Improve Your Knowledge (IYK)

DO-1778: Software Assurance - A Chat with Certifiers

***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 58 – JUL 15, 2016

The document RTCA DO-178B / C has never been so in vogue as now, due to the advance of electronic systems with software-based functions (SW). The document has been required in all areas of aviation, whether military or civilian, and even the Air Traffic Control products such as radar, DME, etc. Herein, we will present just a summary on the subject

The RTCA DO-178B/C, or, for simplicity DO-178, is a joint development of the Radio Technical Commission for Aeronautics (RTCA), in the United States and the European Organization for Civil Aviation Equipment (EUROCAE). The equivalent version of the European organization is the EUROCAE/ED-12B/C.

First of all, we must keep in mind that the document is not a SW development engineering requirement from the Authority, but a standard of care to guarantee quality of this development.

Considering just DO-178, for simplicity, we should make it clear that the Authority do not certifie SW, but the system that contains it; however, the Applicant will have to apply the DO-178 criteria, otherwise it will not occur the system certification.

The company which develops SW is free to use its own SW engineering methods, provided that the results reflect the inclusion of assurance criteria from DO-178 in the processes: planning, requirements definition, design and coding, integration, verification, management configuration and quality assurance.

The quality assurance process is immersed in all the other processes, in order to seek to ensure that these processes will follow the DO-178. Therefore, the specialist in quality assurance is a critical piece to the full implementation of the DO.

The starting point for implementation of DO-178 is the Functional Hazard Assessment - FHA, the first assessment of the Safety Assessment activity.

That assessment considers the severity of each failure condition. After that, we have to allocate the levels of quality assurance for the development of the SW, according to the following grading:

- ***A*** *for the failures conditions with Catastrophic severity;*
- ***B*** *for the failures conditions with Hazardous severity;*
- ***C*** *for the failures conditions with Major severity;*
- ***D*** *for the failures conditions with Minor severity; and*
- ***E*** *for the failures conditions with No Safety Effect.*

An example leading to the A-level is the catastrophic failure condition whose potential effect is the loss of the function that provides the pilot the indication of attitude of the aircraft in roll and pitch, today present on a EFIS (Electronic Flight Instrument System), which acts as Primary Flight Display (PFD).

At the other extreme, that is, level E, we have, for example, SW passenger entertainment functions_ since their failures conditions do not bring any effect on safety.

Well, would say someone, then the function of providing accident data (fulfilled by a Flight Data Recorder- FDR) and the function of providing the conversation in the aircraft cabin (provided by a Cockpit Voice Recorder - CVR) would also be level E, since the loss of these systems does not have any effect on safety. Wrong. In fact, because of the importance of these systems in a possible accident investigation, the SW of both systems must be at the level D,

After all, all of SW development information based on DO-178 must be delivered to the Authority? Of course not because it would be too much to pass to the Authority. In general, the Applicant presents only a subset of data, a priori discussed and agreed with the Authority. However, the Applicant shall retain and preserve all relevant data, as provided in the DO-178.

Of course, the certifier must have a good idea of the paraphernalia of data and documents produced in the SW development processes to identify, together with the Applicant, which data and documents to be submitted by the Applicant

The authority may, at any time, examine the Applicant facilities applied in the development process of the SW and any relevant data from the development relative to the DO-178 which are preserved by the Applicant.

If there's one thing that worries businesses is the issue of the cost of the DO-178 application. According to some already well experienced in SW development, the application of DO-178 can cost in average about 30% of the total cost of the system that incorporates it; but, they say yet that it can until cost more or less up to 6 times more than that if the experts do not become aware of the pitfalls that can arise in the application of the document.

Of course, the costs are higher for SW level A, decreasing to the level E.

To end this brief flash, we summarize the key ideas here inserted.

(1) DO-178b is not a requirement, but just a standard quality assurance of the SW development.

(2) The company that develops SW is free to use its own SW engineering methods, provided that the results reflect the inclusion of assurance criteria from DO-178.

(3) SW is not certified, but just the system that contains it ; However, if the OD-178 is not followed, it will not occurs the system certification.

(4) The identification of the quality assurance level (DA) for the SW depends on the results of the Functional Hazard Assessment (FHA).

(5) Sometimes, the Authority sets out a DAL for systems that do not have the slightest influence on safety (Ex .: FDR and CVR, both with level D).

6) The certifier must be well informed of the processes, data and documents produced by the applicant as a function of the DO-178 application, mainly to know how to choose those that the Applicant should realy pass him.

See you later.

References

1. *HILDERMAN V., BAGHAI T. Avionics Certification – A Complete Guide to DO-178B (Software), DO-178C (Upgrade), DO-254 (Hardware). Avionics Communications Inc. (USA), 2014.*
2. *Radio Technical Commission for Aeronautics (RTCA). DO-178C: Software Considerations on Airborne Systems and Equipment. RTCA (USA), 2012.*
3. *Radio Technical Commission for Aeronautics (RTCA). DO-178B: Software Considerations on Airborne Systems and Equipment. RTCA (USA), 1992.*