SAFETY NETS: A CONTINUING JOURNEY WITH EN ROUTE SUCCESSES

by Captain Ed Pooley

I thought it might be interesting to start by taking a step back and asking what exactly is a 'safety net'? But having played around with that rather esoteric question I will move on to consider how they work, how much difference they appear to make to safety, what makes a good one and finally whether their increasingly important role may have a downside.

A short answer to my first question might be "something which prevents an undesirable outcome when normal provisions and procedures have failed to do so". But what is 'normal' in this context? Using the word normal in a definition is problematic if the definition of what is normal changes almost continuously as it has for pilots and controllers over recent years. The 'normal' role of the pilot has been transformed by the rapid rise of task automation so that 'normal' is not direct control of the aeroplane but indirect control. This change has been accompanied by a rise in prescriptive working where 'free-style' tactical decision making is a much smaller component of a pilot's 'normal' than it used to be. Concurrently, pilots have also been provided with equipment which can undoubtedly be described as safety nets on any definition. Stall Protection Systems (SPS) have been joined by Enhanced Ground Proximity Warning Systems (EGPWS) as a final defence against CFIT, by Traffic Collision Avoidance Systems (TCAS II) as a final[1] defence against mid air collision, by the Runway Overrun Prevention System (ROPS) as a final defence against runway overrun and by Flight Envelope Protection as a final defence against loss of control. Of course the latter is still very much a work in progress – the pioneering work of Airbus to leverage the possibilities of 'Fly-by-Wire' aeroplanes has, until recently[2], only provided this safety net when the aeroplane is being operated in 'Normal Law' yet the evidence shows that such a safety net would be even more valuable as the level of automation available reduces and especially so if the pilot ends up 'back' in the unfamiliar world of 'Direct Law'. Controllers too have increasingly been provided with access to safety nets which seek to help them prevent ground and airborne collisions. The key feature of all these and all other 'active' safety nets is that their activation thresholds have to be configured either at manufacture or by the user. And of course they then activate without regard to the origin of the identified risk, of which more on both later.

I described the examples of safety nets quoted above as 'active' – they come into effect only when certain criteria are met and the majority have two levels of 'urgency'. We can generically distinguish the possible (an alert) from the probable (a warning) so that complete surprise has been eliminated if a rapid response is subsequently required to a worsening threat after an initial alert has been given. An initial visual display alert can be upgraded to an aural alert or a second more urgent aural alert can be generated. And it should be noted that in the case of aircraft flight decks, safety net activation is usually linked to a master warning system which will initially generate a low-level aural alert even if the safety net itself generates only a visual one.

We might, of course, be tempted to include in a definition of safety nets a passive variant. For example, a Runway End Safety Areas (RESA) or an Engineered Materials Arresting System (EMAS) is certainly not in place to cater for the 'normal' but it is entirely passive – always available but rarely needed. Are features like these, which exist to mitigate the consequences of a situation which has unexpectedly transitioned rapidly from the normal to the abnormal, also safety nets? We could even extend this concept of a passive safety net to proactive safety enhancement activity like bird scaring at aerodromes.

We might also contemplate whether there is such a thing as a boundary between the normal and the point where safety nets 'earn their keep'. And we should perhaps think of the normal as 'the expected' so that routinely-trained abnormal and emergency procedures can be considered part of what is 'normal'. Of course, as noted earlier, whatever the 'normal' condition is, we can be sure that it will often be mobile over time, sometimes rather rapidly.

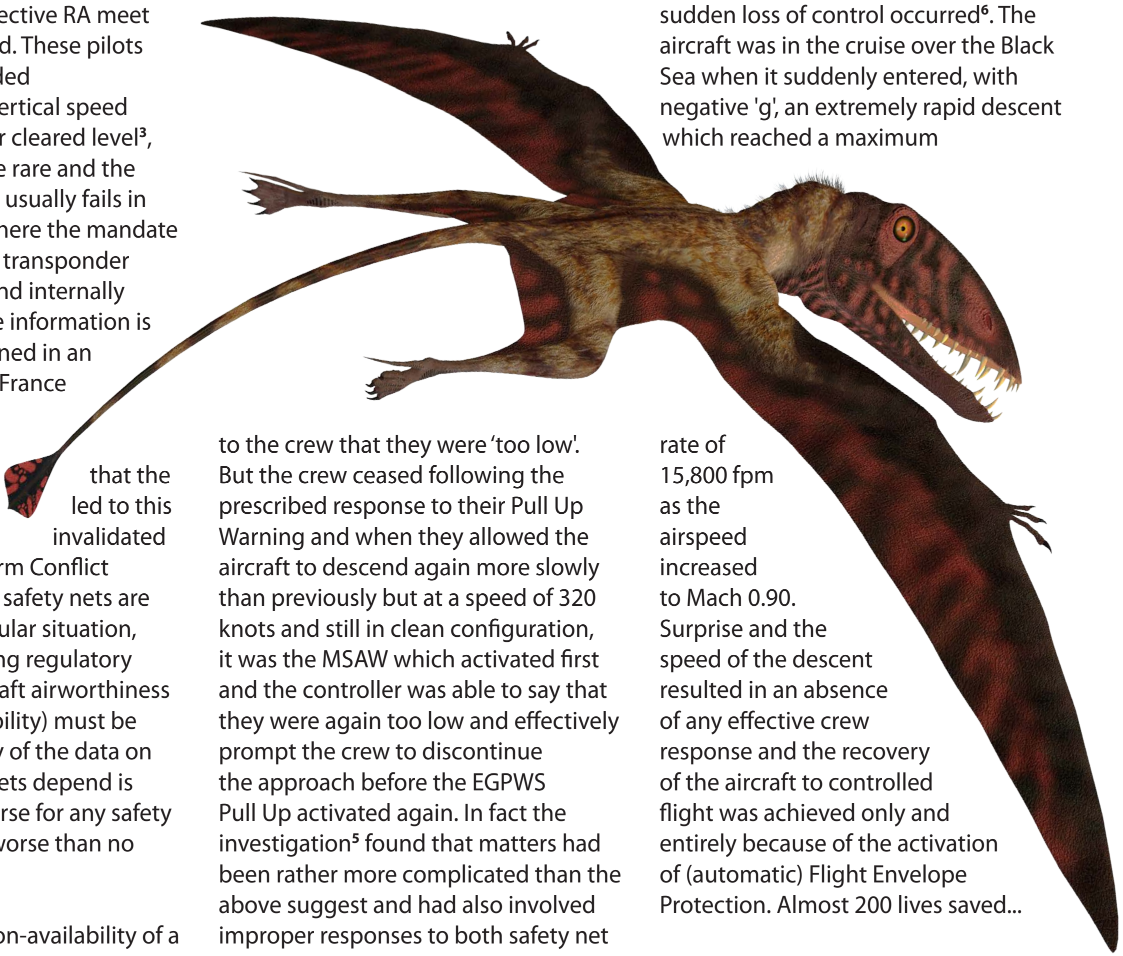
Anyway, leaving the rather esoteric question of definition unanswered, I'll move on, limiting my further remarks to what I have described as 'active' safety nets. We can be sure that the absolutely essential input to any active safety net in a fast-moving environment like aviation, 'instant' and (usually) accurate data, will increasingly be available. After that, timing is everything. Activation of an alert must occur when there is still time to return to 'normal' levels of safety. Back in the days when safety nets were in their infancy, pilots had the Ground Proximity Warning System (GPWS) which depended entirely on radio altimeter inputs – the height of the terrain immediately below the aircraft. Rapidly rising ground on track would – and often did – result in no useful warning being given and a CFIT accident fatal to all on board followed. Fortunately, the vision of Honeywell's Don Bateman leveraged the new GPS capability to bring us EGPWS which pretty well solved the problem of the original GPWS using a terrain/obstacle/airport database – provided it was fed with GPS position.

Nowadays, we can be confident that all current safety nets are technically capable of activating in time to allow a detected loss of safety to be resolved. In the case of factory-configured equipment, we can also be pretty confident that if the user instructions are followed, there actually will be time to respond even if the time allowed doesn't sound generous. For example, TCAS II requires pilots to follow a corrective Resolution Advisory (RA) within 5 seconds and any subsequent

CAPTAIN ED **POOLEY**

is an Air Operations Safety Adviser with over 30 years experience as an airline pilot including significant periods as a Check/Training Captain and as an Accident/Incident Investigator. He was Head of Safety Oversight for a large short haul airline operation for over 10 years where his team was responsible for independent monitoring of all aspects of operational safety.

[1] at least in IMC
[2] The Airbus A350 has now extended Flight Envelope Protection to operations in 'Alternate Law', the next level 'down' from 'Normal Law'



reversal RA within 2.5 seconds. Initially, this took some pilots quite a while to get used to, especially since few full flight simulators were initially fitted with TCAS ll and actual exposure to corrective RAs during line flying was (and for many still is) infrequent. But pilot training in many operators is now more effective and the majority of pilots receiving a corrective RA meet the responses required. These pilots also know that, provided theyavoid excessive vertical speed as they approach their cleared level[3], nuisance TCAS RAs are rare and the alerting afforded only usually fails in controlled airspace where the mandate to carry a functioning transponder supplied with valid (and internally corroborated) altitude information is inadequate, as happened in an airway over southern France in 2010[4].

It is worth noting that the circumstances which led to this near collision also invalidated the available Short Term Conflict Alert (STCA). Clearly if safety nets are to function in a particular situation, then the corresponding regulatory requirements for aircraft airworthiness (and vehicle serviceability) must be such that the integrity of the data on which critical safety nets depend is protected. And of course for any safety net, bad data is a lot worse than no data.

Now given that the non-availability of a single data source in this near collision event had the effect of invalidating two safety nets both aimed at collision prevention, it is perhaps worth taking time to consider if a controller and a pilot safety net that exist provide alerts for the same risk should depend on the same input data. Clearly, if they do, then duplication becomes less useful than it ought to be.

An example which illustrates the advantages of duplicate independently-driven safety nets is a 2012 CFIT risk event. The crew of an A320 approaching Lyons Saint Exupéry at night – a Training Captain overseeing a trainee Captain – lost situational awareness as they were being vectored to establish on an ILS approach and descended far below the ILS glideslope. So far, that when the aircraft reached 930 feet agl in clean configuration and was descending at 230 knots, an EGPWS 'Pull Up' Warning sounded. As the crew reacted, the controller received a Minimum Safe Altitude Warning (MSAW) because the aircraft was 500 feet below 'radar safety altitude' and was able to confirm to the crew that they were 'too low'. But the crew ceased following the prescribed response to their Pull Up Warning and when they allowed the aircraft to descend again more slowly than previously but at a speed of 320 knots and still in clean configuration, it was the MSAW which activated first and the controller was able to say that they were again too low and effectively prompt the crew to discontinue the approach before the EGPWS Pull Up activated again. In fact the investigation[5] found that matters had been rather more complicated than the above suggest and had also involved improper responses to both safety net alerts.

Safety nets are clearly a key addition to the layered/additive/barrier approach to safety portrayed so well by James Reason's analogy with a set of slices of Swiss cheese. But in the majority of these defences, the weakness will be in the human response. Even where a safety net provides clear guidance on how to fix the problem, those able to take this action must still take it and humans are not 100% predictable. So whilst two independently-driven safety nets are clearly better than one, the ultimate individual safety net is always likely to be one in which alerts automatically lead to resolution if this becomes necessary. Here, Flight Envelope Protection on Airbus aircraft has proved its worth more than once. A salutary example is the 2013 incident to a UK Royal Air Force Voyager transport aircraft – a modified version of the Airbus 330 aircraft – which came close to a fatal accident when a sudden loss of control occurred[6]. The aircraft was in the cruise over the Black Sea when it suddenly entered, with negative 'g', an extremely rapid descent which reached a maximum rate of 15,800 fpm as the airspeed increased to Mach 0.90. Surprise and the speed of the descent resulted in an absence of any effective crew response and the recovery of the aircraft to controlled flight was achieved only and entirely because of the activation of (automatic) Flight Envelope Protection. Almost 200 lives saved...

However, a fully automated response to alerts generated by some safety nets may be neither realistic nor necessary. A good example of this is the runway conflict alerting provided by the FAA's Runway Status Lights (RWSL) and Final Approach Runway Occupancy Signal (FAROS) safety nets. Here, the alerts are generated to the pilot or vehicle driver directly and the required response is obvious and simple enough to be actioned manually – stop the aircraft or vehicle or go around respectively. And both affected pilots/drivers and ATC are simultaneously aware of these activations – a key factor.

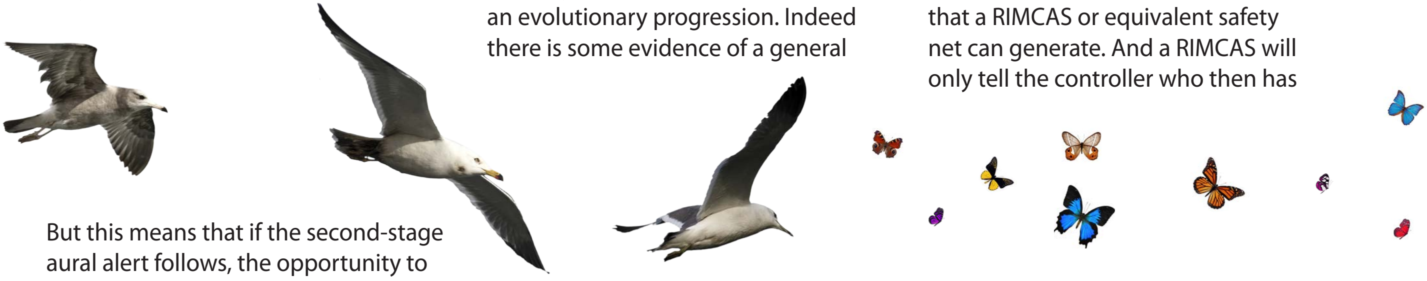
[3] This has, in any event, been a Standard Operating Procedure at many airlines for years now

[4] see http://www.skybrary.aero/index.php/PC12_/A318,_en-route_north_east_of_Toulouse_France,_2010_(LOS_AW_HF)

[5] see: http://www.skybrary.aero/index.php/A320,_vicinity_Lyons_Saint-Exup%C3%A9ry_France,_2012_%28CFIT_HF_AGC%29

[6] see: http://www.skybrary.aero/index.php/A332_MRTT,_en-route,_south_eastern_Black_Sea,_2014_(LOC_HF)

In general, ground based safety nets are user-configured rather than factory configured and there are good reasons for this. A key issue for any safety net is to ensure that 'nuisance' activations are the exception rather than the rule. Once this is allowed to happen, the direct effect is that any activation will be seen firstly as a probable nuisance activation and only later seen to have been a 'real' one. The solution applied to this problem is often to reduce the activation threshold without regard to the time which dealing with a 'real' alert will require. Alternatively, the problem of 'nuisance' alerting may be addressed by setting the initial alert generated (either indirectly or directly) to 'visual only' to reduce the 'irritation' factor.



But this means that if the second-stage aural alert follows, the opportunity to consider potential responses and to be prepared to action them if necessary has been lost. The result is that resolution of the problem is delayed by a finite number of seconds. And it is seconds that count when reacting to a safety net alert.

Unless a 'second-stage' alert comes in the form of a solution as in the case of a TCAS RA rather than just as a 'problem statement', the amount of time required between the receipt of an alert and solving the problem it is associated with must include the time to work out what has to be done to achieve a solution. In order of the total time required ahead of a problem in the order maximum to minimum, it is possible to distinguish the following situations:

- the existence of a problem (but not also a solution) is received by a person who must then determine and communicate corrective action to those who will implement the solution. Most current ATC safety nets are like this.
- a solution to the detected problem is presented directly to a person who can immediately communicate this corrective action to those who can implement it.
- a solution to the detected problem (but not necessarily the nature of the problem) is presented directly to a person who can implement it. Most safety nets installed on aircraft are like this.
- an alert is accompanied by a high-integrity simultaneous automatic solution. Flight Envelope Protection and Autopilot-enabled TCAS RA are like this.

It is possible to regard the above types of safety net output as representing an evolutionary progression. Indeed there is some evidence of a general but somewhat erratic tendency to move through the above sequence. For example, Airbus built upon the success of TCAS II by automating the response to a TCAS RA and received certification approval for this on the A380 as long ago as 2009. However, it remains the case that, bearing in mind the range of outputs from safety nets currently in use, it is still far from clear that they can all guarantee that the time available from the activation of an alert being annunciated aurally will be sufficient to resolve the detected loss of safety.

This is especially true of most of the safety nets available to controllers given that on receipt of an alert, they must often work out what to do about it and communicate it to the pilot(s) involved before the latter can act. The amount of 'thinking time' needed on receipt of an alert (controller) and on receipt of action to take (pilot) will variously depend on individuals, on their training and on the dynamics of the problem or solution presented. The setting of alert thresholds must recognise this, not forgetting also that if either party recognises themselves as the actual or potential cause of the identified problem, then their reaction time may be further increased by the 'distraction' which such knowledge might create. But of course setting the boundary so as to achieve an adequate advance warning also has to address the potential problem of nuisance alerts discussed earlier.

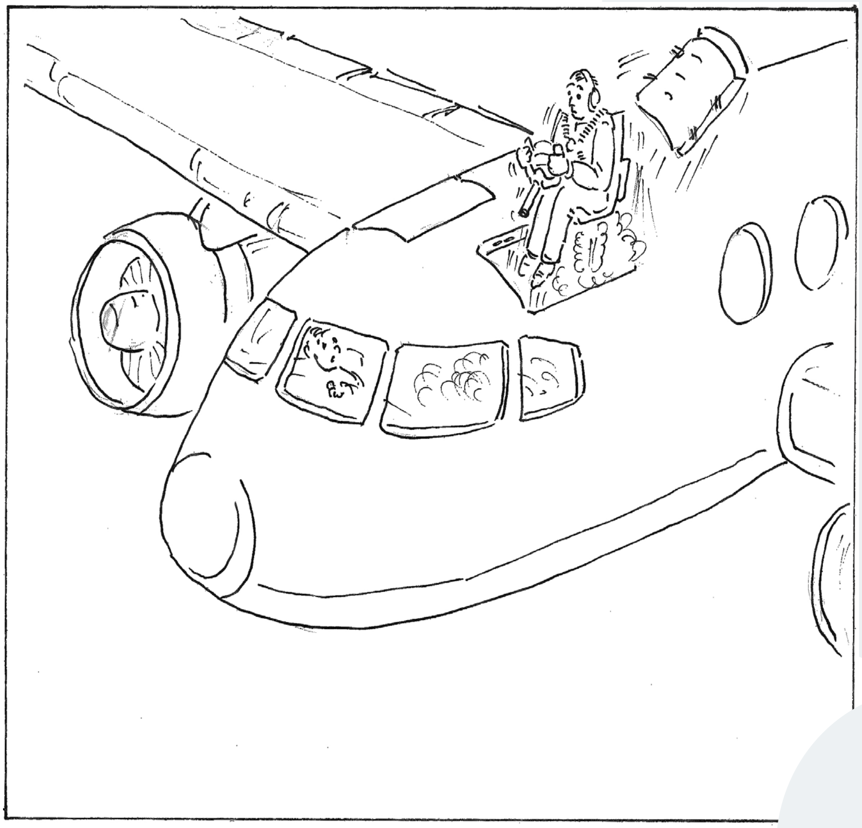
The challenging case of Runway Incursion Monitoring and Conflict Alert Systems (RIMCAS) involves both aspects of safety net set-up. There is not much time to fix an intersecting runway conflict between two departing aircraft. And there is a limit to the available 'advance warning' that a RIMCAS or equivalent safety net can generate. And a RIMCAS will only tell the controller who then has to decide which aircraft to stop and communicate the instruction. The pilot receiving the stop instruction has to react immediately with an emergency procedure. When you realise that a typical short haul jet takes little more than 30 seconds to get airborne, it is obvious that the activation must be as soon as possible to allow effective resolution. Over a period of ten years, Zurich Airport had a significant history of runway intersection conflicts (runways 16 and 28) during which RIMCAS was initially not installed and then ineffectively configured. The investigation of one such event in 2011[7] concluded that with two aircraft departing on intersecting runways (both in accordance with valid clearances) approaching the intersection at respective speeds of 143 knots and 100 knots, RIMCAS activation had (again) been too late to render any useful collision prevention function.

Of course, even when those who can take action are immediately guided as to what they must do, the success of the solution may depend not only on whether this action is taken, but also on whether another 'actor' must also take complimentary action to restore

[7] - see http://www.skybrary.aero/index.php/A320/A320,_Zurich_Switzerland,_2011_(LOS_HF)
[8] - Since this accident, TCAS II version 7.1 has introduced a change to the RA reversal logic which will generate a modified RA to one or both aircraft if the initial resolution does not prevent closure.
[9] - see http://www.skybrary.aero/index.php/T154_/_B752,_en-route,_Uberlingen_Germany,_2002_(LOS_HF)

safety. Most will remember that the mid air collision over Überlingen in 2002 occurred because co-ordinated TCAS RAs generated in both the aircraft involved were followed by only one of them[8]. The investigation of this collision[9] also concluded that although STCA covered the area of conflict, the aural alert activation at 32 seconds before the collision (and after the two aircraft had, unknown to ATC, received TCAS RAs) showed that "in case of a separation infringement with high closing speeds the aural STCA offers little use". However, it must be added that the initial (visual display) STCA Alert was not functioning at the time because the radar system was in 'degraded mode' during night-time maintenance activity.

The lack of such simultaneous awareness by ATC of action about to be taken on the basis of on-aircraft collision avoidance alerts from TCAS II was unresolved until the arrival of Mode S EHS DAP allowed TCAS RA activation to be displayed to ATC. Mention of Mode S EHS DAP allows me to note a new safety net for controllers which has already begun to show real potential for corrective intervention in good time, well before pilots have realised a problem may be heading their way – the provision of the selected altitude DAP to controllers. And in the UK, where the atmospheric pressure can be both very changeable and frequently significantly below 1013 hPa, another DAP, altimeter sub scale setting, has provided the data for a new safety net to counter incorrect action by pilots[10].



Safe Mode activated! Error purging complete!

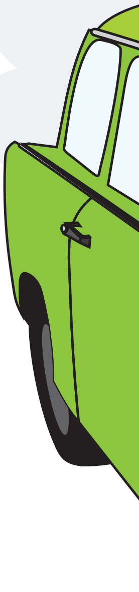
So what can we conclude from this quick look at current 'active' safety nets and their mechanisms? There is of course absolutely no question that all these well-known safety nets have markedly enhanced operational safety and have built upon the increasing extent to which today's wide ranging and reliable automation helps pilots fly their aeroplanes and controllers manage the resulting traffic. Together the combination is one of the main reasons why the fatal accident rate has remained consistently low as the amount of air traffic has continued to grow.

I think that we're beginning to get nearer to what might make for a really good 'active' safety net. It must:

- be fed with data which is both accurate and as near to instantaneous as possible.
- provide the user with immediate awareness if the integrity of input data is no longer assured but is still available and being used,
- generate both a precautionary and, if matters worsen, an 'action' alert
- be configured so that nuisance alerts are not so frequent that the impact of alerts on users is degraded
- prioritise the communication of the action required over a description of the problem.
- whenever possible deliver action alerts directly to the party which can take the action – or cause an automated action to occur.
- be linked to an automated response only when its 'action' alerting is extremely reliable.
- duplicate all actions communicated directly to pilots to ATC without the delay caused if the action has to be advised on the R/T.

I conclude that the developers of new safety nets for both ground and airborne risks and the improvers of existing ones – as well as the users of those systems already available – would do well to familiarise themselves with the way that essentially similar safety nets outside of their immediate area of interest work as a means to understanding how to maximise the effectiveness of those that directly concern them in terms of both design and, where permitted, user set up.

One final thought. In the future, safety nets in some areas may become so reliable that they are seen as integral to the 'new normal'. Now that may not be where we presently see ourselves ending up, but it may not be too far from what eventually happens!



[10] The Barometric Pressure Advisory Tool (BAT) developed by UK NATS, see http://www.skybrary.aero/index.php/Barometric_Pressure_Setting_Advisory_Tool_(BAT)