– Safety Assessment (SA) –

Part Two: Talking About AC 25.1309 (IV/V)

Berquó, Jolan Eduardo – Electronic Engineer (ITA)·.
Certificador de Produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

IYK 08 – JUN 19 2012

Here we are again, this time to show the way to allocate safety requirements for the system-level functions, which isolated or associated with other leading to the aircraft level functions.

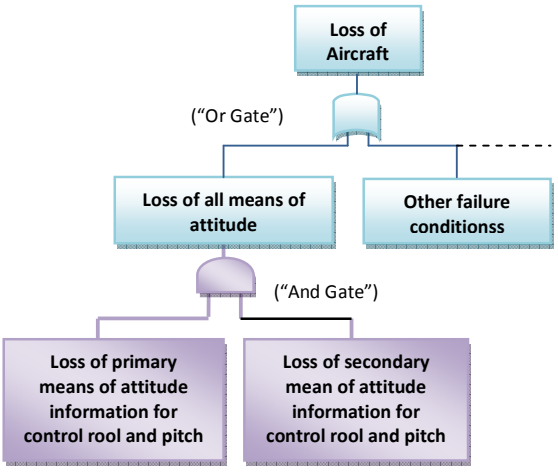
We said that the FTA is a good tool to perform this allocation. However, it is necessary to make it clear that there are other tools (Ref. 2) that can be used for the same goal. However, the FTA is, by far, the preferred way by safety analysts.

The FTA used in aircraft level is said a preliminary FTA because later, in the systems level FHA, the failure conditions and the requirements identified for the level aircraft shall be confirmed and/or updated.

We will use here the function in aircraft-level handled in AC 23.1309-1E: "Display of attitude information to control roll and pitch".

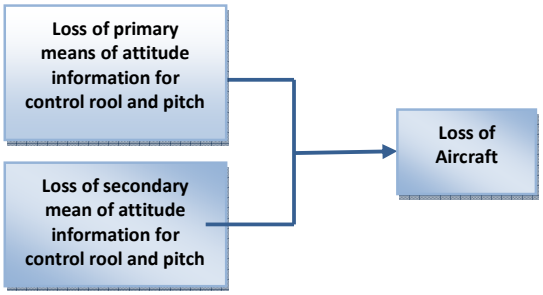
The worst failure condition for this function is the "Loss of all means of attitude information for control roll and pitch". This is a catastrophic condition for all phases of the flight.

The FTA would have the following structure:



Where the event "loss of aircraft" is the called Top Event (TE) of the FTA. The gate "And" is a symbol used to express that is necessary occur the loss of both means of attitude indication to occur ET. On the other hand, the symbol "Or" is used to express that ET occurs if at least occurs the loss of one of the means of indication.

In a Reliability block diagram (DBC) configuration, the scheme would be like a parallel configuration, as shown in figure below.



That is, to occur the ET (loss of Aircraft), it is necessary that occur both failure conditions.

In the case of a catastrophic event, the requirement states that the rate of occurrence must be less than 1.10^{-9} per flight hour. Assuming the average flight time is 6 hours, we have a allowed Unreliability[1] in the range of $<6.10^{-9}$ per flight.

Taking into account that in a gate "AND" the output is the product of input probabilities, we could establish, for example, for the primary means of indication system a range of

[1] *Unreliability (**F**) or Probability to failure in a time t. Taking into account that* $e^{-\lambda t} = 1 - \frac{\lambda t}{1!} + \frac{(\lambda t)^2}{2!} - \frac{(\lambda t)^3}{3!} + \ldots$ *and that for* $\lambda t < 0{,}1$*, the expression formed by two first terms of the series, that is,* $\mathbf{1-\lambda t}$*, is a good approximation for* $e^{-\lambda t}$*, i.e. for the Reliability,* $F = 1 - R = 1 - (1 - \lambda t) = \lambda t$ *is also a good approximation for* F*, since* $\lambda t < 0.1$*(See Ref. 1, Page 39 and Appendix 2).*

"probability less than 3.10^{-6}", resulting in a requirement "less than 2.10^{-3}" for the secondary system, because 3.10^{-6}. 2.10^{-3} = 6.10^{-9}.

It is not difficult to get the range "less than 3.10^{-6}", using a platform stabilized by laser gyroscopes, for example. But the choice of these ranges of probabilities for the systems is no doubt heavily influenced by the experience of designers.

This procedure is repeated for all failure conditions functional aircraft level classified as catastrophic or severe major.

After performing the FHA at aircraft level, we perform a FHA at systems level which are responsible for the level aircraft functions. This is the second step of the SA.

Step 2: Perform a system level FHA.

From the safety requirements established for the systems responsible for aircraft function in analysis, designers must obtain an architecture for both systems such that the probability of each one, as a whole, meets those requirements.

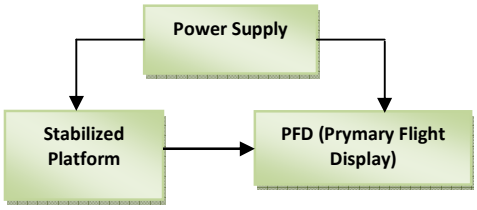
Note that with this procedure, the designers begin to configure the systems, in accordance with the certification authorities' safety requirements.

So we can consider that we have to have two systems for attitude indication: a primary one and a secondary one.

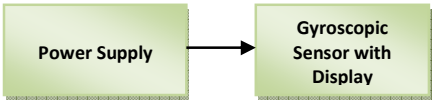
The primary system can be provided with a Primary Flight Display (PFD) and its associated remote gyroscopic sensor, and the secondary or alternative system can be installed directly on the aircraft Panel.

Step 3: Perform a Preliminary System Safety Assessment-PSSA.

The results of the FHA level systems are the inputs to the PSSA. However, the decision to undertake a PSSA depends on the architecture of the project, its complexity, in addition to other considerations. In this case, the systems are simple[2]. The architecture of each could be as shown in the figure below.



(a) Primary Attitude Indication System.



(b) Secondary Attitude Indication System.

The equipment available to build the systems are likely off-the-shelf, that is available on the market and with specified failure rates.

We will make the final considerations on the next MSC.

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, 12/01/1996.

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

(4) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, 11/08/2007.

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

[2] For a complete example of a PSSA, please go to the Ref.2.