ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)
2.3: Safety regulation

SAFETY REGULATION OF CNS/ATM IN AUSTRALIA: A BRIEF SKETCH

(Presented by Australia)

1. INTRODUCTION

1.1 The 1980s and 1990s brought about the increased separation of two roles within Australian aviation, regulation and service provision, as well as the strict application of the principle of user pays to the latter. Today, the situation is as follows:

a) the Civil Aviation Safety Authority Australia (CASA), an arm of the Commonwealth of Australia, has safety regulatory responsibility for all aviation activities;

b) domestic airlines are privately owned, including QANTAS;

c) all major airports and some small ones are privately owned and operated. Operation and ownership of the reminder have been devolved to the municipalities where they are located; and

d) air traffic management and most of the CNS infrastructure is delivered by two Commonwealth agencies: Airservices Australia (on a cost recovery basis) and the Department of Defense.

1.2 The occasion of such changes was also an appropriate one to examine the safety regulations related to CNS/ATM.

1.3 After carefully considering how to best achieve a balance between effectiveness, flexibility and efficiency across all affected parties in these times of rapid technological change, CASA adopted the method outlined in the next section[1].

[1] It is noted that this method is not a new invention by CASA but summarises the world trends in practice, standards and research. An extensive list of references is available for the interested reader.

2. OUTLINE OF THE METHOD

2.1 Systems are no longer considered to be formed by just the equipment (hardware, software). A system is regarded as the combination of people, procedures, technologies and data working together to perform a function in a particular environment.

2.2 Regulations do not prescribe all the details of an implementation of a solution to a potential problem needing regulation, but rather state the principles governing the design and operation of such implementation and the objectives sought.

2.3 Thus, in actual practice and beyond the actual structure of headings/topics, the set of regulations requires service providers to adopt a system safety approach[2].

2.4 Inherent to such approach is the fact that the service provider must develop a safety case[3] for any change to a system, since a change means a departure from pre-approved operational boundaries[4] and it is not possible to determine *a priori*, i.e. without analysis, whether a change will impact safety or not.

3. EXPERIENCE

3.1 The experience has been positive. The new method has required a period of significant cultural change within the service provider and the regulator alike. Aside from the central fact that it seeks to visibly and traceably build safety in, it also provides an effective arena within which to resolve the natural tension between the forces of hopeful, anxious change and cautious conservatism. It provides flexibility while ensuring visibility. Through the need to develop and argue a safety case for a system, now regarded as much more than just equipment, it also provides an administrative focus that solves some of the approval difficulties some times faced by industry[5].

---

[2] System safety approach: A systematic and explicit approach defining all activities and resources (people, organizations, policies, procedures, time spans, milestones, etc.) devoted to the management of safety. This approach starts before the fact, is documented, planned and explicitly supported by documented organizational policies and procedures endorsed by the highest executive levels. The system safety approach uses systems theory, systems engineering and management tools to manage risk formally, in an integrated manner across all organizational levels, across all disciplines and all system life cycle phases.

[3] Safety case: Both the argument and the document that contend the level of safety attained will satisfy the safety requirements. It intelligently and coherently argues the degree of safety achieved at any point of a system's life cycle by making rational and coherent reference to the documented results of the system safety approach.

[4] Although self evident from the definitions, it is noted that the analysis should include all necessary routine and foreseeable emergency configurations.

[5] See Final Report of RTCA Task Force 4, Certification (1999).

4. ACTION BY THE CONFERENCE

4.1 The Conference is invited to note the contents of this paper.

— END —