THE JOURNAL OF NAVIGATION (2004), **57**, 231–243. © The Royal Institute of Navigation
DOI: 10.1017/S0373463304002735 Printed in the United Kingdom

Why the Eurocontrol Safety Regulation Commission Policy on Safety Nets and Risk Assessment is Wrong

Peter Brooker

(*Cranfield University*)
(*Email: P.Brooker@cranfield.ac.uk*)

Current Eurocontrol Safety Regulation Commission (SRC) policy says that the Air Traffic Management (ATM) system (including safety minima) must be demonstrated through risk assessments to meet the Target Level of Safety (TLS) without needing to take safety nets (such as Short Term Conflict Alert) into account. This policy is wrong. The policy is invalid because it does not build rationally and consistently from ATM's firm foundations of TLS and hazard analysis. The policy is bad because it would tend to retard safety improvements. Safety net policy must rest on a clear and rational treatment of integrated ATM system safety defences. A new safety net policy, appropriate to safe ATM system improvements, is needed, which recognizes that safety nets are an integrated part of ATM system defences. The effects of safety nets in reducing deaths from mid-air collisions should be fully included in hazard analysis and safety audits in the context of the TLS for total system design.

KEY WORDS

1. Eurocontrol. 2. Safety Regulation Commission. 3. ATM. 4. ATC.

1. INTRODUCTION. This paper sets out reasons why the recently issued Eurocontrol SRC policy on safety nets and risk assessment is wrong. The source document for the SRC policy is SRC Policy 2: Use of Safety Nets in Risk Assessment & Mitigation in ATM, Edition: 1.0 dated 28 April 2003, referred to here as the SRC Policy.

Extracts from the SRC Policy are shown here within inverted commas, plus italic font when it is embedded in the text. Its Executive Summary reads:

> '*F.6 EXECUTIVE SUMMARY*
> *Questions raised by various parts of the ATM industry, including some EATMP Programmes, have identified the need for an ATM safety regulatory policy on the use of "safety nets" in the ATM risk assessment process. Such use can be in the context of both the assessment of the safety adequacy of the existing ATM system, within the SMS required by ESARR 3, and when assessing the safety adequacy of a change to the ATM system, as required under ESARR 4.*
>
> *Safety nets are engineered systems which are designed and operated for the purpose of collision avoidance.*

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

> *Any safety benefit which may be provided by a safety net shall be considered as an additional overlay to that provided by the ATM system, as safety nets are considered to be in the collision avoidance layer outside the scope of ESARR 4.*
>
> *The ATM system must be able to demonstrate that it satisfies applicable tolerable ATM safety minima without reliance upon the safety benefit expected to be provided by safety nets.*
>
> *As safety nets can themselves induce new hazards to flight operations, they will be subject to specific safety objectives.*'

In the following, the main concern is with mid-air collisions in controlled airspace, although the points made are generally applicable. Similarly, STCA, which has a vital role in preventing mid-air collisions, is taken as a generic safety net. Section 2 provides the necessary background for Section 3, Aspects of Safety Net Policy, which then leads on to Section 4, Does the SRC Policy provide reasoned arguments? There is minor repetition in the text to obviate the need for internal referencing.

2. BACKGROUND.

Eurocontrol safety policies should focus on progressively reducing the numbers of deaths from aviation accidents. Every policy, every procedure, every regulation must therefore be kept under review and scrutinised to determine if any other feasible option offers better prospects of saving lives. This continuous review process must take into account information about risks, ways of analyzing safety, and the impact of innovation and the use of new technology. This section outlines some background on important features of Target Levels of Safety, system safety defences, and separation minima; including comments on their relevance to safety net policy. These should be seen in the context of the strategic safety policy for ATM, e.g. 'to minimise the risks of causing an aircraft accident as far as is reasonably practicable' (Profit, 1995).

2.1. *The basics of target levels of safety.* The fundamental quantitative safety concept in ATM is that of a Target Level of Safety (TLS). This is a design hurdle, a quantified risk level that a system should – i.e. be designed to – deliver. A TLS covers all aviation-related causes, but does not usually attempt to cover the consequences of terrorism or criminal behaviour (although the literature has not always been clear on this).

Most of the practical problems are not actually with the TLS but with the proper estimation of the safety level that is, or would be, achieved. There is an Achieved Level of Safety (ALS) – the risk level being achieved in the system under examination. How is this to be calculated with sufficient accuracy for there to be confidence that the $\text{ALS} < \text{TLS}$?

A TLS appropriate for accidents arising from mid-air collisions has been developed since the 1970s. It is usually derived by taking historical accident rates, which show a progressive reduction over time, and extrapolating forward. Thus, the TLS value gets tighter and tighter over time.

The TLS is measured in fatal aircraft accidents, i.e. accidents in which at least one person in the aircraft was killed, per so many aircraft flying hours. The recent ICAO figure of $1{\cdot}5 \times 10^{-8}$ fatal aircraft accidents per flying hour (RGCSP, 1995) is the rate corresponding to mid-air collisions – for any reason and in any spatial dimension – in en route flight in controlled airspace.

TLSs and ALSs are by their very nature statistical statements rather than guarantees. Collisions are most likely to be caused by human error in the largest

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

sense – and these would be very infrequent probabilistic events. Decades ago, collisions might have been more likely to be caused by equipment and navigation hardware problems, but today's Airprox and other incident data (UK Airprox Board, 2003) shows that the highest likelihood for collision arises – in crude terms – from being in the 'right place but on the wrong flight path'.

The TLS was derived as a system design target against all the risks to which an aircraft could be exposed. The TLS thus relates to total system design, i.e. 'the implication is that all types of failure, mechanical, procedural and human, which generate a risk of collision will be accounted for' (Brooker and Ingham, 1977). The phrase *Total System* is crucial in the present context. There are good reasons for judging STCA to be a systematic integrated part of the ATM safety system defences. It should therefore be fully included in hazard analysis and safety audits – in the context of the TLS for total system design.

Note that the TLS was not developed on the basis that certain types of system, technology or procedure would be either present or absent. The risk calculations for an ATM system's ALS were seen as potentially including all mitigating factors, from controller monitoring and intervention to automatic warning systems. The TLS is therefore not produced in the context of the causal factors or mechanisms by which safety is either at risk from or protected by. The ICAO teams that developed the TLS philosophy did not a priori rule out the use of ground-based safety nets such as STCA in delivering the TLS (Brooker and Ingham, 1977, sets out the key references).

Consistency in risk philosophy is an important principle. Safety defences are part of an integrated ATM safety system and it is therefore unreasonable arbitrarily to count some elements in risk calculations and to omit others, as the SRC Policy would suggest for STCA. When there may be good hazard analysis reasons for omitting particular elements – e.g. See-and-Avoid as noted later – then the case has to be made.

2.2. *System safety defences.* ATM-related accidents are very rare because of the system safety defences, barriers and safeguards that are in place. These defensive layers and engineering redundancies range from human monitoring to automatic warning systems, such as STCA, to the procedural rules followed in setting up system operations (e.g. separation minima, as described below). Accidents are the consequences of several, often inherently unpredictable, circumstances that breach all of the system safety defences.

The present ATM system thus has several distinct components in its operational concept and hence its safety defences. Some strategic defence layers are:

- Controllers and pilots: people monitoring and acting are an integral part of the whole system.
- Formal Rules: for the control of traffic, including the structures of controlled airspace and the minimum separation permitted between aircraft.
- Technology: radiotelephony, radar, computer processing of radar and flight data, high quality aircraft navigation.
- Conflict Alert (STCA).
- Airborne Collision Avoidance Systems (ACAS): not discussed here.

This description strengthens the use of the phrase *ATM system*, in which the safety defences have progressively been added and enhanced, and for which systems are considered as a whole (Profit, 1995). In the following, the ATM system is defined

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

as: *Everything that contributes to the safe movement of air traffic* – the Total System. The concept of safety defensive barriers for ATM is explained in Brooker (2002/2), which inter alia refers to the extensive work carried out by Reason and his colleagues in this area (Reason, 1990; Maurino *et al*., 1995).

The fundamental point here is that the TLS was never intended to be a measure of 'acceptable ATC failure' but as a target that the ATM system should achieve. The point is well made by Baumgartner's (2003) definition: 'TLS: The level of safety which the total system is designed to meet'. The present SRC Policy in essence excludes STCA from such calculations, i.e. it is somehow deemed *not* to be a part of the Total System.

2.3. *Separation minima.* One of the fundamental safety defences used to protect against mid-air collisions is the use of separation minima (sometimes referred to as separation standards – ICAO (1976 and 1998) and Brooker (2002) are general references). In simple terms, they are the minimum distances that controllers should permit between aircraft. Any sensible theory or framework for mid-air collision risk estimation has to provide an understanding of the steps required to get from considerations of separation minima to estimates of collision risk. From a system viewpoint, separation minima are formal rules that help set up the structure of safety defences against mid-air collision. Originally, these were required because of inaccuracies in radar and altimetry data (which are still important aspects) but they are increasingly seen as buffers to permit effective warnings and controller/pilot actions. Some fraction (*sic*) of the TLS is allocated to failures relating to the magnitude of the separation minima (e.g. see Harrison and Moek (1992) re vertical separation).

Any view that the existence of separation minima can somehow guarantee safety by protecting against technical errors on the flight path is wrong. Separation minima of themselves do not guarantee safety, any more than a road speed limit prevents car crashes. It is actually the control of the failure process when minima are breached that delivers the required safety. This depends on people – controllers and pilots – noticing potential hazards, in which they are supported by machines, such as STCA, which direct their attention to such circumstances. Separation assurance, through separation minima and human intervention, and collision avoidance, through STCA, are therefore complementary safety defences. One reduces the complexity of decisions that controllers have to take; the other alerts pilots and controllers to the need to take a decision. Both of them are now integral parts of the ATM safety system – so why should only one of them be included in risk calculations?

Thus, separation minima are tools for ATC. They do not offer protection in themselves – the consequent low density of traffic in airspace helps to produce a low mid-air collision risk. As noted earlier, most Airproxes arise from one aircraft being on what could crudely be called 'the wrong track' (Brooker, 2002/2). Therefore, safety barriers are required which do not work on the supposition that what the aircraft are doing, through pilot and controller actions, is inherently correct. STCA meets this need.

One final point about STCA and separation minima needs to be made, which can be a source of confusion for newcomers to the topic. STCA is concerned with potential conflicts in projected flight paths. STCA alerts generally occur many tens of seconds before the lateral separation minimum is breached. They are not intended to tell the controller or operational supervisors about separation minimum infringements.

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

3. ASPECTS OF SAFETY NET POLICY.

3.1. *Introduction.* Although short, the SRC Policy is quite difficult to read, because it generally deals in abstract concepts and cross-refers to related documents. A good policy surely needs to set out evidence, logical connections, and consideration of the potential practical consequences of different options. The method adopted here is to try to understand the subject by taking a very simple picture of the ATM system and then posing some practical risk assessment and safety management questions about the implications and consequences of adopting certain views and policies on safety nets. The answers proffered should then illuminate different aspects and implications of the policy. The significant issues raised by the SRC Policy can thus be scrutinised by the use of this 'toolkit'. The simple picture – the ATM Baseline – is: en route ATM in controlled airspace with the usual technology; the usual controller and pilot tasks and interactions; STCA operational; and the usual TLS.

3.2. *Question: Did the original derivations of TLSs say that safety nets should be excluded from risk assessment?* The answer is no. TLSs were derived as system design targets against all the risks to which an aircraft could be exposed. The risk calculations for an ATM system's ALS were seen as potentially including all mitigating factors, from controller monitoring and intervention to automatic warning systems, to even See-and-Avoid (e.g. ICAO (1976) paragraph 3.2a on Visual avoidance).

In the present context, there were very interesting discussions in 1970/80s ICAO panels about the effectiveness of See-and-Avoid and its possible inclusion in risk calculations. Recent research (BASI, 1991; Moore, 1998) tends to confirm the views expressed then about the effectiveness of See-and-Avoid. In visual conditions, in the absence of some form of traffic alert, the probability of a pilot visually acquiring a threat aircraft is generally low until a short time before closest approach. At commercial aircraft speeds, See-and-Avoid usually fails to alert potential collisions, as, even under the best conditions, visual search can be like looking for a needle in a haystack, and in poor visibility the chance of it succeeding would be negligible. Thus, the pilot cannot visually acquire other traffic reliably or consistently. Recent trials under test flight conditions (Moore, 1998) suggest that visual acquisition alone, i.e. without any cues from an alerting system, is less than 50% effective.

Thus, See-and-Avoid does not reduce risks significantly, but, much more important, it is an unsystematic method for reducing risks. Taking a philosophical view about the nature of safe ATM for aircraft flying in controlled airspace under IFR, it is surely very dubious to be reliant on visual, non-instrument, means for any part of the protection against catastrophic system failures – which a mid-air collision would certainly represent. This is why the inclusion of risk reduction effects arising from See-and-Avoid in ALS estimates was judged a weak line of reasoning. In the present context, the important point to note regarding these comments on See-and-Avoid is that it was not excluded because of any conflict with TLS principles but through analyses of its reliability and effects in a controlled environment.

This helps in the understanding about what should constitute a safe ATM service (e.g. see Profit, 1995). Acceptable safety should not place any quantitative reliance on 'last ditch' avoidance action by a pilot who happens to catch a glimpse of an approaching aircraft. In controlled airspace, it is the job of the ATM system to deliver the necessary safety objective of maintaining safe separation between aircraft. It is necessary that the system's safety defences should each perform this function in a systematic and consistent fashion.

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

This then highlights the issue about what actually constitutes the ATM system. STCA is an integrated function within the ground-based ATM system, operated according to specified rules that are formally documented in official ATM provider and regulator documents. The pilot does not have to know what combination of people and machines is providing a safe ATM service. All that the pilot really needs to be able to trust is the safety performance that is delivered to the aircraft – the exposure to risk from the flight being in the ATM system.

3.3. *Question: Would ATM providers have developed STCA if they would get no 'safety credit' for doing so?* Do the public or people in the aviation industry measure ATM providers' performance excluding STCA? The ATM system fails when people die, not when pilots or controllers make potentially (*sic*) catastrophic mistakes. The public's concern is surely with the safety level *achieved* in the real world, not with what it might have been in some theoretical universe – composed of what ifs – in which STCA did not exist.

The history of National Air Traffic Services (NATS) introduction of STCA in the UK provides some useful lessons. First, it should be noted that the responsible senior managers in NATS are primarily judged by the safety performance of the organisation, and this has been true since the earliest days. Given the great rarity of accidents, the measure of safety in the present context is the frequency of serious Airproxes (previously, Airmisses, which were the subset of Airproxes reported by pilots). Serious Airproxes are those judged by an independent panel as having some degree of hazard. Thus, the serious Airprox rate per hour is a proxy for the mid-air collision rate – it is the best evidence available to the ATM provider and its airline and passenger customers. [NB: Airproxes attributable to equipment failures and poor interfaces are a very small proportion of the total, e.g., in the last five years, for only one UK Airprox – 184/2001 – was radar performance even a contributory factor.]

In the late 1980s, NATS suffered some extremely serious Airproxes, and NATS management came under great pressure from the regulatory authorities, professional bodies, parliamentary bodies and the public to demonstrate that action was in hand to assure a safe ATM service. This accelerated the development and implementation of STCA, which had comparatively recently become practically feasible with the progressive introduction of new-generation SSRs. STCA has turned out to be a major success story, as evidenced by the infrequency of serious Airproxes in recent years and by the fact that less serious Airproxes have been prevented from becoming serious by controllers' action following STCA warnings. The main point is that NATS performance has been judged on the safety performance that it has delivered to flights and passengers. The safety track record of NATS has been seen as successful because the ATM services stakeholders – regulatory authorities, professional bodies, parliamentary bodies and the public – monitor the rate of serious Airproxes. They do not ask what the rate would have been had STCA not been operational.

Suppose that stakeholder judgement of the NATS management were indeed to be through estimation of the rate of Airproxes without STCA, as implied by the SRC Policy. Thus, STCA could not be a solution to the perceived problems with serious Airproxes – NATS would get no safety credit for implementing STCA. NATS would therefore tend to focus efforts on improving the traditional system, mainly through its controllers' performance. This would be of limited value, because the degree of improvement, e.g. through extra selection, training and monitoring of controllers,

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

would need to take place over a period of years, and would in any case not add an extra safety defensive barrier to ATM system safety. Thus, in this alternative universe implied by the SRC Policy, the incentive on NATS responsible managers to improve the delivered safety of the ATM system could be changed dramatically. Progress on STCA which, to repeat, has been demonstrated to reduce serious hazards very significantly, would probably have been considerably retarded.

It is aircraft collisions or serious Airproxes that measure the failure rate of ATM, not the number of times that STCA produces alerts. But ATM providers still need to have a very strong interest in their safety contributions without safety nets. Without doubt, they need to monitor STCA alerts and Airproxes generally, and indeed to have an operational target for their rate per flight hour, but that is not logically equivalent with equating such a target to the TLS derived for total ATM system design. This appears to be the core fallacy underlying the SRC Policy: a desire to set an ATM provider a performance target without safety net does not imply that such a target must be the TLS. There could be two targets, one for mid-air collisions, for which serious Airproxes would be a proxy, and the other for (say) Safety Separation Breaches, composed of incidents in which separation was significantly breached (rather than a minor infringement by a fraction of a nm) or in which the controller had to act on a STCA alert. This produces a hierarchy of safety targets:

Type of Event	Target (as flying hours rate)
Mid-air collision	TLS
Serious Airproxes	TLS × cautious ratio of serious Airproxes to collisions
Safety Separation Breach	TLS × cautious operational management factor

If some sloppy ATM provider were to neglect the traditional – sans STCA – ATC elements, then the number and complexity of system defects (measured by Safety Separation Breaches) would tend to show marked increases; and hence represent a failure to maintain an essential part of the safety defences in good order. But, to reiterate, a requirement to monitor these kinds of performance is not logically equivalent to requiring the elimination of STCA from hazard analysis calculations, let alone a requirement that the ATM system should meet the TLS on the supposition that STCA is effectively inoperative.

3.4. *Question: Are safety nets different from extra controllers?* In what sense are safety nets different from extra controllers? This is at first sight a rather odd question! The underlying hypothesis being tested is that if two ways of doing things produce equivalent effects on safety then they should be assessed on the same basis.

STCA works on the basis of specified software algorithms, which are actually decision rules about how to process information on aircraft flight paths as derived from radar data. If the product of the decision rules is that there is some reasonable possibility of a near mid-air collision or worse, then an appropriate alert is given to the controller. The fundamental points are that the information source is secondary surveillance radar data – basically the same information that the controller sees on the screen – and that the decision rules are essentially based on geometrical extrapolations of aircraft paths.

Suppose that additional monitoring controller jobs were to be created, one for each radar controller. [This is not a wholly artificial example: some controllers do actually

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

function largely as monitors of other controllers – the Precision Runway Monitor arrangements in the USA are an example.] The only task of these individuals would be to monitor the radar data on the screen and lean over the radar controller's shoulder to tell him or her that two aircraft might be coming into conflict. Suppose they receive training to identify potential conflicts with exactly the same decision rules as STCA. When fully trained and effective, they would then perform exactly the same function as STCA, so that every alert that STCA would have made they would tell the radar controller about – and no more than that.

Given the existence of these monitoring controllers, the mechanical STCA software could be shut down – because the humans would be delivering a completely equivalent service. The radar controller would be receiving equivalent information and presumably making the same decisions and issuing the same instructions to pilots. But ATM system safety – if the SRC Policy view of what constitutes the ATM system were to be adopted – would show huge improvements, because the safety benefits would somehow be being transferred from being part of an additional overlay to being an integral part of the ATM system. Thus, a safety defensive barrier is regarded as having different implications for risk assessment depending on how it is implemented, even though its effects and safety benefits to the end user are identical. This inconsistency is an absurd consequence of the SRC Policy.

In reality, monitor controllers would probably be less effective than ordinary STCA. Human factors research (e.g. see Wickens and Hollands, 2000) provides a great deal of evidence that people's monitoring performance is subject to various types of error. The radar controller might in practice be rather better at monitoring than the over the shoulder individual because of his or her role in creating and evolving the traffic pattern on the screen.

To summarise: the simple point made above is that if the function of STCA were carried out by controllers rather than by a machine then it would not count as a safety net. But consistency in risk philosophy must be a guiding principle. The SRC Policy is absurd in suggesting that information provided to the controller through the aid of computer software should be treated as having less merit in safety terms than identical information provided by a colleague.

3.5. *Question: Are there lessons from risk estimation methods?* Risk assessment of ATM systems is generally a complex exercise, involving computer or mathematical models of the hazard process involved, and data collection to fix the parameters in these models. The FAA/Eurocontrol (1998) review document shows the range of modelling that has been employed. Risk assessments of even comparatively straightforward concepts of operation are hard to carry out in terms of robust quantitative estimates – but these are precisely what is required if an ALS is to be estimated for comparison with the required TLS. Risk assessments usually have to make assumptions in deriving quantitative estimates. These assumptions often cannot be fully verified through data collections. In these circumstances, cautious assumptions are made, by which is meant that upper limits of parameters are used in order that the final risk estimate will to some degree over-estimate the true level of risk.

There is a particular problem with new types of operational concept, in which the protection offered by some of the safety defensive barriers has to rest on experiments or simulations. In these cases, several parameters may need to be estimated cautiously. This then produces a risk estimate that is in all probability much worse

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

than the true value. The danger is then that the new concept will be judged over-pessimistically, and hence will not be pursued as a future system – whereas it could well have been a real improvement over the present system. This inherent problem is exacerbated if the SRC Policy is followed, i.e. with the defensive barrier benefits of safety nets being excluded from ATM System safety calculations. Hazard analysis calculations incorporating STCA provide a measure of the true risk potential in the real world. Excluding STCA puts an extra burden on risk estimation, in that the calculations will tend to be even more cautious – and hence more pessimistic about the value of new concepts. This will act to retard the introduction of acceptably safe systems embodying novel operational concepts, because it has become more difficult to prove their safety.

The exclusion of STCA can make a substantial difference to risk calculations, particularly when new concepts (e.g. Airborne Separation Assurance Systems – ASAS) are being examined. P-RNAV routes separation minima are difficult to determine cautiously unless some allowance is made for safety benefits from STCA (there is a particular problem about aircraft flying wrong tracks, e.g. see DNV (2003). Eurocontrol studies are being carried out into the effectiveness of STCA and normal controller intervention for RNAV routes (Eurocontrol, 2003). See Brooker (2002/2) for some approximate sums on UK ATM safety defences as evidenced by Airproxes.

3.6. *Question: At what point does a conflict probe become a safety net?* Conflict probes are software tools used by the controller to investigate whether changes need to be made to the aircraft flight paths under his or her control. ['Controller' here could be an aircraft pilot if some kind of ASAS were to be adopted.] They have been the subject of much past and current research (in the present context, Shakarian and Haraldsdottir, 2001 is an interesting recent paper). Conflict probes are seen as medium term detection/prediction tools, with look-ahead times of some minutes, whereas STCA might have a look-ahead time of 90–120 seconds (for comparison, ACAS RAs would be ~25 seconds).

What would be the dividing line between a conflict probe and STCA? It is quite possible that STCA algorithms could effectively be embedded in a conflict probe tool. Thus, the controller might carry out different types of sweep of his or her traffic – with varying look-ahead times. Would the safety benefits from a conflict probe be counted as part of ATM system safety? What would be the critical look-ahead time? Is some specific slice of risk reduction to be allocated to the ATM system and to the additional overlay?

3.7. *Are the safety benefits from STCA unnecessary or marginal?* Is STCA somehow icing on the cake – a small bonus in safety terms. The facts about Airproxes (Brooker, 2002/2; UK Airprox Board, 2003) demonstrate the importance of STCA and the extent to which is integrated into ATM to ensure safety. It is not a marginal bonus.

It should not be assumed that the present European en route ATM system is safe – in TLS terms – in the absence of STCA. For the system to be assured of delivering the incredibly demanding TLS, the array of safety defences of Section 2 are *all* needed (e.g. see Brooker (2002)). It cannot be proved with confidence that en route ATC without STCA will be sufficient to ensure that the TLS is met. Even in strictly controlled experiments with fixed route systems, e.g. Eurocontrol (2003), controllers fail to detect and resolve 10+% of potential collisions. Thus, warning systems such

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

as STCA are not in practice last ditch safety bonuses, but vital pieces of safety equipment, integral to the delivery of the very demanding safety targets for en route ATM.

Full hazard analyses of the en route system have seldom been attempted. Most studies focus on a specific element of risk, a half or a tenth in one or two dimensions, which is then matched against some fraction of the TLS by use of a risk budget philosophy (Profit, 1995). Examples are Reduced Vertical Separation Minima – see Harrison and Moek (1992) – and radar separation minima – see Sharpe (1991). The case of the latter is very relevant: the choice of minimum needs to ensure, to a very high degree of confidence, that radar inaccuracies per se are not putting the aircraft into a risk of collision – but the full picture has to recognize how controllers use minima for operational reasons.

How serious in quantitative terms is this false confidence in ATC safety performance, i.e. that without STCA it can meet the TLS? If STCA's beneficial effects were removed, how many Airproxes would have been more serious?

4. DOES THE SRC POLICY PROVIDE REASONED ARGUMENTS?

This section examines points made in the SRC Policy. There ought to be some logical or evidence-based rationale in the paper or in its references. As noted, text from that document is shown here in italic font with quotation marks. The extracts quoted below all derive from the text in "*Appendix A 1. Supporting Rationale*". Note that much of the justification refers to Eurocontrol SRC (2000) – referred to as 'ESARR 4'.

The relevant paragraphs are:

> '*Within ESARR 4, the approach taken is that the ATM system can only mitigate the effects of the hazards within the Strategic Conflict Management and Separation Provision functions of the ATM system itself. When an ATM hazard has an effect on the aircraft, it is concluded that there is nothing further that the Separation Conflict Management and Separation Provision functions of the ATM system can do to reduce the effect of the hazard. At the point where the hazard has or is about to have an effect on the aircraft, the Collision Avoidance function of ATM is responsible for reducing the effect of that hazard.*
>
> *Any system that is designed to reduce the severity of effect of a hazard on aircraft and third parties, given that an effect on the ATM system (e.g. infringement of separation minima) has already occurred, is therefore outside the scope of ESARR 4 and cannot be considered in ATM Risk Assessment and Mitigation for the Strategic Conflict Management and Separation Provision functions.*
>
> *Safety nets, as considered by this document, are all designed to reduce the effect of a hazard on aircraft and subsequently on third parties, given that an effect on the ATM system has already occurred, and therefore cannot be used within the risk assessment and mitigation process of ESARR 4.*'

This text therefore uses a three layer picture of conflict management:

- Strategic conflict management.
- Separation provision.
- Collision avoidance.

The first two are stated to be part of the ATM system in ESARR terms and the third is not. Safety nets are counted as being in the collision avoidance layer. No substantive arguments about hazard analysis are set out in the SRC Policy as to why

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

these classifications are adopted. The Policy rests on an appeal to other documents, in which an apparently arbitrary judgement has been made. Vital safety policies should surely not depend on assertions, but rather should rest on a clear and rational treatment of integrated ATM system safety defences. The right policy should be based on evidence, logical connections, and consideration of the potential practical consequences of different options; and the process for policy development should include a rigorous challenge element.

To say that STCA, in *safety benefit* terms, is an *additional overlay* to the ATM system does seem a very bold – indeed perverse – statement. An intelligent non-aviation person visiting an ATC centre would find it very strange that STCA – enabled through software in the main ATC computer, carefully designed into the controller's display, and the subject of detailed guidance in the ATM provider's and regulator's formal operating documents – is not part of the ATM system.

To say that STCA is part of a collision avoidance (*sic*) layer separate from the ATM system seems a sweeping decision, given the differences between STCA and ACAS. ACAS is announced to the pilot and STCA to the controller. ACAS-induced (vertical) manoeuvres are atypical, whereas a controller will generally react to an STCA warning by normal vectoring instructions, little different from his or her typical instructions when that controller alone detects a potential conflict.

The final paragraphs of Appendix A appear to be a mixture of the sensible and the perplexing:

> '*Safety Nets are not considered to form part of the Safety Assessment of the Strategic Conflict Management and Separation Provision function of the ATM system required by ESARR 4. However, they do have the potential to affect the operation of that system, and also contribute to the overall level of aviation safety achieved.*
>
> *As safety nets, intended for operation in the Collision Avoidance part of ATM, can themselves induce new hazards to the Separation Provision function of ATM, they shall be subject to specific safety objectives and requirements derived by the application of ESARR 4.*'

The second paragraph is sensible. Obviously, the full consequences of STCA have to be taken into account in risk assessments. STCA alerts can sometimes induce hazardous aircraft configurations, so the need is similar to that for vaccines and inoculations – can the positive improvements be shown to outweigh markedly any deleterious impact? It is the first paragraph of the quotation that causes most concern. What is this concept *overall level of safety achieved*? Is it some new kind of target? If so, on what basis is it to be derived and how should it be used? As it stands, it is no more than a vaguely positive phrase, which provides no additional guidance about design, risk assessment or operations.

5. CONCLUSIONS.

The Eurocontrol SRC Policy on safety nets and risk assessment is wrong. The Policy is invalid because it does not build rationally and consistently from ATM's firm foundations of TLS and hazard analysis. The Policy is bad because it would tend to retard safety improvements. It appears that the core fallacy underlying the SRC Policy is that a desire for an ATM provider to have a performance target without safety net does not imply that such a target must be the TLS.

The ATM system fails when people die, not when pilots or controllers make potentially (*sic*) catastrophic mistakes. The public's concern is surely with the safety

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

level achieved in the real world, not with what it might have been in some theoretical universe – composed of what ifs – in which safety nets such as STCA did not exist.

STCA can be shown to be formally equivalent to the use of extra controllers, carrying out a monitoring function. It is absurd that information provided to the controller through the aid of computer software should be treated as having less merit in safety terms than identical information provided by a colleague. If two ways of doing things produce equivalent effects on safety then they should surely be assessed on the same basis.

The SRC Policy lacks clarity about the dividing line between a conflict probe and STCA, as the latter's algorithms could effectively be embedded in a conflict probe tool. The safety benefits from a conflict probe would presumably be counted as part of ATM system safety – opening up a further inconsistency.

Hazard analysis calculations incorporating STCA provide a measure of the true risk potential in the real world. Excluding STCA puts an extra burden on risk estimation, in that the calculations will tend to be even more cautious – and hence more pessimistic about the value of new concepts. This will act to retard the introduction of acceptably safe systems embodying novel operational concepts, because it has become more difficult to prove their safety.

All systematically applied safety defences should be considered as part of the integrated ATM safety system. STCA is a tool used by control teams; enabled through software in the main ATC computer; carefully designed into the controller's display; and the subject of detailed guidance in the ATM provider's and regulator's formal operating documents. Controller instructions and aircraft manoeuvres post STCA alerts are the same as those that the controller would have instituted had he/she noted the problem in the absence of STCA advice.

Safety net policy must rest on a clear and rational treatment of integrated ATM system safety defences. A new safety net policy, appropriate to safe ATM system improvements, is needed. This must recognize that STCA is an integrated part of ATM system defences. The right policy should be based on evidence, logical connections, and consideration of the potential practical consequences of different options. The process for policy development needs a rigorous challenge element. The effects of STCA in reducing deaths from mid-air collisions should be fully included in hazard analysis and safety audits in the context of the TLS for total system design.

ACKNOWLEDGEMENTS

I would like to acknowledge support through a research grant by the Civil Aviation Authority's Safety Regulation Group (SRG). I stress that SRG is in no way responsible for this material. I also thank Peter Stastny, the Head of Eurocontrol's Safety Regulation Unit, for his comments on an earlier draft, which prompted the addition of detailed explanations and relevant references. He is in no way responsible for the form or content of the present text.

REFERENCES

BASI (1991). Limitations of the See-and-Avoid Principle. Australian Department of Transport and Communications.

Baumgartner, M. (2003). One safe sky for Europe – A revolution in European ATM. *The Controller*, July, 8–12.

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press

Brooker, P. (2002). Future Air Traffic Management: Quantitative En Route Safety Assessment Part 1 – Review of Present Methods; Part 2 – New Approaches. This *Journal*, **55**, 197–211 and 363–379.

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

DNV (2003). Safety Assessment of P-RNAV Route Spacing and Aircraft Separation Final Report. *TRS 052/01 for Eurocontrol Job No. C321556 Revision 1*, April.

Eurocontrol (2003). P-RNAV Route Spacing Simulations, Tampere, Finland, 14–18 October 2002 Simulation. TARA/23, IP.

Eurocontrol SRC (2000). Risk Assessment and Mitigation in ATM. *Eurocontrol Safety Regulatory Requirement ESARR 4. Edition 1.0*, Eurocontrol, Brussels.

Eurocontrol SRC (2003). SRC Policy 2: Use of Safety Nets in Risk Assessment & Mitigation in ATM. *Edition: 1.0*, dated 28 April.

FAA/Eurocontrol (1998). A Concept Paper for Separation Safety Modeling: An FAA/Eurocontrol Cooperative Effort on Air Traffic Modeling for Separation Standards.

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.

ICAO (1976). Methodology for the Derivation of Separation Minima Applied to the Spacing between Parallel Tracks in ATS Route Structures. *ICAO Circular 120-AN/89/2, Second Edition.*

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

Maurino, D. E., Reason, J., Johnston, N. and Lee, R. B. (1995). *Beyond Aviation Human Factors.* Ashgate Publishing, Aldershot, UK.

Moore, S. M. (1998). Comparison of Alerted and Visually Acquired Airborne Aircraft in a Complex Air Traffic Environment. *Proceedings of the 1998 Advances in Aviation Safety Conference, SAE/P-321, 981205*, Daytona Beach, Florida, April 6–8, 1998. SAE.

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

Reason, J. (1990). *Human Error*, Cambridge University Press, Cambridge, UK.

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

Shakarian, A. and Haraldsdottir, A. (2001). Required Total System Performance and Results of a Short Term conflict Alert Simulation Study. *4th USA/Europe Air Traffic Management R&D Seminar.*

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.

UK Airprox Board (2003). Analysis of Airprox in UK Airspace. Twice-yearly series of Reports.

Wickens, C. D. and Hollands, J. (2000). *Engineering Psychology and Human Performance*, Addison Wesley, Longman, New York.

https://doi.org/10.1017/S0373463304002735 Published online by Cambridge University Press