Safety: There is Something New on the Horizon

***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 51– JAN 15, 2015

In the IYK 48, we talked about the causes of catastrophic aviation accidents. We put there the human being as the main responsible for this. We said even that only 10% of these accidents could be assigned to systems, while the human being would be responsible for approximately 80%. Now that we have a kind of wave of catastrophic accidents, we consider appropriate bring it up again, since we have good news, in our opinion, in this area of prevention (Before the fact), where the human being is the main focus. Let's talk a little about that in this IYK.

We're always concerned about the preventive safety of aircraft or any other type of system. We have seen their respective methodologies and analytical techniques bringing improvements in this area, focusing, however, only 10% of the catastrophic accidents, i.e. the percentage assigned to the aircraft systems.

The latest at FAA recommended use and that is contained in the ARP 4754, and more specifically, in the ARP 4761. They are tasteful documents, but refer only to the aircraft systems. The objective is to eliminate or alleviate the effects of system failures. There are techniques used in ARP 4761 which are in focus for more than 50 years.

Not that we are against these techniques; rather, they are excellent for the purposes of their proposal: risks of failures of aircraft systems. However, what is in our minds is what to do with human error, especially those of the crew. We have thought much on how to attack this kind of problem.

Okay, we see a new methodology in this context, now thinking actually in the triad human, machine and the environment. We can say then that there is something new on the horizon. That has interested us and took us to studies about the theme. This is indeed the subject of this IYK.

Conversations in forums dedicated to the subject, information from colleagues who know that we care about this, just dipping in the study of this "new" methodology, that actually cares about this triad and, in a way, is already being applied by some spatial and aeronautical entities.

However, like all methodology that takes place, there are people for and against. It is the natural reaction to changes or to the introduction of the new.

We forget that and try to see what it would bring as a good addition to fill this gap, in which the human being is the main protagonist.

We are talking about the methodology known by the acronym STPA (System-Theoretic Analysis Process).

As far as we are aware, the precursor of this methodology is Nancy G. Leveson, Professor Doctor of Aeronautics and Astronautics and Engineering Systems at the Massachusetts Institute of Technology (MIT) in the United States.

It is a methodology that seeks to decisively enter the human interaction of the processes that the system as a whole performs, also considering the environment surrounding the system in

operation. We might say that this is a methodology of "whole body".

Those who defend this position consider STPA as an improvement of those types of analyses which are among us for over 50 years, as the FTA (Fault Tree Analysis) and FMEA (Failure, Mode and Effect Analysis). They claim that STPA does everything that these "old" methods do, with the advantage of adding the human being in the process. This last part, no doubt, is a truth.

Clarifies that this is a hazard analysis which tries, first of all, identify the hazards and then develops processes to eliminate or mitigate them.

Differently of the so-called Safety Assessment (SA), it does not consider the failure of system to define the risks, including probability of occurrence. It begins by identifying the potential hazards that may occur in the operational phase, including strongly the behavior of human beings, without inserting probabilities.

We can see that this is an activity for an intense "brainstorming", that is, with experts trying to identify all the hazards that may occur in the operational phase. This is fascinating!

Importantly, this methodology has been tested in some systems; the most significant, in our opinion, the Japanese manned spacecraft of the Japan Aerospace Exploration Agency, to be launched from Tanegashima Space Centre (TNSC)conducted by a rocket also Japanese and must fly to the INSS (International Space Station).

The details of this methodology, as far as we understand, would occupy the space of several MSC. However, what we pass here, right now, is the existence of this new horizon, inviting everyone to study it. Let's at least try to engage together with this trend, making each his research on the subject.

Part of this material we have at this moment is presented in the bibliography of this IYK. It is all in English, as it should be. However, also, consult Google, on the Internet entering with the "STPA" acronym.

We advise our readers to be patient in reading that material. Read and reread it and make notes, to have a reasonable familiarity with the subject. Safety is a discipline whose study requires a lot of patience, a lot of insistence.

In another IYKs, in the future, we will return to this issue, but certainly with many of our readers already familiar with the subject.

We will try to quickly assimilate this new methodology. Perhaps we can work with several forums dealing with this subject. It will be good for everyone.

Perhaps also, in the near future, we can address the issue in seminars in Brazil.

Thank you and see you soon.

References:

1. M.A.B. Alvarenga, P.F. Frutuoso e Melo, R.A. Fonseca. 2014. A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. Progress in Nuclear Energy 75, 25-41. [CrossRef].

2. Cody Harrison Fleming, Nancy G. Leveson. 2014. Improving Hazard Analysis and Certification of Integrated Modular Avionics. Journal of Aerospace Information Systems 11:6, 397-411. [Abstract] [Full Text] [PDF] [PDF Plus].

3. Leveson, Nancy. G., Enginedering a Safer World: Systems Thinking Applied to Safety, MIT Press, Jamuary, 2012.