Improve your Knowledges (IYK)

Systems Safety: what is indeed the scope of the activity of Safety Assessment?

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 48 – JUL 25, 2014

When we establish that a catastrophic failure condition of an aircraft system must have a probability (P) of occurrence less than 10-9 (a failure in every billion flight hours), in an one-hour flight, what does it mean indeed? It would mean that this is the allowed range of probability for a catastrophic accident of an aircraft? Let's talk about this theme in this IYK.

We put up that theme here, just because a colleague one time told us he could not understand why the designs of aircraft in general have never meet this requirement, during the operational phase, in spite of the Airworthiness Authority certify these projects.

In fact, in reality, this probability is higher. Let us explain

The requirement of $P<10^{-9}$ refers only to accidents arising from failures of the aircraft systems. However, the accidents are not due only to systems failures. In fact, the part due to the

In fact, only about ten percent (1/10) of catastrophic accidents are attributed to conditions of system failures

To show this, let us recall something that we have already addressed in the MSC 08.

We said there that the analysis of accident rate of occidental commercial aircraft for the period from 1970 to 1980, showed that, during that period, the catastrophic accident rate was <u>slightly less than 1×10^{-6}</u>, i.e. an accident every one million hours flown.

In numbers: $\frac{N_C}{10^6} < 1 \times 10^{-6}$, where N_C is the total number of catastrophic accidents.

Considering the large amount of hours involved (10^6), the value above can be regarded as probability, obtained according to the empirical concept of probability, i.e:

$$P = \lim_{N\to\infty} \frac{n}{N}$$ (assuming 10^6 hours is a sufficiently large number)

where, n: number of failures observed; and
N: number of hours computed.

However, an analysis of the causes of these accidents showed that 10% were caused by failures of systems. In numbers:

$$N_C = N_S + N_O \text{, ou seja: } \frac{N_C}{10^6} = \frac{N_S + N_O}{10^6} =$$

$$= \frac{0{,}1(N_C) + 0{,}9\,(N_C)}{10^6},$$

where N_S is the number of accidents attributed to systems and No is the number of accidents attributed to other items.

Thus, the part allocated to systems was:

$$\frac{N_S}{10^6} = \frac{0{,}1\,N_C}{10^6} < 0{,}1\,(1 \times 10^{-6}) = 1 \times 10^{-7}.$$

This would be therefore the range of probability, in the empirical concept, of an accident occurs due to a catastrophic system failure condition, obtained from a sample in one million flight hours.

Starting from an arbitrary hypothesis, it was established that there are about 100 potential catastrophic failure conditions attributable to systems in large commercial aircraft. This way, we would have a subset **C** of events of the sample space $\mathbf{S}_C$ of catastrophic failure conditions consisting of 100 events, one for each condition of catastrophic failures attributable to systems. We could then represent such subset as follows:

$$\mathbf{C} = \{C_1 , C_2 , C_3 , \ldots, C_{99} , C_{100}\},$$

where C_i is a generic catastrophic event.

Then we have $P(\mathbf{C}) = P(C_1) + P(C_2) + P\ (C_3)$
$+ \cdots + P(C_{99}) + P(C_{100}) < 1 \text{ x } 10^7$.

Admitting that **C** is a set with equally likely events[1], i.e. that each one of its 100 events has the same probability of occurrence, we have:

$P(C_1) = P(C_2) = P(C_3) = \cdots = P(C_{99}) = P(C_{100}) = P(C_i)$.

where C_i is any event in the space S_C

we have $P\ (C) = P\ (C_1) + P\ (C_2) + P\ (C_3) + \cdots + P\ (C_{99}) + P\ (C_{100}) = 100\ P\ (C_i)$.

Therefore, $100 \text{ x } P(C_i) < 1 \text{ x } 10^{-7} \Rightarrow P(C_i) <$

$$< \frac{1 \text{ x } 10^{-7}}{10^2} \quad \text{or} \quad \boxed{\mathbf{P(C_i) < 1 \text{ x } 10^{-9}}}$$

Okay, but if only ten percent of the accidents were due to catastrophic system failures, what are the other causes? Statistics say that the human being is the largest portion of these causes. It is known that only the crew, due to their errors, must be contributing with a percentage between 75% and 80%.

Thus, when someone is traveling and prays to no happen an accident, it should do so focused on the crew, begging for it to be well trained and that has had a good night sleep before getting in the plane.

Mas e os outros 20% ou 25% dos acidentes catastróficos, a quem ou a que atribuir?

But and the other 20% or 25% of catastrophic accidents, to whom or to what assign them?

Going to other causes, we can mention, readily, maintenance as a significant source of accidents. We have to consider also the Environmental aggressions, that is, electromagnetic interference, meteorological factors, and so on. We can not disregard the flight control in ground, sometimes with wrong instructions. Also malfunctions on navigation aid radios on the ground. We might even add, in lower doses, terrorist acts.

But the goal here is to make clear that the aircraft does not only precipitates due to system failures. The main cause is still the humans.

And the unmanned aerial vehicle (UAV)? — Well, in that case, one could say that the accident is only due to system failures. It will be? And the human being that is in the earth station, controlling the flight of the UAV?

What that must be clear is that the Safety Assessment process, provided in the AC 1309 (Parts 23, 25, 27 and 29) and SAE ARP 4761, that guide the applicants in their analysis, at least for now, just takes care of a small portion that can cause catastrophic accidents, i.e: the systems.

Some researchers, with whom we have exchanged ideas, are continually thinking of an expansion of that scope, but that's another discussion.

Thank you. See you later

References

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

[1] Strictly, this is not true, but taking into account that for our analysis the interest is in the range assigned to each severity, we can consider a single and generic representative value of probability for each event of each range, which, in this case, is the range of catastrophic events.

(2) **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, USA, 1996.

(3) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, 2007.

(4) **De Florio**, Filippo, Airworthiness: An Introduction to Aircraft Certification. Elsevier. 2nd. Ed., USA, 2011.