

ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

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

2.1 Safety management systems and programmes :

ATM SAFETY MANAGEMENT SYSTEMS (SMS)

(Presented by IFATCA)

SUMMARY

The introduction of safety management systems (SMS) in air traffic management (ATM) presents challenges to the air traffic service providers, the national safety regulatory authorities and the operational air traffic services staff. The development of a safety culture within the ATM organization is an essential element of a successful SMS which, in turn, impacts on management/labour relationships. This paper identifies some of the important issues facing all stakeholders and explains the controller concerns and needs in respect of SMS, safety regulation, safety cases and risk mitigation. It acknowledges the need for change in attitudes and the development of trust between all parties if the introduction of SMS is to be successful.

Action by the conference is in paragraph 6.

1. INTRODUCTION

1.1 The development of communications, navigation, and surveillance/air traffic management (CNS/ATM) systems has been driven from the early days of future air navigation systems (FANS) by the need to increase capacity of the air traffic services (ATS) system to meet the rapidly increasing demands of the airline industry. The implementation of ATM/CNS systems has invoked major structural changes within the provision and regulation of the ATS including such diverse developments as harmonisation on regional and global scale, the commercialisation of ATS providers and the separation of the regulatory function from the provision of ATS.

1.2 Historically, the safety of the ATS system is an overriding priority and as such remained the responsibility of the sovereign state. However, the development of regional groupings and plans places the existing status in doubt even though these are still in a formative stage. This move towards harmonisation has identified weaknesses in the way that different States have applied safety standards. Consequently, in an attempt to homogenise and standardise the approach to safety, ICAO has mandated the use of safety management systems (SMS) and by 27 November 2003, the acceptable level of safety and safety objectives applicable to the provision of ATS within airspaces and at aerodromes shall be established by the State or States concerned. When applicable, safety levels and safety objectives shall be established on the basis of regional air navigation agreements.

1.3 The ATM/CNS system is in a state of transition which has or will have a major impact on the three primary elements: people, procedures and equipment. Although IFATCA is primarily concerned with the role and responsibility of the controller in this changing environment, it recognises the essential interrelationships with the other elements to ensure that the safety of the ATM system is maintained at the required standard. Therefore, this paper takes a holistic approach and considers the issues arising from the systematic approach to the safety of future ATM operations.

2. THE NEED FOR SMS

2.1 Within ATM, it has been acknowledged that risk is ever present and cannot be eliminated unless you ground all the aircraft! The acceptance of this fact has identified that risk in the ATM/CNS system must be reduced to a level that is as low as is reasonably practicable. The purpose of a safety management system is to provide an ATM service-provider with a management tool, which will ensure a systematic and pro-active approach to safety throughout the whole ATM organisation.

2.2 Three definitions that should be considered:

- a) safety is defined as freedom from the unacceptable risk of harm¹;
- b) safety management is defined as the systematic management of the risks associated with ATM activities to achieve high levels of safety performance²; and

¹ Eurocontrol Safety Regulation Commission

² UK CAP 730 Safety Management Systems for Air Traffic Management, 12 September 2002

- c) safety management system is a systematic and explicit approach defining the activities by which safety management is undertaken by an organization in order to achieve acceptable or tolerable safety³.

2.3 A fully developed SMS contains a number of important features such as a statement of policies and principles, allocation of safety accountabilities and responsibilities to all levels of management, means to establish safety assurance, requirements for measuring safety performance and procedures for safety promotion. To ensure the success of the SMS, a positive safety culture needs to be developed throughout the service-provider's organisation. This requires an explicit commitment to safety from board level downwards. Also, it represents a challenge to many of the existing working practices and attitudes both at senior/middle management levels and the operational level. The introduction of an SMS will neither guarantee safety nor install a positive safety culture just through its presence alone. Ownership of the SMS must be seen to be inclusive of all staff, otherwise if it is perceived that the SMS is in place to protect senior management from responsibility for accidents or incidents, an atmosphere of distrust will be created resulting in a lack of commitment to the SMS from the staff.

2.4 By its very nature of defining the activities by which safety management is undertaken, the SMS will be bureaucratic and, as such, always liable to be submerged in its own documentation. Clearly this is not acceptable and the service-provider should take steps to minimize the impact of administration. The inclusion of all staff is a key element of a successful SMS; therefore, the operational staff need to be involved from the outset of design and implementation. This operational input is essential in many of the SMS functions from safety assessment, hazard identification and risk analysis, trend analysis, incident reporting systems, to operational training and competency issues. Some of this input is already in place e.g. controller training therefore appropriate on-the job instructor training will have been completed. However, for many of the other SMS requirements, specialised training will be required to ensure the required standard of operational input.

2.5 A properly constructed SMS will not only provide a transparent, recorded system to manage safety but also a monitor of system performance with the ability to input corrective actions in the event of underachieving set safety performance indicators. In order to perform accurately and efficiently, it is essential that comprehensive reporting systems are in place and allowed to operate in a just environment (excepting deliberate violations and gross negligence). By comparing agreed and established safety criteria with the performance indicators, system performance can be gauged and, where deficiencies are identified, remedial action can be taken.

3. THE ROLE OF THE SAFETY REGULATOR

3.1 The ATM service-provider can be subjected to a wide range of pressures such as cost and performance, which have the potential to conflict with safety. Also, these pressures may be increased when the ATM service provision function is devolved from the State responsibility and placed in the hands of an independent service-provider. Therefore a need exists to ensure that these conflicts of interest do not cause any reduction in safety levels. Also, the State retains a responsibility to ensure that the levels of safety achieved by the ATM service-provider are acceptable, both publicly and politically, and these can be demonstrated satisfactorily.

³ ESARR 3 The use of Safety Management Systems by ATM Service Providers, 17 July 2000

3.2 The ATM service-provider can be subjected to a wide range of pressures such as cost and performance, which have the potential to conflict with safety. Also, these pressures may be increased when the ATM service provision function is devolved from the State responsibility and placed in the hands of an independent service-provider. Therefore a need exists to ensure that these conflicts of interest do not cause any reduction in safety levels. Also, the State retains a responsibility to ensure that the levels of safety achieved by the ATM service-provider are acceptable, both publicly and politically, and these can be demonstrated satisfactorily.

3.3 The Eurocontrol Safety Regulation Commission⁴ has listed the responsibilities of the national safety regulator as:

- a) establishing a national safety regulatory framework, including any applicable safety regulatory policies, objectives and directives;
- b) setting minimum acceptable levels of safety (in the public interest), including by means of target levels of safety;
- c) defining applicable national safety regulatory requirements, including those necessary to meet international commitments;
- d) defining any relevant Standards and Practices that apply to support or complement the requirements;
- e) ensuring that minimum acceptable levels of safety are met by service-providers; and
- f) ensuring ongoing compliance with national safety regulatory objectives and requirements.

3.4 The relationship between service-provider and safety regulator is crucial to the achievement of safety objectives and the establishment of acceptable levels of safety. On the one hand, an over stringent application of safety levels may place an unacceptable workload on the ATM service-provider and consequently the operational staff, whereas too low a level may put not only the public at risk but also the controllers.

3.5 Whilst this may be a rather simplistic observation, it does highlight the requirement for the safety regulator to be competent and experienced in the provision of ATM services. Also, a comprehensive knowledge of safety management systems and the associated procedures such as risk analysis and mitigations, safety cases, and safety assurance is required to ensure that satisfactory and adequate oversight is achieved.

3.6 The safety regulator should apply his responsibility to safety oversight to proposed operations of new ATM systems (initial safety oversight) and to continuous operation of in-service ATM systems (ongoing safety oversight). Oversight would normally be achieved through external auditing of the service-provider to gain assurance that national and the service-provider's safety requirements were being met.

⁴ SRC Pol Doc 3 National ATM Safety Regulatory Framework, 27 February 2002

4. THE SAFETY CASE

4.1 Within the infrastructure of the SMS, procedures should be in place for the development of the safety case which is the focal point of the risk management process. A safety case is a structured documented argument that a function is adequately safe in a given context⁵. A major portion of the safety case will deal with hazard identification associated with each function that, in turn, determines the risk. Risk is the combination of the severity of an accident and the probability that it occurs; therefore, to reduce the risk to as low as reasonably practical, the severity and/or the probability have to be reduced. The prime objective of this process is to identify the acceptable probability that will be either defined in quantitative or qualitative terms.

4.2 Part of the risk reduction argument will be based on acceptable mitigations supported by objective argument and evidence. Mitigations can be related to equipment (e.g. a requirement to have alternative powered stand-by radio), procedures (e.g. loss of communications procedure) or people (e.g. apply procedural control in the event of radar failure). However, over reliance on mitigating arguments, particularly those involving controllers, will have a detrimental effect on the risk management process by embedding a weakness in the robustness of the safety case.

4.3 The concern for IFATCA is that it is very easy to make a persuasive argument in favour of controller mitigation as a result of the controllers' active role in the ATM service. Some of these claims are acceptable particularly when relating to tactical control because that is part of the controller task. However, the difficulty arises in two particular areas: controller workload and use of controller support tools.

4.4 For example, if mitigation claims that in the event of a specific system failure, the controller will take over the extra function(s) then controller workload must be examined carefully. Although a controller may have been taught, and indeed, practiced the fallback procedures, he could conceivably be unsuccessful through an unacceptably high workload. In other words, the mitigation should be subject to the hazard identification and risk management process. This process should take into account all concurrent events that include the controller as mitigator in order to address the workload issue. The difficulty that is faced by service-providers is that the alternative to controller mitigation is likely to be expensive in extra equipment and/or other resources. The temptation will be to be persuaded by a flawed mitigation based on controller expertise.

4.5 The continuing introduction of controller support tools gives further cause for concern particularly where the tools will be used for capacity enhancements. The argument used for increasing controller workload applies; however, the potential for increasing capacity is significant and going beyond the average controller's capability. In this case, controller mitigation as the sole means (reverting to manual at its most basic) is not an option and the risk management process will need to be considered in that light.

4.6 IFATCA would expect that the safety regulator would have a pivotal role to play by auditing service-provider's safety cases to ensure that the claims and mitigations were supported by objective argument based on substantial evidence. Also, IFATCA believes that an independent regulator should be aware of all safety cases being processed and decide to audit those which involve major change, innovative

⁵ Presentation by Peter Madden to the UK CAA SMS Workshop, October 2002

developments, and those which provide the regulator with the assurance that the provider is meeting both national safety regulatory requirements and his own requirements derived from the SMS.

5. CONCLUSION

5.1 During the development and implementation stages of a safety management system, IFATCA believes that it is essential to consider the following points:

- a) commitment to safety must be a priority throughout the service-provider's organization;
- b) the development of a pro-active safety culture is essential for the success of the organization's SMS;
- c) the SMS should be user friendly and not unduly bureaucratic;
- d) controllers, along with other operational staff, should be involved at the design stage of the SMS;
- e) appropriate safety training should be provided to controllers to ensure meaningful participation in the SMS procedures; and
- f) incident reporting is an essential part of the SMS therefore the service-provider should ensure that a just reporting system is in place.

5.2 The role of safety regulation of ATM is a key element in the ATM safety process. IFATCA would emphasize the following:

- a) the function of service provision and safety regulation should be separated;
- b) the safety regulatory organization should be staffed by competent and experienced people who have relevant knowledge in safety management systems and safety oversight; and
- c) appropriate training is provided in ancillary tasks such as auditing.

5.3 The use of controller mitigation is widely used throughout the risk management process, therefore IFATCA is concerned that:

- a) the use of controller mitigations should be carefully monitored to ensure that the mitigation is valid and the issues of controller workload and capability have been tested; and
- b) controller liability and responsibility in respect of advisory tools should be clarified.

6. ACTION BY THE CONFERENCE

6.1 The Conference is invited to consider the points from this paper in the discussion(s) on systemic safety in ATM.

6.2 The Conference is invited to task ICAO to take the points into consideration when developing guidance material on systemic safety programmes for ATM.

— END —