Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-624

Safety case in ATM is more than accident risk assessment alone

H.A.P. Blom and M.H.C. Everdij

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-624

Safety case in ATM is more than accident risk assessment alone

H.A.P. Blom and M.H.C. Everdij

This report is based on an article published in Air Traffic Technology International 2000.

Division:	Air Transport
Issued:	December 2001
Classification of title:	Unclassified

Summary

New CNS/ATM concept developments are typically undertaken without feedback from appropriate safety assessments. Capacity-efficiency enhancements are realised by exploiting new technology, changing human controller roles and introducing new procedures. However, effectively supporting demand and safety is more than making sure that every ATM function is safe.

Contents

(13 pages in total)

1 Introduction

Traditional air traffic management (ATM) design approaches tend first to design advanced ATM that provides sufficient capacity, and then to extend the design with safety features. The advantage of this approach is that ATM developments can be organised around the clusters of individual elements, e.g. communication, navigation, surveillance, automation tools, HMI and advanced procedures.

The key disadvantage is that safety effects stay unclear: ATM is the result of complex interactions between human operators, procedures and technical systems (hardware and software), all highly distributed; these complex interactions significantly determine safety as a function of demand. Therefore, jointly supporting capacity and safety is more than making sure that each of the capacity-providing elements is completely safe.

A far more effective approach is to try to design an ATM system that is inherently safe at the capacity level required. From this perspective, safety assessment should be one of the primary filters in ATM concept development. An early filtering of ATM design concepts on safety grounds can potentially avoid a situation where a costly development programme turns out to be ineffective, or where an even more costly implementation programme fails.

Although understanding this idea is principally not very difficult, it can only be brought into practice if an ATM safety assessment approach is available that provides appropriate feedback to the ATM designers already at an early stage of the concept development (Figure 1). This feedback should not only provide information on whether the design is safe enough, but it should also identify the safety-capacity bottlenecks.

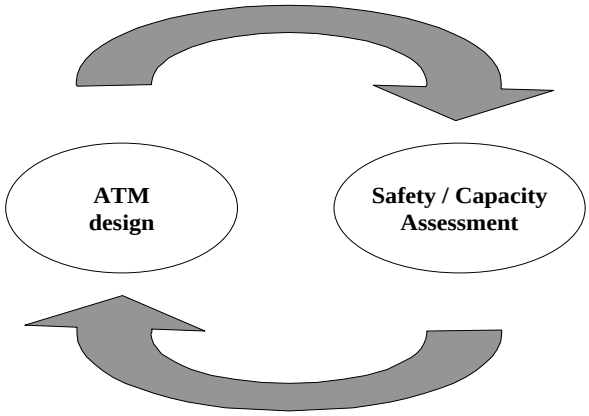

Figure 1: Safety feedback based ATM design

2 Modern Safety Case

For various safety-critical products, services or operations in other domains, the safety judgement is in general based on a series of documents describing the results of a safety validation process. Such a series of documents is often referred to as a 'safety case', with the top-level documents providing the argumentation and the other documents providing the supporting evidence. By now, consensus is building that appropriate modern safety case approaches are needed to understand the mechanisms behind designing advanced ATM. It is also recognised that once such a safety case approach is available, a safety feedback based design approach of future capacity-efficient ATM will become feasible.

A modern safety case is a living document that is updated on a regular basis, for example when new hazards have been identified and assessed. The coverage of hazards rather than failure modes is particularly important if human operators are in the loop of safety-critical services or operations, since in those cases most hazards are not of the failure mode type. A safety case should serve as a guide in improving safety at the physical level. This means continual updating and verification of its application.

A complementary recent development is that top-level management has recognised the modern safety case as a valuable decision-support management tool during all stages of a safety-critical operation. For example, during the conceptual development stage of a new safety-critical operation, management may have to make a decision regarding improving the design or starting the preparation and procurement for the operational implementation of a new or improved operation. To be fully informed, management needs the complete picture provided by a modern safety case, rather than the partial picture provided by several technical evaluations.

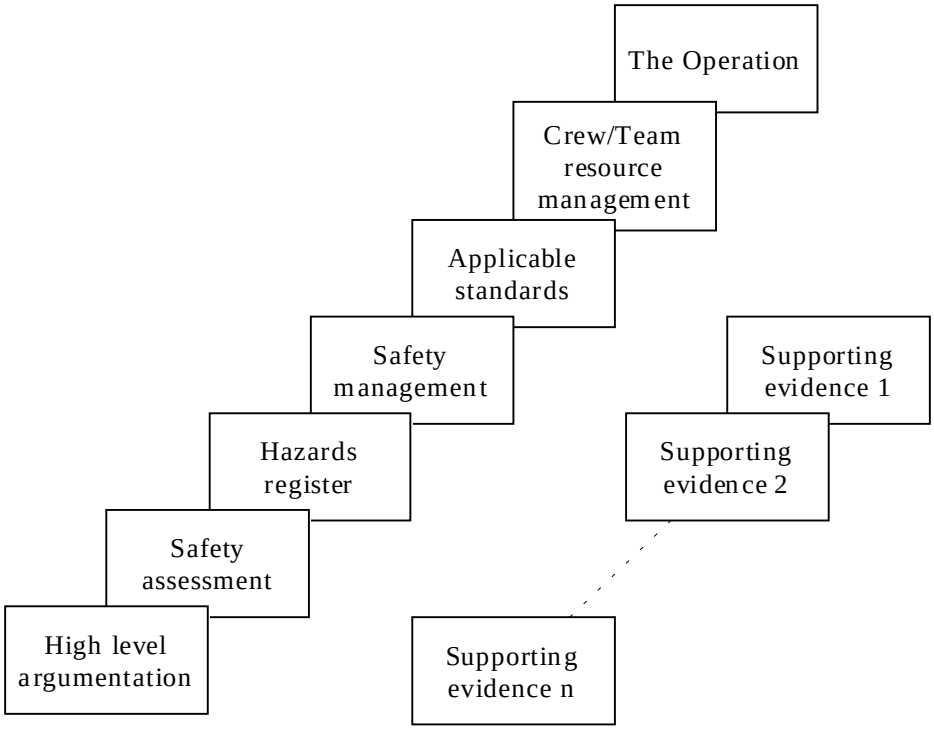

Figure 2. Modern safety case takes safety management and crew/team resource management into account.

3 Safety metrics

Safety is a general notion that is typically studied from one of three perspectives:

- Safety perception (by pilot, controller, passenger, human society, etc.). An ATM design that is perceived unsafe will not easily be accepted by the humans involved. A positive perception about the safety of an ATM design is an implementation-critical requirement. However, by its very nature, safety perception is a subjective notion, and therefore insufficient to really base safety cases on.
- Dependability of a technical system (of a computer program, an aircraft navigation system, a satellite based communication system, etc.). Dependability metrics are objective and are widely studied in literature. However, they have been developed to cover technical systems only and not the human operators and procedures of ATM.
- Accident risk (e.g. for 1st, 2nd and 3rd parties in air transport) metrics are objective and are commonly in use for other human-controlled safety-critical operations such as chemical and nuclear industries. Two well-known ICAO-adopted accident risk metrics are used for collision of an aircraft with another aircraft during en route phase, or with fixed obstacles during landing. Related metrics exist for wake vortex induced risk.

In view of the ATM safety assessment needs, the accident risk perspective has the best joint characteristics:

- It implies the use of objective risk metrics;
- It has proven its usability to human-controlled safety-critical operations;
- It is supported by ICAO.

In this article ATM safety will be considered from the accident risk perspective.

4 Established approaches

Accident risk assessment problems have been widely studied for other safety-critical operations, such as in the nuclear and chemical industries, for these applications, numerous techniques and tools have been developed. To take maximal advantage of this existing knowledge, The National Aerospace Laboratory made a thorough study of the applicability of these techniques to accident risk assessment in air traffic.

A large variety of techniques were identified, from qualitative hazard identification methods such as preliminary hazard analysis, common cause analysis and failure mode and effect analysis, to static assessment techniques such as fault tree analysis and event tree analysis, and dynamic assessment techniques such as Petri net modelling, Markov chain modelling and dynamic event trees.

So far, only relatively simple ATM situations could be handled by these established techniques. The key finding is that the established techniques fail to support a systematic approach towards modelling stochastic dynamical behaviour over time, for complex interactions of highly distributed ATM (Figure 3). These techniques would therefore force one to adopt a rather heuristic type of argumentation in trying to capture the complex interactions inherent to advanced ATM.

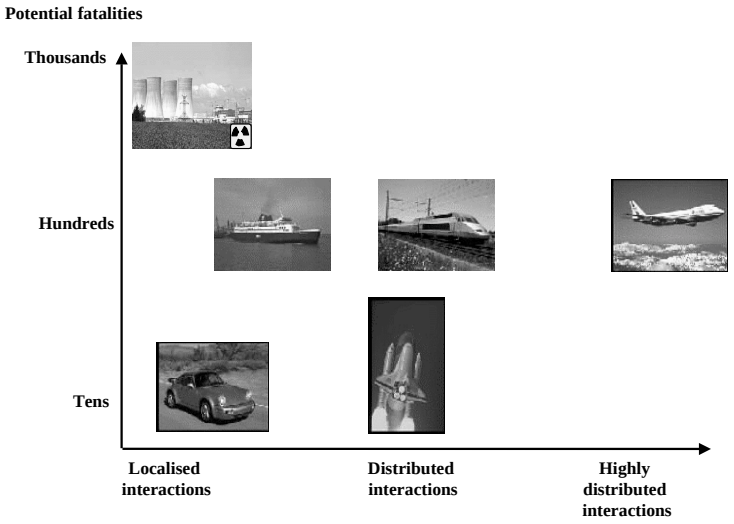

Figure 3: Potential fatalities and distribution level of ATM and other safety-critical activities.

Another problem with many established techniques exists due to the rarity of fatal air traffic accidents. For air traffic, the fatal accident risks should be of the order of 10^{-7} - 10^{-10} per aircraft flight hour. To develop some feeling of the difficulty to assess such rare events, it is quite helpful to understand why the well-known fast-time simulators such as National Airspace Systems Performance Analysis Capability (NASPAC), Recognised ATC Mathematical Simulator (RAMS) and Total Airspace and Airport Modeller (TAAM) fall short of that objective.

One major shortcoming of these tools is that they are not really capable of simulating the aviation safety-critical combinations of non-nominal events; for example, they often do not even simulate the single non-nominal events. Another major shortcoming is that an accident rate of, for example, 10^{-9} per aircraft flight hour cannot, in a reasonably practical way, be assessed using a straightforward simulation, since this would require a simulation of 10^{10} aircraft flight hours. This problem is well illustrated by the ATM safety iceberg (Figure 4). To assess a catastrophic accident rate, one really needs to deconstruct the risk assessment problem into an effective hierarchy of simpler conditional assessment problems, where simpler refers to an appropriate combination of scope (e.g. volume of airspace) and depth (i.e. level of model detail) at each conditional assessment level.

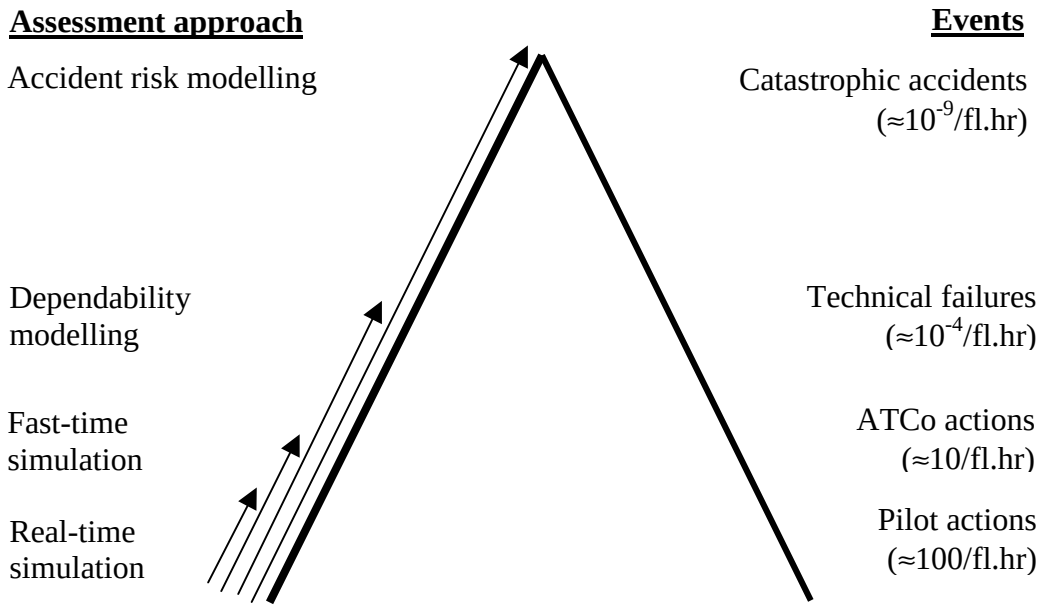

Figure 4: ATM safety iceberg

5 Human cognition modelling

When assessing ATM safety, an essential role is played by procedures, human operators, and their responsibilities. At present, the view on human reliability has shifted from a context-free error centred approach in which unreliability is modelled by failures of human information processing, towards a contextual perspective in which human actions are the product of human internal states, strategies and the environment.

By now, it is a widely accepted belief that for the modelling of the human, the established human reliability analysis (HRA) techniques fall short for complex situations, and that the aim should be for contextual performance models that are based on generally applicable human cognition and responsibility principles. Moreover, in HRA widely used skill-, rule- and knowledge-based errors essentially do not make allowances, for example, for situations where the operator chooses to let a more urgent problem receive attention when the subjectively available time is short, or when a heavy workload causes them to make quick decisions, without bothering excessively about the quality of those decisions. It should be noticed that these effects are inextricably bound with human flexibility and the ability of humans to deal with unforeseen situations. When assessing ATM safety, it is necessary to consider these aspects of human performance.

The main benefits expected from contextual models is that they provide better feedback to designers and that they also remove the need to use overly conservative individual submodels

for relevant operator actions that may blur understanding of how safety is achieved in ATM. To develop appropriate models for this, mathematicians and psychologists are jointly developing high-level models of human cognition performance, in a sequence of studies. Currently, this collaboration has led to a novel contextual human task-network model, which effectively combines the control modes of Hollnagel with the multiple resources theory of Wickens, the classical slips/lapses model of Rasmussen and the human capability to recover errors. In addition to this, the National Aerospace Laboratory has developed a model for the evolution of situational awareness errors.

6 TOPAZ methodology

The Traffic Organization and Perturbation AnalyZer (TOPAZ) methodology has been developed to provide feedback on safety/capacity to designers of advanced ATM, following each (re)design cycle. Figure 5 gives an illustrative overview of how such feedback is obtained.

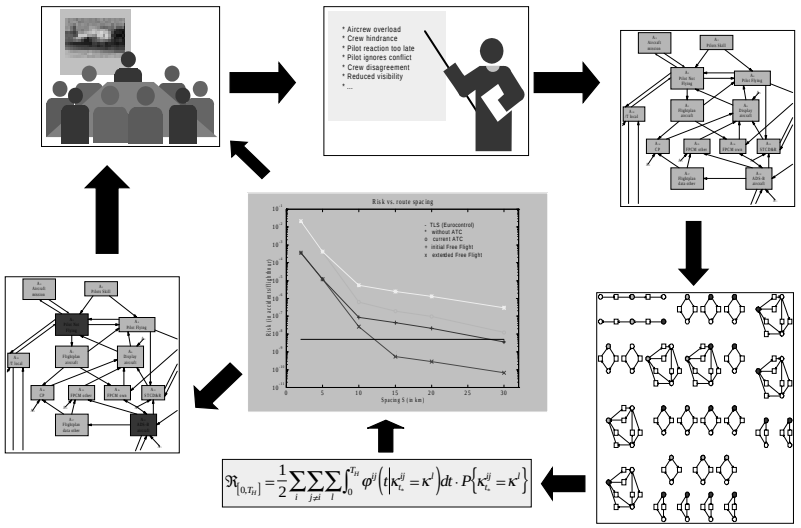

Figure 5: TOPAZ risk assessment cycle.

During each risk assessment cycle two types of assessments are conducted: first a qualitative safety assessment (upper drawings in Figure 5), and then a quantitative safety assessment (middle and lower drawings). The qualitative assessment starts with a systematic gathering of information about nominal and non-nominal behaviour of the concept design considered, concerning the human roles, the procedures, the technical systems, etc, with involvement of relevant experts. For the gathering of non-nominal information, explicit use is made of

structured hazard identification sessions with a variety of experts, and hazard data bases (upper middle drawing).

The resulting list of identified potential hazards is subsequently analysed using established qualitative hazard analysis techniques, to identify the safety-critical encounter scenarios and associated hazards, to select one or more of those safety-critical encounter scenarios for quantitative safety assessment, and to develop a modular system engineering type of representation of the ATM design (upper right drawing). Such modular representation is easily recognisable and understood by ATM designers and therefore it also supports effective communication between ATM designers and safety analysts.

From this point on, the TOPAZ assessment cycle continues with the quantitative phase, which is based on stochastic modelling, stochastic analysis and numerical evaluation. First, an appropriate stochastic dynamic model instantiation of the ATM concept design is developed in an iterative way, including human cognitive behaviour and with verification against the results of the qualitative safety assessment phase (lower right drawing). The format of this model is dynamically coloured Petri net (DCPN). Next, the accident risk is assessed for this stochastic dynamical model (lower middle and middle drawing) by making use of the collision and wake vortex risk models available within TOPAZ. Subsequently, the safety/capacity critical elements are identified (lower left drawing). Finally, these results are fed back to the ATM concept designers.

An important TOPAZ step is to validate to a certain level that a risk assessment exercise is performed to an acceptable degree, without the need to first employ very expensive large-scale real-time simulations of new concepts. As a result of the underlying stochastic analysis framework, such a validation can be done by executing the following activities:

- Judge the level of conservatism of the assumptions adopted during the development of the DCPN instantiation for the situation considered. This should be done with active involvement of operational and design experts;
- Verify the correctness of the instantiated DCPN versus the results of the qualitative assessment and the assumptions adopted. This should be done by stochastic analysis TOPAZ experts, with at least one who was not involved in instantiating the DCPN;
- Verify the correctness of the mathematical transformations applied to the instantiated stochastic dynamical model. This should be done by applying mathematical tools from stochastic analysis theory;
- Verify that the various assessment activities have been executed according to the unambiguous mathematical model developed, including the decomposition. This should be done by stochastic analysis experts.

7 Conclusion

This article has given an outline of the TOPAZ methodology to assess advanced ATM on safety/capacity, and has illustrated that this approach may provide effective feedback to designers of advanced ATM. This feedback is an essential source of information in the process of building a modern safety case for the ATM design. One of the major features of the new approach is that it incorporates advanced human cognitive modelling. This provides a way to assess the effect on safety/capacity of new technological advances, including changes in operator workload due to these advances.

Currently, a high level of expertise in stochastic analysis is required for an effective application of the methodology. One should however, be aware that the need for sophisticated mathematical expertise is well accepted in other complex design areas of civil aviation, such as the area of aerodynamic optimisation of aircraft structures.

Recently, through a joint effort of Eurocontrol and the FAA, in collaboration with some key developers of aviation risk assessment tools, an overview was produced that outlines the relevant approaches currently under development and/or in use for the safe separation assessment of advanced procedures in air traffic (Cohen and Hockaday, 1998).

In addition to TOPAZ, four other collision risk directed approaches, Analytic Blunder Risk Model (ABRM), Airspace Simulation and Analysis for Terminal instrument procedures (ASAT), ICAO's Collision Risk Model and Reduced Aircraft Separation Risk Assessment Model (RASRAM), were identified and reviewed; TOPAZ appeared to be most advanced in going beyond established approaches.

8 Further reading

For further reading on safety assessment methodology and modern safety cases for ATM, see:

1. S. Cohen and S. Hockaday, A concept paper for separation safety modelling, FAA/Eurocontrol, May 1998.
2. H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij and M.B. Klompstra, Accident risk assessment for advanced ATM, Proc. 2nd USA/Europe Air Traffic Management R&D Seminar, Orlando, 1-4 December 1998. Also in G.L. Donohue and A.G. Zellweger (eds.), *Air Transportation Systems Engineering*, Reston: AIAA. 2001, pp. 677-694. Also available as NLR-TP-2001-642, 2001.

3. H.A.P. Blom and H.B. Nijhuis, Safety certification framework in ATM, ARIBA Consolidation Report Part I, October 1999 (www.nlr.nl/public/hosted-sites/ariba/index.html). Also available as NLR-TR-99576, 1999.
4. H.A.P. Blom, M.H.C. Everdij and J. Daams, Modern Safety Cases for a new operation in air traffic, ARIBA Consolidation Report Part II, October 1999 (www.nlr.nl/public/hosted-sites/ariba/index.html) Also available as NLR-TR-99587, 1999.

9 Acronyms

ABRM	Analytic Blunder Risk Model
ASAT	Airspace Simulation and Analysis for Terminal instrument
ATCo	Air Traffic Controller
ATM	Air Traffic Management
CNS	Communication, Navigation and Surveillance
DCPN	Dynamically Coloured Petri Net
HRA	Human Reliability Analysis
ICAO	International Civil Aviation Organisation
NASPAC	National Airspace Systems Performance Analysis Capability
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
RAMS	Reorganized ATC Mathematical Simulator
RASRAM	Reduced Aircraft Separation Risk Assessment Model
TAAM	Total Airspace and Airport Modeller
TOPAZ	Traffic Organization and Perturbation AnalyZer