Cranfield UNIVERSITY

AIR TRAFFIC MANAGEMENT ACCIDENT RISK
PART 2: REPAIRING THE DEFICIENCIES OF ESARR4

Peter Brooker

Version 1.0
6 May 2005
Cranfield Research Report PB/5/2/05

ISBN 1 861941 17 X

Contact details:

Professor Peter Brooker
Cranfield University
Building 83
Cranfield
Bedfordshire MK43 0AL
England
Tel +44 (0) 1234 750111 Extn.5086
Fax +44 (0) 1234 750192
e-mail: p.brooker@cranfield.ac.uk

CONTENTS

FIGURES

AIR TRAFFIC MANAGEMENT ACCIDENT RISK
PART 2: REPAIRING THE DEFICIENCIES OF ESARR4

Peter Brooker

Cranfield University

"But he has nothing on at all."
'The Emperor's New Suit' by Hans Christian Andersen

ABSTRACT

This is a critique of ESARR4 and its main supporting documents. ESARR4 is the Eurocontrol Safety Regulatory Requirement Number 4 (Eurocontrol SRC, 2001): 'Risk Assessment and Mitigation in ATM', ATM standing for Air Traffic Management. It is demonstrated that ESARR4 and its supporting documents are defective. There is a lack of clarity about responsibilities for ATM safety. The claims ESARR4 etc make for its proposed methodologies are overstated – not supported by sound evidence from real world hazard analysis. Serious negative effects from this defective document include mis-allocation of scarce safety resources and the diversion of attention away from real safety improvements – wasteful of regulators' and managers' time. Suggestions are made for repairing these deficiencies. The most important underlying change would be a refocusing on practical safety assessment based on methods that have already demonstrated their merits.

1. INTRODUCTION

The prime goal of the Air Traffic Management (ATM) system is to control accident risk. This leads to some important questions:

> What are the essential ingredients for ATM systems to be designed safely?
>
> How best can the lessons learned from accidents and incidents influence safe system design?
>
> What do design safety targets really mean and imply for risk modelling?
>
> In what circumstances can future accident risk really be modelled with sufficient precision?
>
> If risk cannot be estimated with precision, then how is safety to be assured with traffic growth and operational/technical changes?

This is the second of two papers endeavouring to answer these questions through an analysis of the nature of accidents, causal factors and practical collision risk modelling. The main theme of Part 1 (Brooker, 2005a) is how best to combine sound safety evidence and real world hazard analysis in a coherent and systematic framework. This is achieved through a variety of general principles and factual observations about the nature of ATM safety and risk modelling methodologies.

This second paper, which rests on Part 1, applies this framework and thinking to the important ESARR4 document and its supporting material, first through a critique and then by an attempt to repair ESARR4's methodology. ESARR4 is the Eurocontrol Safety Regulatory Requirement Number 4 (Eurocontrol, 2001), which is entitled 'Risk Assessment and Mitigation in ATM'. To quote:

> "*This requirement concerns the use of risk assessment and mitigation, including hazard identification, in Air Traffic Management when introducing and/or planning changes to the ATM System. This requirement shall apply to all providers of ATM services in respect of those parts of the ATM/CNS System and supporting services for which they have managerial control.*" [All direct quotes from ESARR4 etc here are put into italic font on their first appearance.]

The main supporting document to ESARR4 is 'EAM4/GUI1', which is the Eurocontrol SRC's (2003) 'Explanatory Material on ESARR4 Requirements'.

The present ESARR4 material, whilst no doubt being created with good intentions, is defective. It will be demonstrated that it lacks the necessary rigour for regulatory material in a vital safety domain.

ESARR4's main technical problems are with its incomplete picture of ATM safety, the understanding of (and evidence from) real-world hazard analysis, and the delivery of safety improvements. This then leads to subsequent flaws in the intended application of ESARR4, with a lack of clarity about safety responsibilities. This could produce mis-allocations of scarce safety resources, and potentially divert attention away from real safety improvements, by being wasteful of regulators' and managers' time.

2. HOW IS ESARR4 DEFECTIVE?

ESARR4 is a SRC Requirement. An Ideal Requirement would look something like Figure 1.

Figure 1. An Ideal Requirement structure

The diagram focuses on the word 'specified'. The data needed to do the job is clearly set out. It is then to be processed in well-defined ways. The data would be a description of the ATM sub-system and its relevant performance. The process would be a logical set of calculations and well-defined assessment procedures.

ESARR4 does not deliver. It does not produce answers usable by prudent decision-makers. It is in practice more complex and less helpful than Figure 1. Its operation is more like Figure 2.

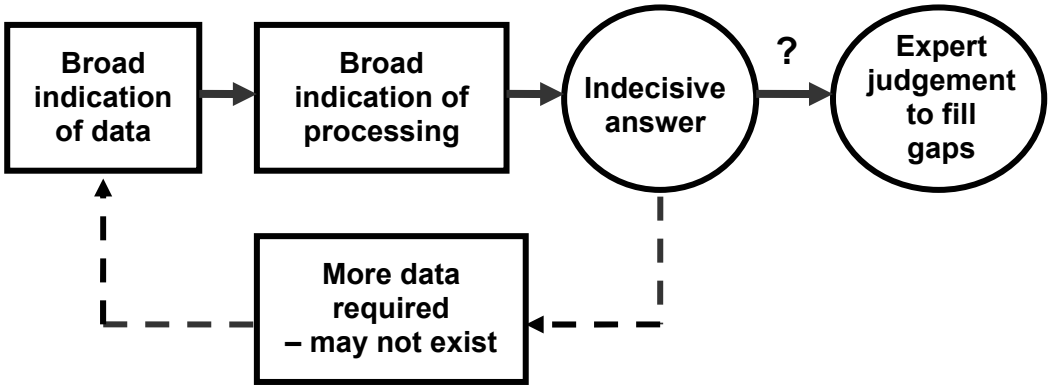

Figure 2. How ESARR4 fails

The problem is that the specific nature of the Requirement is no longer there. Specific statements are in fact just broad ones. The answer that comes out at the end is usually an indecisive one. This leads to a need for more data – which often does not exist – or the need for some kind of 'expert judgement' in order to make a decision. Expert judgement is open to many criticisms – illustrated in Part 1. Consistency may just be consistently wrong. Differences in viewpoint may be expressions of people's pessimism or optimism.

The following sections describe how ESARR4 and its supporting material are defective and hence will not work in practice, and then set out some ways of repairing ESARR4. Some practical and technical flaws of ESARR4 are:

- Not based on practically proven techniques.
- Reliance on Probabilistic Safety Assessment – PSA
- Ignoring risk assessment techniques successfully used in ATM
- Giving no guidance about practical methods
- Not distinguishing between different types of ATM sub-system
- Unstructured use of expert judgement
- Careless use of 'worst case'

Safety regulations such as ESARR4 must be demonstrated both to be rational and to focus people's attention on aspects that will deliver real safety improvements. By their nature, safety regulations tend to generate further explanatory material, guidance statements and advice. When examined as a whole, it is essential that there is significant worthwhile and valid content. It would be a serious lapse to generate unnecessary and/or unproductive bureaucracy in safety regulation.

Draft safety regulations need to be exposed to scrutiny by the full range of professional criticism, with all the key source material underpinning regulations being in the public domain. ESARR4's logic rests on a number of assumptions, some implicit, which all need to be brought out in the open. Thus, the scope of definitions and characteristics should be as comprehensive and open as possible, and safety responsibilities should be clear, complete and comprehensive.

The present abstract system approach of ESARR4, with its apparent 'one size fits all' approach is unlikely to deliver real safety benefits. Ideals do not necessarily exist. When there is a feasible quantitative way of doing something, then this should be explained clearly, with real-life examples. When there is not good evidence that a feasible quantitative way of doing something exists, then the conditions in which this holds should be clearly stated, so that resources are not wasted in fruitless activity.

3. CRITIQUE OF ESARR4

This section is a detailed critique of the text and arguments of ESARR4. The sub-headings follow the order of that document. All extracts from ESARR4 are put into italic font when first quoted, and identified by the ESARR4 paragraph number. The headings from ESARR4 are in bold italic font

Much of ESARR4 is concerned with routine 'good housekeeping' and safety process/documentation issues – the kinds of things that are clearly set out in Profit (1995). The problems arise where assumptions are made, sometimes implicitly, about the kinds of strategic safety and hazard analysis issues examined in the previous sections here: the focus here is very much on these critical pieces of text.

1 Scope

Para 1.1 states that:

This requirement concerns the use of a quantitative risk based-approach in Air Traffic Management when introducing and/or planning changes to the ATM System.

The phrase 'quantitative risk-based approach' certainly sounds splendid, but caution is needed. Virtually all ATM safety-related numbers are estimates based on statistical analysis and mathematical/computer modelling. Such estimates may have very different degrees of precision. They may have limited accuracy, may not be verifiable against operational data, and may rest on untestable assumptions. They may be affected by very large statistical fluctuations inherent in observations and extrapolations of rare events. Safety resources must not be wasted on conjectural mathematical exercises producing estimates of very low precision, which are dependent on many assumptions.

The second key point concerns the phrase 'Air Traffic Management' and 'ATM System'. These do not mean what has been discussed in Part 1, which essentially uses 'ATC' to mean ESARR4's 'ATM'. The definitions in ESARR4 are:

> ***"ATM*** *The aggregation of ground based (comprising variously ATS, ASM, ATFM) and airborne functions required to ensure the safe and efficient movement of aircraft during all appropriate phases of operations.*
>
> ***ATM System*** *ATM System is a part of ANS System composed of a Ground Based ATM component and an airborne ATM component.*
>
> **Notes:-**
>
> *a. The ATM System includes the three constituent elements: human, procedures and equipment (hardware and software).*
>
> *b. The ATM system assumes the existence of a supporting CNS system."*
>
> ***CNS/ATM*** *The aggregation of functions used in provision of CNS services and used by ATM.*
>
> ***CNS system*** *All the hardware and software that make up a function, tool or application that is used to provide one or more air traffic management services. The CNS system is an enabler to the provision of ATM services.*

In the Abstract of ESARR4, it is noted that:

> *This requirement shall apply to all providers of ATM services in respect of those parts of the ATM/CNS System and supporting services for which they have managerial control.*

But, strangely, the phrase ATM/CNS System appears nowhere in the text.

From these definitions, it is clear that CNS is taken to include data processing (DP) functions. The sentence in the Abstract then actually makes it (apparently) clear that CNS is to be included in the ATM/CNS System for which ESARR4 applies. Therefore, to all intents and purposes set out in ESARR4, CNS (including DP) is a full part of the System being regulated. So why not include CNS in the ATM System?

Is it terrible that ESARR4 takes a restrictive view of 'ATM'? It certainly omits the question of the Guardian functions sketched in Part 1. ACAS is not mentioned in the document – but it is surely one of '*airborne functions required to ensure the safe and efficient movement of aircraft*'. There does not appear to be any mention in ESARR4 of any Guardian responsibilities, in particular there is no mention of accidents attributable to safety regulatory decisions or practices. Perhaps such things do not need to be in this particular document – but where are they? Surely total ATM system safety is to be assured, immaterial of the causes and responsibilities involved?

5 Safety Requirement

The Note to paragraph 5.2 states:

> *"Note: It is recognised that a combination of quantitative (eg mathematical model, statistical analysis) and qualitative (eg good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met."*

Is this a statement of the obvious? No, it is not. It raises crucial questions, particularly about the phrase 'good enough'. 'Good enough' has no intrinsic logical or safety content. It was 'good enough' is hardly a defence following a fatal accident.

An important safety principle discussed in Part 1 is that there is a 'duty of care', which requires everything reasonably practicable to be done to protect people's lives. Safety assessments must be done by competent people; they must show explicitly what data and assumptions have been used; and there must be independent checks by competent people. The whole process must be open to peer review and expert criticism.

There can hardly be any kind of objection to 'good working processes', but 'professional judgement' (equating to 'expert judgement' and 'engineering judgement') is an entirely different matter. Strigini (1996) makes the points very well in respect of engineering assessments:

> "…there are good reasons to doubt the ability of experts in some of the judgement tasks in which they are usually employed. Experimental research both about the way humans think and integrate evidence, and about the performance of experts in tasks similar to engineering judgement, support the idea that the ability of experts may be overrated.
>
> …For most of the tasks just discussed, there is thus a basis for trusting expert engineers to be effective at them, thanks to peculiarly human information-processing skills, although not completely reliable in terms of doing a complete job. *Tasks like conjecturing the probabilities of rare events, or drawing inferences about and from the correlations among factors in our experience, are definitely not in this category…we often reason about rare events via a "simulation" heuristic, i.e., by building scenarios for the rare events, causing significant errors in judgement…There is not, and there*

cannot be, any strong evidence of good judgement for small sets of predictions about very rare events." [Italic font added]

Nor can the judgements of pilots and controllers be seen as consistently better than those of engineers. Controllers are chosen to be 'can do', positive people, rather than introverted individuals who agonise about problems. Hence, their view of what is operationally 'impossible' sometimes bears a poor relationship to reality, presumably because of their confident attitude.

Two examples make the case. In the mid-1970s, there were safety studies of North Atlantic flights. All the controllers involved in the ICAO team said that it was impossible for a controller to mis-communicate an Atlantic ATC clearance. But radar monitoring of flights exiting the region's boundary showed that these happened several times every summer (Brooker and White, 1979). More recently, Eurocontrol (2003) reported on a MITRE Study in which controllers did not report ever observing any ACAS Resolution Advisory events where an evasive manoeuvre was taken without their anticipation. It seems unlikely that this reflects USA controller performance in reality – UK Airprox data certainly provides many examples where an RA surprises a controller.

In summary, it is necessary to be prudent about whether professional judgement arguments will provide a good enough – and consistent – level of assurance about rare events and correlations in ATM.

A-1 Hazard Identification and Severity Assessment in ATM

This is a very unsatisfactory part of the ESARR4 text. It fails to make use of the tools and results available from past research and practical safety analysis. Probably the most unfortunate sentence is:

"As there is no such scheme today as an accident/incident causation model, the severity classification shall rely on a specific argument demonstrating the most probable effect of hazards, under the worst case scenario."

It is just factually incorrect to write that there 'is no such scheme today as an accident/incident causation model'. This has been an area where considerable progress has been made – indeed, Eurocontrol documents report on, and have added to that progress. References include FAA/Eurocontrol (1998), ICAO (1998), Luxhøj (2003), Rasmussen (1990), Reason (1990), and Villiers (1968). Brooker (2002, 2004a, 2005a/b/c/d) builds on these foundations. Part 1 sketches the thinking that underlies the kinds of models that can, and have been, employed, including the use of Probabilistic Safety Assessment (PSA), Collision Risk Modelling (CRM), and Loosely- versus Tightly-coupled system models. Loosely-coupled aviation system safety may be better described by the Health and Safety Executive (HSE) version of risk assessment (Brooker, 2004b) using 'ALARP' principles.

Tightly- and loosely-coupled models are distinguished by:

Tightly-coupled models – accident risk is a function of specific failures, eg gross navigational errors or a restricted set of Human Factor failures occurring

comparatively regularly. Risk can be numerically quantified in terms of a limited number of key failure modes using CRM.

Loosely-coupled models – safety is provided through a structure of defensive layers: risks occur if these layers perform poorly and do not filter out potentially hazardous situations. In some circumstances, risk can be roughly numerically quantified, based on past defensive layer performance.

These two types of models provide the necessary accident/incident causation models for ATM. Something like *Figure A-1* in ESARR4 would then be a starting point for a proper understanding of the importance of different kinds of failures and hazards. As it stands, it is no more than a list of possibly serious – or minor – symptoms.

Figure A-1 in ESARR4 is extremely difficult to follow. For example, just taking the column marked "Accidents":

- *one or more catastrophic accidents,*
- *one or more mid-air collisions*
- *one or more collisions on the ground between two aircraft*
- *one or more Controlled Flight Into Terrain*
- *total loss of flight control.*

No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).

This raises many questions:

There is no doubt that the accidents noted here would generally involve fatalities – but why not specify that as a vital piece of information? Surely, preventing people's deaths must always be at the forefront of everyone's mind?

What is loss of aircraft flight control to do with ATM? That is surely a non-ATM/aviation accident, as discussed in Part 1.

Are all collisions on the ground between taxying aircraft to be judged of equal importance to those in mid-air? On the ground, the relative velocities are small, the aircraft do not fall from the sky, and fatal injuries are generally absent. A clear distinction must be made between taxying accidents and those involving runway incursions, which certainly can be catastrophic. [The KLM B-747 and Pan Am B-747 collision at Tenerife Airport, Spain in 1977 involved one of the aircraft taking off, as did the Cessna Citation and SAS MD-87 collision at Milan Linate in 2001.]

What does the note about "*no independent…*" actually mean? It surely cannot imply that the accident 'could not have been avoided', whatever that might mean? Did people not make choices and decisions – and could they have done otherwise? What, for example, does this statement mean if

applied to the causal factors identified in the Überlingen accident report's findings discussed in Part 1?

A-2 Risk Classification Scheme in ATM

The text of this section associates a safety objective based on risk with the severity classes discussed in Section A-1. The only quantitative statement made concerns the 'tolerable ECAC safety minimum', which is a

> *"maximum tolerable probability of ATM directly contributing to an accident of a Commercial Air Transport aircraft of 1.55 x 10^{-8} accidents per Flight Hour'"*

[ECAC stands for European Civil Aviation Conference, roughly equivalent to ICAO's European Region.] The phrase 'safety minimum' is used to mean what is normally understood to be 'safety target', a performance that the system should achieve in future. The derivation of this figure is sketched in Brooker (2004b). It is very disturbing that the source derivation is in fact contained in a document that it is not available to the public. It surely cannot be good safety management practice to conceal these kinds of regulatory and policy information from technical criticism. Brooker (2004b) also lists a number of criticisms of the tolerable ECAC safety minimum calculation. Some problems are with the details, but there are very significant problems with the source accident statistics, which are for <u>all</u> kinds of accident contained in the database used, ie are not restricted to a category such as fatal aircraft accident, hull loss or 'catastrophe' (compare RGCSP, 1995; Brooker, 2004b; JAA, 2003). Moreover, the so-called ATM-related figure of 2% [NB: with the ESARR4 restricted definition of ATM], relating to the <u>dominant</u> ATC causal factor, is explicitly declared as an assumption.

This special ECAC calculation is in fact hardly necessary. Brooker (2004b) explains how the ECAC safety minimum can be fitted into the ICAO/JAA framework, and how its rational foundations can be improved. Such a framework is surely acceptable to ECAC given that the major separation change in Europe – Reduced Vertical Separation Minimum (RVSM) – was developed using the ICAO Target Level of Safety (TLS) philosophy described in RGCSP (1995) (see ECAC (2005) and also Harrison and Moek (1992)). The TLS for RVSM, based on the ICAO RGCSP TLS philosophy was specifically approved by ECAC's Airspace and Navigation Team for application in the European RVSM Airspace.

The ESARR4 text also comments:

> *"Note: Figure A-2 only refers to an overall safety performance of ATM at ECAC and national level and is not directly applicable to the classification of individual hazards. To achieve this a method of apportionment of the overall probability to the constituent parts of the ATM system may need to be developed- This apportionment may be done per phase of flight and/or, per accident types."*

As has now has been stressed in Part 1 and in Brooker (2004b), it is one thing to partition a safety target for sub-systems, it is another thing entirely to be able to estimate the achieved performance against such a target with any precision. In general, this is feasible only for sub-systems that can be accurately described

through tightly-coupled models. Brooker (2004b and 2005a) sets out some examples of the ATM sub-systems for which this has proved feasible.

4. CRITIQUE OF EAM4/GUI1

A companion document to ESARR4 is referred to here as 'EAM4/GUI1', which is the Eurocontrol SRC's (2003) 'Explanatory Material on ESARR4 Requirements'. To quote:

> "*This guidance material has been prepared by the Safety Regulation Commission to provide guidance for ATM safety regulators and support the implementation of ESARR4. The main purpose of this document is to provide guidance about the provisions established in ESARR4 and more specifically in its Section 5 'Safety Requirements'. Each requirement is illustrated by giving explanatory material that includes a rationale, the most significant implications mainly for Regulator but also sometimes for Provider, and information about further development.*" [All direct quotes from EAM4/GUI1 here are put into italic font on their first appearance.]

EAM4/GUI1 is in some ways a helpful document, because it provides some explanation about points that are addressed very briefly in ESARR4. But it does not change the general themes in ESARR4. As for the previous section, the sub-headings here follow the order of EAM4/GUI1, and all extracts are put into italic font and identified by the EAM4/GUI1 paragraph number. Criticisms are generally made against just the first appearance of the logical error or un-evidenced assertion.

2.2.3 Rationale and Implications (Air Traffic Management)

The EAM4/GUI1 text actually provides support for the view that ATM should be an open description rather than any restriction to (say) ATC (as defined here).

> *"Note: It is however advisable to apply ESARR4 to all changes to the Air Navigation System which could have a potential safety impact. e.g., Aeronautical Information Service."*

The full inclusion of CNS into the ESARR4 framework is noted subsequently (eg Section 2.3.3)

The second bullet point notes:

> *"All airspace classes are addressed in ESARR4; airspace management and related airspace design may well induce unacceptable risks, and is therefore subject to ESARR4 (Note: It is recognised that there might be a difference in the levels of safety achieved today in controlled airspace and in noncontrolled airspace)."*

Surely, passengers in commercial air transport aircraft should not be exposed to markedly higher risk by being required to operate in noncontrolled airspace? See Brooker (2003).

2.2.3 Rationale and Implications (Quantified Risk Based Approach)

Bullet point two notes:

> *"A risk based approach is the most commonly used approach in aviation3, both internationally and in the aircraft community (Refer to both Federal Aviation Requirements and Joint Aviation Requirements applicable to aircraft certification),"*

So why use safety criteria that differ from the JAA? Why not implement similar criteria to those already successfully used by RGSCP (1995), and indeed by Eurocontrol itself for reduced vertical separation minima (ECAC, 2005)?

Bullet point 4:

> *"Quantitative criteria provide a clear target and, when derived and applied to lower level events, allow manufacturers to get on designing their equipment without having to analyse the entire ATM System,"*

This is only true for equipment that is part of a tightly-coupled sub-system. The bulk of failure events in ATM incidents have Human Factors components and causes.

Bullet point 5:

> *"The safety performance measurement of actual safety occurrences (with ATM contribution) may enable the verification a posteriori of whether or not quantitative objectives allocated to specific failures in a 'fault tree' for example are being met. Indeed, quantitative objectives could be derived from ATM safety minima and allocated to specific failures in a 'fault tree', hence providing for a range of probabilities which can be reasonably assessed over a short or medium period of time, [This would hopefully not be true for ATM induced accidents.]"*

This exaggerates wildly the value of PSAs in ATM safety assessment. Part 1 explains why such claims for PSA are not supported by the realities of ATM hazard analysis. The ESARR4 text here is no more than a conjecture about how things might be done; it is at best fractionally true. Part 1 shows that PSA risk calculations are seldom relevant to situations where safety relies on complex intervention and action by controllers and pilots (Brooker, 2002, 2004b, 2005a). The footnote (in square brackets) then says that these methodological advantages are unlikely to be achieved for ATM-induced accidents – but these are surely the topic of interest here?

Note (1):

> *"The feasibility of setting quantitative objectives/targets for specific parts of the ATM System was discussed, especially when it comes to their allocation to human contributions, procedures and software. It is recognised that demonstration of compliance won't always be quantitative- based, as it does not seem feasible to demonstrate a priori and in a quantified manner that a good working process, such as training, Safety Management System, or software codes of practices, enable specific quantitative objectives to be met.*

This will only be based on professional judgement and potentially verified over time."

The earlier text here and Part 1 have explained why generalised 'professional judgement' is an unreliable tool except in very controlled circumstances. Note also that potential verification of risk estimates is extremely difficult. If the sub-system is performing markedly worse than the supposed safety allocation then problems could well appear over a few million flying hours observation, but a system that is just under-performing is statistically unlikely to show such failure modes.

Note (2):

"The feasibility of setting quantitative objectives/targets was also discussed for another reason:- the review of existing safety data in ATM across the ECAC region has identified limitations and inconsistencies. Relying solely on historical data to derive ATM safety minima could lead to very high constraints being placed on the ATM system [7]. This is why it is advised to combine professional judgement with historical data when setting safety minima [8]. [[7] For the only reason that ATM may be reported as being safer than it actually is.] [[8] This was done when developing SRC Policy Doc 1.]"

It is not obvious how 'professional judgement' was used in deriving the ECAC safety minimum (Brooker, 2004b). The comments about 'very high constraints' are unclear. Surely, future safety levels should be improvements on past performance?

Bullet point 1 (second set):

"An equivalent minimum level of safety should be provided to aircraft wherever they fly in the ECAC airspace."

This is certainly a worthy objective. But should it apply in all types of airspace, for all types of flight (not just commercial airliners), for all types of control/information service…?

Bullet Point 2 (second set):

"Further quantitative refinements of the ECAC Safety Minima in ATM should be undertaken at national level, possibly by the national ATM safety regulator, according to the principles described in SRC POLICY Doc 1 and ESARR4 Appendix A."

This can only be done for 'refinements' that examine sub-systems that are tightly-coupled. There is little point in producing these kinds of targets if the corresponding performance cannot be estimated with the necessary precision.

Bullet point 3 (second set):

"A priori demonstration of compliance of the quantified objectives won't necessary rely on quantified demonstration and a posteriori verification of the quantified objectives with statistical data will rely on the implementation of a safety performance measurement system at the lower levels of the 'fault tree'."

This is complicated jargon rather than a clear explanation. To reiterate, the quantitative fault trees required for PSAs will only exist practically for tightly-coupled sub-systems where there are a limited number of probability branches.

6.2.3 Rationale and Implications

This Subsection discusses the 'Total System Approach'. It mentions equipment carriage, flight management systems, and hazards generally, but makes no mention of Human Factors, pilot/controller errors, etc. These are far more important to current and future ATM safety.

6.3.3 Rationale and Implications - Definition of the system under assessment

First paragraph:

> *"The 'system' is determined by what the ATM service provider wants to introduce at the time. Defining exactly the 'system' may be sometimes difficult. This is however an essential first step to start an assessment of the safety impact of proposed changes."*

One of the key problems, addressed in Part 1, is that the 'system' is being taken to be that which is provided by Air Navigation Service Providers (ANSP) etc, ie there is no recognition of the importance of Part 1's Guardian functions.

6.3.3 Rationale and Implications - Severity of effects

Second (extract), third and fourth paragraphs:

> *"…The ultimate aim of any aviation safety assessment should therefore be to minimise the chance (probability, or frequency) of aircraft incidents/ accidents, and the number of resulting deaths and injuries.*
>
> *Explicit consideration of the extent or number of injuries and deaths does not seem to be justified and very helpful when assessing ATM services, since these will depend on many circumstantial and widely varying factors, such as aircraft size, speed, collision geometry, survivability and the availability of rescue services, and not on ATM. The uncertainties in such factors may tend to obscure the objective of the risk assessment and mitigation process in ATM. As these factors are considered as outside the control of ATM, their consideration would therefore not add any additional inputs to the safety constraints placed on ATM.*
>
> *This implies that ESARR4 severity scale is not 100% aligned to the FAR/JAR AMJ 25.1309 as both schemes do not address the same purpose. However, should there be a need for comparing both schemes, the most severe class of ESARR4 would be equivalent to "catastrophic accident", as ESARR4 assumes the worst case scenario for elements outside of its control."*

It is very difficult to understand why ESARR4 uses a different kind of safety target from RGCSP (1995) or the JAA (2003). Fatal aircraft and catastrophic accidents have the advantages that they are well defined (whereas the ESARR4 version is

vague), and that they have been well documented, peer-reviewed and made publicly available. To reiterate, the ESARR4 calculation is stylised and secret.

The use of a new safety metric in ESARR4 is actually unnecessary. A perfectly satisfactory safety target for ATM-related accidents can be derived on RGCSP/JAA principles using NLR research inputs (Brooker, 2004b; van Es, 2001).

From an accident-modelling viewpoint, the use of fatal aircraft and catastrophic accidents is a cautious approach, because virtually all such models cautiously assume that ATM accidents would produce fatalities (eg as evidenced in the references in FAA/Eurocontrol (1998)). Thus, a mid-air collision between aircraft is assumed always to produce two fatal accidents.

Fifth, six and seventh paragraphs:

> *"At a lower level, secondary criteria to be used include the potential for collision between aircraft and aircraft/ground/something else, and the degree of ability to recover from such hazardous situation.*
>
> *The rationale is that the physical proximity of an ATM induced accident whether distance or time based) alone does not determine the level of risk. The geometry of the situation and other factors equally contribute to the level of risk.*
>
> *This implies that there can not but be some subjective judgement in any assessment of severity, hence advocating for putting together the rationale for a severity class."*

Again, this tends to focus on mechanistic views of accidents. The Human Factors element is not given its proper importance, nor is the nature of the ATM systems 'defence in depth' explored (Brooker, 2005a/b/c/d):

A useful metaphor here is 'threads of safety' (Brooker, 2004c). Threads secure a button on a coat: the more threads there are then the less likely that the button will be pulled off. The safety threads for aircraft operations at airports are the crew's competence, standard procedures, aircraft controllability and performance within the certificated limits, warning devices such as GPWS, reliability of engines, avionics and navigational aids, etc. If one or more of these threads breaks then the risks of an accident are greater – because the 'defences' have been weakened. In some instances, the defences are valuable because they prevent the crew from getting 'boxed in', eg an automatic alarm system tells the pilot that the present course of action is a hazardous one, and some different option must be adopted if the pilot is not to be trapped in a dangerous situation without safe exit routes.

The text almost manages to focus on the key issue by its use of the word 'subjective' - but it then does not consider how a rational version of subjectivity can be used, one that makes sense out of a variety of truly expert judgements. The right questions need to be posed. There needs to be a focus on a concept such as 'system controlled', meaning something like:

> system controlled – the ability to determine the outcome against reasonably foreseen changes and variations of system parameters, such as the abilities

of the participant(s), the environment (in the largest sense), and the safety mechanisms in place.

System controls in this sense cover all the means by which the system is held stable (ie defended) against the potential negative consequences: designers, pilots, controllers, software engineers, etc, not just the operational controller. A failure of system control covers situations both where the mechanisms make the situation worse and when they essentially fail to intervene (eg a conflict alert system could fail either by putting the aircraft into more danger or by not alerting).

The key phrase here is 'reasonably foreseen', meaning that the assessment of hazard must be carried out against 'reasonable' system parameters. What is unreasonable is a matter for debate and assessment by Human Factors, safety analysis and operational experts. To say that a past situation was hazardous – ie in a high severity class – would imply that if some of the system parameters applicable during that situation had been 'slightly different' then significant negative consequences would have resulted. Something was hazardous because of what might have happened. To return to the metaphor, the safety defensive threads were fraying and the button was only just being held on the coat. It is essential to assess the performance of the integrated safety system defences as a whole. See Brooker (2005b) for further analysis of the implications of this thought process.

Eleventh and twelfth paragraphs:

> *Elements to be considered in the severity assessment could include those mitigating means that the safety regulator would a priori consider as acceptable or unacceptable.*
>
> *An example could be the use of safety nets as mitigation means or not, for which the national regulator may have issued a policy, or for which the regulator may make a statement at the beginning of the project.*

It has already been noted elsewhere that the SRC policy on safety nets and risk assessment is wrong (Brooker, 2004d).

6.3.3 Rationale and Implications - Worst case scenario

The text reads:

> *"The severity of hazards will be determined by the credible consequences on the managed aircraft, when the outcome of all the safeguards which may exist in the other parts of the ATM System have been taken into consideration.*
>
> *For example, the most severe class will only be chosen in such cases when the total ATM System has exhausted its possibilities to affect what continues to happen and only chance determines if the consequence will be a collision or not.*
>
> *Equally, the severity of hazards will be determined by the credible consequences on the managed aircraft, when the outcome of all the weaknesses and potential failures which may exist in the other parts of the ATM System have been taken into consideration.*

This implies that applying the worst case scenario means that one can not assume rely solely on chance to avoid an accident."

Unfortunately, the phrase 'worst case' wrecks the hoped-for logical chain. The phrase 'worst case' places no reasoned limitation on the options considered. Such a concept has to be defined carefully in terms of 'reasonable' system parameters, as discussed above. Without such a careful definition, it is just too vague for practical use in safety critical applications. [To take an absurd extreme, but within the scope of the phrase allowed here, on a 'worst case' view, nobody would ever travel.]

6.3.3 Rationale and Implications - Tolerability of effects

Second note:

Professional judgement was used to determine the maximum acceptable ATM direct contribution to accidents; an historical baseline over a time-span of 20 years was selected to confirm the credibility of the expert judgement on past identified ATM direct contribution to accidents and future acceptable targets.

The word 'judgement' is mentioned twice, but it is not obvious how it is actually being employed. It is difficult to work out what the phrase 'confirm the credibility of expert judgement' means in any rational sense of the words used.

First bullet point:

"the quantified elements may not necessarily apply to airspace where there is no commercial transport aviation,"

General aviation flights are not managed by ANSPs. The ATM safety system defences – formal safety rules, controllers actively handling traffic, conflict detection equipment, etc, etc are completely different. An examination of general aviation accident statistics provides the evidence.

Third bullet point:

"the quantified targets are applicable to the global ATM system (human/procedure/equipment)."

'Global' is never defined.

Second group of bullet points:

The rationale is that:

- *targets for ATM indirect contribution to accidents,*
- *targets for ATM incidents, and*
- *targets for ATM specific occurrences …*

… could not be developed for ECAC as no reliable statistical data on those occurrences could be collected at ECAC level to provide a good enough level of assurance that related targets would be realistic. It would have been unreasonnable to mandate those lower level targets at regulatory level.

Surely, it is worth attempting to deliver improved European safety? Surely, the aim is to bring everyone in Europe up to the best practice standards? Surely, the aim is to set Europe's sights on improved incident recording and analysis systems?

Text before final group of bullet points:

> *"An ATM service provider, in order to deal with specific constituent parts of the ATM system (e.g., modification of displays) may also not use directly the top level national ATM risk classification scheme to assess the severity of hazards related to such a change. It may need to develop a scheme consistent with the top level one that it adequately reflects the operational environment of the system under consideration (eg interfaces with other systems, phases of flight, classes of airspace).*
>
> *The rationale for ESARR4 not providing guidance to do so is that there is a need to analyse the entire ATM System, and understand how the specific system is going to be used and in which context, to be able to determine how it will affect overall safety."*

How can this be adequate 'guidance' material? Real practical examples need to be given – covering the whole range of potential problems – of <u>how</u> such tasks are to be accomplished. The present text just seems to offers vague abstractions rather than a well-founded learning process based on a reasoned assembly of factual and logical material.

6.3.3 Rationale and Implications - Apportionment of ATM Safety Minima and derivation of safety objectives

This is probably the most important, but also probably the most unsatisfactory, part of the document.

Paragraphs one to four:

> *"The text and quantitative levels given in ESARR4 (and in equivalent national safety regulatory requirement) only refer to the classification of the overall ATM safety performance ECAC-wide and are not directly applicable to the classification of individual risks.*
>
> *This implies that the overall target (of minimum) level of safety has to be allocated among/apportioned to all the top-level risks identified in the realm of the state's responsibility. Thus, the maximum probability of a single hazard will usually be much smaller than the maximum probability derived from the overall minimum level of safety.*
>
> *There is indeed a practical difficulty with the ESARR4 scheme in determining safety objectives for the constituent parts of the ATM system as required under 5.2 (b). While the scheme in Appendix A sets safety objectives for ATM induced accidents and incidents, it does not lead to an approach for determining the quantitative relationship between these and ATM hazards and failure conditions.*
>
> *The rationale is that ESARR4 remains at a high level and, being a regulatory requirement does not mandate a specific architecture for the ATM System.*

Additionally, ESARR4 can not mandate a specific approach to deriving safety objectives and requirements as there may be more than one solution. Finally, there is no such thing today as an identified reliable causality model for accident which would help determine such relationship, at least at regulatory level."

This is another instance of vague abstractions rather than a structured learning process based on sound premises.

Reiterating some messages from Part 1: ATM sub-systems can broadly be categorised as tightly-coupled or loosely-coupled. The first can potentially be modelled with some confidence, if certain conditions (mainly regarding data) are met, so that accident rates can be expressed in terms of sub-system failure rates. The second relies on safety defences in depth – a multiplicity of formal, technical and human safety defensive layers – to deliver the necessary safety, but cannot usually be modelled quantitatively with great precision. Examples of the kinds of tightly-coupled models used successfully are ILS (Howard, 1992), Obstacle Clearance (Hunter, 1980), NAT Track System (Brooker and White, 1979), RVSM (Harrison and Moek, 1992), radar separation (Sharpe, 1991). Examples of rough risk calculations for loosely-coupled models are Brooker (2002, 2003, 2005d).

Target levels of safety – oddly termed 'safety minima' by the SRC – can be apportioned down from an overall TLS to a particular accident mode, eg it is straightforward to derive a TLS for loss of vertical separation attributable to an altimetry error/failure. But this can only be done for tightly-coupled sub-systems (Brooker, 2004b).

Problems with apportionment arise if it is attempted at too fine a level. It can then become impossible to estimate, measure or monitor anything that provides useful information about error/failure rates. Thus, if a particular ATM failure mode requires a gross error rate in some kind of equipment to be less than 1 in 10^7 flying hours, then it is necessary to monitor ~10^8 flying hours to have some statistical confidence that the error rate target is actually being achieved. Monitoring for markedly less than 10^7 flying hours, and finding no gross errors, tells the analyst very little, because even a much less safe operation would produce no such errors.

The final paragraph in this extract is of particular concern. The factual record from the policy/research literature, much of it under Eurocontrol auspices, speaks for itself. There are useful models for ATM accident and incident processes, including many workers in Eurocontrol and European states, have contributed to international work in this area (eg FAA/Eurocontrol, 1998). For tightly-coupled sub-systems it is the rate of some variety of gross error/failure that must be monitored; for loosely-coupled sub-systems, lessons have to be learned from the performance of safety defensive layers as evidenced in incidents where separation is lost or conflict alert systems are needed to prevent potential accidents.

Paragraphs five to eight:

"The pros of this approach is that ESARR4 remains "objective" driven, and leaves full flexibility to those demonstrating compliance with its intent. (Note:

*The con of this approach, however, is that ESARR4 does not provide explanations on **how** it can be implemented).*

This implies that, to set safety objectives to specific hazards, a method of apportionment of the overall probability and /or a derivation of the top level quantified target down to the lower levels such as functions or elements of the ATM System (equipment, people, procedure) has to be developed. The development of such method falls within the remit of the ATM System designer(s). It will be left to the ATM service provider to give a robust argument for any particular application of ESARR4.

This apportionment may be done in different ways, per phase of flight, per type of risks/accident, per ATM service/function, assuming a maximum of hazards in ATM which will have the potential to lead an ATM accident [With adequate justifications and means to verify over time that assumptions are correct.], or a combination thereof.

Related detailed approach will need to be assessed and accepted by the safety regulatory authority."

Where is the proper regulatory responsibility demonstrated here? The onus is surely on the regulator to ensure that the regulated organisation does not waste valuable time searching for something that does not exist. The regulator must surely only set regulations that have a good chance of being achieved through reasonable efforts.

The vague comments about 'adequate justifications' compound the imprecision of this approach. The regulator must demonstrate the kinds of evidence that would be accepted. Regulators cannot evade this responsibility.

Some portion of ATM system risk must be attributed to regulator and other Guardian failings as explained in Part 1. Note again the conclusions of the accident report into the Überlingen tragedy (BFU, 2004). This identified weaknesses in ACAS policy, and posed specific questions about the regulators' checks and scrutiny of the service provider's operating practices.

6.3.3 Rationale and Implications - Aviation harmonisation

First bullet point:

"ICAO for example addresses specific risks and does not specify any airspace TLS which would be valid worldwide or on a regional basis. ICAO Target Levels of Safety (TLS) are often based on historical baseline which are worldwide, not European based, and rely on a lot of assumptions, which are not always documented, nor valid everywhere;"

This is a very unfortunate sentence. It is both careless and false. ICAO material on this topic is well documented and has been made available in formal ICAO publications to States for 30 years. The assumptions are well documented (eg Brooker and Ingham, 1977; Davies and Sharpe, 1993; Brooker, 2004b, FAA/Eurocontrol, 1998). The phrase here 'a lot of' rather exemplifies the vagueness and casual approach in ESARR4 to the extensive research and policy literature. The

TLSs are applicable to European airspace, and indeed Eurocontrol has adopted them for ECAC RVSM (ECAC, 2005) website. To quote from that website:

> "Collision Risk Assessment The numerical safety standards appropriate to operations in a European RVSM environment were derived from those developed by the ICAO Review of the General Concept of Separation Panel (RGCSP) in which the agreed tolerable level of risk was defined as a Target Level of Safety (TLS) expressed in terms of fatal accidents per aircraft flight hour."

Second bullet point:

> *Harmonisation of ESARR4, Appendix A-2 with the quantitative targets of FAR/ JAR 25 is difficult and may be irrelevant as the scope and applicability of the two risk matrices are different. (Refer to SRC DOC 1 "Safety Minima Study", Ed 1.0, which identifies the rationale for JAA/FAA quantification levels and related scope of application);*

As noted already, this is not the massive intellectual problem hinted by the ESARR4 text. For example, Brooker (2004b) shows how RGCSP (1995) and JAA (2003) can be integrated into a consistent ATM safety formulation. The interesting European Commission funded work on ATM safety targets, ARIBA (1999), is also well worth studying.

6.3.4. Future development

First and fifth Paragraphs:

> *"Once a limited number of categories of environment of operations have been identified across ECAC (or even world-wide) together with practical experience in the assessment of effects of typical ATM hazards/Failure Conditions and related severity, more guidance to regulators may be developed for them to develop a more refined view on the acceptability of the proposed severity and associated rationale.*
>
> *Once enough hazards have been analysed and associated rational or severity classification well documented and collated in a structured manner, once national safety reporting schemes compliant with ESARR2 have allowed for consistent safety data to be collected and analysed, it should become feasible to initiate a study to develop an approach for determining the quantitative relationship between the scheme in Appendix A (which sets safety objectives for ATM induced accidents and incidents) and ATM hazards and failure conditions."*

These are unfortunately hazy conjectures rather than rational plans or time-specific road-maps. The second paragraph here consists of an unedifying sequence of conditional statements. Putting ***!*** markers between the phrases shows this lengthy series of suppositions:

> *"Once enough hazards have been analysed **!** and associated rational or severity classification well documented and collated **!** in a structured manner, **!** once national safety reporting schemes compliant with ESARR2 have allowed for consistent safety data to be collected and analysed, **!** it*

should become feasible ! to initiate a study ! to develop an approach ! for determining the quantitative relationship ! between the scheme in Appendix A and ATM hazards and failure conditions."

5. COLLATED DEFICIENCIES AND POTENTIAL REPAIRS

The deficiencies of – and suggested repairs for – ESARR4 and EAM4/GUI1 are collated and summarised in the following paragraphs.

The defective ESARR4 and EAM4/GUI1 could be handled in several ways. It cannot be right to ignore the problems: this would produce mis-allocations of scarce safety resources, and potentially divert attention away from real safety improvements by being wasteful of regulators' and managers' time. It cannot be right to abandon ESARR4: those European States that are still developing their ATM safety systems would have nothing to aim for. Editing ESARR4 piecemeal would be very difficult – too many elements would need to be reworked.

A fundamental structural repair of ESARR4 and its supporting documents appears to be the only rational approach. A great deal could be improved in ESARR4 if the kinds of ATM safety management processes described in Profit (1995) and ARIBA (1999) which inter alia cover 'ALARP' principles, were adopted. Suggestions are made for how to repair ESARR4 and its supporting documents. In most cases, the repair is simple, given that the deficiency has been identified.

The nature of the ATM system

ESARR4 takes a restrictive view of the 'ATM system'. It omits any mention of the responsibilities of regulators and other Guardian functions. ACAS is not mentioned in the document – but it is surely one of the 'airborne functions required to ensure the safe and efficient movement of aircraft'. There is no mention of accidents attributable to safety regulatory decisions or practices. Surely, Total ATM System safety is to be assured, immaterial of the causes and responsibilities involved? This incompleteness of ESARR4 is exposed when confronted by information about a real life catastrophe. Thus, it fails to demonstrate its relevance adequately to the kinds of systematic causal factors identified in the Überlingen tragedy.

To repair: use explanations and definitions of the ATM system on the lines of Part1.

Reliance on Probabilistic Safety Assessment – PSA

PSAs are used to attempt to estimate the risk of accidents by analysing the sequences of events that could produce an accident – the 'causal chains'. Failures arise from 'errors' from 'normal operations'. At each stage, the probability of an event's success or failure in safety terms has to be quantified. For mechanical or electronic components, the failure probability can in theory – and often in practice – be determined by observations of the performance of that particular sub-system.

But ATM systems contain people who have to make decisions and act on the information presented to them, so some of the events require probabilities to be

estimated for 'human components' – the task of Human Reliability Analysis (HRA). It is much more difficult to produce usable estimates of these kinds of infrequent risk components. The models may well be appropriate in theory, but the practical safety problem is in 'populating' them with relevant real-life data.

ESARR4 essentially proposes the use of PSA/HRA as a general tool. The practical problem is that PSA/HRA does not work for ATM. A PSA/HRA is a very complex (and no doubt formally correct) model, but which at best would produce usable answers at some indefinite point in the future rather than now. Most important, much of the data required is just not there. This is why PSA/HRA has been so heavily criticised in the nuclear power plant industry, which is a less complex system than ATM. The onus is on the SRC to demonstrate, by reference to past successful work, documented in the policy/research literature, that the ESARR4 approach actually delivers the goods.

To repair: Use CRM, as discussed in Part 1, plus 'ALARP' principles.

Ignoring the literature on ATM risk assessment techniques

ESARR4 exaggerates when it says that there 'is no such scheme today as an accident/incident causation model'. This is been an area where considerable progress has been made, which has produced successful real-life ATM applications. These productive applications are well documented in the research and policy literature by States and Europe's own experts. Part 1 provides a conspectus and references to key sources.

To repair: Refer to models that have been used successfully in ICAO and State work.

Giving no guidance about practical methods

ESARR4 leaves it to the service provider to make a safety case, but provides no examples about how this might reasonably be done. This is very poor 'guidance' material. Examples need to be given – examples covering the whole range of potential problems – of <u>how</u> such tasks are to be accomplished. It is not sufficient for a safety regulatory body to deal in blurred abstractions: a well-founded learning process for service providers is needed. The regulator must surely act professionally, only setting regulations that have a good chance of being achieved through reasonable efforts.

To quote a former CAA colleague: "Its high level principles are good but the detail [of ESARR4] is seriously flawed. It certainly seems odd that a piece of regulation can be produced for which there is no agreed method of compliance – and possibly no practical means of compliance."

To repair: Set out criteria and practical examples for the use of CRM and other methodologies.

Not distinguishing between different types of ATM sub-system

ESARR4 discusses the 'Total System Approach'. But, in practice, it focuses on equipment, flight management systems, and abstract hazards. It makes little mention of human factors, pilot/controller errors, etc, which are in reality far more important to current and future ATM safety. This is surely dangerous selectivity.

Technically, ESARR4 fails to distinguish between two kinds of ATM safety sub-system: tightly-coupled and loosely-coupled. The first can, given appropriate data and if various conditions (see Part 1) are met, be modelled with some confidence, so that accident rates can be expressed in terms of sub-system failures, eg gross navigational errors. The second relies on safety defences in depth – a multiplicity of formal, technical and human safety defensive layers – to deliver the necessary safety. The safety levels achievable with loosely-coupled sub-systems can usually only be modelled roughly. ESARR4 tends to assume that all ATM sub-systems are of the first kind. The present abstract ESARR4 approach, with its apparent 'one size fits all' mentality and too much focus on PSA methods, is unlikely to deliver real safety benefits.

Thus, ESARR4's statements about hazard analysis, fault trees, verification, probabilities, etc are theoretical (in the pejorative sense of the word). They have very weak foundations in the realities of ATM hazard analysis. They exaggerate what can be done in practice by PSAs– the claims are not supported by evidence covering the range of ATM risks. At best, the claims are conjectures about how things might be done – and even then only if the safety occurrences arise from a tightly-coupled sub-system.

To repair: Distinguish between tightly- and loosely-coupled systems.

Non peer-reviewed safety target

It is very difficult to understand why ESARR4 uses a different kind of safety target – 'the ECAC safety minimum' – from ICAO or the JAA. Fatal aircraft and catastrophic accident statistics used by ICAO/JAA have the advantage that they are well-defined – whereas the ESARR4 version is vague. Moreover, they have been well documented, peer-reviewed and made publicly available – whereas the ESARR4 calculation is stylised and kept secret from the public.

This secret ECAC calculation used in ESAAR4 is actually unnecessary. The ECAC safety minimum can easily be fitted into the ICAO/JAA framework, and its rational foundations improved. ICAO safety targets are surely acceptable to the Eurocontrol SRC given that the major separation change in Europe – RVSM – was developed using the ICAO Target Level of Safety philosophy.

Safety target levels can be apportioned down from an overall TLS to a particular accident mode, eg it is straightforward to derive a TLS for loss of vertical separation attributable to an altimetry error/failure, but this can only be done for tightly-coupled sub-systems. The problems with apportionment come about if it is done too finely. Too fine an analysis of too detailed a sub-system is likely to involve estimates of very

low precision that are dependent on many assumptions. It can thus become impossible to estimate, measure or monitor anything that provides useful information about error/failure rates.

To repair: Use ICAO TLS-based safety targets.

Unstructured use of expert judgement

In several instances, ESARR4 suggests the use of generalised 'professional/expert judgement'. But this is an unreliable – and hence unprofessional – tool when applied to rare events not experienced by the operational/analytical experts concerned. Calibration and consistency are major problems. To quote Moray (1990), re nuclear power plant (much less complex than ATM): "The use of 'expert judgement' is a polite name for 'expert guesses', and we do not have data to validate the accuracy of the guesses."

To repair: Restrict expert judgement to those topics and events that have been experienced by operational experts.

Careless use of 'worst case'

The phrase 'worst case' is used in several places in ESARR4 and its supporting material. This is wholly unhelpful, because it places no reasoned limitation on the options considered. Such a concept would have to be defined very carefully in terms of 'reasonable' changes to system parameters; otherwise, it is just too vague for use in safety critical applications. But a collection of 'cautious' assumptions can produce over-pessimistic, and hence impractical, risk estimates.

One could even argue that the 'worst case' scenario arising from almost any ATC error is an accident. This would make the rest of the severity scheme in Fig A-1 redundant, except in terms of monitoring. Quoting again a former CAA colleague: "Excluding the use of chance in a risk assessment focused on ATM accidents also seems to be irrational. If this were to be applied for (say) North Atlantic flights, the result would be a risk estimate several orders of magnitude higher than reality."

To repair: Define 'worst case' explicitly in terms of reasonable changes to specific system parameters.

Future Development

ESARR4's statements on future development are conjectures not rational plans or time-specific road-maps. The text consists of no more than a sequence of conditional statements.

6. CONCLUSIONS

It has been shown that ESARR4, with its main supporting documents, have significant deficiencies. There is a lack of clarity about responsibilities for ATM safety. The claims ESARR4 and EAM4/GUI1 make for the methodologies proposed are overstated – not supported by sound evidence from real world hazard analysis.

This obviously implies subsequent problems with the intended application of ESARR4. Continued use of this document could mis-allocate scarce safety resources and divert attention away from real safety improvements.

Suggestions are made for repairing these deficiencies. The most important underlying change would be a refocusing on practical safety assessment based on methods that have already demonstrated their merits. The documents should include realistic specimen risk calculations. The present abstract system approach, with its apparent 'one size fits all' mentality is unlikely to deliver real safety benefits. The key point to note is that aviation decision-makers usually have to make decisions based on evidence that is inherently incomplete quantitatively.

A checklist for an improved ESARR4 would include:

- best practice in the context of published methodologies and data quality management
- models that embed clear and complete physical pictures of accident causation
- calculations based on measured data
- data extrapolations that would be agreed to be cautious by independent competent people
- expert judgement restricted to topics and events that have been experienced sufficiently often by operational experts
- indications of statistical precision and parameter sensitivities for decision-makers
- openness to peer review

The items in the checklist have to be ideal goals: the important point is that best efforts and best practice are used.

ACKNOWLEDGEMENTS

This work was in part supported by a research grant by the Civil Aviation Authority's Safety Regulation Group (SRG). I would like to thank SRG staff for useful comments on earlier drafts. The text does not of course commit SRG to any future policy changes – although the author hopes that SRG experts will take note of factual and rational points made here. I would like to thank NATS and Eurocontrol safety experts for discussions and moral support.

REFERENCES

ARIBA, 1999. WP6 Final Report Part II: Safety Cases for a new ATM operation. http://www.nlr.nl/public/hosted-sites/ariba/rapport6/part2/title.htm

BFU [German Federal Bureau of Aircraft Accidents Investigation], 2004. Investigation Report 'Überlingen Mid-air collision'. AX001-1-2/02. http://www.bfu-web.de/berichte/02_ax001efr.pdf

Brooker, P., 2002. Future Air Traffic Management: Quantitative En Route Safety Assessment Part 2 – New Approaches. Journal of the Institute of Navigation 55(3), 363-379.

Brooker, P., 2003. The Risk of Mid-Air Collision to Commercial Air Transport Aircraft receiving a Radar Advisory Service in Class F/G Airspace. Journal of the Institute of Navigation 57, 277-289.

Brooker, P., 2004a. Airborne Separation Assurance Systems: Towards a Work Programme to Prove Safety. Safety Science. 42(8), 723-754.

Brooker, P., 2004b. Consistent and Up-To-Date Aviation Safety Targets. Aeronautical Journal. July, 345-356.

Brooker, P., 2004c. Delivering Safety in the context of Environmental Restrictions: Aviation Expert and Research Review. CAA Paper 2004/08. CAA, London

Brooker, P., 2004d. Why the Eurocontrol Safety Regulation Commission Policy on Safety Nets and Risk Assessment is Wrong. Journal of the Institute of Navigation 57(2), 231-243.

Brooker, P., 2005a. Air Traffic Management Accident Risk Part 1: The Limits of Realistic Modelling. Cranfield University.

Brooker, P., 2005b. Reducing Mid-Air Collision Risk in Controlled Airspace: Lessons from Hazardous Incidents. – to appear in Safety Science.

Brooker, P., 2005c. Airborne Collision Avoidance Systems and Air Traffic Management Safety. Journal of the Institute of Navigation 58(1), 1-16.

Brooker, P., 2005d. STCA, TCAS, Airproxes and Collision Risk. – to appear in the Journal of the Institute of Navigation.

Brooker, P. and Ingham, T., 1977. Target Levels of Safety for Controlled Airspace. CAA Paper 77002. CAA, London.

Brooker, P. and White, F. A., 1979. Minimum Navigation Performance Specification and Other Separation Variables in the North Atlantic Area. Journal of the Institute of Navigation, 32(3) 357-374.

Davies, E. H. and Sharpe, A. G., 1993. Review of the Target Level of Safety for NAT MNPS Airspace, CS Report 9301, NATS, London.

ECAC, 2005. ECAC RVSM website. http://www.ecacnav.com/rvsm/safety.htm

Es, G. W. H. van, 2001. A Review of Civil Aviation Accidents: Air Traffic Management Related Accidents: 1980-1999. 4th International Air Traffic Management R&D Seminar, 2001. http://atm2001.eurocontrol.fr/finalpapers/pap05.pdf

Eurocontrol, 2003. Review of ACAS RA Downlink: An assessment of the technical feasibility and operational usefulness of providing ACAS RA awareness on CWP. http://www.eurocontrol.int/ra-downlink/Library/Review%20of%20ACAS%20RA%20Downlink%20ver%2010.pdf

Eurocontrol SRC, 2001. Risk Assessment and Mitigation in ATM, Eurocontrol Safety Regulatory Requirement ESARR4, Edition 1.0., Eurocontrol, Brussels. http://www.eurocontrol.int/src/gallery/content/public/documents/deliverables/esarr4v1.pdf

Eurocontrol SRC, 2003. Explanatory Material on ESARR4 Requirements. EAM 4 / GUI 1. Edition 1, Eurocontrol, Brussels. http://www.eurocontrol.int/src/gallery/content/public/documents/deliverables/esarr4_awareness_package/eam4gui1_e10_ri_no_signatures.pdf

FAA/Eurocontrol,, 1998. A Concept Paper for Separation Safety Modeling An FAA/EUROCONTROL Cooperative Effort on Air Traffic Modeling for Separation Standards. http://www.faa.gov/asd/ia-or/pdf/cpcomplete.pdf

Harrison D. and Moek G., 1992. European Studies to Investigate the Feasibility of using 1000 ft Vertical Separation Minima above FL 290: Part II – Precision Data Analysis and Collision Risk Assessment, Journal of the Institute of Navigation 45, 91-106.

Howard, R. W., 1992. Breaking through the 10^6 Barrier. Aeronautical Journal, August, 260-270.

Hunter, R. D., 1980. The development of obstacle clearance criteria for ILS operations at civil airports. CAA Paper 80009, CAA.

ICAO, 1998. Manual on Airspace Planning Methodology for the Determination of Separation Minima. ICAO Doc 9689-AN/953.

JAA, 2003. Advisory Joint Material relating to JAR 25 Large Aeroplanes, AMJ 25.1309, Change 16, Joint Airworthiness Authorities, 2003.

Luxhøj, J. T., 2003. Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport. Second Workshop on the Investigation and Reporting of Incidents and Accidents, IRIA 2003. http://shemesh.larc.nasa.gov/iria03/p02-luxhoj.pdf

Moray, N., 1990. Dougherty's Dilemma and the One-sidedness of Human Reliability Analysis. Reliability Engineering and System Safety, 29, 337-344.

Profit, R., 1995. Systematic Safety Management in the Air Traffic Services, Euromoney, London,

Rasmussen, J., 1990. Human error and the problem of causality in analysis of accidents. Philosophical Transactions of the Royal Society B 327, 449-462.

Reason, J., 1990. Human Error. Cambridge University Press, Cambridge UK.

RGCSP [Review of the General Concept of Separation Panel], 1995. RGCSP Working Group A Meeting: Summary of Discussions and Conclusions, ICAO.

Sharpe, A. G., 1991. Application of the 5 nm radar standard separation at ranges up to 160 nm from Claxby, Debden and Pease Pottage SSRs. CAA Paper 91013, Civil Aviation Authority, London.

Strigini, L., 1996. Engineering judgement in reliability and safety and its limits: what can we learn from research in psychology? SHIP project Technical Report T/030. http://www.csr.city.ac.uk/people/lorenzo.strigini/ls.papers/ExpJudgeReport/ExpJudgeReport96.pdf.

Villiers, J., 1968. Perspectives for Air Traffic Control for Advanced Phases of Automation - the Method of Layers, in French: Perspectives pour le contröle de la circulation aérienne dans les phases avancées d'automatisation - la méthode des filtres), Navigation n° 61, January.