

A SYSTEMIC MODEL OF ATM SAFETY: THE INTEGRATED RISK PICTURE

Eric PERRIN, Barry KIRWAN, EUROCONTROL, France, Ron STROUP, FAA, US

Abstract

There are many new concepts being developed for future ATM, e.g. conflict detection and resolution systems, new traffic management and airport throughput systems, etc. Each can have its own safety assessment and assurance programme. But the future vision of e.g. 2020, may involve a number of such new tools or systems or concepts. This raises a number of questions:

- What is the safety assessment of the overall system?
- How might these new elements interact?
- 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?
- Where are the strong and weak safety areas in the overall system?
- Is the resultant system risk sensitive to the sequence and timing of implementation?

These are not easy questions, but deserve an answer. Therefore an Integrated Risk Picture (IRP) is being developed within EUROCONTROL which has as its scope gate-to-gate operations. This development is closely co-ordinated with the FAA within the scope of the FAA/EUROCONTROL Action Plan 15 on Safety. What is being achieved in this paper is the description of the baseline risk picture for 2005 and the risk picture for 2012 (predictive mode for the Single European Sky implementation). Lessons learnt related to practical techniques for risk analysis are provided as well.

Introduction

Background

The EUROCONTROL strategy for safety in Air Traffic Management (ATM) requires a detailed understanding of the potential contribution of ATM to aviation accidents, in order to optimise safety improvement efforts. At present, the safety of new

ATM tools and concepts is ensured through a detailed safety assessment process, but until now there has been no system for evaluating their combined effects on safety. It is possible that unrecognised interdependencies between ATM systems may prevent their planned safety benefits from being realised. EUROCONTROL therefore decided to construct an Integrated Risk Picture (IRP), showing the overall ATM contribution to aviation accident risks, and highlighting possible interdependencies, so that the priorities for safety improvements can be identified in a systematic way.

The ATM 2000+ Strategy sets the objective of ensuring that the numbers of ATM induced accidents do not increase and, where possible, decrease. Since demand for air travel is expected to double by 2015, this implies that the rate of accidents per flight hour must be halved. Following recent serious aviation accidents, the EUROCONTROL High Level European Action Group for ATM Safety (AGAS) identified priority actions to improve safety in European airspace, including research to develop an integrated risk picture for ATM in Europe.

The project to develop the IRP was initiated by the EUROCONTROL Experimental Centre (EEC), working with EUROCONTROL DAP/SAF (Directorate of Programmes / Safety Enhancement), and was closely co-ordinated with the FAA within the scope of the FAA/EUROCONTROL Action Plan 15 on Safety.

Required Result

The purpose of developing the IRP is to show the relative safety priorities in the gate-to-gate ATM cycle. To do this, it must be capable of showing:

- The overall contribution of ATM to aviation risk, i.e. the reduction in accident risk that would result if ATM were somehow perfect.
- The relative importance of different accident categories and the causal factors underlying the ATM contribution to risk.
- The contribution of ATM in both causing and preventing aviation accidents. This will

show areas where risk reduction would be desirable in principle.

- The relative importance of the different phases of the G2G cycle, e.g. the effects of strategic versus tactical conflict management.
- The effects of interdependencies between different ATM sub-systems.
- The safety impacts of changes in ATM as it develops in the future (predictive mode).

It must be able to combine all the above contributions and influences in consistent units, in order to make clear comparisons between them. This is necessary to show the benefits that could be achieved by improvements to the various safeguards that control the ATM contribution to risk.

Consequently, an “integrated” risk picture is primarily one that shows the sum of the effects of all causal factors within the G2G cycle. However, this is not a simple matter of adding up independently estimated parts of the risk picture, because of interdependencies (common cause failures and interactions between ATM sub-components) between them.

Presently, two risk pictures have been developed: (1) the baseline risk picture (“IRP 2005”); and (2) a future benchmark risk picture (“IRP 2012”).

Paper Structure

The “stamp image summary” below is structuring the paper around Barrier Model, Influence Model, Data Sources, Risk Picture Results, Validation and Uses

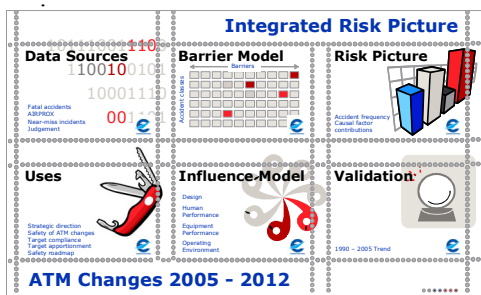


Figure 1: IRP – an overview

Modeling overview

The IRP has been developed using techniques whose applicability to aviation risk modeling has been proven in practice. The chosen techniques are fault trees, event trees and influence diagrams. This

is not intended to dismiss the potential of other techniques; merely to ensure that the project meets its objectives within the available time frame.

The IRP is the output of a “risk model”, representing the risks of aviation accidents, with particular emphasis on ATM contributions. In order to ensure that the risk model reflects ATM as it develops in the future, the risk model is founded on an “ATM model”, describing the ATM system whose risks are to be modeled (Figure 2).

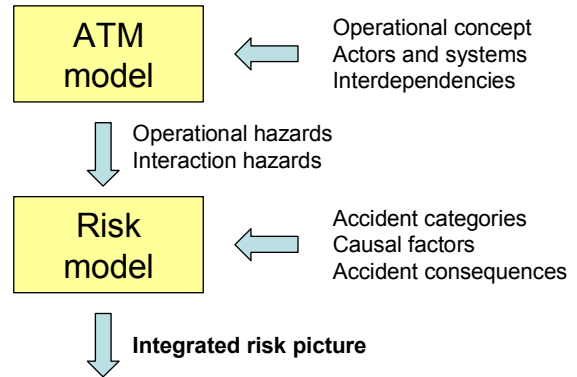


Figure 2: Modelling approach

The chosen structure of the risk model is shown in Figure 3. A separate causal model is used for each accident category, constructed using fault trees. These represent the distinct causal factors such as technical failures and human errors, which are the immediate causes of failure of the barriers against accidents. The fault trees are quantified using historical accident and incident experience, with judgmental modifications to represent future ATM changes.

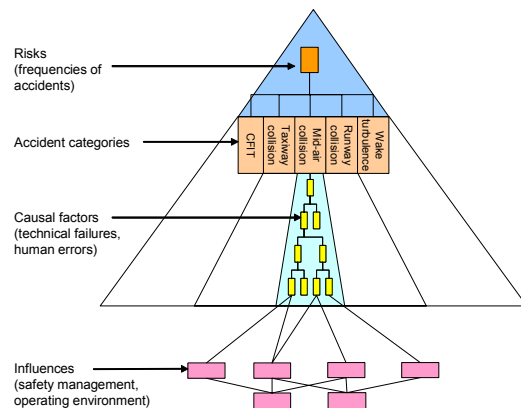


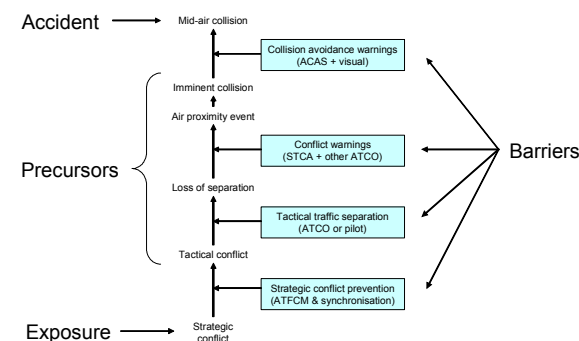
Figure 3: Overall Risk Model Structure

An influence model is used to show the effects of more diffuse factors such as safety management and operating environment, which are usually the underlying causes of accidents. One influence model is used to cover all accident categories. This represents common causes of apparently separate failures. It also avoids the exponential growth in

tree size that can occur if a fault tree is expanded to cover management influences. The structure of the influence model is based on the ATM model, so as to highlight the effects of future ATM changes. The influence model is quantified using the influences apparent in historical accidents and incidents, with judgemental modifications to represent future ATM changes. The output of the influence model is a set of modification factors, which are applied to the frequencies and probabilities of the base events of the fault tree models. This allows the accident frequencies and causal breakdowns to be estimated for any specific situation.

In order to enable data (see data sources below) to be superimposed onto the fault tree structure given the huge number of different causes associated with each event, three possible options have been considered: 1) Develop a vast meta-tree to which were added all the causes from every event (rejected as too unwieldy), 2) Develop a large network (rejected as losing the explanatory power of a fault tree) and 3) Developing a barrier model and relating all events to these barriers (chosen option).

To develop the fault tree, the concept is represented in a barrier model (Figure 4) showing a series of barriers and a resulting sequence of accident precursors corresponding to incidents where some (but not all) of the barriers have failed. Failure (or ineffectiveness) of the barriers is here defined in a very wide sense, including not only technical failures but also human failures to respond promptly enough to prevent the next stage precursor. In reality, barriers do not always fail in the strict sequence shown, but this is a useful simplifying assumption in forming the model.



D Figure 4: Barrier Diagram for Mid-Air Collision

Having simplified the analysis down to selected barriers for each accident category, some additional complication was then re-introduced via the use of “scenarios” to reflect the fact that certain groups of events did not always have to fail all barriers. Overall the barrier model conforms to the ICAO Doc 9854 [1] description of Conflict Management [2]:

Whose purpose is to limit, to a tolerable level, the risk of collision between aircraft and hazards;

Which is applied in three layers: strategic conflict management; separation provision; and collision avoidance.

As mentioned above, underlying the direct human and technical causes of accidents are various organizational and cultural factors, which cannot be satisfactorily represented as distinct failure events in a fault tree. These factors are invariably influential to some extent in an accident, but no specific failure is necessary or sufficient for the accident to occur.

Such causal factors are most efficiently modeled separately from the fault tree, having an *influence* on selected bottom events in the tree. In turn, they may be influenced by other causal factors, and several factors may combine to influence individual events in the fault tree.

The chosen structure for the IRP influence model is intended to highlight the interdependence of ATM tasks, as expressed through the ATM model. This requires each base event in the fault tree to be associated with a task in the ATM model. The influences on each task are then categorized as (Figure 5):

- Performance of the actor responsible for the task (e.g. ATCO, flight crew etc). This is broken down into human factors fundamentals as proposed in [3].
- Performance of the equipment provided for the task (e.g. ATC systems, aircraft systems etc).
- Quality of the inputs to the task, which result from the performance of other connected tasks.
- Quality of the managed constraints (e.g. airport/airspace design).
- Nature of the operating environment (e.g. traffic, weather, terrain etc).

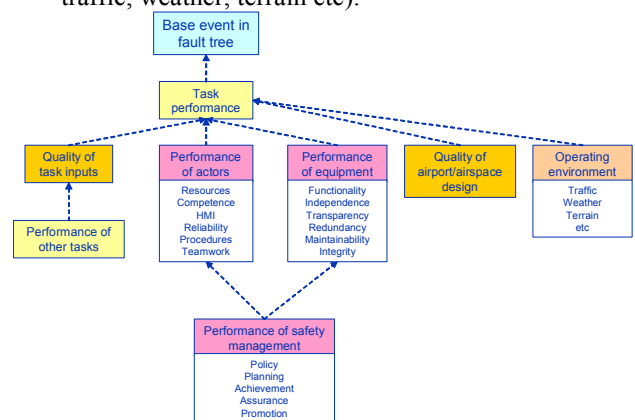


Figure 5: Generic Influence Model

Quantification & sources

Quantification of the fault tree for IRP 2005 begins from the actual historical frequency of accidents, and proceeds gate by gate in a top-down sequence towards the base events of the fault tree. Once the complete set of base events has been quantified, these generic frequencies/probabilities may be adjusted to represent any specific case and effects propagated bottom-up through the tree to predict the risk picture for that case. Predicted cases may be obtained for future ATM changes (e.g. 2012), retrospective validation (e.g. 1990), or for specific units (e.g. airports, airspaces or even individual flights).

Historical experience has been used to supply three types of data for the model:

- Accident and precursor frequencies.
- Causal breakdowns.
- Maximum effects of influences

For quantification of accident and precursor frequencies, suitable data sources were restricted to those for which exposed populations were known.

For each accident and incident, a text description of the known causal factors has been obtained and used to identify the reasons for failure of each of the barriers. These failures have been categorised according to the base events in the fault trees. Other influences that might potentially have prevented the barrier failures are considered separately in the influence model.

The barrier failures and influences identified for each accident form the basis of the estimation of the potential benefits of improvements to these aspects of ATM, which form part of the IRP results.

In order to predict the ATM contribution to accident risk in 2012, the IRP attempts to define all expected ATM changes, together with changes in traffic and the operating environment, and estimate their effects through the risk model. The combined effects of all changes forms the prediction of overall risks and ATM contributions in 2012.

Although IRP is able to make use of detailed safety assessments of ATM changes, few of these are available at present, and hence the modelled effects are mainly based on judgements.

For further reading ([4]):

The connection between the influence model and the base events of the fault tree is expressed as a modification factor (MF), which depends on a performance score (PS) for each task, on a scale from 0 to 100. The performance score is benchmarked as follows:

- PS = 70 represents ECAC average in 2005, for which MF is 1 by definition.
- PS = 100 represents “perfect performance”, meaning that failures would be reduced by the maximum effect (ME) of the influence identified in the accident and incident data.

A smooth logarithmic variation in MF is assumed for other values of PS (Figure 6).

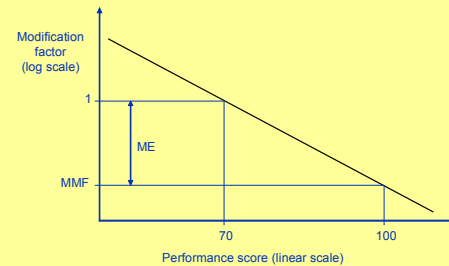


Figure 6: Conversion PS-MF

$$MF_{ij} = \frac{F(E_i | I_j)}{F_G(E_i)}$$

where:

- E_i = base event in the fault tree, for $i = 1$ to N
- N = number of base events in the fault tree
- $F(E_i)$ = case-specific frequency of event E_i
- $F_G(E_i)$ = generic frequency of event E_i
- I_j = influence, for $j = 1$ to Q
- Q = number of influences

$$MF_{ij} = 10^{\left[\frac{PS_j - 70}{30} \log(1 - ME_{ij}) \right]}$$

IRP Type of Results

The following accident categories are modeled in detail in the IRP in order to quantify the ATM contributions to them:

- Mid-air collision - two aircraft come into contact with each other while both are in flight.
- Runway collision - two aircraft come into contact with each other on the airport runway, including cases where one aircraft is on the ground and the other is in flight close to the ground. At present, collisions with obstacles, vehicles or people on the runway are not modelled.
- Taxiway collision - two aircraft come into contact with each other on the airport manoeuvring area. This includes collisions where one aircraft is parked, being pushed back, under tow, or taxiing up to the point of runway entry.
- Controlled flight into terrain (CFIT) - an aircraft collides with terrain, water or another obstacle while in flight without prior loss of control.
- Wake turbulence accident - an aircraft suffers major damage or serious injuries to occupants due to an encounter with wake turbulence from another aircraft.

For completeness, results are also provided for the following accident categories based on historical statistics, although ATM is not expected to make a major contribution to them: Loss of control in flight.

- Loss of control in take-off.
- Loss of control in landing.
- Structural accident.
- Fire/explosion.

The measure of risk is the frequency of fatal and non-fatal accidents. The frequency is the average number of accident involvements per flight. It is a frequency of involvement in an accident, since collisions involving two commercial aircraft are counted as two involvements. Fatal accidents are defined as accidents causing at least one fatality among people on-board, on the ground or in other aircraft. In order to estimate the frequencies of fatal accidents, the IRP also

quantifies other measures of risk that may be precursors to such events (Figure 7).

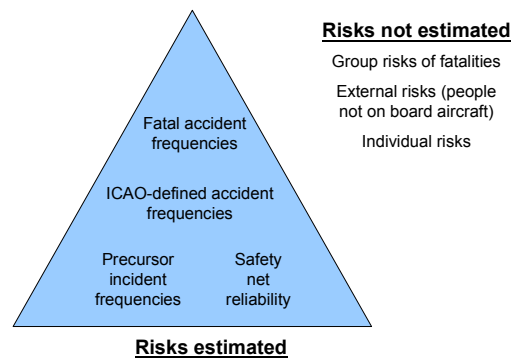


Figure 7: Scope of Risk Estimates

The risk results are averages across all commercial air traffic within the ECAC region. This includes all scheduled and non-scheduled passenger and cargo operations, but excludes military and general aviation traffic (except where they are involved in an accident with commercial traffic).

The risk model is capable of predicting the frequencies of fatal and non-fatal accidents and incidents, and different types of causal breakdowns for any specified situation. These risks are averages over all commercial (passenger and cargo) flights in the ECAC region.

Accidents are usually the result of a combination of causal factors and influences. In the risk results, these are categorized into four groups:

- Direct causes of the failure of the primary barriers against accidents. The primary barrier is considered to be tactical separation in the case of collision and wake turbulence, runway entry and take-off procedures in the case of runway collision, ground movement procedures in the case of taxiway collision, and trajectory commands in the case of CFIT. Failures may be caused by ATC or pilots, typically involving acts of commission, or technical failures in ATC equipment or avionics.
- Prevention failures, which are the causes of failure of the various barriers intended to provide warnings that an accident may be imminent. These may be caused by ATC or pilots, typically involving acts of omission or technical failures in safety nets. Communication problems, where ATC and pilots jointly contribute to failure of the primary barrier, are also included in this group.

- Prevention opportunities, where extended coverage of safety equipment or enhanced performance by ATC or pilots would have been able to prevent the accident, even though they would not be regarded as “failures” in an accident investigation.
- Indirect influences, where performance of one element of ATM leads to errors or failures by another element (e.g. poor controller performance influencing pilot errors). These exclude direct influences that are modelled in the categories above.
- Dissemination of the techniques used in the IRP through peer-reviewed journals or other risk studies.
- Evaluation of independent proposals for improving accident safety. If these were either consistent with conclusions from the IRP or different for a clear reason, this could be considered a validation of it.
- Expert review of the conclusions from the IRP. If the recommendations from the IRP were supported by industry experts, this could also be considered a validation of the IRP.

Causal breakdowns are expressed as “contributions” to the fatal accident frequency. This is a simple estimate of the maximum fractional reduction in accident frequency that would occur if the causal factor were eliminated and other factors remained constant.

[4]:

- Presents the 2005 baseline risk picture, showing the current overall ATM contribution to accident risks for commercial aircraft in Europe
- Describes how the 2012 risk picture has been developed through quantification of the effects of all ATM changes that are planned to occur by then.

Validation & Uncertainties

Classical validation of the IRP model, in the sense of an independent dataset that is shown to agree with the IRP results to within an acceptable level of accuracy, has been up to now impractical for this type of causal model. This is because: (1) Most available data has been used in constructing the model; and (2) No other model seems to be currently able to obtain comparable results.

The IRP has been validated against historical experience since 1990. This date was chosen because it is the beginning of the period for which accident data has been analyzed in detail. Older data would show more significant differences in risks, but the aircraft and the ATM practices would be less consistent with the current risk model. . It would be desirable to obtain more thorough validation. Possible approaches include:

- Validation against accident and incident experience in the coming years.
- Retrospective prediction of risks for specific regions or units for which there is accident or incident data suitable for validation of aspects of the risk model.
- The overall fatal accident frequencies are based on an average of 13 accidents per accident category, consisting of the relevant events in the overall accident dataset. If occurrences follow a Poisson distribution, the 90% confidence ranges for the frequencies would be from approximately 0.6x to 1.6x the estimated values. Similar uncertainties will apply to the ICAO accident frequencies, since they have been derived from the fatal frequencies, not from independent larger datasets.
- The individual causal factors are each based on an average of approximately 3 incidents, which are the relevant events in the overall accident and incident dataset. If occurrences follow a Poisson distribution, the 90% confidence ranges for the contributions would be from approximately 0.25x to 3x the estimated values. In future work, it would be desirable to reduce these uncertainties by analysing more accidents and incidents.
- The contributions for the ATM elements or for ATM as a whole combine the contributions from several causal factors. Provided the uncertainties in the components are independent, this will tend to reduce the uncertainties in the summed values. As a rough indication, it is judged

that the 90% confidence ranges for the overall ATM contributions would be from approximately 0.5x to 2x the estimated values. These uncertainties could be explored further through sensitivity tests on selected key results.

Use Cases sing Styles

The IRP may be used in many different ways, each requiring different types of results. The following use cases are being considered presently:

Strategic direction for safety improvements and safety research: For this, the baseline risk picture indicates the priorities and key safety issues.

Safety impacts of individual ATM changes: For the 2012 benchmark, the IRP has modeled the safety impacts of all known ATM changes, and the detailed results include a high level qualitative identification of their main safety benefits and hazards, as well as a model of their quantitative effects.

Overall safety target compliance: Based on current assumptions, the results for 2012 show that in order to comply with the ATM 2000+ target of no increase in the number of ATM induced accidents, it will be necessary to implement all the planned ATM safety improvements by 2012. Comparison with the ESARR4 [5] target of 1.55×10^{-8} per flight hour for ATM contributions is sensitive to the precise definitions used, but it would be necessary to select additional safety improvements beyond 2012 to achieve compliance.

Safety target apportionment: Once the overall ATM risks for the future case meet the overall target, the modeled performance of each ATM element can be used as its safety objective. Thus IRP provides a convenient way of apportioning safety targets that takes account of actual attainment and interactions with expected future developments.

Risk picture for specific units: The IRP has the capability to make predictions of risks for a specific unit (airport, airspace or individual flight). However, this capability requires validation.

Consistency of safety cases: The IRP fault tree model can be recast as a standard event tree for different types of failures, which can help achieve consistency in the modeling for safety assessments of individual projects.

Safety roadmap: The IRP can be used to make risk predictions for individual ATM changes and groups of ATM changes, combined with different implementation dates or growths in safety net usage. This allows definition of a sequence of

ATM changes to ensure that risks are decreased as soon as possible.

Alignment of severity classifications: The IRP includes a set of incidents of different severities, which are precursors of each accident category. These can be used to derive quantitative targets consistent with the ESARR4 severity classification.

Safety performance monitoring: The precursor incidents are also suitable for monitoring of trends in actual safety performance, as well as new data gathering to validate and improve the IRP.

Conclusions and further work

This type of risk modeling is challenging and not yet fully mature. At present, the results are sensitive to interpretations. For instance, IRP 2005 presents point estimates of the contributions of ATM elements to aviation risks. Some of these are based closely on large, well-established datasets, whereas others are based on uncertain judgments. It would be desirable if the source of the data (pedigree) could be made plain, along with the collected results of sensitivity analyses, and if possible the degree of uncertainty in the results could be estimated. It will not be possible to show this information succinctly for all results, but it would be possible to develop a format that showed all necessary information for selected results. However, it is believed that the IRP is suitable for the wide range of intended uses and recommendation of safety improvements. Progressive improvement would still be desirable through analysis of further data, incorporation of expert judgments, alternative validation exercises, improvements in user-required capabilities, and improved consistency with safety targets.

Over 2007-2008, the major development will consist in developing the IRP into a tool that can show how risks will be affected as the Operational Improvements (OIs) are implemented and traffic grows. IRP 2005/2012 predicts the current and future risk, but is not optimized to show the changes in risk between these points and explore alternative implementation strategies to minimize risks. The so-called *Safety Roadmap* will address the definition of the sequence of changes between the present and the planned future ATM system, so that the safety target is met at all stages, and in particular that risks are decreased where possible. It will enable to appraise whether the predicted safety improvements throughout the period are not outweighed by the extra traffic. Ultimately, the Roadmap will include safety monitoring targets, so that as OIs are introduced, it can be determined if expected safety impacts are realized, exceeded, or

fall short. This will lead to a true risk management system based on operational feedback.

The elements that you will need for your paper have been formatted for you through the use of the “styles” capability of the software. Styles are selected from the box on the far left of the tool bar. Note: if you position your cursor anywhere in this paragraph, the “styles” box will say “Body Text;” we’ve also noted different styles in parentheses following some of the elements on this page of these instructions (Title, Author, Heading 1, Heading 2, etc).

To use styles, you can either select the style you wish to apply and start typing, or select the text you wish to apply a style to; then, using the mouse, point to the style box on the toolbar. Click once on the downward pointing arrow to the right, and select the appropriate style.

References

- [1]. ICAO Document 9854, Global Air Traffic Management Operational Concept, 1st Edition, 2005
- [2]. EUROCONTROL, Safety Assessment - Success and Failure Approaches, draft, 2006
http://www.a2di.com/SAM_Newsletter/08/HTML/doc/Success&failure.doc
- [3]. EUROCONTROL, Safety Screening Technique for the Future Air Traffic Management Safety Strategy”, 2005
- [4]. EUROCONTROL, Main Report for the 2005/2012 Integrated Risk Picture for Air Traffic Management in Europe, 2006
http://www.eurocontrol.int/eec/public/related_links/safety_documents.html
- [5]. EUROCONTROL, Risk Assessment and Mitigation in ATM, ESARR4, 05-04-2001, Edition: 1.0
http://www.eurocontrol.int/src/public/standard_package/src_deliverables.html

Biography

Mr. Eric Perrin joined EUROCONTROL in 2002 as GPS Ground-Based Augmentation System (GBAS) Manager. He holds an Engineer degree in Aeronautics and Computer Science from the French Civil Aviation School (ENAC) (1993). Eric Perrin has twelve years’ experience in aviation, six of which have been spent on safety assessment and management. Currently he is Deputy Safety Research Team Manager and Safety Management System (SMS) Manager at the EUROCONTROL Experimental Centre.

Dr Barry Kirwan joined EUROCONTROL in 2002, and was formerly Head of Human Factors for National Air Traffic Services (NATS) in the UK, and prior to that was Head of Human Reliability in British Nuclear Fuels. He holds degrees in Psychology, Ergonomics and Human Reliability Assessment, and lectured for five years in these areas at the University of Birmingham in the UK. He has worked in the area of Human Factors and Safety for twenty-five years in nuclear power, offshore oil and gas, chemical, and air traffic management sectors of industry. He currently leads a small team of safety and Human Factors people in EUROCONTROL’s R&D Centre, South of Paris, working on a range of short and medium term issues such as safety assessment, safety culture, and safety nets.

Mr. Ronald Stroup joined the Federal Aviation Administration as an Aerospace Engineer in 1989. He holds a Bachelor of Science degree in Avionics Engineering from Parks College of Saint Louis University (1989) and a Masters in Information Management from Syracuse University (2006). Mr. Stroup served, as a Systems Engineer in the Aircraft Certification Services’ Chicago Aircraft Certification Office and in 1997 became the Software Technology Specialist for the Aircraft Certification Service. In 1998, Mr. Stroup served as the Software Safety and Certification Lead for the Office of Information Services and Chief Information Officer. In 2002, Mr. Stroup completed the DOD’s Advanced Management Program and holds a NSTISSI 4011 Certificate in Information System Security. In March 2003, Mr. Stroup became the Chief System Engineer for Airborne and Ground System Integration for the FAA Air Traffic Organization.

The views expressed herein are authors’ own and do not necessarily reflect EUROCONTROL policy.