PROPOSAL FOR ORGANIZING THE INDUSTRIAL COOPERATION ON COMMERCIAL SPACE SAFETY AND TECHNICAL STANDARDS

Tommaso Sgobba
International Association for the Advancement of Space Safety (IAASS)
Kapteynstraat 1, 2201BB, Noordwijk ZH, The Netherlands
Email: (1) iaass.president@gmail.com

ABSTRACT

For commercial human spaceflight to flourish and expand, industry has to develop a notion of safety as the collective responsibility and common strategic business goal of all members.

In 2004, the U.S. private spaceflight industry welcomed a law (i.e. the Commercial Space Launch Amendment Act (CSLAA)) postponing the ability of FAA to issue safety regulations, except for aspects of public safety until 2012. The deadline was later moved to 2015. The law, currently undergoing a second postponement until 2020, offers a historic opportunity for space industry to engage in the development of a comprehensive set of industrial consensus standards, based on the experience gained in more than 50 years of government programs.

This paper proposes framework and rules of an industrial cooperation for consensus standards, in the form of textual content for a Memorandum of Understanding (MoU). Those standards, when established, could become the basis of a mixed regulatory regime, where industry takes care of self-certifying the vehicles safety, while government regulators would continue to cover launch and reentry operations for all aspect of public safety.

This paper also suggest to carry out standardization activities within the broader scope of a Space Safety Institute.

1. ACCEPTABLE RISK

To be "absolutely safe" a system, product, device or material should never cause or have the potential to cause an accident; a goal practically impossible to achieve. In the realization and operation of systems the term "safety" is generally used to mean "acceptable risk level", not "absolute safety".

Acceptable risk level is not the same as personal acceptance of risk, but it refers to risk acceptability by stakeholders' community or by society in a broad sense. Acceptable risk levels vary from system to system, and evolve with time due to socio-economic changes and technological advancement. Implementing proven best-practices at status-of-art is a prerequisite for achieving an acceptable risk level, or in other words to make a system "safe". Best-practices are traditionally established by government regulations and norms, and/or by industrial standards. Without such reference the term "safety" or "acceptable risk" becomes meaningless. In other words compliance with regulations, norms and standards represents the "safety yardstick" of a system.

2. SAFETY-BY-DESIGN

In the development of a space system, safety is achieved through the implementation of a combination of requirements that go under 'Fault Tolerance' and 'Fault Avoidance', plus requiring certain emergency response capabilities, (e.g. escape system).

Fault-Tolerance, consists in the designed-in characteristics that maintains prescribed functions or services to users despite the existence of faults. Fault tolerance is implemented for example by redundancies and barriers.

Fault-Avoidance, consists in reducing the probability of a fault by increasing the reliability of individual items (design margins such as factor of safety, designing to worst case scenarios, materials selection, use of hi-reliability components, de-rating, quality control, testing, etc.). Fault avoidance is essentially achieved through the use of proven best practices (i.e. technical standards).

3. STANDARDS

3.1 What is a standard?

"*Today, standards are no longer considered to be just stacks of dusty papers containing unjustified requirements and constraints. Standardisation is generally viewed as a process that drives commercial viability and success. Successful companies recognise that developing and using standards is the path to remaining competitive and producing quality products*"[1].
There are three major elements in the concept of "standard":

- something widely agreed
- minimum necessary
- approved and monitored for compliance by an authoritative organization

Often it is considered that wide agreement can be reached only as a result of long and successful application of a technical practice, which is then "promoted" to the level of standard. Traditionally, industrial standards, are not the enunciation of generic principles or goals, but they mandate specific design solutions. In other words, traditionally, safety requirements in standards tend to be <u>detailed and prescriptive</u>.

3.2 Technical standards and safety standards

Often technical standards are seen as something different or separated from safety standards just because

they are under the authority of different groups, respectively Engineering and Safety & Mission Assurance (S&MA). As a matter of fact, a large number of requirements in space technical standards are aimed at safety.

As human space transportation transitions from government activity to commercial or mixed commercial and government activities, the need arises for industry to develop a notion of safety as its collective responsibility and common strategic goal for business growth. To that end it is in the best interest of industry to cooperate among themselves and with regulators at developing, adopting, and enforcing safety and technical standards.

In government space programs a large body of knowledge already exists in the form of standards, which has been accumulated for more than 50 years. Such standards cannot be directly used in commercial programs because on one hand the language identifies specific organizations (e.g. NASA), internal relationship and development processes, and on the other hand they weren't established with industry concurrence.

3.3 Prescriptive standards and performance standards

In the early hours of 15 April 1912, the RMS *Titanic* struck an iceberg on her maiden voyage from Southampton, England, to New York, and sank. A total of 1,517 people died in the disaster because there were not enough lifeboats available. During the *Titanic* construction Alexander Carlisle, one of the managing directors of the shipyard that built it had suggested using a new type of larger davit, which could handle more boats thus giving *Titanic* the potential for carrying 48 lifeboats providing more than enough seats for everybody on board. But in a cost cutting exercise, the customer (White Star Line) decided that only 20 lifeboats would be carried aboard thus providing capacity for only about 50% of the passengers (on the maiden voyage) [2]. This may seem a carefree way to treat passengers and crew on-board, but as a matter of fact the Board of Trade regulations of the time stated that all British vessels over 10,000 tons had to carry 16 lifeboats. The regulation had become obsolete within a short period of time at the beginning of the 20th century that had seen ship tonnage raising up to *Titanic's* 46,000 tons. In addition the RMS *Titanic* was believed to be unsinkable by design, therefore why to worry about lifeboats!

The *Titanic* accident illustrates what a *prescriptive* requirement is (i.e. an explicitly required design solution for an implicit safety goal), and how it can sometimes dramatically fail by obsolescence.
The underlying motivation for prescriptive requirements is to prevent circumvention by avoiding any subjective interpretation in the implementation as well as in compliance verification. Violation of requirements can be unequivocally determined by simple inspections.

The vast majority of standards in use in aviation and other "evolutionary" industries are the result of lessons learned from incidents and accidents, and steady technological advancement. They are detailed according to type and prescriptive.

In contrast there are industries in which building on future experience is simply not possible, because the system is completely new, highly safety-critical (e.g. nuclear power plants) and/or extremely expensive.

4. GOVERMENT REGULATION AND / OR SELF-REGULATION

4.1 U.S. Government regulations

In 2004, the U.S. private spaceflight industry welcomed a law (i.e. the Commercial Space Launch Amendment Act (CSLAA) [3] postponing the ability by the FAA, to issue safety standards and regulations, except for aspects of public safety, until December 23, 2012, or until an accident occurs. The deadline was later moved to 2015. Currently a further postponement to 2020 is under approval. The CSLAA requires that a prospective spaceflight participant shall be debriefed about the risk of spaceflight and sign an informed consent. The CSLAA states that "*for each mission the operator must inform a space flight participant, in writing, of the known hazards and risks*