Imagining Safety in European Air Traffic Management

Short paper prepared for 3rd International Conference on Occupational Risk Prevention (ORP 2004; Santiago, Spain, June 2-4)

Barry Kirwan¹, Eric Perrin
Safety R&D, Eurocontrol Experimental Centre
Brétigny/Orge, F-91222
France
barry.kirwan@eurocontrol.int, eric.perrin@eurocontrol.int

Outline of Presentation

Air Traffic Management has been seen for some years as being a High Reliability Organisation (HRO). This means that it is very safe, compared to other industries. However, this implicit safety situation could change. Already in recent years there have been several tragic accidents at least partly attributable to ATM, most notably the Überlingen mid-air collision in 2002, the Milan runway incursion in 2001. Furthermore, despite the initial drop in civil air traffic following 9/11, traffic is likely to continue to increase due to passenger demand, thereby putting more stress on the system. To deal with this increased capacity of ATM, there are a range of initiatives in ATM and aviation more generally, such as giving the controller computerised assistance tools, considering new ways of structuring airspace and traffic flows, and delegating separation assurance in certain situations to the cockpit crew and systems. ATM is therefore showing potential signs of strain (accidents), is under pressure (capacity increases) and is undergoing an extended period of fundamental change. To anyone who has worked long enough in safety, these three ingredients mean that a serious safety system must be in place to avoid a sharp increase in safety-related events and ultimately more accidents. This requires a structured process to ensure that safety is built into conceptualisation and design phases of project and this is the road onto which the Eurocontrol Experimental Centre has stepped.

The problem with High Reliability Organisations is that it is not always clear why they are so reliable/safe. Indeed, with air traffic it appears that the system evolution until now, has managed to incorporate traffic increases in its stride. Certainly the training of controllers is excellent, and the controllers themselves as a cultural entity embody the hallmarks of professionalism and care about safety. This is not surprising since controllers have safety very directly in their hands – their actions, second to second, dictate whether aircraft stay apart or not. Additionally, it has to be said that pilots and cockpit systems (most notably TCAS, the traffic alert and collision avoidance system) add significant safety to our air travel also, and until recently (Überlingen) have been seen as an entirely independent safety net on top of those used on the ground by air traffic controllers. Lastly, and perhaps not least, there is what is called providence: there is a lot of space up there, even today, so there is a degree of luck or space, depending on your perspective, which undoubtedly has occasionally saved the day. It is perhaps a salient and tragic point that the two aircraft in the mid-air collision only just touched each other, a wing slicing through the last section of a tail-plane – another fraction of a second and they would have missed each other.

These aspects, a good overall system design and procedures, professional and very involved controllers, good cockpit crews and systems, and a healthy safety margin in the sky, are therefore no doubt part of the reasons ATM is still so (relatively) safe. But Agencies such as Eurocontrol have not been content with these aspects, in part because they are implicit and so less amenable to management, and also because other industries rely more on explicit safety management systems. Therefore, Eurocontrol has been developing a series of means to help

¹ Opinions expressed in this paper are those of the authors only and nor necessarily those of Eurocontrol or other organisations.
ensure that ATM does not lose its status as a HRO. These measures include formal safety management systems, risk assessment approaches, and attempts to develop an industrial safety learning system. The first means that European national organisations managing air traffic recognise their role and responsibilities in terms of safety. The second ensures that new systems and operational changes are checked using tried and tested safety assurance methods such as hazard identification, and risk assessment, to show that vulnerabilities are either removed from the system design or else are of a tolerably low risk. The third demands that national member states record and analyse incidents as a means to learning how safe they are and where their individual priorities are in terms of safety concerns. These measures, and others, are enshrined in a series of documents called ESARRs (Eurocontrol Safety Regulatory Requirements).

ATM safety is often called ‘implicit safety’, since it resides in the culture of operations, rather than in formal safety procedures and policies, or in terms of alarm systems (although some of these exist). It is recognised however, that ATM would benefit from the addition of ‘explicit’ safety measures such as those indicated in the ESARRs. Yet this move from implicit to explicit raises at least two fundamental questions:

- What is the danger of losing some of the implicit safety by a move to a more explicit safety basis? [in English – ‘throwing the baby out with the bathwater’]
- Should ATM simply borrow from other industries, or does it need either substantial adaptation of such approaches or indeed new ones?

The second of these is the main concern of this paper, though the first is referred to later on. ATM is in the position of trying to engineer a new safety approach. This is what is meant by the title of this paper – imagining safety – because ATM has moved from an implicit safety approach and being almost ‘backward’ in terms of safety assessment technology (e.g. compared to the nuclear power industry), to trying to envision new safety paradigms. The rest of this short paper therefore outlines seven novel approaches currently being considered in ATM, largely in research and development of new systems. These may flower, or wither, the future will tell, but in any case they are worthy of discussion and may also be relevant to other industries, whether or not they gain a foothold in ATM.

1. Safety Principles

Safety principles are not new, e.g. they have been used in the nuclear industry for some time. However, what is being attempted in ATM is the development of a causally-linked set of principles. This arose out of a simple question during a presentation of proposed safety initiatives. The question, evocative of a Total Quality Management or simply a Systems Thinking perspective, was as follows:

‘how do you know that these [the proposed safety initiatives] will make us safe?’

This led to an initial hierarchical mapping of the problems and challenges in safety, to see whether indeed the initiatives were tackling the key risk areas. This then grew into a more formalised ‘safety architecture’, starting with the top-level axiom that ‘ATM is safe’. Then, underneath, a set of boxes as to ‘why’ ATM is safe, and underneath each box further boxes etc. The stopping rule for this decomposition is when a measurable or otherwise solid foundation is reached, and it was realised in many cases that research was needed to create foundations in key areas that were otherwise unfounded. An extract of the mapping itself is shown in Figure 1. The mapping has focused on ATM, and on achieving safe basic operational systems, and on safety management. There is no doubt that the focus on safety management is because this is (explicitly) relatively new to ATM. The safety mapping reflects our concerns today, and therefore is not the ‘one and only true’ mapping of safety. Nevertheless, it enables an answer to the question posed earlier, and is open to argument and
scrutiny, and ultimately to learning (e.g. if some event occurs that does not fit the mapping). This safety architecture is still under development at Eurocontrol and also involving input from the FAA who, in particular, will validate the model from their own principles and will develop the larger aviation context into which ATM fits. Overall, this elaboration of safety principles can be used to identify safety shortcomings, and the hierarchy model has already revealed certain missing elements in current safety assessment and management approaches that has led to safety-related research activities discussed below.

2. Safety Assessment Toolkit

Another initiative that has been running in parallel in Europe and in the US, is the development of a toolkit for safety assessment in ATM. In a Eurocontrol study with NLR (the Dutch research agency), more than five hundred safety techniques from nine industries (including ATM and aviation) were reviewed to see their utility for ATM. Nineteen were identified as being adaptable for ATM, with a range of others identified as being potentially useful with further development. As an example, since the review techniques such as Bow-Tie Modelling (using fault & event tree techniques) Human Error Identification, Task Analysis and HAZOP have been applied in a number of development projects to show their power and limitations. Other techniques are now undergoing adaptation (e.g. common cause failure; human dependency analysis; formal expert judgement techniques). As these techniques are adapted and tried out on actual projects, decisions are made about their utility and if useful, they are documented along with case studies, and appended to the overall Safety Assessment Methodology (SAM) guidance material linked to ESARR 4 (risk assessment). Such guidance is then available for safety managers throughout Europe (or indeed worldwide).

3. Integrated Risk Picture & Cross-boundary Hazard Identification

There are many new concepts being developed for future ATM, e.g. conflict detection and resolution systems, new traffic management and airport throughput systems. Each can have its own safety assessment and assurance programme. But the future vision of e.g. 2012, may involve a number of such new tools or systems or concepts. What is the safety assessment of the overall system? How might these new elements interact, whether these are planned or unplanned interactions? Are there negative interactions that can be avoided, or even positive interactions, as yet unplanned into the system design concept, which could yield extra safety? Is the resultant system risk sensitive to the sequence and timing of implementation, assuming that such a future architecture cannot be implemented in a single ‘big bang’ solution? These are not easy questions, but require an answer. Therefore two new approaches are starting in safety R&D. The first is the development of an integrated risk picture, which will have as its scope gate-to-gate operations. The second is a means of assessing interactions between elements of the future system. The net result should be a risk picture that accurately can propose the true safety benefits of each new element, alone and in collaboration with other elements, and the dangers of unplanned interactions. This risk picture will also ultimately address the implementation strategy (its sequence and timing) as a function of safety. By taking a baseline risk picture of 2004, and one of 2012, a ‘roadmap’ can then be construed between the two risk pictures, and a risk-informed implementation strategy developed. This would also allow risk performance to be tracked during the implementation itself, via recording of rate of safety-related events during the intervening period, to see if we are ‘on track’, or not making safety targets, or if the roadmap itself needs refinement (due to unforeseen events).

4. Safety Learning

Every day, somewhere in Europe, there is an incident we can learn from. Perhaps it contains some elements of a precursor to an accident, perhaps not. We need to know. It is necessary to
record incidents, to have controllers able to report and discuss them openly, and to be able to have them analysed at a sufficient level to learn from them. There are now sufficient tools to detect incidents (losses of separation) automatically (e.g. Automatic Safety Monitoring Tool, ASMT), and sufficient analytical tools to be able to dissect them and reach both local and more widely applicable conclusions. What is missing, in many states, is the commitment and/or resource (is there a difference?) to carry out such collection and analysis. It is also necessary to remove certain ‘legal impediments’ that could see controllers prosecuted if they report honest mistakes (as has happened recently in the Netherlands). Other industries (e.g. the nuclear power industry) have this ability to collect safety information, analyse it, and share the safety knowledge. ATM needs this ability, and it needs it soon.

One novel aspect that is happening at the moment, however, is the analysis of incidents to generate lessons for future systems and tools. In Eurocontrol in a project called SAFLEARN, incidents are being analysed to learn lessons for future tools such as conflict resolution advisors, datalink, etc. This enables two things to happen: first, known problem areas should become avoidable with future systems (leading to safety progress), and second, as with the integrated risk picture), the analysts can look for ways to actually enhance safety further, perhaps going beyond the proposed system element’s original safety ‘role’.

5. Safety Evidence

European ATM has relied for many years on running simulations to check the acceptability of a new system element or tool, or airspace re-sectorisation, etc. Such simulations are expensive and very powerful tests of a new system addition, before it actually is developed for final implementation. However, although there may be questions about safety in such simulations, the way evidence is collected and analysed, leads to little hard evidence in terms of safety, despite for example having thirty controllers use a system in a high fidelity real-time simulation for three weeks. Work in Eurocontrol is therefore continuing to develop better methods to learn from simulations. This should ultimately link simulations to safety cases, and may include the ‘seeding’ of some safety case scenarios into simulations to see how controllers cope. Additionally, the simulation itself may raise some safety scenarios that may have been over-looked by the safety assessment. Thus, simulations can be seen as a way of deriving explicit evidence for safety considerations. At the moment the focus of this work is on real-time simulations, but in the future it aims to consider also prototyping simulations, fast-time simulations and model-based simulations.

6. Implicit Safety in Key Risk Areas

There are certain ‘key risk areas’ in ATM, for example ‘level busts’, ‘interactions between safety nets’ (ground and airborne), and ‘runway incursions’. There are measures being applied throughout Europe to try and reduce these events, but there is also a residual uncertainty about why they occur and how to prevent them more effectively. Therefore work is progressing, for example in the area of level busts and safety nets, to try and understand them in terms of explicit and implicit barriers and assumptions. A new method called SMART, based on the concepts of Professor James Reason and others, is being used to systematically elucidate all such barriers and determine which have failed in various recorded incidents. This enables a picture of the safety vulnerabilities to be developed, and can lead to the identification of new safety measures or barriers.

7. Safety Culture

When moving from implicit to a more explicit safety paradigm, there is a danger that safety culture, literally ‘the way we do safety’, will be changed for the worse. Safety culture is not
the clearest of fields of endeavour, but its importance is largely accepted. There are methods

to evaluate safety culture in a range of industries, but there have been very few applications to

ATM. Moreover, the need is not simply to measure safety culture and predict its degree of

change (leading to so-called ‘safety climate’ measurements on some arbitrary scale), but to be

able to diagnose how to maintain or improve actual safety culture throughout a period of

change. Work in Eurocontrol is therefore commencing in the area of safety culture impacts of

Airborne Separation Assurance, and its impact on controller safety effectiveness. If this is

effective, further work will commence on safety culture of future trans-national centres,

wherein different national boundaries will no longer be relevant, and different national safety

cultures must work together at an operational level.

At the same time, the Eurocontrol Experimental Centre itself has been evaluating its own

safety culture, which is not a common occurrence, to see how the general level of safety in

research can be improved. This also means that Eurocontrol is not simply saying ‘Do as I say,

not as I do’, as would otherwise be the case.

8. An observation on the long term future: ATM, Aviation, and Beyond: breaking
down the walls

An ATM system’s boundaries are not like those of a nuclear power plant, which can be

ultimately considered as a closed system, definable in terms of functionality and location, and

even in terms of maximum risk. ATM, in contrast, is an open system. Whilst there are

borders, these are easily transgressed. Moreover the national boundaries do not make much

sense in risk terms since many flights are international and a large proportion inter-

continental. Similarly, there can be distinctions made within the industry between En Route,

Airport, and Terminal Manoeuvring Area, but, to put it in the safety context, do the

passengers care which leg of a flight they will die on? Similarly, does it mean much to a

passenger to say that a CFIT (Controlled Flight into Terrain) was not ATM’s fault, but was

pilot error (i.e. aviation’s fault)? Should the ATM ‘world’ take any comfort from this? Should

not ATM be trying to consider not just its own patch but how to help passenger safety

overall?

From a personal perspective, the days of considering ATM safety and aviation safety

separately seem numbered, though undoubtedly in terms of years. If passenger (and other

humans around the aircraft) is paramount, then the best way of tackling safety should be

pursued. Compartmentalising aviation safety and ATM safety in the past has occluded such

considerations as TCAS-ground based alarm system interactions, and more generally leads to

a vagueness about the pilot side by ATM safety professionals, or controller behaviour by their

aviation counter-parts. The two, particularly in Europe, need to be brought together more

closely so that risks at the ATM/aviation ‘borders’ are not under-assessed.

Ultimately, safety assurance will have to go even further. If an airport suddenly closes due to

a fire, this causes more travel on road and by train, thus ‘exporting’ risk to other parts of the

public transport sector. And environmental considerations around airports may lead to
difficult landing and take-off procedures that ultimately result in crashes. ATM is an open

system, and ultimately must be considered within the total system, or at least the total

transport system. However, this is possibly along way off. There are many steps to be taken

beforehand.

Conclusions

Seven new approaches being developed in safety R&D in ATM have been outlined. These are

seen as an appropriate response to the challenge posed by ATM’s rate of growth and change.

Time will tell which, if any, of these ‘imaginings’ of safety become a sustained reality. What
is hoped for is that they have sufficient time to mature and have useful impact, before another major accident reminds us of how little we know, and of just how hard it is to be this safe.

**Figure 1 – Part of Preliminary Safety Principles Architecture for ATM**