USE OF COMMON CAUSE ANALYSIS IN THE CZECH GENERAL AVIATION

Rostislav Koštial
Institute of Aerospace Eng.,
Brno University of Technology
Technicka 2, 616 69 Brno
Czech Republic
Ykosti02@stud.fme.cz

Abstract. The paper deals with the extension of the safety and reliability assessment methods used for design of General Aviation (GA) aircrafts. Since the late 90`s of the past century the General Aviation aircraft systems became more complex and sophisticated. This paper specifically involves extended safety (reliability) analysis of the airplane Common Cause Analysis (CCA). This analysis was used in the past for large airplanes, in the present is also used in simplified form for General Aviation. Analysis assesses the overall airplane conditions after the installation of all systems. This analysis is useful in the certification assessment procedure. The paper describes experience with practical use of Common Cause Analysis on the General Aviation aircraft developed in the Czech Republic.

Keywords. Aircraft, General Aviation, Safety, Analysis, Reliability.

1 Introduction

The beginnings of a solution of reliability and safety can be tracked down to 1930`s. Great progress was made in the theory of dependability during World War II and 1950`s. The safety assessments with requirements defined in regulation standards definitely took place in aviation in 1960`s. Sophisticated methods were developed and first used on large transport aircraft in civil aviation, such as Boeing 747 aircraft developed in 1960`s. These methods have been first widely applied in Europe in the development of Airbus A300 and BAC Concorde. Development of theory of reliability enabled detailed reliability analysis. Complexity of the safety assessment has risen, partially also as a result of more complex aircraft systems.

Complexity of the aircraft systems was significantly lower in General Aviation and therefore detailed and complex analysis of reliability was requested in a simplified form. Since 1990`s with the adoption of highly complex avionics systems to smaller aircraft also requirements has increased for reliability and safety. Application of safety assessments methods made a great step toward more complex and more detailed analyses.

Basic requirements for reliability and safety assessments for General Aviation aircraft are described in the FAR/CS-23 airworthiness documents and more specifically in §23.1309. Requirements are used in design and certification phase (as mandatory requirements). This paragraph is important for system development and modifications, the requirements and recommendations contained in are very general and cannot be used for design and certification of aircraft. For showing compliance with paragraph and to support the certification phase, was issued an amendment to Regulation Advisory Circular AC 23.1309-1E ref. [1]. Although the document [1] provides valuable information about the safety assessment process and provides useful recommendation methods for

certification of aircraft in that category, it is not the single one. There are numerous documents and other materials that can be used for preliminary and detailed safety assessment process.

The most important documents, also referred in the Advisory document, are ARP 4754 [2] and ARP 4761 [3]. Document describes detailed guidelines and methods for performing the safety assessment process. Overview of the safety assessment is based on the typical development cycle of aircraft, can be observed in Fig.1 which is taken from document ARP 4761.

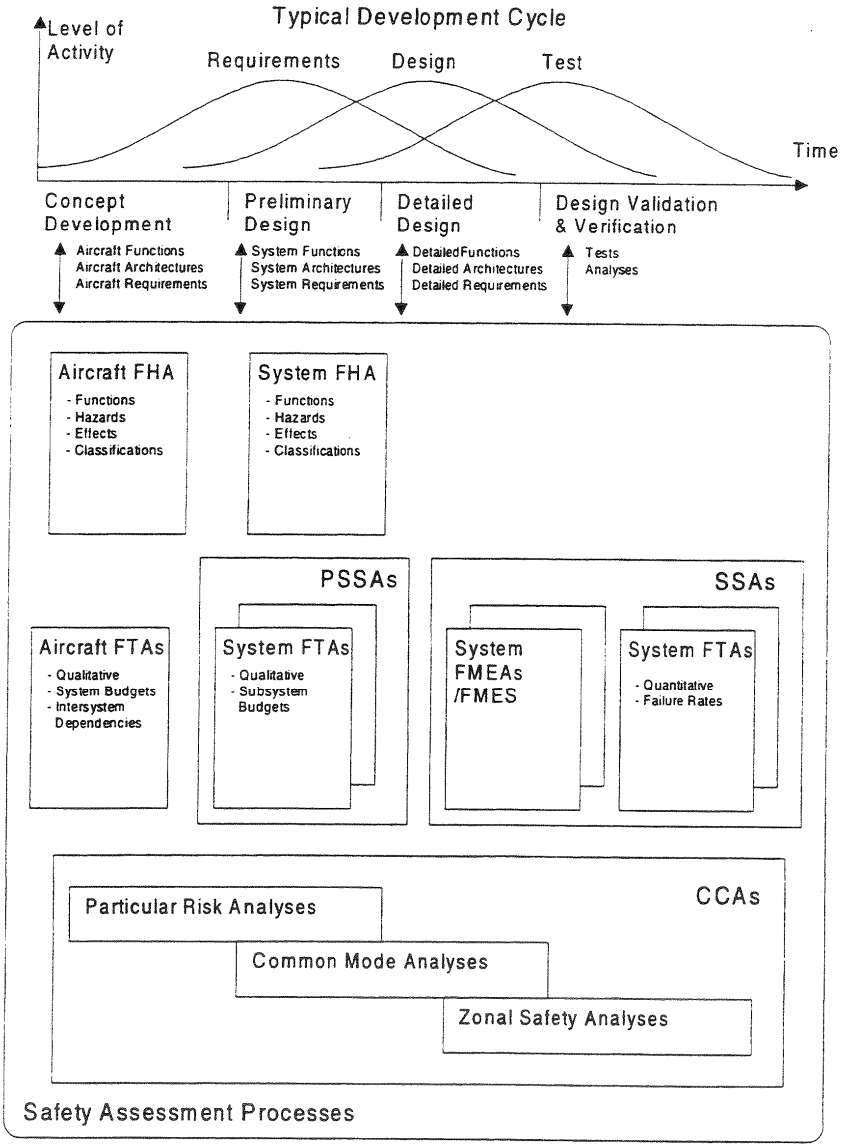

Figure 1: Overview of the Safety Assessment Process

The next part of the paper will deeply describe Common Cause Analysis (CCA) and its use in General Aviation in the Czech Republic.

2 Common Cause Analysis

Common Cause Analysis (CCA) techniques are an extension of deductive safety analysis especially targeted at the detection of non-independence between events which would be otherwise treated independently. Generally CCA analyses independence between systems, functions or items, which may be required to satisfy the safety requirements. For CCA is required detailed knowledge of aircraft systems.
CCA is subdivided into three types of analysis

2.1 Zonal Safety Analysis

Zonal Safety Analysis (ZSA) is used to satisfy the safety requirements in each zone of aircraft with respect to: - Installation and design requirements
- Interference between Systems
- Maintenance errors

"In those zones of the aircraft where multiple systems and components are installed close to each other, it should be ensured that the zonal analysis would identify any failure or malfunction which by itself considered sustainable but which have more serious effect when adversely affecting other adjacent systems or components."[4] This will either result in a design changes, redesign of the system or will be shown to be accepted in the appropriate safety assessment.

Aircraft zones are used to support airworthiness regulation (CCA-ZSA), design process and maintenance. The guidelines for determining airplane zones and their numbering can be found in the ATA iSpec 2200 standards. Example the aircraft zones are on Fig.2.

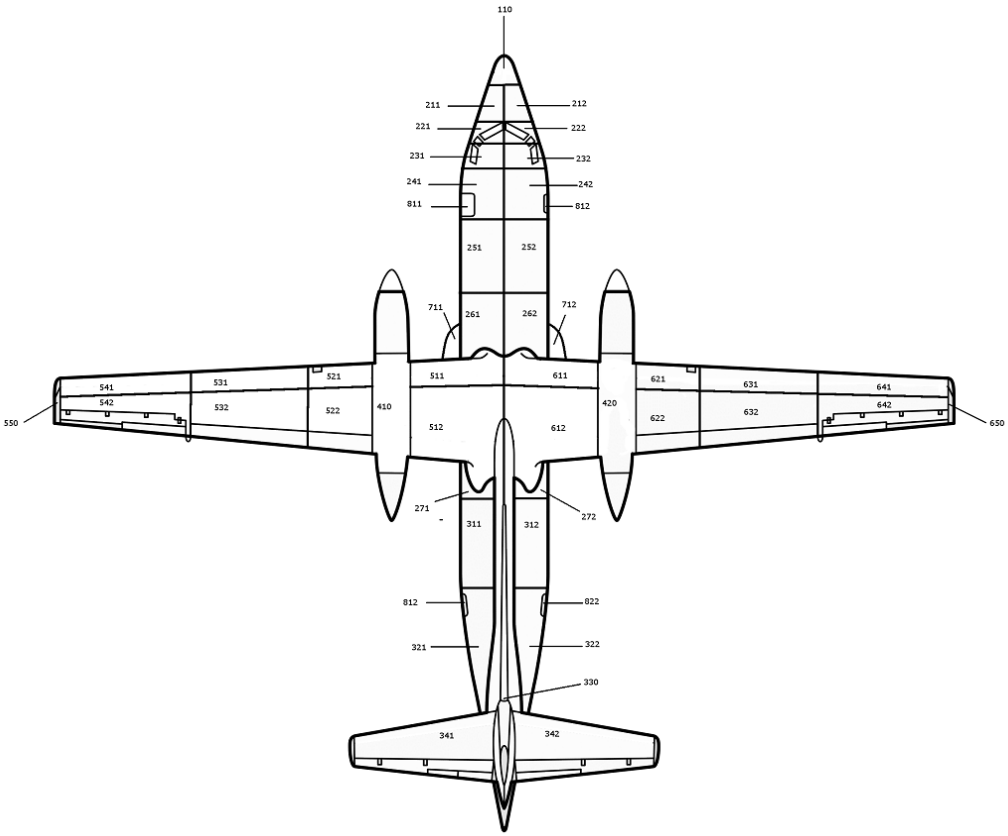

Figure 2: Example of aircraft zones on aircraft

For example, the use of CCA is used in the imaginary airplane model XX-YYY. Zoning and design of the aircraft is performed according to Figure.2. Certification base is considered in accordance to CS-23. CCA is used in simplified form. The example analyzed system of electrical wing flaps control. Wing flaps control is backed up by a hydraulic circuit. The hydraulic circuit enables single extrusion of wing flaps to the maximum position of 45°. In Tab. 1 it is example of summary of simplified ZSA for one zone of a given system.

ZONAL SAFETY ANALYSIS (ZSA)				Prepared by: *Rostislav Koštial*	Date: 22. 09. 2012
				Approved by:	Date:
				Revision:	Date:
Aircraft: **XX-YYY**	SYSTEM: Flaps Control			No.Drawing.:	Page:5
	ZONE: 200 UPPER FUSELAGE			No.Drawing.:	Pages: 6

Subz.	Subsubz.	Subzone Description	Interactions of Systems	Effect on System	Symptoms to: 1.Flight Crew 2.Ground Crew	Justification
260	261	Subzone is defined between the fuselage counters No.8 to No.11 in the upper part of the fuselage above the passenger cabin ceiling.	Fragments detached from rotating parts of the air conditioning system.	The result is an immediate interruption function of electrically controlled flaps. System is backed up by hydraulic control flaps, as appropriate, once ejectedflaps into position 45 °. Safety effect: **MINOR**	1. Pilot detects a problem only after intervention to the flaps control 2. The damage will be detected during the preflight inspection	Auxiliary rotor casing must be able to prevent damage caused by failure of the rotor blades with high energy according to § 23.1461.
			High temperatures or fire components adjacent to wiring harnesses.	Damaged insulation of electrical cables and short-circuiting cause of the complete interruption of the primary functions of control and indication flaps. System is backed up by hydraulic control flaps, as appropriate, once ejectedflaps into position 45 °. Safety effect: **MINOR**	1. Pilot detects a problem only after intervention to the flaps control 2. The damage will be detected during the pre-flight inspection	Electrical wiring insulation in fuselage is against the overheating of surrounding systems or fire retardant and not dripping, therefore it seems unlikely that it could lead to further spread of the fire in the fuselage. It is not expected that the smoke from the damaged insulation can have significant effects on work crew
			Leakage of hot air in system of collection air from the engines.			
			Leakage fluids at high pressure and temperature of the air conditioning system.			

Table 1: Simplified Zonal Safety Analysis

2.2 Particular Risk Analysis

Particular Risk Analysis (PRA) deals with the Particular Risks which are events or influences that are outside of the concerned systems, but may violate required independence of the system. Particular risk can cause and influence several zones at once, and therefore PRA can meet several zones at once, as opposed to the ZSA which is restricted to each specific zone. Some of these risks may be subject to specific airworthiness requirements (tire burst. etc.).

Some typical risks are:

- Fire
- Leaking Fluids (Fuel, Hydraulic, Water etc.)
- Lighting strike
- Tire burst, flailing thread
- Hail, ice, snow
- High temperature air duct rapture
- etc.

After identification of particular risks with respect to the design of the system, there should be a separate study for each risk. The objective of this analysis is to determined, if all effects on safety are identified and designed out or shown to be acceptable. Example of Particular Risk Analysis Summary report based on example from chapter 2.1 it´s on Tab 2.

Particular risk analysis

1.1 Tire burst

Tire burst occurs when the wheel is in contact with the ground produces tire tread debris. This may be projected in the wheel plane between 45° and 180° measured from ground horizontal plane in reward direction. In this addition, tire may be projected at up to 15° either side of wheel plane, spread on a Gaussian distribution.

Affected areas: Zone 100 - Lower Fuselage, Zone 700 - Gear Bay

The effect on system: Under normal circumstances, it is not expected to affect the electrical control flaps

Safety effect: NO SAFETY EFFECT

Justification: Harnesses of electrical cables and all components of the electrical control flaps are located outside the expected impact of tire debris.

Table 2: Simplified Particular Risk Analysis

2.3 Common Mode Analysis

Common mode analysis (CMA) is a qualitative analytical tool used to ensure the "goodness" of a design and it is performed throughout the safety assessment process. "*This analysis is performed to confirm the assumed independence of the events, which were considered in combination for a given Failure Condition The effects of specification, design, implementation, installation, maintenance, and manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered."*[4]

Common mode fault can fall into several categories which should be analyzed. Some typical common mode faults are:

- Hardware error
- Software error
- Production/ Repair flaw
- Installation error
- Maintenance error
- etc.

Example of Common Mode Analysis Summary based on example from chapter 2.1 it´s on Tab. 3.

COMMON MODE ANALYSIS (CMA)			Prepared by: *Rostislav Koštial*	Date: 16. 09. 2012
			Approved by:	Date:
			Revision:	Date:
Aircraft: **XX-YYY**		SYSTEM: Flaps Control	No.Drawing.:	Page: 1
		SUBSYSTEM: Electric Control	No.Drawing.:	Pages: 1
	Common Mode Source	*Common Mode Error*	*Justification*	
Concept and Design	Design architecture Technology, materials, equipment type Specifications	A common source of electrical energy for various electrical control circuits Flaps.	They used elements and materials certified for aviation. It is also used proven technologies of production and assembly, and performed independent output control. System is backed up hydraulic control flaps, as appropriate, once ejected flaps into position 45 °.	
		Use of elements of the same type-repetitive failures		
		Faulty system design, faulty technology, use of inappropriate materials or design values.		
Environmental Factors	Thermal and Mechanical Electrical and Radiation Chemical	Fault of electrical wing flaps control system created as a result of thermal and mechanical stresses, possibly due to chemical influences.	Installation is performed in accordance with the requirements AC43.13-AC43-1B and 2A. Used wires compliant MIL-W 22759/16 with operating temperatures up to 150 ° C. Cable routes are conducted when possible, away from areas with high temperature, mechanical stress or chemical influences. Electrical circuit designed with electromagnetically insensitive elements.	
		Fault of electrical wing flaps control system due to the aircraft hit by lightning or strong electromagnetic field with a subsequent power failure critical loads.	In case of overload and fire wire harness applies that this isolation is self-extinguishing when the temperature drops and not dripping, which significantly reduces the possibility of further spread of the fire in the fuselage. Also, it is not anticipated that the smoke from the damaged insulation could significantly affect the operation of the crew. Flame retardant cables are tested in accordance with the requirements of paragraph 23.1359 prescription.	
Manufacturing and Installation	Manufacturer Procedures Process	Fault of electrical wing flaps control system due to faulty manufacturing processes and assembly.	They will used certified manufacturing and assembly processes. To minimize repetitive errors during production and assembly will be applied to a system of independent quality control of production. Connectors and cable sets are labeled and conducted in such a way as to avoid their exchange	
Operation and Maintenance	Staff Procedures	Fault of electrical wing flaps control system due to faulty operating procedures or improper maintenance procedures.	Errors and failures are minimized by conducting checks at various levels after the prescribed period of operation. The various levels are meant control by the operator and manufacturer. In order to achieve maximum reduction of repetitive errors will be used at different levels of the different procedures.	
		Maintenance errors.		

Table 3: Simplified Common Mode Analysis

3 Using CCA in the Czech republic

Czech Republic is one of the largest producers of small transport aircrafts and ultralight aircrafts in the Europe. It has a long tradition in the manufacture of small transport aircraft. Requirements on safety and reliability assessments are less strict comparing to category FAR/CS-25. This is determined by using a simpler systems and more simple design arrangements. However, complex systems and designs which are typical for FAR/CS-25 aircrafts have been used in FAR/CS-23 aircrafts in past years. Installation of more complex systems has rising demands on reliability and safety assessment. Requirements and recommendations safety assessments for GA are divided into several classes (according to AC23.1309). This is based on the historical experiences. More information sees in Tab.4. AC 23.1309 also recommends analysis to prove safety and reliability. They include:

- Functional Hazard Assessment (FHA)
- System Safety Assessment (SSA)
- Failure Mode and Effects Analysis (FMEA)/Failure Mode, Effects and Criticality Analysis (FMECA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTR)
- Markov Analysis (MA)
- Common Cause Analysis (CCA)

Since recommendations of the regulation were created for large and complex aircrafts, it is not necessary the best option to use all analyses, especially for small airplanes. Using all analyzes could prohibitively increase the development budged without significant improvement in a safety and reliability of systems. It is responsibility of analyst to choose suitable analyses for the particular aircraft or system.

Classification of Failure Conditions	No Safety Effect	<---Minor--->	<---Major--->	<--Hazardous-->	< Catastrophic>
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	**Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development Assurance Levels (Note 2)**				
Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.
Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for Primary System (P) and Secondary System (S). For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.
Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.
Note 4. Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria.

Table 4: Recommendations of AC 23.1309, Source [1]

In past years some of the new CS-23 aircrafts were developed in the Czech Republic and Common Cause Analysis has been used in their development. Among these planes also belong VUT100 Cobra, AE-270 Ibis and EV-55 Outback. More information about these aircrafts are in Fig.3.

For VUT100 Cobra aircraft were used following reliability analyses [5]: FHA, FMEA, RBD and for the first time in the Czech Republic also CCA. Because this aircraft belongs to the Class 1 according AC.1309, it was necessary to create a simplified option of CCA. CCA were used for EV-55 in more detailed form. For significant systems there were performed preliminary CCA (PCCA). Content of this analysis is still not comparable in scale of large transport aircraft.

CCA used for GA aircraft are based on the document ARP 4761. Recommendations and guidelines described in this document are issued for large transport aircrafts. These analyzes are simplified in GA. The main simplifications are:

- There are selected only certain categories, conditions or elements from ARP4761 for the analyses. For example in Chapter 2.3 Tab.3 it is example of CMA which solves only

Concept and Design; Environmental effects; Installation and Manufacturing; Operational and Maintenance categories.

- We can simplify the writing of results. Results can be entered in tabular form (chapter 2.1 Tab.1 and Chapter 2.3 Tab.3), simply described in the text (Chapter 2.2 Tab.2) or combination of written and tabular forms.
- CCA does not have to be conducted during the entire development of the aircraft in GA. They can be used for the specific phase of development, for example they can be used in the detailed design phase of development of the new aircraft.

Aero AE-270 Ibis	**VUT100 Cobra**	**EV-55 Outback**
Seats: 10	Seats: 4	Seats: 9
Length: 12,23 m	Length: 8,00 m	Length: 14,35 m
Wing span: 13,82 m	Wing span: 10,2 m	Wing span: 16,10 m
Height: 4,78 m	Height: -	Height: 4,66 m
Wing Area: 21,00 m^2	Wing Area: 13,11 m^2	Wing Area: -
Empty Weight: 1788 kg	Empty Weight:-	Empty Weight: 2626 kg
Max. Takeoff Weight: 3300	Max. Takeoff Weight:1330 kg	Max. Takeoff Weight: 4600
Max. Cruise Speed: 409 km/h	Max. Cruise speed: 287 km/h	Max. Cruise speed: 408 km/h
Range: 2916 km	Range: 2000 km	Range: 2240 km
Classification (AC.23.1309): Class III	Classification (AC.23.1309): Class I	Classification (AC.23.1309): Class III

Figure 3: Information about airplanes Aero AE-270 Ibis, VUT100 Cobra, EV-55 Outback

Results of CCA are not strictly connected to safety related applications. MSG-3 mainly used for large aircrafts also started to be used in GA. Safety assessment and MSG-3 are closely linked and results obtained from the analysis of reliability (FHA, FMEA/FMECA, CCA) are very useful for application MSG-3 on aircraft. CCA are very useful for every group in MSG-3. Especially useful may be for a group of Systems/Powerplant and Zonal Inspections. IAE is involved in the application of the MSG-3 for small transport aircraft.

IAE-BUT (Institute of Aerospace Engineering – Brno University of Technology) closely cooperates with industry and cooperate with EVEKTOR Company in terms of developing aircrafts VUT-100 and EV-55. It was also involved in international projects CESAR and PPLANE where it dealt reliability assessment. IAE educates its student's safety and reliability in the subject Dependability of Aircraft Systems. In this subject, students learn basic information about the commonly used analysis and safety assessment methods in aviation. CCA can be very useful in implementation of Reliability Centered Maintenance.

4 Conclusion

The paper looks at safety and reliability of small transport aircrafts in the Czech Republic. Specifically, it deals with the use of CCA in recent years due to increasing complexity of aircraft systems. We can assume that this trend will continue in the future. CCA will become a common part of safety and reliability assessment accompanying the development of a small transport aircraft.

These methods have been used in the Czech Republic only in simplified form. It can be assumed that these analyses will be used in full range in the future. And these analyses will be implemented progressively throughout development of the aircraft.

The results of these analyzes can be useful for maintenance, especially useful for maintenance solution according to Reliability Centered Maintenance (RCM) and MSG-3. These methods of maintenance are about to be applied in GA.

IAE-BUT closely cooperates with the industry of the application by latest knowledge available in this field.

References

[1] Advisory Circular 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] ARP4761 *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, The Engineering Society for Advancing Mobility Land Sea Air and Space, Warrendale USA, 1996

[4] CS-25 *Certification Specification for Large Airplanes*, European Aviation Safety Agency, Cologne-Germany, 2010

[5] HLINKA, J. A0F301 Adaptace Progresivních Metod Analýz Spolehlivosti Soustav Letadel, BUT-IAE, LU63-2010-ARC.SY, 2011

[6] CS-23 Certification *Specifications for Normal, Utility, Aerobatic and Commuter Category Aeroplanes*, European Aviation Safety Agency, Cologne-Germany, 2012

[7] Information Standards for Aviation Maintenance, ATA iSpec 2200

[8] Operator/Manufacturer Scheduled Maintenance Development, ATA MSG-3, Revision 2005

[9] FINDA, J.; HLINKA, J.; WEISMAN, A. Relation Between Safety Assessment Methods and Reliability Centered Maintenance- Impact on the Aircraft Systems Architecture. Aerospace Proceedings. 2008. 2008(2). p. 9 - 14. ISSN\~1211-877X.

[10] FINDA, J.; HLINKA, J.; WEISMAN, A. Options for Interconnection of Safety Assessment Methods And Reliability Centered Maintenance in General Aviation. Paper ICAS 2010-10.10.3. 2010

[11] http://www.evektoraircraft.com