Taylor & Francis
Taylor & Francis Group

AVIATION
ISSN 1648-7788 / eISSN 1822-4180
2015 Volume 19(4): 180–186
doi:10.3846/16487788.2015.1128048

STANDARD AND FUTURE-POTENTIAL METHODS FOR SAFETY AND RELIABILITY ASSESSMENT ILLUSTRATED BY AN AIRBORNE ELECTRIC SYSTEM EXAMPLE

Luboš JANHUBA

Brno University of Technology, Faculty of Mechanical Engineering, Institute of Aerospace Engineering, Brno, Czech Republic
E-mail: janhuba@fme.vutbr.cz

Received 29 September 2014; accepted 1 December 2015

Luboš JANHUBA
Education: Brno University of Technology
Affiliation and function: post-graduate student at Brno University of Technology since 2011.
Research interests: aircraft design, safety and reliability, airborne systems.

Abstract. This paper is focused on the description of complex airborne safety and reliability assessment methods mostly used in general aviation. It is a short presentation of standard approaches, principles and methods for the evaluation of aircraft critical systems. There are many techniques that may be used during safety and reliability assessment of an airborne system.

The complexity of airborne system components and their interconnection is rapidly growing. System safety assessment is an essential part of an airplane certification process. Therefore, the means of safety and reliability have to evolve. This paper presents one of future potential concepts of safety and reliability analysis.

The conclusion of this paper gives a brief summary of a standard and a future-potential technique.

Keywords: airplane, airborne system, reliability, safety, analysis, electric system, general aviation.

1. Introduction

Nowadays airborne systems are becoming more and more complex and sophisticated. Hence, the safety and reliability analysis has to evolve and adapt to the extended complexity. It is essential to find a proper balance between various approaches and techniques of safety and reliability, followed by an appropriate evaluation method.

In the past two decades, Brno University of Technology Institute of Aerospace Engineering (IAE) has participated in several projects focused on the safety and reliability analysis of sophisticated aircraft systems, such as electric systems. Therefore, in this paper the aircraft electrical system (AES) is chosen for the demonstration of advanced safety and reliability evaluation methods. However, the presented certification requirements, safety assessment methods and interpretations of results are mostly applicable to the aircraft systems in the field of general aviation.

2. Complex system definition

The most fundamental question to be raised at the beginning of this paper is – what is a complex or, more precisely, a sophisticated system? The best way to get the answer is to begin with the definition proposed in the FAA advisory circular 23.1309-1E, where a complex system is defined as:

"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" (FAA 2011a).

This definition is applicable to these systems: avionics systems, flight control system, hydraulic and pneumatic systems, electric systems etc.

The structured assessment methods are the tools for the examination of system integrity and reliability. There are several diverse methods based on a few basic principles. The approach of these methods can be either predictive or inductive. In some cases, it is sufficient to quantitatively evaluate and describe a system, but, in the safety assessment of essential airborne systems, it is necessary to use both qualitative and quantitative methods.

3. Problems and issues

Generally, the system safety assessment is a long, expensive and difficult process. Nevertheless, the development of a modern general aviation airborne system (flight control system, fly-by-wire, engine utility system, etc.) has already reached the stage where it is not possible to avoid the safety and reliability process (at least at a minimal level). This is due to the fact that with the increase of the level of complexity the level of interconnection has been elevated as well.

Now safety and integrity analyses have to be undertaken to ensure that the system meets the necessary safety goals, and a variety of other trades studies and analytical activities have to be carried out (Moir 2003).

4. Certification requirements

The paper deals with the certification process, and the safety and reliability assessment of a general aviation aircraft system, but what is general aviation?

In North America, most operations using general aviation aircraft used for for-hire passengers and/or cargo service are certified under the FAR part 135 (National Air… 2014).

In the European Union (EASA) the term "General Aviation" is considered to be equal to the EASA CS-23 category. EASA CS-23 covers airplanes in the normal (limited to non-aerobatic operations), utility (limited operation due EASA 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), and advisory circular AC 23. 1309-1E (recent). The advisory circulars are not mandatory and do not constitute regulations. It is a set of acceptable means for demonstrating compliance with applicable regulations (EASA CS-23).

The concept of failure condition consequence classification is derived from upper FAR 25 or EASA CS-25 aircraft class (see Fig. 1). Advisory circulars have established the definitions for the classification of failure conditions, relationship between probabilities, and severities of failure conditions. Further ACs describe the safety assessment objective, which is to ensure an acceptable safety level for equipment and systems installed on an airplane (FAA 2011a).

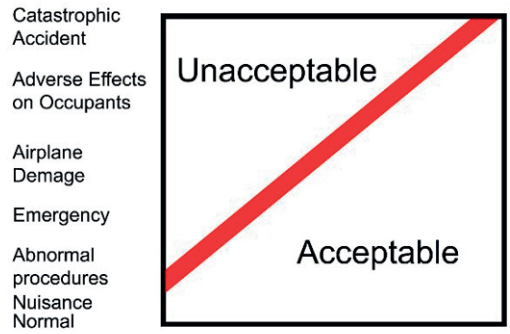

Fig. 1. FAA AC 25.1309 Probability vs. consequence graph (FAA 2011a)

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

The FAA AC 23.1309-1E classification of failure conditions is:

(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 be extremely improbable.

For example, the failure conditions of the selected case study of an AES (EASA CS-23 Commuter) are:

- **Minor** failure condition – failure of one generator;
- **Major** failure condition – simultaneous failure state of two generators;
- **Hazardous** failure condition – simultaneous failure state of two generators;
- **Catastrophic** failure condition– simultaneous failure state of all power sources.

The advisory circulars are based on related industrial documents, such as the SAE ARP 4754A (Guidelines for Development of Civil Aircraft and Systems), SAE ARP 4761 (Guidelines for Development Conduction of 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 the demonstration of compliance with applicable regulations. It is up to each analyst to choose appropriate assessment procedures, methods and evaluation means.

5. Airborne electric systems

At first it is necessary to describe a typical aircraft electric system, although an aircraft electric system is unique and is designed to meet specific requirements. In general aviation (namely EASA CS-23 Commuter Class), most of airborne electric power systems consist of at

least three separated power sources. This is designed as a safety measure as a two channel system. The main electric power comes from DC generators connected to the aircraft engines; reserve power comes from one or two batteries. The electric system of a typical general aviation aircraft is further divided (as illustrated in Fig. 2. General aviation generic system).

DC generators are used for generating the required voltage (usually 28V DC) to supply aircraft electric loads. The generators are driven and controlled by the Generator Control Units. Those units provide a fully automatic control during the start of engines and transition to the generator mode, regulate the generator output voltage, control parallel function and provide a protective function.

The generated power is distributed by a primary electric distribution system (sequence of relays, contactors, fuses etc.) to the main buses (basically electrical sockets). Airborne batteries are usually connected to those main buses as well.

The secondary electric distribution system is connected to the primary system by the main buses. The generated power continues to the essential and non-essential buses. Non-essential buses are used to supply aircraft systems which are concidered non- essential to maintain safe flight and landing. In contrast, essential buse supply systems are indispensable to continue the control of a safe flight and landing, such as basic avionics instruments, engine instruments, radio transmitter, etc.

The aircraft electric system is mainly defined as being complex and conventional (its function, technological means to implement its function, and its intended usage are the same as, or closely similar to previously approved systems that are commonly used (FAA 2011a)). Typically, a functional hazard assessment (FHA) establishes the following important failure conditions.

Table 1. Generic electric system failure conditions

Generic electric system
(1) Failure of one generator
(2) Failure of one generator without indications
(3) Simultaneous failure state of two generators
(4) Simultaneous failure state of two generators without indications
(5) Failure of one or both batteries
(6) Simultaneous failure state of all power sources
(7) Simultaneous failure state of all power sources without indications

Table 2. Electric distribution system failure conditions

Electric distribution system
(1) Partial loss of bus-bar due to failure state (loss of power supply to part of substantial appliances connected)
(2) Total loss of bus-bars (loss of power supply to substantial appliances connected)
(3) Total loss of bus-bars without indications
(4) Failure of main bus tie- false indication (connection of the both main buses)
(5) Failure of main bus tie without indications (connection between main buses)

The presented failure conditions are applicable for EASA CS-23 Commuter class twin engine aircraft with a two channel electric system. Two main buses are usually connected together for cross-function by a "Bus Tie" contactor. The classification of the failure conditions depends on system specifications (see Table 1 and Table 2).

For instance a single engine VUT 100 (EASA CS-23 normal class) aircraft's electric distribution system consists of one main distribution bus and one essential bus. The essential bus is connected to the alternator and airborne battery. Essential avionic equipment is supplied by the essential distribution bus. The function and certification requirements are different for twin engine commuter aircraft, so the depth and processes of the analysis are diverse.

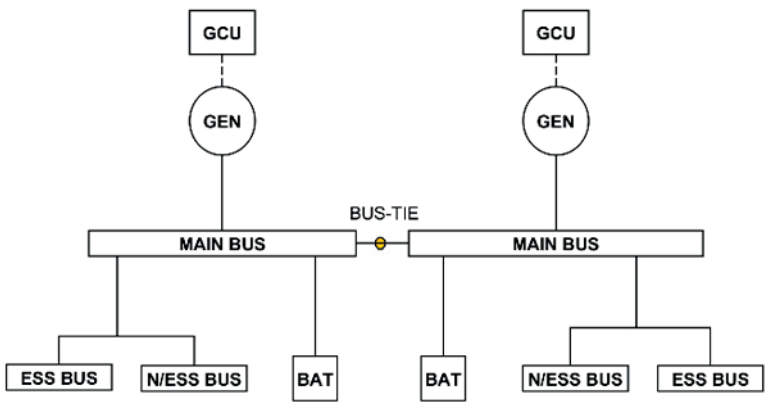

Fig. 2. General aviation generic system

In the case of complex airborne systems, which are unique for each particular aircraft, it is imperative to pay attention to the system specifications, required function and safety and reliability assessment.

6. Standard safety and reliablity analysis techniques

This chapter gives a brief overview of standard reliability tools, which are used during the safety assessment of a complex system, in this case an electric system.

The assessment process starts with the identifications of system requirements, design specifications and functional principles. The approach and depth of the analysis have to be in compliance with these requirements. The following methods are described according to their use in safety assessment.

6.1. Functional hazard assessment

Functional Hazard Assessment identifies potential system failures and the effects of these failures. The failures are tabulated and classified according to their possible effects, and the safety objectives are assigned according to the criteria (Moir 2003).

This analysis creates the basis for the determination of individual system criticality during the first phase of development of an aircraft. The analysis also defines the system specification which will be the subject of a further quantitative analysis.

In the previous section of this paper the top level AES failure conditions, like failure of one generator, partial loss of bus-bar, simultaneous failure state of all power sources, etc., were described. The failure conditions were identified during the functional hazard assessment. During the development phase of the project basic requirements were identified and a preliminary draft of an electric system was established.

6.2. Failure Mode and Effects Analysis

The FMEA is a structured, qualitative method used for the identification of the failure modes and the effects on system operations. It was created within the study of military system malfunctions in 1950s.

It is probably the most used reliability analysis method. The principle of the FMEA is to consider each mode of failure of every component or function of a system and to assert the effects on system operation of each failure mode in turn (O'Connor 2002).

There are three basic FMEA levels – Functional, Design and Process. It can be extended from being only a qualitative technique to a quantitative technique by adding a criticality level. The analysis procedure and structure is described in detail in SAE ARP4761.

In the process of aircraft electric system evaluation, the FMEA is the most important part of the analysis. The FMEA analysis describes the failure modes of each element considered in the system safety assessment. The FMEA identifies the critical elements and functions, which should be analyzed in the necessary depth.

6.3. Reliability block diagrams

The reliability block diagram assessment method shows the logical concession between the componets of the system. A block diagram is a special kind of pseudo graph. It is used for the modeling of a system with an assumption that the *system will operate if any sequence of components operates.*

The system is described within a serial (AND gate) and a parellel conection (OR gate).

Block diagrams can also be used for the description of a failure condition. In this case the serial conection represents the OR gate, whereas the parallel conection – the AND gate.

In the system safety assessment of an electric system, the RBD is used for difficult convectional failure conditions, such as a total loss of bus-bars supply without indications or a simultaneous failure state of all power sources without indications. Failure of one main bus supply block diagram shows a block diagram of a failure of one main bus supply (Fig. 3).

The RBD analysis is highly useful in the analysis of a traditional electric system which consists of separate elements.

6.4. Fault Tree Analysis

The Fault Tree Analysis (FTA) is a deductive, top-down method based on oriented graphs and Boolean logic. This method was created during the development of the intercontinental ballistic missile LGM-30 Minuteman in 1960s. The fault trees are used to represent important failure modes identified by the functional hazard assessment.

The Fault Tree Analysis uses probability to assess whether a particular system or architecture will meet

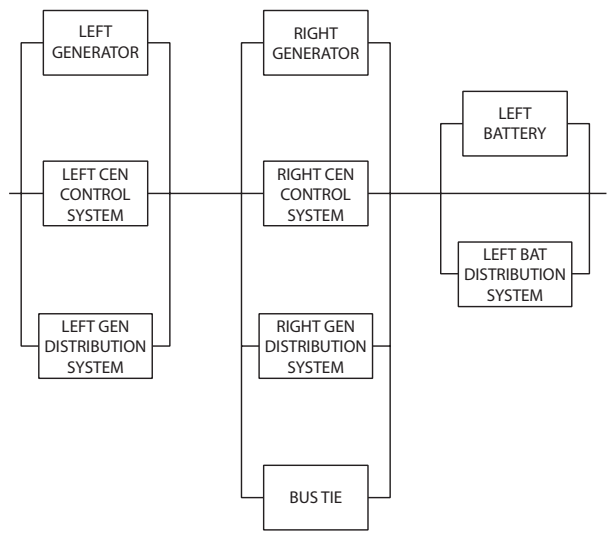

Fig. 3. Failure of one main bus supply block diagram

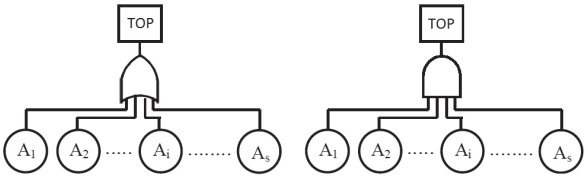

Fig. 4. FTA Left AND gate, right OR gate

the requirements. It starts with the consideration of the system failure effect, referred to as the "Top Event". The analysis proceeds by determining how these can be caused by individual or combined lower level failures or events (O'Connor 2002; Moir 2003). The procedure and structure of the analysis is also described in detail in SAE ARP4761 (1996).

The Top Event is a failure condition, such as a simultaneous failure state of all power, in the case of an electric system.

Figure 4 shows two basic gates. On the right side is the AND gate, where the output TOP event occurs only if all inputs occur. On the left side is the OR gate where the output occurs if any input occurs.

The Fault Tree Analysis is the "ultimate weapon" in the assessment of a modern modulated electric system consisting of replaceable units, adaptive configuration and additional elements.

7. Common Cause Analysis

According to the ARP4754A, the Common Cause Analysis (CCA) establishes and verifies physical, functional separation, isolation and independence between systems and items. The CCA techniques are an extension of a deductive safety assessment targeted to the detection of dependence between events which would otherwise be treated independently. Generally, the CCA analyzes the 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 – the Zonal Safety Analysis (ZSA), the Particular Risk Analysis (PRA) and the Common Mode Analysis (CMA).

7.1. Zonal Safety Analysis

It consists of the consideration of the installation aspects of individual systems and components and the mutual influence between several systems/components installed in close proximity in the aircraft.

The conclusions of the ZSAs will provide inputs to the relevant system safety assessment (ARP4754 1996).

In the ZSA process the airplane is divided into physically and functionally separated zones, according to the SAE ARP 4754 (Fig. 5). The ZSA is focused on the interaction between systems, for example, the influence of a hydraulic system failure on the electric wiring (system), etc.

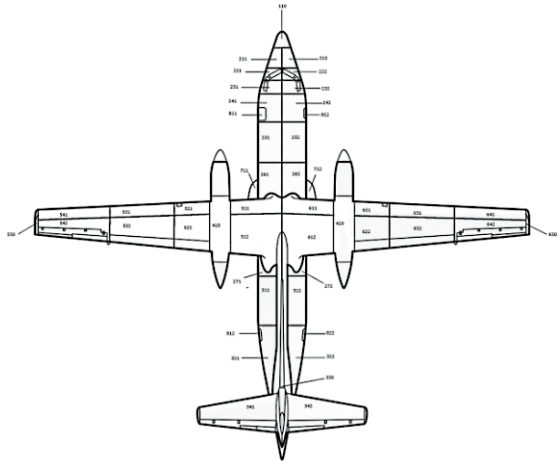

Fig. 5. ZSA aircraft zones (Koštial 2012)

7.2. Particular Risk Analysis

The task of the Particular Risk Analysis is to assess the aircrafts design for external threats that may compromise a continued safe flight and landing (ARP4761 Particular Risk Assessment). These threats are limited to those external to the system in question (ARP4754 1996).

7.3. Common Mode Analysis

The CMA contributes to the verification that independent principles have been applied when necessary. Consideration should be given to the independence of functions and their respective monitors (ARP4754 1996).

7.4. When is the CCA needed?

The answer is simple. The CCA is needed when it is necessity to prove that several components can fail (or just became unavailable) due to a particular cause of failure which generates the condition for multiple components to be affected by the same cause (NRC 1988).

8. System safety assessment

The system safety assessment in the case of an EASA CS-23 airborne system begins when the development process reaches the system level (Fig. 6). The aircraft requirements are already identified. The preliminary functional hazard assessment identifies potential system failures and their classifications. The design team prepares a solution (system design). The FMEA analysis

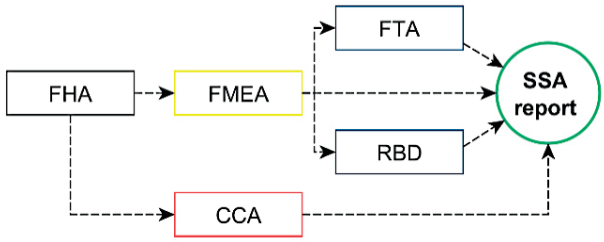

Fig. 6. The SSA process for an EASA CS-23 system

considers each mode of failure of every component or/and the function of a system and asserts the effects on system operation of each failure mode. A failure condition with a catastrophic and hazardous classification has to be analyzed by the FTA or RBD. The Common Cause Analysis is carried out parallel to the previous process. After this first phase there is a system verification and an aircraft verification.

9. Future-potential assessment technique

The safety assessment process still relies almost exclusively on human judgment (especially in general aviation safety assessment). The recommended practices defining the processes for system modeling and safety assessment are based on the understanding of a particular system by analysts. The review of many system components, assemblies, element functions, followed by the assessment of each failure modes and their resulting effects on the system is a complicated process.

The reliability assessment in the field of modern aviation involves an analysis of a huge number of mutually connected elements of a different system. Each system affects other systems in a different way.

A future-potential method (based on the author's opinion and experience) of how to represent and easily assess any complex airborne system uses a simple mathematical tool – a graph theory. It is natural to represent a system by drawing a graph. A set, consisting of points together with lines joining parts of these points, represents a particular system and its interconnection.

Logically, this method is based on various similar possible methods that were suggested by several research and development groups.

The most promising starting point for developing an advanced way of how to model and evaluate a complex airborne system is the technique described in the article *Mechanical system reliability analysis using combination of graph theory and Boolean logic* (FAA 2011b).

The suggested reliability technique using a combination of graph theory and Boolean logic provides an easy accessible system representation along with a qualitative evaluation of the system's interconnection and reliability (Tang 2001).

It is possible to utilize the system representation in the form of a graph as a universal data structure for the safety and reliability assessment.

The author intends to develop an integrated algorithm for the system safety assessment of airborne systems in his dissertation thesis. This algorithm should serve as (partially at the beginning) a computerized means which makes reliability analysis easier and more effective with much more consolidated results. Together with the application of fuzzy criticality assessment, the suggested algorithm should be applicable during the whole safety and reliability process even in the case of an insufficiency of reliability data (failure rate, reliability, etc.) (see Fig. 7).

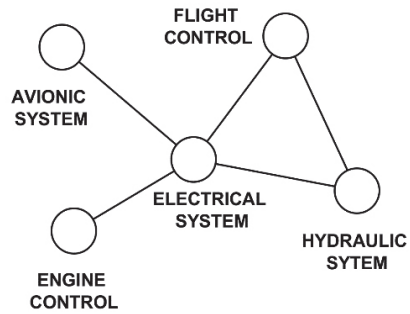

Fig. 7. Graphic representation of a system

Using common tools for graph creation, such as general-purpose diagramming programs (for instance with results in the XML format) and open source programing languages like Python, it is possible to establish an accessible parametric model of a particular airborne system.

Generally any future-potential techniques for the assessment of airborne systems should overcome the disadvantages of standard reliability techniques, such as extensive time consumption and inconsistent results (in the case of a complex system). The presented method is one of the possible techniques.

Conclusion

This paper gives an overview of standard safety and reliability assessment methods used during general aviation aircraft development, and presents a system safety assessment process illustrated by an electric system example. Standard safety and reliability assessment techniques became obsolete in the term of effectiveness. Modern airborne system are deeply interconnected. Common procedures assess separated system. The influences of other system is then analyzed separately (for instance in zonal safety analysis).

Discussed future potential safety and reliability method can be useful in order to overcome standard methods disadvantages like huge extensive time consumption and inconsistent results.

Acknowledgements

The research leading to these results has received funding from the MEYS under the National Sustainability Programme I (Project LO1202).

References

ARP4754. 1996. *Certification considerations for highly-integrated or complex systems*. Warrendale, USA: The Engineering Society for Advancing Mobility Land Sea and Space.

ARP4761. 1996. *Certification considerations for highly-integrated or complex systems*. Warrendale, USA: The Engineering Society for Advancing Mobility Land Sea and Space.

Federal Aviation Administration (FAA). 2011a. *System Safety Analysis and Assessment for Part 23 Airplanes,* Advisory Circular AC 23.1309-1E, Washington DC, USA.

Federal Aviation Administration (FAA). 2011b. *System Safety Analysis and Assessment for Part 25 Airplanes*, Advisory Circular AC 25.1309, Washington DC, USA.

Koštial, R. 2012. Use of common cause analysis in the Czech general aviation, in *Research and Education in Aircraft Design*, 17–19 October 2012, Brno, Czech Republic.

Moir, I. 2003. *Civil avionics systems*. 1st ed. Chichester: John Wiley. 395 p.

National Air Transport Association. 2014 [online], [cited 18 September 2014]. Available from Internet: http://www.nata.aero/

NRC. 1988. Procedure for treating common cause failures in safety and reliability studies*, NUREG/CR-4780* 1(2).

O'Connor, P. D. 2002. *Practical reliability engeneering*. 4th ed. Chichester: John Wiley. 513 p.

Thang, J. 2001. Mechanical system reliability analysis using combination of graph theory and Boolean logic, *Reliability Engineering and System Safety* 72: 21–30.