Eurocae Technical Forum – May 22/23 2003

TOTAL SYSTEM MANAGEMENT: Strategic Engineering Design

Peter Brooker
CAA Professor of Air Traffic Management and Environmental Policy
Cranfield University, UK

p.brooker@cranfield.ac.uk

Introduction

The subtitle is 'Strategic Engineering Design'. The origins of these words are very interesting. 'Strategic' is from the Classical Greek for leading an army. Engineering is from the Latin ingenium word for skill. Design has many meanings: an attractive one is to 'plan and execute artistically'. The discussion here is about the things that need to be done to achieve these very positive words, with engineering used in the widest sense. The main need is for 'system understanding' of potential systems.

Aviation – 'The Golden Age'

It is quite common for people to look back to a past golden age. In aviation, there seemed to be one in the 1920s. There was a tremendous expansion in services and amazing developments in passenger aircraft. People just got in an aircraft whenever they wanted, were flown in comfort to wherever they wanted to go, and arrived on time. You would navigate by railway lines, roads and gasometers, the stars at night: and ATC had not been born. Flying from London to Paris was a joy. But it ended – if it had even really existed.

The first airline mid-air collision was in 1922. It happened in Beauvais about 60 miles north of Paris, at the small town of Thieuloy-Saint-Antoine, near Grandvilliers. A French Farman Goliath and a British de Havilland DH18 were on the Croydon/Le Bourget routeing. The visibility was bad and seven people died. The mid-air collision was reported in Flight magazine, but only at the bottom of page 7 – there were rather a lot of fatal accidents in those days. This was probably the start of serious air traffic management (ATM). It can therefore be argued that ATM has an Anglo-French origin.

The European ATM System

The current European ATM System is the product of 80+ years of ATM development. This is a list of some key current ingredients of the European ATM system:

- Controllers and pilots – people are an integral part of the whole system
- Formal Rules for the control of traffic
- Radio Telephony
- Controlled Airspace – sectors handled by controller teams
- Flight Progress Information – flight plan computing
- Radar – processed Secondary Surveillance Radar (SSR) – displayed aircraft symbols complemented by callsign/height information
- Computer Processing of radar and flight data
- High Quality Aircraft Navigation – VOR/DME to INS through to satellite-based aids
- Conflict Alert (STCA) – the computer processing system can analyse SSR tracks to predict if aircraft might come into close proximity and warn the controller by radar screen messages.
- Traffic alert and Collision Avoidance System TCAS – on board collision avoidance system based on detection of other aircraft in the vicinity carrying SSR transponders

Most of these features are additional safety defences, but some are there to help flights use the capacity of congested runways.

Air traffic controllers are important decision-makers in the present system. They communicate through radiotelephony; they use flight plans agreed with pilots; they monitor highly processed SSR data. These data flows are embedded in 'safety structures', with well-defined controlled airspace and formal rules for control such as the minimum separation permitted between aircraft.
In the last 30 or so years, navigation has developed enormously. The system has moved from point source aids, VOR and DME, to satellite-based aids, eg GPS, which are incredibly accurate. In the UK, there are STCA systems available to warn of aircraft coming into close proximity. Commercial aircraft now carry TCAS.

The present operational concept has evolved over the decades. It is 'overlaid': new technology has been added on to the immediately previous concept, rather than being a clean sheet redesign.

"We have the Technology"

It does not seem much like the 'golden age' that people vaguely believe once existed. So the focus moves towards the desired future ATM system. People are concerned about many ATM questions. "We have the technology" is a quote from the TV series 'The 6 Million Dollar Man' in the 1970s.

But the quote raises the question: 'What bits of potential technology are actually going to be used?' Here is a list of 'worry questions': they are not actually very

helpful. They have to be converted into more positive questions that respond to the need to understand potential future systems – to have 'Total System Management'.

- Many past examples of good technology solutions 'not finding a problem'
- Are the real problems being addressed?
- Do the operational concepts make sense?
- Will anybody pay?
- Is 'The ATM System' understood?
- Should there be an 'Optimal Solution'?
- Is there a 'Theory of ATM'?

These are all 'worry questions'. How are these turned into Strategic Engineering Design principles?

Thinking about ATM: System Assessment Dimensions These are some starting points:

- Real-life goal is not some vague state of perfection.
- Should be attained through specific proposals and criticisms.
- Needs rigorous assessment tools.
- Should be dynamic and adaptive – nobody knows what all the products of technology will be.
- Should recognise that particular elements of the future ATM system will be 'price-driven', ie with utilisation of resources reflecting markets.

These are very much the list of a rational analyst. As usual, they state obvious things – but if one adds enough obvious things together, it starts to narrow down the possibilities quite considerably.

There are many ways of trying to think about the ATM system. The structure here focuses on four system assessment dimensions: Cybernetic Control, Individual Control Workload, Safety Targets, and Total Costs. The definition of Cybernetics is 'the theoretical study of communication and control processes in biological, mechanical, and electronic systems, especially the comparison of these processes in biological and artificial systems'. Figure 1 presents the process as a sequence of questions. The dimensions are distinct but interrelated. For example, new aviation equipment comes into cybernetics – the acquisition, processing and routeing of information; and into workload – the displays, computers tools used in control; and obviously into the costs of investment, operations and maintenance. Only safe systems can be investigated.

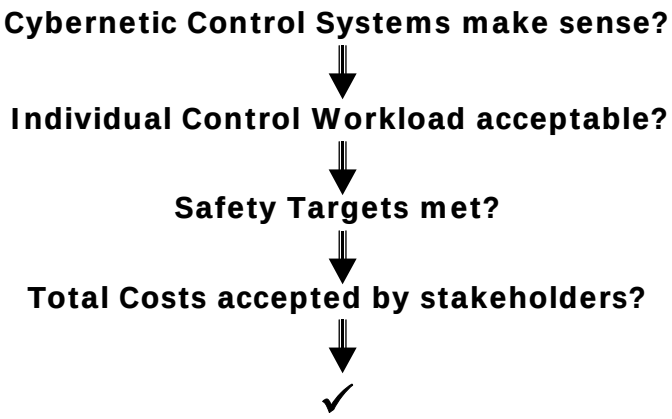

Figure 1. System assessment dimensions.

The comments here about safety and costs are brief. Cybernetic system and control workload aspects are at the centre of attention.

Safety History

Figure 2 shows worldwide fatalities for the people travelling in airlines, not including third parties on the ground. The long-term trend is slowly downward; currently it is at a level of 1500 a year, but that is against a huge increase in traffic over five decades. In the 1960s, a man called Lundgren suggested that there was a feedback loop to public opinion: if crashes or deaths went up a lot in a particular year, then the industry reacted to improve safety levels. Public perception is certainly an important factor. But, to compare, about 3000 people die every year in the UK in road accidents.

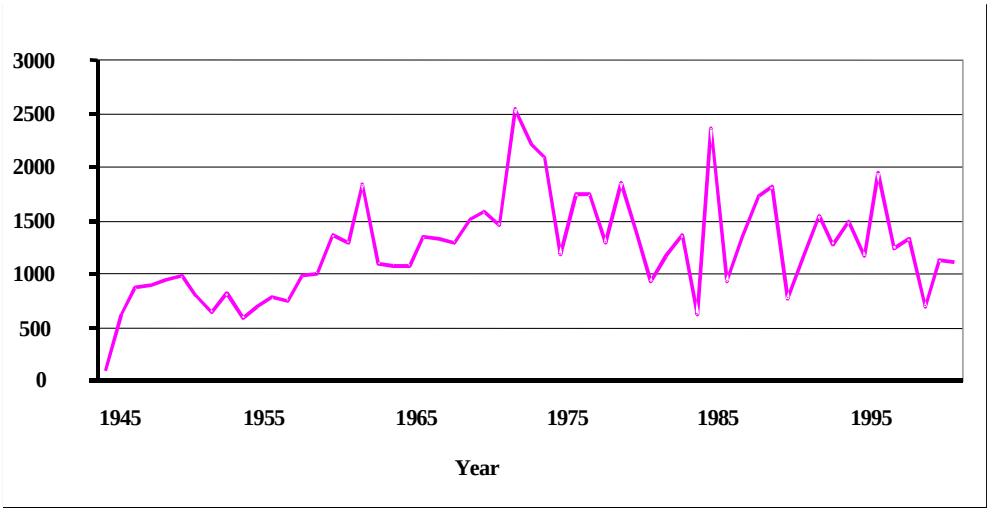

Figure 2. Historical Airline Fatalities (adapted from Airline Safety Network Statistics)

Safety Targets

It is essential to design safe ATM systems. These are two safety targets, from ICAO and the JAA, that are used in assessing new and improved systems:

> ICAO: 1.5×10^{-8} fatal aircraft accidents per flying hour for mid-air collisions – of any type and for all causes – for en route flight in controlled airspace.
>
> JAA: 10^{-9} catastrophic aircraft accidents per flying hour is taken as an 'upper-risk limit' for any single failure condition (AMJ 25.1309).

These are incredibly demanding. Have these design targets reached their limits? Should they be taken as the target for a new system, recognising the importance of improving safety performance over the system's life?

The difficulty with anything new is the work programme to prove safety. The design may well assure the required level of safety, but can it actually be proved? The use of Probabilistic Risk Assessment, which requires the probabilities of safety-critical events to be estimated for 'human components' – Human Reliability Analysis – is extremely difficult. The danger is the creation of 'over-elaborate' models – whose parameters cannot be reliably estimated from the data likely to be obtainable. There needs to be a focus on robust simple models that can be soundly based on available data.

Safety Case

Changes increasingly require the use of a 'system safety case' philosophy. The problem 'owners' have to construct a formal safety case. This system safety case' summary is taken from Richie Profit of the CAA:

- A formal document that provides the evidence, arguments and assumptions to support the claim that the system is safe enough for operational use.
- This should describe the 'system' – equipment, information links, procedures and people – and its functions, identify the hazards, assess the risks, identify the measures in place to control the risks, and define the safety management arrangements for the operational system.
- This provides an assurance that any risks introduced by the changes have been minimised as far as is reasonably practicable.

System Costs and Stakeholders

Cost improvements – reduced delays and operating costs (eg through more fuel-efficient flight paths), increases in airspace capacity – are very valuable, but generally require capital investment. ATM is part of the aviation business and, over the long run, has to obey the same business rules. Some people say that Cost Benefit Analysis (CBA) does not work, but the people who have the money do not agree. At some point in any major change or investment, there will be a 'gate-keeper' who will want good sensible answers to financial questions about

real cash flows. ATM developments will increasingly be assessed by decision-makers on the same sorts of basis as other aviation investments, which implies need for 'macro-level' CBA models.

Future ATM systems can only be those that would be reached because of decisions – real resource decisions to spend or not to spend money in some particular way, not 'plans'. Some visions of the future cannot be realised as a sequence of individually cost-beneficial changes, ie there is not a pathway with a succession of 'marginal' changes. Airlines and ATC operational designers are intelligent and adaptive, so predictions about long-term system gains do not have high accuracy. Net Present Value calculations need to use heavily risk-adjusted discount rates for later years. The drivers for successful ATM investment are large early paybacks, more assurance about quantitative costs and benefits, and reduced implementation risks. Evolutionary analogies are common in ATM R&D, but many proposed R&D solutions do not offer sufficient 'selective advantages' – the cost/benefits are not sufficiently strong in themselves to justify implementation.

Note the trade-offs: in some ATM scenarios the airlines might save money operationally per flight but then pay more money for on-board equipment investment and in ATC charges. Large early financial gains, sufficient to justify major ATM expenditure, would come about by affecting the whole operational cost base – through substantial reductions in controller workload required per aircraft and associated redesigns of airspace sectors.

Cybernetic Control Systems

The letter 'C' in ATC stands for 'Control'. 'Control' can have many meanings and aspects. ATC is of course a special subject, but the theory of control processes has relevant implications and lessons. The standard cybernetic model used in systems management is based on a feedback loop – Figure 3 – with information about the result of a transformation or an action being sent back to the controlling functions. Actions that produce a result in the opposite direction to previous trends are 'negative feedback' – effects that act to stabilise the system. The read-across to ATC is straightforward. A productive way of envisaging control is the two-block arrangement here. It focuses on the different functions and roles embedded in a control system. The controller's workload regulates the controlled system's behaviour. Regulation is used here in a system sense – it has nothing to do with regulatory organisations!

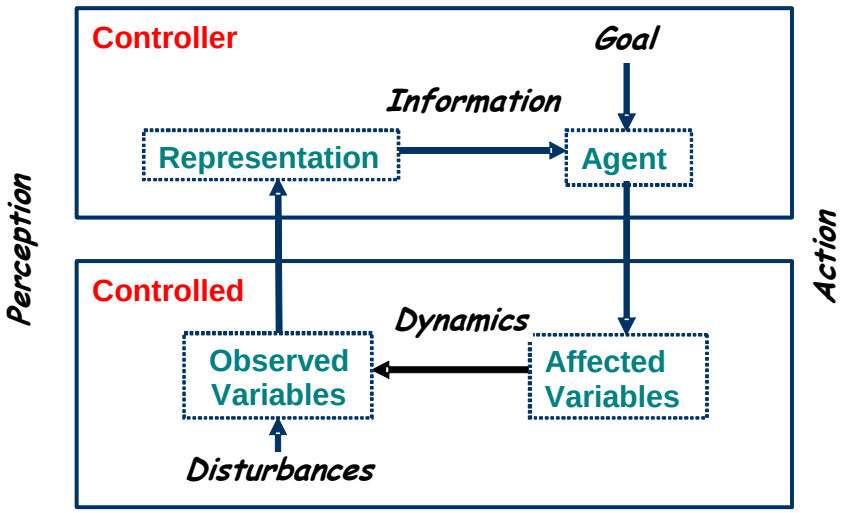

Figure 3. A Cybernetic Control System (adapted from Turchin et al, 1996)

This picture is thought provoking for ATC. It introduces the ideas of perception and representation. For example, in a Free Flight Automated environment, the controller would have to possess information about the intent of aircraft; information presented in ways that the controller could use effectively.

Ashby's 'Law of Requisite Variety'

There is a key law of Cybernetics: Ashby's 'Law of Requisite Variety'.

> *'Given a system with a regulatory process R, intended to maintain a goal state G, but affected by a disturbance D: the goal state can only be maintained if the regulator R has sufficient variety and channel capacity to counter the variety in D.'*

ATC's 'goal state' is safety. 'Channel capacity' is information processing capability. An (ATC) controller needs to have the necessary information to resolve a problem in sufficient time to make a good decision. If aircraft are flying in a complex fashion, then the controller needs to be able to possess and absorb this information.

For a system with some degree of shared separation, there would have to be three blocks with two 'control' loops, one for the (ATC) controller and the other for the pilot, perhaps with the pilot receiving a subset of the controller's information plus limits on the actions that the pilot could initiate. This three-block system is structurally complex, because the ATC controller would decide on how much control to pass down to the pilot block and in extremis would take over that control block.

The regulatory ability of the control loops determines the 'right' number of levels. Increasing the number of levels has negative effects on the system performance, because of data errors and delays. System designers therefore generally try to

minimise the number of loops that necessary to deal with the system variations and perturbations, to satisfy the Law of Requisite Variety. Thus, the question for shared separation is if the two control loops are indeed necessary.

Regulation in the sense used here is a modelling (representing processes in a the real world) activity, in that an ATC controller has to be able to make model predictions, through judgements on flightpaths and speeds, probably with computer aids, of how the present system is going to evolve. Conant and Ashby (1970) observed that *'Every good regulator of a system must be a model of that system'*. This explains why Automation options require information on aircraft intents, rather than today's system, which has aircraft generally on a small number of airway routeings – and hence a small number of crossing points or confliction.

Individual Control Workload

Let us examine in more detail the nature of Control in ATM. At the heart of the present Operational Concept is the controller – or rather the workload that has to be performed in handling aircraft: see Figure 4. . Some attempted definitions of workload:

> "…the amount of effort, both physical and psychological, expended in response to system demands and also in accordance with the operator's internal standard of performance."

This has the advantage of introducing the concepts of taskload (= system demands) and internal standard of performance. Another attempt:

> "…the more difficult the task is, then the more complex the mental operations are, the more mental processing power and capacity is used, and the more human physiological variables (eg heart rate) are affected, and the more the subject 'feels' a higher degree of workload."

So, workload is a multi-dimensional concept encompassing both the difficulty of tasks and the effort – physical and mental – that has to be brought to bear, plus a personal dimension.

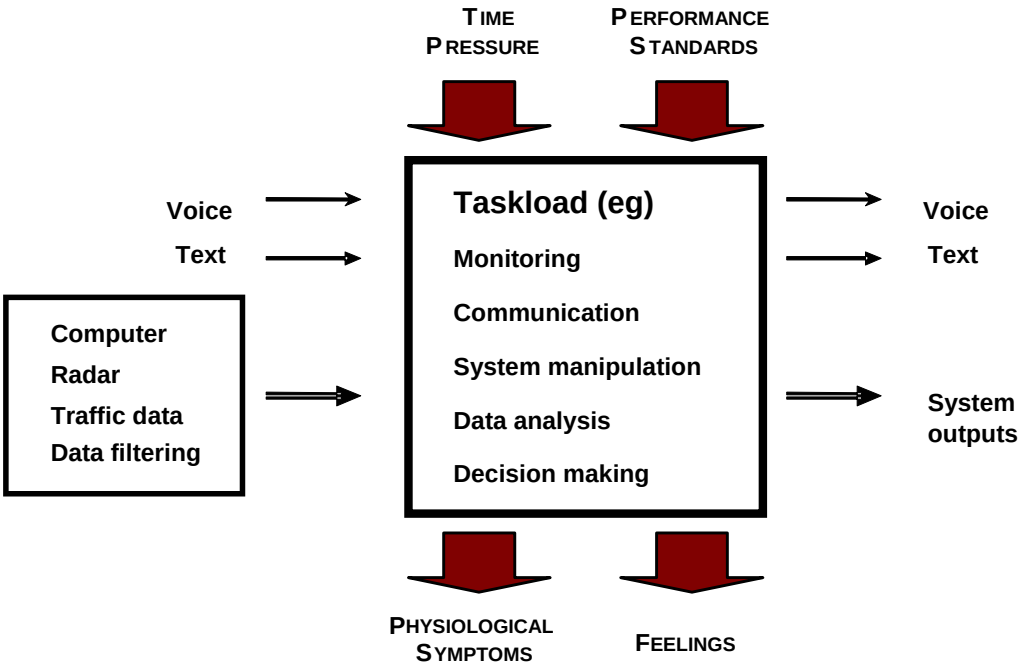

Figure 4. Aspects of Control Workload

How best to start to think about different operational concepts? Figure 5 uses a simple piece of Euclidean geometry. This shows an equilateral triangle, with the sides the same length and the angles between them at 60 degrees. From any point O inside the triangle, three lines are drawn so that they are perpendicular to the triangles' sides. It can be proved that the sum of the lengths – S, T and U – of these lines is constant, no matter where O is located within the triangle. This enables the possible values of an equation:

S + T + U = Constant,

to be explored as points within the triangle.

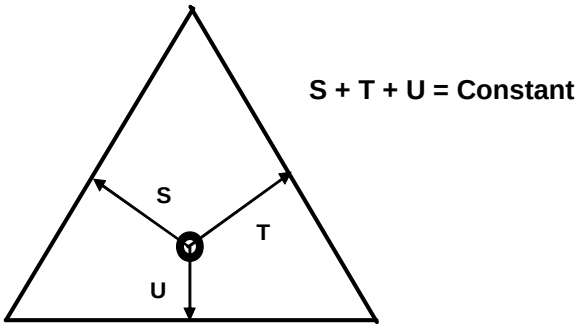

Figure 5. Equilateral triangle: perpendiculars from a point

What are the variables S, T and U? Here are the definitions (Figure 6):

S = Controller workload

T = Pilot control workload

U = Technology/redesign workload equivalent

The second and third of these need some explanation. The second is the control workload component of the pilot's total workload. The third is essentially a residual after pilot and controller workload have been counted. It consists of the 'workload equivalent' of those tasks that have been allocated to 'the computer', in the widest sense. It also includes the equivalent for any eliminated tasks, eg if all control functions were passed to the pilot then there would be no controller/pilot communication tasks.

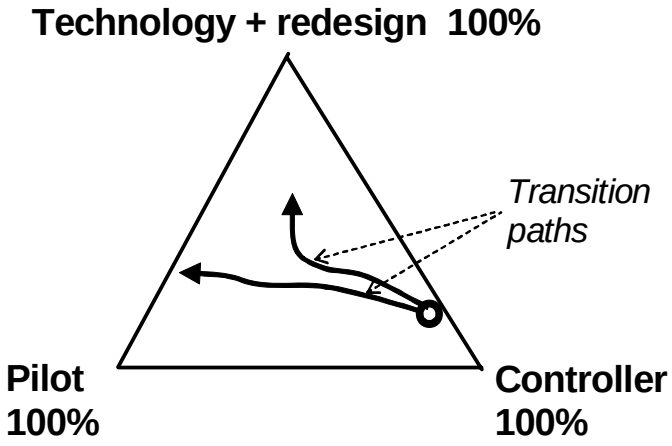

Figure 6. Possible migration paths in the STU triangle

Control workload is considered for a volume of airspace for a constant traffic level. The present system is shown by the O label. This is almost entirely controller workload, but some tasks have had some degree of computer assistance, eg Short Term Conflict Alert systems supplement controller scanning of the screen for conflicts. Two possible migration paths are shown in Figure 6. The lower one moves from the present system to one in which pilots carry out most of the control functions and there is increased automation. The upper one moves to a system in which there is much more 'automation' and in which pilots and controllers share tasks in some way. In the jargon of Airborne Separation Assurance Systems, the first would be termed full delegation and the latter shared responsibility.

Which precise tasks might pass from one actor to another is not the question here. It is assumed that the system represented by each point is the best that can be achieved with such an STU combination, ie it is safe and with minimum full running cost (ie operating cost plus capital investment, equipment maintenance, etc).

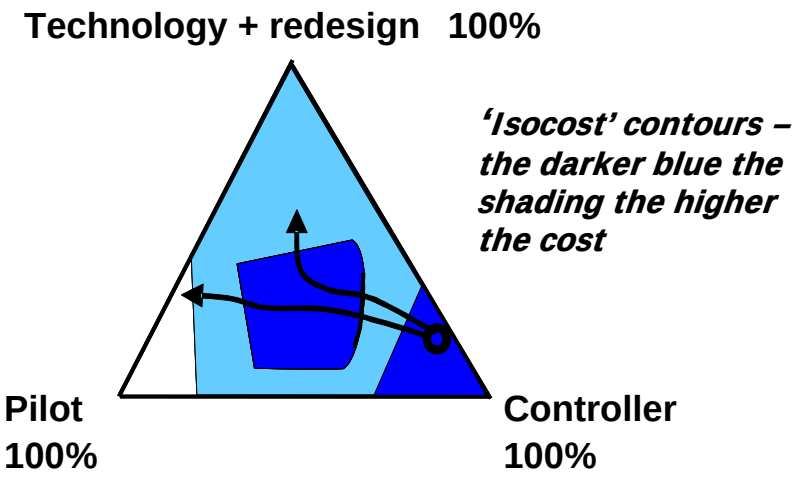

Figure 7. Isocost contours for safe optimised systems

This operational cost dimension can be displayed by creating a three dimensional representation – Figure 7. For present purposes, it is sufficient to add in some (purely illustrative) 'isocost' contours in the triangle: the darker blue the shading the higher the cost. The lower path finishes up with a lower cost endpoint than the upper one. This now shows the difficulty involved in both the migration paths. The first part of the migration looks appealing because there is an improvement in the cost function for comparatively small changes in operational concept. Then both paths move into an extensive higher cost region, so the benefits of marginal changes are not apparent.

The thickened boundary at the entry to the high cost region points out what is effectively a barrier for the next phase of changes – what decision-maker would want to incur higher costs? The answer is a decision-maker who could be convinced by workload research results, predicting accurately that the end of the migration path delivers substantial cost effectiveness improvements. This is the challenge for workload research on future systems. Considerable faith would be needed to act on this advice from a psychologist. When all you can see is an expanse of desert, you have to have a great deal of trust in a guide who says that beyond the desert is the 'promised land'.

Figure 7 is a considerable simplification. There is a time/traffic dimension – increased total workload would correspond to a larger triangle. The nature of the isocost contours changes for higher traffic levels. Some STU combinations, eg continuing with existing control concepts, could become infeasible, so their costs would be very much higher – they would have to include the economic opportunity cost of the flights that could not operate. Moreover, there may well be areas within the triangle that are infeasible in safety terms, because such STU combinations could never achieve the necessary safety targets: these would effectively have infinite cost.**Messages and Next Steps**

To conclude: there are many ways of trying to think about the ATM system. The focus has been on four system assessment dimensions: Cybernetic Control, Individual Control Workload, Safety Targets, and Total Costs. These are some of the key messages: Need for critical assessment against the four dimensions.

- Safety targets may now be indicating the limits for engineering design (but operational performance can be improved post O-date).
- Requires an understanding of cybernetic control – more complex systems do not necessarily improve performance/cost-efficiency. More technology/data flows/players do not guarantee a safer, higher capacity, more cost-efficient system.
- Control workload models are essential to understand the cost structures of the future system. It is 'average workload per aircraft – and its cost' that matters.

Some ideas of next steps:

- Need for stakeholders to take system engineering perspectives – in the largest sense – on how ATM could be organised
- Single European Sky concept needs to be developed addressing the four fundamental dimensions.
- European-level action to involve the key players – Industry (aircraft and ATM), Airlines, ATS providers, Regulators and Standardisation bodies.
- Sponsor research on Cybernetic Control Systems and Individual Control Workload.Opportunities for major European contributions to strategic engineering design.

Acknowledgements

I would like to thank Eurocae for the invitation to present this paper, and John McIntyre for his helpful comments on an earlier draft.

Bibliography

Ashby, W. R. (1956). Introduction to Cybernetics. John Wiley, London.

Aviation Safety Network (2002). Statistics – Fatalities per year http://aviation-safety.net/statistics/year-fig.htm.

Brooker, P. (2002). Future Air Traffic Management – Passing the Key Tests. The Aeronautical Journal, 106(1058), 211-215.

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

Brooker, P. (2003). Control Workload, Airspace Capacity and Future Systems. to appear in 'Human Factors and Aerospace Safety'.

Brooker, P. (2003). Future Air Traffic Management Systems and Financial Decision-Making Constraints. to appear in 'Transportation'.

Brooker, P. (2003). Future Air Traffic Management: Strategy and Control Philosophy. to appear in 'The Aeronautical Journal'.

Brooker, P. (2003). Single Sky and Free Market. to appear in 'Economic Affairs'.

Conant, R. C. and Ashby, W. R. (1970). Every good regulator of a system must be a model of that system. International Journal of Systems Science, 1(2), 89-97

Profit, R. (1998). The Safety Case – A Means of Managing Change Safely. Presentation to IBC Aviation Safety Management Conference 14/15 May 1998, CAA, London.

Turchin, V., Heylighen, F., Joslyn, C., and Bollen, J. Control, Principia Cybernetica Web, vub.ac.be/CONTROL.html, 1996.