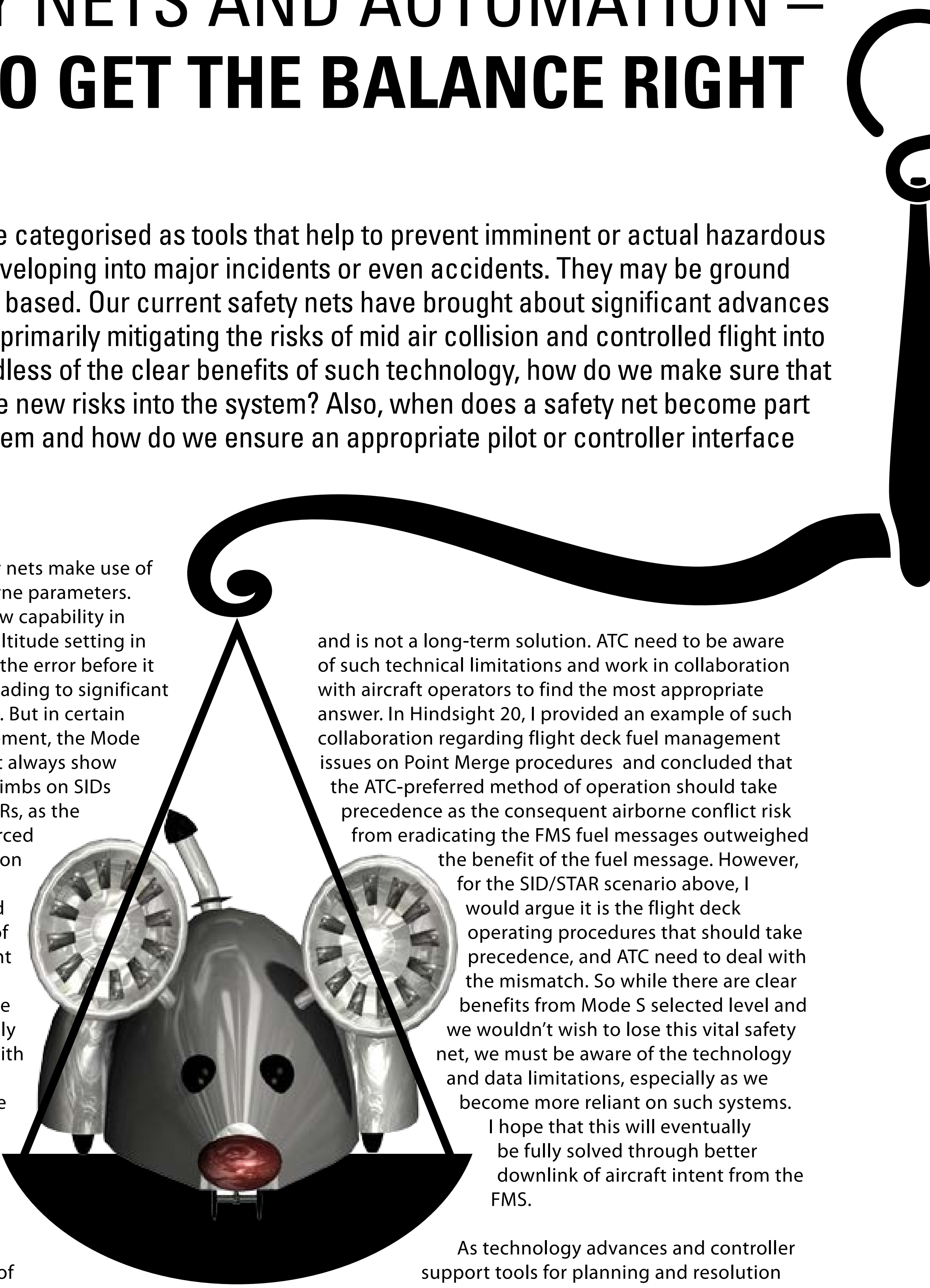
SAFETY NETS AND AUTOMATION – HOW TO GET THE BALANCE RIGHT

by Colin Gill

Safety nets can be categorised as tools that help to prevent imminent or actual hazardous situations from developing into major incidents or even accidents. They may be ground based or airborne based. Our current safety nets have brought about significant advances in aviation safety, primarily mitigating the risks of mid air collision and controlled flight into terrain. But regardless of the clear benefits of such technology, how do we make sure that we don't introduce new risks into the system? Also, when does a safety net become part of the routine system and how do we ensure an appropriate pilot or controller interface with such tools?



A number of ATM safety nets make use of downlink Mode S airborne parameters. This has generated a new capability in ATC to detect errors in altitude setting in the cockpit and correct the error before it becomes a level bust, leading to significant reductions in safety risk. But in certain modes of flight management, the Mode S Selected Level will not always show compliance with step climbs on SIDs or step descents on STARs, as the level information is sourced directly from the selection made on the Mode Control Panel (MCP) and does not take account of other inputs to the Flight Management System (FMS). Unfortunately, the mode of flight most likely to ensure compliance with step climb SID and step descent STAR, where the aircraft automatically follows the vertical profile without the need for pilot intervention, results in the controller only seeing the top altitude of the SID or the bottom altitude of the STAR. We must also ensure that solutions to any mismatch between flight deck and ATC procedures take a 'total system' safety risk viewpoint. For example, encouraging pilots to fly in a mode of flight that is more likely to result in level bust just to satisfy an ATC safety net would be counterproductive and is not a long-term solution. ATC need to be aware of such technical limitations and work in collaboration with aircraft operators to find the most appropriate answer. In Hindsight 20, I provided an example of such collaboration regarding flight deck fuel management issues on Point Merge procedures and concluded that the ATC-preferred method of operation should take precedence as the consequent airborne conflict risk from eradicating the FMS fuel messages outweighed the benefit of the fuel message. However, for the SID/STAR scenario above, I would argue it is the flight deck operating procedures that should take precedence, and ATC need to deal with the mismatch. So while there are clear benefits from Mode S selected level and we wouldn't wish to lose this vital safety net, we must be aware of the technology and data limitations, especially as we become more reliant on such systems. I hope that this will eventually be fully solved through better downlink of aircraft intent from the FMS.

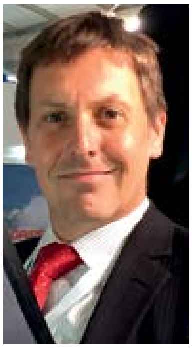
As technology advances and controller support tools for planning and resolution advice develop further, the gap between what is a safety net and what is core standard equipment is becoming blurred. For example, it is technically feasible today to deploy a near fully automated ground control system that integrates Advanced Surface Movement Guidance and Control Systems (ASMGCS) with the aerodrome lighting such that the pilot just follows the green taxiway lights illuminating the path to follow. The system has the ability to adapt routings and to ensure aircraft clearances are safe and do not conflict. Therefore have we eradicated the potential for a lot of human errors and created a safer system with the controller acting primarily in a monitoring role?

Pilots and controllers bring significant safety benefits to the aviation system that are not able to be automated. They detect subtle cues and indications that cannot be picked up by equipment alone. Pilots and controllers are also flexible and adaptive and these attributes are very hard to replicate in technical systems; these benefits are often not adequately articulated and can be inadvertently ignored. Therefore, for the foreseeable future, I believe that there is the need for human integration with technology and it is vital that in designing the next ATM system we maximise the beneficial aspects of pilot and controller involvement and use automation to assist and support their task.

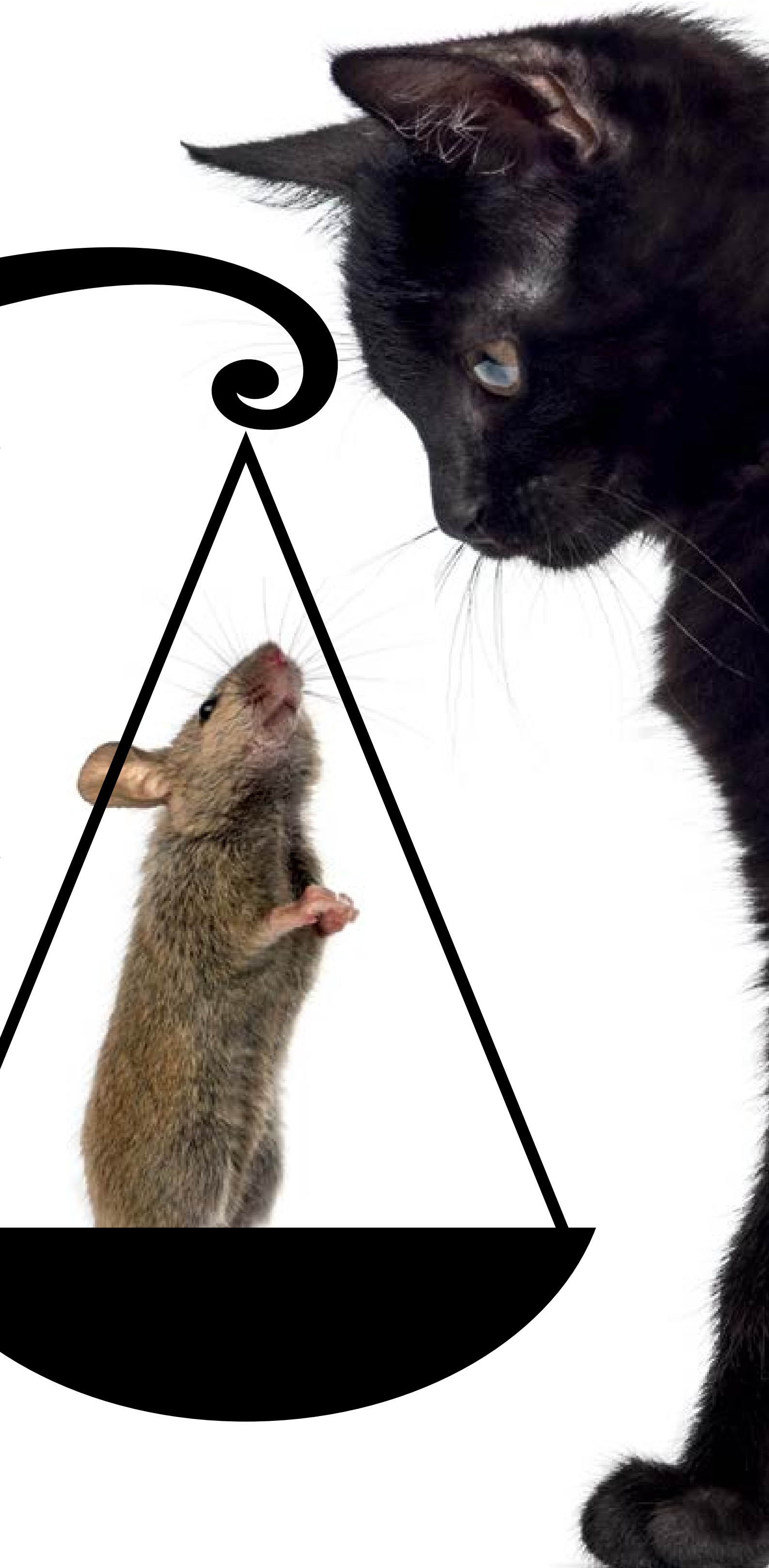
This must also ensure appropriate controller engagement in the task as humans are inherently weak in performing monitoring tasks.

Safety nets have a vital part in our future systems but I believe they will be much closer integrated with the core routine. Using the example of automated ground control, it is likely that airports will require a residual controller capability to deal with unique situations and to resolve unusual situations. A fallback capability is also likely to be needed to ensure resilience in case of technical failure. Therefore, an appropriate level of controller skill needs to be maintained to deliver this capability; it might be more appropriate to lower the level of automation so that the controller interacts with the technical system to provide a degree of hands on control, assisted by the automation. The technical capability of the system could then be used to provide medium term conflict alert whilst still allowing controller resolution. However, ultimately if the system detects a safety critical situation then it could step in and put a stop bar to red or not illuminate a certain taxi path. With such a system, we can see that the controller support tool blends with a safety net and we can monitor and measure the alerts generated so we have an indication of emergent controller behaviour and potential over reliance on the support tool.

COLIN **GILL**



started his aviation career as a military air traffic controller, subsequently specialising in safety management systems. Since 2007 he has worked for the UK CAA in a variety of posts including Head of ATM Policy. He is currently the UK CAA Safety Strategy lead for future systems and equipment.



Technology, automation, and safety nets, have significant benefits to offer in both capacity/efficiency and safety. But if we accept that the controller and pilot still have a role to play in partnership with technology, it is therefore more important than ever that human system interaction and integration is managed appropriately in the design, development, deployment and in operational service. To that end UK CAA is currently working with ANSPs, aircraft operators, staff associations and academia to develop themes and principles for ATM automation. These are intended to guide the development of safety assurance for automated ATM systems and should assist the ANSP in complying with SMS regulatory requirements.
The themes and principles are currently as follows:

1. **SCOPE – Understand the current operation and identify the real need for automation:**

   - Clearly identify and articulate the need, aims and desired benefits of the automation on the system as a whole.
   - Identify the complexities of the operating environment, its boundaries and dependencies, and the strengths and weaknesses of the current ATM system (people, processes, technology). Maximise the strengths and address the weaknesses.
   - Make a conscious decision on the degree and level of automation that takes into account and balances business needs with reliability and residual human capabilities.
   - Identify and consider the organisational and social effects of the proposed change.

2. **HUMAN - Design, develop and deploy automation with human performance in mind:**

   - Involve operators/users/contributors in all stages of design and development, facilitated by systems engineering, human factors, and safety expertise.
   - Ensure that the technical performance and integrity meets the trust needs of the operator/user, taking account of the natural human tendency to over rely on highly reliable automation and be biased by large data sets.
   - Design information presentation to optimise situational awareness and workload.

3. **OBLIGATIONS - Roles, responsibilities, and accountabilities resulting from the introduction of automation need to be bounded and reasonable:**

   - Minimise reliance on the operators/ users as a monitor and ensure human task engagement appropriate to intervention needs.
   - Don't hold users responsible for reasonable decisions based on information/data that is incorrect but credible.
   - Ensure new or transferred accountabilities/ responsibilities/roles are appropriate and unambiguous to the individuals concerned.

4. **INTEGRATION - Automation interfaces and dependences must be robust:**

   - Ensure that new or changed operator/user technical tools work in a coherent and collaborative way with other internal and external systems and technology.
   - Align and ensure compatibility of the air/ground data and procedure interfaces.

5. **RESILIENCE - Plan for technical failures and fallbacks:**

   - Design automation such that failures are obvious and graceful.
   - Identify residual skills, or alternative systems, required to cater for fallback or contingency situations and implement processes to ensure their maintenance.
   - Ensure that fallback procedures place reasonable demands on the residual capability and capacity of operators/users.

6. **TRAINING - Train people to understand not just to operate automation:**

   Operator/user training on the use of automated systems should include:
   - Clarity on the underlying system logic, functions, modes, design assumptions, data fusion.
   - How to evaluate the automation information/ solutions in the operational context that the automation may not be able to recognise.
   - How to adapt cognitive work flows to incorporate the automation information/solutions offered into core role and practices.

7. **TRANSITION - Manage the adaptation to, and normalisation of the automation:**

   - A transition plan for each deployment should address:
     - The social dimension of automation deployment.
     - The effects of transition on human performance.
     - Interim capacity management.
     - Roll back contingencies.
   - For deployment of multiple tools a longer-term roadmap to deployment and incremental deployment should be considered.

8. **EMERGENCE - Monitor and act on emergent properties and behaviours:**

   - In service SMS monitoring processes should be designed to identify and address emergent behaviour of humans using the system inoperation.
   - Technical design performance assumptions and predictions should be routinely reviewed, assessed, validated and updated in service.

We hope to complete our project and publish the findings in early 2016. S