Improve Your Knowledge (IYK)

The Core of the SAE ARP 4754A

Berquó, Jolan Eduardo – Electronic Eng. (Technological Institute of Aeronautics - ITA)

- *Aerospace Product Certifier (DCTA/IFI)*
- *Government Representative for Quality Assurance – RGQ (DCTA/IFI)*
- *Post-graduated in Reliability Engineering and System Safety Engineering (ITA)*
- *Specialization in Systems Engineering and Analysis (Italy)*
- *Participation in the joint development program (Brazil-Italy) for the AM-X military fighter-bomber aircraft*
- *Experience of one decade as an engineer responsible for off-line maintenance of electronic systems and aircraft instruments*
- *Logistic Technical Support manager in Embraer*

Dec,15 2020

The avalanche of highly complex avionics systems, which are currently installed on aircraft, has, by its nature, promoted a revolution in the aircraft system development process, which has eliminated a major concern from the aviation industry and certification authorities, giving rise to ARP 4754A, which describes this new process to solve the safety problem of these systems. This is the ***core*** *of ARP 4754A, which will be summarized in this MSC.*

What is a complex system? It is one that cannot be properly analyzed by so-called known structured analyzes, such as the conventional FMEA analysis (Failure Modes and Effects Analysis). Such is the functional sophistication of today's complex systems that these conventional analyzes fail to detect errors that can lead to serious safety problems.

In fact, the current proliferation of highly complex systems, with their items containing integrated circuits (chips) with a very high density of functions, makes an FMEA absolutely ineffective to analyze the items of these systems. But these types of analysis, it should be noted, continue to apply well to simple systems.

An example of a highly complex system is the Primary Flight Information System, which presents on an electronic display, among others, information from avionics systems that are also complex, such as ADS (Air Data System: altitude, direction) and AHRS (Attitude), Heading Reference System: attitude, direction), both integrated in a digital bus, which forwards your information to the mentioned display.

Depending on weather conditions, an error in the design of these integrated systems can have tragic consequences for the flight.

Another example is the Fly-By-Wire hybrid avionics flight control system with mechanical parts (control surfaces), actuators and the system brain: the Flight Control Computer - FCC. The complexity of the system is attributed to the FCC.

The guidance material presented in DO 178B (software design) and DO-254A (electronic hardware design), with its rigorous process for developing items in these systems, was recognized by the industry and by several regulatory authorities as sufficient to establish the necessary confidence levels of absence of design errors in these items (see the first edition of ARP: ARP 4754).

The fact is that, in view of this incessant growth in complexity of the systems, it became clear the need to establish confidence levels for the design, not only for items, but for all levels of the aircraft.

Thus, the so-called Development Assurance Process (DAP), applied to aircraft, Systems and Items has emerged. This is the ***core*** *of the ARP 4754A.*

It is important to note that the assignments of the development assurance level depend, promptly, on the classification of the failure conditions of the aircraft level functions, which are identified in the Safety Assessment Process (Safety Assessment Process - PSA). Thus, the PSA is part of the DAP.

We must take into account that a failure condition can be caused by one or more failures or by one or more design errors. Regarding the failures and before the advent of ARP 4754A, the PSA, in the case of complex systems, already required the manufacturer of systems and items to contain the failures, through a project assurance project (Design Assurance Level - DAL) , suggesting to these manufacturers the use of DO-178B and DO-254A.

However, when it comes to design errors, they are mitigated by the DAP. Finally, the PSA forces the manufacturer of systems and items to contain the failures; but, in the case of complex systems, there is usually only one way out: the DAP, which, as we have seen, also applies to the design of system items.

Safety requirements are functionally identified at the aircraft, systems and item levels. At the aircraft level, they are those generated in the AFHA (Aircraft Functional Hazard Assessment), from the aircraft functions generated in the functional analysis (Functional Analysis). Eg: Provide Directional Control on the Ground; Provide Ground Deceleration, etc. At the systems level, they are those generated by the FHA system level (SFHA - System Functional Hazard Assessment), based on the AFHA. Ex .: Provide Wheel Braking. At the item level, they are those arising from the PSSA.

The Common Cause Analysis (CCA) is also part of the PSA and occurs at each stage of this process, to ensure independence between functions or to accept certain dependencies, through considerations discussed in their analysis.

The assurance levels for the aircraft development of the aircraft and systems are characterized, in the DAP, through the Functional Development Assurance Level (FDAL), depending on the severity of the aircraft level failure conditions.

The following table shows the characterization of these levels, according to the failure condition:

Failure Condition	FDAL
• Catastrophic	A
• Hazardous	B
• Major	C
• Minor	D

Regarding the system items, the development assurance levels are characterized in the Item Development Assurance Level (IDAL), guiding the item's design rigor, as provided for in DO-178C and DO-254A.

The ARP presents the way to allocate the FDAL to the respective system that will perform the function under analysis and, from the system, the allocation of IDAL to the items in the system.

Nowhere does the ARP make considerations about failure rates, as in the case of the PSA; what matters in DAP is the severity of the effects of a failure condition.

Well, dear reader, we stop here, in this MSC. Our goal was to present the core of ARP 4754A and show its importance, when dealing with the safety of complex systems. We would just like to add that the study of ARP, in totum, is an arduous task. It requires a lot of concentration, considerations and reconsiderations, until the correct understanding of each item and paragraphs.

By the way, we are preparing material related to this ARP, which we titled "Interpreting the Vision of the Industry and Aviation Authorities in ARP 4754A". It is a meticulous work, in which we will try to clarify paragraph by paragraph, seeking to facilitate the understanding of those interested in familiarizing themselves with this important document.

As this MSC was developed in the month of December (2020), we end by thanking and wishing everyone a Merry Christmas, a prosperous 2021 year and a lot of health for you and all your family.

References:

1. ***SAE: ARP 4754*** *– Certification Considerations for Jighly-Integrated or Complex Systems, USA, November 1996.*

2. ***SAE: ARP 4754A*** *– Guidelines for Development of Civil Aircraft and Systems, USA, December 2010.*