Improve Your Knowledge (IYK)

Safety Assessment: Conversations with Applicants and Certifiers – I

***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 54 – JUL 13, 2015

When we were students of electronic engineering course in ITA (São José dos Campos), in the decade of 70, we had the opportunity to hear from some teachers a few lapidary phrases. One of them, said in the basic course (first two years), said: "In this world, only the simple things are important." It is with this spirit that we have written our MSC; but this in particular by complication as it has been presented by others, we are much more aware of these teachings.

Some might be thinking, "but what Safety Assessment (SA) has to do with the above sentence"? Answer: a lot to do, not only with SA, but with everything that comes in our professional lives and, perhaps, in the routine of our family and social life. However, we want to demonstrate herein as much as we can, that SA is not that complication which we see in the daily activities of safety systems.

To begin with, we present what we mean by the Assessment and Analysis terms, in order to serve as a "North", in relation to the theme, in the course of this MSC.

Our understanding, which shares with that of AC 25-1309-1A (Ref. 1) or 23-1309-1E (REF. 2), Federal Aviation Administration, is that Assessment is a set of analyses, which, in this context, allows us to assess the safety of the design of a system. However, under the mathematical point of view, we know that a set can contain one or more elements. In the special case of a single element, the set is called unitary; despite of having one analysis, it can be called Assessment.

Now, let's go to the subject.

The term Safety Assessment does not impose a particular methodology, but a philosophy relevant to safety systems. It is up to those who propose to develop it and execute it, do it the best way they can. Suggestions of the universe, of course, will always be very welcome, but its final modeling depends on each area that is willing to develop it.

One thing is certain: whatever the methodology to carry out a safety assessment, it necessarily starts with a binomial analysis, namely: Hazard Analysis (HA) and Risk Analysis (RA), which, taken together, call for Risk Assessment. There is no getting away from it. Understand this, believe me, is to overcome the first barrier or milestone of an SA.

In fact, we wonder: what we are trying to do, all the time in our lives, in terms of safety? We're looking for, we believe, consciously or subconsciously, identifying hazards and assess the risks (consequences), as for example: death, minor injuries or more or less severe, leading to physical disability or not, etc.

Well, when we want to identify the level of these consequences, we are trying to know the severity those consequences. Is it or isn't it simple? However, if we want to complicate, it is easy.

When someone says that will conduct a Safety Assessment of a system any, necessarily have to perform first a risk assessment (HA and RA). It is pacific point.

How to do this? Well, that's another speech. We said so far, "what has to be done"; now we will talk about "how it has to be done."

With this purpose, let us consider an aircraft because it, for us, is more familiar; however, the discussion can be extended to any system, with the necessary adjustments in the area referred to, what needs to be done very well, we repeat, very well done, to avoid difficulties in the development of the assessment.

Well, we know that for an aircraft to take off and reach a destination safely, it has to be under the command of a pilot, which commands and controls the aircraft. This is simple, but fundamental: command and control of a pilot, this is the focal point.

It is with this focus that an aircraft is designed, that is, with systems providing pilots active means to command it and control it. Such media are the functions of the aircraft. Just to name one, presented by its simplicity in others MSC: "Display the pilots their spatial orientation," or "Indicate to the pilots the attitude of the aircraft."

There are, however, many other functions, all within the concept of presenting means to the pilots for controlling and commanding the aircraft.

Another important factor is that in the case of an aircraft, the pilots coexist with it, or are in its interior; in another words, they are an integral part of it. Any carelessness on the command and control can lead to an accident; they know that it will be reflected in themselves, which allows us to say that they are one of the targets, so their concern about the risks is certainly enormous.

That said, let's focus on this our first evidence: functions of an aircraft. There are several functions which are repeated in a given class of aircraft; however, each design is a design. Thus, the first concern of the analyst is to identify each function clearly. This is done with the help of the people of the systems engineering area. It is a task that has to be comprehensive, that is, at the end we cannot have doubt that we have all the functions identified. We emphasize: we cannot go ahead without this task be perfectly executed.

After fulfilled, meticulously, the task of identifying the aircraft functions, safety analyst asks the question, valid for all functions, "What can go wrong if this function is lost or has a distortion because of a failure "? At this point, the analyst is starting the search for hazards.

Well, we stopped here. We will continue in the next MSC.

Thank you.

References:

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

(2) **FAA**: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes, USA, 11/17/2011.