MID-AIR COLLISIONS, ELEPHANTS, AND SYSTEMS APPROACHES

By Barry Kirwan

Barry Kirwan is the Coordinator for Safety & Human Factors Research at the EUROCONTROL Experimental Centre, Bretigny, France. barry.kirwan@eurocontrol.int

- Could a civil mid-air collision happen tomorrow in Europe?
- Have we done everything we can to prevent such an accident?

These are two questions which sit uncomfortably with me, because in my personal opinion (I have to state this) the answers 'Yes' and 'No' don't fit where I would like them to, even more than five years after Überlingen, and even after strenuous efforts by many people (myself included). Several of the discussions in this issue of Hindsight already point out why it is difficult to improve the situation: more traffic, more conflict complexity; no more obvious 'low-hanging fruit', etc. Okay, but we still need to improve. So what do we do? When you have a really complex problem, people may say to you - 'take a systems approach'. This sounds boring and unlikely to deliver, however - so first, a little on elephants, a story you may already know…

Three blind men encounter an elephant. The first touches its trunk and says that an elephant is like a palm tree, another touches its side and says that an elephant is like a rough wall. Another feels its tail and says that an elephant is like a piece of rope. Each comes into contact with a different part of the elephant and is convinced that their own explanation is correct and that the others are wrong. None of them realises that they are all experiencing just one part of the same elephant and that none of their explanations are complete.

I won't labour the metaphor. Suffice it to say, systems approaches entail looking at the whole problem in all its richness and complexity, to determine a solution. If there is no single 'magic bullet' solution, then inter-related solutions must be developed: a 'system' of safety defences. 'Compartmentalised' safety won't work on complex problems. It will fail.

The Überlingen accident involved a tragically unfortunate interaction between the controller and TCAS (amongst other factors), and highlighted a fatal vulnerability in the mid-air collision defence system, which principally involves controllers, pilots, STCA and TCAS. The central 'morphology' concerned the pilot following a controller's resolution rather than his TCAS RA. Since 2002 and persisting until today, there have been a number of incidents, including some very close near-misses, which continue to follow this 'failure path', despite major efforts by ICAO to reinforce the rule of 'Follow the RA'. The threat of another mid-air collision involving a controller and TCAS may have reduced, but has certainly not gone away. So, what are the options? A number exist: some we're looking at, some not. Here are some to put on the table (to which Bert Ruitenberg's 'off-set' solution [this issue] can be added, along with his caveat that the same off-set rule must be applied internationally).

IMPROVED ACAS REVERSAL LOGIC

The first, TCAS reversal, could have prevented the Überlingen accident if it had worked comprehensively (i.e. for all scenario geometries) at the time. Work since the accident has striven to close the gaps in the reversal logic so that a situation with geometry and development like Überlingen would indeed be prevented if the same conditions arose. It is however not yet clear when the new logic will be implemented.

AUTOMATED DOWNLINK OF ACAS RA

The second, downlinking of the TCAS Resolution Advisory or RA, is a more complex area, and also discussed in this Issue (see Doris Dehn's article). At first sight it seems logical that if the controller had been aware of the TCAS RA, he would not have given contrary instructions. But in the details of EUROCONTROL's RA downlink study and in the complex and tight timing of real incidents and accidents, it is not always so clear cut. Hence for the RA downlink concept, the jury is still out, awaiting further and more precise evidence. This further evidence is likely to be in two main forms. The first is a better understanding of what incidents and near-incidents actually occur, so that RA downlink (or other approaches) can be formulated on a more evidence-based understanding of the problem. This is not easy since the events of interest are rare and do not occur to order, but a study to do this is being launched by EUROCONTROL. The second form of evidence relates to a risk-based model and results confirming that the benefits of RA downlink outweigh any potential side-effects. There are still some open issues as to what represents the right risk framework and model with which to judge any intervention, but work is in progress.

IMPROVED STANDARDISATION OF STCA LOGIC

The third, namely enhancement and harmonisation of STCA, can help reduce the exposure to TCAS by warning controllers more efficiently in advance of TCAS activation (i.e. STCA and the controller resolve the situation before TCAS triggers). This area has great safety merit in its own right, but is unlikely to reduce exposure sufficiently to remove completely the specific threat of negative interactions between controllers (and STCA) and TCAS (also because, as my colleague Ben Bakker commented to me, there are inevitably some conflict geometries where STCA may not occur before TCAS).

CONTROLLER PRACTICES TO MANAGE SPECIFIC HIGH-RISK SITUATIONS

The fourth is an interesting area in that although it was discussed in the original post-Überlingen High-Level Action Group on ATM Safety (AGAS) forum, it has received comparatively little attention. The approach would entail controllers giving lateral resolutions when aircraft are getting close enough for TCAS to occur (since TCAS only gives vertical dimension instructions). This would necessitate either that controllers have prior criteria for deciding when to give lateral instructions only, or else STCA predicts time to TCAS RA and informs the controller. The controller would also benefit from (down-linked) information about aircraft TCAS serviceability.

There are some potential disadvantages, e.g. lateral resolutions may not be as effective (fast) as vertical ones depending on altitude and speed as well as conflict geometry (see UK CAA SRG CAP 717 - Radar Control Collision Avoidance Concepts, 2006); a pilot who initiates a lateral manoeuvre then gets a TCAS vertical instruction may have significant difficulties complying with the latter; potential impacts on third-party aircraft in busy airways, etc. Yet there is a certain logic that suggests that lateral instructions could avoid the Überlingen-type accident. Such a lateral dimension would also constitute a more clearly coordinated air-ground concept of conflict and collision avoidance. Even if the lateral solution does turn out not to be a good idea, it should be examined seriously with other potential solutions, because it might lead on to better remedies.

AUTOMATE TCAS RESOLUTION EXECUTION

The fifth option, that of automated TCAS, is contentious but an obvious solution for many who have considered that if the human was taken out of the equation in this narrow, time-stressed and unclear situation, then the world might, on balance, be a safer place. Application of such full automation (probably with pilot veto [i.e. return to manual] available) is not without precedent (e.g. automated aircraft landings), but requires a significant safety advantage (e.g. an order of magnitude, or a 'factor of ten' safer than non-automation) to be demonstrated to overcome concerns relating to trust in automation and automation failures. Even if we in ATM are not considering this option, we can be sure at least some of our wider aviation partners are (e.g. Airbus), and we should therefore investigate the likely impacts on ATM.

IMPROVED UNDERSTANDING OF SEPARATION ASSURANCE

The sixth approach attempts to move the problem upstream, and focuses on enhancing controller separation assurance procedures based on a better understanding of how assurance is currently achieved, and the nature of vulnerabilities in such assurance processes, based on the analysis of data from actual ACCs. This work complements studies of actual incidents. Incidents deal with events 'after the fact' - often investigations find it hard to uncover what was happening before, and therefore ignore what constitutes 'normal' separation assurance practices. From a systems perspective, if you want to put something right, it is not enough to look always at what is going wrong - 'normal' behaviour must also be analysed, otherwise assumptions about how controllers control traffic may be incorrect. It is also important to understand the variability in ACC working practices and separation assurance in Europe (including use of safety nets), in case there is not a 'one size fits all' solution. A good example of beginning to understand what is actually happening in separation assurance, albeit from the safety event perspective, is the NATS article in this issue.

IMPROVED CONFLICT DETECTION AND RESOLUTION TOOLS

The seventh approach also attempts to tackle problems 'upstream' and so reduce the number of times STCA and TCAS are called into action. Tools such as Medium-Term Conflict Detection (MTCD) and Tactical Controller Tool (TCT - under development) may offer significant promise for safety more generally. A key question for such tools however, as found in real-time simulations in 2006 at the EUROCONTROL Experimental Centre (EEC), is what is the best timeframe for such tools? Again, it is here that a better understanding of actual tactical control and separation assurance is needed. Often, new tools are aimed at 8-20 minutes' advance prediction, yet the EEC study in 2006 suggested 4-7 minutes was what the controllers actually needed and wanted (TCT can work in this shorter timeframe). Probably both are needed, when considering Planner and Executive (Tactical) controllers. Even if such tools do work most of the time, there will inevitably be encounters and conflicts (e.g. so-called 'pop-ups') that arise in the STCA/TCAS timeframe (MAC-3mins), so again these tools can only be part of a larger integrated solution set, but could add significantly to safety.

SELF SEPARATION LOGIC

The eighth approach is free flight (possibly also including advanced ASAS - Airborne Separation Assurance) wherein the pilots are in control of their own separation. This could prevent controller-TCAS interactions (though there might be ASAS-TCAS ones), but is probably many years away, and so does not help with the immediate threat.

WHERE FROM HERE?

I am clearly proposing that a more integrated approach be adopted - that the different people and groups holding different parts of the elephant work together somehow, with a single aim of developing a Coordinated Safety Defences System, which includes safety nets, their interactions, and barriers further 'upstream' (separation assurance tools and practices). Within EUROCONTROL things are already moving firmly in this direction, but could probably go further. Clearly in this respect we also need constructive engagement with the ANSPs we aim to serve, as is already happening for example through the SPIN (Safety-nets Performance Improvement Network) initiative.

There is also a clear need for a better understanding of separation assurance, as well as loss of separation, so that we can make the right decisions based on the best evidence available.
EUROCONTROL is currently seeking to look deeper into these two sides of the same coin, with ANSP partners. Once such an understanding exists, different 'solutions' and 'solution partnerships' can be evaluated, improved, modified, shelved, or even discarded - to design an optimal system of safety defences.

Returning to my two uncomfortable questions at the start of this article, the answer to the first is likely to remain a 'Yes' for some time, since removing the possibility completely is very difficult to achieve. However, it would be good to have the same affirmative response to the second question.