Safety: There is Something New on the Horizon - II

***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 52– FEB 03, 2015

Here we are once again, talking about this new methodology known by acronym STPA ("Sistem-Theoretic Analysis Process"), which we presented in the IYK 51. We consider this methodology as paramount, in these times when the systems are extremely complex, involving such the interaction be-human, system and environment, that we could not stop to continue to address this issue. We strongly believe that we are facing a new horizon in the safety area ("safety"). Then we will continue this theme in this IYK. More will come. Come with us.

When dealing with safety, we face two terms: event and state. The event is something that occurs. It has a beginning and an end, not having reversibility. State is a condition that continues and may or may not have consequences.

The failure of one system is an event. When it occurs, arises a state which can bring from consequences with negligible severity, i.e. with only a minor nuisance, up to undesirable consequences, culminating in those so-called catastrophic consequences, affecting severely the human-being and/or the environment. This state with undesirable consequences is referred to as "Hazard". There is therefore a range of hazards.

In safety, we call Causality the set of causes identifiable by a hazard analysis (Hazard Analysis), which can generate these undesirable results for a system. Its elements are called causes or simply hazards. Depending on system complexity, it is difficult to identify this set.

Over the past 50 years, we've been dealing with these sets, but always considering only the failures of hardware components (and its software) with your specific causality set. Said in other words, we have not inserted the human failures in these sets.

Recently emerged among us a new model of causality named System-Theoretic Accident Modeling Processes (STAMP), incorporating as causes, in addition to the mentioned hardware failures, those assigned to the human being, in its interaction with the hardware (with its embedded software) and the environment.

A theoretical system (System-Theoretic) could be the one still in a conceptual design phase, that is, without a defined physical configuration; with known functions, but without a hardware architecture (with its software) defined.

The STPA is based on the STAMP model. It is a Hazard Analysis, including in specific causality set all the causes of hazards that may arise, incorporating the human being as a component of the system.

Of fundamental importance is that inclusion of the human being, since a large proportion of accidents stems from undue or misleading actions of individuals.

According to the pattern STAMP, accidents occur as a result of inadequate control actions. In fact, the human being who is commanding an aircraft, for example, performs a control function. If he performs an inappropriate or untimely control action, there may be a hazard.

The methodology adepts claim that the STPA has the huge advantage of being applied when the system design is still in the conceptual stage, only knowing the system functions, that is, when

there is still no system structure and the same indeed could be called a theoretical system.

According Nancy G. Steveson, creator and advocate of STPA, the methodology applies to both in the design phase (before the fact, i.e, before an accident) as in the operational phase (after the fact). We agree.

When we use safety analysis of the type of FTA, they say*, the respective causality set will become clear just at the end of the development phase of the system.*

Well, at this point, we would like, first, to reproduce a paragraph of IYK 51: *Those who advocate the regard as an improvement over those who are with us for more than 50 years, as the FTA (Fault Tree Analysis "") and FMEA (Failure Mode and Effect, "Analysis"). Claim that STPA makes all these "old" methodologies make, with the advantage of adding the human being in the process*. This last part is, without discussion, a truth. (underline added in this IYK).

We add more the following paragraph of the IYK 51: *However, as every methodology that arises, there are pros and cons. It's a natural reaction to the changes or to the introduction of the new.*

We still remember that any theory, in its infancy, has pros and cons. It always receives criticism from one or other person. And we're no different.

We are seeing the STPA as a new horizon, yes, but only by the approach of human interaction with the hardware, simply because this was the first time we saw something that fortunately has been spreading, includin the human being as part of the system, in the generation of hazards.

The STPA, however, does not establish probabilistic requirements, but constraints (constraints) to be considered by the designers.

Unlike STPA, we would not call the FTA a methodology, but a powerful tool, for example, for the methodology called Safety Assessment, being used even as a tool to the allocation of safety requirements, still in the conceptual design phase (initial project), after a hazard analysis focused on the assumption of loss of system functions.

During the system development, the FTA remains present until it is proven that the total project complies with the safety requirements allocated in the conceptual design phase.

What we are saying is not only our creation. It was largely discussed in a forum that we have opened in Reliability and Safety Group on Linkedin site, with the participation of experts from some parts of our planet.

We open this forum with the following question: *Hello! I would like to know your opinions about that "new" approach in Hazard Analysis: STPA (System-Theoretic Analysis Process).*

It was a flurry of opinions and heated discussions.

As a matter of fact, we must say that the application of the STPA is not a very easy task. Its Learning requires the presence of an instructor with experience in the practice of STPA and much study. In a timely occasion, we return to the subject.

Thank you.

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., Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, January, 2012.