- Safety Assessment - *SA*) -

Part Two: Talking About AC 25.1309-1A (V/V)

Berquó, Jolan Eduardo – Eletrônic Eng. (ITA)·.
Aerospace Product Certifier (DCTA/IFI)
Government Representative for Quality Assurance – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

IYK 11 – JULY 11, 2012

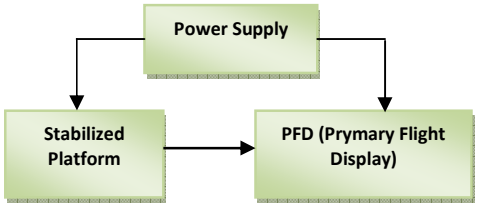
We return here just to close the series about "Safety Assessment.

In the previous MSC, we presented the Preliminary System Safety Analysis. But we have forwarded, purposely, for a simple system, given that the space for this section is intended for "flashes". So, we try, in this space, just give an idea to the reader, i.e. our intention here is just to familiarize the reader with the subject, trying to encourage him to get deeper into the matter, by consultation to the marked references, in which he will find as well other he will also find other references. It is a continuing study.

Strictly speaking, we should pass from a PSSA to an SSA and also perform other analysis, but, due to the circumstances shown, we will close the subject, considering the proposed architecture for the primary and secondary systems of attitude.

We will take into account only the primary attitude indicator system. The secondary system has a similar analysis, but with different numbers.

The structure presented in the previous MSC 10 is shown in the following figure.



The power Supply is a general equipment, that is, it is dedicated to all aircraft systems that need electrical energy, being so their failure conditions common to all systems that require electrical power.

In this way, we will consider just the system dedicated to the function in analysis.

Thus, the configuration that interests us is that one shown in the following figure.

We need to consider that we are using the negative exponential distribution function. We have said that when we adopt such a function to our system, this means that it behaves always as new (v. IYK 05), that is, every time it is switched on, everything happens as if it were connected for the first time (at least while the failure rate is approximately constant). It is a property named “forgetting Property” or “Memory Loss Property”. In this case, this is very close to the reality, whereas the system that we are analyzing is predominantly electronic.

Thus, while the system is on the porch of constant failure rate, we will always have the following probability of failure for the average flight: 6:0.6, for a constant λ and $\lambda t < 0.1$. For the stabilized platform, we would have $6.\lambda < 3.10^{-6}$. It follows that

$$\lambda < \frac{3.10^{-6}}{6} = 3{,}3.10^{-7}.$$

The reasoning would be similar to the PFD. The analyst, however, are free to handle these failure rates, according to the conveniences of the design, always having in mind the probabilities values established as requirements in the first FHA, i.e. in FHA aircraft level.

Finally, we would like to deal a bit about the Major failure conditions.

As we have seen, the Major failure conditions should be improbable. This means that the rate of occurrence of failure must be in the range between 1.10^{-7} and 1.10^{-5}.

As we have said, in general the equipment constituting the system under analysis has a failure rate identified by analysis and/or burn in tests, which permits to check if the system architecture of that part meets the safety requirements. For the sake of more safety, we can request from the manufacturer test reports and/or analyses that led to the rate displayed. In terms of analysis, we cano request, for example, the FMEA (Failure Mode, and Effects Analysis) made to the equipment.

The similarity with other certified aircraft can be also regarded as satisfactory by the Authority

We finish here this series of "flashes", suggesting to the reader to consult the references listed.

Thank you for your patience to read us. We will return with new subjects of interest about the airworthiness world.

See you

References

(1) **O'CONNOR, P.D.T**. Practical Reliability Engineering. John Wiley & Sons, Inc., New York, 1991.

(2) **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, USA, January, 12 - 1996.

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

(4) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, November, 8-2007.

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