THE JOURNAL OF NAVIGATION (2005), **58**, 1–16.
DOI: 10.1017/S037346330400308X Printed in the United Kingdom

THE JOURNAL OF NAVIGATION

VOL. 58 JANUARY 2005 NO. 1

Airborne Collision Avoidance Systems and Air Traffic Management Safety

Peter Brooker

(*Cranfield University*)
(Email: p.brooker@cranfield.ac.uk)

A new ICAO Policy on Airborne Collision Avoidance Systems is needed, which recognizes it to be an integrated part of the air traffic management system's safety defences; and that should be fully included in hazard analyses for the total system's design safety targets.

KEY WORDS

1. ATM. 2. ATC. 3. Mid-air collision. 4. Collision Avoidance.

1. INTRODUCTION. ACAS (Airborne Collision Avoidance Systems) is the ICAO name for what in the USA is referred to as TCAS (Traffic alert and Collision Avoidance System). ACAS refers to ACAS II, the kit used by airliners. Present International Civil Aviation Organization (ICAO) policies for the use of ACAS – the 'ACAS Policy' – are restrictive. In particular, air traffic control (ATC) systems and procedures have to be judged safe without considering the effect of the ACAS safeguard. The general background is well set out at Honeywell (2002). The

history of ICAO decisions and policies shows that its choices are largely based on 'consequentialism', i.e. with the 'rightness' of actions being judged by the value of their consequences. ICAO should focus on progressively reducing the numbers of deaths from aviation accidents. Are the reasons for this Policy therefore valid? Would a change ensure that more people can travel in a safe system or that safety can be delivered more cost effectively?

After a short background Section 2, Section 3 sets out the problems with the present Policy. Section 4 is then a critique of the ANC11 ACAS paper (ICAO AN11, 2003), in which arguments were put forward by ICAO to justify the present Policy. Section 5 is a series of questions and answers about the present ACAS Policy, in essence a set of straw man questions that might be conceived as support for it. Conclusions are at Section 6.

2. BACKGROUND

2.1. *ICAO ACAS Policy*. ICAO Policy on ACAS (ICAO Annex 11 and Doc 4444 PANS RAC/501) can be summarized as:

- ACAS is a 'last resort' airborne safety net, and has no other role in the ATM system.
- The provision of ATC services in a given airspace shall not be based on the ACAS equipage of the aircraft.
- ATC units shall provide the same services to ACAS and non-ACAS aircraft.
- ATC systems and procedures have to be judged safe without considering the effect of the ACAS safeguard.

The Policy is therefore that 'separation provision by ATC' and collision avoidance must be separately effective. Thus, separation provision by ATC must therefore achieve the required level of safety without any consideration of the benefits from collision avoidance.

2.2. *The ATM Total System*. A distinction will be made here between 'ATC' and the 'Air Traffic Management (ATM) system':

- *ATC* A service provided by controllers in ATC units to prevent collisions between aircraft and expedite orderly traffic flows.
- *ATM system* Everything that contributes to the safe movement of air traffic – the 'Total System'.

Safety in ATM is 'the interaction between Procedures, People and Equipment' (Baumgartner, 2003). The pilot is part of the ATM system. Total System Safety depends on the pilot's actions, which include following instructions from the controller (given the latter's greater knowledge of the ATM environment and the risks posed by neighbouring aircraft) – **and** on the pilot acting in accord with ACAS alerts.

2.3. *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 to the procedural rules followed in setting up system operations. No safety barrier offers perfection – people make mistakes, information is misunderstood, and equipment works only within specific parameters. ATM safety defences have progressively been added and enhanced, and for which systems are considered as a whole (Profit, 1995). The concept of safety defensive barriers for ATM is explained in

Brooker (2002), which *inter alia* refers to the extensive work carried out by Reason and his colleagues in this area (Reason, 1990; Maurino et al., 1995).

2.4. *Separation Minima.* One of the crucial safety barriers used to protect against mid-air collisions is the use of separation minima (sometimes referred to as separation standards – ICAO (1998) and Brooker (2002) are general references). Separation minima are the minimum distances that controllers should permit between aircraft – they help to set up the structure of safety defences against mid-air collision. Separation minima of themselves do not guarantee safety, any more than a road speed limit prevents car crashes. It is the existence of an effective 'failure process' when minima are breached that delivers the required safety. 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. Most Airproxes (UK Airprox Board, 1999-) arise from one aircraft being on what could crudely be called the 'wrong track' (Brooker, 2002). Therefore, safety barriers are required which do not work on the supposition that what the aircraft are doing, through pilot and controller actions, is 'correct'. ACAS meets this need.

3. THE PROBLEMS WITH THE POLICY.

There are four problems with the present ACAS Policy:

- The current Policy fails to live up to ICAO's aims.
- Safety defences are not viewed as part of an integrated ATM safety system.
- The Policy is not consistent with TLS and hazard analysis philosophy.
- The Policy retards the introduction of innovative safe systems.

These are outlined in order.

3.1. *Failure of current Policy to meet ICAO's Aims.* ICAO's aims include phrases such as: 'meet the needs of the worldwide population for safe, efficient, and economical air transport'; 'promote flight safety'; and 'promote the development of all aspects of international civil aeronautics'. All of ICAO's policies are subordinate to ICAO's objectives. ICAO's ethics of safety underpin everything that ICAO does. The burden is that every policy, every procedure, every regulation must be kept under review and scrutinised to determine if any other feasible option offers better prospects of saving lives. This continuous review and search process must take into account new information about risks, ways of analyzing safety, and the probable effects of new technology. Hence, if better policy options can be identified – reducing the risk of aviation deaths, improving the changes of meeting traffic growth successfully, etc – then they must be seriously considered. It is vital that ICAO's policies match its declared objectives on safety, which translates into reductions in aviation deaths. To achieve this, it is essential to move forward from the present ACAS Policy, which essentially 'freezes' the ATM concept to a 1980s vintage.

3.2. *Integrated Safety System.* Safety defences are part of an integrated ATM safety system and it is therefore irrational to count arbitrarily some elements in risk calculations and to omit others. A general principle for ICAO should be to consider all systematically applied safety defences as part of the integrated ATM safety system. No proof of this general principle can exist, but it would seem to be a prudent position to adopt. Baumgartner's comments on the importance of system integration recognize the importance of the aim (Baumgartner, 2003).

On 1 July 2002, two ACAS-equipped aircraft collided over the Swiss-German border. The flight crew of one aircraft did not follow the ACAS alert, but followed the ATC instruction. Guidance material following the Überlingen tragedy (e.g. Eurocontrol, 2002) now stresses that pilots should follow Resolution Advisories (RA) and that controllers should not attempt to modify the flight path of an aircraft responding to an RA. Indeed, the controller 'ceases to be responsible for separation' for the aircraft involved in such manoeuvres. If ACAS is seen as dominant over ATC in these circumstances, then it must surely be an integrated element of ATM system safety?

3.3. *Consistent TLS and Hazard Analysis Philosophy*. The crucial quantitative safety concept in ATM is that of a Target Level of Safety (TLS), a quantified risk level that a system should – i.e. be designed to – deliver. A TLS covers all aviation-related causes. It is measured in fatal aircraft accidents per so many aircraft flying hours. The TLS relates to total system design: 'all types of failure, mechanical, procedural and human, which generate a risk of collision will be accounted for' (Brooker and Ingham, 1977). 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. The TLS value therefore gets tighter and tighter over time. The accidents it counts are those in the real world: they do not include any prevented through the uses of ACAS.

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. 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 ALS < TLS? The point about the ATM system is well made by Baumgartner's (2003) definition: 'TLS: The level of safety which the total system is designed to meet'. Risk calculations in hazard analysis essentially multiply the probabilities of each of the ATM safety system defences being breached – the present ICAO Policy in essence excludes ACAS from such calculations. Therefore, current ICAO Policy deems ACAS not to be a part of the Total System.

However, the TLS was not developed on the basis that certain types of system, technology or procedure would be either present or absent, i.e. did not *a priori* rule out the use of ACAS in delivering the TLS. The risk calculations against the TLS were seen as potentially including all mitigating factors, from controller monitoring and intervention to automatic warning systems. ACAS is now a systematic integrated part of the ATM safety system defences, and therefore should be fully included in hazard analysis and safety audits in the context of the TLS for total system design. Figure 1 sums up these points.

3.4. *Risk Assessment Over-pessimism*. New ATM systems must be proved to deliver the necessary safety. Risk assessment of ATM systems is generally a complex modelling exercise. These assessments usually have to make assumptions in deriving quantitative estimates of the protection offered by safety defensive barriers. 'Cautious' assumptions are used, by which is meant that upper limits of parameters are used so that the final risk estimate will to some degree overestimate the true level of risk.

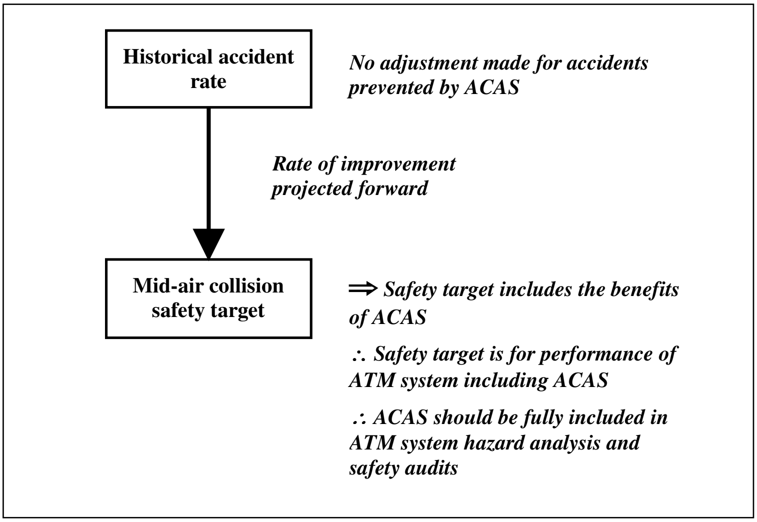

Figure 1. The correct Safety Target process and ACAS.

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 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 in reality it could well have offered real improvements. This process therefore retards the introduction of acceptably safe systems embodying novel operational concepts, because it has become more difficult to prove their safety. This inherent problem is exacerbated if the ICAO Policy is followed, i.e. with the defensive barrier benefits of ACAS being excluded from ATM System safety calculations. Not doing this puts an extra burden on risk estimation, in that the calculations will tend to be even more cautious – and hence unjustifiably over-pessimistic about the value of new concepts. Hazard analysis calculations that incorporate ACAS provide a measure of the true risk potential in the real world.

Figure 2 illustrates the problem: the factor 10–100 comes from McLaughlin (1999); the factor 100–1000 comes from consideration of Poisson sampling (usually appropriate for rare events). [NB: these figures implicitly assume that ACAS is properly integrated into the ATM system.] These tough targets pose major problems for the development – and proof of safety – of dramatically new and complex ATM systems, e.g. in 'integrating aircraft trajectory information into the system', 'combination of existing ground-based systems and advanced satellites for global communications, navigation and surveillance services' (Boeing, 2003).

4. CRITIQUE OF ANC11 ACAS PAPER.

What arguments have been put forward by ICAO to justify the present Policy? There are several documents on the topic: a recent short paper was presented to the ANC11 Meeting in 2003

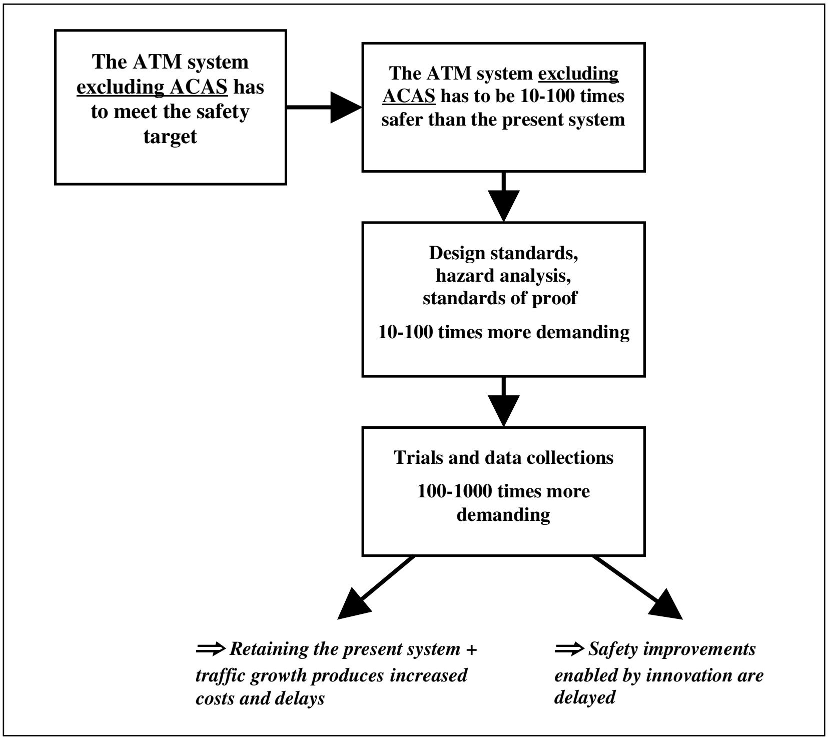

Figure 2. The bad consequences of the current ACAS Policy.

(ICAO, 2003). The following critique analyzes the points made by ICAO. ICAO text here is in italics. ICAO text that largely repeats or summarises earlier points is not included below.

The paper's summary states: '*The global air traffic management* (*ATM*) *operational concept defines three layers of conflict management, the last of which is collision avoidance. The role of collision avoidance is an important part of the operational concept. This working paper provides additional information to the references to collision avoidance as contained in the operational concept, including the use of the phrase* '*level of safety*' *and the term* '*independent*' *in the context of collision avoidance.*'

1.1 *The ATM operational concept (AN-Conf/11-WP/4 refers) defines three layers of conflict management. These are: strategic conflict management, separation provision and collision avoidance ....*	There can be no problems with general terms such as 'separation provision' and 'collision avoidance', or 'layered approach'. But it is how they are actually to be used in design and quantitative terms that is important. This needs to be as clear as possible.
2.2 *Section 2.7.6 of the operational concept: Collision Avoidance, contains the following paragraph:*	This is a series of assertions. Taking sentences one by one:

https://doi.org/10.1017/S037346330400308X Published online by Cambridge University Press

Collision avoidance is the third layer of conflict management, and must activate when the separation mode has been compromised.	Just a general definition.
Collision avoidance is not part of separation provision, and collision avoidance systems are not included in determining the calculated level of safety required for separation provision.	The first phrase restates the earlier definition but the second part is a huge jump in 'logic'. Is there a calculated level of safety for 'separation provision' different from the TLS? On this basis, future ATM systems therefore have to be designed to be safe (in TLS terms) as if collision avoidance did not exist – why? What good safety or design purpose does such a declaration serve? How would fewer people die?
Collision avoidance systems will, however, be considered part of the ATM safety management.	The phrase 'considered part of safety management' only does a fraction of the job needed. Of course, they have to be 'considered' in some way, but in what logical or quantitative sense is this to be done? What targets for their performance should be set? If the ATM system without collision avoidance meets the TLS then why should the latter even be needed? Is there some new hyper-TLS? On what basis would it be justified?
The collision avoidance functions and the applicable separation mode, although independent, must be compatible.'	What does 'compatible' actually mean in practical terms? Is present ACAS compatible with current ATC or not? If not, what is being done?
2.3.2 *… and must activate … when the separation mode has been compromised. In the future, when an ATM system based on the operational concept is implemented, collision avoidance will not be an optional extra but 'must activate when the separation mode has been compromised'. For this to occur in all environments is a challenge; however, collision avoidance equipment is already compulsory for some hazards in some environments today. Separation mode comes under the heading*	It is vital that collision avoidance is part of the present ATM system! People make mistakes. 'We believe that ACAS must be used … to account for those rare human errors.' Newman and McVenes, (2002). The use of a layered approach does not imply that collision avoidance has to be seen as outside the ATM safety system.

of Separation Provision and is a wide subject for discussion on its own. The operational concept uses a layered approach which recognizes that any system of separation provision can fail and that a layer is required to avoid collision when the separation provision layer has failed.	
2.3.4 *… and collision avoidance systems are not included in determining the calculated level of safety required for separation provision.*	This is mysterious. What is meant? Again, the sentences have to be examined one by one:
The operational concept deliberately avoids use of target level of safety (TLS) due to the fact that TLS has particular meanings today.	TLS has particular, well-understood, workable meanings, and has been applied successfully over decades, so why is it to be abandoned?
The 'calculated level of safety required', used in the operational concept, is not defined as either being 'determining' or 'demonstrating' a level of safety.	This informs the reader that what he or she is most interested in is not going to be defined in a transparently useful fashion.
In fact, the 'level of safety' may be something that is dynamically determined and proved in routine ATM operations in the future based on the operational concept.	What does 'dynamically determined' mean in practice? Does 'proved' mean the same as in normal English? It can only be speculation as to what this means in rational or pragmatic terms.
The current understanding of meaning and use of TLS is expected to evolve, and the operational concept makes provision for this.	The writer has not explained anything in simple terms and is suggesting that such as yet unknown understanding may arise over time – not that helpful to designers (compare para 2.1(a)).
In addition, there may be levels of safety for each layer of ATM system design, including conflict management.	It is aircraft collisions or serious Airproxes that measure the failure rate of ATM, not the number of times that ACAS produces alerts. But ATM service providers still need to have a very strong interest in their safety contributions without ACAS. Without doubt, they need to monitor ACAS 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

https://doi.org/10.1017/S037346330400308X Published online by Cambridge University Press

	to the TLS derived for ATM system design.
This sentence is provided to make clear that, at least in relation to separation provision, there will be a different level of safety in separation provision to the overall ATM system level of safety, as the latter will include collision avoidance.	This is not clear. Is it being suggested that there will be a 'hyper-TLS' corresponding to the 'overall ATM system level of safety', with the current TLS being reserved for the subsystem excluding the collision avoidance layer? If so, where do the numbers come from for designers?
2.3.5 *Collision avoidance systems will, however, be considered part of the ATM safety management. This is a continuation of the previous concept statement. While current arguments sometimes suggest that we justify the cost of collision avoidance equipment by reducing separation standards, the operational concept clearly proposes an alternative to this approach. The concept's previous sentence (and definition of layers) indicates that collision avoidance systems are not to be mixed with separation provision. However, the concept does recognize the importance of collision avoidance systems and their value to overall ATM safety management, which can justify their expense.*	It is difficult to believe that a professional safety analyst would attempt to justify the existence of collision avoidance systems as a reason for reducing separation minima. Rational arguments must focus on what would be the best way to ensure that the TLS is met. The key point is that the ATM system is designed and that such minima are parameters in that design, no doubt bounded by considerations of equipment performance and controllers' ability to act on separation breaches. The text here provides no quantitative or cost-benefit grounds for the introduction of effective collision avoidance systems. 'We introduce them because of their contribution to 'overall safety management' has little information content.
2.3.6 *The collision avoidance functions and the applicable separation mode, although independent, must be compatible. The operational concept, having established that the particulars of separation provision (the separation mode) and collision avoidance are separate layers of conflict management, also states that these layers must be compatible. Compatible, in this context, means that the activities of one layer do not compromise the activities of the other layer. A correctly implemented separation mode should not invoke the collision*	These would surely seem obvious points to anyone responsible for total ATM system design. But note that Airborne Separation systems would need to be integrated – both in terms of equipment and in operational usage – with an aircraft's ACAS. There are practical issues about the extent to which an aircraft's and ACAS data could be presented on the same display. Some degree of data fusion of Airborne Separation and ACAS might improve surveillance performance: this would presumably have to be in a context of ensuring the

https://doi.org/10.1017/S037346330400308X Published online by Cambridge University Press

avoidance layer. Independent, in this context, means not dependent on the other layer for operation. This, however, does not prevent one layer being aware of the activities of the other layer. The subject of how the ATM system is designed to meet these requirements is expected to generate some discussion. However, as an example, consider the following.	independence of the separation assurance and 'last resort' functions. There is already an extensive research literature on these aspects of ACAS.
As collision avoidance systems are designed to activate when a separation mode has been compromised, the ATM system design should take into account the effects of the failure of an ATM system component that changes the separation mode to a larger separation minima. This would require collision avoidance systems to ensure, despite that ATM component failure, that collisions are avoided between aircraft operating at less than the new separation minima.	But the point surely is that collision avoidance systems should prevent collisions immaterial of the separation minimum being used by the controller (or pilot?).
***3.1** In the context of the ATM operational concept:*	
(*a*) *collision avoidance is an important, but separate, layer of conflict management;* (*c*) *collision avoidance systems are of value to the ATM system and are an important part of the ATM system design and ATM safety management;*	(a) and (c) are True
(*b*) *the level of safety required for separation provision is both 'determining' and 'demonstrating', and does not include allowances for collision avoidance systems;*	(b) is either unintelligible and/or not demonstrated rationally.
(*d*) *as collision avoidance systems must activate to overcome failure of separation provision, the collision avoidance system must not be dependent on ATM system components used for separation provision.*	(d) is too simplistic – see the text in 2.3.6 above re data fusion and surveillance.

The reasoning in the ICAO paper is disappointing. It has two crucial defects:

- It fails to get to the point. It does not define its terms clearly or specifically. It largely begs the question – assuming the Policy to justify the Policy.
- It does not derive the Policy from ICAO's aims and objectives. It fails to examine different options. It does not examine other kinds of policy, in particular if they could reduce future aviation deaths.

The right Policy must be based on consideration of the potential practical consequences of different options, with people's future safety being paramount. It should be based on clear definitions, factual evidence and sound reasoning.

5. QUESTIONS AND ANSWERS ON ACAS POLICY. This section sets out a series of strawman questions that might be conceived as support for the present ACAS Policy.

5.1. *Pilots and controllers don't want ACAS integrated into the ATM safety system.* Airline pilots and controllers must get very irritated when they are represented as caricature 'Neanderthals'! The message from incidents is that they are aware of ACAS implications and that it is factored into decision-making. It is in practice seen as a part of the ATM system – pilots rely on ACAS for situational awareness of hazards: 'ACAS must be used … to account for those rare human errors that no modelling process can predict' (Newman and McVenes, 2002). ACAS is in reality seen as a part of the ATM system in which the controller works; controllers are in practice relying on ACAS to help them ensure that aircraft avoid each other. This is useful information about the reality of the ATM system – in which the controller and pilot work **with** ACAS and STCA in a **systematic** fashion. See also Hale and Law (1989). In particular, ACAS's traffic display provides valuable situational awareness for collision avoidance. This is a 'good start' for improving the traffic display on the flight deck for a function such as Airborne Separation Assurance Systems (ASAS), where separation control is delegated to the (properly equipped) aircraft, i.e. aircraft pilots take some degree of responsibility for their aircraft's separation from other flights.

5.2. *The Statistics and Guarantees Contention.* FAA/Eurocontrol (2001) comments that 'The use of ACAS does not amount to separation provision because it provides no guarantee that the risk of collision is reduced to an acceptable level'. But it is not rational to think that separation minima somehow 'guarantee safety'. Collision risk estimates to meet the TLS are by their very nature statistical statements rather than any kind of 'guarantee'. Separation minima and ACAS alerts are different safety barrier components, and these barriers are statistical in nature rather than providing 'guarantees'. One reduces the complexity of decisions that controllers have to take, while the other alerts pilots and controllers to the need to take a decision. Both of them are now integral parts of the ATC safety system – so why should only one of them be included in risk calculations?

5.3. *It is not fair to discriminate against non-equipped aircraft.* The principle of allocating some categories of airspace to aircraft whose systems achieve certain kinds of performance or which can interact with ATC in specific ways has a long and successful history. This delivers safety and meets the TLS in a cost effective fashion.

Minimum Navigation Performance System Airspace for the North Atlantic Region was introduced in the 1970s: it requires aircraft to possess navigational systems that perform about as well as triple Inertial Navigation fits. Required Navigation Performance (RNP) was developed as a tool where specific levels of navigation performance would be specified in the "development of airspace and to enhance operational efficiency". RNP was defined as a "statement of the navigation performance accuracy necessary for operation within a defined airspace." Aircraft flying IFR in European controlled airspace are required to possess and operate SSR transponders: aircraft without such kit are generally required to fly in other parts of the airspace (i.e. a 'mixed traffic' problem can be resolved). ICAO's global mandatory equipage of aircraft with ACAS has made huge progress over the last decade. The great majority of commercial transport aircraft and many other aircraft using controlled airspace will very soon be equipped with a switched-on ACAS.

5.4. *What about all the side effects caused by ACAS?* ACAS produces fewer side effects for ATC, in terms of serious incidents, than (cautiously) estimated a decade or so ago (compare Harrison (1993) and McLaughlin (1999)). ACAS certainly generates some nuisance alerts, but they do not frequently lead to hazardous incidents – the real measure of what matters in safety terms. The successes of ACAS – the lives it saved – generally get very little publicity, but they are 'the headlines that were never written, the lives that were saved' (Sabatini of the FAA quoted re aviation safety improvements, Fiorino (2003)). The parameterization of a warning device such as ACAS is a balancing act: if it is set too sensitively then many of the alerts would be considered false alarms; if it is set too coarsely then potentially hazardous aircraft configurations can be missed. Lengthy and detailed studies on ACAS have produced what is judged the best balance, given the restricted information set used by ACAS. But this is still open to improvement in the light of system changes, e.g. TCAS version V7.0 is preferred to TCAS version V6.04a given the RVSM (Reduced Vertical Separation Minima) change (Eurocontrol, 2002).

5.5. *See-and-Avoid is not part of hazard analysis – ACAS is the same kind of thing*. 'See-and-Avoid' means that the pilot visually searches for other aircraft, and then changes course if this is necessary to avoid them. Aircraft crews are exhorted to maintain vigilance so as to see and avoid potential mid-air collisions. Research has shown that See-and-Avoid does not reduce risk significantly (BASI, 1991).

For aircraft flying under IFR, it is surely dubious to rely on 'non-instrument means' for protection against mid-air collisions. Thus, there is not a strong argument for risk reduction from See-and-Avoid being included in the risk estimate. Acceptable safety should not place any quantitative reliance on 'last resort' avoidance action by a pilot who happens to catch a glimpse of an approaching aircraft. See-and-Avoid does not offer systematic protection – but ACAS does. ACAS is not dependent on random visual conditions but on the geometry of the potential conflict. For aircraft flying under IFR, it would seem rather dubious to be reliant on non-instrument means for any part of the protection against catastrophic system failures – which a mid-air collision would certainly represent. Thus, there is not a strong argument for risk reduction from See-and-Avoid being included in the ALS estimate.

5.6. *People measure ATC's performance excluding ACAS.* Do the public or people in the aviation industry measure ATC's performance 'excluding ACAS'? The ATM system fails when people die, not when pilots or controllers make potentially catastrophic mistakes. It is aircraft collisions or Airproxes that measure the failure rate of the ATM safety system, not (say) the number of times that ACAS produces alerts. 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 ACAS did not exist. It must be stressed that it is certainly important for ATC service providers to monitor ACAS interventions, and perhaps 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'.

5.7. *ACAS is icing on the cake.* The 'icing on the cake' phrase suggests that ACAS is a small bonus in safety terms. But the facts demonstrate that ACAS is a vital piece of system equipment. Before ACAS was introduced, it was quite often believed by ATC providers that ACAS would not be 'necessary' and that it would just be a 'final safeguard', seldom used. It certainly is a safeguard, but one that is used very frequently, rather than in exceptional circumstances. UK Airproxes (UK Airprox Board, 1999-) provide hard evidence: if ACAS's contributions were removed, in many cases the situation would have been markedly more hazardous. Moreover, Airproxes provide hard evidence about ACAS's performance in practice – real representative operational data scrutinized by experts.

It should not be assumed that the present European en route ATM system is 'safe' – in TLS terms – in the absence of ACAS. Full hazard analyses of the en route system have seldom been attempted. It cannot be proved with confidence that en route ATC without ACAS would be sufficient to ensure that the TLS is met. Warning systems such as ACAS are not in reality 'last ditch' safety bonuses, but rather vital pieces of safety equipment, integral to the delivery of the very demanding safety targets for en route ATM. An ACAS warning is frequently the first indicator of potential hazard, and there are numerous occasions when a pilot detects potential problems by monitoring the traffic information on the ACAS display, before even a TA; i.e. ACAS is being used as a situational awareness device. Before ACAS was introduced, it was quite often believed by ATC providers that ACAS would not be 'necessary' and that it would just be a 'final safeguard', seldom used. It certainly is a safeguard, but one that is used very frequently, rather than in exceptional circumstances. Such old beliefs about ATC safety performance without ACAS cannot be substantiated by the facts.

5.8. *Issues with Developing Countries?* Developing countries' safety records are often poorer than those of developed states – there are certainly differences in accident rates in different parts of the world. Sometimes, people have said that "ACAS being counted against the TLS" would deter developing countries from ground-based infrastructure/personnel expenditure. This is not to imply anything necessarily improper but to reflect the tightness of budgets in developing countries. It is certainly possible to imagine such possibilities. However, there is a simple answer to the criticism: ICAO exists to ensure worldwide safety. Current ICAO initiatives are working to expand – using qualified and experienced independent experts – the ICAO Universal Safety Oversight Audit Programme to include *inter alia* ICAO Annex 11.

5.9. *It is surely premature to change the current ICAO Policy.* Many potential changes provoke the response that 'it is premature and that more experience/development is required'. On this argument, the change should wait until all the problems with its use have been resolved and it is as near perfection as it ever will be. The motives behind such comments are usually well intentioned. These fall into two categories, which can be labelled 'analysis paralysis' and 'the best is the enemy of the good'.

Analysis paralysis is common – more research and analysis work can always be done. More and different simulations can be carried out. More data can be collected on failure types. "Let us wait until everyone is equipped." The consequence is that many years – possibly decades – can elapse before decisions are made and actions are taken to implement the new systems of policies.

Voltaire's comment that 'the best is the enemy of the good' is a related problem, and seems rather more sensible at first sight. In the present context, the scenario is that some 'best' version of ACAS performance is required and, until it is achieved, ACAS will not be implemented in new ways. If this best version is difficult or impossible to achieve, then there can be no implementation. This scenario certainly happens in aviation but it would be invidious to quote examples.

The answer is that the decision-making body has to make a reasoned judgement about how 'good' the system has to be before changes in policy and actions can commence. For example, with the original introduction of ACAS in 1993, challenging – but practical – criteria, such as 'reduce the Airprox rate, and hence the risk to the typical passenger, by a factor of 10' were met, and so ICAO could judge that ACAS should proceed to implementation.

5.10. *This is just not the way things are done.* Some people may express unspecified worries about ACAS being a full part of the ATM safety system: somehow it is just 'wrong'. A metaphor may be helpful to them. Consider a property developer who builds many houses of very good quality, each having a roof made out the best tiles available. He rents these houses to tenants. But when it rains heavily in one particular direction, the water comes in through the edges of some tiles. It is found that the problem cannot be fixed by doing anything to the tiles. The developer's solution is to provide every tenant with a special waterproof tape to put in the tile gaps, and this patch is successful in stopping the water coming in. Each tile is part of the roof – that is what tiles are for. But is the tape patch part of the roof? Yes, it is. It will always have to be there, and it works **with** the tiles to stop the water coming through. It was not originally part of the roof 'protection system', but it is now integral to delivering the roof's desired performance. Without the tape, the tiles will never be quite good enough to do the full job. The tape may not have been part of the original design, or even very attractive compared with the tiles, but it is now a long-term need, recognised by everyone, until somebody finds a better kind of tile.

It would be a strange sort of argument to say that something that acts permanently to protect people from the rain – even though it is not a tile – is not an integral part of the roof structure. Perhaps there is some kind of aesthetic element here? The tiles are elegant and traditional, so it is sad to have to concede that they do not do the complete job for which they were designed. Attachments to old traditions surely count for little in comparison with real-world assessments of potential impacts on people and design needs?

6. CONCLUSIONS.

All of ICAO's policies must derive from ICAO's aims and objectives. If better policy options can be identified then they must be seriously examined. It is vital that ICAO's policies match the organization's declared objectives on safety – which translates into reducing future aviation deaths.

The present ACAS Policy says that ATC systems and procedures have to be judged safe without considering the effect of the ACAS safeguard. This Policy has poor foundations and bad consequences. A change in Policy is needed. It must resolve four problems:

- The current Policy fails to live up to ICAO's aims.
- Safety defences should be viewed as part of an integrated ATM safety system.
- Safety policies should be consistent with TLS and hazard analysis philosophy.
- The Policy retards the introduction of innovative safe systems.

It is essential to move forward from the present ACAS Policy, which essentially 'freezes' the ATM concept to a 1980s vintage. The right Policy should be based on a formal examination of the potential practical consequences of different options, with people's future safety being the paramount objective. The right Policy should regard ACAS to be a fully integrated part of the ATM safety system, not some kind of supplement.

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.

Boeing (2003). Backgrounder: Air Traffic Management – Boeing Unit continues progress toward Integrated Global Air Traffic System. http://www.boeing.com/atm/pdf/ATM_backgrounder.pdf

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

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

Eurocontrol (2002). ACAS brochure. Version 2.0. http://www.nbaa.org/intl/acas2_training_brochure.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

FAA/Eurocontrol (2001). Cooperative R&D: Principles of Operation for the Use of Airborne Separation Assurance Systems (Version: 7.1). http://human-factors.arc.nasa.gov/ihi/documents/PO-ASAS.pdf

Fiorino, F. (2003). FAA's 'stock' in safety. *Aviation Week*, July 14, 48–51.

Hale, S. and Law, M. (1989). Simultaneous Operation of Conflict Alert and ACAS II in UK En-Route Airspace. DORA Report 8914, CAA, London.

Harrison, D. (1993). Results of ACAS II Safety Analysis. ICAO Secondary Surveillance Radar Improvements and Collision Avoidance Systems Panel (SICASP/5).

Honeywell. (2002). ACAS/TCAS website Guidelines & Mandates. http://www.honeywelltcas.com/mandates.htm

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

ICAO ANC11 (2003). Eleventh Air Navigation Conference Montreal, 22 September to 3 October 2003. The Role Of Collision Avoidance In Future Atm Systems (Presented by the Secretariat) ANConf.11.WP.034.1.en.wpd AN-Conf/11-WP/34

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

McLaughlin, M. (1999). Predicting the Effect of TCAS II on Safety. *Air Traffic Control Quarterly*, **7**(1), 1–18.

Newman, Capt. L. (Delta) and McVenes, Capt. T (US Airways) (2002). PRM Comes to Philly. *Air Line Pilot*, May/June 2002, 12–15. https://cf.alpa.org/internet/alp/2002/May-June_2002/may-june2002p12.html

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. (1995). ICAO.

UK Airprox Board (1999-). Analysis of Airprox in UK Airspace. Twice-yearly series of Reports. http://www.caa.co.uk/ukab/document.asp?groupid=430.

https://doi.org/10.1017/S037346330400308X Published online by Cambridge University Press