Improve Your Knowledge (IYK)

System Safety Assessment (SSA): Science or Art?

***Berquó**, Jolan Eduardo – Electronic Eng. (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)
jberquo@dcabr.org.br/jberquo@uol.com.br

YIK 62– Jun 10, 2017

Here we are again, this time hammering in the System Safety Assessment (SSA), a subject we recently explored in some depth, in the three modules of PDC-01 - "Interpreting the Civil Aviation Authority's Vision in the Safety Assessment Process".

Because it is a controversial theme (and always will be), among those who dedicate to this area, we decided to explore the subject further, seeking to improve the understanding of all who are interested in the subject. We will try to answer the question contained in the title of this IYK: After all, how would we classify the Safety Assessment Process? Science or Art?

The theme may seem irrelevant, but we do not consider it that way. It is important for those who decide to enter this area, or even for those already in it, to have a conceptual view of the SSA process, avoiding even possible frustrations.

First, a little history of SSA. Prior to 1960, the SSA was performed through the now legendary FMEA (Failure Modes and Effect Analysis). The SSA landscape changed when the Concorde project emerged in 1960. It was noticed that there was a great functional interaction, due to the integration of systems, i.e., there were systems whose functions depended on the functions of other systems. The functional approach of the current SSA then emerged. A new era was emerging.

However, the FMEA did not leave the scene; Just changed level. Once unique, it now enters the stage where it is necessary to demonstrate that the equipment of a system meets the security requirement allocated to said system.

At this point, we will present here the objective of SSA, as evidenced by the current regulations of the Airworthiness Authorities (FAA, EASA and ANAC). It is SSA's goal:

"To Demonstrate to the Authority that aircraft systems and their equipment, considered separately and in relation to other systems, are designed in such a way that:

(1) any Catastrophic Failure Condition
   a. Is extremely improbable; and
   b. Does not result from a single (singular) failure.
(2) any Hazardous Failure Condition is extremely remote; and
(3) any Major Failure Condition is remote."

It seems very simple, but when the SSA process is analyzed in its details, the doubts arise. For example: "which means Extremely Improbable, Extremely Remote or just Remote"? If the Authority simply left these safety requirements thus expressed, there would probably be an avalanche of questions as to the subjectivity of the interpretation of one and the other.

It seems to be reasonable to believe that this was the reason for the quantitative requirements arose, that is, that numerical values, or rather numerical values of probabilities, with maximum permissiveness limits were inserted for each Failure Condition.

This insertion of probability bands, as we discussed in previous IYK and PDC-01, was based on the statistical analysis of catastrophic accidents in the 1970s, with the conclusion that

the systems were responsible for only 10% of these accidents.
Did the subjectivity stop there? No. Given the qualitative and quantitative requirements, the Applicant, quite naturally, must have asked: "So, how do I demonstrate this?"

So, came the Authority's help, through suggestions to the Applicant to demonstrate the compliance of their systems with the quantitative and qualitative safety requirements. This assistance came through the Advisory Circulars (FAA) and similar documents of other Authorities.

Not satisfied with the content of these documents, the Aeronautical Community addressed the issue and, with the assistance of SAE Aerospace, established the S-18 and WG-63 committees (Working Group 63) to develop SAE ARP 4754 (Ref. 1) and SAE ARP 4761 (Ref. 2).

The development of document ARP 4754 was attended by three Brazilian members (ANAC, Embraer and CTA-IFI). The development of ARP 4761, on the other hand, was not attended by Brazilian representatives.

These documents, although written with good intention, in our opinion did not alleviate much the difficulties of the Applicants. Controversies in the interpretation of the subject have continued, and so it is today. It is difficult to find two Safety Assessment analysts with the same interpretation. This difficulty is generated by subjectivity in the interpretation of the SSA process.

We have chosen the way to focus on the suggestions of the Authorities (AC's and similar documents from other Authorities), counting on the support of the mentioned ARP's.

This difficulty of harmonizing the positions of several analysts led us to consider SSA more as art than science. The fact is that an unambiguous methodology is not achieved. For the most part, it remains to the skill or genius of the Analyst. The final decision, of course, will be of the Authority

What is well established is the chain of process steps, going through the following sequence of assessments: FHA (Level of Functional Hazard Assessment) aircraft level, FHA level systems, PSSA (Preliminary System Safety Assessment) and SSA (System Safety Assessment) and CCA (Common Cause Analysis). But, the way they are performed, again, depends on the skill of the analyst. Some omit important considerations, while others go over the details, making the process cumbersome.

This is our interpretation. Nevertheless, we leave the reader free to oppose it. We would be very pleased to hear the arguments from other points of view.

This discussion will also be part of the course we will be conducting on PDC-01 at DCA-BR in July of this year.

Thank you

References:

(1) *SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems , USA, 2010*

(2) *SAE ARP 4761 - Guidelines and Method for Conduction the Safety Assessment Process on Civil Airborne Systems and Equipment, USA, 1996.*

(3) *FAA: AC 25.1309-1A, System Design and Analysis, USA, 21/06/1988.*

(4) *FAA: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes, USA, 2011.*