- Safety Systems: Civil and Military Approaches –

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

IYK 20 – OCT 3, 2012

We have already discussed the subject, generally speaking, in the IYK 15, but with a philosophical approach. This time, we will seek to make a closer analysis of the civil and military treatment of the subject which we have assimilated and still are assimilating, with practice and with the continued study.

First, it is prudent to discuss the meaning of the term *Segurança* in Portuguese. This word can has two meanings in Brazil: (1) may be hazardous conditions arising from unintentional failures in a system; and (2) hazardous conditions resulting from intentional actions, such as damage caused by terrorists..

Generally speaking, the term Security is linked to any danger of attacks, aiming to destabilize the security status of people and facilities.

But we will deal here just about safety, ie, the hazardous conditions that occur unintentionally. This means that we will talk just about the preventive actions, seeking to avoid or minimize the occurrence of accidents (before the fact), acting directly on the design phase and on the operational phase.

We begin by treating the civil area. Until recently, the civil authority was concerned almost exclusively with the safety of the development design of the aircraft (Type Certification - CT) or the safety-oriented design to install a device on an aircraft certified, ie Supplemental Type certification (CST).

Recently, the Civil Authority began to worry about the safety also in the operational phase, appearing then the activity which was called "Safety Management System - (SMS)", literally in Portuguese: Sistema de Gerenciamento de Segurança, but the translation for the Portuguese seems that it has consecrated itself as *Sistema de Gerenciamento de Segurança Operacional - SGSO*" ("Operational Safety Management System"), a title translation well placed because it states that it is a system used in the operational phase of the aircraft. SGSO details can be found in Ref 1, a translation performed by the DCA-BR.

On the military side, we have the MIL-STD-882E (Ref. 2). This standard is concerned about safety, but throughout the entire life cycle of the system. The first version was released in July 1969. The last version ("E") appeared in May 2012, and therefore is very recent.

When this standard is inserted in the contract, without specifying that parts of it should be taken into account by the contractor, just the chapters 3 ("Definitions and Acronyms") and 4 ("General Requirements") are required. So let's focus on Chapter 4.

We can see that there are several differences between this standard and those regulations facing civil aviation. But there are also commonalities. For example, both documents work with the binomial "Severity-Probability" (S & P).

Regulations 14 CFR Part 25 § 1309 - for large aircraft - and 14 CFR Part 23 § 1309 - for small aircraft , more popularly known as FAR 25.1309 and 23.1309, classify the severities, in the order of most severe to least severe, as follows: **Catastrophic, Severe Major (Hazardous** in 23.1309), **Major** and **Minor**.

MIL-STD-882E, on the other hand, presents the following classification: **Catastrophic**, Criticism **Critical, Marginal** and **negligible**.

We've already dealt with the severity scale of the civil aviation, for example in the MSC 06. We saw there that the severity of the failure condition is measured considering the adverse effects on the crew and passengers.

The severity in military aviation also includes the adverse effects of occupational illness, loss of equipment, property damage, environmental damage and financial loss.

One marked difference between civil and military standards is the inclusion, by the military, of financial values in the all levels of severities.

Thus, if the effect of a failure is the financial loss equals or exceeds 10 million dollars, it should be classified as catastrophic, with or without loss of human lives.

In the case of the critical severity, the financial loss allows has to be situated in a range between 10 million and 1 million. In the case of less severe (Negligible), the loss can not exceed $ 100,000.

On the other hand, we can use in the military area, the qualitative likelihood of failure, when it is difficult to establish quantitative requirements.

The qualitative requirements fall into the following levels: **Frequent** (expected to occur frequently), **Probable** , (expected to occur several times), Occasional , (expected to occur sometime), Remote , (unlikely but can occur), Improbable (very unlikely) and Eliminated , (not expected to occur). This last level applies to risks that have been identified, but then eliminated with design modifications or mitigation measures.

Annex A of the MIL-STD presents a table as an example of quantitative requirements. The standard establishes that the requirement for the level Improbable is P <10-6. The remaining levels can fall into ranges based on lessons learned or other criteria established by contract by competent military authority.

The standard recognizes the difficulty of having quantitative probability values at the beginning of the program, but once these requirements be considered, they must be allocated to the design, similar to what is done in Civil Aviation, where such allocation is made, already in the initial design phase, for the functions of the aircraft - the Functional Hazard Assessment (FHA), spreading later to the systems and ultimately to the equipment.

Curiously, the more restricted range for probability, in the military area, be P <6.10 (one-millionth), while in civil we have P <9.10 (one-billionth), i.e. 1000 times more restricted. However, we have to remember that the military activities, even in peacetime, has more risk, being unrealistic a range similar to the civil one.

With the data obtained for each failure condition, we call for the risk assessment matrix, as shown in the table below.

Risk Assessment Matrix				
Severit. / Probab.	Catastr.	Crit.	Marg.	Neglig.
Probable (B)	High	Alto	Serious	Medium
Frequent (A)	High	Alto	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated (it cannot occur)			

The responsibility for accepting these risks is defined by the competent national military echelon, and it seems logical that such responsibility be included in the acquisition contract.

The standard suggests that the responsibility for acceptance of High Risk (HR) must be of the authority that conducts acquisition programs; that the Serious Risk (SR) must be of the responsibility of the executive dedicated to that specific program; that the responsibility for Medium Risk (MR) must be assigned to the program Manager: and the Low Risk (LR) can be accepted automatically, ie without submission to any level of authority.

Well, we stop here.

See you.

References:

(1) Stolzer, Alan J.; Halford, Carl D.; Goglia, John J. Sistemas de Gerenciamento da Segurança Operacional na Aviação. (Tradução Equipe DCA-BR). São José dos Campos (SP): DCA-BR – Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica, 2011.

(2) DoD: MIL-STD-882E, System Safety. USA, May 2012.

(3) FAA: CFR 14 Part 23 § 1309, Equipment, Systems, and Installations, Amendment 23-49, USA, January 1996.

(4) FAA: CFR 14 Part 25 § 1309-1A, Equipment, Systems, and Installations, Amendment 25-123, USA, November 2007.