDOUS FS 8 (<i>Loss of function</i>)
	IFR/ CATASTROPHIC FS 10 (<i>Loss of function</i>)
AV3 DISTANCE MEASURE 34-50	MINOR FS 2 (<i>Loss of function</i>)
AV4 VOR/ LOC 34-50	MINOR FS 2 (<i>Loss of function</i>)
AV5 GPS 34-50	MINOR FS 2 (<i>Loss of function</i>)
AV6 ATTITUDE INFORMATION 34-20	HAZARDOUS FS 8 (<i>Loss of function</i>)
	IFR/ CATASTROPHIC FS 10 (<i>Loss of function</i>)
AV7 MARKER BEACON 34-50	MINOR FS 2 (<i>Loss of function</i>)
AV8 ADF 34-50	MINOR FS 2 (<i>Loss of function</i>)
AV9 AIRSPEED INDICATION 34-10	MAJOR FS 5 (<i>Loss of function</i>)
	IFR/ HAZARDOUS FS 8 (<i>Loss of function</i>)
AV10 AUDIO	MINOR FS 2 (<i>Loss of function</i>)

7.2.3 Elevator trim system

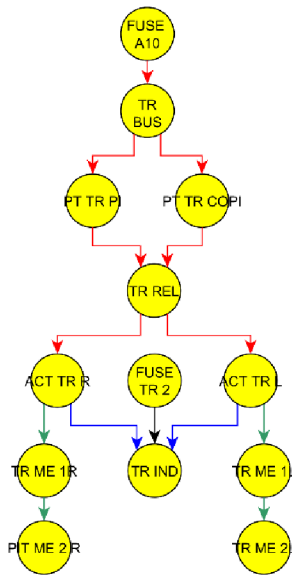


Figure 67 Case study elevator trim

Elevator trim system consist of electrical control system, indication, actuator generating kinetic energy and mechanical parts transforming this energy into an elevator trim movement.

System is connected to the electrical system through **FUSE A10** to the **L MAIN** bus. Flight crew is able to control elevator trim using the **PT TR PI** switch, co-pilot controls system using **PT TR COPI**. Pilot action is transfer from switches through **TR** relay to the actuators.

Actuator **ATC PT L** generates kinetic energy to operate left elevator trim, this energy is transformed through mechanical interconnection **PT ME 1L** and **PIT ME 2L**. **ATC PT R** generates kinetic energy to operate right elevator trim, this energy is transformed through mechanical interconnection **PIT ME 1R** and **PIT ME 32R**.

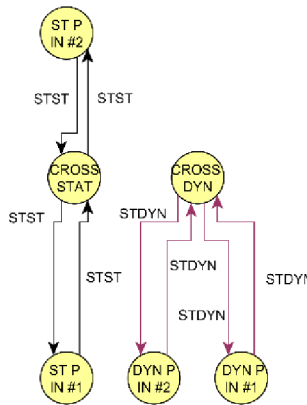
Position of elevator trim is indicated to the flight crew; this information is transferred to the display through the **TR IND**.

System consist of 14 items, interconnected by 14 wires and mechanical parts.

Table 44 Case study elevator trim system allocated functions.

ELEVATOR TRIM SYSTEM ALLOCATED FUNCTIONS (selected for doctoral thesis)	
<i>ATA 100</i>	<i>Preliminary Classification/ Function severity</i>
ET1 PITCH TRIM L (27-30a)	MAJOR FS 5 (Loss of function)
ET2 PITCH TRIM R (27-30b)	MAJOR FS 5 (Loss of function)
ET3 PITCH TRIM IND (27-30c)	MINOR FS 2,5 (Loss of function)

7.2.4 Pitot-static system



System provides static and dynamic pressure for various avionics. There are two pairs of static pressure inputs (**ST P IN #1/ #2**), located on the both sides of pilot cabin. Both channels could be connected through the static pressure cross valve (**CROSS STAT**) in the case of one channel blockage or leakage. Static pressure is provided for instance to airspeed indicators (**AS #1/ #2**).

There are also two dynamic pressure inputs. Pitot-static tubes are located on left and right side of pilot cabin (**ST D IN #1/ #2**). Both channels could be connected through the dynamic pressure cross valve (**CROSS DYN**) in the case of one channel blockage or leakage. Pitot-static tubes ice and rain protection is part of other system.

Table 45 Case study Pitot-static system allocated functions

PITOT-STATIC SYSTEM ALLOCATED FUNCTIONS (selected for doctoral thesis)	
<i>ATA 100</i>	<i>Preliminary Classification/ Function severity</i>
DYNAMIC PRESSURE INPUT	-
STATIC PRESSURE INPUT	-

7.2.5 Engine indication system

Aircraft is equipped by two reciprocating engines. Flight crew has to be notified about their functionality. Engine indication system provides information about engine ongoing parameters, processed advisory notification, caution and warning indication in the case of engine (or engines) malfunction. Minimal flight crew response time could reduce possibility of engine damage or minimize airplane safety impact. Key role of engine indication system have two data acquisition units (DAU) which carry out system intended functions. DAU units are connected to the central warning panel and particular warning lamps- **L-ENGINE**, **R-ENGINE**, **OIL PRESS L**, **OIL PRESS R** and **MAIN ELC**.

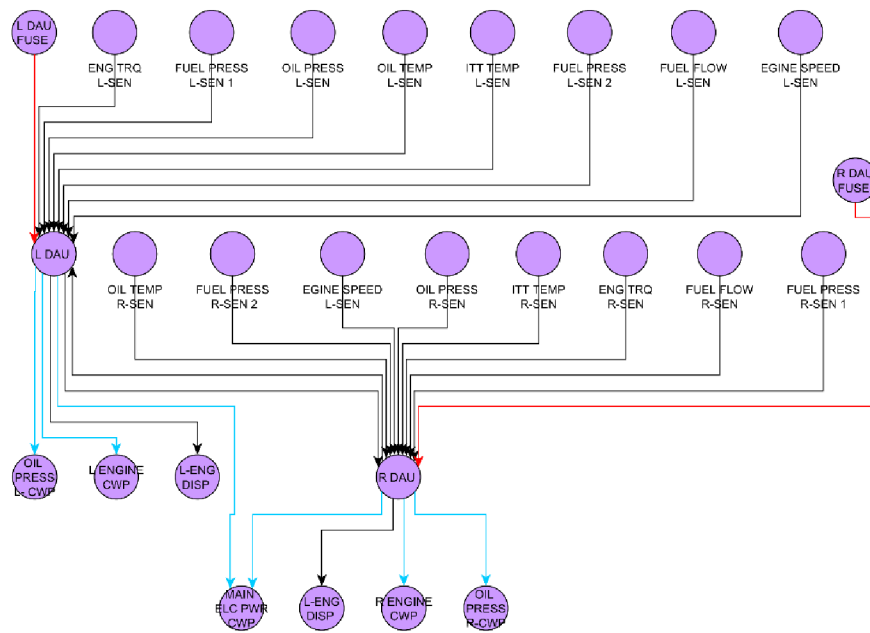


Figure 69 Case study engine indication system

Table 46 Case study Engine indication allocated function

PITOT-STATIC SYSTEM ALLOCATED FUNCTIONS (selected for doctoral thesis)	
ATA 100	Preliminary Classification/ Function severity
E11 TACHO INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E12 OIL PRESSURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E13 FUEL PRESSURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E14 TORQUE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E15 FUEL FLOW INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E16 OIL TEMPERATURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
E17 ITT INDICAITON 77-10	MINOR FS 2,5 (Loss of function)

7.3 EVALUATION PROCESS RESULTS

This chapter summarizes case study evaluation results. Case study analysis itself is attached as **Appendix C**. 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.

7.3.1 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).

Table 47 Case study global model evaluation- basic parameters

<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

There are 11 multi edge pairs. These pairs are strongly connected (integrated avionics units, DAU units or L MAIN- BUSTIE- R MAIN interconnection). Each node has in average two neighbors (preceding and succeeding item).

7.3.2 Extended criticality results

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).

Table 48 Case study global model evaluation results- extended criticality list

<i>Most critical items (Global)</i>	#	Name	WNTP	HLS	Occurrence	Detectability	Extended criticality
	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
	9	R MAIN (ELEC)	51,64	3,00	2,50E-07	6,5	4,252264671
	10	GTN #2 (AVIO)	46,71	4,75	4,58E-05	2,0	4,181228147
	11	R DAU (ENGIND)	68,60	3,75	3,74E-06	2,0	4,151774628
	12	L DAU (ENGIND)	68,25	3,75	3,74E-06	2,0	4,151774628
	13	GTN #1 (AVIO)	46,06	4,75	4,58E-05	2,0	4,108015073
	14	AS #1 (AVIO)	5,24	4,00	8,12E-05	6,0	4,008398077
	15	AS #2 (AVIO)	5,09	4,00	8,12E-05	6,0	4,008398077

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 extended criticality) of Pitot-static system are identified **CROSS STAT/ DYN** valves (not on this list) and sixteenth and seventeen globally.

Complete list of critical items is stated in **Appendix C**.

7.3.3 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).

Table 49 Case study global model evaluation results- node interconnection

<i>Name</i>	<i>#</i>	<i>Local importance (SubG)</i>	<i>#</i>	<i>Name</i>	<i>Global importance (BC)</i>
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
L MAIN (ELEC)	9	6,60	9	RLC (ELEC)	0,0160
AVION RMB (ELEC)	10	6,59	10	FUSE A10 (TRIM)	0,0129

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 items. 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.

7.3.4 Robustness parameters results

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**.

Table 50 Case study- system robustness parameter

SYSTEM ROBUSTNESS PARAMETERS				
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

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.

7.3.5 Rough tree evaluation results

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).

Table 51 Case study rough tree evaluation

<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
AIRSPEED 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

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).

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.

BIBLIOGRAPHY

- [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] ARP4754 *Certification Considerations for Highly-Integrated or Complex Systems*, the Engineering Society for Advancing Mobility Land Sea and Space, Warrendale USA, 1996
- [3] MIL-STD-1629A *Military Standard Procedures for performing a failure mod, effect and criticality analysis*, Department of Defense Washington, DC USA, 1977
- [4] FAA Air Traffic Organization, *Safety Management System Manual v.4*, Department of Defense Chapter 3
- [5] 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
- [6] 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
- [7] ROSS, T.J., *Fuzzy logic with Engineering Application*, McGraw-Hill, New York, N.Y., 1995
- [8] 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
- [9] BRAGLIA, M., *MAFMA: Multi-attribute failure mode analysis*, International Journal of Quality & Reliability Management, Vol. 17 Iss 9 pp. 1017 – 1033, 2000
- [10] HIPAP 8: *HAZOP Guidelines*, State of New South Wales through the Department of Planning, 2008
- [11] NOVÁK, V., PERFILIEVA, I. and MOČKOŘ, J.: *Mathematical principles of fuzzy logic*, Dodrecht: Kluwer Academic
- [12] ROSS, T.J. *Fuzzy logic with engineering applications*. 2nd ed. Hoboken, NJ: John Wiley, c2004, xxi, 628 p. ISBN 0470860758-.
- [13] RAO, Singiresu S. *Reliability-based design*. New York: McGraw-Hill, c1992. ISBN 0-07-051192-6.
- [14] HOLUB, R., VINTR, Z., *Spolehlivost letadlové techniky (elektronická učebnice)*, VUT-FSI, Brno, 2001, 233 str.
- [15] GROSS, J. L., YELLEN, J., ZHANG, P.; *Handbook of Graph Theory*, Taylor & Francis Group, LLC, 2014
- [16] THANG. J., *Mechanical system reliability analysis using combination of graph theory and Boolean logic*, Reliability Engineering and System Safety 72 (2001) 21-30
- [17] SHANNMON R.M., ANDREWS J.D., *New approaches to evaluating fault tree*, Reliability Engineering and System Safety 58 (1997) 89-96

- [18] 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.
- [19] O'CONNOR, P.D., *Practical reliability engineering*. 4th ed. Chichester: John Wiley & Sons, 2002, 513 s. ISBN 0-470-84463-9.
- [20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*
- [21] 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
- [22] 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.
- [23] 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
- [24] MOIR, I. *Civil avionics systems*, 2003, Chichester: John Wiley, 2006, 395 p. ISBN 1 86058 342 3.
- [25] *Procedure for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, Vol. 1, 2, NRC, 1988.
- [26] NASA System Safety Handbook vol2.: Available from:
<https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150015500.pdf> [17. 8. 2018]
- [27] MIL-HDBK-217F NOTICE 2 *Reliability Prediction of Electronic Equipment*, US Department of Defence, Washington DC 20301, February 1995
- [28] MIL-HDBK-338B *Electronic Reliability Design Handbook*, US Department of Defence, Washington DC 20301, October 1998
- [29] SRC SPIDR *System and Part Integrated Data Resource v.1.0*, System Reliability Center, Rome, New York 13440, 2007
- [30] RIAC Databook 3.0.1 *NPRD-2011C, FMD-97CD, EPRD97-CD, VZAP-95C, 2011*
- [31] NEGNEVITSKY, Michael. *Artificial intelligence: a guide to intelligent systems*. 2nd ed. New York: Addison-Wesley, 2005. ISBN 0321204662.
- [32] ZHOU W., SHEN H. *Function-oriented Risk Model for Engineering System*. *Advance Materials Research*, Vols. 433-440 (2012) pp 2899-2903
- [33] Brandes, U.: *A faster algorithm for betweenness centrality*. *J Math Sociol* 25 (2001) 163-177
- [34] 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

- [35] NEWMAN, M.E.J.: *A measure of betweenness centrality based on random walks*. arXiv (2003) cond-mat/0309045
- [36] SHANNON P, MARKIEL A, OZIER O, BALIGA NS, WANG JT, RAMAGE D, Amin N, SCHWIKOWSKI B, IDEKER T. *Cytoscape: a software environment for integrated models of biomolecular interaction networks*. Genome Res, 13:11 (2498-504). 2003 Nov. PubMed ID: 14597658.
- [37] SCARDONI G., TOSADORI G., LAUDANNA C., FABBRI F., FAIZAAAN M., *CentiScaPe: Network centralities for Cytoscape*, Available from: <https://f1000research.com/articles/3-139/v2>
- [38] ESTRADA E., RODRÍGUEZ- VELÁZQUEZ J., *Subgraph centrality in complex networks*, Physical Review E 71, 056103, 2005
- [39] M. Zeleňáková and L. Zvijáková, Using Risk Analysis for Flood Protection Assessment, DOI 10.1007/978-3-319-52150-3_2
- [40] Let L-410UVP-E8 Turbolet, Available from:
<http://www.airliners.net/photo/Untitled-ABC-Air/Let-L-410UVP-E8-Turbolet/2732835?qsp=eJwtjEEKAkEMBL8iOXtQFJG96VnQgx8ISaOLqzMkAR2W/bszq7fqaqiRjL0Cn7iWDOrlwSZ3WlJm46dTN9ID5Z1MK9NpsV2v6unJ4liqUA4cRJAD%2BvdnU1i74DJ3bq27bwi7/NZmV6f2ngeeKwjuB5qmLx3BLec%3D> [17. 8. 2018]
- [41] EASA CS-23, *Certificaiton Specificaiton for Normal, Utility, Aerobatic, and Commuter Category Airplanes*
- [42] FAR/JAR 25.1322 & AC/ACJ 25.1322, *Warning Caution and Advisory Lights*
- [43] FAA AC 25.1581-1, *Airplane Flight Manual*
- [44] KOŠTIAL, R. Plán prohlídek a údržby draku malého dopravního letounu s využitím moderních přístupů. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2017. 198 s. Vedoucí dizertační práce doc. Ing. Jiří Hlinka, Ph.D..
- [45] Evektor VUT 100-120IX Cobra VPR. Available from:
<http://www.airliners.net/photo/Untitled/Evektor-VUT-100-120IX-Cobra-VPR/2430993/L?qsp=eJwtjMEKwkAMBX9FcvbQInjoTX9AD9V7SB5arO6SDehS%2Bu/GxdswA7OQpJfj42PNolEK2OROW8ps/Cw0LPRAfSfTYLpexk3fdZFLMj/WUMqOgwiwQ/%2BZAr7JRRpp1uc%2BwDYuTht9uF1Knnm9oDzNNO6fgEv9C5L> [17. 8. 2018]
- [46] Piper PA-31-350 Chieftain, Available from:
<http://www.airliners.net/photo/Untitled/Piper-PA-31-350-Chieftain/2502004?qsp=eJwtjUEKwjAURK8if21BCe2iO72AWXiBTzLUYDXh50MNPxc3qe5m5g0zK7n4Vnz0XhJopAwW96AjJRZ%2BZRpxeqIsUXzVZEOCHCx35tyZ/IRrOYpeS0WeFRfnkBT%2Bn9/EQxpCdvvi1B76JiH258xQrQ85zbyvQDnMtG1f/%2B8xCg%3D%3D> [17. 8. 2018]
- [47] Line replaceable unit LRU, Available from: <http://www.aircraftengineer.info/line-replaceable-unit-lru/> [17. 8. 2018]

- [48] Airbus A330-243 - Hawaiian AirA330 Landing gear, Available from:
<http://www.airliners.net/photo/Hawaiian-Air/Airbus-A330-243/2211908/L?qsp=eJwtjEEKAjEQBL8ic/YmCO5NP6AHPzBkmmwwJmEyoGHZv5use%2BvqbmohI5Pha89WQBNVsLqZiIRY%2BV1pWuiF9skqPVPkJCH5g%2B%2Bv/qlZ7dZ6L2y4OodikL2/q0DHHoO2nR/6y4jQx59O544Saom8WWAclq3rD/IHMYM%3D> [17. 8. 2018]
- [49] Graph centralities, Available from: <http://chato.cl/research/> [17. 8. 2018]
- [50] 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.
- [51] Shannon P, Markiel A, Ozier O, Baliga NS, Wang JT, Ramage D, Amin N, Schwikowski B, Ideker T. *Cytoscape: a software environment for integrated models of biomolecular interaction networks*. *Genome Res*, 13:11 (2498-504). 2003 Nov. PubMed ID: 14597658.
- [52] Yu Tang, Min Li, Jianxin Wang, Yi Pan, Fang-Xiang Wu. CytoNCA: a cytoscape plugin for centrality analysis and evaluation of biological networks. *BioSystems*, 2014, DOI: 10.1016/j.biosystems.2014.11.005
- [53] 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*.

ACRONYMS AND ABBREVIATIONS

A/I	Acting item
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

LIST OF FIGURES

Figure 1 Simplified ARP 4761 process	11
Figure 2 EASA CS-23 Commuter aircraft basic systems example (based on [18])	17
Figure 3 Avionic system evolution (based on [18])	18
Figure 4 UAV system example	19
Figure 5 Failure of one main bus supply block diagram	20
Figure 6 Fault Tree Example	20
Figure 7 Markov Chain Example.....	21
Figure 8 Petri Net Example.....	21
Figure 9 Avionics system example in the form of graph	28
Figure 10 Simplified portrayal of safety process [18]	30
Figure 11 Functions hierarchy- illustration	31
Figure 12 Function- based modeling	32
Figure 13 Aircraft function examples	35
Figure 14 Integrated method architecture	39
Figure 15 System modeling	39
Figure 16 Rough failure tree “System Example-Loss of function”	40
Figure 17 System installation routing example	41
Figure 18 Simplified trim system model example	42
Figure 19 Graph theory application	43
Figure 20 Function based modelling example.....	44
Figure 21 Case study engine indication model.....	45
Figure 22 Global and local model.....	46
Figure 23 Case study avionics system with various types of interconnection illustration.....	47
Figure 24 Case study avionics filtered for HAZARDOUS associated nodes and edges (restricted for illustration)	48
Figure 25 $V = u, v, w, x; E = a, b, c, d, e, f$	49
Figure 26 Oriented graph example	50
Figure 27 Multi-graph example	51
Figure 28 Shortest path tree for graph example.....	52
Figure 29 Processing platform [Cytoscape. org]	52
Figure 30 Case study R MAIN bus predecessor example	53
Figure 31 (a) Case study R MAIN bus successors example (restricted for illustration purposes) (b) Pitch trim sequence.....	54
Figure 32 Case study GTN #2 succeeding function	54
Figure 33 Recursive algorithm block- Field-operator-field	56
Figure 34 System example- partially in failure	56
Figure 35 Recursive algorithm block- single input example.....	57
Figure 36 Recursive algorithm block- multiple input of same type example.....	57
Figure 37 Recursive algorithm block- complex inputs example.....	58
Figure 38 Recursive algorithm logic applied on system model example	58
Figure 39 Recursive algorithm out before (left) and after OR gates aggregation (right).....	59

Figure 40 Centrality, degree and clustering coefficient definition.....	60
Figure 41 A strongly connected (left) and weakly (right) connected directed graph	61
Figure 42 Example system betweenness centrality illustration (BC correspond to the edge size)	62
Figure 43 Classlessness centrality example.....	62
Figure 44 Clustering coefficient.....	64
Figure 45 Graph centralities illustration [49]	65
Figure 46 Combined influences on the extended criticality.....	73
Figure 47 High-level severity evaluation process.....	74
Figure 48 Function severity failure effects aggregation example	75
Figure 49 Item HLS and FS.....	76
Figure 50 Item High-level severity aggregation	77
Figure 51 Occurrence levels	78
Figure 52 Combined influences on the robustness number	80
Figure 53 PA-31-350 Chieftain (left)[46], VUT 100 (right) [45]	83
Figure 54 Fuzzy membership function for linguistic variable- detectability	87
Figure 55 Fuzzy membership function for linguistic variable- node topology	87
Figure 56 Fuzzy membership function for linguistic variable- high level severity	89
Figure 57 Fuzzy membership function for linguistic variable- occurrence	90
Figure 58 System parameters answer membership function	91
Figure 59 Extended criticality output membership function	92
Figure 60 Robustness parameter output membership function	93
Figure 61 Fuzzy inference process.....	95
Figure 62 Fuzzy logic rule application [31]	97
Figure 63 Fuzzy logic rules aggregation and de-fuzzification [31]	98
Figure 64 VUT 486- DX4.....	105
Figure 65 Case study electrical system.....	106
Figure 66 Case study avionics system	107
Figure 67 Case study elevator trim	109
Figure 68 Pitot-static system.....	110
Figure 69 Case study engine indication system	111

LIST OF TABLES

Table 1 General description of relevant regulation requirements	15
Table 2 Aircraft main functions	33
Table 3 Node- edge relation explanation	45
Table 4 Case study GTN #2 functions severity preliminary classification (restricted for illustration purposes).....	55
Table 5 Recursion operators application.....	57
Table 6 FTA direct technique estimation [14]	59
Table 7 Case study model parameters (global)	66
Table 8 Case study model parameters (avionics).....	66
Table 9 Case study model parameters (elevator trim).....	66
Table 10 Case study evaluation process output.....	68
Table 11 Case study evaluation process output 2.....	68
Table 12 Case study evaluation process output and allocated functions.....	69
Table 13 Case study evaluation process output- weighted	70
Table 14 Case study importance list based on NTP and weighted NTP	71
Table 15 Function severity	74
Table 16 HLS aggregation volumes	76
Table 17 Cumulated severity corrective measures	77
Table 18 Detectability criteria definition	79
Table 19 Questionnaire review - separation/ segregation class	81
Table 20 Questionnaire review - diversity/ redundancy class	82
Table 21 Questionnaire review example- Environmental class	82
Table 22 Classification database structure.....	83
Table 23 Classification knowledge database content	84
Table 24 Structure of basic parts reliability database	84
Table 25 Detectability scoring table.....	85
Table 26 Detectability examples	86
Table 27 Detectability levels definition	86
Table 28 NTP levels.....	88
Table 29 High- level severity levels	88
Table 30 Occurrence definition	90
Table 31 Questionnaire answers definition	91
Table 32 Extended criticality level definition	92
Table 33 Robustness level definition.....	94
Table 34 Extended criticality inputs fuzzification	96
Table 35 Robustness Inference rule base – separation/ segregation	98
Table 36 Robustness inference rule base- diversity/ redundancy	99
Table 37 Robustness inference rule base- Complexity/ Design/ Maturity	99
Table 38 Robustness inference rules- Environmental.....	100
Table 39 Extended criticality inference rule base	101
Table 40 Robustness parameters- case study example	103

Table 41 Extended criticality- case study selected items	103
Table 42 Case study electrical system allocated functions	106
Table 43 Case study avionics system allocated functions.....	108
Table 44 Case study elevator trim system allocated functions.....	109
Table 45 Case study Pitot-static system allocated functions	110
Table 46 Case study Engine indication allocated function.....	111
Table 47 Case study global model evaluation- basic parameters	112
Table 48 Case study global model evaluation results- extended criticality list	113
Table 49 Case study global model evaluation results- node interconnection	114
Table 50 Case study- system robustness parameter.....	115
Table 51 Case study rough tree evaluation.....	116

APPENDICES

Appendix A

Airborne Systems Classification Knowledge Database (44 pages)

Appendix B

Basic Items Reliability Data Overview (5 pages)

Appendix C

Case Study Evaluation (42 pages)

Appendix D

Robustness Questionnaire (8 pages)

Appendix E

Case Study Evaluation Detailed Figures (3 pages)

Appendix A

Airborne Systems Classification Knowledge Database

Effect evaluation

N/E (No effect or no direct effect as result of failure mode)	
Effect on:	
Airplane	No effect on operation capabilities or safety
Crew	Maybe inconvenience for passengers
Passengers	No effect on crew.
SLIGHT	
Effect on:	
Airplane	Slight reduction in functional capabilities or safety margins
Crew	Slight increase in workload or use of emergency procedures
Passengers	Physical discomfort for passengers
SIGN (Significant)	
Effect on:	
Airplane	Significant reduction in functional capabilities or safety margins
Crew	Physical discomfort or a significant increase in workload
Passengers	Physical distress to passengers, possible light injuries
LARGE	
Effect on:	
Airplane	Large reduction in functional capabilities or safety margins
Crew	Physical distress or extensive workload impairs ability to perform tasks
Passengers	Serious or fatal injury to an occupant
CAT	
Effect on:	
Airplane	Normally with hull loss
Crew	Fatal injury or incapacitation
Passengers	Multiple fatalities

Platform definition and Tags

Single Engine Aircraft ①
Definition: General aviation (EASA CS-23, with restriction UL, LSA), <ul style="list-style-type: none"> - DC power, Glass cockpit avionics with aerometric backup and autopilot, airborne batteries, flaps, symmetric trims - No cabin pressurization, No retractable landing gear
Multi Engine Aircraft ②
Definition: General aviation (EASA CS-23, multi engine classes, commuter) <ul style="list-style-type: none"> - Two generators, Glass cockpit avionics with aerometric backup and autopilot, airborne batteries, flaps, symmetric trims, hydraulic system, operable by single pilot, fuel cross-feed and electric bus-tie. Retractable landing gear (nose and main), heated cabin for passengers and crew - No cabin pressurization

PREFIXES and NOTES	
<p>POSSIBLE: It means, that there is a high possibility of particular effect based on critical review, however in real application effects could be different. Example P/SLIGHT (possible slight effect on Airplane/ Crew/ Passengers) <i>Note: Type of effects is based on FAA AC23.1309-1E</i></p> <p>IFR Flight: It means, that failure mode is analyzed for worst case scenario of Instrument Flight Rules IF/SIGN (In IFR condition significant effect on Airplane/ Crew/ Passengers)</p> <p>IMC Flight: It means, the failure mode is analyzed for worst case scenario of Instrument Meteorological Conditions</p> <p>IMC/SIGN (In ICM condition significant effect on Airplane/ Crew/ Passengers)</p>	<p>MITTIGATION MEANS: It refers to the chapter 3.7. It intends to state potentially applicable mitigation means. <i>MM # (number refers to the precise mitigation mean).</i></p>

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

ATA 100 (Selected chapters)		
22	AUTO FLIGHT	Those units and components which furnish a means of automatically controlling the flight of the aircraft. Includes those units and components which control direction, heading, attitude, altitude and speed.
23	COMMUNICATION	Those units and components which furnish a means of communicating from one part of the aircraft to another and between the aircraft or ground stations, includes voice, data, C -W communicating components, PA system, inter -com and tape reproducers - record player.
24	ELECTRICAL POWER	Those electrical units and components which generate, control and supply AC and/or DC electrical power for other systems, including generators and relays, inverters, batteries, etc., through the secondary busses. Also includes common electrical items such as wiring, switches, connectors, etc.
26	FIRE PROTECTION	Those fixed and portable units and components which detect and indicate fire or smoke and store and distribute fire extinguishing agent to all protected areas of the aircraft; including bottles, valves, tubing, etc.
27	FLIGHT CONTROL	Those units and components which furnish a means of manually controlling the flight attitude characteristics of the aircraft, including items such as hydraulic boost system, rudder pedals, controls, mounting brackets, etc. Also includes the functioning and maintenance aspects of the flaps, spoilers, and other control surfaces, but does not include the structure which is covered in the Structures Chapters. Does not include rotorcraft rotor controls which are covered in the Rotor Chapter 65.
28	FUEL	Those units and components which store and deliver fuel to the engine. Includes engine driven fuel pumps for reciprocating engines, includes tanks (bladder), valves, boost pumps, etc., and those components which furnish a means of dumping fuel overboard. Includes integral and tip fuel tank leak detection and sealing. Does not include the structure of integral or tip fuel tanks and the fuel cell backing boards which are covered in the Structures Chapters, and does not include fuel flow rate sensing, transmitting and / or indicating, which are covered in Chapter 73.
29	HYRAULIC POWER	Those units and components which furnish hydraulic fluid under pressure (includes pumps, regulators, lines, valves, etc.) to a common point (manifold) for redistribution to other defined systems.
30	ICE AND RAIN PROTECTION	Those units and components which provide a means of preventing or disposing of formation of ice and rain on various parts of the aircraft. Includes alcohol pump, valves, tanks, propeller / rotor anti-icing system, wing heaters, water line heaters, pitot heaters, scoop heaters, windshield wipers and the electrical and heated air portion of windshield ice control. Does not include the basic windshield panel. For turbine type power plants using air as the anti-icing medium, engine anti-icing is contained under Air System.
31	INDICATING/ RECORDING SYSTEMS	Pictorial coverage of all instruments, instrument panels and controls. Procedural coverage of those systems which give visual or aural warning of conditions in unrelated systems. Units which record, store or compute data from unrelated systems. Includes systems/units which integrate indicating instruments into a central display system and instruments not related to any specific system.
32	LANDING GEAR	Those units and components which furnish a means of supporting and steering the aircraft on the ground or water, and make it possible to retract and store the landing gear in flight. Includes tail skid assembly, brakes, wheels, floats, skids, skis, doors, shock struts, tires, linkages, position indicating and warning systems. Also includes the functioning and maintenance aspects of the landing gear doors but does not include the structure which is covered in Chapter 52 DOORS.

ATA 100 (Selected chapters)		
33	LIGHTS	Those units and components (electrically powered) which provide for external and internal illumination such as landing lights, taxi lights, position lights, rotating lights, ice lights, master warning lights, passenger reading and cabin dome lights, etc. Includes light fixtures, switches and wiring. Does not include warning lights for individual systems or self -illuminating signs (see Chapter 11).
34	NAVIGATION	Those units and components which provide aircraft navigational information. Includes VOR, pitot, static, ILS, flight director, compasses, indicators, etc.
46	INFORMATION SYSTEMS	Those units and components which furnish a means of storing, updating, and retrieving digital information traditionally provided on paper, microfilm, or microfiche. Includes units that are dedicated to the information storage and retrieval function such as the Electronic Library mass storage and controller. Does not include units or components installed for other uses and shared with other systems, such as flight deck printer or general use display.
76	ENGINE CONTROLS	Those controls which govern operation of the engine. Includes units and components which are interconnected for emergency shutdown. For turbo-prop engines, includes linkages and controls to the coordinator or equivalent to the propeller governor, fuel control unit or other units being controlled. For reciprocating engine, include controls for blowers. Does not include units or components which are specifically included in other chapters.
77	ENGINE INDICATING	Those units, components and associated systems which indicate engine operation. Includes indicators, transmitters, analyzers, etc. For turbo-prop engines includes phase detectors. Does not include systems or items which are included in other chapters except when indication is accomplished as part of an integrated engine instrument system (ref. 77-40).
80	STARTING	Those units, components and associated systems used for starting the engine. Includes electrical, inertial air or other starter systems. Does not include ignition systems which are covered in chapter 74, IGNITION.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
AIR CONDITIONING									
Related MF: -					Related systems: 24, 72				
System corrective measures: -									
Mitigation means: EMERGE CNY DESCENT OR LANDING (MM4,MM5)									
21	10	Pressurization	-	-	-	-	-	-	<i>Not applied in the field of interest.</i>
	20	Distribution	-	-	-	-	-	-	
	30	Pressurization Control	-	-	-	-	-	-	
	40	Heating	At flight	Loss of function.	SIGN	P/LARGE	P/LARGE	<i>Up to</i> HAZARDOUS FS 8,5	In the case of low outside temperatures it leads to the passenger serious discomfort or injuries. Extensive increase of flight crew workload. Functionality of aerometric and navigational equipment is jeopardized. Front windshield freezing. Crew has to rapidly descent to the lower altitudes or conduct emergency landing.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
21	AIR CONDITIONING								
	50	Cooling	At flight	Loss of function.	P/SLIGHT	SLIGHT	SLIGHT	MINOR FS 3	Cabin temperature could be outside optimal parameters. There is slight possibility of flight crew workload increase.
	60	Temperature Control	At flight	Loss of function or incorrect function resulting in cabin temperature decrease.	SIGN	P/LARGE	P/LARGE	Up to HAZARDOUS FS 8,5	At worst leads to the loss of ability to heat cabin. Passenger serious discomfort or injuries. Extensive increase of flight crew workload. Functionality of aerometric and navigational equipment is jeopardized. Front windshield freezing. Crew has to rapidly descent to the lower altitudes or conduct emergency landing.
			At flight	Loss of function or incorrect function resulting in cabin temperature increase.	P/SLIGHT	SLIGHT	SLIGHT	MINOR FS 3	Cabin temperature could be outside optimal parameters. There is slight possibility of flight crew workload increase.
70	Moisture/Air Contaminant Control	At flight	Loss of function or incorrect function.	P/SLIGHT SIGN <i>Coolant contamination</i>	SLIGHT SIGN <i>Coolant contamination</i>	SLIGHT SIGN <i>Coolant contamination</i>	MINOR FS 3 MAJOR FS 6 <i>Coolant contamination</i>	Cabin temperature could be outside optimal parameters.	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
AUTO FLIGHT									
Related MF: NAVIGATION, FLIGHT CONTROL					Related systems: 24, 27, 34				
System corrective measures: -									
Mitigation means: HUMAN OVERRIDE (MM4,MM5), FUSE SHUT DOWN (MM6), EMERGENCY PROCEDURES									
22	10	Autopilot	ALL	Loss of function	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew is able to continue flight without aid of autopilot.
			ENR	Spurious activation.	N/E	SLIGHT	N/E	MINOR FS 1	Crew is able to deactivate system by switch or using the particular fuse. Significant increase of crew workload during critical flight phases.
			TOF, ICL, APR, LDG		SLIGHT	SIGN	N/E	MAJOR FS 4,5	
			ENR	Spurious deactivation.	N/E	SLIGHT	N/E	MINOR FS 1	Flight crew continue flight without autopilot. System is not activated in other flight phase.
			ENR	It is not possible to deactivate.	N/E	SLIGHT	N/E	MINOR FS 1	In standard configuration. Crew is able to deactivate system using the particular fuse.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
22	AUTO FLIGHT								
	20	Speed - Attitude Correction	-	-	-	-	-	-	Mainly not applied in the field of interest.
	30	Auto Throttle	-	-	-	-	-	-	Not applied in the field of interest.
	40	System Monitor	ALL	Loss of function.	N/E	SLIGHT	N/E	MINOR FS 1	There is possibility of system failure without indication. Crew is able to safely continue flight without auto pilot.
Incorrect function.				SLIGHT	SLIGHT	N/E	MINOR FS 2	In the case of incorrect failure indication, crew continues flight without aid of autopilot. In the case of system failure, crew is able to identify it due to collateral effect and turn down autopilot.	

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
23	COMMUNICATIONS								
	Related MF: NAVIGATION AND COMM.					Related systems: 24			
	System corrective measures: HEADPHONE								
	Mitigation means: EMERGENCY PROCEDURES, 34-50 DEPENDENT POSITION DETERMMINING (MM2)								
	10	Speech Communication	ALL	Loss of function.	SLIGHT	LARGE	N/E	HAZARDOUS FS 7,25	In the case of inability to communicate with ATC and other aircrafts. Crew follows emergency procedures (Loss of ATC voice comm.) according to the AFM.
	20	Data Transmission & Automatic Calling	-	-	-	-	-	-	Mainly not applied in the field of interest.
	30	Passenger Address and Entertainment	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT	-
	40	Interphone	ALL	Loss of function.	N/E	SLIGHT	N/E	MINOR FS 1	Crew is able to communicate without headphones.
	50	Audio Integrating		Loss of function.	SLIGHT	LARGE	N/E	HAZARDOUS FS 7,25	Crew follows emergency procedures according to the AFM.
60	Static Discharging	-	-	-	-	-	-	-	
70	Audio and Video Recorder	-	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT		
80	Integrated Automatic Tuning	-	-	-	-	-	-	Mainly not applied in the field of interest.	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ELECTIRAL POWER									
Related MF: PROPULSTION, NAVIGATION AND COMM., FLIGHT CONTROL, LANDING AIDS					Related systems: 39, 34, 23, 22				
System corrective measures: BUS-TIE (MM1), 24-10 BATTERY POWER (MM2)									
Mitigation means: EMERGENCY PROCEDURES									
24	10	Generator Drive	ALL	Complete loss of function.	LARGE	SIGN	SLIGHT	HAZARDOUS FS 7,85	Mechanical disconnection of generator and engine. Flight manual emergency procedures. Mitigation means- flight on batteries (30 minutes) is mandatory due to EASA CS-23 requirements.
				Loss of function- one generator. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Normal configurations of electrical system allow to power all loads using remaining generator.
	20	AC Generation	ALL	-	-	-	-	-	-
	30	DC Generation	ALL	Loss of function.	LARGE	SIGN	SLIGHT	HAZARDOUS FS 7,85	Flight manual emergency procedures. Mitigation means-flight on batteries (30 minutes) is mandatory due to EASA CS-23 requirements.

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ELECTRICAL POWER									
24	30	DC Generation	ALL	Loss of function- one generator ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Normal configurations of electrical system allow to power all loads using remaining generator.
			ALL	Loss of function (battery power).	SLIGHT	N/E	N/E	MINOR FS 2	Under the normal situation, power network is supplied by airborne generators. In the case of generator(s) common failure, it leads possibly to the catastrophic conditions.
	40	External Power	STD	Loss of function	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	Not applied during in air flight phases.
	50	AC Electrical Load Distribution	ALL	Loss of function.	-	-	-	-	<i>It is based on particular system design; it is not possible to generally evaluate.</i>
				Incorrect function.	-	-	-	-	
	60	DC Electrical Load Distribution	ALL	Loss of function.	LARGE	SIGN	SLIGHT	HAZARDOUS FS 7,85	Flight manual emergency procedures. Mitigation means-flight on batteries (30 minutes) is mandatory due to EASA CS-23 requirements.
ALL			Loss of function. (One generator) ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Normal configurations of electrical system allow to power all loads using remaining generator.	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FIRE PROTECTION									
Related MF: ALL					Related systems: 24				
System corrective measures: HANDHELD FIRE EXTINGUISHER									
Mitigation means: EMERGENCY PROCEDURES									
26	10	Detection	ALL	Loss of function.	P/LARGE	P/LARGE	P/LARGE	HAZARDOUS FS 9	High probability of serious or fatal injury in the case of fire.
				Misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 3	Crew has to visually identify misleading situation.
	20	Extinguishing	ALL	Loss of function.	P/CAT	P/CAT	P/CAT	CATASTROPHIC FS 10	High probability of serious or fatal injury in the case of fire.
	30	Explosion Suppression	ALL	Loss of function.	P/CAT	P/CAT	P/CAT	CATASTROPHIC FS 10	Extreme probability of multiple fatalities and hull loss in the case of flame propagation especially in fuel system.

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FLIGHT CONTROLS									
Related MF: FLIGHT CONTROL					Related systems: 22, 24				
System corrective measures: FLIGHT CONTROL SURFACES COMBINATION									
Mitigation means: EMERGENCY PROCEDURES (MM6)									
27	10	Aileron and Tab	ALL	Aileron jam.	CAT	CAT	CAT	CATASTROPHIC FS 10	Extensive increase of force in control mechanism. Increasing airspeed in spiral movement. No Mitigation means.
			ALL	Aileron disengagement.	SIGN	SIGN	SLIGHT	MAJOR FS 5,5	There is high probability, that disengagement occurs only on one side. Crew is able to partially control flight using remaining aileron.
			ALL	Tab spurious extension to the uttermost position. <i>(Tab on both ailerons)</i>	SIGN	SIGN	N/E	MAJOR FS 5,5	There is high probability, that disengagement occurs only on one side. It is possibility to eliminate increase force using remaining tab on other side.
			ALL	Tab spurious extension to the uttermost position. <i>(Tab on one aileron)</i>	SIGN	LARGE	N/E	HAZARDOUS FS 7,5	Extensive increase of force in control mechanism.

ATA 100			CLASSIFICATION KNOWLEDGBASE						Preliminary classification/ Function severity	Note
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on					
					Airplane	Crew	Passengers			
FLIGHT CONTROLS										
27	10	Aileron and Tab	ALL	Tab disengagement.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	It is not possible to control tab position. There is high probability of flutter occurrence (depends on tab aerodynamic balance).	
			ALL	Loss of tab position indication or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	There is no direct safety effect. Crew is able to seek incorrect indication due to aircraft response (force in control mechanism).	
	20	Rudder and Tab	ALL	Jam.	SLIGH	SIGN	N/E	MAJOR FS 4,5	Increasing forces in control mechanism, pedals resistance. It is possible to execute control skidding together with non-symmetric engine thrust (multiengine aircraft).	
			ALL	Disengagement.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Usually, rudder is aerodynamically balanced. The possibility of flutter is minimal (depends on configuration).	
			ALL	Tab jam.	SLIGHT	SLIGHT	N/E	MINOR FS 2	It is possible to compensate effect of jammed rudder tab by control aircraft skidding.	

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FLIGHT CONTROLS									
27	20	Rudder and Tab	ALL	Tab spurious extension .	LARGE	SIGN	N/E	HAZARDOUS FS 7,5	Increasing forces in control mechanism, extensive pedals resistance.
			ALL	Tab disengagement.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	Tab is not controllable. In the case, that tab is not aerodynamically or mass balanced, there is a possibility of flutter occurrence.
			ALL	Loss of tab position indication or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 3	There is no direct safety effect. Crew is able to seek incorrect indication due to aircraft response (force in control mechanism).
			ALL	Loss of tab position indication or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 3	There is no direct safety effect. Crew is able to seek incorrect indication due to aircraft response (force in control mechanism).

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FLIGHT CONTROLS									
27	30	Elevator and Tab	ALL	Jam.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	It not possible to control elevator. Increasing forces in control mechanism.
				Disengagement.	LARGE (extremely P/CAT)	P /CAT	P /CAT	CATASTROPHIC FS 10*	In the case of simple disengagement, the elevator is usually aerodynamically or mass balanced (it stays in neutral positon). *There is a possibility of common disengagement and jam, in worst case scenario, jam of control mechanism occurs.
			ALL	Tab jam.	LARGE	SIGN	N/E	HAZARDOUS FS 7,5	It is not possible to balance the tab. In the case of change of flight mode, forces in control mechanism exceeds maximal limits.

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FLIGHT CONTROLS									
27	30	Elevator and Tab	ALL	One side trim loss of function. (Both sides of elevator are equipped by trim).	SIGN	SIGN	N/E	MAJOR FS 5	It is possible to eradicate negative influence of stuck trim using trim on other side.
			ALL	Tab disengagement.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	It is not possible to control tab position. If the tab is not aerodynamically or mass balanced, high probability of flutter occurrence.
			ALL	Tab spurious extension.	LARGE	SIGN	N/E	HAZARDOUS FS 7,5	Tab is in incorrect position. In the case of change of flight mode, forces in control mechanism could exceeds maximal limits.
			ALL	One-tab spurious extension. (Both sides of elevator are equipped by trim).	SIGN	SIGN	N/E	MAJOR FS 5	It is possible to eradicate negative influence of stuck trim using trim on other side.
			ALL	Loss of tab position indication or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	There is no direct safety effect. Crew is able to seek incorrect indication due to aircraft response (force in control mechanism).

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FLIGHT CONTROLS									
27	40	Horizontal Stabilizers	-	-	-	-	-	-	-
	50	Flaps	LDG	Loss of function.	SLIGHT P/LARGE Short runway	SLIGHT P/SIGN Short runway	N/E	MINOR FS 2 HAZARDOUS FS 7,5 Short runway	Crew is able to increase airspeed and execute landing (with extent length of landing). In the case of short runway and inconvenient airport configuration.
			ICL, ENR, LDG	Asymmetrical extension/retraction.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	It is possible to partially correct effect of asymmetrical flap extension by aileron extension. There is high probability of wing applied force limit.
			ICL, ENR, LDG	Spurious extension/retraction.	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	In the case of high angle of extension, there is high probability of wing applied force limit. Crew reacts to the lift distribution change.
		ALL	Loss of Flaps position indication or misleading indication.	SLIGH	SIGN	N/E	MAJOR FS 4,5	Crew is able to seek the positon of flaps due to aircraft response.	

ATA 100			CLASSIFICATION KNOWLEDGEBASE								
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note		
					Airplane	Crew	Passengers				
FUEL											
Related MF: PROPULSION				Related systems: 24, 72							
System corrective measures: 2 28-30 DISTRIBUTION (CROSS-FEED) (MM1, MM2)											
Mitigation means: EMERGENCY PROCEDURES, 24-10 BATTERY POWER (MM0)											
28	10	Storage	ALL	Leakage.	SIGN	SLIGHT	-	MAJOR FS 4,5			
	20	Distribution	ALL (except TOF, ICL)	Loss of function. (resulting in loss of propulsion).	LARGE	LARGE	SLIGHT	HAZARDOUS FS 8,5	Indicated failure mode. Emergency procedures application, resulting in emergency landing. MM1; MM2 (auxiliary pumps); MM3		
			TOF, ICL		IMC/CAT	P /CAT	P /CAT	Up to CATASTROPHIC FS 10		Extreme probability of emergency landing in inconvenient situation. MM3	
			ALL		Loss of one engine fuel supply. 2	SIGN	N/E	N/E		MAJOR FS 4	Failure mode is notified due caution and warning system. Remedy- engine cross-feed. MM1
			ALL		Loss of cross-feed function.	SLIGHT	N/E	N/E		MINOR FS 1	Under normal situation, there is only possibility of fuel non- symmetric distribution.
	30	Dump	-	-	-	-	-	-	-		

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
FUEL									
28	40	Indicating	ALL	Loss of function.	SLIGHT	N/E	N/E	MINOR FS 1	Standardly, there are multiple indicated parameters of fuel system. Crew is able to monitor system functionality.
				Misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Possible loss of all engines. Flight manual emergency procedures- emergency landing.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
29	HYDRAULIC POWER								
	Related MF: FLIGHT CONTROL, LANDING AIDS				Related systems: 24, 32				
	System corrective measures: CHANNEL CROSS CONNECTION (If it is installed) (MM1), AUXILIARY CHANNEL (MM2)								
	Mitigation means: EMERGENCY PROCEDURES, MECHANICAL BACKUP (Landing gear) (MM0, MM2)								
	10	Main	ALL	Loss of function. (Applied on flight control, landing gear retraction and break) 2	SIGN	SIGN	SLIGHT	MINOR FS 3	Main hydraulic system is usually backed up by axillary system. Crew is able to seek system parameters (pressure, temperature) indication and react. This type of configuration is usually used on commuter type aircrafts.
	20	Auxiliary	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	Auxiliary hydraulic power is used for landing gear break; flaps are operated by main hydraulic system.
40	Indication	ALL	Main system.	SLIGHT	N/E	N/E	MINOR FS 1	It is possible to seek function system function by using flaps or another connected system.	
			Auxiliary system.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ICE AND RAIN PROTECTION									
Related MF: FLIGHT CONTROL					Related systems: 24				
System corrective measures: -									
Mitigation means: EMERGENCY PROCEDURES (MM5, MM6, MM7)									
30	10	Airfoil	ALL	Wing leading edge airfoil deicing system - loss of function.	SLIGHT IMC/P/CAT	SLIGHT IMC/P/CAT	SLIGHT IMC/P/CAT	MINOR FS 3 IMC/P/CAT FS 10	In the case of icing condition, crew urgently change altitude. Aircraft performance is than limited due to failure mode.
			ALL	Wing leading edge airfoil deicing system- loss of function in combination with indication failure.	LARGE	SIGN	SLIGHT	HAZARDOUS FS 7,75	There is high probability of aircraft performance influence in icing condition. Crew is able to visually detect leading icing and change altitude.
			ALL	Tail stabilizations leading edge airfoil deicing system - loss of function.	SLIGHT	SLIGHT	SLIGHT	MINOR FS 3	In the case of icing condition, crew urgently change altitude. Aircraft performance is than limited due to failure mode.
			ALL	Tail stabilizations leading edge airfoil deicing system - loss of function in combination with indication failure.	SIGN	SIGN	SLIGHT	MAJOR FS 5,5	High probability of aircraft performance influence in the case of icing. Crew is not able to detect tail icing. It is possible to determine icing due to aircraft performance change.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ICE AND RAIN PROTECTION									
30	20	Air intakes	-	-	-	-	-	-	-
	30	Pitot and Static	ALL	Pitot-static system heating- loss of function	SIGN	LARGE	SLIGHT	HAZARDOUS FS 7,75	In the case of icing conditions, pitot-static tube is jammed by ice. All aerometric systems are affected. Crew urgently leave icing conditions.
			ALL	Pitot-static system heating- loss of function in combination of indication failure.	LARGE	LARGE	SLIGHT	HAZARDOUS FS 8,5	In the case of icing conditions, pitot-static tube is jammed by ice. All aerometric systems are affected. Crew seek failure mode due to flight response and urgently leave icing conditions.
	40	Windows and Windshields	ALL (except APR, LDG)	Windshield deicing system- loss of function.	SLIGHT	SLIGHT	SLIGHT	MINOR FS 3	In the case of icing condition, crew urgently leave icing conditions.
			APR, LDG	Windshield deicing system- loss of function.	SIGN	SIGN	SLIGHT	MAJOR FS 5,5	In the case of icing condition, crew urgently leave icing conditions. During landing phases crew workload extensively increases.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ICE AND RAIN PROTECTION									
30	50	Antennas and Radome	-	-	-	-	-	-	<i>Mainly not applied in the field of interest.</i>
	60	Propellers	ALL	Propeller leading edge deicing system- loss of function.	SLIGHT P/CAT Icing condition	SLIGHT P/CAT Icing condition	SLIGHT P/CAT Icing condition	MINOR FS 3 P/CAT FS 10 Icing condition	In the case of icing condition, crew urgently leave icing conditions. Failure mode is indicated.
			ALL	Propeller leading edge deicing system- loss of function in combination of indication failure.	SIGN	SIGN	SLIGHT	MAJOR FS 5,5	In the case of icing condition, crew urgently leave icing conditions. Crew is able to seek information of failure mode due to propeller thrust reduction and occurring vibrations.
	70	Water Lines	-	-	-	-	-	-	<i>Mainly not applied in the field of interest.</i>
	80	Detection	ALL	Detection of occurring icing conditions- loss of function	SLIGHT	SLIGHT	SLIGHT	MINOR FS 3	Crew visually detects indication (windows, leading edges).
ALL			Detection of occurring icing conditions- loss of function in combination with loss of indication.	SIGN	SIGN	SLIGHT	MAJOR FS 5,5	Crew is able to seek information of failure mode due to aircraft performance. Crew visually detects indication (windows, leading edges).	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
INDICATING/ RECORDING SYSTEMS									
Related MF: PROPULSION, FLIGHT CONTROL					Related systems: 24, 72, 73, 76				
System corrective measures: -									
Mitigation means: PARTICULAR SYTEM INDICAITON (MM0, MM2), EMERGENCY PROCEDURES									
31	10	Instrument and control panels	-	-	-	-	-	-	<i>Not applied in the field of interest.</i>
	20	Independent instruments	-	-	-	-	-	-	<i>Not relevant to the knowledge base.</i>
	30	Recorders	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECTS FS 0	There is no direct relation to the flight safety.
	40	Central computers	-	-	-	-	-	-	<i>Not applied in the field of interest.</i>
	50	Central warning systems	ALL	<i>Warning indication-loss of function</i>	SLIGHT	SLIGHT	N/E	MINOR FS 2	Classification applicable only in the case of no collateral damage (that supposed to be indicated).
				<i>Warning indication-misleading</i>	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Flight crew has to identify misleading indication. Classification applicable only in the case of no collateral damage (that supposed to be indicated).

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
INDICATING/ RECORDING SYSTEMS									
31	50	Central warning systems	ALL	Caution indication-misleading	SLIGHT	SLIGHT	N/E	MINOR FS 2	Classification applicable only in the case of no collateral damage (that supposed to be indicated).
				Caution indication-loss of function	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Flight crew has to identify misleading indication. Classification applicable only in the case of no collateral damage (that supposed to be indicated).
			ALL	Advisory indication-loss of function	SLIGHT	SLIGHT	N/E	MINOR FS 2	Classification applicable only in the case of no collateral damage (that supposed to be indicated).
				Advisory indication-misleading	SLIGHT	SLIGHT	N/E	MINOR FS 2	Flight crew has to identify misleading indication (notification). Classification applicable only in the case of no collateral damage (that supposed to be indicated).
	60	Central display systems	-	-	-	-	-	-	-
	70	Automatic data reporting	-	-	-	-	-	-	Not applied in the field of interest.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
LANDING GEAR									
Related MF: LANDING AIDS					Related systems:				
System corrective measures: -									
Mitigation means: EMERGENCY PROCEDURES									
32	10	Main Gear and Doors	-	-	-	-	-	-	Not relevant to the doctoral thesis.
	20	Nose Gear and Doors	-	-	-	-	-	-	
	30	Extension and Retraction	LDG	Main extension mean-loss of function. ②	SIGN	SIGN	N/E	MAJOR FS 5	Flight crew is notified about occurring failure and uses back mean of landing gear extension. Significant workload increase.
				Extension – complete loss of function. ②	LARGE	LARGE	LARGE	HAZARDOUS FS 9	Landing gear extension is ensured by redundant mean based on diverse principle (hydraulic/ mechanical). These type of failure leads to the emergency landing on fuselage.
				ALL	Spurious extension. ②	SIGN	SIGN	N/E	MAJOR FS 5

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
LANDING GEAR									
32	30	Extension and Retraction	ICL	Retraction- loss of function. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	If landing gear is locked in the extended position, flight crew could continue flight. Failure affects aerodynamic performance and fuel consumption.
			APR	Spurious retraction. ②	LARGE	LARGE	N/E	HAZARDOUS FS 8	Failure mode is indicated. Flight crew interrupt landing and uses back mean of retraction.
	40	Wheels and Brakes	LDG	Breaking- complete loss of function. ②	LARGE	LARGE	LARGE	HAZARDOUS FS 9	Decoration distance is significantly extended. It could lead to the dangerous outcome in the case of inconvenient runway and situation.
			LDG	Breaking- partial loss of function (one wheel). ②	LARGE	LARGE	LARGE	HAZARDOUS FS 9	Decoration distance is significantly extended. These effect could be compensated by asymmetric reverse thrust and remain brake.
			TOF, LDG	Breaking- spurious complete braking. ②	LARGE	LARGE	LARGE	HAZARDOUS FS 9	It could lead to the serious damage of wheels or flip to the nose gear.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
LANDING GEAR									
32	40	Wheels and Brakes	TOF, LDG	Breaking- spurious partial braking (one wheel). ②	LARGE	LARGE	LARGE	HAZARDOUS FS 9	Failure effect could be compensated by asymmetric reverse thrust and remain brake.
	50	Steering	-	-	-	-	-	-	Not relevant to the doctoral thesis.
	60	Position and Warning	TOF, ICL, APR, LDG	Extended position of landing gear indication-loss of function. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Flight crew is not notified about extended landing gear position. However, landing gear retraction/ extension. functionality is affected.
				Extended position of landing gear indication-misleading. ②	P/CAT	P/CAT	P/CAT	P/ CATASTROPHIC FS 10	Misleading information of landing gear extension possible leads to uncontrolled landing on fuselage. Flight crew could identify failure through the collateral effects.
				Transition position of landing gear indication-loss of function. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Flight crew is not notified about extended landing gear position. However, landing gear transition. functionality is affected.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
LANDING GEAR									
32	60	Position and Warning	TOF, ICL, APR, LDG	Transition position of landing gear indication-misleading. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Flight crew seek information about landing gear position through the retract/ extended position indication.
			TOF, ICL, APR, LDG	Transition position of landing gear indication-loss of function. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	Flight crew is not notified about extended landing gear position. However, landing gear retraction/ extension. functionality is affected.
				Transition position of landing gear indication-misleading. ②	SLIGHT	SLIGHT	N/E	MINOR FS 2	If landing gear is locked in the extended position, flight crew could continue flight. Failure affects aerodynamic performance and fuel consumption.
	70	Supplementary Gear	-	-	-	-	-	-	Not relevant to the doctoral thesis.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
33	LIGHTS								
	Related MF: -				Related systems: 24				
	System corrective measures: EXTERNAL LIGHT								
	Mitigation means: -								
	10	Flight Compartment	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	Pilots are equipped by backup handheld light.
	20	Passenger Compartments	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-
	30	Cargo and Service Compartments	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-
40	Exterior	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	ATC communication, anti-collision systems (TCAS).	
50	Emergency Lighting	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
33	LIGHTS								
	Related MF: -				Related systems: 24				
	System corrective measures: EXTERNAL LIGHT (MM0)								
	Mitigation means: -								
	10	Flight Compartment	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	Pilots are equipped by backup handheld light.
	20	Passenger Compartments	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-
	30	Cargo and Service Compartments	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-
40	Exterior	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	ATC communication, anti-collision systems (TCAS).	
50	Emergency Lighting	ALL	Loss of function.	N/E	N/E	N/E	NO SAFETY EFFECT FS 0	-	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
NAVIGATION									
Related MF: NAVIGATION					Related systems: 24				
System corrective measures: BACKUP AEROMETRIC INDICATORS (MM2)									
Mitigation means: -									
34	10	Flight Environment Data	ALL	Altitude indication- complete loss of information.	SIGN IFR/ CAT	SIGN P /CAT	N/E P /CAT	MAJOR FS 5 IFR/ CATASTROPHIC FS 10	Crew is able to use visual navigation reference. It is possible to partially use GPS altitude information.
			ALL	Altitude indication- Misleading information.	LARGE IFR/ CAT	SIGN P /CAT	N/E P /CAT	HAZARDOUS FS 7,5 IFR/ CATASTROPHIC FS 10	Avionics system is equipped by backup altitude indicator. Flight crew ability to identify misleading information strongly depends on particular situation and magnitude of difference between indication and real state.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
NAVIGATION									
34	10	Flight Environment Data	ALL	Airspeed- complete loss of information.	SIGN IFR/ LARGE	SIGN IFR/ LARGE	N/E	MAJOR FS 5 IFR/ HAZARDOUS FS 8	Crew uses stall- warring system to avoid proximity of stall speed.
			ALL	Airspeed- Misleading information.	SIGN IFR/ LARGE	SIGN IFR/ LARGE	N/E	MAJOR FS 5 IFR/ HAZARDOUS FS 8	Avionics system is equipped by backup altitude indicator. Flight crew ability to identify misleading information strongly depends on particular situation and magnitude of difference between indication and real state.
			ALL	Vertical speed- complete loss of information.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Altitude and airspeed information is still available. There is only slight increase of flight crew workload.
			ALL	Vertical speed- Misleading information.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew is able to identify misleading information due to altitude and airspeed information.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
NAVIGATION									
34	10	Flight Environment Data	TOF, ICL, LDG	Stall speed proximity warning- loss of function. <i>(In combination with stall speed)</i>	CAT	P /CAT	P /CAT	CATASTROPHIC FS 10	Crew is not informed about stall speed proximity. In worst case scenario crew is not able to react in time.
			ALL	Altimeter – complete loss of function or misleading.	SIGN IFR/ LARGE	LARGE IFR/ CAT	N/E P/ CAT	HAZARDOUS FS 7,5 IFR/ CATASTROPHIC FS 10	Loss of all information about altitude. Crew uses visual references.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
NAVIGATION									
34	20	Attitude and Direction	ALL	Magnetic compass-complete loss of function.	SLIGHT	SLIGHT IFR/SIGN	N/E	MINOR FS 2 IFR/ MAJOR FS 4,5	Complete loss of magnetic dereliction. Crew can use visual navigation reference together with ATC communication/ GPS navigation.
			ALL	Magnetic compass-misleading.	SLIGHT	SLIGHT IFR/SIGN	N/E	MINOR FS 2 IFR/ MAJOR FS 4,5	Crew is able to seek correlation using GPS navigation.
			ALL	Attitude indicator-complete loss of function or misleading.	SIGN IFR/ CAT	SIGN P /CAT	N/E P /CAT	MAJOR FS 5 IFR/ CATASTROPHIC FS 10	Crew uses reaming navigation instruments and visual navigation reference to resolve occurring situation.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
34	NAVIGATION								
	20	Attitude and Direction	ALL	Turn and slip indicator- loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses reaming navigation instruments to partially seek required information.
	30	Landing and Taxiing Aids	APR, LDG	Instrument landing system- loss of function.	SIGN IFR/IMC/ CAT	SIGN IFR/ IMC/ CAT	N/E IFR/IMC/ CAT	MAJOR FS 5 IFR/IMC/ CATASTROPHIC FS 10	Flight crew is able to conduct controlled landing without ILS system. In the IMC/ IFR conditions, extremely dangerous situation possible resulting in catastrophic outcome.
				Instrument landing system- misleading.	LARGE IFR/IMC/ CAT	LARGE IFR/IMC/ CAT	N/E IFR/IMC/ CAT	HAZARDOUS FS 8 IFR/IMC/ CATASTROPHIC FS 10	Ability of misleading function identification is minimal. In IMC/ IFR conditions, there is high probability of catastrophic outcome.
	40	Independent Position Determining	ALL	Traffic collision avoidance system- loss of function.	IFR/ SIGN	IFR/ SIGN	N/E	IFR/ MINOR FS 2	Crew visually control air traffic. There is still ATC communications and transponder information.
			ALL	Proximity warning- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew is on high visual alert in terrain proximity.
			ALL	ATC identification- loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses continues flight according to AFM. Crew uses visual references.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
34	50	Dependent Position Determining	NAVIGATION						
			ALL	Distance measuring equipment- loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses reaming to instruments to seek information about proximity to VOR beacon.
			ALL	VHF omnidirectional range- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses reaming to instruments to navigate (DME, GPS, ADF).
			ALL	Automatic direction finder- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses reaming to instruments to navigate (DME, VOR, GPS).
			ALL (except LDG)	Global positioning system- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Crew uses reaming to instruments to navigate (DME, VOR, ADF, ILS). During landing is crew in high alert.
	LDG	Global positioning system- misleading.	SIGN	LARGE	N/E	HAZARDOUS FS 7,5	Crew uses other instruments to seek misleading information and uses secondary GPS.		
-	Selected multiple failure mode	ALL	Complete loss of navigation and communication (GPS, VOR, ADF, DME, VOR).	SIGN IFR/ LARGE	SIGN IFR/ LARGE	N/E	MAJOR FS 5 IFR/ HAZARDOUS FS 8	Crew uses visual reference navigation to continue flight and emergency landing.	

ATA 100			CLASSIFICATION KNOWLEDGBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
46	INFORMATION SYSTEMS								
	Related MF: -				Related systems: 24				
	System corrective measures: -								
	Mitigation means: EMERGENCY PROCEDURES								
	10	Airplane general information systems	-	-	-	-	-	-	-
	20	Flight deck information systems	ALL	Engine data acquisition system-complete loss of function	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Engine functionality is not affected by the failure. Flight crew is able to partially control engine functionality due to other engine indication.
				Engine data acquisition system-multiple indication misleading.	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Engine functionality is not affected by the failure. Flight crew is able to identify indication misleading due to other engine indication and collateral effects.
	30	Maintenance information systems	-	Loss of function or incorrect function.	N/E	N/E	N/E	NO SAFETY EFFECTS FS 0	There is no direct relation to flight operations.
40	Passenger cabin information systems	-	-	-	-	-	-	Mainly not applied in the field of interest.	
50	Miscellaneous information systems	-	-	-	-	-	-	-	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ENGINE CONTROL									
Related MF: PROPULSION					Related systems: 24, 72, 73				
System corrective measures: EMERGENCY SETTING									
Mitigation means: EMERGENCY PROCEDURES									
76	10	Power control	ALL	Single engine power control- loss of function. 2	SIGN	SLIGH	N/E	MAJOR FS 4,5	Standard configuration of engine power control sets engine to the flight idle. Loss of engine control. Crew follows AFM emergency procedure in the case of single engine loss.
			ALL	Engine power control- loss of function.	LARGE	SIGN	N/E	HAZARDOUS FS 7,5	Engine power control systems are separated (it has to result of multiple failures). Standard configuration of both engine power control sets engine to the flight idle. Crew follows flight manual emergency procedure in the case of both engine losses.
	20	Emergency shutdown	ALL	Loss of function	SLIGHT	SLIGH	N/E	MINOR FS 3	Flight crew is able to cut fuel flow to engine by backup fuel valve and shutdown the engine.

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
77	ENGINE INDICATING								
	Related MF: PROPULSION				Related systems: 72				
	System corrective measures: -								
	Mitigation means: COLLATERAL EFFECTS (MM6), EMERGENCY PROCEDURES								
	10	Power	ALL	Tachometer indication - loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Assumes fixed pitch propeller and reciprocating engine; otherwise, a propeller governor will maintain the engine r.p.m. Refer to 14 CFR part 23, § 23.1311. [1]
		ALL	Oil pressure indication - loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Assumed oil pressure is used as back up. [1]	
		ALL	Manifold pressure indication - loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Assumes backup use of CHT, Engine Gas Temperature (EGT), and possible fuel flow readings if installed. [1]	
		ALL	Fuel pressure indication - loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	-	

ATA 100			CLASSIFICATION KNOWLEDGEBASE							
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note	
					Airplane	Crew	Passengers			
ENGINE INDICATING										
77	10	Power	ALL	Power-plant thrust- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2	System is not normally used in field of interest. Torque, Engine Pressure Ratio (EPR), EGT, or Turbine Inlet Temperature (TIT), fuel flow, and RPM are normally displayed. [1]	
				Power-plant thrust indication - misleading.	SIGN	LARGE	N/E	HAZARDOUS FS 7,5		
			ALL	Power-plant torque indication- loss of function.	SLIGHT	SLIGHT	N/E	MINOR FS 2		Misleading torque could affect takeoff. [1]
				Power-plant torque indication- misleading.	SLIGHT	SIGN	N/E	MAJOR FS 4		
	20	Temperature	ALL	Cylinder head temperature indication loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Assumes a CHT indicator is required. Refer to 14 CFR part 23, § 23.1305 [1]	
			ALL	Power-plant coolant temperature indication- loss of function or misleading	SLIGHT	SLIGHT	N/E	MINOR FS 2	Refer to 14 CFR part 23, § 23.1305 [1]	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
ENGINE INDICATING									
577	20	Temperature	ALL	Oil temperature indication- loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	Assumes as oil pressure as back up. [1]
			ALL	Power-plant air inlet temperature- loss of function or misleading.	SLIGHT	SLIGHT	N/E	MINOR FS 2	-
	30	Analyzers	-	-	-	-	-	-	-
	40	Integrated engine instruments systems	ALL	Engine data acquisition system- complete loss of function	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Engine functionality is not affected by the failure. Flight crew is able to partially control engine functionality due to other engine indication.
ALL			Engine data acquisition system- multiple indication misleading.	SLIGHT	SIGN	N/E	MAJOR FS 4,5	Engine functionality is not affected by the failure. Flight crew is able to identify indication misleading due to other engine indication and collateral effects.	

ATA 100			CLASSIFICATION KNOWLEDGEBASE						
System Chapter	Sub-system	Definition	Flight phase	Failure mode	Assumed effect on			Preliminary classification/ Function severity	Note
					Airplane	Crew	Passengers		
STARTING									
Related MF: PROPULSION					Related systems: 24, 72, 73, 76				
System corrective measures: -									
Mitigation means: EMERGENCY PROCEDURES									
80	10	Engine starting*	ALL <i>(except ground phases)</i>	One engine start- loss of function. <i>(Multiple engine aircraft)</i>	SIGN	SLIGHT	N/E	MAJOR FS 4,5	Crew continues flight using remaining engine according to the flight manual emergency procedure.
			ALL <i>(except ground phases)</i>	Both engine start- loss of function. <i>(Multiple engine aircraft)</i>	LARGE	SIGN	N/E	HAZARDOUS FS 7,5	Crew executes emergency landing with significant speed reduction (complete loss of propulsion) according to the flight manual emergency procedure.

* Chapter structure is adjusted for the proposes of doctoral thesis

Appendix B

Basic Items Reliability Data Overview

BASIC ELECTRICAL ITEMS					
Item	Failure mode	Failure rate [hr-1]	Occurrence level	Information source	Note
Circuit breaker	Total failure rate.	2,38.10⁻⁶	REASONABLE PROBABLE	MIL-HDBK-217F Notice 2	Total failure rate was calculated in accordance with MIL-HDBK-217F Notice 2, chapter 14.2 Switches, Circuit Breakers (Magnetic, SPST, not used as a power ON/OFF switch, MILSPEC, AIC). Calculated value was compared with RIAC Databook 3.0.1 (Circuit Breaker)
	Does not open circuit.	1,17.10⁻⁶			Distribution between failure modes was calculated in accordance with MIL-HDBK-338B (Section 7-194-CircuitBreaker: Opens Without Stimuli, Does Not Open).
	Spurious opening.	1,21.10⁻⁶			
Relay	Total failure rate.	1,86.10⁻⁶	OCAASIONAL	RIAC DATABOOK 3.0.1	Total failure mode was taken from RIAC Databook 3.0.1 (Relay)
	Fails to open/ close.	1,02.10⁻⁶	OCAASIONAL	MIL-HDBK-338B	Distribution between failure modes was calculated in accordance with MIL HDBK-338B (Section 7-197-Relay: Fails to Trip, Spurious Trip, and Short).
	Spuriously open/ closes.	4,83.10⁻⁷	REASONABLE PROBABLE		
	Other failure.	3,53.10⁻⁷			
Switch	Total failure rate	2,73.10⁻⁶	OCAASIONAL	RIAC DATABOOK 3.0.1	Total failure mode was taken from RIAC Databook 3.0.1 (Switch, Toggle)
	Fails to open/ close.	8,87.10⁻⁷	REASONABLE PROBABLE	MIL-HDBK-338B	Distribution between failure modes was calculated in accordance with MIL HDBK-338B (Section 7-198-Switch, Toggle: Open, Sticking, and Short).
	Spuriously opens/closes.	5,18.10⁻⁷			
	Short.	4,37.10⁻⁷			

BASIC ELECTRICAL ITEMS					
Item	Failure mode	Failure rate [hr ⁻¹]	Occurrence level	Information source	Note
Contactor	Total failure rate.	1,06.10⁻⁴	FREQUENT	MIL-HDBK-217F Notice 2	Total failure rate was estimated according to database SPIDR (Relay, Contactor)
	Fails to open/ close.	5,83.10⁻⁵	REASONABLE PROBABLE	MIL-HDBK-338B	Distribution between failure modes was calculated in accordance with MIL HDBK-338B (Section 7-197-Relay: Fails to Trip, Spurious Trip, and Short).
	Spuriously opens/closes.	2,65.10⁻⁵			
	Short.	2,01.10⁻⁵			
Ammeter shunt	Total failure rate.	6,72.10⁻⁸	OCAASIONAL		
Current sensor	Total failure rate.	1,86.10⁻⁵	FREQUENT	RIAC DATABOOK 3.0.1	Total failure mode was taken from RIAC Databook 3.0.1 (Sensor, Current)
	Loss of information	Less than 1,86.10 ⁻⁵		RIAC DATABOOK 3.0.1	-
	Incorrect information				
Fuse	Total failure rate.	2,62.10⁻⁶	OCAASIONAL	System and Part Integrated Data (SPIDR, 2006)	Total failure rate was taken from SPIDR, 2006 (Fuse)
	Fuse does not open circuit.	1,28.10 ⁻⁶		MIL-HDBK-338B	Distribution between failure modes was calculated in accordance with MIL HDBK-338B (Section 7-195-Fuse: Fails to open, Slow to open, Premature open).
	Slow to open circuit.	1,26.10 ⁻⁶			
	Spuriously opens circuit.	2,01.10 ⁻⁷			

BASIC ELECTRICAL ITEMS					
Item	Failure mode	Failure rate [hr-1]	Occurrence level	Information source	Note
Slot box	Total failure rate.	4.10^{-9}	EXTREMELY UNLIKELY	System and Part Integrated data (SPIDR, 2006)	Total failure rate was estimated according to database SPIDR (Socket).
Starter/generator	Total failure rate.	$5,9.10^{-4}$	FREQUENT	RAC Automated Databook, NPRD-95	Starter/Generator, Power equipment used in small commercial aircraft (Lukas Aerospace Power Equipment, 1993)
Electric bus	Total failure rate.	1.10^{-8}	REMOTE	MIL-HDBK-338	Failure rate is established using the MIL-HDBK-338 handbook.
V/A meter	Total failure rate.	$8,57.10^{-6}$	OCCASIONAL	MIL-HDBK-217F	MIL-HDBK-217F (Meters; Direct Current; Ammeter; Lower then MIL quality)
	Faulty indication	$4,37.10^{-6}$		MIL-HDBK-338	MIL-HDBK-338 (Meter, Faulty indication, Unable to adjust, Open, No indication).
	No indication	$1,03.10^{-6}$			
	Other.	$3,17.10^{-6}$			
Speaker	Total failure rate.	$1,5.10^{-6}$	OCCASIONAL	RIAC Databook 3.0.1	RIAC Automated Databook (Speaker).
Light indicator	Total failure rate.	$9,2.10^{-5}$	OCCASIONAL	MIL-HDBK-217F	MIL-HDBK-217F (MIL-R-6106, Mechanical Relays, 3PDT, S=0,8, πQ=3, πF=12, AIC)
Motor-Alternating current	Total failure rate.	$4,91.10^{-6}$	OCCASIONAL	SPIDR, 2006	

BASIC ELECTRICAL ITEMS					
Item	Failure mode	Failure rate [hr ⁻¹]	Occurrence level	Information source	Note
Push button	Total failure rate.	8,21.10⁻⁵	OCCASIONAL	MIL-HDBK-217F	MIL-HDBK-217F (Pushbutton, MIL-S-8805; Stress S=1; SPST; Lower quality; AIC)
	Fails to open/ close.	5,25.10 ⁻⁶		MIL-HDBK-338	MIL-HDBK-338 (Section 7-198-PushButton Switch: Sticking, Open) a NPRD-95C (Light Indicator, Quality-MIL, Environment-A)
	Spuriously opens/closes.	2,48.10 ⁻⁶		RIAC Databook 3.0.1	
	Indication fail.	7,26.10 ⁻⁵		MIL-HDBK-338	
	Other.	1,81.10 ⁻⁶			
Conductor	Total failure rate.	7,2.10⁻¹⁰	EXTREMELY UNLIKELY	MIL-HDBK-217F Notice2	MIL-HDBK-217F (Lower quality).
	Open.	7,2.10 ⁻¹⁰			
	Shor circuit.	<i>Significantly lower.</i>			
Antenna	Total failure rate.	<i>Lower than</i> 6,21.10⁻⁶	OCCASIONAL	RIAC Databook 3.0.1	RIAC Automated Databook (Antenna, Marker, Beacon, ILS).
	Loss of function. Faulty input (misleading).			-	Failure rate of partucalr failure cannot exceed total failure rate of item.
Diode	Total failure rate.	9,36.10⁻⁸	REMOTE	MIL-HDBK-217F Notice 2	MIL-HDBK-217F Notice 2, chapter 6-2 Diodes, Low Frequency (Power Rectifier, Junction Temperature =25°C, Stress Vs=1,0 Metallurgically Bonded, JAN, AIC).
	Open in permeable direction.	1,88.10 ⁻⁸		MIL-HDBK-217F Notice 2	MIL-HDBK-338B (Section 7-194-Diode, Rectifier: Short, Open, Parameter Change).
	Open in blocking direction.	7,48.10 ⁻⁸			

BASIC HYDRAULIC ITEMS					
<i>Item</i>	<i>Failure mode</i>	<i>Failure rate [hr-1]</i>	<i>Occurrence level</i>	<i>Information source</i>	<i>Note</i>
Actuator, hydraulic, aileron	Total failure rate.	1,234.10⁻⁵	OCCASIONAL	RIAC Databook 3.0.1	-
Actuator, hydraulic, linear	Total failure rate.	1,33.10⁻⁴	FREQUENT	RIAC Databook 3.0.1	-
Actuator, hydraulic, rotary	Total failure rate.	8,793.10⁻⁵	OCCASIONAL	RIAC Databook 3.0.1	-
Brake, hydraulic	Total failure rate.	1,73.10⁻⁴	FREQUENT	RIAC Databook 3.0.1	-
Accumulator, hydraulic	Total failure rate.	3,77.10⁻⁶	OCCASIONAL	RIAC Databook 3.0.1	-
Amplifier, hydraulic	Total failure rate.	3,778.10⁻⁵	OCCASIONAL	RIAC Databook 3.0.1	-
Valve, hydraulic	Total failure rate.	7,55.10⁻⁶	OCCASIONAL	RIAC Databook 3.0.1	-
Valve, Bypass, hydraulic	Total failure rate.	4,137.10⁻⁵	OCCASIONAL	RIAC Databook 3.0.1	-
<i>Other selected items</i>					
Fire suppression system	Total failure rate.	1,45.10⁻³	FREQUENT	SPIDR, 2006	
Duct, Air	Total failure rate.	5,4.10⁻⁵	OCCASIONAL	SPIDR, 2006	

Appendix C

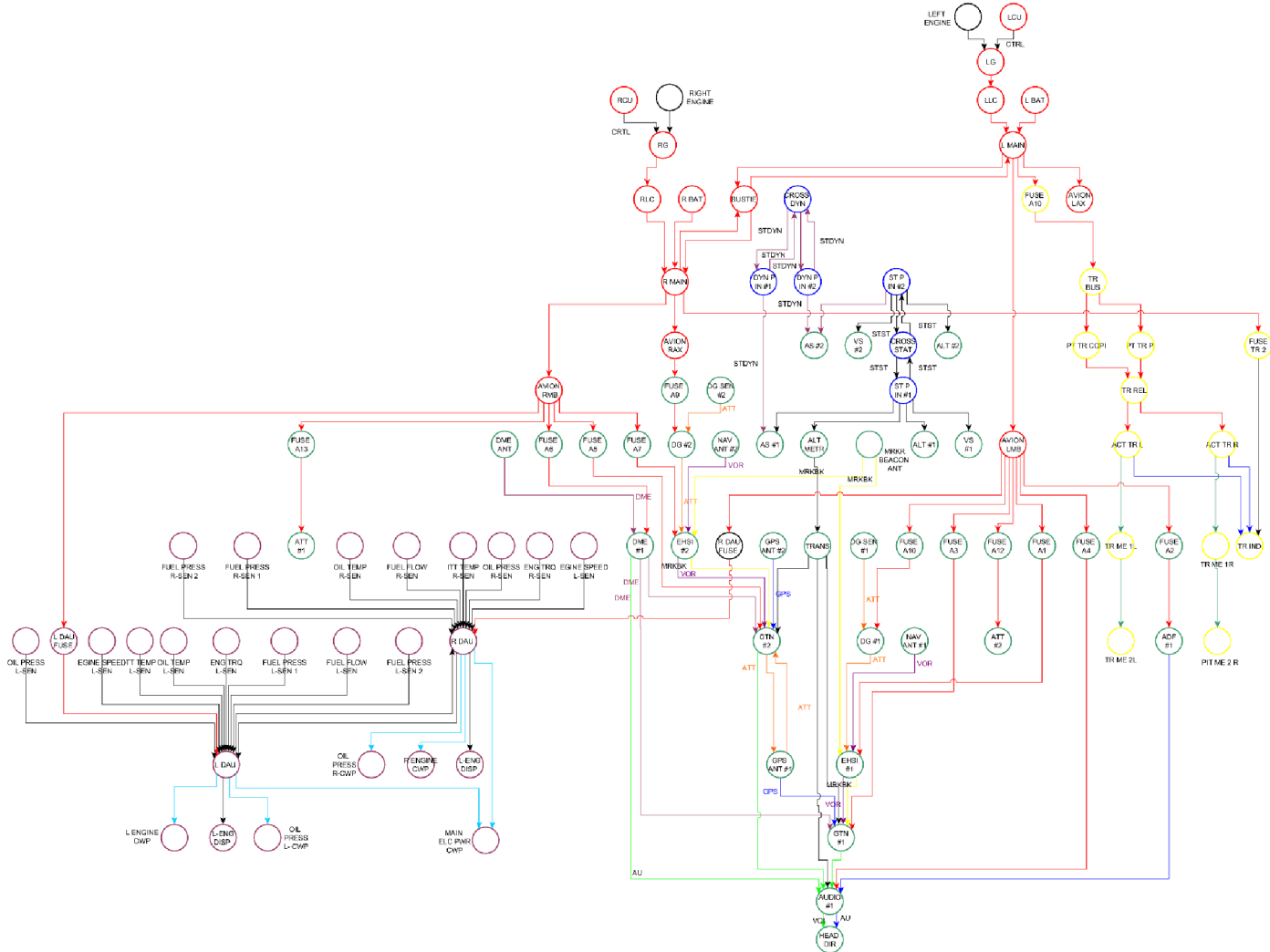
Case Study Evaluation

PREFIXES
REDUNDADNT: There is a redundant connection to the succeeding item. Example R/ ATC PT L (Function of item is back-up by another item)
ACTING ITEM: It is an item, which directly executes function. Example *A/I (Mechanical interconnection converting energy to the trim surface movement).

0. Global model

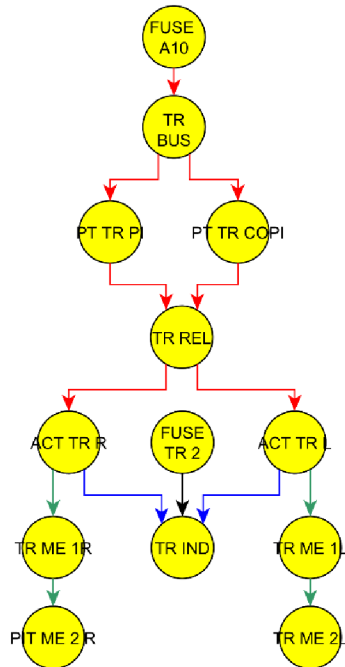
CASE STUDY				
<i>Aircraft: VUT 486-DX4 System: Global</i>				
<i>Number of nodes</i>	102	<i>Diameter</i>	12	
<i>Number of edges</i>	132	<i>Multi edges node pairs</i>	11	
<i>Average number of neighbors</i>	2,37	<i>Shortest paths</i>	1193 (11%)	
<i>Clustering coefficient</i>	0,015	<i>Zones</i>	110, 220, 230, 310, 331, 341, 410, 510, 610, 720, 730	
<i>Most critical items (Global)</i>	<i>Name</i>	<i>Extended criticality</i>	<i>Name</i>	<i>Extended criticality</i>
	LLC (ELEC)	5,000815662	L MAIN (ELEC)	4,252264671
	RLC (ELEC)	5,000815662	R MAIN (ELEC)	4,252264671
	FUSE A10 (TRIM)	5,000815662	GTN #2 (AVIO)	4,181228147
	TR REL (TRIM)	5,000815662	R DAU (ENGIND)	4,151774628
	EHSI #2 (AVIO)	4,375413348	L DAU (ENGIND)	4,151774628
	EHSI #1 (AVIO)	4,350370057	GTN #1 (AVIO)	4,108015073
	TR BUS (TRIM)	4,311464805	AS #1 (AVIO)	4,008398077
<i>Name</i>	<i>Local importance (SubG)</i>	<i>Name</i>	<i>Global importance (BC)</i>	
R DAU (ENGIND)	24,95	L MAIN (ELEC)	0,0436	
L DAU (ENGIND)	24,77	R MAIN (ELEC)	0,0365	
GTN #1 (AVIO)	16,21	BUSTIE (ELEC)	0,0238	
GTN #2 (AVIO)	16,19	AVION LMB (ELEC)	0,0226	
AUDIO #1 (AVIO)	15,92	AVION RMB (ELEC)	0,0186	
DME #1 (AVIO)	10,69	R DAU (ENGIND)	0,0181	
AVION LMB (ELEC)	9,67	L DAU (ENGIND)	0,0181	
TRANS (AVIO)	9,37	LLC (ELEC)	0,0160	
L MAIN (ELEC)	6,60	RLC (ELEC)	0,0160	
AVION RMB (ELEC)	6,59	FUSE A10 (TRIM)	0,0129	

CASE STUDY Aircraft: VUT 486-DX4 System: Global



1. Elevator trim (full version)

CASE STUDY			
<i>Aircraft: VUT 486-DX4 System: Elevator Trim</i>			
GENERAL PARAMETERS			
Type	Electro/ mechanical		
Allocated functions	Analysis ID/ Name / ATA 100	Preliminary classification/ Function Severity	
	ET1 PITCH TRIM L (27-30a)	MAJOR FS 5 (Loss of function)	
	ET2 PITCH TRIM R (27-30b)	MAJOR FS 5 (Loss of function)	
	ET3 PITCH TRIM IND (27-30c)	MINOR FS 2,5 (Loss of function)	
	COMBINATORY PITCH TRIM L/R	HAZARDOUS FS 7,5	
Related operational modes	FLIGHT MODE		
Intersystem succeeding connections	-		
Intersystem preceding connections	L MAIN (ET1, ET2) R MAIN (ET3)		
Number of nodes	13	Diameter	6
Number of edges	14	Multi edges node pairs	0
Average number of nodes	2,15	Shortest paths (global)	53 (33%)
Clustering coefficient	0,0	Zones	230, 331, 341
Most critical items (Global)	Name	Extended criticality	Global Extended criticality Position
	TR REL	5,000817	1
	FUSE A10	5,000817	1
	TR BUS	4,311464	7
	ACT TR R	2,804614	23
Name	Local importance (SubG)	Name	Global importance (BC)
TR REL	4,37	FUSE A10	0,0126
ACT TR R	3,39	TR BUS	0,0105
ACT TR L	3,39	TR REL	0,0053
TR IND	3,33	PT TR COPI	0,0053



CASE STUDY <i>Aircraft: VUT 486-DX4 System: Elevator trim</i>							
SYSTEM PARAMETERS							
<i>Separation/ segregation</i>		<i>Diversity/ redundancy</i>		<i>Complexity/ design/ maturity/ experience</i>		<i>Environmental control/ testing</i>	
Q1	RATHER NO/ 3	Q1	NO/0	Q1	NO/0	Q1	RATHER YES/2,8
Q2	NO/ 0	Q2	NO/0	Q2	YES/4	Q2	RATHER YES/2,8
Q3	NO/ 0	Q3	NO/0	Q3	YES/4	Q3	YES/ 3,6
Q4	YES/ 3,8	Q4	RATHER NO/3,5	Q4	YES/4	Q4	RATHER YES/2,3
-	-	-	-	-	-	Q5	RATHER NO/1,8
-	-	-	-	-	-	Q6	RATHER YES/2,6
Score. 0,775 Level. HIGH SEGREGATION/ SEP.		Score. 0,0967 Level. LOW DEVERSITY		Score. 0,0967 Level. LOW COMPLEXITY		Score. 0,653 Level. HIGH ENVIROMENTAL PROT.	

<p>CASE STUDY Aircraft: VUT 486-DX4 System: Elevator trim</p>		
<p>ALLOCATED FUNCTION PITCH TRIM L 27-30a</p>		
	<p>TOP: $2,45.10^{-5}$ CLASSIFICATION: MAJOR RESULT: OUTSIDE RANGE LIMITATION: Elevator Trim System</p> <p><i>Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</i></p>	<p>ITEM LIST</p> <p>PIT ME 2L: 1.10^{-9} (Loss of function) PIT ME 1L: 1.10^{-9} (Loss of function) ACT TR L: 2.10^{-5} (Complete failure) TR REL: $1,86.10^{-6}$ (Complete failure) TR BUS: $2,5.10^{-7}$ (Loss of function) FUSE A10: $2,38.10^{-6}$ (Spurious open) PT TR PI: $2,73.10^{-6}$ (Complete failure) PT TR COPI: $2,73.10^{-6}$ (Complete failure)</p>

CASE STUDY Aircraft: VUT 486-DX4 System: Elevator trim		
ALLOCATED FUNCTION PITCH TRIM R 27-30b		
	<p>TOP: $2,45.10^{-5}$</p> <p>CLASSIFICATION: MAJOR</p> <p>RESULT: OUTSIDE RANGE</p> <p>LIMITATION: Elevator Trim System</p> <p><i>Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</i></p>	<p>ITEM LIST</p> <p>PIT ME 2R: 1.10^{-9} (Loss of function)</p> <p>PIT ME 1R: 1.10^{-9} (Loss of function)</p> <p>ACT TR R: 2.10^{-5} (Complete failure)</p> <p>TR REL: $1,86.10^{-6}$ (Complete failure)</p> <p>TR BUS: $2,5.10^{-7}$ (Loss of function)</p> <p>FUSE A10: $2,38.10^{-6}$ (Spurious open)</p> <p>PT TR PI: $2,73.10^{-6}$ (Complete failure)</p> <p>PT TR COPI: $2,73.10^{-6}$ (Complete failure)</p>

<p>CASE STUDY <i>Aircraft: VUT 486-DX4 System: Elevator trim</i></p>		
<p>ALLOCATED FUNCTION</p>		
<p>PITCH TRIM IND 27-30c</p>		
	<p>TOP: 2,41.10⁻⁶ CLASSIFICATION: MINOR RESULT: IN RANGE LIMITATION: Elevator Trim System</p> <p><i>Note: TOP event is defined as complete loss of elevator trim indication. Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out</i></p>	<p>ITEM LIST</p> <p>TR IND: 3.10⁻⁸ (Complete failure) ACT TR L: 2.10⁻⁵ (Complete failure) ACT TR R: 2.10⁻⁵ (Complete failure) FUSE TR 2: 2,38.10⁻⁶ (Spurious open)</p>

CASE STUDY				
<i>Aircraft: VUT 486-DX4 System: Elevator trim</i>				
Item	Connectivity			
	<i>Preceding items</i>	<i>Succeeding influence on items</i>	<i>Direct Succeeding influence on function</i>	<i>Preliminary classification/ Function Severity</i>
TR1 <i>(Fuse)</i>	L MAIN	BUS, PT TR PI, PT TR COPI, RELE TR, ATC PIT L, ME 1L, ME 2L	PITCH TRIM L 27-30	MAJOR/ 5
		BUS, PT TR PI, PT TR COPI, RELE TR, ATC PIT R, ME 1R, ME 2R	PITCH TRIM R 27-30	MAJOR/ 5
		<i>Failure combination</i>	COMPLEX TRIM JAM 27-30	HAZARDOUS/ 7,5
		BUS, PT TR PI, PT TR COPI, RELE TR, ATC PIT L, ATC PIT R, TR IND	PITCH TRIM IND	MINOR/ 2
TR BUS	L MAIN, TRI	PT TR PI, PT TR COPI, RELE TR, ATC PIT L, ME 1L, ME 2L	PITCH TRIM L 27-30	MAJOR/ 5
		BUS, PT TR PI, PT TR COPI, RELE TR, ATC PIT R, ME 1R, ME 2R	PITCH TRIM R 27-30	MAJOR/ 5
		<i>Failure combination</i>	COMPLE TRIM JAM 27-30	HAZARDOUS/ 7,5
		PT TR PI, PT TR COPI, RELE TR, ATC PIT L, ATC PIT R, TR IND	PITCH TRIM IND 27-30	MINOR/ 2
PT TR PI	BUS	R/ RELE TR	-	MAJOR/ 5
PT TR COPI	BUS	R/ RELE TR	-	MAJOR/ 5
TRR <i>(Relay)</i>	BUS	ACT PT L, ME 1L, ME L2	PITCH TRIM L 27-30	MAJOR/ 5
		ACT PT R, ME 1R, ME R2	PITCH TRIM R 27-30	MAJOR/ 5
		<i>Failure combination</i>	COMPLE TRIM JAM 27-30	HAZARDOUS/ 7,5
		ACT PT L, ACT PT R, TR IND	PITCH TRIM IND	MINOR/ 2

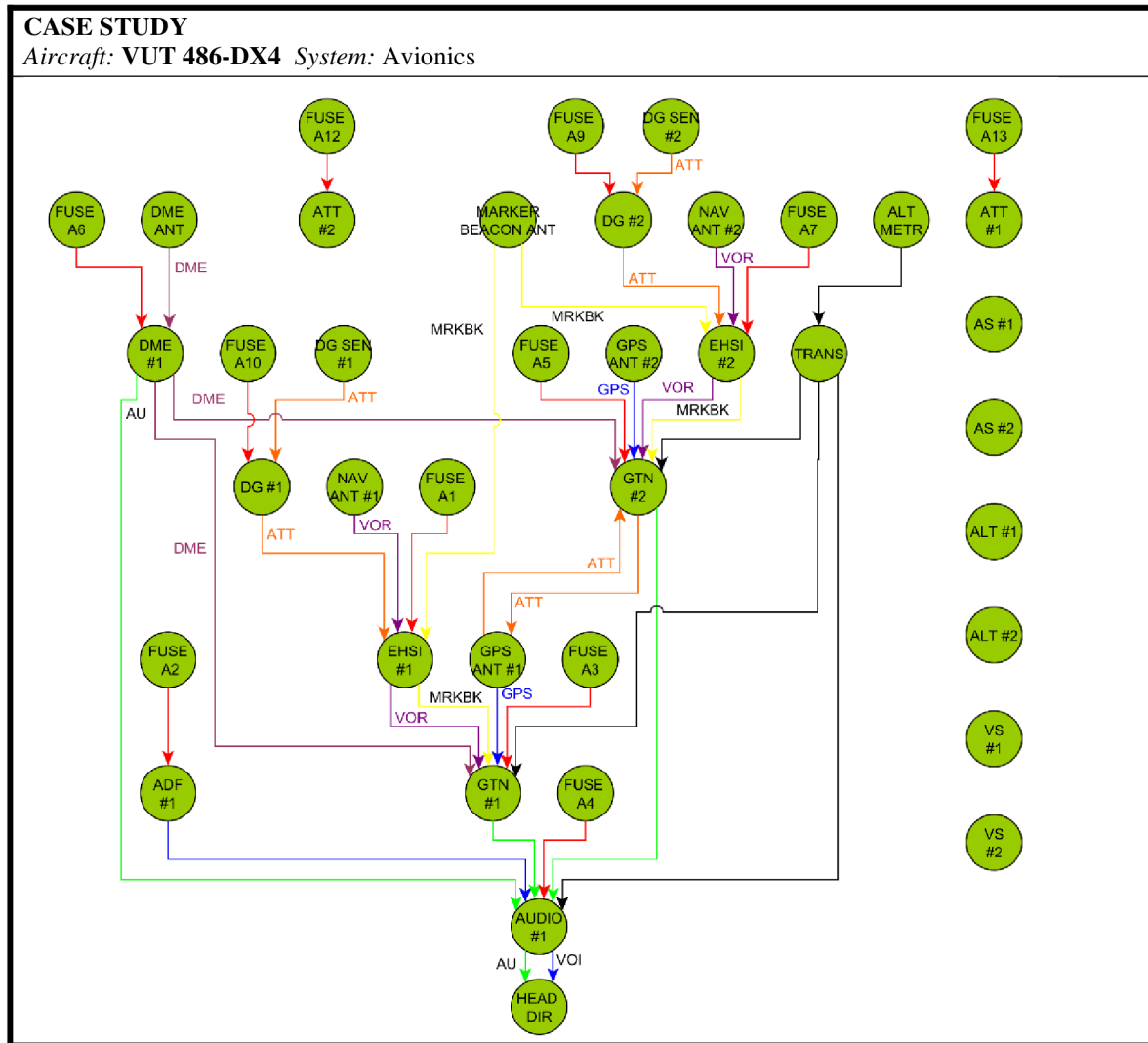
CASE STUDY				
<i>Aircraft: VUT 486-DX4 System: Elevator trim</i>				
Item	Connectivity			
	<i>Preceding items</i>	<i>Succeeding influence on items</i>	<i>Direct Succeeding influence on function</i>	<i>Preliminary classification/ Function Severity</i>
ACT PT L	TRR	PT 2L, ME 2L	PITCH TRIM L 27-30	MAJOR/ 5
		TR IND	PITCH IND 27-30	MINOR/ 2
ACT PT R	TRR	PT 2R, ME 2R	PITCH TRIM R 27-30	MAJOR/ 5
		TR IND	PITCH IND R	MAJOR/ 5
ME 1L	ACT PT L	ME 2L	PITCH TRIM L 27-30	MAJOR/ 5
ME 2L	ME 1L	*A/I	PITCH TRIM L 27-30	MAJOR/ 5
ME 1R	ACT PT R	ME 2R	PITCH TRIM R 27-30	MAJOR/ 5
ME 2R	ME 1R	*A/I	PITCH TRIM R 27-30	MAJOR/ 5
TR IND	ACT PT L, ACT PT R	*A/I	PITCH IND	MINOR/ 2

CASE STUDY									
<i>Aircraft: VUT 486-DX4 System: Elevator trim</i>									
<i>Item</i>	<i>Zone</i>	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
		<i>Node topology parameter</i>	<i>High- level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
TR REL <i>Relay</i>	230	40,90	7,50	1,86E-06	5,5	5,00081566	0,0105	4,37	7
FUSE A10	230	40,90	7,50	2,38E-06	7,0	5,00081566	0,0129	2,58	11
TR BUS <i>Busbar</i>	230	42,15	7,50	2,50E-07	6,5	4,3114648	0,0126	3,21	10
ACT TR L <i>Actuator</i>	331	14,96	5,00	2,00E-05	5,5	2,80461382	0,0038	3,39	3
ACT TR R <i>Actuator</i>	341	14,96	5,00	2,00E-05	5,5	2,80461382	0,0038	3,39	3
TR ME 1L <i>Mechanical part</i>	331	8,80	5,00	1,00E-09	6,0	2,42168675	0,0019	2,29	1
TR ME 1R <i>Mechanical part</i>	341	8,80	5,00	1,00E-09	6,0	2,42168675	0,0019	2,30	1
TR ME 2L <i>Mechanical part</i>	332	4,25	5,00	1,00E-09	6,0	2,42168675	0,0000	1,59	0
TR ME 2R <i>Mechanical part</i>	342	4,25	5,00	1,00E-09	6,0	2,42168675	0,0000	1,59	0
FUSE TR 2	230	4,44	2,50	2,38E-06	7,0	2,13888889	0,0013	2,58	1
PT TR COPI <i>Switch</i>	230	8,52	2,50	2,73E-06	5,5	2,13888889	0,0053	2,58	8
PT TR PI <i>Switch</i>	230	8,52	2,50	2,73E-06	5,5	2,13888889	0,0053	2,58	8
TR IND <i>Diode</i>	230	4,45	2,50	3,00E-08	7,0	2,13888889	0,0000	3,33	0

2. Avionics system (semi-full version)

CASE STUDY		
<i>Aircraft: VUT 486-DX4 System: Avionics</i>		
GENERAL PARAMETERS		
Type	Electro/ mechanical	
Allocated functions	Analysis ID/ Name / ATA 100	Preliminary classification/ Function Severity
	AV1 VERTICAL SPEED 34-10	MINOR FS 2 (Loss of function)
	AV2 ALTITUDE INDICATION 34-10	HAZARDOUS FS 8 (Loss of function) IFR/ CATASTROPHIC FS 10 (Loss of function)
	AV3 DISTANCE MEASURE 34-50	MINOR FS 2 (Loss of function)
	AV4 VOR/ LOC 34-50	MINOR FS 2 (Loss of function)
	AV5 GPS 34-50	MINOR FS 2 (Loss of function)
	AV6 ATTITUDE INFORMATION 34-20	HAZARDOUS FS 8 (Loss of function) IFR/ CATASTROPHIC FS 10 (Loss of function)
	AV7 MARKER BEACON 34-50	MINOR FS 2 (Loss of function)
	AV8 ADF 34-50	MINOR FS 2 (Loss of function)
	AV9 AIRSPEED INDICATION 34-10	MAJOR FS 5 (Loss of function) IFR/ HAZARDOUS FS 8 (Loss of function)
	AV10 AUDIO	MINOR FS 2 (Loss of function)
Related operational modes	FLIGHT MODE	
Intersystem succeeding connections	-	
Intersystem preceding connections	AVION LMB (AV3, AV4, AV5, AV6, AV7, AV10) AVION LMB (AV4, AV5, AV7, AV10) AVION RAX (AV6)	

CASE STUDY			
<i>Aircraft: VUT 486-DX4 System: Avionics</i>			
<i>Number of nodes</i>	39	<i>Diameter</i>	5
<i>Number of edges</i>	40	<i>Multi edges node pairs</i>	4
<i>Average number of neighbors</i>	1,846	<i>Shortest paths</i>	130 (8%)
<i>Clustering coefficient</i>	0,012	<i>Zones</i>	230, 110, 510, 610, 310
<i>Most critical items (Global)</i>	<i>Name</i>	<i>Extended criticality</i>	<i>Global position</i>
	EHSI #2	4,375413348	5
	EHSI #1	4,350370057	6
	GTN #2	4,181228147	10
	GTN #1	4,108015073	13
<i>Name</i>	<i>Local importance (SubG)</i>	<i>Name</i>	<i>Global importance (BC)</i>
GTN #1	16,21	AUDIO #1	0,0046
GTN #2	16,19	GTN #2	0,0038
AUDIO #1	15,92	GTN #1	0,0032
DME #1	10,69	EHSI #2	0,0026



CASE STUDY <i>Aircraft: VUT 486-DX4 System: Avionics</i>							
SYSTEM PARAMETERS							
<i>Separation/ segregation</i>		<i>Diversity/ redundancy</i>		<i>Complexity/ design/ maturity/ experience</i>		<i>Environmental control/ testing</i>	
Q1	RATHER NO/ 1,5	Q1	YES/4	Q1	YES/4	Q1	RATHER YES/2,8
Q2	YES/4	Q2	RATHER YES/ 2,6	Q2	YES/4	Q2	RATHER YES/ 2,9
Q3	RATHER YES/ 2,6	Q3	RATHER YES/ 2,4	Q3	RATHER YES/2,8	Q3	YES/3,6
Q4	YES/ 3,8	Q4	NO/0	Q4	RATHER NO/ 1,3	Q4	RATHER YES/2,9
-	-					Q5	YES/3,2
-	-	-	-	-	-	Q6	RATHER YES/2,9
Score. 0,901 Level VERY HIGH SEGREGATION/ SEP.		Score. 0,633 Level. HIGH DIVERSITY		Score. 0,903 Level. VERY HIGH COMPLEXITY		Score. 0,743 Level. HIGH ENVIROMENTAL PROT.	

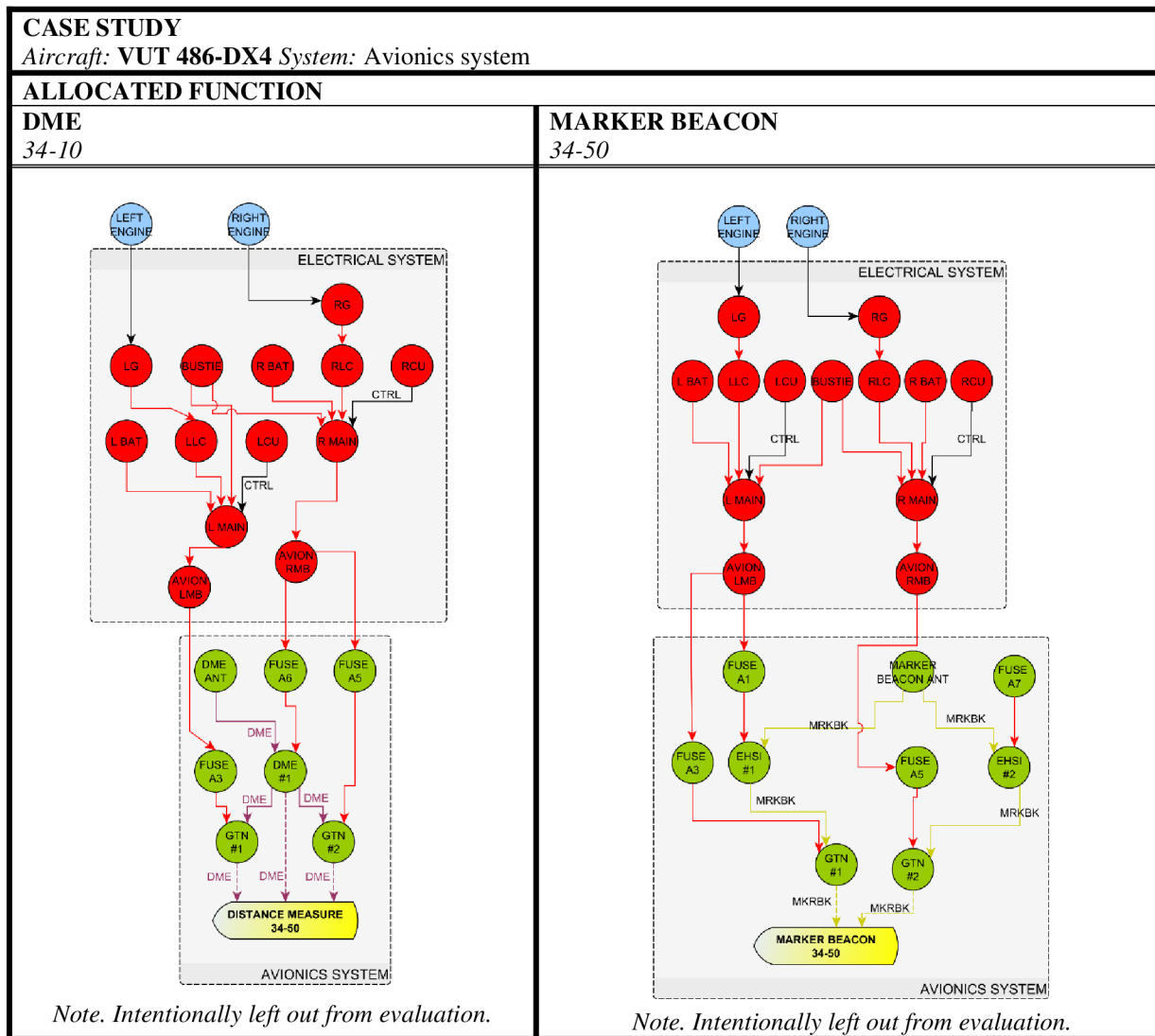
CASE STUDY Aircraft: VUT 486-DX4 System: Avionics system			
ALLOCATED FUNCTION AUTOMATIC DIRECTION FINDER 34-50		AIRSPEED INDICATION 34-10	
	<p>TOP: $1,94.10^{-5}$ CLASSIFICATION: MINOR RESULT: IN RANGE LIMITATION: Electrical system <i>Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</i></p>		<p>TOP: $6,59.10^{-9}$ CLASSIFICATION: IFR/HAZ RESULT: IN RANGE LIMITATION: Electrical system <i>Note: Probability of TOP event occurrence is estimated only on the system level. Pitot-static system is left out.</i></p>
	<p>ITEM LIST</p> <p>ADF #1: $1,7.10^{-5}$ (Complete failure) FUSE A2: $2,38.10^{-6}$ (Complete failure)</p>		<p>ITEM LIST</p> <p>AS#1: $8,12.10^{-5}$ (Complete failure) AS#2: $8,12.10^{-5}$ (Complete failure)</p>

CASE STUDY					
Aircraft: VUT 486-DX4 System: Avionics system					
ALLOCATED FUNCTION					
VERTICAL SPEED 34-10		ALTITUDE INDICATION 34-10			
		<p>TOP: $1,08.10^{-8}$ CLASSIFICATION: MINOR RESULT: IN RANGE LIMITATION: Electrical system <i>Note: Probability of TOP event occurrence is estimated only on the system level. Pitot-static system is left out.</i></p>			
<p>ITEM LIST</p> <p>VS#1: $1,04.10^{-4}$ (Complete failure) VS#2: $1,04.10^{-4}$ (Complete failure)</p>				<p>TOP: $6,92.10^{-10}$ CLASSIFICATION: IFR/CAT RESULT: IN RANGE LIMITATION: Electrical system <i>Note: Probability of TOP event occurrence is estimated only on the system level. Pitot-static system is left out.</i></p>	
<p>ITEM LIST</p> <p>ALT#1: $2,63.10^{-5}$ (Complete failure) ALT#2: $2,63.10^{-5}$ (Complete failure)</p>		<p>ITEM LIST</p> <p>ALT#1: $2,63.10^{-5}$ (Complete failure) ALT#2: $2,63.10^{-5}$ (Complete failure)</p>			

<p>CASE STUDY Aircraft: VUT 486-DX4 System: Avionics system</p>		
<p>ALLOCATED FUNCTION</p>		
<p>GPS 34-50</p>		
	<p>TOP: $2,54.10^{-9}$ CLASSIFICATION: MINOR RESULT: IN RANGE LIMITATION: Electrical system Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</p>	<p>ITEM LIST</p> <p>GTN #1: $4,58.10^{-5}$ (Complete failure) GTN #2: $4,58.10^{-5}$ (Complete failure) GPS ANT #1: $2,26.10^{-6}$ (Complete failure) GPS ANT #2: $2,26.10^{-6}$ (Complete failure) FUSE A3: $2,38.10^{-6}$ (Complete failure) FUSE A5: $2,38.10^{-6}$ (Complete failure)</p>

<p>CASE STUDY <i>Aircraft: VUT 486-DX4 System: Avionics system</i></p>		
<p>ALLOCATED FUNCTION VOR/LOC 34-10</p>		
	<p>TOP: $1,36.10^{-7}$ CLASSIFICATION: MINOR RESULT: IN RANGE</p> <p>LIMITATION: Electrical system <i>Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</i></p>	<p>ITEM LIST</p> <ul style="list-style-type: none"> GTN#1: $4,58.10^{-5}$ (Complete failure) GTN#2: $4,58.10^{-5}$ (Complete failure) FUSE A3: $2,38.10^{-6}$ (Complete failure) FUSE A5: $2,38.10^{-6}$ (Complete failure) EHSI #1: 3.10^{-4} (Complete failure) EHSI #2: 3.10^{-4} (Complete failure) FUSE A1: $2,38.10^{-6}$ (Complete failure) FUSE A7: $2,38.10^{-6}$ (Complete failure) NAV ANT #1: $1,73.10^{-5}$ (Complete failure) NAV ANT #2: $1,73.10^{-5}$ (Complete failure) FUSE A9: $2,38.10^{-6}$ (Complete failure)

<p>CASE STUDY Aircraft: VUT 486-DX4 System: Avionics system</p>		
<p>ALLOCATED FUNCTION ATTITUDE INFORMATION 34-20</p>		
	<p>TOP: $1,41.10^{-18}$ CLASSIFICATION: IFR/CAT RESULT: IN RANGE</p> <p>LIMITATION: Electrical system Note: Probability of TOP event occurrence is estimated only on the system level. Electrical system is left out.</p>	<p>ITEM LIST</p> <p>ATT#1: $1,36.10^{-6}$ (Complete failure) ATT#2: $1,36.10^{-6}$ (Complete failure) EHSI #1: 3.10^{-4} (Complete failure) EHSI #2: 3.10^{-4} (Complete failure) FUSE A1: $2,38.10^{-6}$ (Complete failure) FUSE A7: $2,38.10^{-6}$ (Complete failure) DG #1: $5,28.10^{-4}$ (Complete failure) DG #2: $5,28.10^{-4}$ (Complete failure) FUSE A9: $2,38.10^{-6}$ (Complete failure) FUSE A10: $2,38.10^{-6}$ (Complete failure) DG SEN#1: $3,93.10^{-5}$ (Complete failure) DG SEN#2: $3,93.10^{-5}$ (Complete failure)</p>



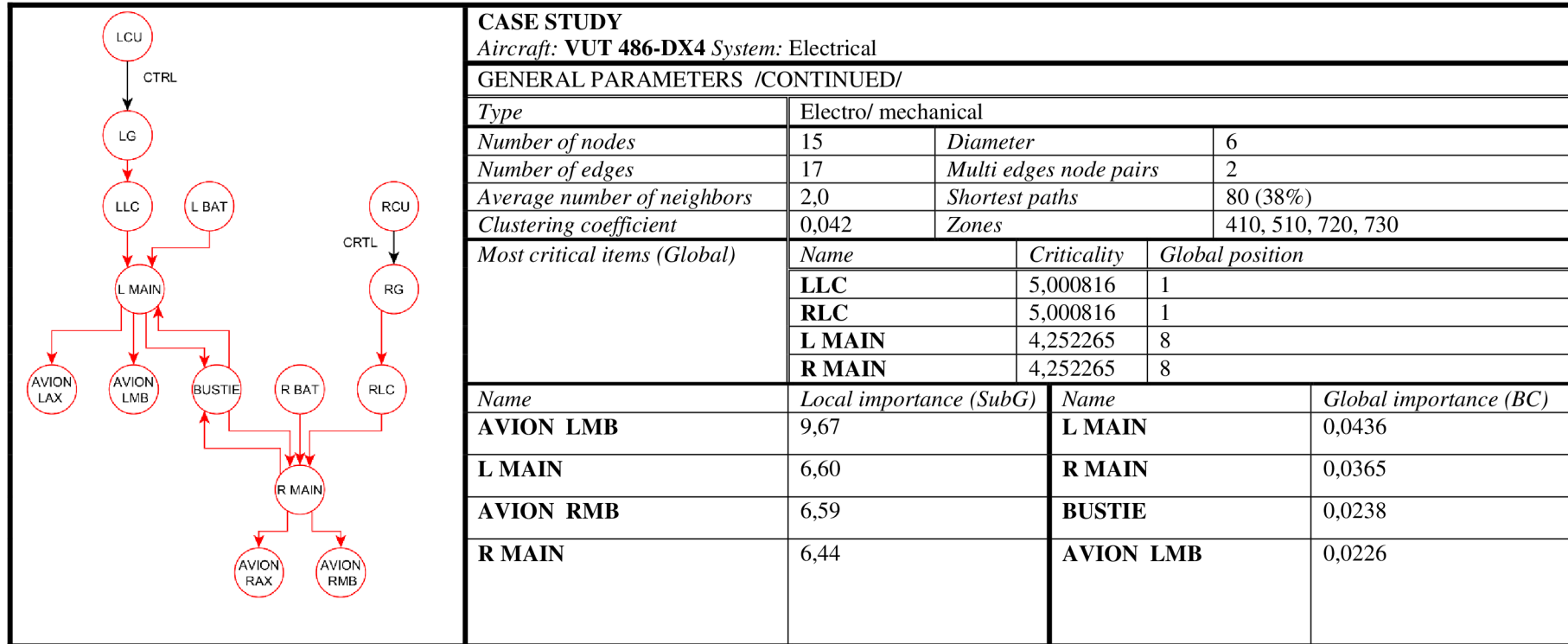
CASE STUDY <i>Aircraft: VUT 486-DX4 System: Avionics system</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High- level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
GTN #1 <i>Integrated avionics unit</i>	46,06	4,75	4,58E-05	2,0	4,10801507	0,0032	16,21	3
GTN #2 <i>Integrated avionics unit</i>	46,71	4,75	4,58E-05	2,0	4,18122815	0,0038	16,19	3
TRANS	23,11	4,00	3,73E-06	7,5	3,06133238	0,0016	9,37	4
AUDIO #1 <i>Audio panel</i>	19,31	2,00	1,24E-05	5,0	2,06071952	0,0046	15,92	1
EHSI #1 <i>Electronic Flight Instrument System</i>	18,00	4,50	3,00E-04	3,5	4,35037006	0,0022	5,79	4
EHSI #2 <i>Electronic Flight Instrument System</i>	18,32	4,50	3,00E-04	3,5	4,37541335	0,0026	5,75	4
DME #1	13,09	2,00	4,09E-06	3,0	0,90185185	0,0018	10,69	4
FUSE A3	12,56	5,00	2,38E-06	8,0	2,42168675	0,0015	3,30	4
FUSE A5	11,26	4,50	2,38E-06	8,0	2,42168675	0,0018	3,13	4
FUSE A1	9,56	4,00	2,38E-06	8,0	2,42168675	0,0014	2,92	5
FUSE A7	9,18	4,00	2,38E-06	8,0	2,42168675	0,0014	2,75	5
FUSE A2	8,31	4,00	2,38E-06	8,0	2,42168675	0,0014	2,72	3
ALT METR	9,19	4,00	2,63E-05	7,5	3,00937974	0,0015	2,71	5

CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Avionics system</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High- level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
AS #1 <i>Airspeed indicator</i>	5,24	4,00	8,12E-05	6,0	4,008398077	0,0000	2,45	0
AS #2 <i>Airspeed indicator</i>	5,09	4,00	8,12E-05	6,0	4,008398077	0,0000	2,38	0
NAV ANT #1	5,83	4,00	1,73E-05	3,0	2,708872491	0,0000	1,77	5
NAV ANT #2 <i>Antenna</i>	5,83	4,00	1,73E-05	3,0	2,708872491	0,0000	1,77	5
ALT #1 <i>Altitude indicator</i>	3,74	4,00	1,73E-06	6,0	2,421686747	0,0000	1,75	0
ALT #2 <i>Altitude indicator</i>	3,61	4,00	2,63E-05	6,0	3,009379744	0,0000	1,69	0
FUSE A4	4,65	2,00	2,38E-06	8,0	0,901851852	0,0016	3,29	2
FUSE A6	5,22	2,00	2,38E-06	8,0	0,901851852	0,0024	2,89	5
ADF #1	3,56	2,00	1,70E-05	3,5	0,901851852	0,0002	2,86	2
MR, BEAC ANT <i>Antenna</i>	4,11	2,00	1,73E-05	3,0	0,901851852	0,0000	2,70	6
HEAD DIR <i>Headset</i>	2,24	2,00	1,25E-05	2,0	0,901851852	0,0000	2,10	0
DME ANT <i>Antenna</i>	3,05	2,00	1,73E-05	3,0	0,901851852	0,0000	1,90	5
DG #1 <i>Direction gyro</i>	2,48	1,00	3,93E-05	6,5	0,901851852	0,0010	3,27	5
DG #2 <i>Direction gyro</i>	2,57	1,00	3,93E-05	6,5	0,901851852	0,0015	3,23	5

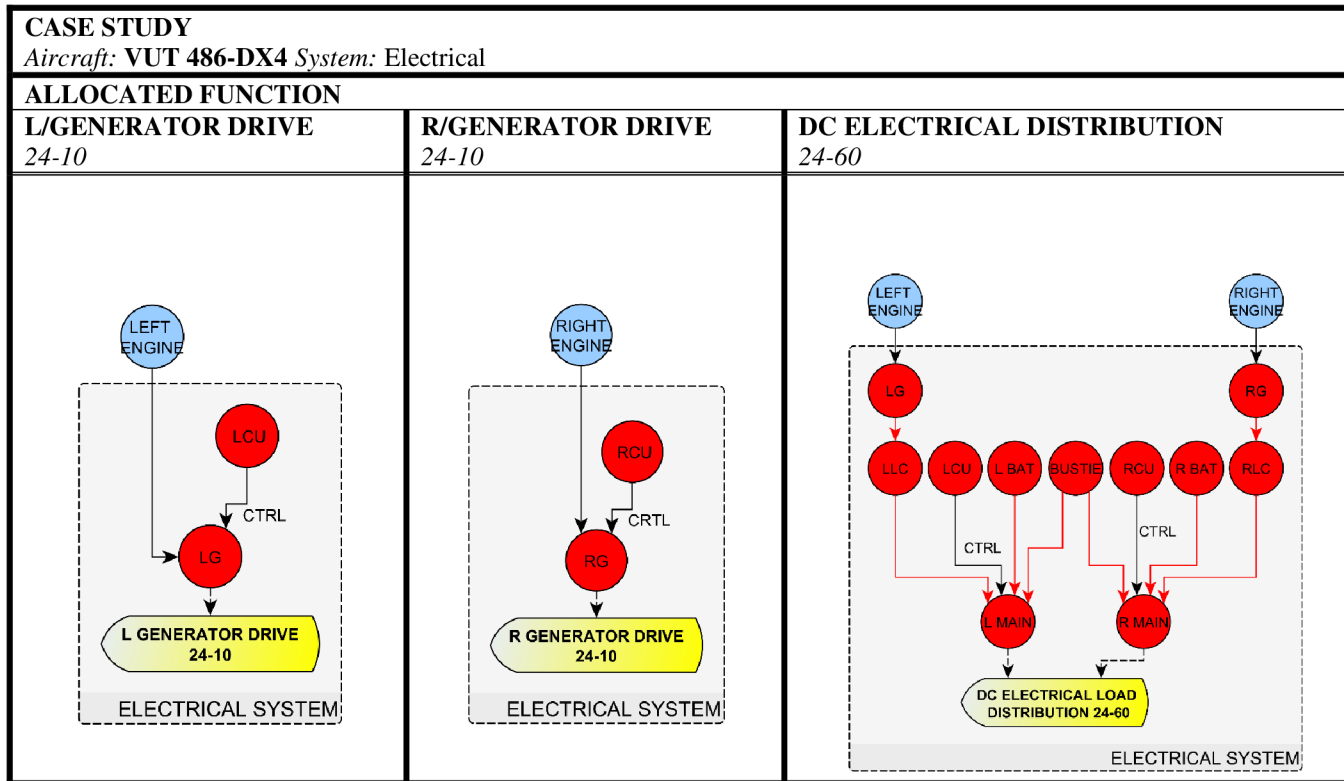
CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Avionics system</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High-level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
FUSE A11	2,40	1,00	2,38E-06	8,0	0,901851852	0,0014	2,76	6
FUSE A12	1,82	1,00	2,38E-06	8,0	0,901851852	0,0014	2,63	1
FUSE A13	1,74	1,00	2,38E-06	8,0	0,901851852	0,0014	2,47	1
FUSE A9	2,29	1,00	2,38E-06	8,0	0,901851852	0,0019	2,34	6
GPS ANT #1 <i>Antenna</i>	1,54	1,00	2,26E-06	3,0	0,901851852	0,0000	2,11	4
GPS ANT #2 <i>Antenna</i>	1,54	1,00	2,26E-06	3,0	0,901851852	0,0000	2,11	4
VS #1 <i>Vertical speed indicator</i>	0,94	1,00	1,04E-04	6,0	0,901851852	0,0000	1,75	0
VS #2 <i>Vertical speed indicator</i>	0,90	1,00	1,04E-04	6,0	0,901851852	0,0000	1,69	0
DG SEN #1 <i>Direction gyro sensor</i>	1,49	1,00	5,28E-04	2,0	0,901851852	0,0000	1,65	6
DG SEN #2 <i>Direction gyro sensor</i>	1,49	1,00	5,28E-04	2,0	0,901851852	0,0000	1,65	6
ATT #2 <i>Antenna</i>	0,86	1,00	1,36E-06	3,0	0,901851852	0,0000	1,61	0
ATT #1 <i>Antenna</i>	0,85	1,00	1,36E-06	3,0	0,901851852	0,0000	1,59	0

3. Electrical system safety and reliability assessment (short version)

	CASE STUDY														
	Aircraft: VUT 486-DX4 System: Electrical														
	GENERAL PARAMETERS														
	Type	Electro/ mechanical													
	Allocated functions	<table border="1"> <thead> <tr> <th>Analysis ID/ Name / ATA 100</th> <th>Preliminary classification/ Function Severity</th> </tr> </thead> <tbody> <tr> <td>EL1 L/GENERATOR DRIVE 24-10</td> <td>MINOR FS 3</td> </tr> <tr> <td>EL2 R/GENERATOR DRIVE 24-10</td> <td>MINOR FS 3</td> </tr> <tr> <td>EL3 DC GENERATION 24-30 (L BATTERY)</td> <td>MINOR FS 3</td> </tr> <tr> <td>EL4 DC GENERATION 24-30 (R BATTERY)</td> <td>MINOR FS 3</td> </tr> <tr> <td>EL5 DC ELECTRICAL 24-60 DISTRIBUTION (single item)</td> <td>MINOR FS 3</td> </tr> <tr> <td>COMBINATORY DC ELECTRICAL DISTRIBUTION (24-60)</td> <td>HAZARDOUS FS 7,85</td> </tr> </tbody> </table>	Analysis ID/ Name / ATA 100	Preliminary classification/ Function Severity	EL1 L/GENERATOR DRIVE 24-10	MINOR FS 3	EL2 R/GENERATOR DRIVE 24-10	MINOR FS 3	EL3 DC GENERATION 24-30 (L BATTERY)	MINOR FS 3	EL4 DC GENERATION 24-30 (R BATTERY)	MINOR FS 3	EL5 DC ELECTRICAL 24-60 DISTRIBUTION (single item)	MINOR FS 3	COMBINATORY DC ELECTRICAL DISTRIBUTION (24-60)
Analysis ID/ Name / ATA 100	Preliminary classification/ Function Severity														
EL1 L/GENERATOR DRIVE 24-10	MINOR FS 3														
EL2 R/GENERATOR DRIVE 24-10	MINOR FS 3														
EL3 DC GENERATION 24-30 (L BATTERY)	MINOR FS 3														
EL4 DC GENERATION 24-30 (R BATTERY)	MINOR FS 3														
EL5 DC ELECTRICAL 24-60 DISTRIBUTION (single item)	MINOR FS 3														
COMBINATORY DC ELECTRICAL DISTRIBUTION (24-60)	HAZARDOUS FS 7,85														
Related operational modes	FLIGHT MODE														
Intersystem succeeding connections	FUSE A1 (AV4) FUSE A2 (AV8) FUSE A3 (AV3, AV4, AV5, AV6, AV7) FUSE A4 (AV10) FUSE A5 (AV3, AV10, AV7, AV5, AV6) FUSE A9 (AV3, AV4, AV5, AV6, AV7) FUSE L DAU (LEI1, LEI2, LEI3, LEI4, LEI5, LEI6, LEI 7)	FUSE A6 (AV3) FUSE A7 (AV4) FUSE A9 (AV2) FUSE A10 (ET1, ET2) FUSE A11 (AV6) FUSE TR 2 (ET3) FUSE R DAU (REI1, REI2, REI3, REI4, REI5, REI6, REI 7)													
Intersystem preceding connections	LEFT ENGINE (EL1) RIGHT ENGINE (EL2)														

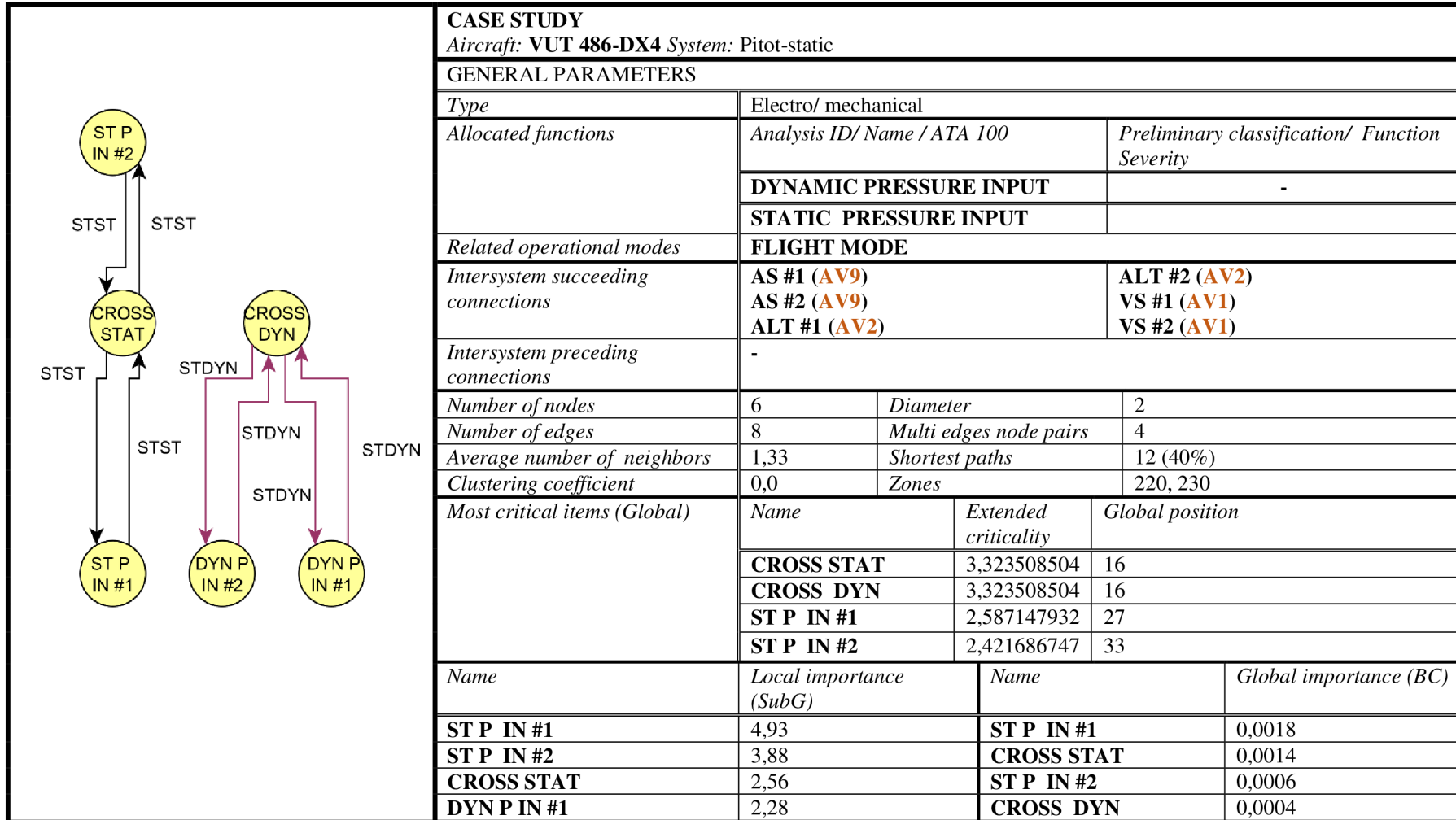


CASE STUDY <i>Aircraft: VUT 486-DX4 System: Electrical</i>							
SYSTEM PARAMETERS							
<i>Separation/ segregation</i>		<i>Diversity/ redundancy</i>		<i>Complexity/ design/ maturity/ experience</i>		<i>Environmental control/ testing</i>	
Q1	RATHER NO/1,6	Q1	YES/4	Q1	YES/3,8	Q1	RATHER YES/2,8
Q2	RATHER YES/ 2,4	Q2	RATHER YES/ 2,3	Q2	YES/4	Q2	RATHER YES/2,8
Q3	RATHER YES/ 2,4	Q3	NO/0	Q3	YES/4	Q3	RATHER YES/2,3
Q4	RATHER YES/ 2,8	Q4	NO/0	Q4	YES/4	Q4	YES/ 3,3
-	-					Q5	RATHER YES/2,6
-	-	-	-	-	-	Q6	RATHER YES/3,2
Score. 0,773 Level. VERY HIGH SEGREGATION/ SEP.		Score. 0,5 Level. MEDIUM DIVERSITY		Score. 0,495 Level. MEDIUM COMPLEIXTY		Score. 0,715 Level. HIGH ENVIROMENTAL PROT	

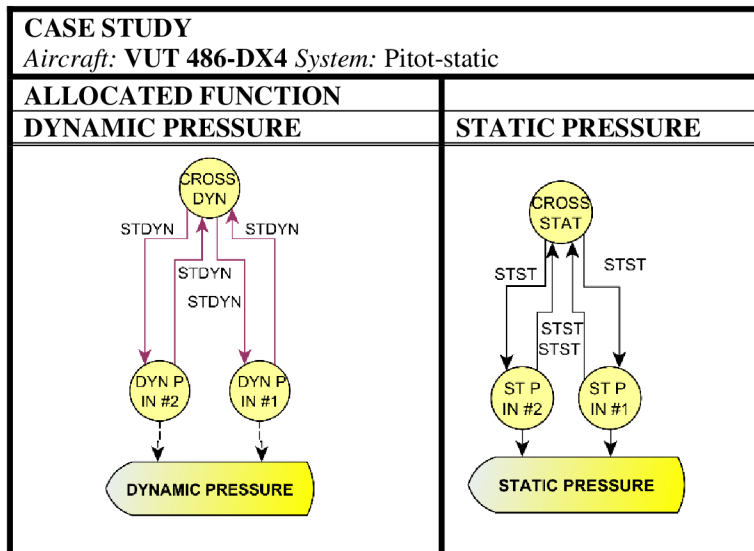


CASE STUDY									
<i>Aircraft: VUT 486-DX4 System: Electrical</i>									
Item	Zone	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
		<i>Node topology parameter</i>	<i>High- level severity</i>	<i>Detectability</i>	<i>Occurrence</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
LLC <i>Contactor</i>	720	36,97	3,50	1,06E-04	6,0	5,000815662	0,0160	2,57	54
RLC <i>Contactor</i>	730	36,94	3,50	1,06E-04	6,0	5,000815662	0,0160	2,56	54
L MAIN <i>Busbar</i>	720	56,80	3,00	2,50E-07	6,5	4,252264671	0,0436	6,60	53
R MAIN <i>Busbar</i>	730	51,64	3,00	2,50E-07	6,5	4,252264671	0,0365	6,44	53
RCU <i>Control Unit</i>	730	23,07	3,50	1,12E-04	2,0	3,057076345	0,0000	1,64	56
LCU <i>Control Unit</i>	720	23,06	3,50	1,12E-04	2,0	3,056469643	0,0000	1,82	54
R BAT <i>Battery</i>	730	22,68	3,50	2,72E-05	2,0	2,523247912	0,0226	9,67	24
AVION LMB <i>Busbar</i>	720	38,41	3,00	2,50E-07	6,5	2,509062254	0,0186	6,59	21
AVION RMB <i>Busbar</i>	730	29,76	3,00	2,50E-07	6,5	2,509062254	0,0109	2,99	55
LG <i>Generator</i>	410	33,98	3,50	4,50E-06	1,5	2,421686747	0,0109	2,94	55
RG <i>Generator</i>	510	33,88	3,50	4,50E-06	1,5	2,421686747	0,0026	2,52	7
AVION RAX <i>Busbar</i>	730	7,96	3,00	2,50E-07	6,5	2,421686747	0,0000	1,82	0
AVION LAX <i>Busbar</i>	720	2,92	3,00	2,50E-07	6,5	2,421686747	0,0238	2,76	53
BUSTIE <i>Contactor</i>	720	18,50	1,50	1,06E-04	6,0	1,945567198	0,0000	1,82	54
L BAT <i>Battery</i>	720	9,73	1,50	2,72E-05	2,0	0,901851852	0,0000	1,64	56

4. Pitot-static system (short version)



CASE STUDY							
Aircraft: VUT 486-DX4 System: Pitot-static							
SYSTEM PARAMETERS							
Separation/ segregation		Diversity/ redundancy		Complexity/ design/ maturity/ experience		Environmental control/ testing	
Q1	RATHER YES/ 2,3	Q1	YES/4	Q1	NO/0	Q1	RATHER YES/2,8
Q2	NO/0	Q2	NO/0	Q2	YES/4	Q2	YES/ 3,6
Q3	NO/0	Q3	NO/0	Q3	YES/4	Q3	YES/ 3,6
Q4	RATHER NO/0,9	Q4	NO/0	Q4	YES/4	Q4	YES/ 3,6
-	-	-	-	-	-	Q5	NO/0
-	-	-	-	-	-	Q6	RATHER NO/1,2
Score. 0,5 Level. MEDIUM SEGREGATIIN/ SEP.		Score. 0,35 Level. MEDIUM DIVERSITY		Score. 0,0967 Level. LOW COMPLEXITY		Score. 0,686 Level. HIGH ENVIROMENTAL PROT.	

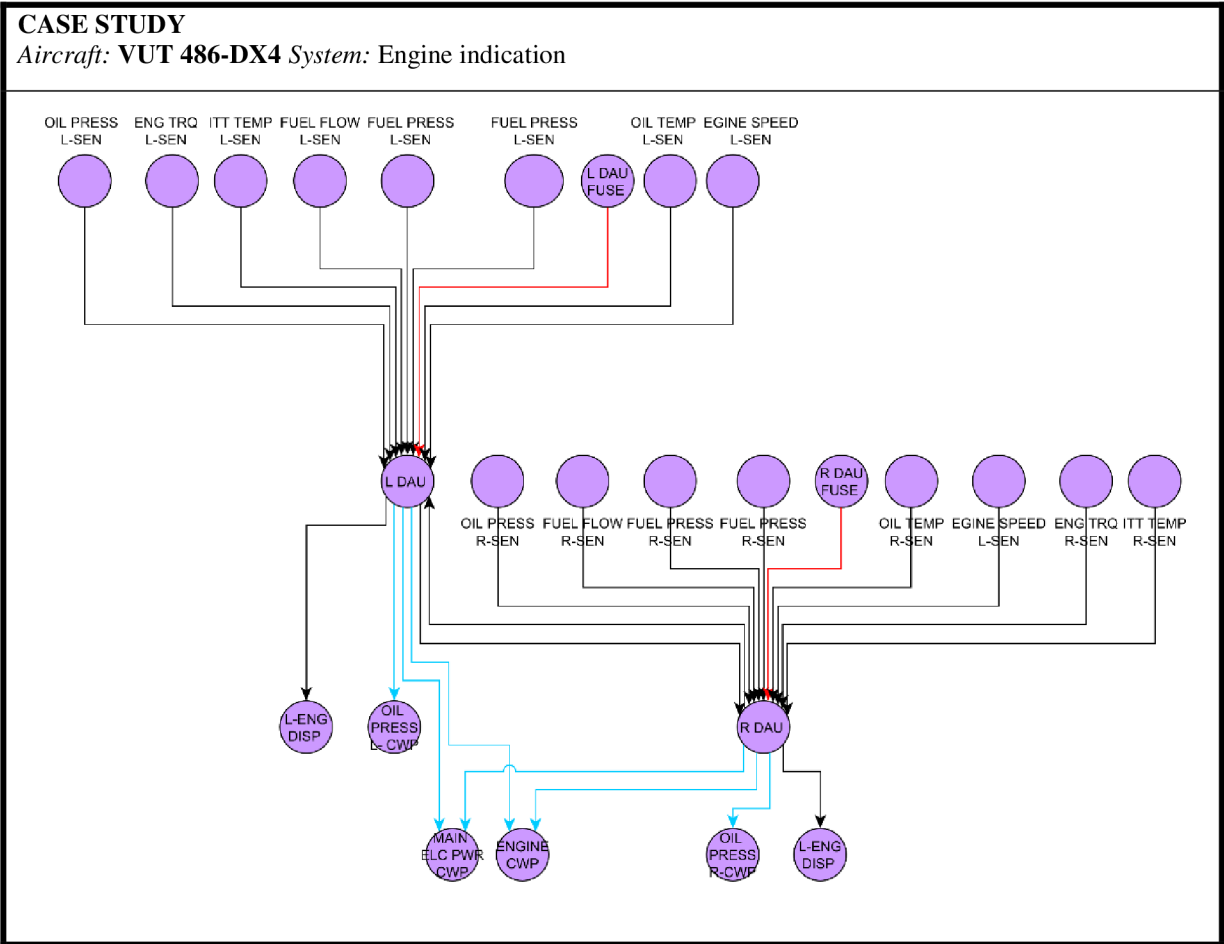


CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Pitot-static</i>								
Item	Fuzzy Extended criticality Evaluation Inputs				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High- level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
ST P IN #1	17,89	4,00	1,00E-09	8,5	2,587147932	0,0018	4,93	14
CROSS STAT	13,24	4,25	3,78E-05	6,0	3,323508504	0,0014	2,56	14
ST P IN #2	14,55	4,00	1,00E-09	8,5	2,421686747	0,0006	3,88	14
CROSS DYN	7,72	4,50	3,78E-05	6,0	3,323508504	0,0004	2,28	4
DYN P IN #1	7,53	4,50	1,00E-09	8,5	2,421686747	0,0002	2,28	4
DYN P IN #2	7,52	4,50	1,00E-09	8,5	2,421686747	0,0002	2,28	4

5. Engine indication (short version)

CASE STUDY		
<i>Aircraft: VUT 486-DX4 System: Engine indication</i>		
GENERAL PARAMETERS		
<i>Type</i>	Electro/ mechanical	
<i>Allocated functions</i>	<i>Analysis ID/ Name / ATA 100</i>	<i>Preliminary classification/ Function Severity</i>
	EI1 TACHO INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI2 OIL PRESSURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI3 FUEL PRESSURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI4 TORQUE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI5 FUEL FLOW INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI6 OIL TEMPERATURE INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	EI7 ITT INDICAITON 77-10	MINOR FS 2,5 (Loss of function)
	COMBINATORY ENGINE INDCAITON L/R	MAJOR FS 5 (Loss of function)
<i>Related operational modes</i>	FLIGHT MODE	
<i>Intersystem succeeding connections</i>	-	
<i>Intersystem preceding connections</i>	AVION LMB (LEI1, LEI2, LEI3, LEI4, LEI5, LEI6, LEI 7) AVION RLMB (RLEI1, REI2, REI3, REI4, REI5, REI6, REI 7)	

CASE STUDY			
<i>Aircraft: VUT 486-DX4 System: Engine indication</i>			
<i>Number of nodes</i>	26	<i>Diameter</i>	3
<i>Number of edges</i>	28	<i>Multi edges node pairs</i>	1
<i>Average number of neighbors</i>	2,01	<i>Shortest paths</i>	158 (24%)
<i>Clustering coefficient</i>		<i>Zones</i>	230, 410, 510, 720, 730
<i>Most critical items (Global)</i>	<i>Name</i>	<i>Extended criticality</i>	<i>Global position</i>
	R DAU	4,151774628	11
	L DAU	4,151774628	11
	R DAU FUSE	2,500971083	31
	L DAU FUSE	2,483595637	32
<i>Name</i>	<i>Local importance (SubG)</i>	<i>Name</i>	<i>Global importance (BC)</i>
R DAU	24,95	R DAU	0,0181
L DAU	24,77	L DAU	0,0181
MAIN ELC PWR CWP	5,33	R DAU FUSE	0,0067
R DAU FUSE	3,66	L DAU FUSE	0,0067



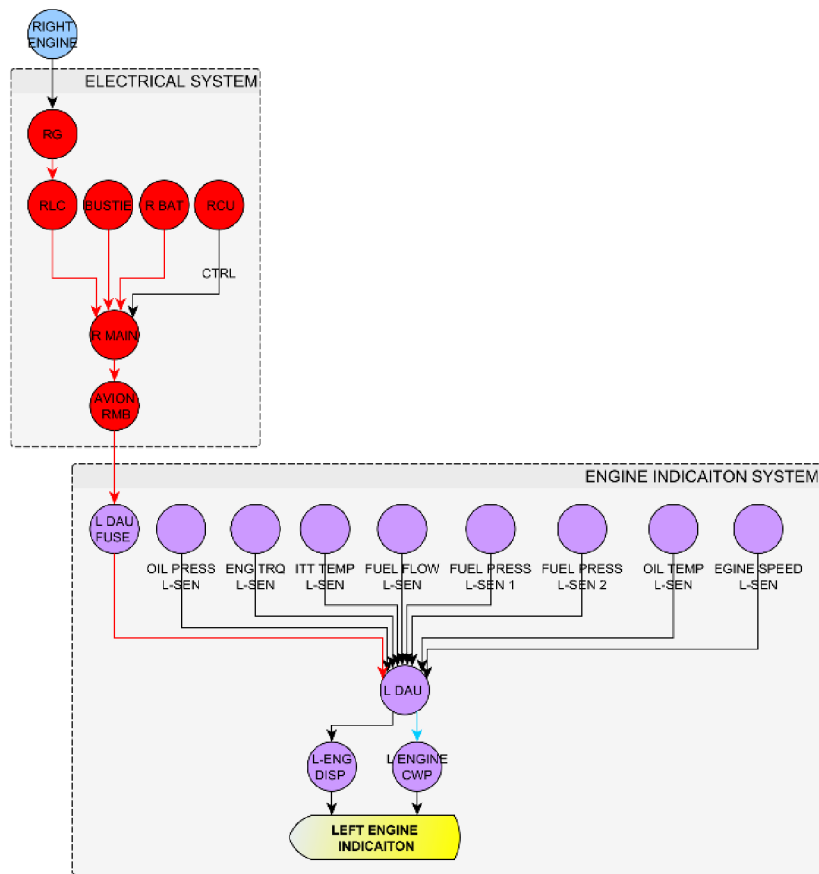
CASE STUDY <i>Aircraft: VUT 486-DX4 System: Engine indication</i>							
SYSTEM PARAMETERS							
<i>Separation/ segregation</i>		<i>Diversity/ redundancy</i>		<i>Complexity/ design/ maturity/ experience</i>		<i>Environmental control/ testing</i>	
Q1	RATHER NO/ 1,4	Q1	RATHER YES/2,9	Q1	NO/0	Q1	RATHER YES/ 2,8
Q2	NO/ 0	Q2	NO/0	Q2	YES/3,5	Q2	RATHER YES/2,8
Q3	NO/ 0	Q3	NO/0	Q3	YES/3,5	Q3	RATHER YES/2,8
Q4	YES/ 3,8	Q4	NO/0	Q4	NO/0	Q4	RATHER YES/2,8
-	-					Q5	RATHER YES/2,6
-	-	-	-	-	-	Q6	RATHER YES/2,6
Score. 0,805 Level. VERY HIGH SEGREGATION/ SEP.		Score. 0.0983 Level. LOW DIVERSITY		Score. 0,5 Level. MEDIUM COMPLEXITY		Score. 0,659 Level. HIGH ENVIROMENTAL PROT.	

CASE STUDY

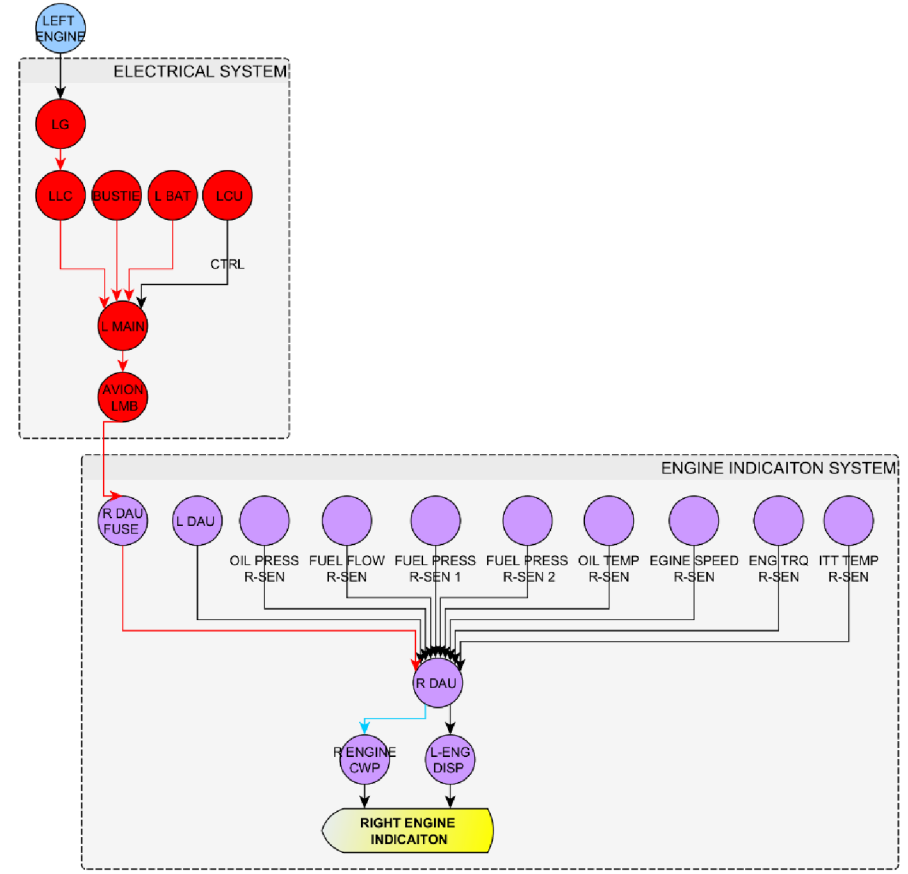
Aircraft: VUT 486-DX4 System: Engine indication

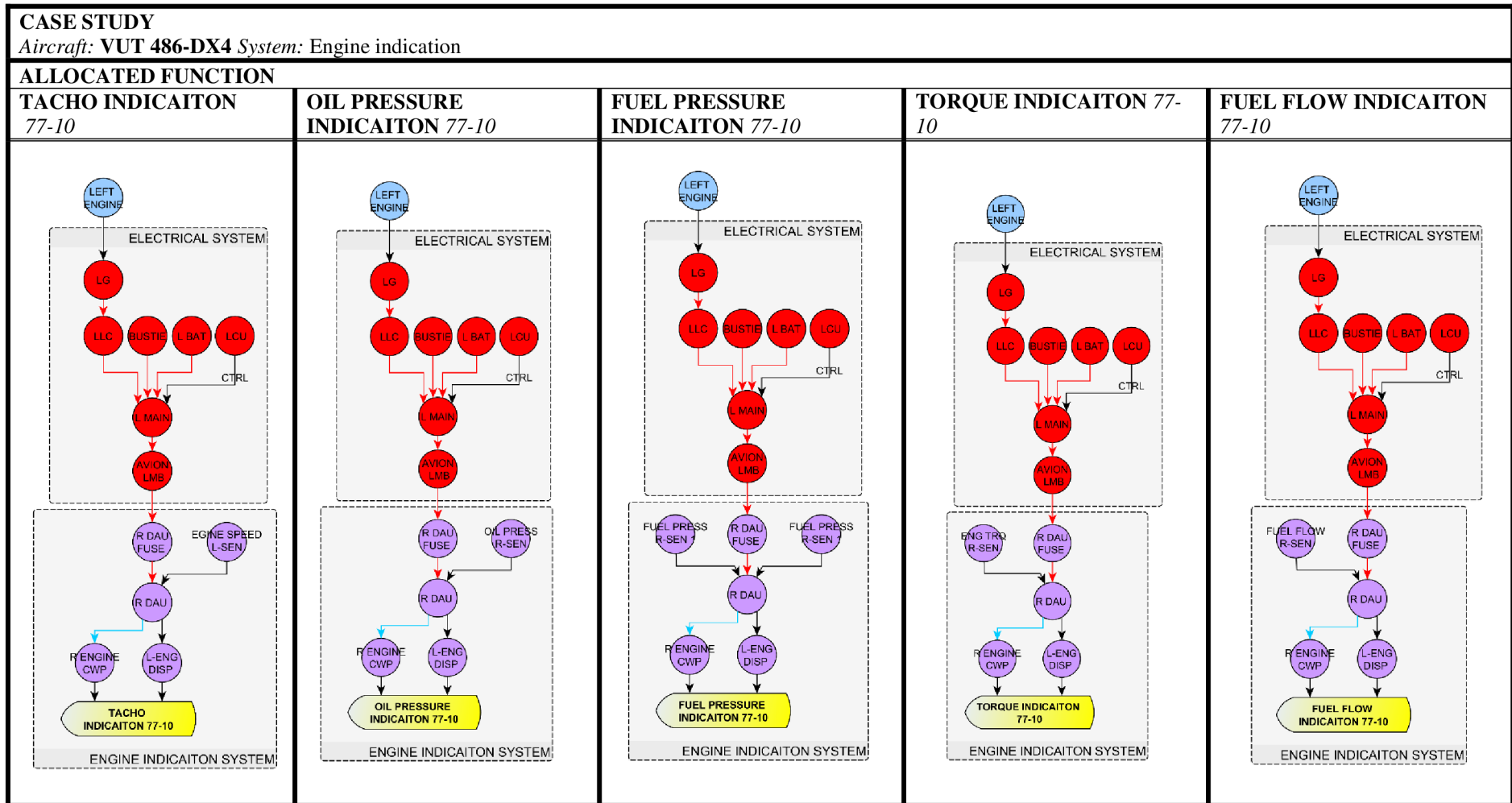
ALLOCATED FUNCTION

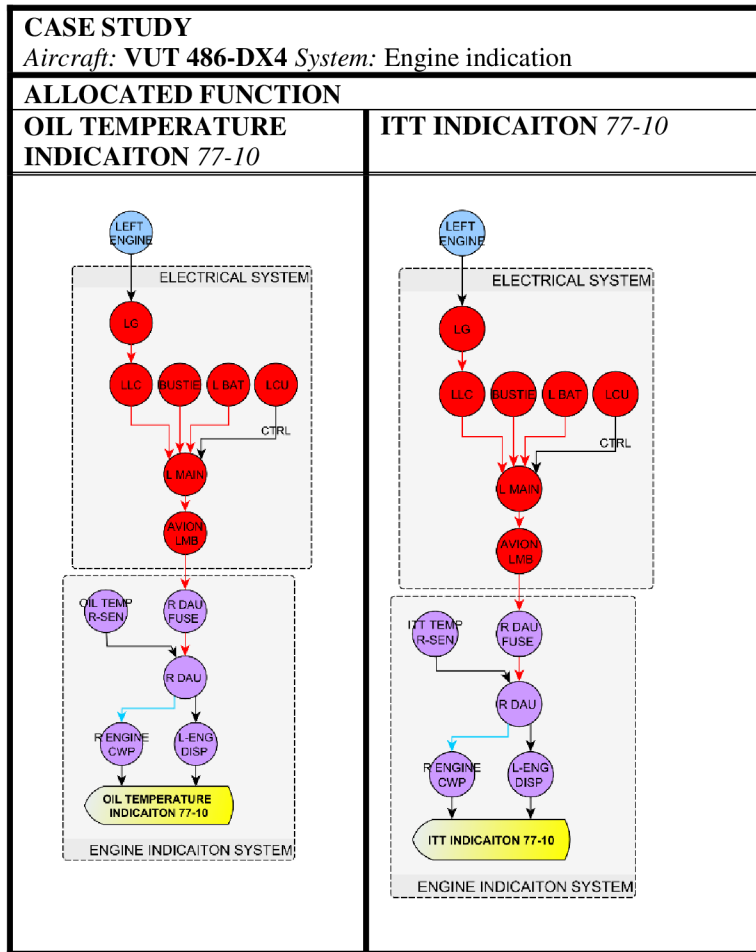
LEFT ENGINE COMPLETE INDICATION



RIGHT ENGINE COMPLETE INDICATION







CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Avionics system</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High-level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
GTN #1 <i>Integrated avionics unit</i>	46,06	4,75	4,58E-05	2,0	4,10801507	0,0032	16,21	3
GTN #2 <i>Integrated avionics unit</i>	46,71	4,75	4,58E-05	2,0	4,18122815	0,0038	16,19	3
TRANS	23,11	4,00	3,73E-06	7,5	3,06133238	0,0016	9,37	4
AUDIO #1 <i>Audio panel</i>	19,31	2,00	1,24E-05	5,0	2,06071952	0,0046	15,92	1
EHSI #1	18,00	4,50	3,00E-04	3,5	4,35037006	0,0022	5,79	4
EHSI #2	18,32	4,50	3,00E-04	3,5	4,37541335	0,0026	5,75	4
DME #1	13,09	2,00	4,09E-06	3,0	0,90185185	0,0018	10,69	4
FUSE A3	12,56	5,00	2,38E-06	8,0	2,42168675	0,0015	3,30	4
FUSE A5	11,26	4,50	2,38E-06	8,0	2,42168675	0,0018	3,13	4
FUSE A1	9,56	4,00	2,38E-06	8,0	2,42168675	0,0014	2,92	5
FUSE A7	9,18	4,00	2,38E-06	8,0	2,42168675	0,0014	2,75	5
FUSE A2	8,31	4,00	2,38E-06	8,0	2,42168675	0,0014	2,72	3
ALT METR	9,19	4,00	2,63E-05	7,5	3,00937974	0,0015	2,71	5

CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Engine indication</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High-level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
R DAU <i>Data acquisition unit</i>	68,60	3,75	3,74E-06	2,0	4,151774628	0,0181	24,95	8
L DAU <i>Data acquisition unit</i>	68,25	3,75	3,74E-06	2,0	4,151774628	0,0181	24,77	8
R DAU FUSE	16,53	3,75	2,38E-06	8,0	2,500971083	0,0067	3,66	9
L DAU FUSE	16,22	3,75	2,38E-06	8,0	2,483595637	0,0067	3,51	9
MAIN ELC PWR <i>CWP Diode</i>	7,12	2,50	3,00E-08	8,0	2,138888889	0,0000	5,33	0
OIL TEMP L-SEN <i>Sensor</i>	5,10	2,25	1,24E-06	8,0	1,757189542	0,0000	2,52	9
ENGINE SPEED L-SEN <i>Sensor</i>	4,53	2,00	2,98E-04	3,0	0,901851852	0,0000	2,52	9
OIL PRESS L-CWP <i>Diode</i>	2,70	2,00	3,00E-08	8,0	0,901851852	0,0000	2,52	0
L ENGINE CWP <i>Diode</i>	4,72	3,50	3,00E-08	8,0	2,421686747	0,0000	2,52	0
L-ENG DISP <i>Diode</i>	4,04	3,00	6,32E-06	6,0	2,421686747	0,0000	2,52	0
ITT TEMP L-SEN <i>Sensor</i>	4,53	2,00	1,24E-06	8,0	0,901851852	0,0000	2,52	9
FUEL FLOW L-SEN <i>Sensor</i>	4,53	2,00	1,73E-04	3,0	0,901851852	0,0000	2,52	9
OIL PRESS L-SEN <i>Sensor</i>	4,53	2,00	1,99E-04	3,0	0,901851852	0,0000	2,52	9

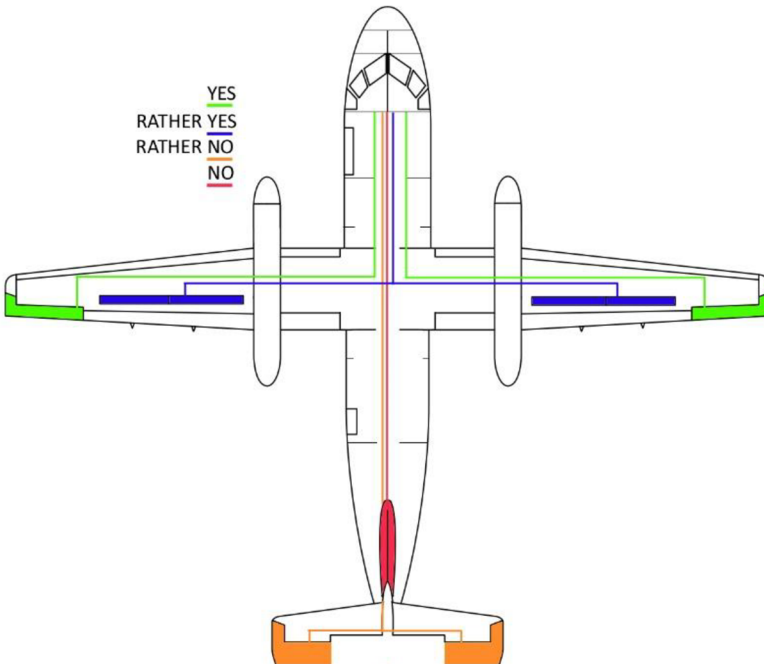
CASE STUDY								
<i>Aircraft: VUT 486-DX4 System: Engine indication</i>								
Item	<i>Fuzzy Extended criticality Evaluation Inputs</i>				EXTENDED CRITICALITY	<i>Graph model parameters</i>		
	<i>Node topology parameter</i>	<i>High-level severity</i>	<i>Occurrence</i>	<i>Detectability</i>		<i>BC</i>	<i>Subgraph centrality</i>	<i>Centroid volume</i>
ENG TRQ L-SEN <i>Sensor</i>	4,53	2,00	1,00E-06	8,0	0,901851852	0,0000	2,52	9
FUEL PRESS L-SEN 2 <i>Sensor</i>	2,27	1,00	1,99E-04	2,0	0,901851852	0,0000	2,52	9
FUEL PRESS L-SEN 1 <i>Sensor</i>	2,27	1,00	1,99E-04	2,0	0,901851852	0,0000	2,52	9
ENGINE SPEED L-SEN <i>Sensor</i>	4,53	2,00	2,98E-04	3,0	0,901851852	0,0000	2,52	9
FUEL FLOW R-SEN <i>Sensor</i>	4,53	2,00	1,73E-04	3,0	0,901851852	0,0000	2,52	9
OIL PRESS R-SEN <i>Sensor</i>	4,53	2,00	1,99E-04	3,0	0,901851852	0,0000	2,52	9
FUEL PRESS R-SEN 1 <i>Sensor</i>	2,27	1,00	1,99E-04	2,0	0,901851852	0,0000	2,52	9
L-ENG DISP <i>Diode</i>	4,72	3,50	6,32E-06	6,0	2,421686747	0,0000	2,52	0
R ENGINE CWP <i>Diode</i>	4,72	3,50	3,00E-08	8,0	2,421686747	0,0000	2,52	0
OIL TEMP R-SEN <i>Diode</i>	5,10	2,25	1,24E-06	8,0	1,757189542	0,0000	2,52	9
OIL PRESS R-CWP <i>Diode</i>	2,70	2,00	3,00E-08	8,0	0,901851852	0,0000	2,52	0
FUEL PRESS R-SEN 2 <i>Sensor</i>	2,27	1,00	1,99E-04	2,0	0,901851852	0,0000	2,52	9
ITT TEMP R-SEN <i>Sensor</i>	4,53	2,00	1,24E-06	8,0	0,901851852	0,0000	2,52	9


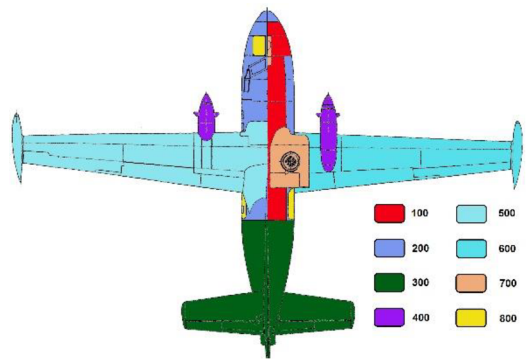
Appendix D


Robustness Questionnaire (derived from IEC 61508)

<i>Question level of relevance</i>	
R	Relevant
N/R	Non- relevant
P/R	Partially relevant

<i>Potential questionnaire answers</i>	
YES	It does fulfil definition.
P/YES	Partially fulfill definition.
P/NO	Partially not fulfill definition.
NO	It does fulfil definition.

SEPARATION/ SEGREGATION CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Separation					
Q1: Are connection (cables, wires, pipes) for the channels routed separately at all positions?	R	R	R	R	R
<p><i>Question aims to evaluation of system connection especially in the case of symmetrical system (flaps, engine control, etc.).</i></p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;">  </div> <div style="width: 50%;"> <p><i>Answer YES: It means, that all channels are routed separately.</i></p> <p><i>Answer RATHER YES: Majority of channel connections is routed separately.</i></p> <p><i>Answer RATHER NO: Majority of channel connection is routed together.</i></p> <p><i>Answer NO: Channels are roted together. Channels are exposed to the same ambient influeces.</i></p> <p><i>Note. Figure shows visual example.</i></p> </div> </div>					
Separation					
Q2: Are the logic sub-system channels on separate printed-circuits boards?	R	R	N/R	N/R	N/R
<p><i>Logic channels separation to the separate circuit board ensures redundant system control even in the case of shortcut or ambient influence. It is essential in the case of complex control system with high severity.</i></p>					

SEPARATION/ SEGREGATION CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Segregation					
Q3: Are the subsystem channels in separate cabinets (physically separated)?	R	R	N/R	R	R
 <p>[47] Line Replaceable Unit</p>		<p>Analyst express level of physical separation of system items. Separate cabinets isolate items (fully or partially) from ambient effects, like humidity or temperate variation. Electronics logic are electrical systems are the most venerable to these effects. On the other side of spectrum, mechanical system could by easily protected against these effect (protecting surface layers, maintenance).</p>			
Segregation					
Q4: Is system protected against ambient influences caused by collateral system (electrical, mechanical, temperature, humidity condensation)?	R	R	R	R	R
		<p>Analyst should express level of collateral system effect on particular item and system. Also, It should considerate installation aspects of individual item/ system and protection against influences between several systems. Logically, it not substitution of Zonal Safety Analysis (see, ARP 4761). Answer expanses system parameters overview.</p>			
Figure. Example of L410 zonal division [44]					
Maximal score: 16					

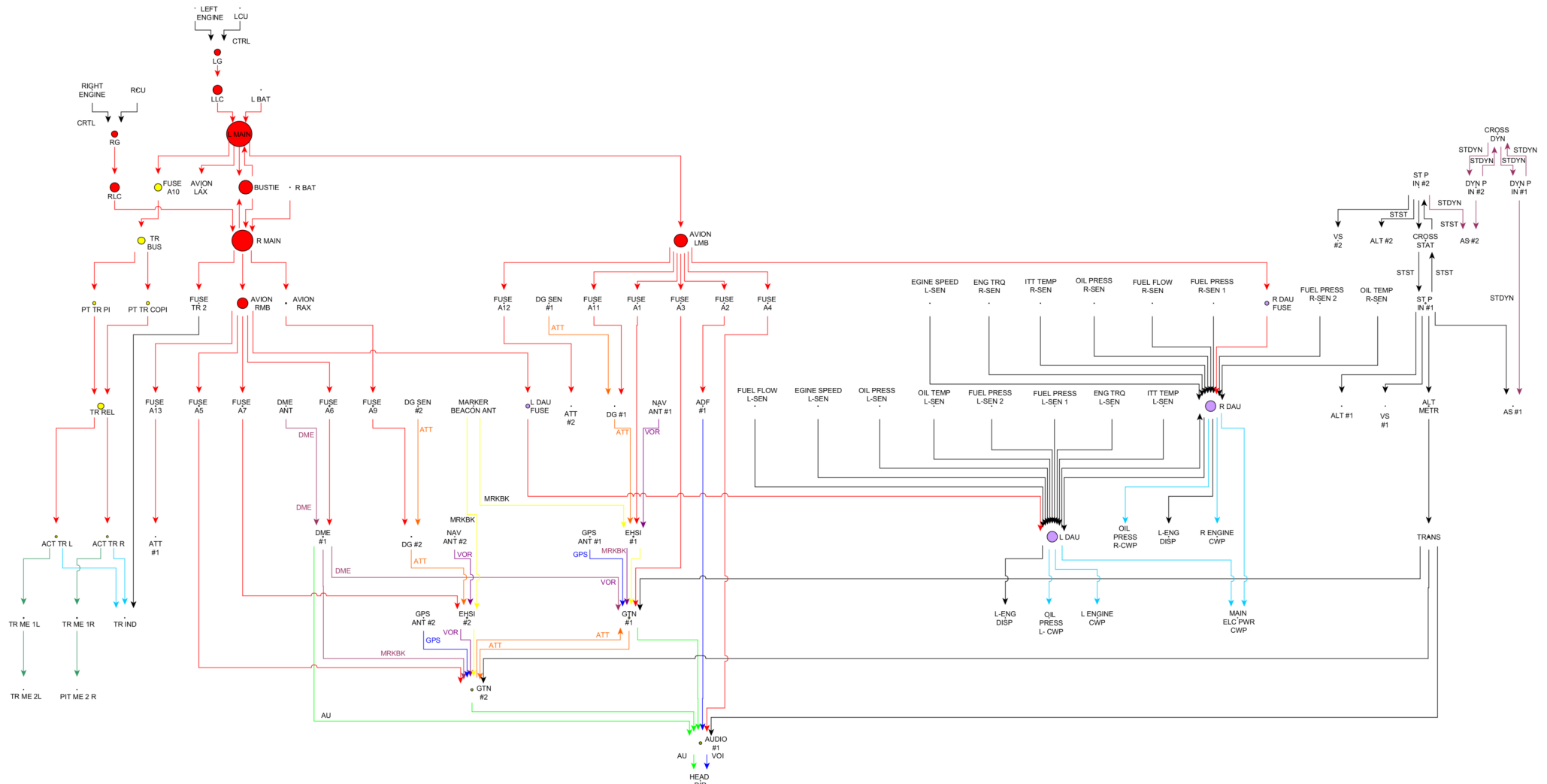
DIVERSITY/ REDUNDANCY CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Redundancy					
Q1: Are the main parts of system designed as redundant?	R	R	R	R	R
<i>Function redundancy significantly elevates system reliability and safety in the case of failure.</i>					
Redundancy					
Q2: Do the channels employ different electronic technologies (for example, one electronic, the other programmable electronic)?	R	R	R	R	R
<i>Different technology application ensures high level of redundancy based on redundancy by more reliability item (despite potential lowered functionality).</i>					
Diversity					
Q3: Do the devices employ different physical principles? (for the sensing elements for example, pressure and temperature, vane anemometer, etc.)	R	R	R	R	R
	<p><i>Employment of different physical principle protect system against common cause failures. For instance, landing gear system is usually driven by hydraulic system (EASA CS-23 and higher), in the case of system failure, system is equipped by mechanical backup. Electrical system is could be influenced by shortcuts, over voltage or electromagnetic radiation. Higher level of diversity should be applied in the case of safety critical system. Analyst express level of system diversity (from the employment of different physical principles.</i></p>				
A330 Landing gear [48]					

DIVERSITY/ REDUNDANCY CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Diversity					
Q4: Is maintenance on each channel carried out by different people at different times?	R	R	R	R	R
<i>Maintenance carried out by different personal at different time could avoid eventual mistakes.</i>					
Maximal score: 16					

COMPLEXITY/ DESIGN/ MATURITY/ EXPERIENCE CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Complexity					
Q1: Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	R	R	N/R	R	R
<i>Information cross-connection could potentially lead to cascading failure based on false information spread. Typical example is cross-connection between integrated avionics units.</i>					
Maturity					
Q2: Is the system design based on techniques used in equipment that has been used successfully in the field for > 5 years?	R	R	R	R	R
<i>Long term successful application benefits particular system design. Typical examples of system maturity are new generations of Aircraft Industries L-410 NG and Aero L-29. Various system (and items) stood up test of time and they are used on new generations.</i>					
Experience					
Q3: Is there more than 5 years- experience with the same hardware used in similar environments?	R	R	R	R	R
<i>Experience with given items of system prefers it for further application. Moreover, it the case of application in the similar environment.</i>					
Complexity					
Q4: Is the system simple, for example no more than 10 inputs or outputs per channel?	R	R	P/R	P/R	P/R
<i>Highly complex systems are more venerable to the cascading failures. Complexity elevates level of systems mutual interconnection.</i>					
Maximal score: 16					

ENVIRONMENTAL CONTROL AND TESTING CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanica l (full or partially)	Pneumatic	Hydraulic
Environmental control					
Q1: Have designers been trained to understand the causes and consequences of common cause failures?	R	R	R	R	R
<i>System engineers familiarized with concept of common cause failure design system in respect with potential common failure and create required mitigation means.</i>					
Environmental control					
Q2: Is the system likely to operate always within the range of temperature, humidity and corrosion, without the use of external environmental control?	R	R	R	R	R
<i>System designed in regard with RTCA DO-160 testing requirements are inherently better protected against ambient influence of temperature variation and shocks, humidity and altitude (even without external environmental control.</i>					
Environmental control					
Q3: Is the system likely to operate always within the range of, operational shock, crash safety and vibration?	R	R	R	R	R
<i>System designed in regard with RTCA DO-160 testing requirements are inherently better protected against ambient influence of operational shocks and vibrations.</i>					
Environmental control					
Q4: Are items of system design to operate in range of operation conditions?	R	R	R	R	R
<i>System design in respect with range of operational conditions are adjusted and tested for this particular application.</i>					

ENVIRONMENTAL CONTROL AND TESTING CLASS					
QUESTIONS					
Relevance	Electrical (full or partially)	Electronics (full or partially)	Mechanical (full or partially)	Pneumatic	Hydraulic
Environmental testing					
Q5: Are critical items authorized for aviation application by ETSO/ TSO or other authority approval?	R	R	R	R	R
<i>ETSO, TSO approval ensure that item (in this case critical to the system) is design for application in aviation. It has at least minimal level of performance (resistance to ambient influences- temperature, humidity, operation shocks).</i>					
Environmental testing					
Q6: Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	R	R	R	R	R
<i>Immunity testing could proof system protection or reveal potential weak parts of system.</i>					
Maximal score: 28					



- INDICATION (CWP)
- ELECTRICAL
- DATA
- MECHANICAL

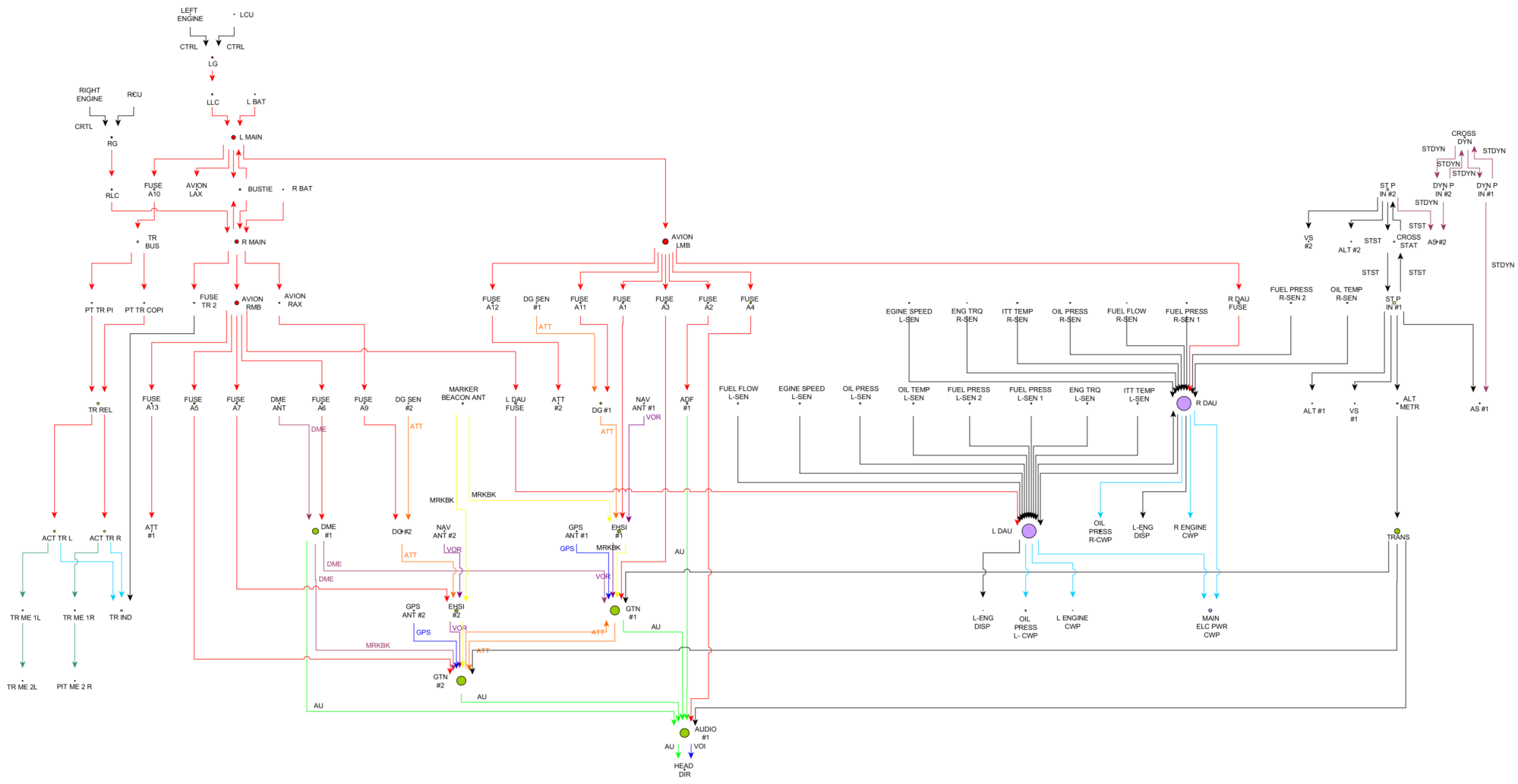
STDYN - Dynamic pressure
 STST - Static pressure
 MRKBK - Marker beacon
 AU - Aural information
 VOI - Voice communication
 Note. Other connections are clearly labeled

Appendix E

Case Study Evaluation

Global importance

Node size corresponds with item Betweenness centrality



— INDICATION (CWP)
 — ELECTRICAL
 — DATA
 — MECHANICAL

STDYN - Dymnic pressure
 STST - Static pressure
 MRKBK - Marker beacon
 AU - Aural information
 VOI - Voice communication
 Note. Other connection are clearly labeled

Appendix E

Case Study Evaluation

Local importance

Node size corresponds with item Subgraph centrality