HindSight 22

The ability or opportunity to understand and judge an event or experience after it has occured

EUROCONTROL

SAFETY NETS

FROM HOMO SAPIENS TO HOMO SOSPITAS
by Professor Sidney Dekker

WHY DISPLAY TCAS RESOLUTION ADVISORIES AT CONTROLLER WORKING POSITIONS? by Tony Licu

FUNCTIONAL SAFETY NETS FROM A RESILIENCE ENGINEERING PERSPECTIVE
by Professor Erik Hollnagel

HAS EGPWS (TAWS) HELPED LOWER THE FLYING RISK FOR COMMERCIAL TRANSPORT AIRCRAFT?
by Don Bateman

Winter 2015

TABLE OF **CONTENTS**

37

78

CONTACT US

The success of this publication depends very much on you. We need to know what you think of HindSight.

Do you find the contents interesting or boring?

Did they make you think about something you hadn't thought of before?

Are you looking forward to the next edition?

Are there some improvements you would like to see in its content or layout?

Please tell us what you think – and even more important, please share your difficult experiences with us!

We hope that you will join us in making this publication a success.

Please send your message – rude or polite – to:
tzvetomir.blajev@eurocontrol.int

Or to the postal address:
Rue de la Fusée, 96
B-1130 Brussels

Messages will not be published in HindSight or communicated to others without your permission.

SKYBRARY DOWNLOAD

EDITORIAL TEAM

Editor in Chief: *Tzvetomir Blajev*
Editorial Adviser: *Captain Ed Pooley*
Graphic Designer: *Frédérique Fyon*

Dear readers,

This edition considers the range of tools, both airborne and on the ground that fall under the heading "safety nets". Such systems do need to be designed and installed carefully, so as to avoid too many alerts or alarms and to ensure that operators do not rely too much on automation. However, with the right design, fine tuning and training, there is no doubt that safety nets make a major contribution to aviation safety, for example by reducing CFIT (controlled flight into terrain) and also mid-air collisions.

Designers and users of these systems face considerable challenges in the coming years – in order to respond to changes in ATM and also to take advantage of the increasing capability of the available systems. We are already seeing an increase of traffic in Europe and EUROCONTROL's latest forecast is for traffic to grow at an average rate of 2.5% p.a. over the next six years. This means that by 2021 we could be seeing over 1.7 million more flights than in 2014.

Those flights will be operating much more in free routes airspace, with a significant increase in the availability of FRA anticipated over the next few years – as regards days of the week, hours of the day and flight levels. Together with more sophisticated trajectory management and flow management techniques (such as 'Target Time Over'), this will have significant implications for the flow of aircraft across Europe.

Other areas where we can expect significant change include the use of RPAS (Remotely Piloted Aircraft Systems) and the use of remote towers. At airports, we can expect to see more sophisticated control of aircraft (for example, through more interactive runway and taxiway lighting) and also of ground vehicles. Runway excursions and incursions remain a serious safety concern and a particular challenge for the aviation industry.

However, in all this change, we must continue to recognise the importance of the human being. People are fallible but also able to enhance safety in ways that systems cannot begin to replicate – just look at the Hudson River incident. Safety nets need to work with humans and to support their decision making.

The articles in this edition cover a wide range of topics and reveal just how much progress is being made in this area and how much informed debate is needed to determine the best way forward. In this respect, the views on the issue of downlinking TCAS Resolution Advisories are particularly interesting. I am sure that you will find this edition both relevant and interesting.

FRANK **BRENNER**

has worked in Air Traffic Management for his entire career. He has been Director General of EUROCONTROL since 1 January 2013.

Since taking up his functions at EUROCONTROL, he has initiated the development of a Vision and Strategy, including the development of Centralised Services as part of the SESAR deployment concentrating on how to support controllers with new technology which increases safety.

Before joining EUROCONTROL, Frank Brenner was General Manager Operations for FABEC, Vice Chairman of EUROCONTROL's Performance Review Commission and a member of the Performance Review Body. Trained as an air traffic controller, he has held a number of posts at DFS including Head of ATM Operations, Director of Operations at the Business Unit for Aeronautical Data Management and Director of DFS's Control Centre Business Unit. operational posts.

Save the Date

SINGAPORE AVIATION SAFETY SEMINARS

SASS

Singapore Aviation Academy

March 14–18, 2016

Maintenance and Engineering Seminar
March 14–15, 2016

Safety Management Information and Sharing Seminar
March 16, 2016

Flight Operations Seminar
March 17–18, 2016

The Singapore Aviation Safety Seminars (SASS) are organized annually by the Flight Safety Foundation and Singapore Aviation Academy. The objective of the multi-day events are to bring together aviation safety professionals from civil aviation authorities, air navigation service providers, airlines, maintenance, repair and overhaul organizations (MROs) and airports to discuss the latest safety challenges and issues. The seminars will include a Maintenance and Engineering Safety Seminar on March 14–15, 2016, a Safety Management Information and Sharing Seminar on March 16 (complimentary) and a Flight Operations Safety Seminar on March 17–18. Participants are invited to attend any one event or combination of events.

For further information please visit:
<flightsafety.org/meeting/singapore-meetings-2016>

SINGAPORE AVIATION ACADEMY

FLIGHT SAFETY FOUNDATION

TZVETOMIR BLAJEV
Editor in Chief of Hindsight

A SENSE OF SAFETY

"All is now set for January. We will have a lot of fun! The forecast is for a good dump of snow. We will have at least 60 cm of fresh powder up there and, I will tell you what, we should ride that powder." The two from the nearby table in the café I was sitting in were in discussion with vivid animation and gestures. "Let me tell you that for advanced riders it pays-off to invest in some winter gear. Some body armour, elbow pads, wrist guards and definitely a new helmet. You should see the new double-shelled advanced piece. Ventilation, anti-penetration, multi-directional impact protection …you name it…going for some freestyle excitement at over 100 km per hour with such protection. At speeds like that it's terrifying stuff and pure adrenaline, I can tell you."

What do you think the chance is to get some paramedics involved in this "winter thrill story"?

What additional risk-taking behaviour is encouraged by the additional feeling of protection provided by the new gear?

Helmets are safety gear, safety nets to protect us in case of an impact. We wear them to protect ourselves but knowing we have such a protection consciously or subconsciously affects the way we act.

This is called 'risk compensation'. This theory suggests that, in general, people adjust their behaviour as a response to their perceived level of risk. They become less vigilant when they feel more protected and more vigilant when they feel less protected. Overall, risk compensation yields lower net benefits from risk protection than might be expected.

I remember the time when I first experienced the stability control technology in my car. As I knew that I had many protection devices in my car, I think my way of driving slowly evolved to take advantage of them. Until one December day, when on the road at a normal speed and taking a slight bend one would hardly notice, I suddenly felt I was losing control. The road surface must have been frozen. The car started 'dancing' left and right and the fences on either side came dangerously close…and yet the car corrected the skidding itself and gave me the chance to decelerate and re-gain normal control.

Could this have happened to me in a car without stability control? Definitely yes, but probably not at this speed! I realised that the stability control may have saved my life which I had endangered by relying on stability control! Job well done by the device one may say, but the point is that the benefits of a safety net may turn out to be less than we expect. Some[1] even controversially argue that the risk compensation effect is so great that it completely offsets the expected benefits. Others[2] have found that the effect exists in many contexts, but generally offsets less than half of the directly positive effect. Unfortunately, these studies are for road safety and we do not know if the mechanisms apply to aviation safety nets as well.

Nevertheless, I would like to caution those who calculate the benefits of safety nets not to omit factoring-in some user opportunism.

Such factoring-in will help us appreciate and maximise the benefits from our safety nets. And the benefits are real - the likelihood of having a mid-air collision over Europe is very, very slim. This level of likelihood

1- "The effects of automobile safety regulation", Sam Petlzman, Journal of Political Economy, 1975, last retrieved from http://www.jstor.org/stable/1830396?&seq=1#page_scan_tab_contents

2- https://doclib.uhasselt.be/dspace/bitstream/1942/4002/1/behavioraladaptation.pdf

is supported by the safety nets we have. Ground-based Short-Term Conflict Alert systems and Airborne Collision Avoidance Systems provide complimentary layers of protection in ours skies. These 'loyal guardians', these last lines of defence, are there to 'cast their safety nets' and capture the most dangerous events. It is not surprising that when safety nets which exist are called-on but are unavailable or not properly used then the result is serious.

Every year, as part of European Network Manager work on prioritising the Top 5 risk, I study with European Air Navigation Service Providers a sample of the most serious safety incidents, using comprehensive barrier models of safety protection called Safety Functions Maps (SAFMAPs). This year's sample included four incidents which breached all the barriers in the mid-air collision SAFMAP and were 'saved' only by providence, by pure chance.

All four of these dangerous incidents had something to do with relevant safety nets. Two of them involved pilots' manoeuvring in the opposite direction to an ACAS RA and two involved a failure of a transponder. It is a real concern to me to know that, after all these years of promotion, awareness and strong emphasis on operating procedures, some TCAS RAs are followed by a manoeuvre in the opposite direction!

Transponder failure is another paradox. Not many will consider a transponder to be as critical as an aeroplane engine. And it is not awarded with the same attention. After all, aeroplanes can fly without a serviceable transponder! Yet, transponders can be as safety critical as engines are. Inoperative transponders can be the single point of failure in the overall aviation structure we have that manages the mid-air collision risk - no surveillance if ATC is using only secondary radar, no STCA and no ACAS. Yes, all these rely on the transponder!

Talking to pilots about this problem I am told that ATC would see the failure promptly and would react accordingly. Talking to Controllers I am advised that for sure pilots would immediately be aware of a transponder failure and switch to the other one or even that there would be an automatic switch from the faulty transponder to the alternate one. None of this is really true!

Transponder failure is an example of an underestimated problem where everyone expects that someone else would take care of it.

Both risk compensation and risk underestimation affect the benefits gained from safety nets by not properly ensuring the reliability of the safety nets as an overall aviation concept involving ground and air, automation and procedures.

As more 'gear' is designed and brought into use, we are becoming more and more 'advanced riders'. We should fix these two issues, otherwise safety nets will actually give us a lower margin of safety than we perceive to be the case.

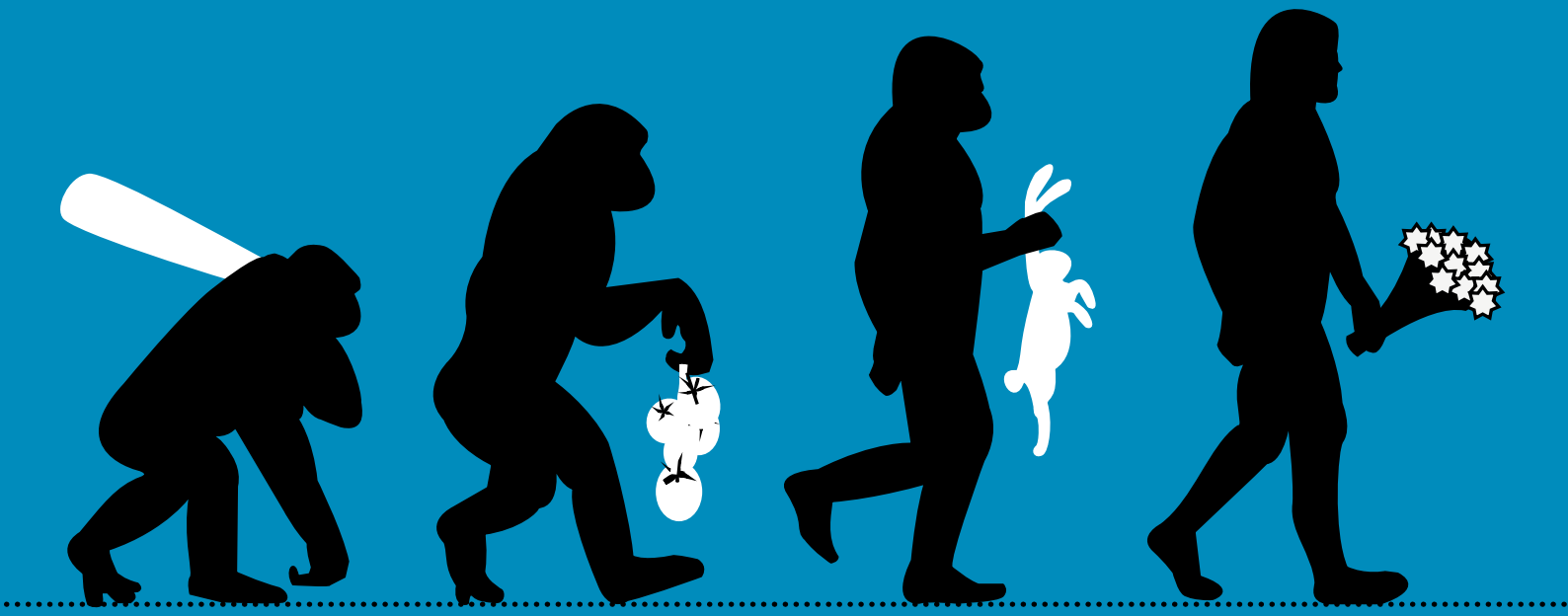
Enjoy reading HindSight!

FROM HOMO SAPIENS TO HOMO SOSPITAS

[Sospitas (Latin): safety, health, welfare]

By Professor Sidney Dekker

I passed by a kindergarten playground recently. On the sandy patch, in the broken-up shade of a Jacaranda tree, a clump of four- to six-year olds was milling about. They were doing what small children do: some digging and playing, some jumping, running, some throwing sand at others – all the time emitting their typical shrieks and cries.



Draped around the sandy patch, there was something disturbing. Kindergarten teachers were keeping guard. But they were not just like the silent sentries that lurk in a corner, quiet and statue-like. Or like my kindergarten teachers a long time ago, who sat in their own little huddle far removed from the kiddie noise, having a gossip and a smoke.

No, these teachers were right at the edge of the action, forming what looked like a riot police cordon. I counted four, five of them: all standing with grand, military authority, legs apart, with their arms outstretched so that their hands reached out toward the next teacher in the cordon. All were intensely focused on the children in front of them, monitoring and inspecting their every move, and stepping in immediately at the slightest sign of trouble or transgression. Believe me that the kid throwing the sand didn't get to do that twice.

This was the kids' human safety net.

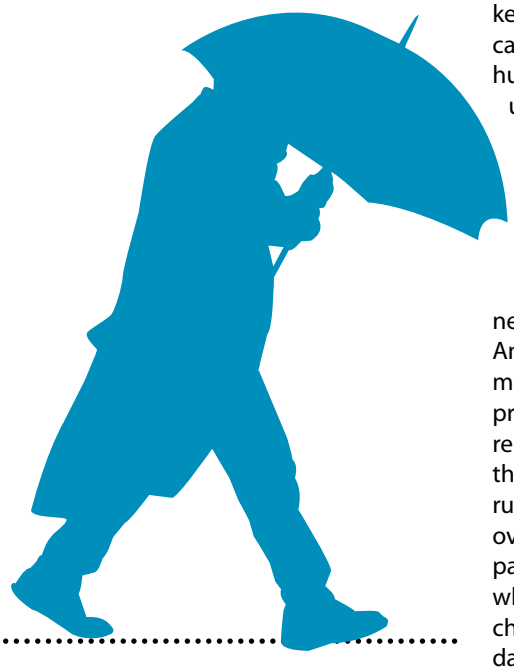
Something in me would hate to be a kid today. I grew up in the Seventies. As many of you might remember, that was an age in which parenting was an exercise in benign neglect, in well-meaning abandonment, in leaving kids alone to be self-sufficient. On days off from school, you might get booted out of the house in the morning, told not to show up until it was time for dinner, and if you didn't show up in time for dinner, then pretty much the only consequence was that you got no dinner. You made plans on the fly. You got in trouble, you got bullied, beaten up, and you figured it out, sometimes with the help of older brothers or bigger friends.

To be sure, it is not that I live in the fantasy and idealised memory of a fictional and glorified past. I am not cheerleading things as they were. Compare our aviation community from the Seventies with what we have today. It is vastly safer now. Work, in

general, has never been as safe as it is today.

But at what cost? What has been the price? And who has often ended up paying that price?

Think of Tom Wolfe's epic book The Right Stuff from 1979 (which many of us today are taught to believe to be exactly the Wrong Stuff when it comes to aviation safety). In it, Wolfe details the bravado, courage and heroism of the first Americans to enter space, tracing them back to their WWII fighter pilot years and their test pilot years in their efforts to break the sound barrier. Chuck Yeager



takes center stage. Of all his 'right stuff' features, his ability to survive, succeed and thrive without 'safety nets' must be the most renowned. His eyesight, for example, was legendary. Chuck was able to accurately pick out enemy aircraft from huge distances, way ahead of his fellow pilots and, indeed, way before the enemy saw him. Imagine Chuck flying around with a safety net with pretty colours and perky alerting sounds that would precisely identify for him what to hit and what not to hit. What would that have done to his pluckiness, his resilience, his skills, his peer status?

Again, I am not cheerleading for the past. I don't think we should go back to relying on the 'right stuff.' If anything, relying on it killed a whole lot of people. And there is more. The immense progress we have made in building safety nets, of all kinds, is testimony to the inventiveness and ingenuity of humanity. Our prowess in programming is too, as is our development of micro-technologies that make calculations and decisions a lot faster than we ourselves can. And our eagerness to develop safety nets says something beautiful about who we are, what we care for, what we want to protect.

But back to the kindergarten. The teachers were eager to construct a safety net. At first sight, they were keen to protect the children in their care, to make sure they didn't get hurt, that they weren't bullied, beaten up, ignored or thrown sand at. The safety net was there for the kids.

Or was it?

Think about it this way. Perhaps the teachers had created the safety net for themselves, for the teachers. And perhaps it was there for their managers. Perhaps what they were protecting was the leadership, the reputation and the bottom line of their kindergarten, and the company running it. Protecting it against the over-eager, lawsuit-ready, over-parenting, hyper-concerned parents whose little precious defenceless children got a face full of sand one day.

We seem to have evolved a stage further: from homo sapiens - the wise, sensible, judicious human - to homo sospitas: a human obsessed with safety, security, health, welfare and the limitation of liability.

I wonder about those children. With a safety net like that, how are they ever going to learn to be wise, sensible, judicious? I wonder what the sources are going to be in their upbringing of resilience, of autonomy, independence, self-determination, self-sufficiency. With safety nets that are really intended to protect other people, but that might well stand in the way of who they, the children, need to become.

We could ask a similar question of our safety nets. Who are they protecting? Whose safety are they really looking out for? Whose liability are they really managing?

I am not talking about the 'alarm problem' or the 'false alarm problem' or the issues of 'data overload' or contradicting indications from different safety nets per se. All of those have been described extensively in the human factors literature, and are intuitively known to every controller in the world. No, what I am talking about is our elephant in the room: the controller who one day might stand accused of not responding or responding 'wrongly' to the indications, clues or exhortations of one of the many safety nets. Never mind the many times that the very same safety net generated indications, clues and indications that could, or should, be ignored in order to get the job done, and get it done safely. Except that one time. The people and the organisation and the regulator that all helped provide the safety net can say: "Look, we gave you everything you needed to do the right thing and still you didn't. You made the wrong decision." This is where we might get a glimpse of who wins and who loses, independent of any commitment to a just culture. This is where, I believe, we might discover who benefits and who might sometimes, paradoxically, suffer from the existence of a safety net.

PROFESSOR SIDNEY **DEKKER**

is Professor and Director of the Key Centre for Ethics, Law, Justice and Governance at Griffith University, Brisbane, Australia. Author of best-selling books on human factors and safety, he has had experience as an airline pilot on the Boeing 737.

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.

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'

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**

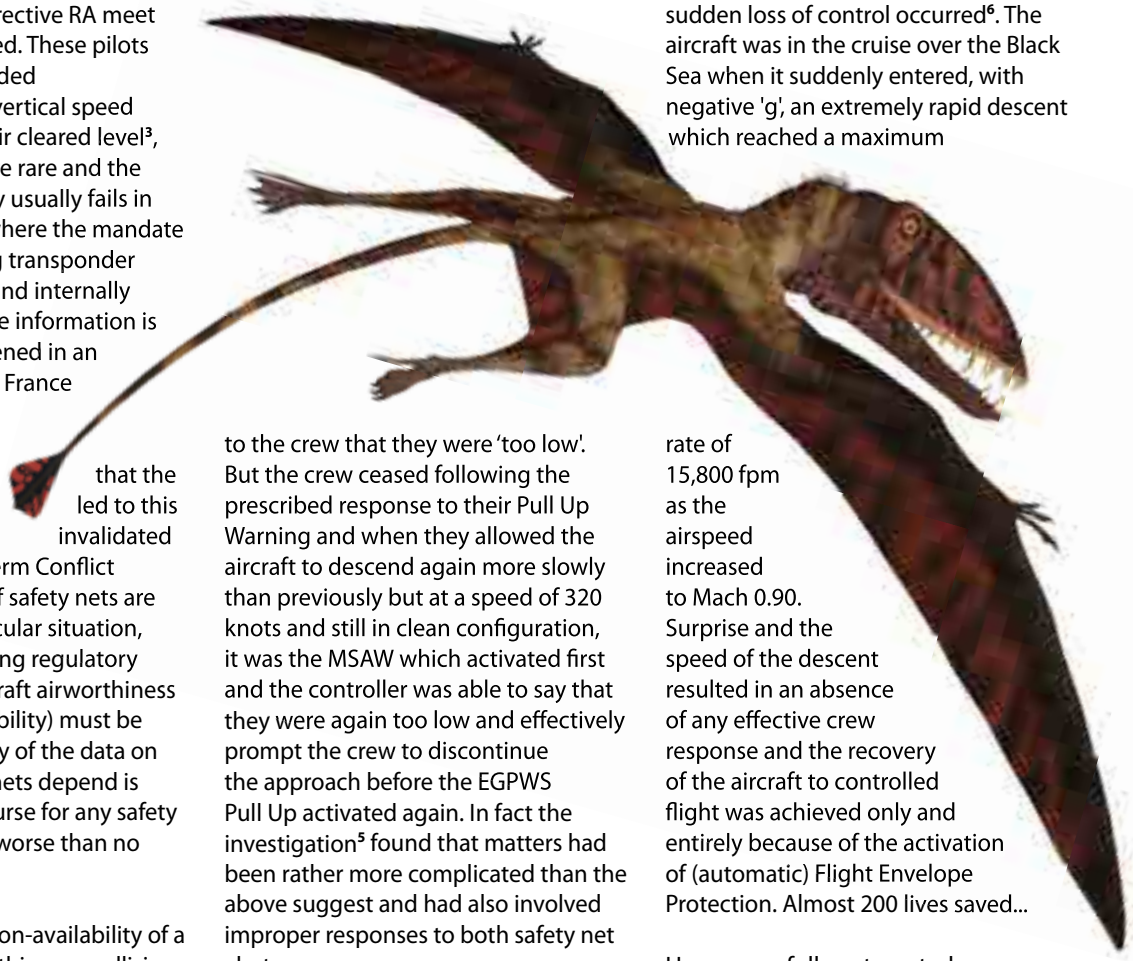
is an Air Operations Safety Adviser with over 30 years experience as an airline pilot including significant periods as a Check/Training Captain and as an Accident/Incident Investigator. He was Head of Safety Oversight for a large short haul airline operation for over 10 years where his team was responsible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

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_(CFIT_HF_AGC)
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.

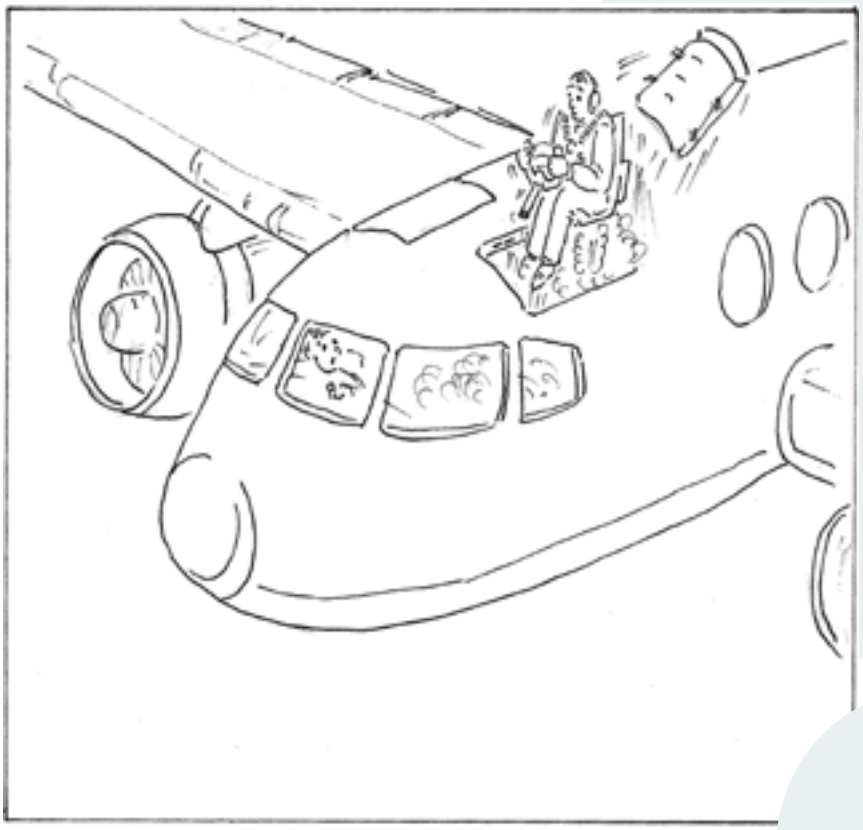
Of course, even when those who can take action are immediately guided as to what they must do, the success of the solution may depend not only on whether this action is taken, but also on whether another 'actor' must also take complimentary action to restore

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].

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.



Safe Mode activated! Error purging complete!

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)

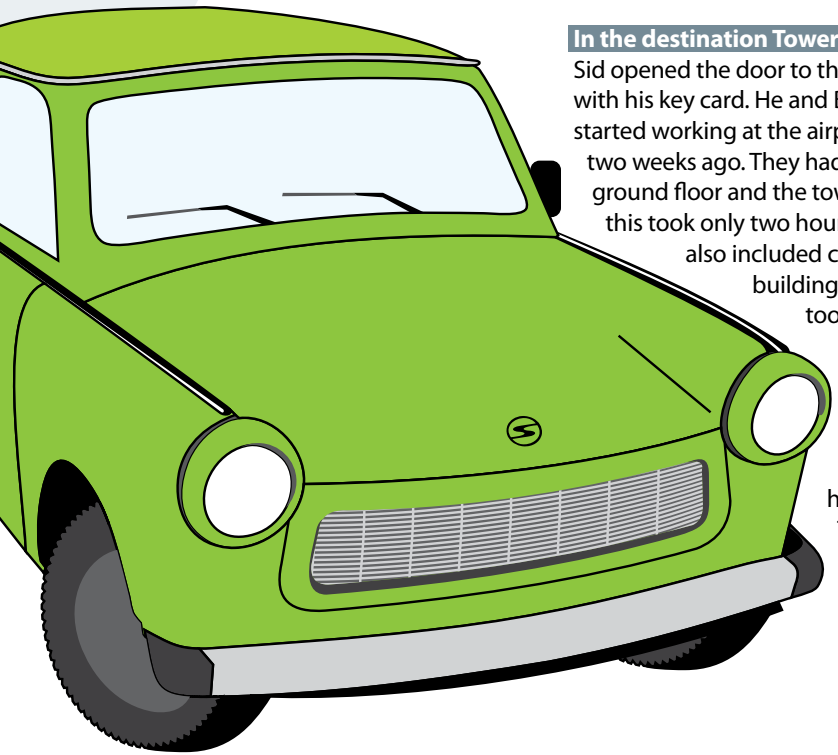
BRENT'S TRABANT 601 by Bengt Collin

Somewhere in Europe

On a sunny day with clear blue skies, he was hit by lightning. It was a strange feeling, it was very bright around him, he didn't hear anything at all and everything appeared in slow motion. Suddenly he could see clearly again and in front of him it was the Trabant 601. Two days later he managed to track down the owner, an old gentlemen dressed in sandals, brown socks, lederhosen, an orange shirt and a green Tyrol hat. The price was 800€, it was a 1989 model. The car was in poor condition, but possible to restore. He bought it.

At the destination airport

"What do you think Sid", Brent asked with a big smile on his face? It took me two years of hard work, but now it's in mint condition. The Trabant 601 was carefully parked on its own at a remote parking lot outside the airport. However they could see it clearly from their position in front of the ATC building. "Looks good from here", Sid replied. "Is the engine powerful"? "Yep" Brent replied, "27 hp at 4200 rpm". "That's impressive" Sid said with irony, but Brent didn't notice.



At the departure airport

The technical crew and the Captain had been delayed and were now arriving together in a green SAAB 95. He was the First Officer, for the moment the only pilot on the flight deck. He had carefully prepared for the flight well ahead of the planned departure time. No problems were expected – the en route and destination airport weather were excellent. Now they would be leaving late, so to save time, he requested start up as the Captain sat down in the left seat. He had already received the departure clearance and the details had been carefully entered into the Flight Management System. The purpose of the flight was to carry out a standard scheduled check of the ILS and VOR at the destination airport. The Captain was somewhat concerned at the late departure – they needed to complete all the checks today, knowing that they were due at another airport the following day.

In the destination Tower

Paul was together with Liza in the Tower. This was the standard procedure, two controllers. The traffic didn't require ATC at all hours but today it was busy. The good weather had inspired many light aircraft pilots to fly. Not that he couldn't cope with it, he preferred it that way instead of long hours with very little to do.

In the destination Tower building

Sid opened the door to the ATC building with his key card. He and Brent had started working at the airport some two weeks ago. They had to clean the ground floor and the tower cabin. As this took only two hours, their tasks also included cleaning other buildings at the airport too. Brent loved his job title 'Household Technician'; it was the best job title he had ever held. They started cleaning downstairs.

BENGT **COLLIN**

formerly worked at EUROCONTROL HQ as a Senior Expert involved in operational ATC safety activities. Bengt has a long background as Tower and Approach controller at Stockholm-Arlanda Airport, Sweden

On the Flight Deck

They began descent towards the destination airport and went through the necessary pre-landing check lists. They were vectored for a standard ILS approach to Runway 22 – they needed to drop off one of the technical crew at the airport prior to starting the checks. The runway was relatively short but still more than enough for the type of aircraft they were flying. The Captain (non flying) was instructed to contact the Tower.

In the destination Tower

"I don't like this stop bar control", Liza moaned. "It's unreliable, sometimes it's on when you believe it's off and vice versa". "I know" Paul replied. "I've talked to the management about it and they say they known about it for years, so why not do something about it then", he continued. "I agree" said Liza, sipping her coffee "and the PAPI both runways went out of service two hours ago, when is it going to be fixed". A vehicle called asking for permission to enter the runway for a runway inspection. ABCDE, called on Paul's frequency. "Hello Tower, ABCDE on your frequency passing four thousand feet, established on the Localiser long final Runway 22". "ABCDE continue approach Runway 22, report passing outer marker"; Paul had VFR traffic crossing final approach at 1500 feet – probably no conflict, he would deal with it later. He expected the VFR traffic to be clear of the zone by the time ABCDE passed the Outer Marker and anyway he expected the latter to reduce speed any second now.

On the Flight Deck

"Will we be on the ground soon?" asked one of the technical crew in a not very friendly way. "We are late for the checks so make it a quick one please". The Captain instructed the First Officer to delay the speed reduction; after all they were both very experienced. No problem at all.

In the destination Tower building

"Is it OK if I leave you down here and start with the cleaning of the tower cabin" Brent asked Sid. "No problem Brent, see you at the entrance door in ten minutes or so" Sid replied. Brent took the stairs up to the tower cabin, opened the door and entered. He was so impressed with all the equipment, not to mention the outside view; it must be fantastic to work as an air traffic controller. Best of all; he could see his Trabant down to the left, near the runway extension.

In the destination Tower

"Now it's happening again, the stop bar is staying on when I switch it off, can you please help me Paul, what am I doing wrong?" Liza's eyes began to darken, not a good sign for people in her vicinity. Paul came over and looked at the HMI in front of Liza. "ABCDE TCAS Climb".

On the Flight Deck

They were 1900 feet and descending when they suddenly received a TCAS Resolution Advisory to climb. The First Officer was surprised that this was possible at such a low altitude. He commenced the climb, the Captain reported the RA to ATC and almost immediately the RA changed to "Adjust Vertical Speed". Could it be another aircraft below, they didn't know but "Clear of Conflict" soon followed. "Sorry about that" the controller's voice on the frequency broke a moment of silence. They continued the approach, still confused over what had happened in what felt like a few seconds.

In the destination Tower

"Can you stay off the runway with the vehicle Liza, I have an inbound rocket". Paul was surprised at the speed of the ABCDE aircraft. "No problem Paul". Liza had calmed down as quickly as she had become upset and suddenly she started laughing.

"I just started thinking about that MITRE guy I fancied dating, he was really cute". Paul was not surprised with her sudden change of focus, that's the way she was, just accept and forget. Paul had returned to his own working position. He turned around and asked the cleaner politely but firmly to stop vacuuming the floor. It disturbed him; "clean the panels to the left of Liza instead, we can fix the rest later".

On the Flight Deck

They passed the Outer Marker for Runway 22. Now those in the back can't complain about being late thought the First Officer. He began slowly reducing the speed from 180 knots. They were on the Localiser but still slightly above the Glideslope.

In the destination Tower

"ABCDE, wind two one zero degrees eleven knots Runway 22 cleared to land ". Paul watched the ABCDE aircraft on final getting close but it was still rather fast. "He must be very late, with that speed" Liza said to him turning away from the cleaner and looking out of the window. "Should I ask him to go around"? Paul's question was not immediately answered. "Wait and see, he must know what he is doing" Liza calmly replied. Following the request from Paul, Brent started cleaning the panel. Wow so many buttons." VOR", wonder what that stands for; Volume on Radio? "GP" - Green Power? Brent's continued to imagine what all the buttons did while cleaning them all carefully. Unintentionally and without noticing, he pressed the "GP" button a little bit too hard. No warning sound occurred indicating the failure of the Glideslope signal – all acoustic alarms had been removed following strong complaints from the controllers. "Alarms which go on and off all the time are a distraction." they had said.

On the Flight Deck

Gear down, landing flap set. Then the glideslope indication disappeared - never mind, focus on the view out of the window instead - but no PAPI either.... The First Officer increased the rate of descent which led to an EGPWS Warning "Whoop Whoop, PULL UP, PULL UP". The synthetic voice disturbed him more than the Warning – he knew what he was doing. It sounded again. I wish someone could stop that voice, why can't you turn down the volume he thought. Then the Warning activated for a third time making him, if that was possible, even more upset. He knew he was a bit high but he had recovered from such a situation successfully before without any problem. At his last session in the simulator he had shown the Instructor exactly how he did this, although he had been surprised when the Instructor had subsequently debriefed his working methods unsympathetically. "Make a go-around and circle to the other runway, we are too fast", the Captain instructed him. The Captain reported their intentions to the Tower Controller.

In the destination Tower

Both Paul and Liza had seen the jet on very short final a lot higher than usual. "ABCDE, making a go-around, can we circle to land on Runway 04?" "ABCDE turn right to join a left hand circuit for Runway 04, wind two two zero degrees one zero knots, Runway 04, cleared to land" Paul replied. He observed the aircraft climb and join the downwind for Runway 04.

On the Flight Deck

"Please turn inbound soon; we haven't all day you know" said the Captain. The First Officer turned onto final for Runway 04 – no PAPI again! Although initially a bit high, he recovered to cross threshold at almost the correct speed and height. Given the maximum tailwind, the adequate length in the other direction had now become hardly enough in the other. He landed the aircraft before the touchdown zone.

In the destination Tower

The smoke they saw coming from the brakes confirmed that the pilot was braking hard. Then, as it looked like there might not be enough runway left to stop on, they saw the aircraft deviating left at a relatively low speed, just missing the localiser aerial - this action was later praised by the airport operator's technical manager - before coming to an abrupt stop after hitting and destroying the only vehicle on the adjacent parking lot, a Trabant 601.

On the Flight Deck

At least we got you here on time, the Captain told the technical crew; he tried to stay positive as long as possible.

CASE STUDY COMMENT 1
DRAGAN MILANOVSKI

The chances of something going wrong with a carefully parked Trabant 601 on its own at a remote parking lot in the vicinity of an airport are extremely low. Nevertheless, this story is a very good illustration of a famous universal "law" – if anything can go wrong, it will!

Postponing things and always expecting the best is not really the best strategy one could adopt, even if it is based on previous positive experience from similar situations. This is even more significant for complex systems, such as aviation, and especially for systems where the role of human factors is of great importance for ensuring safety.

Although the flight was carefully prepared by the First Officer well ahead of time and the weather was excellent, the crew took too many chances by leaving issues to be resolved later by experience or by hoping for a favourable outcome. Their problems started when they opted to delay the speed reduction due to a "production pressure" on board (passenger asking for a quick landing in a non-pleasant way). Knowing that the runway length was just about enough this was already a step in a wrong direction. The complexity increased when the TCAS RA to climb was triggered. It was already obvious at that time that they would have to intercept the glide slope from above if they were to continue. Despite being confused at what had happened, the crew decided to continue approach. It was based on their experience – they'd done it before. However, this time it was going to be different.

The first opportunity to restore safety was missed when they realised the glide slope indication had disappeared and there was no PAPI either. At this point the crew should have recognised that this was not an ordinary situation and should have "taken a step back" by initiating a missed approach. Instead, the First Officer increased the rate of descent. One thing led to another, a safety warning to pull up generated by the Ground Proximity Warning System was triggered. Finally, the Captain realised they were too fast and instructed the First Officer to make a go-around and circle to the opposite runway. The decision was still based on his prime objective to land as soon as possible – he was not going to deal with cross passengers. The First Officer followed the Captain's decision without questioning it although there was almost no time to recover from the previous attempt and stabilise the aircraft let alone land on a short runway with a 10 knot tailwind.

A very similar situation occurred simultaneously in the control tower. One of the controllers had VFR traffic crossing the final and made an assumption that it was probably not a conflict and decided to deal with it later. The assumption was made on previous experience and the expected average performance of the aircraft type in question. This sometimes can be a risky move, aircraft performance of non-routine flights varies more often than for other traffic, and the deviations from the expected average are more significant. In addition, both controllers were dealing with a more or less permanent system degradation (unreliable stop bar controls), and were distracted by the new cleaner vacuuming the floor in the tower. Despite all of this, they both decided to "wait and see".

Just before the accident, the glide path was unintentionally switched

DRAGAN
MILANOVSKI

is an ATC training expert at the EUROCONTROL Institute of Air Navigation Services in Luxembourg. Most of his operational experience comes from Skopje ACC where he worked for a number of years in different operational posts.

off and this was not noticed by the controllers due to a lack of a warning system. It is difficult to say whether the controllers could have prevented the incident at this point had they been aware of this fact, but it is a good example of how safety needs to be seriously considered at all levels in an organisation. The acoustic alarms had been removed following vociferous complaints from the controllers. Indeed, alarms which go on and off all the time are a distraction. Instead of dealing with the underlying reason as to why alarms go on and off all the time, the organisation had decided to switch them off – problem solved.

A RECOMMENDATION:
There are a large number of direct and contributory factors based on which many recommendations could be suggested, but there is one recommendation which will probably be beneficial to all concerned. I cannot say that the actions taken by all those involved are uncommon or unrealistic. On the contrary, it is in our nature to stay positive for as long as possible while dealing with non-standard issues and sometimes improvising in order to find a solution. Most of us are selected for our abilities to do so. However, we need to be aware that regardless of how creative we are, we must ensure that all possible outcomes are "covered" and if necessary that additional safety buffers are embedded in all our actions. We need to be able to recognise a situation where a change of plan has to be executed in order to ensure safety. It is also human nature not to believe a warning from a safety net when we think we have full control of what is going on. However, ignoring it is usually the worst decision we can make. Regular human factors training as part of refresher or continuation training would increase awareness and help everybody involved to perform safer in the future. I hope it will also help Brent understand how it is nobody's fault that his impressive two years' hard work on the Trabant 601 was in vain.

CASE STUDY COMMENT 2
CAPT. ED POOLEY

The type of task-completion pressure which the Captain of an aeroplane conducting an ad hoc flight like this one might be vulnerable to is rather different to that of the Captain of a repetitively-scheduled airline sector...

Meeting whatever nominal schedule which has been planned not infrequently becomes a get-there-as-soon-as-possible task. This story is a classic case of that scenario – and although a low speed collision with a particularly frangible stationary object is not a normal outcome, the rate of 'near misses' generated by this sort of flying is certainly much higher than for airline operations overseen by the same safety regulator.

Probably the main reason is that more tactical decision making is routinely required – especially when running late as in this case. "Can do" makes reputations everywhere if it is accompanied by no (obvious) loss of operational safety. And, perhaps surprisingly, good weather as prevailed here also tends to figure in the history of poor pilot judgement.

So, we start with a rushed departure which provides the context for subsequent judgements. The first decision to delay speed reduction in response to 'pressure' from the passengers sets the scene. Then the unexpected TCAS RA spoils the plan and there is insufficient recognition of its consequences in terms of vectoring to the ILS by both the pilots and the controller. The aircraft establishes on the localiser but continues above the glideslope and without reducing speed yet all but a relatively small number of large transport aeroplane types should expect to be at 160 knots by an Outer Marker position. And anyway, even in the absence of prescribed operator procedures, all aeroplanes should be fully established on an ILS approach by that point. Going down whilst slowing down is not always easy.

Loss of the glideslope signal on a nice day should not in itself worsen the situation. And neither should the absence of the PAPI in those circumstances. Any professional pilot should be able to recognise the normal visual runway perspective, if necessary adjusting for runway width. However – and it would probably have happened anyway – the attempt to regain a normal approach path resulted in a rate of descent which was sufficient to trigger a "hard" EGPWS 'PULL UP' Warning. Although we are not told at what height over terrain the hard warning occurred at, since no prior EGPWS "Sink Rate" Caution is mentioned, this hard warning must have resulted from a pretty sharp pitch down. So even with the runway in sight and maybe without a prescribed Operator procedure to automatically initiate a maximum rate of climb recovery, such a response on the first warning seems likely to have been the obvious

one. That the Captain delayed his intervention until there had been three of them is indicative of "can do" without the essential 'no loss of normal safety standards' caveat.

Then follows the idea that a quick circle to land on the other direction of the runway to take what was almost certainly the maximum permitted tailwind component rather than flying the normal go around straight ahead before joining the visual circuit back to runway 22 was a good one. Rather unusually this plan was also "notified" to ATC as an intention rather than requested, adding to the rush for the First Officer making a relatively unfamiliar manoeuvre. And with increased operational risk given that a 10 knot spot wind speed is always likely to mask variation within non-reportable limits. Even without that risk, there seems to have been no active confirmation that a 10 knot tailwind would still provide the landing distance required.

Intentionally landing before the touchdown zone implies a certain nervousness about the available landing distance too – clearly well founded! At least the pilots steered clear of the localiser aerial – not all of them are yet as frangible as a Trabant and even frangible ones are designed to avoid damage to the aeroplane hitting them not to the installation itself.

We can conclude without much difficulty that most of what happened was about poor piloting and, more specifically, poor Captaincy. But ATC had a secondary role. The controller appears to have vectored the arriving aeroplane into conflict with traffic under their control and then failed to adjust the track miles to compensate for the effect of the RA. And he also accepted the pilot 'go around' intention – although he may have had little choice in the matter if the manoeuvre was already in progress.

ATC management can be criticised for allowing cleaners into an operational environment rather than waiting until it was non operational – or providing enhanced cleaner training for the 'always-open' case. And for the airport operator, perhaps even staff vehicles should not be permitted to park within what sounds like the runway protected area....

A RECOMMENDATION

Difficult to choose – but clearly it is the way the aircraft was operated which was the main cause of the eventual outcome. So I will go for an independent review of the standard operating procedures of the aeroplane operator – or, depending on the relative maturity of the safety regulator responsible for granting the Aircraft Operating Certificate or its equivalent, an allocation of oversight resources and methods which reflects assessed operational risk rather than just the conventional pre-announced inspections at fixed intervals.

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.

CASE STUDY COMMENT 3
SHOTA JANASHIA

Communication is one of the most important things in life and arguably the most important concept in aviation industry...

Sharing the information is crucial at all levels, starting from information exchange between the Captain and the First Officer to communication between different aviation entities. In the aviation industry, a person receiving information is not the only one who benefits from it; often it is helpful to pass on the information you possess so that others can help. Flying the plane or controlling air traffic is a dynamic process and the situation may change drastically in a matter of seconds and thus it is critical to pass the information you receive on to everyone concerned.

On initial training both future pilots and controllers are trained in communication skills. It is clearly explained to them that sharing of the information is the cornerstone of the day-to-day operations in aviation industry. An immense part of an air traffic controller's job is passing relevant information to pilots and pilots, on the other hand, should share pertinent information with controllers. This process creates situational awareness, a condition where both parties have an understanding of the current state and dynamics of a system and are thereby able to anticipate future developments.

And so what do we have in our case?!

The controllers did not advise the pilot that the PAPI was out for both runways. The pilots were not informed about the VFR traffic crossing final approach at 1500 feet. On the other hand, the pilot did not inform the controller that the glideslope indication had disappeared.

All of the above-mentioned contributed to the sad outcome of our case. But things could have been worse. Mid-air collision could have occurred if TCAS did not kick in! The near miss between two aircraft that triggered the TCAS RA could have been easily avoided if the controller had simply passed traffic information to the inbound aircraft. At the same time, because of the TCAS RA, the aircraft had to climb and thus became well above the glideslope. Moments later the glideslope became unavailable, but the pilot did not report it. If he had done, the controller could have switched it back on and the aircraft might have been able to land safely.
To make things worse, the PAPIs were out as well, but that was a surprise for the pilot since the controller did not inform him about it. The First Officer had to increase the rate of descent according to his best judgment which led to an EGPWS warning. At this point the pilots had received two warning signals in quick succession (TCAS RA and EGPWS warning) and that already is a lot of pressure for pilots putting aside the fact that they were behind schedule.

To cut the long story short: lack of communication was a significant contributor in our case.

A RECOMMENDATION
Additional training is needed for both the pilots and the controllers so that they realise the importance of information exchange. The controllers were not aware that the glideslope signal had been switched off and the pilots were not informed about the non-functional PAPIs. The aircraft on final approach and the VFR flight crossing the approach were not aware about each other and that almost caused a mid-air collision! If information had been shared between the controllers and the pilots, Brent's Trabant might have enjoyed another 100,000 km on its odometer!

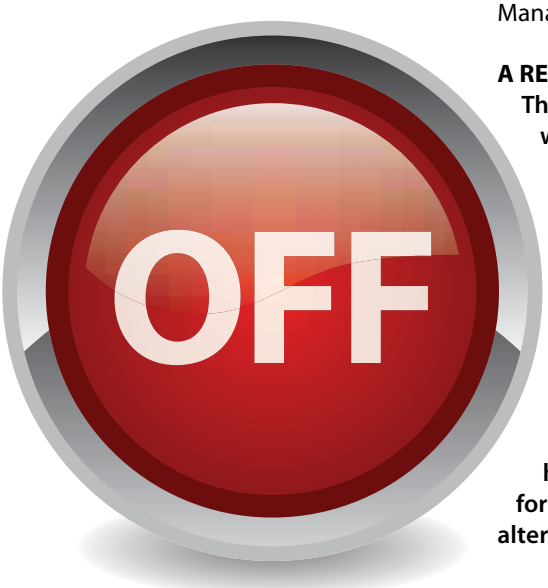
SHOTA
JANASHIA

is currently employed as a safety officer in "Sakaeronavigatsia" Ltd, the Georgian ANSP. He is a licensed air traffic controller and OJTI with 10 years experience in different operational posts.

CASE STUDY COMMENT 4
CAPT. PRADEEP DESHPANDE

The unfortunate end that 'The Trabi' met, apart from being the classic case of 'wrong place at the wrong time', had its origin, like in most accidents, in a series of omissions on the flight deck and elsewhere.

From the time of departure until the incident, the pilots, almost wilfully, manoeuvred themselves through a series of safety nets designed to prevent such an occurrence.
The pressure of not being late at the destination is routine and is something that those who operate these sort of 'on-demand' flights learn to handle very early in their lives. Recommended speeds during descent and approach to an aerodrome are not in every aircraft Operations Manual. They allow for a smooth transition to a stable final approach and also provide ATC with the vital seconds they may need to assess the dynamic environment, to facilitate safe and efficient aircraft and vehicle movement. Importantly, controllers get used to the speed at which things move around them and expect these normal speeds to be flown by arriving and departing aircraft so exceptions should be advised and if necessary approved which they were not.



The confusion caused by an unexpected RA should have alerted the pilots for any other out of the ordinary situation in the aerodrome environment. Therefore, when faced with a sudden ILS glide-slope outage, the pilots should have immediately gone around and advised the outage to the ATC. They instead chose to weave through this safety net as well and persisted with the approach.
The reaction of the pilot flying to the EGPWS warning blaring over the area speakers was to silence it rather than pay heed to the warning. He thought very little of the fact that the warning was indicative of an unstabilised approach

The intervention by the Captain at this stage was timely but inadequate. His unilateral decision to execute a circling approach to the opposite runway without any performance assessment, and that of the pilot flying to follow it without questioning it, points towards insufficient CRM (Crew Resource Management).

A RECOMMENDATION

This must be that the Captain, whether pilot flying or pilot not-flying, must retain the responsibility for the safe conduct of the flight. They must continually assess its conduct and mitigate emerging challenges by virtue of their experience, training, skills and authority as PIC (Pilot In Command). Every approach, no matter how routine, must be briefed for its important aspects. An alternative course of action in the event of inability to execute the planned approach must be a part of the standard operating procedures. Should another approach that has not been planned have to be executed, a proper assessment of the aircraft performance vis-à-vis the prevailing conditions should be mandatory, even at the cost of delaying the landing. Good CRM calls for crew to be of assistance to each other and, where necessary, to convey their apprehensions. Simply issuing instructions or following them without due consideration for safety and one's abilities is indicative of poor CRM and a recipe for an accident.

The impact of such lapses may not always be borne solely by the parties involved but could cause collateral damage to men and material, as was the case with Brent's ill-fated Trabant 601!

CAPTAIN PRADEEP **DESHPANDE**

served as a combat pilot in the military for 22 years. He was a flying instructor and examiner in the military before joining commercial aviation. Commercially he has flown the Airbus A 310 and is currently flying the B 737 800 NG at Air India. He has approximately 9000 hours from 32 years in aviation.

WHY DISPLAY TCAS RESOLUTION ADVISORIES AT CONTROLLER WORKING POSITIONS

by Tony Licu

When TCAS was introduced into operations, the ATC community generally had a negative attitude towards it. *Will it interfere with our work? We are doing an excellent job, so why do we get it over here? Do I want or need to know about it?* Questions like these were on people's minds.
In this article I will look at what has changed since then by examining possible answers to the above questions from different perspectives. Because when anything is commonly agreed about what is known as 'RA downlink', it is the fact that it's a controversial topic!

Because we can do it

It is indeed technically feasible to display RAs at controller working positions. TCAS was designed to downlink sufficient information in real-time and this information was originally intended primarily to enable the monitoring of TCAS performance. Over the years various studies were performed into the practicality and usefulness of displaying RA information to controllers but none of these demonstrated convincing benefits.

Widespread deployment of Mode S radars added a new dimension. Some ATC system manufacturers added RA downlink as a standard feature to their off-the-shelf products. This gave their customers a difficult choice: switch it on or switch it off?

Some ANSPs decided to switch RA downlink on. Some ANSPs decided to switch RA downlink off or are still undecided. EUROCONTROL offered support to early adopters and worked with many of them to ensure that their use of RA downlink was sound and safe.

Perhaps the decisive factor for many early adopters was the legal aspects. Information about RAs is now readily available, so what could be the legal implications of withholding this information from controllers when having such information could make a difference to the outcome of a close encounter? Unfortunately there is no clear answer to this question, it would be for a judge to decide in the court room of the jurisdiction concerned.

Because it increases situational awareness

Pilots are explicitly allowed to deviate from ATC clearances and instructions when in receipt of a TCAS RA. Controllers need to know when this happens because it changes their responsibilities. However, when faced with a RA, pilots are expected the follow the established priority of 'Aviate, Navigate, Communicate' in that order. Consequently, and confirmed by studies, this means that pilot reports of an RA are often delayed.

When asked, some pilots answer that they have never experienced an RA other than in the simulator and in most simulator exercises, pilots are not caught by surprise. Other traffic will often not appear on the Navigation Display, so if an aircraft symbol appears, it is likely to suggest that an RA encounter may well be imminent. Other pilots answer that they have experienced occasional RAs during flight and often have a clear recollection of what happened. In other words and also confirmed in studies, RA events are rare, cause a high workload at an unexpected moment and may be stressful. There are other factors influencing the timing of pilot reports and explanations for frequent errors like using a wrong callsign, omitting the callsign or more generally using wrong phraseology.

RA downlink can alleviate some of these problems with pilot reports. The reason for a deviation from clearance is immediately clear without need for the added pilot workload involved in communication and wrong phraseology is no longer a factor. Traffic information can be given by the controller when considered appropriate, but with 'Clear of Conflict' still pending, opinions on this are divided.

Although ICAO provisions acknowledge the possibility of the display RA information to controllers, there are no other provisions. In other words, the only possibility today is to use RA downlink "For Information Only", which is the usage by all early adopters we know of and they are generally satisfied with that. Of course ICAO provisions could be changed to enable other use. It currently seems unlikely that RA downlink will be globally implemented in the foreseeable future so it cannot (yet) replace the pilot report. But an attractive option, for some at least, RA downlink could be "Same as Pilot Report". There are others who say "Don't Even Think about It" in response to the idea of RA downlink because it could encourage a controller to intervene during an event in which they must hold back.

Because it could prevent accidents

It is now 13 years ago a Tupolev Tu-154 and a Boeing 757 were on crossing tracks at the same flight level near Überlingen (Lake Constance) in Southern Germany. The Tu-154 crew followed their ATC instruction to descend and continued to do so even after they had received a TCAS 'Climb' RA. The 757 crew also descended their aeroplane but did so in compliance with the TCAS RA they had received. The two aircraft collided and all on board perished.

In simple terms TCAS works as follows. It tracks nearby aircraft and estimates horizontal miss distances, vertical miss distances and the times when these will occur. If these fall below defined thresholds, TCAS assumes that a collision may occur with what is now a threat aircraft. From this moment on the TCAS collision avoidance logic determines every second what is now the best vertical escape manoeuvre, based on the estimated vertical miss distance. If the other aircraft is also TCAS equipped, a coordination process between the two TCAS systems ensures that the generated RAs are complementary. If necessary, a vertical sense reversal can occur or the target vertical rate can change.

TONY **LICU**

is Head of the Safety Unit within the Network Manager Directorate of EUROCONTROL.
He leads the deployment of safety management and human factors programmes of EUROCONTROL.
He has extensive ATC operational and engineering background (Masters Degree in avionics).

In the Überlingen collision, no TCAS vertical sense reversal occurred because of a flaw in the logic. During the encounter the estimated vertical miss distance remained smaller than 100 feet, which prevented a reversal. This issue was already known but making and approving changes to complex avionic equipment is time consuming. Only very recently the deployment of TCAS version 7.1, which amongst other things fixes this flaw, was completed in Europe and it will still take some time until this is the case worldwide.

As in all accidents there are many factors that played a role. TCAS is part of a socio-technical system in which roles and responsibilities are not always clear-cut and procedures are sometimes ambiguous. It is beyond the scope of this article to address all aspects, but the Überlingen accident investigation report did recommend further development of RA downlink, which brings us back on topic.

It is not surprising that controllers – and sometimes pilots - have strong opinions about RA downlink. Their professional associations, IFATCA and IFALPA, have formulated positions but my reading of these opinions is that neither is opposed to RA downlink provided that roles and responsibilities are clear.

In the case of "for information only" use of RA downlink, the fear is that in the case of a collision, the mere fact of having RA information could be used against ATC. Ironically, as mentioned earlier, not having RA information could also be used against ATC. In both cases, individuals working in different parts of an ATC organisation involved might, in some countries, find themselves held responsible and open to prosecution, which further complicates the issue.

The "Same as Pilot Report" principle gets much support. However, an argument which has been used against it is that a crew could have overriding safety reasons for not following an RA and expect ATC to continue to provide separation. In any case ICAO provisions would have to be changed to enable use of this principle and that is a time-consuming process with an unpredictable outcome.

The main argument against "Don't Even Think about It", the possible consequences of withholding readily available information, has already been made.

Because we agree to do it

The ATC attitude towards TCAS is now more positive than it was 25 years ago. For controllers and pilots alike, to err is human. TCAS II has made a significant contribution to safety in collision-risk situations and the seeds of Just Culture are bringing results in many organisations by alleviating the fear of unjustified discipline for "honest mistakes".

Early adopters report that RA downlink is not a game-changer. Controllers don't particularly feel that they need it but almost unanimously wouldn't like it removed from their screens once they've experienced it. In an experimental validation environment, they reported that RA downlink information was welcome in many situations and not disturbing in the remaining ones. More generally, there is both practical experience and scientific evidence that RA downlink increases situational awareness.

Will the aviation community ever reach agreement on the topic? Probably not any time soon. But I have observed during the years after Überlingen that the debate has gradually changed from emotional to rational, and rational debates usually lead to sound decisions. One decision has already been made – the technical aspects of RA downlink will be improved in ACAS X. But for now, we all agree to disagree about the use of this capability!

HAS EGPWS (TAWS) HELPED LOWER THE FLYING RISK FOR COMMERCIAL TRANSPORT AIRCRAFT?*

by Don Bateman

A review of relevant incidents for the last three years, as well as the many prior years from flight history recovered from EGPWS computers, indicates that most pilots make recoveries from EGPWS alerts and warnings...

* Answer: The evidence indicates that EGPWS has greatly helped improve flight safety.

Western-built jet transport hull losses have progressively dropped to all time low since the introduction of EGPWS 18 years ago – see Figure 1 which shows the hull loss risk has been reduced by about 2-1/2 times over the last 20 years!

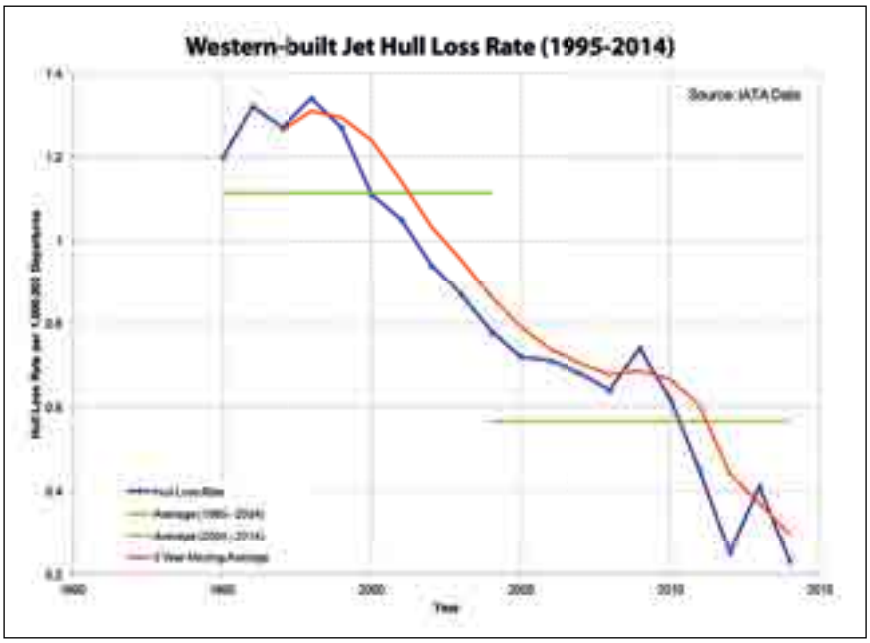


Figure 1 - The declining hull loss rate (IATA Safety Reports 1997-2015)

1. Many examples of positive outcomes have occurred during the years after EGPWS began to be installed in the year 1997. EGPWS is not a panacea for stopping CFIT accidents but it can help interrupt a flight path which is likely to lead to an accident. EGPWS can help provide a "wake up" advisory or a warning.

2. Timely EGPWS activation seems to have helped alert the pilot for flight paths likely to end short of the runway. See Figure 2 which shows that the many EGPWS alerts which occur for Non Precision or Visual Approaches are mostly near Minimum Descent Altitude. Most are unreported when so near to the runway and an EGPWS aural alert seems to result in a very quick recovery response from most pilots.

3. The several software enhancements made starting in 2003 began with a recommendation to use a GPS position feed direct to the EGPWS. IATA recommendations were then made every year to upgrade both the terrain, runway and obstacle databases and software and to support the use of GPS position input. The use of GPS has also helped make EGPWS independent of barometric errors.

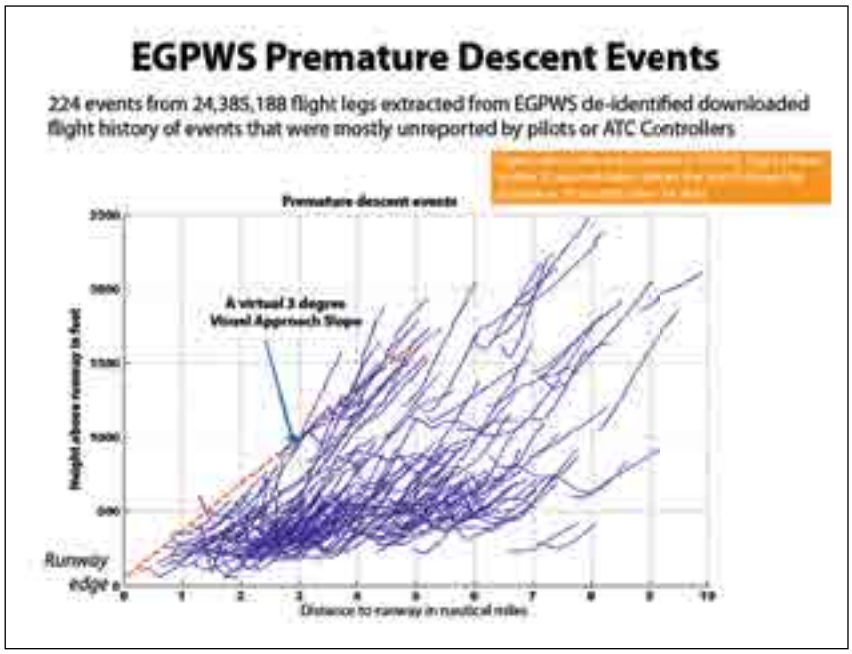


Figure 2 The association of EGWS activations with premature descent [reproduced from Yasuo Ishihara "Continuing trend of landing short/premature descent incidents - ways to reduce risk" presented at the FSF IASS in Abu Dhabi UAE in 2014]

Some official investigation reports of incidents to aircraft fitted with EGPWS during the last three years

To help reduce the risk of Controlled Flight into Terrain (CFIT), EGPWS began to be fitted to aircraft in 1997 (CFIT). 18 years later, a combined total of more than 55,000 Commercial Jet, Turbo-Prop, Business, and Military Transport aircraft are fitted with EGPWS. ICAO Standards require a Class 'A'[1] TAWS should be installed in all turbine-engined aircraft engaged in commercial air transport with an MTOM> 5700kg or more than 9 passenger seats and this requirement also applies to General Aviation aircraft in the same category first registered after 2010.

However, many pilots still hesitate to report a CFIT-risk incident unless a Controller or a passenger or the pilot's airline reports or complains of the incident even though many such incidents are reported in accordance with regulatory requirements.

Honeywell engineers often help airlines investigate some incidents.

1- An important difference between a Class A and Class B TAWS is the requirement for a terrain mapping facility and more effective terrain risk detection and annunciation in the former.

This work is always considered Confidential to the Airline and will not be shared with others. Honeywell will also assist an official accident/incident investigation if requested and if Honeywell equipment is involved.
Here are a few CFIT risk events from the last three years for which Official Reports on independent investigations have been published:

1. On May 15, 2013, the pilots of an ATR 72 on approach to Moranbah, Australia were trying to avoid cloud while descending visually when, the aircraft inadvertently entered into a high rate of descent near the ground which generated multiple EGPWS warnings. A safe recovery was made with no injuries[2].

2. On December 15, 2014 the crew of a SAAB 2000 near Sumburgh, UK lost control of the aircraft after failing to recognise that the autopilot was still engaged after a lightning strike but recovered from a high rate of descent towards the sea surface after EGPWS warnings occurred.[3]

3. On March 31, 2014 the crew of an A320 making an approach to runway 14 at Coolangata, Australia incorrectly set their altimeters during a visual reference approach and continued in VMC until an EGPWS Alert prompted a go around from 159 feet agl.[4]

4. On March 8, 2013 an A330-200 descended to within 600 feet of the terrain at 9 nm from the runway and off the extended centreline of runway 16 at Melbourne, Australia during a visual reference approach. EGPWS Terrain alerts were followed almost immediately by a Pull Up Warning and this was actioned.[5]

5. On April 11, 2012 an A320 descended to 950 feet agl at 11 nm from the runway during a night ILS approach to runway 36 at Lyons Saint- Exupéry Airport, France with no external visual references. An EGPWS Pull Up Warning occurred and eventually, the approach was discontinued.[6]

6. On March 24, 2012 an A-319 descended at high speed towards runway 19 at Tunis in VMC from above the ILS glideslope and after capturing it less than 3 nm from the runway at 220 knots, EGPWS Pull Up and Too Low Terrain Warnings prompted the crew to get clearance for and carry out a 400 feet agl orbit on short final.[7]

DON
BATEMAN

is a Corporate Fellow and the Chief Engineer-Technologist at Honeywell where he heads a small team of scientists and engineers. Don and his colleagues have developed many aircraft instruments and safety devices for aircraft and he has been recognised with many awards including, in 2011, the U.S. Presidential Medal for Technology and Innovation which he received from President Obama. He holds a Private Pilot Licence with Instrument Rating.

Loading CityMaps in EGPWS is a great idea! Now I think it's safe to take a shortcut on approach.....

2- see: http://www.skybrary.aero/index.php/AT76,_vicinity_Moranbah_Queensland_Australia,_2013_(CFIT_HF)
3- see: http://www.skybrary.aero/index.php/SB20,_vicinity_Sumburgh,_UK_2014_(LOC_HF_WX)
4- see: http://www.atsb.gov.au/media/4905339/ao-2014-065_final.pdf
5- see: http://www.skybrary.aero/index.php/A332,_vicinity_Melbourne_Australia,_2013_(CFIT_HF)
6- see: http://www.skybrary.aero/index.php/A320,_vicinity_Lyons_Saint-Exup%C3%A9ry_France,_2012_(CFIT_HF_AGC)
7- see: http://www.skybrary.aero/index.php/A319,_vicinity_Tunis_Tunisia,_2012_(LOC_HF)

There are many other Official Investigation Reports about incidents before 2012 which also had positive outcomes because of EGPWS. One notable example was on October 26, 2010 when the crew of a B737-800 lost positional awareness in relation to terrain during an initial descent to Asahikawa, Japan.[8] The aircraft was following ATC radar vectors and was below MVA and approaching mountainous terrain approximately 16 nm east of the airport during daylight, but in IMC. Two EGPWS Pull Up Warnings were received and acted on and the aircraft passed within 655 feet of a 7208ft high summit - see Figure 3 which is from the Official investigation Report.

Despite these successes, however, negative outcomes still occur to aircraft fitted with EGPWS:

1. On 14 August, 2013, an A300-600 cargo aircraft on a LOC approach to runway 18 at Birmingham, Alabama, USA, descended into terrain short of the runway in IMC at night. The pilots received EGPWS Alerts just before impact but the aircraft was not fitted with the latest recommended software enhancements which would have led to slightly earlier EGPWS activation.

2. On May 9, 2012, a brand new Su95 was on a demonstration flight when it flew into a mountain near Jakarta, Indonesia after the pilot, unaware of the local terrain, ignored 38 seconds of EGPWS Alerts and Warnings in IMC and switched the equipment off, believing that there was a database error. The terrain mapping feature had been demonstrated earlier in the flight but then switched off.

3. On July 28, 2010, an A321 flew into terrain whilst descending at 3000 fpm after loosing visual contact with the aerodrome on the downwind leg of a circling approach to runway 12 at Islamabad, Pakistan. Impact was preceded by EGPWS Cautions and Warnings lasting over a minute on which no action was taken.

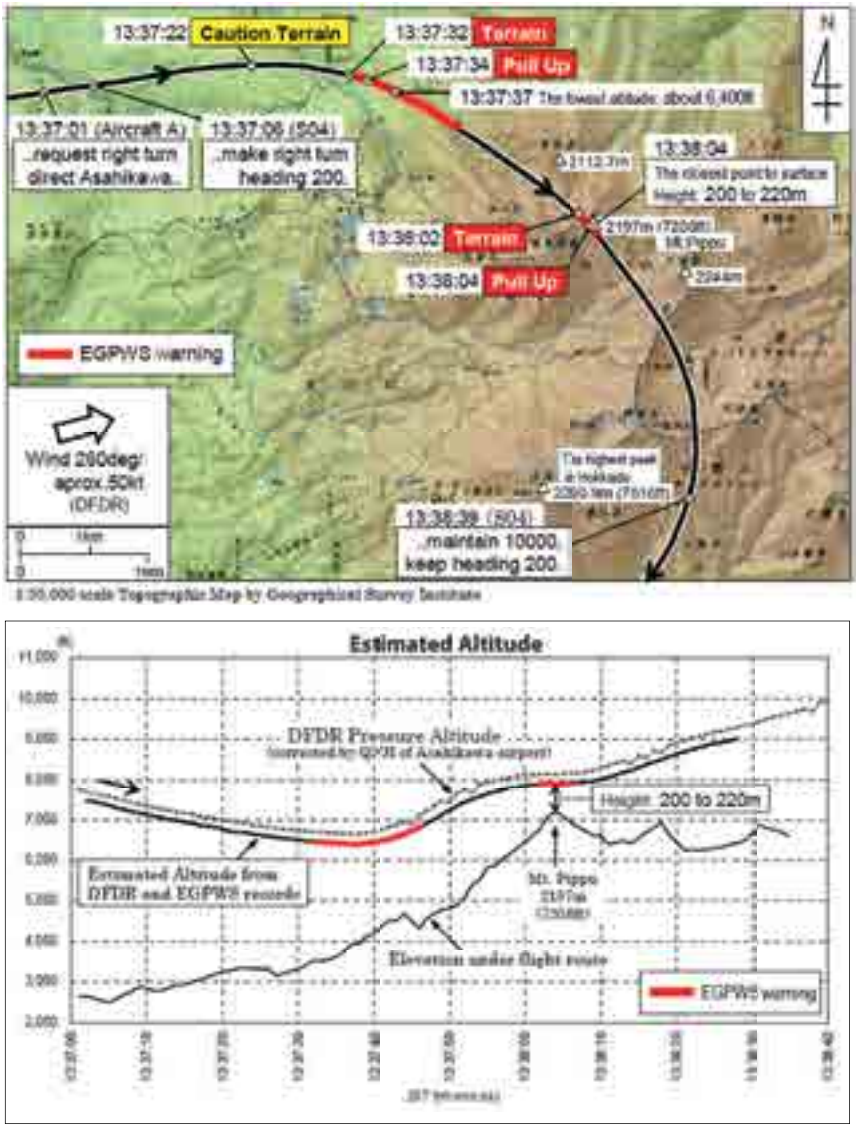


Figure 3 - The Boeing 737-800 Incident Asahikawa, Japan [reproduced from the Official Investigation Report]

4. On 10 April, 2010, a Tu-154 continued descent below the applicable non-precision approach minima at Smolensk, Russia in thick fog and crashed short of the runway and off the extended centreline after the crew ignored 18 seconds of EGPWS warnings culminating in 12 seconds of continuous Pull Up Warnings.

In all these accidents, the crew either significantly violated standard operating procedures before EGPWS Pull Up Warnings began and/or ignored them when they did occur. In three out of the four cases, had the crew responded to the warnings as trained when they began, these accidents would not have occurred.

Reference

Yasuo Ishihara "Reviewing worldwide EGPWS alert statistics -further reducing the risk of a CFIT" presented at the FSF IASS 2012 in Santiago, Chile

8- see: http://www.skybrary.aero/index.php/B738,_En_route,_east_of_Asahikawa_Japan,_2010_(CFIT_HF)
9- see: http://www.skybrary.aero/index.php/A306,_vicinity_Birmingham_AL_USA,_2013_(CFIT_HF_FIRE)
10- see: http://www.skybrary.aero/index.php/SU95,_manoeuvring_near_Jakarta_Indonesia,_2012_(CFIT_HF_FIRE)
11- see: http://www.skybrary.aero/index.php/A321,_vicinity_Islamabad_Pakistan,_2010_(CFIT_HF_FIRE)
12- see: http://www.skybrary.aero/index.php/T154,_vicinity_Smolensk_Russian_Federation,_2010_(CFIT_HF_WX_FIRE)

HOW MUCH IS TOO MUCH?

by Adrian Bednarek

I guess it used to be a sort of obligation for every action movie in the 90s to include a breathtaking scene with warning lights and sirens coming on. Red and yellow lights, a timer counting down and a decision which wire should be cut – it was all that simple and straightforward. Whether it was on a flight deck or at a nuclear missile launch site, there always was our hero ready to save the day (or – very often – the whole world). As always, the reality turns out to be much less spectacular and there is no timer to let us know how much time do we have. And our hero – the system operator, a pilot, an air traffic controller, process specialist or launch site commander – usually seems to be both lost and focused at the same time. Plus, there's no background dramatic music to spice things up…

There are places where all those flashing warning lights give us so much contradictory information at the same time that the person operating the system simply doesn't know what to do. Those places include nuclear power plants, chemical plants, operating rooms in hospitals or - when taking aviation into consideration – aircraft cockpits or maintenance facilities. In air traffic control those signals seem to be simpler to process - a warning comes on when aircraft are too close to each other, or they're flying too close to the ground. Actions to be taken also seem to be equally clear - press the button and tell the pilot to turn or change the altitude. Can it get any simpler than that?

In fact, it's a little bit more complicated. Modern ATM systems are much more complex than they used to be. We're not even aware how much data they process every second and how many data sources they use. Let's think about that for a moment - it's not a pure and raw radar signal being transferred to the screen. There is a whole network of those radars and each aircraft position is calculated in real time, based on the information taken from all of them. Then you have all the maps, sectors, borders, areas and their coordinates put into the database your system is using, along with the flight plans and other information processing - each aircraft is expected to be correlated and that information is exchanged with another system located abroad or in another city. When you have all the data combined it's only the programmers' ingenuity that limits what you can do with it. For example, you can decide to use it to warn the controller if he or she is doing something 'wrong', according to the system's logic.

That opens up a whole new range of possibilities for modern warning systems, or safety nets if you prefer to call them that. It's no longer a question of are those two aircraft too close to each other but also if they are flying assigned headings or following their routes properly. Are they properly equipped to enter RVSM airspace? If not, why did you clear them to such a high flight level? Or why is an aircraft flying into a sector which uses 8.33 MHz channel spacing when, according to the flight plan, it will not be able to select the proper frequency? Or maybe you should double check if your last acknowledged instruction was properly received, because it seems that the altitude entered by the crew into their FMC differs from the one entered by you into the system? And hey, you should look at this aircraft which is being transferred to your frequency! Yes, you get my point – warnings popping on your screen try to tell you more than just a simple "it's too close". Every warning message is supposed to be different but they all follow the most recognisable logic in colour coding - green is the normal state, yellow means something's not right and red means something's definitely not right and it's probably very serious. But that wasn't enough so a few other ways of catching your attention came into your life – flashing, bold, boxed or underlined text, an icon, a letter or a digit to let you know what exactly is going on. The whole idea of giving a warning before something bad happens is

ADRIAN **BEDNAREK**

works in Krakow, Poland as an air traffic controller and a safety manager, focusing on safety culture and practical drift in organisations. He has university degrees in safety engineering and aviation.

brilliant! And it really works when you're dealing with a single situation going wrong. It's not that easy when your screen is full of alerts and symbols which all look similar but only one of them is really important at that particular moment.

On 12 July 2012, a Boeing 737-300 departed Warsaw airport for its cargo flight to an airport in Western Europe. It wasn't an easy departure – several thunderstorms surrounded the airport and most aircraft were trying to avoid them, flying around in more or less random directions. At the same time a Saab 340 was trying to find its way to the airport and was entering the TMA from the west. As you might be expecting, things went badly and the result was a TCAS encounter with minimum distance being 2.69 nm horizontally and 700 ft vertically. A short-term conflict alert (STCA) was also activated on the controller's screen.

> *At the time immediately preceding the occurrence alerts appeared very frequently on the Controller screen. They were irrelevant to the proper operation of the Controller in his area of responsibility (except for the one concerning the analyzed proximity). For a dozen minutes such alerts were displayed on the screen. Each of these alerts was a piece of information which the Controller had to process and make a decision as to its meaning. For example, during the 10 minutes preceding the occurrence there were numerous STCAs, APWs, STSs and HAND OFFs. Each of these warnings was visualized in a color attracting attention (yellow or red, and SPI – white flashing) which means that at the same time they diverted the Controller's attention from other elements shown on the screen.*[1]

Even the most experienced controller still remains a human being (despite what you may have heard!) and his or her ability to move their attention from one part of the screen to another is limited. Most of us know that feeling of uncontrolled focusing on a small part of the screen where a conflict or another problem is developing (also known as tunnel vision). We don't need additional warning about things going on in that part of our sector but it would be nice to know if there's another place where things might also be starting to go wrong. Flashing warning messages can be a great tool to do that, but too many of them will quickly make them ineffective. Our previous ATM system was a perfect example of such a phenomenon – similar flashing messages were used both for an STCA activation and hand-off information. During busy times, our screens were just filled with such signals. And even when the controller realised that a particular message was a conflict warning, it didn't mean much in our approach control environment – STCA alerts were set to the ACC's minimum of 7 nm separation while we were using 3 nm. It made our approach sector look like a Christmas tree!

It turned out that this performance and fine-tuning problem was not an isolated issue and that it was quite common across Europe. For example, the report on the investigation into a one serious AIRPROX incident in Switzerland in 2012[2] stated that "the air navigation services provider Skyguide defines several STCA "suppressed areas" (SSA) throughout Switzerland, in which the triggering of alarms is suppressed. The reason for this at the location involved was the technical limitation of the ATM system which was not able to filter out nuisance alerts on the radar screens of ACC sectors above class D TMAs.

If you're dealing with limitation like this, you quickly realise that you have only two ways to go – turn the warnings off (like they did in Switzerland) or learn how to subconsciously ignore them (like we did in Poland). Whichever you choose, you have to accept the fact that your safety net is not working and it would be an honest step just to stop pretending that you still have one.

It can take many years to develop a long-term solution to problems like this especially if, as in our case, it was necessary to switch to a completely new ATM system. Of course, it would be naive to believe that it solved all of our problems – in fact, we just limited their severity and moved some of them away from controllers' eyes. The new system introduced additional functions and features which came with new types of warnings attached. New colours (and their combinations) are being used and the number of abbreviations and symbols used has grown dramatically so that now we sometimes find ourselves completely lost when some rarely-seen warning pops up. Just out of personal curiosity, I counted how many different warnings can be related to one aircraft and I found that there could be over dozen of them in a track data block! Taking that into consideration, it's not surprising that a priority system developed to display only a few warnings at any one time. There is simply not enough space to show them all!

It's expected and natural that every computer system working in a dynamic environment will sometimes have to handle erroneous signals. It will receive them as an input from various sensors or from a human operator and, at the same time, it will produce such signals as the result of the computations being done. In case of the safety nets those erroneous output signals result in either unwanted alerts or lack of an alert when it is needed. The former became our biggest issue. It's not difficult for current computer systems to detect (based on current values of aircraft position, speed, rate of descent and heading) that some of the detection thresholds for, say, minimum altitude or separation, will be exceeded. The

1- Extract from Final Report of the State Commission on Aircraft Accidents Investigation on the Serious Incident between a Saab 340 and a Boeing 737 on 12 July 2012 in the Warsaw TMA http://dlapilota.pl/files/upld/2012_0800_RK_ang.pdf

2- see http://www.skybrary.aero/bookshelf/books/2985.pdf

real problem, especially in a TMA or tower environment, is that the parameters mentioned above are often subject to sudden changes. Aircraft can make a 90 degree turn or reduce speed significantly when turning upwind. The introduction of simple detection and warning safety nets will surely lead us to the problem mentioned before – too many warnings, too many unwanted alerts. The solution is to employ more complex algorithms and to take additional data such as that from mode S or cleared level or heading information manually entered by the controller into consideration. Such data can greatly improve the overall performance of the safety nets system and, in my experience, significantly reduce nuisance alerts. Of course, it's not a perfect world and this strategy comes with its own drawbacks. It relies on additional data, adds significantly to the complexity of the whole system and can have a negative impact on the overall level of safety. For example, a delay in level bust warning which is based on cleared level entered by the controller can be a potential threat for system performance when we realise that this value could have been entered by mistake.

Safety nets have become standard equipment in our ops rooms and I'm sure most of us cannot even imagine an ATM system without them. They have proved their usefulness and they become more and more effective as computing power increases and more useful input data becomes available. But they still have constraints which we have to accept and we always have to consider their ability to interact with human senses and their limitations. Unwanted alerts can become one of the most important issues when it comes to safety nets as their presence quickly erodes the controllers' trust in the system. This can seriously degrade safety and interfere with your perception of risk. That is the reason we should reconsider our approach to safety nets and the role they play. They simply deserve to be properly managed.

FUNCTIONAL SAFETY NETS FROM A RESILIENCE ENGINEERING PERSPECTIVE

by Professor Erik Hollnagel

Originally, a safety net was a large net that could catch someone who accidentally fell from a height, such as the safety net used in a circus trapeze act or the safety nets used at many building sites ever since the construction of the Golden Gate Bridge in San Francisco (1933-1937). The purpose of such a physical safety net is to prevent harm when something or someone falls unexpectedly, either harm to the someone who is falling or harm to the someone who can be hit by the something that is falling.

Functional safety nets and loss of control

Today, the meaning of the term 'safety net' has been extended to describe not only *physical* safety nets but also *functional* safety nets, in the sense of the various ways in which a situation can be prevented from going out of control, or be saved if control has been temporarily lost. A loss of control can have serious consequences in two different ways. First, that it becomes impossible to ensure that an activity continues as intended: the future becomes more uncertain and neither safety nor productivity – or for that matter quality – can be effectively managed. Second, that the loss of control leads to a loss of life, time, and/or material or immaterial property.

From a resilience engineering perspective, the primary purpose of a functional safety net is, however, not simply to re-establish control but rather to dampen or delay unmanaged developments as a prerequisite to re-establishing control. Examples of functional safety nets are not limited to aviation but can be found in almost every line of activity. They range from a social or economic safety net in the case of unemployment or illness, over the collective experience that an organisation can fall back on when something happens, to the technical and non-technical competencies and experience that are ready for use to manage and stabilise irregular situations. A functional safety net can therefore be seen as a kind of active barrier that limits the consequences of a temporary loss of control.

A functional safety net involves a prepared systemic response that can be carried out either instantaneously or with very little delay. A functional safety net cannot serve its purpose if a response first has to be prepared or if the required resources first have to be activated – just as a physical safety net will fail to serve its purpose if it has to be installed prior to being used when the need arises. A functional safety net also primarily compensates for something that is missing in a situation – such as a specific practical or theoretical competence. The response therefore differs from a recovery action, which may take time to plan and activate and which may also be expected to work over longer periods of time.

In aviation, the term 'safety net' has been used to include also the automated systems that keep an eye on work and that intervene to help keep performance within safe limits, e.g., a TCAS. But in resilience engineering terms it would be

simpler, and more correct, to call these for automated safety (or protection) systems rather than safety nets, if for no other reason then because such systems are unable to learn on their own: they are designed but do not themselves develop. The functional safety nets I will now discuss will therefore exclude automated safety systems.

Today's socio-technical systems are often called complex, or even complex adaptive, systems (CS or CAS). Complex (adaptive) systems are partly intractable and must work in partly intractable environments where demands and resources may change when least expected. This makes it impossible fully to rely on a set of pre-defined responses. A functional safety net must continuously develop and improve its responses to prevent that the discrepancy between what it can do and what is needed becomes too large. And it must do so itself, rather than wait for some *deus ex machina* to bring it up to date.

Resilience engineering proposes that four fundamental abilities are required for a system's potential to perform in a resilient manner – or in short, for its resilience. The first is the ability to respond, the second the ability to monitor, the third the ability to learn, and the fourth the ability to anticipate. A functional safety net represents a subset of the ability to respond because it is only concerned with the responses to the potential or actual loss of control. The everyday functioning of a system clearly requires many other kinds of responses as well. The ability to respond, whether in the broad or the narrow sense, should, however, not be considered in isolation. Resilience engineering makes clear that the four abilities depend on each other and that they therefore must be seen together, as an integrated whole. Before we can begin to measure and manage a system's resilience potential, we must therefore first uncover and understand the ways in which each of the four abilities depends on the others.

In order to understand the ability to respond that is the essence of a functional safety net, we must find out what this ability depends on or requires as support. In other words, how does it depend on the other abilities – and possibly on other system functions?

While responding may be improved by monitoring, which enables timely responses, as well as anticipation, which supports the preparation of responses, the most significant dependence is clearly on the ability to learn. *The reason is simply that without learning, the responses will always remain the same*. But always responding in the same way is bound to be insufficient, unless the environment and the conditions of work are perfectly the stable. This may possibly be the case for some types of physical safety nets; but it will never be the case for functional safety nets, not even for systems that only change very slowly. And aviation is definitely not one of those.

Functional safety nets and organisational learning

Organisational learning is an issue where there are more theories and opinions than there are facts. But the basic idea is simply that organisations learn by encoding inferences from experience into routines that guide or support behaviour. If we consider the role and nature of functional safety nets, we can see that three types of learning may play a role. An organisation can learn from its own experience (direct or intra-organisational learning), from the experience of others (indirect or inter organisational learning), and by developing industry-wide conceptual frameworks or paradigms for interpreting practical experience (systemic learning). Direct and indirect learning are both relevant for functional safety nets.

Learning from own experience is direct and involves little delay, regardless of whether it is done by individuals, by groups, or by the organisations. Typical examples are the sharing of good habits, or even best practices, among colleagues or within a group or an organisation. Direct learning will usually be very specific to the organisation and the type of activity it performs. The advantage is that learning can be directly associated with specific situations or conditions. The disadvantage is that the specificity makes it difficult to generalise, in particular to other organisations.

In the case of direct learning, the time lag or delay between learning and use is short. Because the learning is specific to the organisation and/or some situations, the lessons learned will be readily available when the need arises. Since the safety nets are localised within the organisation they can also be maintained as part of everyday work.

While learning from own experience is valuable, it is inescapably limited. It is therefore important to learn also from other organisations that are involved in the same kind of activity or service, but probably less important to learn from completely different domains. This is the rationale for proposing industry-wide 'best practices' and for defining safety nets as collaborative, mutually-supporting activities to sustain safety within an industry. But while the experience of others may be useful, it suffers from being indirect rather than direct. No two organisations, such as two airlines or two ANSPs, work in exactly the same way or have exactly the same working conditions. The direct experience of one organisation therefore becomes the indirect experience of another, and must be interpreted or 'coded' in some way before this other organisation can use it.

In the case of indirect learning, there may also be a substantial time lag or delay between learning and use. The transmission mostly takes place by informal means, through talks among colleagues or via significant adverse events (though these are not the best to learn from), and therefore without systematic support from either organisation. The assimilation of the learning inevitably requires some form of 'tailoring' of the original responses to the new context. The indirect learning will not be immediately relevant or applicable by an organisation, but must be mediated in one way or another. This means that the readiness to respond is less than for direct learning. Indirect learning therefore has an associated cost that should be carefully considered when safety nets are built.

The Bottom Line

Functional safety nets are by their nature socio-technical rather than technical. They are not designed and fixed, but develop and change over time. They represent part of an organisation's ability to respond and their effectiveness depends on the ability of the overall system to learn. Organisations must therefore look for the best possible ways to ensure the learning on which the efficacy of the functional safety net depends. While individual organisations may find that a combination of direct and indirect learning is sufficient for the development and management of functional safety nets, there is also a need to encode or institutionalise such knowledge for even wider use. We often hear that we must learn from the good experiences of other industries. And strangely enough each industrial domain (e.g. nuclear, aviation, healthcare, off-shore, etc.) seems to believe that other domains are doing better and that one therefore should try to encapsulate or imitate the lessons learned there. But is the grass really greener on the other side of the fence?

PROFESSOR ERIK **HOLLNAGEL**

is Professor at the University of Southern Denmark (DK), Professor Emeritus at the University of Linköping (S). Professional interests: industrial safety, resilience engineering, patient safety, accident investigation, and modelling large-scale socio-technical systems. He has published widely and is the author/editor of 21 books, including five books on resilience engineering. Erik also coordinates the Resilient Health Care net and the FRAMily.

FIT FOR PURPOSE? QUESTIONS ABOUT ALARM SYSTEM DESIGN FROM THEORY AND PRACTICE

by Dr Steven Shorrock

Most safety-critical environments – nuclear power control rooms, flight decks and operating theatres – have one critical system feature in common: alarms. The ATC ops room, by comparison, has few. But this will not always be the case. More complexity, increasing automation, and future changes in ATM, will mean more alarms – something that CNS colleagues have experienced for over a decade.

QF32 and the alarm avalanche

4th November 2010.
Just four minutes after take off, climbing through 7,000ft from Singapore Changi Airport, an explosion occurred in one of the engines of QF32, a Qantas Airbus A380. Debris tore through the wing and fuselage, resulting in structural and systems damage. The crew tried to sort through a flood of computer-generated cockpit alerts on the electronic centralised aircraft monitor (ECAM), which monitors aircraft functions, produces messages detailing failures, and lists procedures to undertake to correct the problem. They crew recalled an "avalanche" of (sometimes contradictory) warnings relating to engines, hydraulic systems, flight controls, landing gear controls, and brake systems.

David Evans, a Senior Check Captain at Qantas with 32 years of experience and 17,000hrs of flight time, was in an observer's seat during the incident. Interviewed afterwards, he said *"We had a number of checklists to deal with and 43 ECAM messages in the first 60 seconds after the explosion and probably another ten after that. So it was nearly a two-hour process to go through those items and action each one (or not action them) depending on what the circumstances were"* (Robinson, 8 December 2010). The Pilot in Command, Captain Richard de Crespigny (15,000hrs) wrote, *"The explosion followed by the frenetic and confusing alerts had put us in a flurry of activity, but Matt* [Matt Hicks, First Officer, 11,000hrs] *and I kept our focus on our assigned tasks while I notified air traffic control … 'PAN PAN PAN, Qantas 32, engine failure, maintaining 7400 and current heading'"… "We had to deal with continual alarms sounding, a sea of red lights and seemingly never-ending ECAM checklists. We were all in a state of disbelief that this could actually be happening."* (21 July, 2012). Subsequently, Captain de Crespigny stated, *"At the point of maximum stress, the cockpit displays didn't make a whole lot of sense"* (Pasztor, 27 June, 2013).

Rewind to 1979

Over thirty years prior to QF32, the Three Mile Island (TMI) partial nuclear meltdown in 1979 was perhaps the first major illustration of the alarm problem. The Report of the President's Commission on the accident stated, *"During the first few minutes of the accident, more than 100 alarms went off, and there was no system for suppressing the unimportant signals so that operators could concentrate on the significant alarms. Information was not presented in a clear and sufficiently understandable form; for example, although the pressure and temperature within the reactor coolant system were shown, there was no direct indication that the combination of pressure and temperature meant that the cooling water was turning into steam. Overall, little attention had been paid to the interaction between human beings and machines under the rapidly changing and confusing circumstances of an accident"* (p. 11). A shift supervisor testified that there had never been fewer than 52 alarms lit in the control room. The computer printer registering alarms was running more than 2 hours behind the events. Similar to de Crespigny's remark above, the TMI control room operator Craig Faust recalled for the Commission his reaction to the incessant alarms: *"I would have liked to have thrown away the alarm panel. It wasn't giving us any useful information".* The accident triggered a flurry of human factors/ergonomics (HF/E) activity.

Many other accidents have featured alarm handling since then, including the Texaco explosion and fires (Milford Haven, UK, 1994) and the Channel Tunnel fire (1996). In the UK, official investigations have found significant deficiencies in alarm handling (see Health and Safety Executive, 2000). Alarm flooding, poorly prioritised

alarms and 'clumsy automation' have prevented users from detecting important alarms, understanding the system state, and reacting in a directed and timely manner. While alarm systems are one of the most essential and important interfaces between human operators and safety-related processes, they can also be one of the most problematic.

In CNS/ATM, alarms are currently most prevalent in system control. Typically, an integrated, centralised control and monitoring system (CMS) is used to monitor and control engineering systems within an ATC centre. Engineers monitor alarms from dedicated workstations, and remedy faults either remotely (via software) or locally. The tasks of a system controller currently have little overlap with air traffic controllers, but with increases in automation, the line between the functions will begin to fade. The complexity and criticality of systems will mean that we all need to pay more attention to the HF/E needs of CNS, and also to the alarms that are likely to migrate to the ATM environment.

Alarm design 101

The purpose of alarms is to direct the user's attention towards significant aspects of the operation or equipment that require timely attention. Much has been written on good practice for alarm management. The Engineering Equipment and Materials Users Association (EEMUA) (1999) summarise the characteristics of a good alarm as follows:

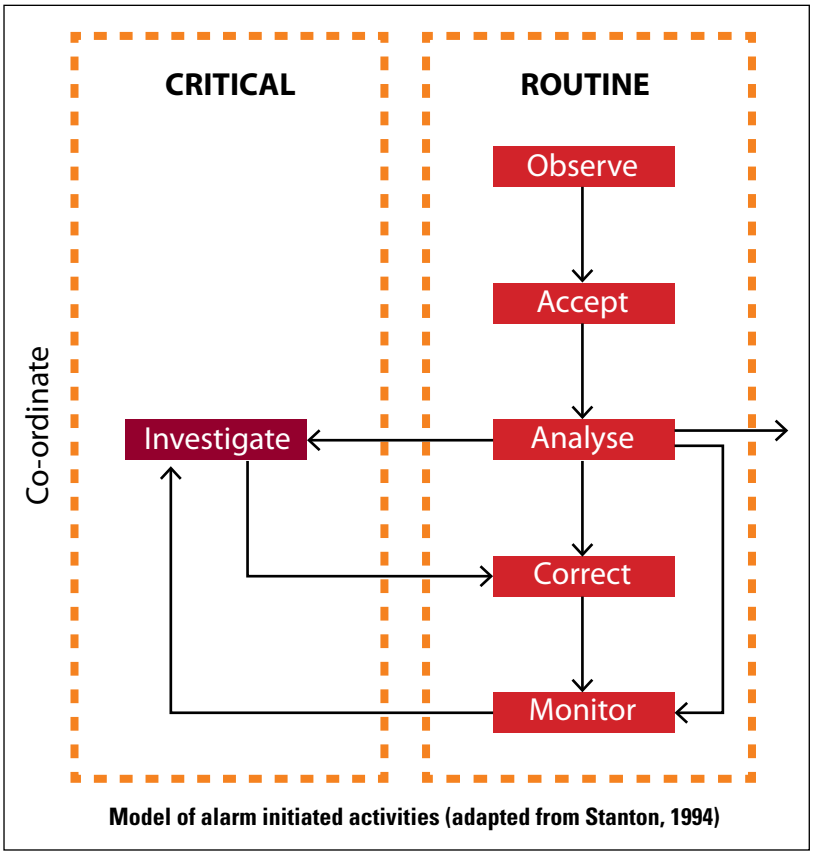
- **Relevant** – not spurious or of low operational value.
- **Unique** – not duplicating another alarm.
- **Timely** – not long before any response is required or too late to do anything.
- **Prioritised** – indicating the importance that the operator deals with the problem.
- **Understandable** – having a message that is clear and easy to understand.
- **Diagnostic** – identifying the problem that has occurred.
- **Advisory** – indicative of the action to be taken.
- **Focusing** – drawing attention to the most important issues.

These characteristics are not always evident in alarm systems. Even when individual alarms may seem 'well-designed' they may not work in the context of the system as a whole and the user's activity.

This article raises a number of questions for consideration in the design of alarm systems, framed in a model of alarm-handling activity. The questions may help in the development of an alarm philosophy (one of the first steps in alarm management), or in discussion of an existing system. The principles were originally derived from evaluations of two different control and monitoring systems for two ATC centres (see Shorrock et al, 2001). These evaluations used an exhaustive HMI guidelines database (MacKendrick, 1998; Shorrock, et al. 2001). The guidelines that were relevant to alarm handling, and put into context by the evaluations, were extracted and grouped to help form preliminary principles. In parallel, a model of alarm-initiated activities (Stanton, 1994) was used to group and form the final set of principles. The resultant principles are included in this article as questions for consideration, structured around six alarm-handling activities (Observe, Accept, Analyse, Investigate, Correct, and Monitor). This is illustrated and outlined below.

Understanding alarm initiated activities

Observation is the detection of an abnormal condition or state within the system (i.e., a raised alarm). At this stage, care must be taken to ensure that coding methods (colour and flash/blink, in particular) support alarm monitoring and searching. Excessive use of highly saturated colours and blinking can de-sensitise the user and reduce the attention-getting value of alarms. Any use of auditory alarms should further support observation without causing frustration due to the need to accept alarms in order to silence the auditory alert, which can change the 'alarm handling' task to an 'alarm silencing' task.



Model of alarm initiated activities (adapted from Stanton, 1994)

DR STEVEN **SHORROCK**

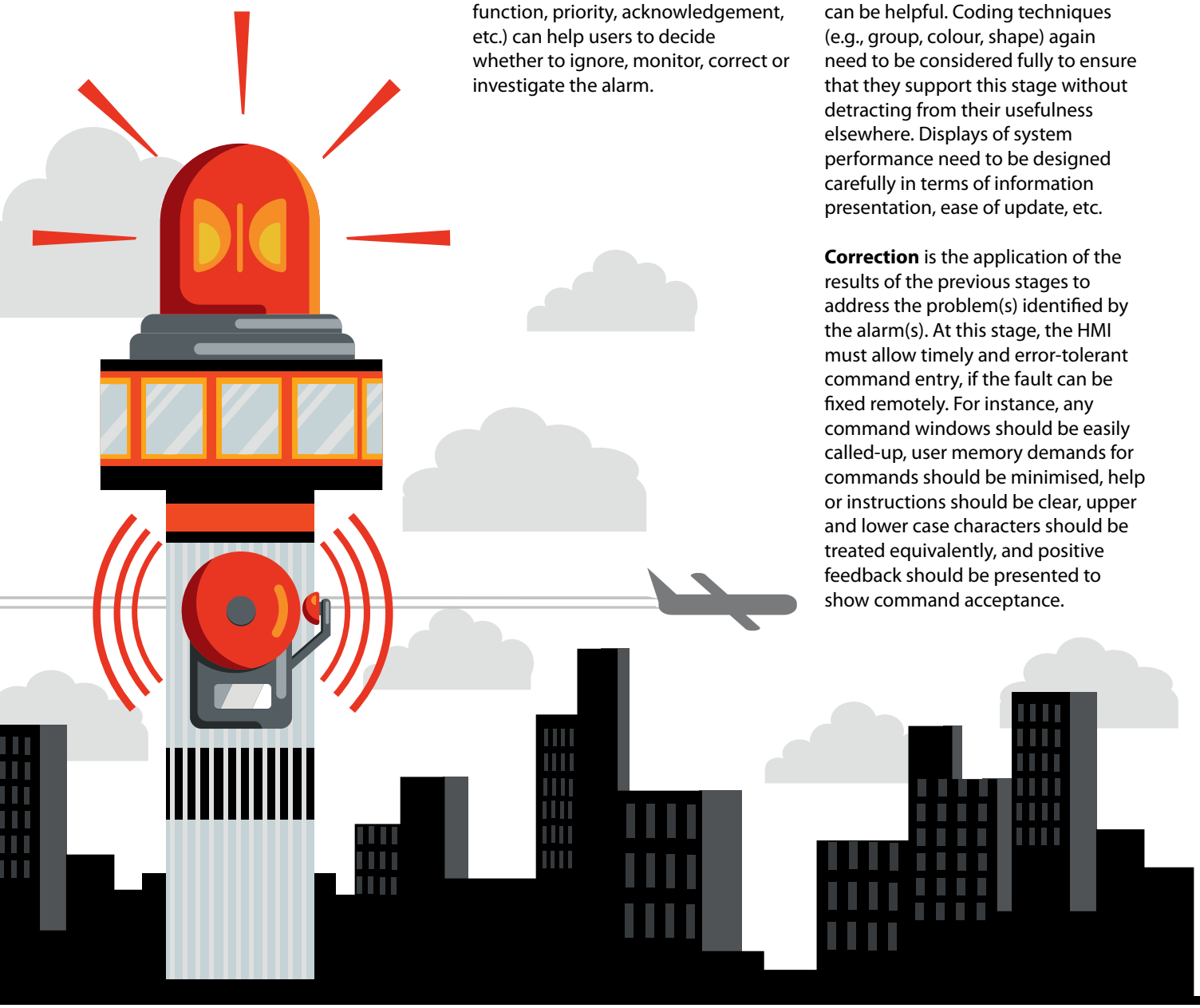
is Project Leader, Safety Development at EUROCONTROL and the European Safety Culture Programme Leader. He is a Registered Ergonomist and a Chartered Psychologist with a background in practice and research in safety-critical industries. Steve is also Adjunct Senior Lecturer at the University of New South Wales, School of Aviation.

Acceptance is the act of acknowledging the receipt and awareness of an alarm. At this stage, user acceptance should be reflected in other elements of the system that is providing alarm information. Alarm systems should aim to reduce user workload to manageable levels; excessive demands for acknowledgement increase workload and unwanted interactions. For instance, careful consideration is required to determine whether cleared alarms really need to be acknowledged. Group acknowledgement of several alarms (e.g. via using 'click-and-drag' or a Shift key) may lead to unrelated alarms being masked in a block of related alarms. Single acknowledgement of each alarm, however, can increase workload and frustration, and an efficiency-thoroughness trade-off can lead to alarms being acknowledged unintentionally as task demands increase. It can be preferable be to allow acknowledgement for alarms for the same system.

Analysis is the assessment of the alarm within the task and system context, leading to the prioritisation of that alarm. Alarm lists can be problematic, but, if properly designed, they can support the user's preference for serial fault or issue management. Effective prioritisation of alarm list entries can help users at this stage. Single 'all alarm' lists can make it difficult to handle alarms by shifting the processing debt to the user. However, a limited number of separate alarm lists (e.g., by system, function, priority, acknowledgement, etc.) can help users to decide whether to ignore, monitor, correct or investigate the alarm.

Investigation is any activity that aims to discover the underlying factors order to deal with the fault or problem. At this stage, system schematics or other such diagrams can be helpful. Coding techniques (e.g., group, colour, shape) again need to be considered fully to ensure that they support this stage without detracting from their usefulness elsewhere. Displays of system performance need to be designed carefully in terms of information presentation, ease of update, etc.

Correction is the application of the results of the previous stages to address the problem(s) identified by the alarm(s). At this stage, the HMI must allow timely and error-tolerant command entry, if the fault can be fixed remotely. For instance, any command windows should be easily called-up, user memory demands for commands should be minimised, help or instructions should be clear, upper and lower case characters should be treated equivalently, and positive feedback should be presented to show command acceptance.



Monitoring is the assessment of the outcome of the Correction stage. At this stage, the HMI (including schematics, alarm clears, performance data and message/event logs) needs to be designed to reduce memory demand and the possibility of interpretation problems (e.g., the 'confirmation bias').

Additionally, in multiple-user systems, co-ordination between operators is required to work collaboratively to attend to system problems. This may involve delegating authority for specific issues to colleagues, or co-ordinating efforts for problems that permeate several different parts of the overall system.

The design questions for each stage of alarm handling are shown in the table. In most cases, questions are applicable primarily in one stage of alarm handling, but also have a bearing on other stages, depending on the system in question. The questions are therefore shown in terms of their primary relevance within the model, but may be considered against other stages.

QF32 and you

The QF32 crew were overwhelmed at every stage of the model of alarm initiated activities described above. But their experience, competence and ingenuity meant that they were able to take control of the aircraft, not by getting caught up in an alarm flood, but by focusing on what was working. They had to take the initiative and adjust their performance in a way that was never previously imagined, as alerts became unusable. Sometimes, system complexity makes it near-impossible to imagine some forms of emergent system behaviour. When he was asked if he had any recommendations for Qantas or Airbus concerning training for ECAM messages in the simulator, David Evans responded, *"We tried to recreate it in the sim and we can't! I think it was just such an extraordinary day"* (Robinson, 8 December 2010). Our inability to specify systems perfectly, or to train for every single eventuality, is one reason why we need highly competent people in control. But the goal is well-designed systems supporting highly competent people, not highly competent people working around systems that fail to meet their needs.

Will alarms ever be as critical in CNS/ATM as they are in the cockpit or control room? It's hard to say, but one thing is for sure, ATM will see more alarms, and CNS is already well on the road. With regard to the issues that have been known for over 30 years in other industries, prevention is better than cure. As the experts in your work, you need to be involved in the design of alarm systems from the beginning, and at every stage. And remember that, fundamentally, human factors/ergonomics is about design, not accidents. So demand competent HF/E design expertise, and a user-centred design process. Understanding the nature of alarm handling, and the associated design issues, can help you – the field expert – to be a more informed user, helping to bring about the best systems to support your work.

References

- de Crespigny, R. (July 21, 2012). This is your captain speaking. *The Australian*. EEMUA (1999). *Alarm Systems: A Guide to Design, Management and Procurement*. EEMUA Publication No. 191. The Engineering Equipment and Materials Users Association: London.
- Health and Safety Executive (2000). *Better Alarm Handling*. HSE Information Sheet - Chemicals Sheet No. 6. March, 2000. See http://www.hse.gov.uk/humanfactors/topics/alarm-management.htm
- Kemeny, J.G. (Chairman) (1979). *President's Commission on the Accident at Three Mile Island*. Washington DC.
- MacKendrick, H. (1998). *Development of a Human Machine Interface (HMI) Guidelines Database for Air Traffic Control Centres*. R & D Report 9822. National Air Traffic Services Ltd.: London.
- Pasztor, A. (June 27, 2013). How Pilot Brought In Crippled Superjumbo. *The Wall Street Journal*.
- Robinson, R. (8 December 2010). EXCLUSIVE - Qantas QF32 flight from the cockpit. Royal Aeronautical Society. http://bit.ly/1LjECi1
- Shorrock, S.T., MacKendrick, H. and Hook, M., Cummings, C. and Lamoureux, T. (2001). The development of human factors guidelines with automation support. *Proceedings of People in Control: An International Conference on Human Interfaces in Control Rooms*, Cockpits and Command Centres, UMIST, Manchester, UK: 18 - 21 June 2001.
- Shorrock, S.T. and Scaife, R. (2001). Evaluation of an alarm management system for an ATC Centre. In D. Harris (Ed.) *Engineering Psychology and Cognitive Ergonomics: Volume Five - Aerospace and Transportation Systems.* Aldershot: Ashgate, UK.
- Shorrock, S.T., Scaife, R. and Cousins, A. (2002). Model-based principles for human-centred alarm systems from theory and practice. Proceedings of the *21st European Annual Conference on Human Decision Making and Control*, 15th and 16th July 2002, The Senate Room, University of Glasgow.
- Stanton, N. (1994). Alarm initiated activities. In N. Stanton (Ed.), *Human Factors in Alarm Design*. Taylor and Francis: London, pp. 93-118.

FIT FOR PURPOSE? **QUESTIONS TO ASK ABOUT ALARM SYSTEM DESIGN**

This checklist may help to inform an alarm philosophy or an informal exploration of an alarm system from the viewpoint of user activity. It should be possible to answer 'Yes' to most questions that are applicable. The questions may be useful in discussions involving users, designers and other relevant stakeholders.

Observe	Yes	No	N/A
1. Is the purpose and relevance of each alarm clear to the user?			
2. Do alarms signal the need for action?			
3. Are alarms presented in chronological order, and recorded in a log (e.g. time stamped) in the same order?			
4. Are alarms relevant and worthy of attention in all the operating conditions and equipment states?			
5. Can alarms be detected rapidly in all operating (including environmental) conditions?			
6. Is it possible to distinguish alarms immediately (i.e., different alarms, different operators, alarm priority)?			
7. Is the rate at which alarm lists are populated manageable by the user(s)?			
8. Do auditory alarms contain enough information for observation and initial analysis, and no more?			
9. Are alarms designed to avoid annoyance or startle?			
10. Does an indication of the alarm remain until the user is aware of the condition?			
11. Does the user have control over automatically updated information, so that information important to them at any specific time does not disappear from view?			
12. Is it possible to switch off an auditory alarm independent of acceptance, while ensuring that it repeats after an appropriate period if the problem is not resolved?			
13. Is failure of an element of the alarm system made obvious to the user?			
Accept			
14. Has the number of alarms that require acceptance been reduced as far as is practicable?			
15. Is multiple selection of alarm entries in alarm lists designed to avoid unintended selection?			
16. Is it possible to view the first unaccepted alarm with a minimum of action?			
17. In multi-user systems, is only one user able to accept and/or clear alarms displayed at multiple workstations?			
18. Is it only possible to accept an alarm from where sufficient alarm information is available?			
19. Is it possible to accept alarms with a minimum of action (e.g., double click), from the alarm list or mimic?			
20. Is alarm acceptance reflected by a change on the visual display (e.g. visual marker and the cancellation of attention-getting mechanisms), which prevails until the system state changes?			
Analyse			
21. Does alarm presentation, including conspicuity, reflect alarm priority with respect to the severity of consequences of delay in recognising the problem?			
22. When the number of alarms is large, is there a means to filter the alarm display by appropriate means (e.g. sub-system or priority)?			
23. Are users able to suppress or shelve certain alarms according to system mode and state, and see which alarms have been suppressed or shelved? Are there *means to document the reason for suppression or shelving?			
24. Are users prevented from changing alarm priorities?			
25. Does the highest priority signal always over-ride, automatically?			
26. Is the coding strategy (colour, shape, blinking/flashing, etc) the same for all display elements?			
27. Are users given the means to recall the position of a particular alarm (e.g. periodic divider lines)?			
28. Is alarm information (terms, abbreviations, message structure, etc) familiar to users and consistent when applied to alarm lists, mimics and message/event logs?			
29. Is the number of coding techniques at the required minimum? (Dual coding [e.g., symbols and colours] may be needed to indicate alarm status and improve analysis.)			
30. Can alarm information be read easily from the normal operating position?			
Investigate			
31. Is relevant information (e.g. operational status, equipment setting and reference) available with a minimum of action?			
32. Is information on the likely cause of an alarm available?			
33. Is a usable graphical display concerning a displayed alarm available with a single action?			
34. When multiple display elements are used, are individual elements visible (not obscured)?			
35. Are visual mimics spatially and logically arranged to reflect functional or naturally occurring relationships?			
36. Is navigation between screens, windows, etc, quick and easy, requiring a minimum of user action?			
Correct			
37. Does every alarm have a defined response and provide guidance or indication of what response is required?			
38. If two alarms for the same system have the same response, has consideration been be given to grouping them?			
39. Is it possible to view status information during fault correction?			
40. Are cautions used for operations that might have detrimental effects?			
41. Is alarm clearance indicated on the visual display, both for accepted and unaccepted alarms?			
42. Are local controls positioned within reach of the normal operating position?			
Monitor			
43. Is the outcome of the Correction stage clear to the user? (A number of questions primarily associated with observation become relevant to monitoring.)			
Co-ordinate			
44. Are shared displays available to show the location of operators in system, areas of responsibility, etc?			

RUNWAY SAFETY ALERTS:
HOW FAST CAN WE REACT TO THEM?

by Gerard van Es

On March 15 2011 an A320 (with callsign SWR 1326) was cleared for take-off on runway 16 of Zurich airport. The crew of SWR 1326 acknowledged this clearance and initiated their take-off roll. Another A320 (with callsign SWR 202W) on runway 28, also received clearance for take-off from the same controller. The crew of SWR 202W acknowledged this clearance and immediately initiated their take-off roll on runway 28. Runway 16 and runway 28 intersect each other about half way along runway 16 and about two-thirds of the way along runway 28. At the time the take-off clearance was being issued to SWR 202W, SWR 1326 had already started its take-off. During the take-off roll, the crew of SWR 202W noticed SWR 1326, which was coming from the right on runway 16, and immediately aborted their take-off. A few seconds later, the air traffic control officer gave the crew of SWR 202W the order to immediately stop their take-off. SWR 202W came to a standstill on the runway just before the intersection with runway 16. The crew of SWR 1326 had not noticed the incident and continued their flight to their destination. Well before the crew of SWR 202W decided to reject their take-off, the air traffic control officer received an alert from the runway Runway Incursion Monitoring and Conflict Alert System (RIMCAS) that was operational at Zurich airport. It took nine seconds for the air traffic control officer to give the stop instruction to SWR 202W after the alert was generated. At that time the crew of SWR 202W already rejected the take-off so this instruction had no effect.

The air traffic control officer was surprised by the runway incursion alert and believed in the first instant that it was a "false alarm with a vehicle"[1]. The SWR 1326 was no longer present in the controller's mental plan at this point in time. The air traffic control officer checked whether a vehicle was close to the runways or whether a landing aircraft was on runway 16. The controller then finally realised that two aircraft were simultaneously taking off on runway 16 and runway 28.

Many airports have runway safety systems in order to avoid collisions due to a runway incursion. Such systems have a sensing/surveillance part that determines the position, direction and speed of aircraft and ground vehicles; a safety logic part which consists of rules and algorithms to interpret these data; and a human interface in which the information is passed on to the aircraft traffic controller or pilot. All systems currently in operation at airports are so-called tower-based systems in which the information from the runway safety system is passed on to the controller only. After receiving an alert from the runway safety system the controller has to make an evaluation of the situation and based on that outcome make a decision of the course of action (e.g. give instructions to the flight crew). This process of evaluating and decision making can take a lot of time as illustrated in the example at the beginning. This single example however does not give us a clear picture on what typical response times are (the response time is the time span between the onset of the alert and the response of the controller). There are a number of variables that influence the response time like age of the controller, experience, workload, environmental conditions (e.g. visibility, light conditions), complexity of the runway layout and trust in the runway safety system. This last variable is influenced by the rate of false and nuisance alerts generated by the runway safety system.

On top of the response time there is also the duration of the controller response which is the total time of the verbal communication with an aircraft or ground vehicle (e.g. giving a directive warning). Human-in-the-

1- Runway safety systems like RIMCAS may provide false alerts if the quality of the surveillance data used by such systems is not optimal. In addition to false alerts, nuisance alerts are generated by runway safety systems. Finally untimely alerts can also occur due to the safety logic design. A high rate of false, nuisance, or untimely alerts may hamper the effectiveness of any warning system. It can change the user's attitude and belief about the warning system. As a result they may lose confidence in the system.

GÉRARD **VAN ES**

works as a Senior Advisor flight safety and operations for the NLR-Air Transport Safety Institute - Amsterdam, the Netherlands.
He is currently involved in the European working group for the prevention of runway excursions.

loop simulations conducted by the MITRE Corporation give us some idea of what the typical response times and response durations can be. These experiments were conducted using a tower simulator and a flight deck simulator. A group of tower controllers was asked to work several scenarios. In some of these scenarios a runway incursion was simulated and alerts were generated by a runway safety system. Of course such an experiment can never fully simulate the real world as the participants were more or less prepared for an alert to occur. Nevertheless the results of the MITRE experiments give us an idea of what you can expect in terms the typical delays of getting an important message to a flight crew or a vehicle driver. The MITRE experiments showed that the mean response time of the controller to an alert was 4.6 seconds with a maximum of 8.1 seconds. The mean response duration was 2.3 seconds with a maximum of 5.3 seconds. By simply taking the averages together, an average time from the alert to instructing the pilots takes about 6.9 seconds with a maximum of 13.4 seconds! These results illustrate that the time the air traffic controller officer in the incident example took (9 seconds) is nothing out of the ordinary. But the story does not stop here because now the pilot or vehicle driver must take action. Let's focus on the pilots a bit more. Just like the controller, the pilot needs some time to respond and act to the instruction given by the controller. However, the pilot just needs to react most of the time whereas the controller needs to assess if the alert is true or not and decide on the best option to resolve any issue. Of course this takes more time for the controller than for the pilot. The experiments by MITRE showed that the time span between the onset of the controller's instruction to the pilot and the start of the action by the pilot can take up to 5.3 seconds with an average of 2.3 seconds. If we assume that the controller has given a stop instruction, the pilot still has to initiate the rejected take-off procedure. Once it has been started, it still takes time for all the stopping devices available to become effective. For instance it can take about 2 seconds before the brakes are fully effective and the lift dumpers fully deployed (if installed). If it is a jet aircraft, and thrust reversers are available, it can take 4 to 8 seconds to get full reverse thrust after reverser deployment. Meanwhile the aircraft is using up runway distance and may be getting closer to the conflicting aircraft or vehicle.

Although runway safety systems can be very effective in avoiding runway collisions, there are cases in which these systems are less effective due to the long time it takes from the activation of the alert to the actual action taken by the pilot or vehicle driver. Runway safety alerts could be send directly to the pilot or vehicle driver, but then they would still need to assess the situation and make a decision. This would take additional time (although less if the air traffic controller was in the loop). Such additional decision time could be avoided by using directive alerts (or advice as in the case of TCAS 2) that tell the pilot or vehicle driver what action they should take, but this would require that the users have a high level of trust in the system. But taking the controller out of the loop could also introduce new problems if both the pilot/driver and the controller were to react differently to the same event with different solutions.

References

- For a summary of the Zurich Serious Incident referred to based on the Official Investigation Report and access direct to that Report see: http://www.skybrary.aero/index.php/A320/A320,_Zurich_Switzerland,_2011_(LOS_HF)
- Sanchez J., Smith E. C., Chong R. S. 2009, Controller and Pilot Response Times to Runway Safety Alerts, MTR090237, The MITRE Corporation, McLean, VA.

THE AIR TRAFFIC CONTROLLER AS A "SAFETY NET": PERHAPS THE MOST IMPORTANT ONE?

by Florence-Marie Jégoux

When considering safety nets, we usually think about technical safety nets: STCA, TCAS, MSAW… And that is the way Safety I taught us to think about safety: technical means that are used to compensate for human failures in preventing incidents and accidents[1].

By this logic, humans are seen as the ones who make errors; the ones who are non-compliant with rules perfectly designed for the system to be safe.

Years ago, a controller in a Human Factors training workshop told me: *"HF appear only when something goes wrong, and when the controller has done something wrong"*. That started me thinking … He was right. As HF facilitators we only showed control examples where the controller had not chosen "the" best solution, and where, with hindsight bias, it is pretty easy to recalculate everything, in the comfort of an office with loads of time to rewrite the entire story, and find better options.

After the Hudson River ditching the findings led me to redesign the introduction of our HF workshop, to give an example of an incident where things went right, where pilots and controllers did the right things, where the human element saved the day. Yet, the challenge was to take things further.

In the French HF National Group, we design and build new HF training programs that are deployed over three-year periods. So for the following period, we decided to highlight the role of controllers as "safety nets", or "double checking elements", our French "safety loops", and to find examples of what they do "right".

We then asked controllers to tell us about events that had gone well, but they did not seem to understand what we were getting at. I was told *"You can't study that! That's just everyday work!"* Nothing to say, nothing to see, move along please.

And move we did. Our HF team studied how the controller is an asset in rectifying control situations, and after research, we managed to find exceptional cases where they sorted out tricky situations, such as in hub peak hours amid horrible thunderstorms.

However, these correcting loops do not solely occur during exceptional situations. Basically, in everyday tower or centre life, controllers sort out situations ***before*** things go awry, even before a technical safety net triggers an alarm signal.

We then came across the notion of a "weak signal" ("Informal and Ambiguous Information", Diane Vaughan, 2009). In a control position, weak signals are by definition not strong enough to trigger an immediate reaction. They are quiet warnings, subjective, intuitive, and difficult to identify. In a nutshell: nothing much to talk about. How a weak signal is interpreted depends on each controller's mindset, thus rendering the notion somewhat abstract and difficult to incorporate into regular training sessions.

In practice, weak signals can be heard as an internal dialogue: "Uh-uh, this doesn't look good", "I really don't like that". They can be felt as emotions: "hey, that's pretty scary", "I don't feel like doing that", " I don't know why, something bothers me". A weak signal may also manifest itself as a faster heartbeat, an impression of stress when checking particular data (speed, altitude, a slow response to a clearance modification …), a feeling of preoccupation, of concern, of annoyance, etc. These small intuitive perceptions can cause controllers to pay more attention to a particular situation, rectify a situation or act with foresight to a slowly changing one. The weak signal may be the stimulus which subconsciously encourages the ATCO to double-check more often, i.e. the uneasiness which is triggered by a VFR pilot's unsure tone of voice or the feeling of discomfort before noticing a slow catch up between 2 aircraft.

A weak signal, when heeded, can help trigger controller action, which may prevent the situation from deteriorating ***before*** it gets out of hand and the radar screen lights up like a Christmas tree!

Weak signals may help controllers to adjust their cognitive trade-off[2] and their ETTO: Efficiency-Thoroughness Trade-Off[3]. Through this constant real-time adaptation and flexibility, they can adjust their actions, reactions and situational awareness to all ATC situations.

The internal assessment of particular situations is an integral part of the decision-making process and is based on experience which heavily relies on implicit, automated skills. In HF training workshops, we render them explicit by talking about these weak signals. We debate about how they work and discuss the possibility that every controller has his very own set of signals. We explain that weak signals may be heard or ignored, as we all remember control situations where we told ourselves "I don't like doing that", but did it anyway, and then found ourselves in quite a predicament.

Control situations often raise doubts, and these doubts are precious tools in helping us to readjust situations. Disregarding them may lead to potentially dangerous outcomes. To be more aware and accepting of those signals can help the controller to assess a situation more clearly. Weak signals can be a useful tool in dispelling doubts: "Did I really hear the correct readback for the frequency change? I'd better ask him again…"

According to the pilots in charge of Human Factors training at one French airline, doubt dispelling is a helpful tool for pilots too. In many companies, pilots are expected to ask for a cross-check if only one pilot has heard the clearance given

1- For more information, please read "From Safety I to Safety II: A White Paper
2- Amalberti, 2001
3- Hollnagel, 2009; and the White Paper: Systems thinking for safety: ten principles, Moving towards Safety II

FLORENCE-MARIE **JÉGOUX**

became an air traffic controller in 2004 working in the ANSP of Western France for the French Civil Aviation Authority (DGAC). For the last 6 years, she has been working as a Human Factors coordinator and specialist for their training department. She also works for the French HF National Group and is trained in systems theory. She was a private pilot for 10 years.

JetBus 250 our radar is down and technicians are working on it...
However, I am following you on Facebook from my tablet...

by the controller. Better double-check than be sorry!

And flight attendants, ground staff, operations, company assistants, firefighters, refuellers, etc., are all part of the bigger aeronautical network, and therefore an integral part of safety.

On a smaller scale, the working team is definitely a safety net: TRM and CRM are completely centered on safety in teamwork. In control centers and bigger approach centers, the team as such is clearly seen as an asset to safety, with team members helping each other to stay ahead of the traffic, resolving blind spots and providing support when it is needed, notwithstanding the fact that it can be delicate to bring a colleague's attention to a seemingly dangerous situation.

The situation is very different in remote towers, where controllers work away from the rest of their team. The "team" is then spread out over different places and different jobs. This extended team can also be seen as a safety net, in spite of the fact that the team members are not physically in the same room. Here the systemic perspective takes on its full significance: understanding that disparate discrete activities are interrelated within a system where each part influences and interacts with the whole. In a complex world there's a bigger picture to one's personal work.

Thus, bearing in mind the controller's cognitive and collective work, let us consider the men and women in the aeronautical operational field as human safety nets, human safety nets which can take action in different situations:

- **before** technical safety nets are triggered. Before the red button flashes and screams "Do something about me! Do something about me! Don't you hear me? DO SOMETHING ABOUT ME!"
- **after** an incident, to get the situation back on track. In our HF workshops, we analyze a very tricky thunderstorm situation where 4 STCA flashed simultaneously. The controller came up with an innovative solution, in the nick of time to prevent the crashes!
- **when** technical safety nets do not "work-as-imagined", just because we live in a complex system where it is highly impossible for safety net specialists to describe and anticipate ***every*** ATC situation.

An exhaustive array of possibilities must be incorporated into a system's programs for it to respond safely in any and every situation and there will always be isolated cases which are not covered. In our HF training, we analyse a "work-as-done" situation where the STCA did not flash, and the controller in the position had a hard time figuring out what was happening. Speaking of overconfidence in technical systems… Technical safety nets are designed to be safety loops for human error. We should recognise that the reverse is equally important. The ATCO should be considered as a resource of the system, if not the most important and valuable one, as is recommended and encouraged by the Safety II approach.

Situational awareness, permanent Efficiency-Thoroughness Trade-Off, adaptability and flexibility to demands are the controller's everyday bread and butter. ATCOs, pilots, field experts, managers and all co-workers alike are part of this very complex system and fulfill their role as everyday safety designers.

Our Group favours an approach where controllers are acknowledged for their everyday positive actions, instead of being singled out when things go wrong. We also believe that it is high time we more thoroughly researched controllers' handling of everyday situations. The rapidly advancing field of neuroscience is likely to prove more than profitable in this area of study. The slap-on-the-fingers approach to safety has been the flavour of the month for too long. Let us move on to the Safety II perspective.

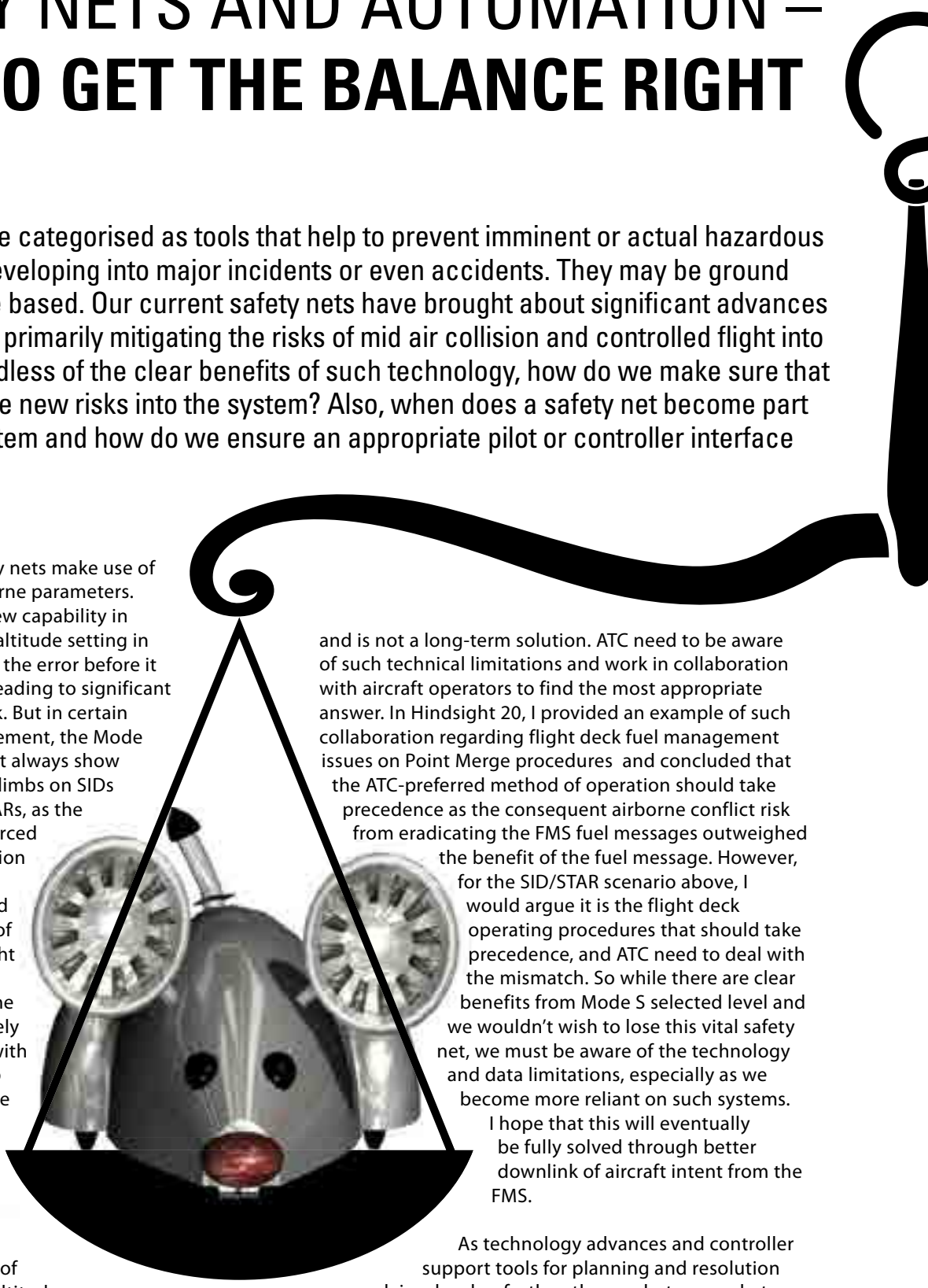
EDITOR'S NOTE:

A copy of the referenced document "From Safety I to Safety II: A White Paper" published by EUROCONTROL in 2013 may be accessed at: http://skybrary.aero/bookshelf/books/2437.pdf

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.

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 and Chairman of the ICAO ATM Operations Panel.

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.

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.

FLAVOURS OF **SHORT TERM CONFLICT ALERT**

by Ben Bakker

STCA came into being in the mid-1980s. At first a number of leading ANSPs incorporated STCA in their home-grown ATC systems. Soon ATC system suppliers incorporated STCA into their off-the-shelf products and today most ATC systems are equipped with STCA.

It was 2007 before the following definition of STCA was generally adopted. *STCA assists the controller in preventing collision between aircraft by generating, in a timely manner, an alert of a potential or actual infringement of separation minima*.

But having a common definition doesn't mean that there is or ever will be a 'one-size-fits-all' STCA. In order to be effective, STCA needs to be adapted to the environment in which it will be used. This adaptation is in fact a balancing act to find the optimum compromise between warning time and proportion of nuisance alerts.

So, how many flavours of STCA are there? Is the answer as many as there are STCA systems in operation? A typical ATC unit contains TMA sectors as well as en-route sectors. Traffic patterns are quite different: lower speeds, more turns and vertical evolution in TMA sectors and higher speeds, less turns and vertical evolution in en-route sectors. The same STCA system will have to serve both types of sectors and at least in theory each individual sector may have its peculiarities that warrant an ever so slightly different flavour of STCA. Let's stop counting and move on to tastes.

Sweet & Sour STCA

A recent study to which many European ANSPs contributed identified three strategies for adaptation of STCA. The first one could be dubbed 'Sweet STCA' and will lead to early STCA alerts for any potential infringement of separation minima. Its sweetness stems from the fact that there will frequently be nuisance alerts – a term used to indicate that the situation is correctly detected but not unsafe. But wait, another way of looking at these alerts is that they provide gentle reminders that the situation may become unsafe in the near future: better safe than sorry.

The opposite taste is 'Sour STCA' which will provide late alerts and only for potentially significant infringements of separation minima. Nuisance alerts are now less frequent – most alerts are not-so-gentle warnings that safety margins are eroding: somebody probably made a mistake.

It's not difficult to guess that the third strategy provides 'Sweet and Sour STCA'. This is an intermediate solution both in terms of warning time and separation protection. So far we have looked at the predictive aspect of STCA. Many STCA also will generate an alert in case of an actual infringement of separation minima…sweet or sour?

STCA Turning Bitter

Choosing the appropriate strategy for a given environment involves operational considerations, including safety aspects and human factors.

Simply put, every additional aircraft in a sector doubles the number of potential conflicts. The proportion of vertical evolutions and the number of crossing routes adds to the complexity. More complexity necessitates moving further away from sweet towards sour.

Other, more indirect considerations are related to safety culture. If the chosen strategy is less appropriate for the environment and if there is a 'naming-and-shaming' safety culture STCA turns bitter. STCA does the naming, making it easy for management to do the shaming. In the past this scenario has led to stand-offs between controllers and management, sometimes leading to the worst possible outcome from a safety point of view: disabling STCA in the entire airspace or in significant parts of it.

Clearly, a 'just-culture' attitude to safety is an enabler for avoiding the above scenario, however not a guarantee. Management must also understand the need for establishing, implementing and maintaining an appropriate strategy, and make sufficient resources available. If not, another scenario may unfold: controllers (some more than others) may ignore or delay their response to alerts. Again, safety suffers.
Why is an appropriate strategy important? Because it makes STCA effective and this in turn makes an important contribution to safety.

Adding a Pinch of Salt

Every dish needs a pinch of salt to enhance the final taste. For STCA the final taste is the human-machine interface. An otherwise effective STCA becomes ineffective if the alert doesn't draw the controller's attention when this is urgently needed.

Some of the human factors involved are illustrated in the 'inattentional blindness experiment' conducted by Simons and Chabris in 1999. Observers were shown videos and tasked to only count the number of passes made by players with white or black shirts. At some point in the video an unexpected event occurred: either a tall woman carrying an umbrella or a shorter woman wearing a gorilla suit walked through the scene. More than half of the observers failed to notice this.

One way of drawing attention is by complementing visual information with aural cues. Visual information consists always of some kind of indication in the track label on the situation display and is often complemented with additional information about the conflict, such as changes to speed vectors or predicted miss distance. Aural alarms were once limited to buzzers, bells and sirens, and these were not popular. However, now, the possibilities for aural alarms are almost limitless. As with cooking, proper dosing the 'salt-of-STCA' is the secret to customer satisfaction.

It is often said that tastes differ. Some people love eating fish, others hate it. In any given ATC unit, controllers are unlikely to have identical opinions about their STCA. That doesn't matter if a large majority find that their STCA is well-flavoured, but it's time for action if this is not the case. After all, sooner or later you may need STCA to save your day, no matter if you are a controller, a pilot or a passenger!

BEN **BAKKER**

has been working on increasing the effectiveness of ground-based safety nets in Europe (and beyond) since shortly after the Überlingen mid-air collision in 2002. As secretary of the related working arrangements, under the auspices of the EUROCONTROL ATM Safety Team, Ben was instrumental in the development of the EUROCONTROL specifications and supporting guidance material for ground-based safety nets.
He as been employed by EUROCONTROL in its Brussels Belgium headquarter as senior expert in the ATS Unit of the ATM Directorate since April 1995.

SAFETY NETS TO PROTECT AGAINST FATIGUE

by Jean-Jacques Speyer

Introduction

We can easily imagine the extent of the challenges faced by the lone Solar Impulse 2 Pilot André Borschberg during his recent trans-pacific journey of nearly 118hours in the air. Working alone in his single-seat cockpit, he could rest for no more than 20minutes at a stretch – and then only at lower altitudes where an oxygen mask was not needed in the unpressurised cockpit. Monaco's Control Centre was keeping a careful watch over the failed autopilot monitoring system to protect the flight against critical stability upsets during his occasional 'catnaps'. Narrow margins indeed, with only 15 seconds to react in case of trouble – 6 to 8 seconds for the pilot to wake up and take over with a 4 to 8 data transmission time to Monaco. A reliable safety net to protect against fatigue, would have come in handy to protect the Solar Impulse and its pilot at rest.

With the advent of the FRMS, pilot fatigue is now clearly recognised as one of the major hazards that can impair safety, crew performance and pilot situational awareness. Back in the early 1990', physiological recordings made during 156 long-haul flights in a project sponsored by the French DGAC and performed jointly by Airbus and the University Rene Descartes in Paris had shown that reductions in alertness were frequent during flight, including the descent & approach phase. But most decreases in alertness were happening during the monotonous part of cruise and could even occur simultaneously for both pilots at the controls. Specific recommendation cards were designed as a function of number of time zone crossings, day or night-time departure, length of stay, crew augmentation. This underlined the positive impact of operational guidelines on pilot alertness and wellbeing. The findings of the project were eventually gathered together in a comprehensive report published by Airbus in French, English[1] and Chinese to help manage long haul fatigue.

One of the main recommendations promoted in these guidelines is based on the alternation of crew rest and activities, including cockpit napping. The efficiency of cockpit napping was first emphasised by NASA about thirty years ago. However, one of the main drawbacks of cockpit napping in two person crews is that it could contribute to increase cockpit monotony (reduced communications, lower light intensity…) and hence decrease alertness of the sole pilot remaining at the controls.

Monitoring Pilot Alertness

Overall, it was considered that a safety net was needed to cope with these various phenomena. Fail-safe monitoring of both pilots could both help manage the risk of simultaneous sleepiness encounters by protecting the alertness of the remaining pilot when their colleague was engaged in a cockpit nap. The Electronic Pilot Activity and Alertness Monitor (EPAM) was intended to provide exactly this support using a concept that could certainly be replicated to the case of ATC Controllers working in pairs.

The activity monitor included two modes. In the first mode, pilots' interactions within the flight deck were continuously monitored. It was based on the assumption that a pilot who is dozing off will, at some point, tend to interact less with their aircraft systems. Connected to different systems of the aircraft (Flight Management System, Electronic Centralised Aircraft Monitor, Radio Management Panel, etc…) the device tracked tactile Human Machine interactions. In a first mode of use (the ALERT function), if no interaction was detected with at least one of these flight systems after a pre-set period of 5, 10 or 25 minutes depending on the flight phase (or at pilot discretion), a precautionary visual alert would be generated. Then, after a further minute of inactivity, an aural warning activated. A second mode (the TIMER) could be considered as an alarm clock or egg timer which the pilot who planned to nap would activate. When the alarm sequence in this mode would occur could be programmed but could not be longer than 45 minutes to avoid sleep inertia[2]. Here, the EPAM was seen as a means to help manage rest-activity cycles that involve naps.

The second part of the device tracked alertness using in-flight video monitoring of pilot eye movement. The reason for this was that pilot inactivity alone would not be sufficient to effectively detect all decreases in alertness, since some pilots could still having some interaction with aircraft systems even in low alertness phases. It is a method of dealing with a problem found in other modes of transport and comparable to the function of the dead man's handle found in train drivers cabs… Using specialised image processing software, various parameters such as eye movement and eyelid closure can be automatically analysed. Initial studies in car driving in the late 1990's had already shown that just a few measurements were enough to detect low alertness stages with the nature of these stages depending on the extent of loss of alertness.

1- a copy of "Coping with Long Range Flying" is available at http://www.skybrary.aero/bookshelf/books/3214.pdf
2- Sleep inertia refers to a feeling of grogginess after awakening typically lasting 15-30 min's. During this period, levels of capacity are reduced even to perform simple everyday actions.

JEAN-JACQUES **SPEYER**

MS El & Mech Eng, VUB, Brussels, Belgium, MS Aero & Astro, MIT, USA, DU HF's & Ergonomics, Univ René Descartes, Paris, France. After an airline start as B707 Flight Engineer, JJ Speyer moved on to Flight Operations Engineering & Certification at Airbus from where he retired as Senior Director Airline Consulting, Fuel & Flight Efficiency at the end of 2009. He is currently Professor in Aircraft Specification & Certification at the Vrije Universiteit Brussel.

Early drowsiness is more associated with strabism[3] and long-duration eye fixations while sleepiness is mainly characterised by increased eyelid closures and slow eye movements.

The EPAM device was subjected to operational evaluation during long-range A340 airline flights in the late 1990's and early 2000's. Some 22 round trips were performed on the Brussels-New York route working with volunteer pilots from the former Belgian airline SABENA on rosters known for their significant fatigue effects: early evening flights departing and late evening flights heading back to base.

Airbus flight trials were also held using an A340-300 test-bed in 1999 during a FANS flight around the globe and the usefulness of the device was monitored over 5 very long sectors. Finally, an A340-600 route-proving return flight was conducted to Hong-Kong in April 2002 to test the concept in terms of HMI with a 'Wizard of Oz' experiment. This consisted of a research experiment in which subjects interacted with a computer system that they believed to be autonomous, but which was actually being operated (or partially operated) by an unseen researcher in the aircraft cabin. This technique enabled an evaluation of the usability of the device whilst recognising that it may not yet have reached technical maturity. Usefulness & usability got high marks from this.

Physiological parameters such as: electro-encephalograms (EEG), electro-oculograms (EOG) and Heart Rate Variability (HRV) were continuously recorded to evaluate the impact of the EPAM both in terms of its sensitivity to fatigue effects and in respect of its ability to maintain alertness. Simultaneously, detailed observations of operating crew-members were carried out to monitor their activity patterns using dedicated Aircrew Data Logging (ADL) software and to re-launch the system's timed ALERT function after crew physical tasks.

Data processing initially focused on sleep quantity and quality during in-flight naps, on in-flights alertness decrements and on EPAM alert warning occurrences. Figure 1 shows the hypnogram during scheduled in-flight nap with an example of results for a New York - Brussels leg with 3 types of data:

- The occurrence of sleep stages 1 to 4[4] (no REM sleep was observed during these flights). When the pilot is supposed to be alert, some stage 1 sleep can occur – this corresponds to "micro-sleeps".
- The inactive time which would yield EPAM warnings for the different selectable periods: 10, 15, 20 or 25 minutes.
- The alpha/delta ratio from the EEG – when the pilot is supposed to be alert, an increase of this ratio represents an alertness decrement (i.e. an increase of alpha power) but during in-flight naps, a decrease of this ratio corresponds to deeper sleep (i.e. an increase of delta power). Increases of this ratio mean lighter sleep.

Figure 1 shows that potential alerts would have occurred around micro-sleeps after at least 15 minutes of inactivity. The very first micro-sleep is not related to any significant increase of inactivity time. This finding confirms the need for additional information related to the pilot's 'internal state', which it was considered could best be traced by monitoring eye movement.

Figure 2 shows an example of two parameters derived from eye movement video recordings, the duration of eye closures and the duration of eye blinking. First results suggested that an increase in the prevalence of these two parameters could reliably predict occurrences of micro-sleep. Analysis was also conducted on other parameters such as eye fixation and strabism to aid the derivation of the best algorithm.

The initial results of this work confirmed that the EPAM concept was feasible finding:

- that reductions of pilot interactions with cockpit interfaces are often related to decreased alertness which can be detected by physiological observation.
- that the measurement of pilot-system physical interaction alone is not sufficient to predict loss of alertness.
- that loss of alertness detection should employ alternative means such as eye movement tracking.

3- Strabism is the inability of both eyes to focus on one object producing the effect of cross-eyes often linked to a discrepancy between accommodation and convergence.

4- The constituents of the EEG trace being:

alpha (7.5-14Hz) :	Deep Relaxation Wave
delta (0.5-4Hz):	Deep Sleep Wave
beta (14-40Hz):	Waking Consciousness & Reasoning
theta (4-7.5Hz):	Light Meditation & Sleeping
gamma (above 40Hz):	The Insight Wave with Rapid Eye Movement Sleep

Further R&D indicated that revived alertness following EPAM cautions & warnings could induce increased situational awareness when pilots performed a systematic flight parameter review procedure as typically required after an absence from the cockpit.

It can be concluded that if pilot in-seat napping is supported, it should better be backed up with a device similar to the tested concept. However, no such systems have yet been developed. And we didn't get through the ten steps towards technical maturity. Somehow, the EPAM concept was ahead of its time since the pilot community was quite worried at the time that this would be a tool to be used to extend flight time & duty limitations as ULR was coming of age. It was indeed well before the heydays of FRMS.

In retrospect, aircraft manufacturers - who had already their plate full at the time - should have teamed up with other industries manufacturing cars, trucks and monitoring facilities in an effort to reach technical maturity and hence dampen costs. Back in 2002, a student team from Brussels' VUB University did their Master's Thesis with me at Airbus on "eye seeing machines" and we even received an award from an electronic display manufacturer that considered this work to be the most innovative of the year.

Thinking about it, this concept should certainly not be restricted to flight crews but could be extended towards Air Traffic Control where difficult rosters do exist for a fact. With today's safety culture we also have the evidence to believe in the need for such protection nets. But it would only work with a solid safety culture not even thinking of identifying any personnel origins of the traces. Only then! With full confidentiality… S

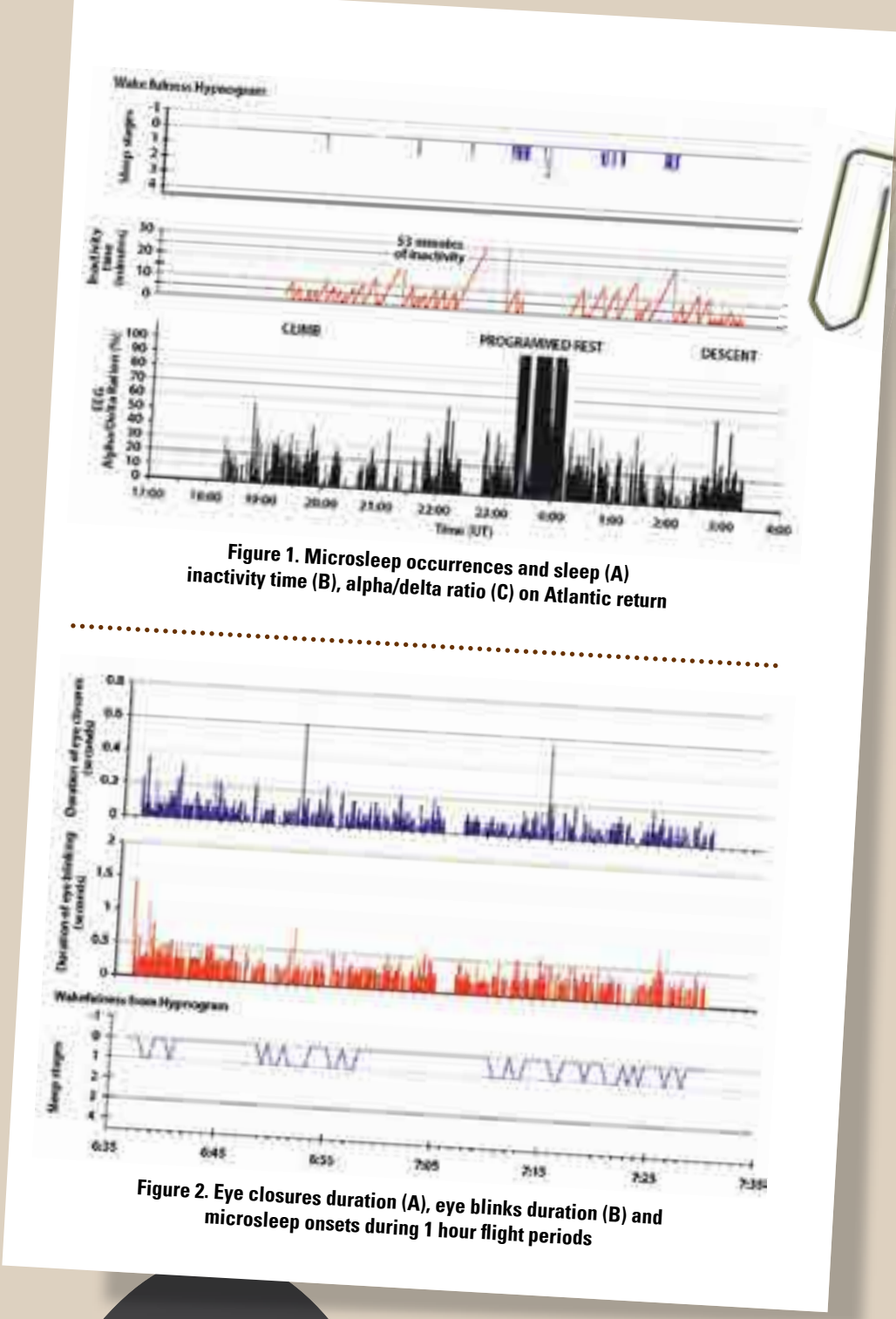
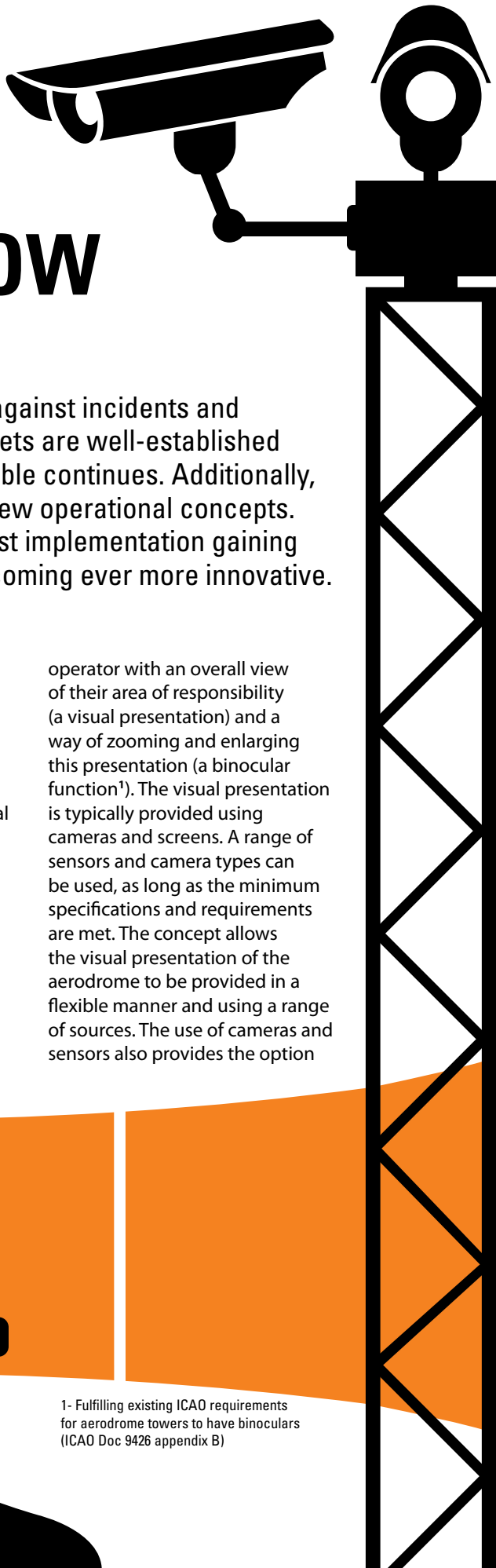


Figure 1. Microsleep occurrences and sleep (A) inactivity time (B), alpha/delta ratio (C) on Atlantic return

Figure 2. Eye closures duration (A), eye blinks duration (B) and microsleep onsets during 1 hour flight periods

REMOTE TOWER TECHNOLOGIES AND THE SAFETY NETS OF TOMORROW



by Raluca Tudorica & Rory Hedman

In aviation, safety nets act as the last system defence against incidents and accidents. Current ground-based and airborne safety nets are well-established and development to make them more efficient and reliable continues. Additionally, future air traffic control safety nets may emerge from new operational concepts. One such concept is Remote Tower, with the world's first implementation gaining operational approval earlier this year and research becoming ever more innovative.

The arrival of Remote Tower is encouraging a re-think of what has been a convention in air traffic control since the first controlled civil airports were introduced in the 1920s at Croydon airport in the UK – that the Tower should be located at the airport being controlled.

Remote Tower enables the provision of ATS from a facility independent of the airport. Removing the controller from the aerodrome control tower means they can no longer use the out-the-window view to visually survey the airport and its vicinity.

When operating remotely the controller is expected to provide ATS to the same level as in current operations and to enable this, the remote facility has to provide the controller with a means of visual observation and sufficient situational awareness.

Before exploring a potential safety net that could emerge from Remote Tower, let us first look at the various technologies used enable and support Remote Tower Operations.

The provision of ATS in a remote environment requires, as a minimum, a means of providing the operator with an overall view of their area of responsibility (a visual presentation) and a way of zooming and enlarging this presentation (a binocular function[1]). The visual presentation is typically provided using cameras and screens. A range of sensors and camera types can be used, as long as the minimum specifications and requirements are met. The concept allows the visual presentation of the aerodrome to be provided in a flexible manner and using a range of sources. The use of cameras and sensors also provides the option

1- Fulfilling existing ICAO requirements for aerodrome towers to have binoculars (ICAO Doc 9426 appendix B)

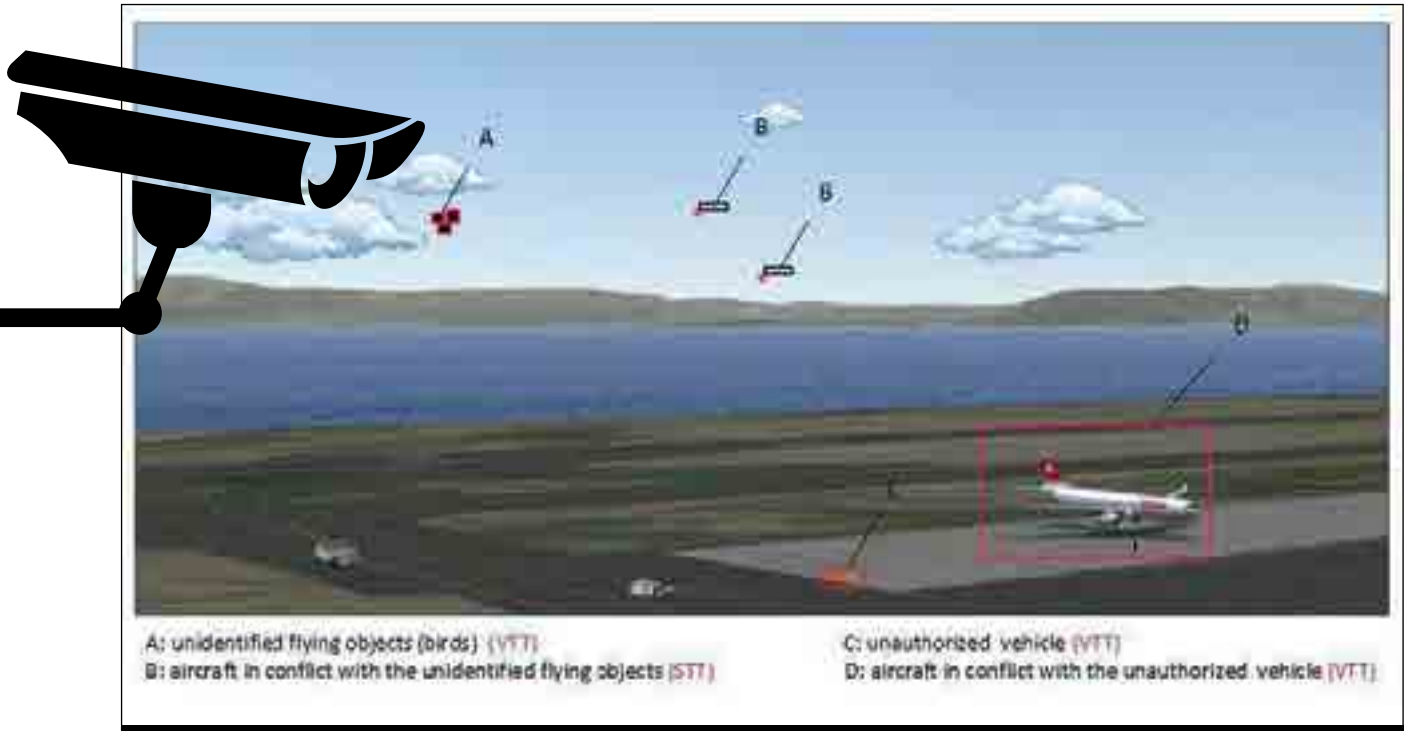


Figure 1: How can Target Tracking act as a safety net?

for additional situational awareness at designated points such as landing thresholds or to cover blind spots not visible from the standard tower.

Other technology is additional and, although not required to maintain safety or for the provision of ATS, can be applied to improve situational awareness, concept acceptance, working methods and capacity. For example infra-red technology and various sensors can be used to provide a variety of viewing angles. Also, the use of sensors and displays allows information such as meteorological data (QNH, Max wind speed, compass roses, etc.), aerodrome layout (highlighted runways and taxiways during low visibility and darkness and labels next to taxiway exit points etc.), target tracking information (for cooperative and non-cooperative targets) and other data may be overlaid onto the visual presentation. All of the above are considered by current research developments. Additionally, technologies such as the use of 3D monitors, speech recognition, eye tracking are also being considered for future Remote Tower applications.

The potential of Remote Tower Technologies as Safety Nets

Seeing the potential of these various forms of technology, and being actively involved in Remote Tower development, we dug deeper to see if any of these technologies are "safety net material".

Given the current stage of research, Target Tracking comes the closest to what it is expected today from a safety net. By piecing together current research and ideas we look into the What? and How? of a Target Tracking safety solution. As part of the Remote Tower SESAR research programme, Target Tracking has been developed and refined to offer support for ATC in more complex working environments. Initial development was prompted when the research programme started to look into Multiple Remote Tower operations, where controllers felt that a technology which allowed them to quickly view the position of traffic and obstacles, both on ground and in the air, would be very useful.

This technology is based on two distinct capacities: Visual Target Tracking and Surveillance Target Tracking. Neither is unique to aviation, camera tracking algorithms which track targets in 2D have been available for more than 30 years and radar based tracking for much longer. Yet the way in which these technologies are used in Remote Tower operations, to assist airport operations and the provision of an aerodrome control service, is unique.

Visual Target Tracking (VTT)
This refers to the technical capability to detect the motion of an object, such as light aircraft and vehicles which may not be equipped with a transponder (non-cooperative targets). In the small rural airports, targeted by the first Remote Tower applications, visual tracking may also be valued for the targeting of birds, large animals, and other moving obstacles.

Surveillance Target Tracking (STT)
This refers to the use of positioning sensors, such as Advanced Surface Movement Guidance and Control System (A-SMGCS), to determine the location of co-operative targets. This feature might prove beneficial for larger airports, where traffic consists mostly of transponder equipped aircraft.

The information gathered from VTT and STT can be displayed in a number of ways. Above is a basic illustration based on the current HMI used to display tracking information in Remote Tower, although of course this may look very different if integrated into a local tower. We can see how conflicts can be displayed, such as possible bird strike (see unidentified objects and incoming aircraft), as well as a ground conflict (an unauthorised vehicle on the taxiway). The information coming from Target Tracking could the integrated onto various visual displays or even overlay the control tower windows. Information from the VTT and STT can be combined with labels, text and other visualisation in order to keep track of targets.

In its current form Target Tracking is only a controller support tool. Yet with improvements in reliability, it may be possible to integrate such tracking technologies into safety net applications. One such application may be a form of Aerodrome Area Incursion Alarm safety net covering both the aerodrome surface and the airspace in the vicinity. Similar to Area Proximity Warning (APW), a current well established ground based safety net, Target Tracking could provide controllers with short term notifications of conflict situations within designated areas.

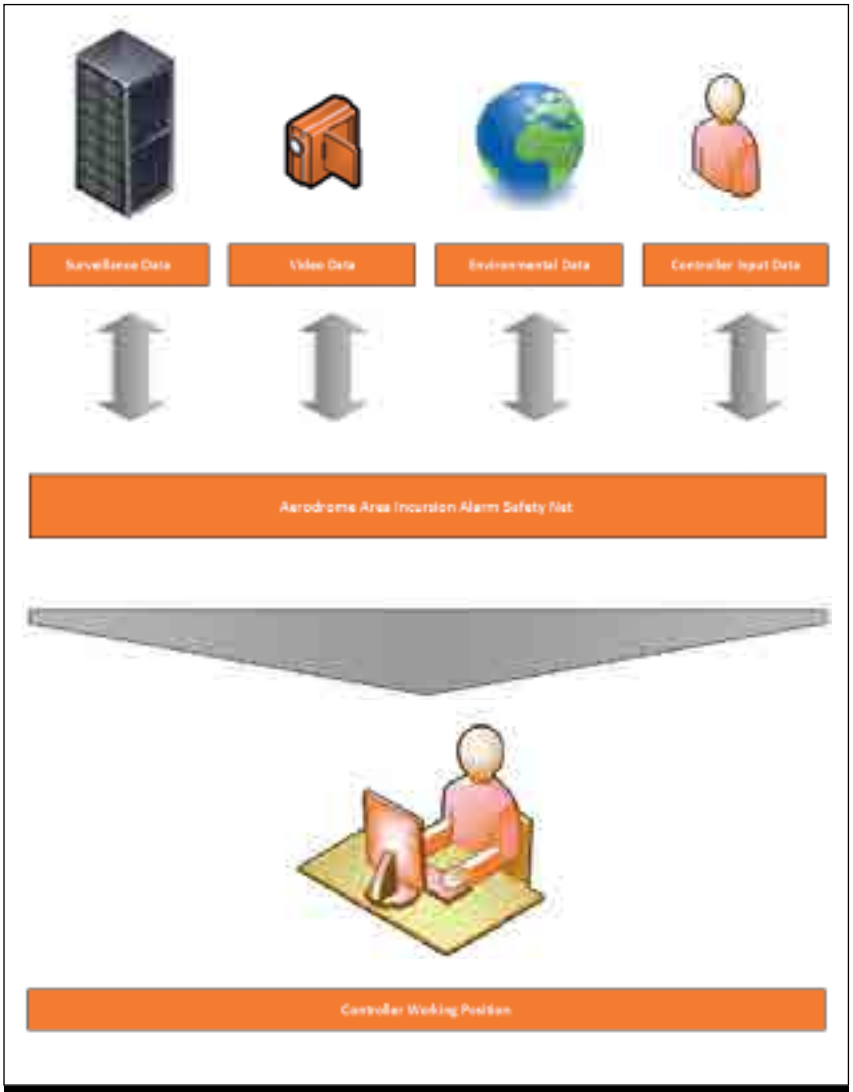


Figure 2: Working diagram for Aerodrome Area Incursion Alarm Safety Net

Current Visual Target Tracking technologies use 2D information gained from cameras placed at the airport. In order for such technologies to be adapted for use in an Aerodrome Area Incursion Alarm, the sensors must be able to identify specific areas and track movement in relation to the entire airport surface. For this, a 3D map of the airport is required. An arrangement of cameras, sensors and other specific surveillance devices could be used to create such a 3D view, which would allow visual tracking algorithms to run in the background and track movement, supported by surveillance sensors. The use of an accurate 3D map of the airport environment would enable alarms to be set off at the appropriate time.

The primary role of such an application could include:

- Warning the controller about unauthorised penetration transponder equipped movements into unauthorised areas of interest (runways, taxiways, CTR etc.);
- Warning the controller about unauthorised penetration non-cooperative movements into unauthorised areas of interest (runways, taxiways, CTR etc.).

Whether a viable safety net option will come from such Target Tracking technologies is not yet clear. But we can theorise about the actual application of such a safety solution and the key considerations required for such a tool.

As in Figure 2 the Aerodrome Area Incursion Alarm Safety Net could obtain its information from various sources. For instance, surveillance technology and an arrangement of camera sensors (video data) could provide the important high-resolution 3D map of the airport. The 3D airport map would also include all the airport geographic/environmental data to enable specific areas of the airport to be highlighted as safety-critical.

When cameras/sensors detect new objects in areas defined to be safety-critical, they could be recorded by the system and their status monitored. To maximise the effectiveness of the system as a safety net, it would also need to include track prediction so that the intended path of targets

could be forecast. If the object is predicted to have a dangerous behaviour or be moving in an erratic manner, then the controller would be notified. Additionally, if a continuously scan of the airport is being made by visual and surveillance sensors then non-moving objects could also be detected.

However, at the moment the technologies required are not available. Search algorithms still identify all targets continuously and without distinction (for example environmental data such as moving clouds, trees blowing in the wind etc.).

A paper on "Geometric Modelling for 3D Support to Remote Tower Air Traffic Control Operations", published by SINTEF (also involved in the verification work within SESAR project P12.04.09) explains how their research may facilitate the 3D mapping of the airport. These techniques can also support object recognition by generation of size and speed information.

Predicting aerodrome area incursions is complex and involves many factors such as object behaviour modelling. The first stage of development may target low capacity utilisation, as was the case for Remote Tower, due to a reduced number of targets and complexity. With faster more accurate algorithms, safety nets based on 3D target tracking may be implemented in more dense, increasingly complex environments. However, such environments also include a higher percentage of cooperative targets so may not always provide the most challenging implementation environment.

Predictive Target Tracking could improve controller confidence and may act as an enabler for Remote Tower operations in a wider range of environments (i.e. larger airports with high traffic density and Multiple Remote Tower applications) and importantly would allow tracking technologies to be used as a form of airport safety net.

Another aspect that needs to be addressed is how the algorithm could identify that the predicted track of an object was no longer in line with expectations. The solution to this is likely to involve integration with controller input data. Considering the human in the loop, it is clear that in order for such a solution to be an effective safety net, it should not rely upon manual intervention by the controller. Any required inputs would have to be normal inputs made by the controller as recorded on electronic flight data strips or data-link so as not to increase workload or alter working methods.

What next?

We think that as a possible contributor to or even as the primary basis of a future safety net, Target Tracking is very promising. Yet, there are still many factors that need to be considered in order to make this type of safety net application a reality. Some key considerations include:

- The Impact on Controller Human Performance;
- The Visual Presentation of the alert/s in the CWP (particularly in local tower environments);
- Integration with existing systems and working methods;
- HMI (alert sounds, use of colours, etc.);
- Ensuring nuisance alerts are excluded and reliability is ensured;
- The business case in terms of cost of implementation;
- Performance benefits

... and many more.

Target Tracking is not the only feature to emerge from the Remote Tower concept with the potential to improve safety. Some of the other technologies it, embraces might be integrated into safety net solutions or used in daily operations as support tools and safety enhancers in their own right.

With the recent implementation of Remote Tower and other concepts to come out of SESAR, innovation and change is in the air. Now is the time to capitalise on this to fuel further cutting edge developments, not forgetting to explore all avenues for their safety potential.

RALUCA-ELENA **TUDORICA**

is Master's student in Air Transport Operations at Delft University of Technology and is currently doing an internship with Think Research Ltd. where she is looking into Remote Tower Research and Implementation. In 2013 she was a trainee in EUROCONTROL's Safety Unit where she supported Safety Maturity activities and the development of the Aerospace Performance Factor.

RORY **HEDMAN**

is a Lead Analyst at Think Research Ltd. His primary expertise is in Remote Tower operations, providing support as a contributing author to the SESAR operational concept document (OSED) and validation documents for simulation exercises and live concept trials in Sweden and Norway. He also has involvement with Remote Tower pre-implementation, standardisation activities (via EUROCAE working group 100) and conformity assessment.

EDITOR'S NOTE:

More on 'Remote Tower Service' can be found at: http://www.skybrary.aero/index.php/Remote_Tower_Service

COLLISION AVOIDANCE FOR LIGHT AIRCRAFT

by Volker Huck

Imagine flying a small aeroplane, only equipped with a Mode-C or Mode-S transponder and all of a sudden you realise you are on collision course with a big airliner. Don't try to avoid it by climb or descent, because the airliner will (in 99 of 100 cases) have TCAS II on board and activated...

This guides pilots to avoid other aircraft using resolutions in the vertical direction and it works on the vertical speed of potentially conflicting aircraft so if you change your vertical speed, it has to modify the resolution given to the other aeroplane and may affect the miss distance (and your composure!). It is also often very hard to judge visually whether you should try to pass above or below.

Avoiding the other aircraft by turning left or right might be better, but maybe not. Yes, the small aircraft may well get visual contact with the big one earlier than vice versa – although the airliner crew will have a traffic display showing the 'intruder'. However, they will be prioritising the accurate flying of any avoidance manoeuvre over visual acquisition once they get one. And an airliner goes faster but consequently takes more space to turn, so it may be hard to believe, but it may be best to do nothing!

Effective collision prevention starts on the ground. If practicable, avoid designated "hot spots" and if you can't then be especially careful when near them - maybe involve your passengers in looking out for traffic. Clean the windscreen – and the side windows - and make sure your seat is properly positioned in height so that you can see everything – and if the adjustment is insufficient, then use a

DR VOLKER **HUCK**

is an ATM Expert at EUROCONTROL HQ in Brussels, working on collision avoidance systems. He has been an active GA pilot since 1977 with flight experience in Europe and the USA. Previously he worked on airport movement planning at German Aerospace Centre's Institute for Flight Guidance in Braunschweig.

pillow. Absolutely don't put stuff on the glare-shield and mentally process radio transmissions even if you think you are not involved. Finalise all your pre-flight preparation before take-off. There is a lot of really useful guidance on the internet. Start with: http://www.skybrary.aero/index.php/Visual_Scanning_Technique

The collision hazard is a nasty problem for light aircraft even if mid air collisions do not contribute much to the risk of flying statistically. Whilst in theory, you could install TCAS II, it costs much more than the average light aircraft. Some aircraft owners install the earlier version of TCAS, TCAS I but this just gives traffic alerts without any guidance on what to do about it The many private pilots flying typical light aircraft will use either:

- **Passive collision avoidance systems or**
- **FLARM or**
- **ADS-B IN (mainly in the USA) or**
- **Combinations of the aforementioned or**
- **Nothing but "see and avoid" (the majority).**

Passive Collision Avoidance Systems

receive (but do not interrogate) active transponders in the vicinity. They have to rely on another source to interrogate the intruder's transponder which means that there must be either an SSR (Secondary Surveillance Radar) or a TCAS-equipped aircraft in the vicinity.

These systems display approximate distance (derived solely from signal strength, see photo!), relative altitude and vertical trend and may display the approximate direction of the intruder (like the one on the right side of the picture). Intruders without transponders will not be displayed at all.

FLARM

FLARM is amazing. It is small, smart and effective, but only works among FLARM-equipped aircraft. It was designed for gliders which fly much closer to each other than other GA-aircraft and are also slower. It is based on broadcasting GPS position, augmented with barometric altitude. The principle is similar to ADS-B (see below chapter), but the alerting logic is specially designed for gliders. Another difference is that FLARM uses frequency-hopping in an open public-use frequency band, which is unprotected. The legal restriction on the use of that band is mainly signal strength.

Automatic Dependant Surveillance – Broadcast (ADS-B)

ADS-B signals can be detected with portable receivers and displayed on many navigation displays, including navigation apps on portable phones and tablets.

Principally, ADS-B signals are only available from equipped aircraft. The ADS-B OUT mandate in Europe is limited to large aircraft. In the USA, ADS-B OUT equipment is mandated for all operations that currently require a Mode-C transponder - which roughly means operations above 10,000ft QNH, in Class B airspace and in and above Class C airspace - from Jan 1st 2020. However, it would be premature to expect ADS-B OUT equipage on all aircraft that carry a Mode-C transponder today due to the cost. Many light aircraft pilots may well decide to stay away from mandated airspace. However, at least in the USA, ADS-B will be the main system support for collision avoidance in

Passive Collision Avoidance System PCAS

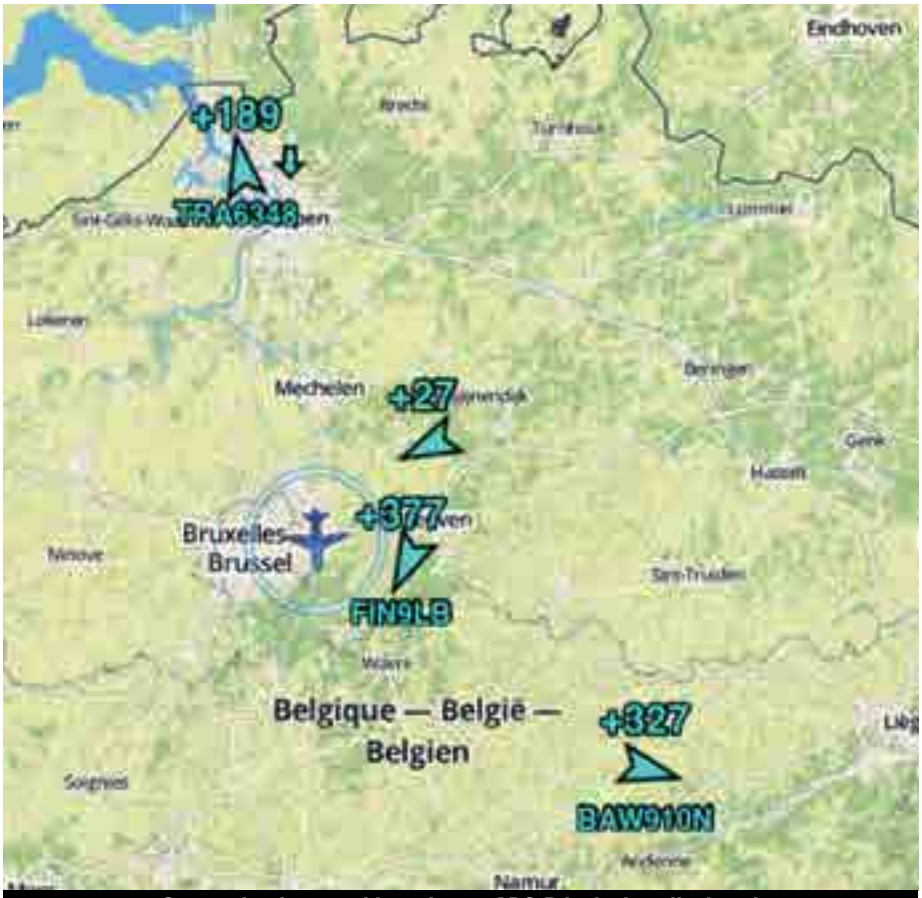
Source: Wikipedia

FLARM

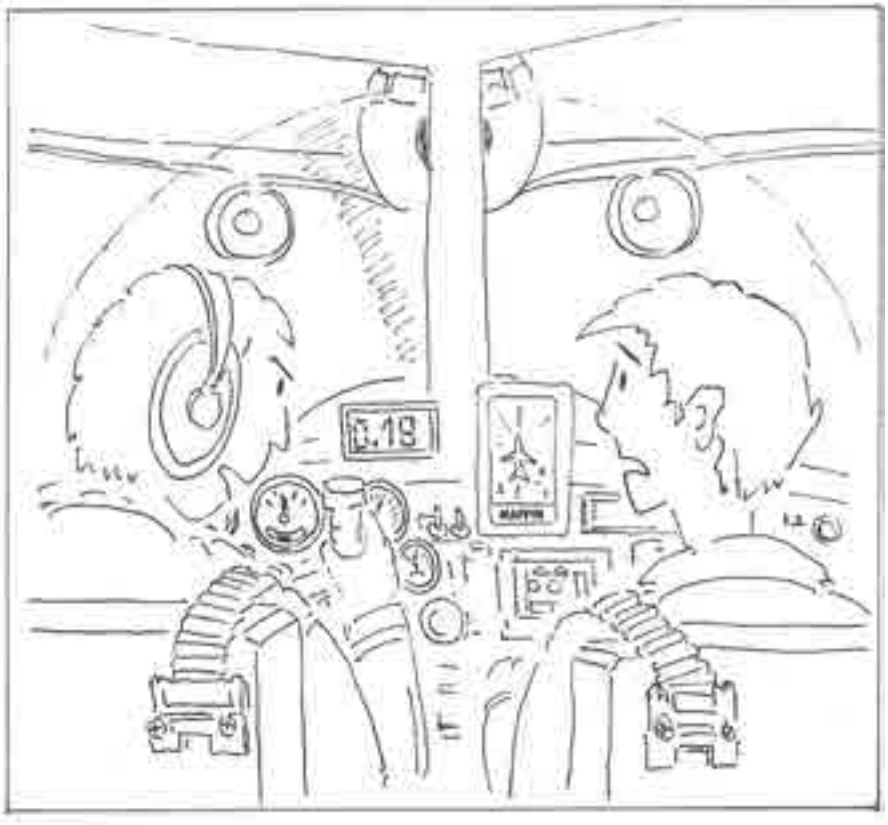
the long term (for light aircraft). In some areas of the USA the position of Mode-C equipped aircraft without ADS-B OUT is rebroadcast and can be received by ADS-B IN.

Low Power ADS-B Transceiver (LPAT)

The installation cost for ADS-B OUT is to some extent due to the mandated system requirements for position accuracy and signal integrity etc. Other equipment is targeted below the standard and cost of the ADS-B out mandate. Flight trials are already under way with a Low Power ADS-B Transceiver (LPAT) being developed by UK NATS and Funke Avionics. This is a light-weight, battery powered carry-on device that is affordable and simple to use and which provides the minimum functionality you need to see and be seen by other traffic. It can also provide warnings against other suitably-equipped aircraft. It could become small enough to be carried also by remotely piloted aviation systems (RPAS).



Screenshot from a tablet using an ADS-B in device, displayed via an air navigation application (here: ForeFlight)



Let's play chicken, shall we!

Conclusions

Mid-air collisions do not contribute much to the risk of flying. The National Transportation Safety Board of the US has 116 fixed wing aircraft involved in a collision on record over the last 10 years before 2015 (http://www.aopa.org/asf/ntsb). Most of them happen in daytime VMC in the traffic pattern of an airport. (http://www.aopa.org/-/media/Files/AOPA/Home/Pilot-Resources/ASI/Safety-Advisors/sa15.pdf)

There are different technical solutions to avoid them, but none of them work with all other air traffic. The most comprehensive effort is being undertaken in the USA with the ADS-B OUT mandate in 2020.

THERE IS NO CAUSE FOR ALARM IF YOU HAVE SOME INFORMATION ON ALERTS TO BEGIN WITH

by Roger Lane

TWO SCENARIOS BASED ON ACTUAL EVENTS

1. It is night time, the controller has lined an aircraft up on Runway 27, a taxiing aircraft takes a wrong turn and then doesn't reply, the controller is busy coordinating with a colleague and trying to contact the wayward taxiing aircraft when another flight calls " finals Runway 27", it is cleared to land and a short time afterwards 2 aircraft are destroyed and 34 people dead.
2. An aircraft has just landed in thick fog (Low Visibility Procedures are in force) and clears the runway and is transferred to the Ground Controller. Another flight is cleared to take off from the same runway. The arriving aircraft is given instructions to taxi but the flight crew are unfamiliar with the airport layout and turn left too early, taking them on a taxiway that leads them back onto the runway. The flight crew sense something is wrong and stop as they enter the runway just in time to hear the departing aircraft pass metres above them. Luckily nobody was injured this time ….

Introduction

In Europe most major airports now have an Advanced Surface Movement Guidance and Control System **(A-SMGCS)** with:

- **Surveillance** which allows the Controller to see the position and identification of mobiles on the airport surface.
- **Runway Incursion Monitoring System (RIMS)**, which provides the controller with a short term conflict alert, triggering 30-45 seconds before potential impact depending on the weather conditions and based on the surveillance position of the mobiles.

In addition to A-SMGCS, other systems such as Electronic Flight Strips **(EFS)** has been installed at many European airports which means that instructions, such as Cleared to Line Up, Take Off and Land, given by the controller are now available electronically and can be integrated with other data such as flight plans, surveillance, routing, published rules and procedures. The integration of this data allows the system to monitor the information and when inconsistencies are detected, the controller can be alerted via the HMI or audibly with a buzzer. The main benefit of this **is the early detection** of controller, and flight crew / vehicle driver errors which, if not detected and resolved, might result in a hazardous situation. The system is then able to predict a possible incident and alert the controller at an earlier stage than the RIMS.

Background

In 2006 EUROCONTROL launched the Integrated Tower Working Position (ITWP) project to study the integration of the existing main system components used by an Controller into a simplified more efficient working environment and to address key issues resulting from the Runway Safety project conducted by EUROCONTROL.

A major and import
ant part of the study was also the development of Human Machine Interface (HMI) functional specifications and prototyping of the A-SMGCS functions -Surveillance, RIMS, Routing, Guidance and Planning at the level of the controller Interface including new Airport

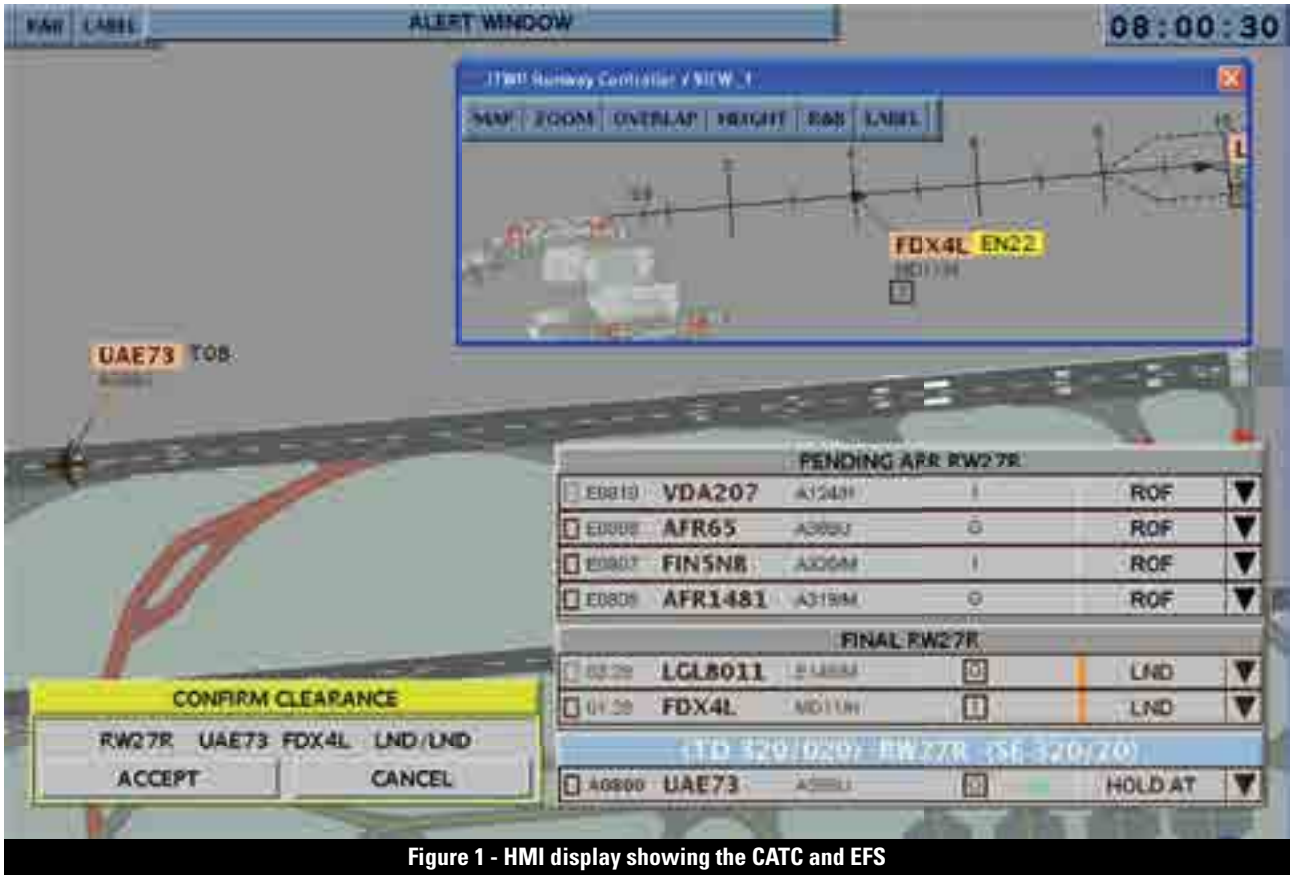


Figure 1 - HMI display showing the CATC and EFS

Safety Nets that predict potential surface and runway conflicts.

SESAR project 06.07.01 (Airport Safety Support Tools for Pilots, Vehicle Drivers and Controllers) continued the development and validation of the concept resulting in the following 2 new categories of alerts:

- **Conflicting ATC Clearances (CATC)**
- **Conformance Monitoring Alerts for Controllers (CMAC).**

The concept has been validated using the European Operational Concept Validation Methodology (E-OCVM) and several different validation exercises have been conducted by different SESAR partners. These Airport Safety Nets are now part of the European Implementation – Pilot Common Project (PCP) and 21 major European airports have been identified to implement them.

Conflicting ATC Clearances (CATC)

In the first example at the beginning of this article the Controller cleared an aircraft to land when another flight was already occupying the same runway. Neither of the flight crews nor the controller realised the error; and the result was that one aircraft landed on top of the other.

For various reasons, humans can be easily distracted and they then simply forget that they have done something or they believe a situation is different to what it actually is. I have to admit to once starting to pour orange juice on my cereals at breakfast as I was tired and thinking of several things I had to do that morning whilst also watching something interesting on the TV news! To avoid controllers having these "senior moments" it is possible to integrate the clearances they make with the surveillance position of the mobiles that they are controlling. **However, this requires a strict way of working where the clearance, such as Cleared to Land, is input on the EFS at almost the same moment it is passed on the radio frequency.**

As the system knows the position of the mobiles and the next possible clearances it is possible to program certain rules which will allow the HMI to show the controller which clearances are possible and which

ROGER **LANE**

works in the Airport Unit of the EUROCONTROL Research Centre at Brétigny-sur-Orge in France. He was a UK ATCO in the Royal Air Force and with NATS before joining EUROCONTROL in 1994. Since then, he has project-managed Real Time Simulations, helped to develop A-CDM and worked on SESAR Surface Management projects including the Integrated Tower Working Position (ITWP) project.

ones are considered as a CATC (in the image above a small orange vertical line is displayed on the EFS next to the FDX4L LND (Cleared to Land) button due to the fact that there is another aircraft UAE73 on the runway).

If the controller doesn't notice the indication on the HMI or chooses to ignore it, they will still receive a pop up window asking them to confirm the input of such a clearance (in Figure 1 this is the yellow box in the bottom left corner).

The detection of CATC will be performed by the ATC system and depending on the situation, some or all of the following data will need to be known by the ATC system:

- The clearances given to the mobiles concerned (Cleared to Land, Cleared to Take Off, Line Up, Enter or Cross. If conditional clearances are used then it will be necessary to be able to input these into the system as well.
- The assigned runway.
- The assigned holding point.
- The route of the mobile/s.
- The position of the mobile/s using A-SMGCS Surveillance data (e.g. position, velocity, track angle…) correlated to flight plans on the mobiles concerned.

Conformance Monitoring Alerts for Controllers (CMAC)

In the second example at the start of the article the flight crew take a wrong turn that leads them back onto the runway. This can be avoided if the cleared route of the aircraft is known to the system and the controller is alerted when a deviation is detected. In this case an Alarm would have triggered and a controller could have prevented the incident occurring by instructing the flight crew to stop the aircraft.

The introduction of EFS means that the instructions given by the controller are now available electronically and can be integrated with other data such as flight plan, surveillance, routing, published rules and procedures. This integration allows the system to monitor the situation and if any inconsistencies are detected, the controller can be alerted via the HMI or audibly. **The current A-SMGCS RIMS will still exist as the last minute warning system based on the position of the mobiles.**

When a potentially hazardous situation is detected, the A-SMGCS will provide the controller with the same two types of alert as RIMS, namely 'INFORMATION' and 'ALARM':

- **INFORMATION:** This means that a potentially hazardous situation may occur. The tower controller can therefore use their skill and experience to resolve the incident without using a drastic action such as issuing a "go around". If successful, there will be no alarm; if unsuccessful the alarm will be triggered and be presented on the HMI.
- **ALARM:** This means that a critical situation exists and that immediate action is necessary. An alarm will also trigger an audio warning (e.g. buzzer) in case the controller is not looking at the HMI at the time.

ROUTE DEVIATION	An aircraft deviates from cleared route on a taxiway (RED Alarm if the deviation occurs close to an active runway).
RWY/TWY TYPE	An assigned runway or taxiway is not suitable for the aircraft type e.g. runway is too short.
STATIONARY	A mobile has received a clearance and fails to move within a specified elapsed time.
RWY CLOSED	An assigned runway is closed (RED Alarm if mobile is on the RWY).
TWY CLOSED	The taxi route is planned to go through a closed taxiway (RED Alarm if mobile enters the taxiway).
NO PUSH/TAXI CLR	An aircraft pushes back or taxis without clearance.
NO CONTACT / NO TRANSFER	An aircraft has reached a defined point without being assumed transferred by the controller.
HIGH SPEED	An aircraft exceeds a specified maximum taxi speed.
RWY INCURSION	An unauthorised mobile is in the runway protected area (e.g. NO LINE UP/CROSS/ENTER clearance).
NO TAKE OFF CLR	An aircraft begins take-off without a clearance.
NO LAND CLR	An aircraft is on short finals to a runway without a landing clearance.
STATIONARY IN RPA	An aircraft that has landed and is within the RPA and does not move for 30seconds.
RED STOP BAR CROSSED	A mobile crosses a RED stop bar.

Table 1

The alerts can be displayed on the EFS, the radar/track label and in a dedicated alert window on the screen. **It is recommended that all alerts are displayed in the alert window until they have been resolved**. In the case where more than one alert is triggered for the same mobile it is recommended to display the alert with the highest priority only in the radar/track label and /or EFS, bearing in mind that all the alerts are always being displayed in the Alert Window.

The CMAC Alerts that have been developed and validated within the SESAR Programme are shown in Table 1.

SESAR validations have identified the following key issues that must be considered before implementation:

- The display of alerts will be subject to local agreement and operations.
- The number of false or nuisance alerts must be kept to a minimum so that controllers do not become complacent and ignore them.
- Where (which controller position) and when to display needs to be agreed at a local level.
- It is recommended to use the same colours as those used with RIMS for the different stages of alert (e.g. RED and YELLOW) and use the SESAR text when displaying the different types of Alert.

Conclusion

The new CATC and CMAC Alerts have been developed taking into account many actual incidents/accidents and simulations have proved that they could have been prevented if the new alerts had been in operation. Introducing these Alerts in addition to the existing RIMS Alerts will allow controllers to identify potential incidents and resolve them before a dangerous situation arises where the current RIMS alert would be triggered. In trial the new alerts have received very positive feedback and a few already have been implemented at some airports. The implementation of all of the alerts will significantly enhance the safety at any airport especially where there are high intensity runway operations and busy ground movements.

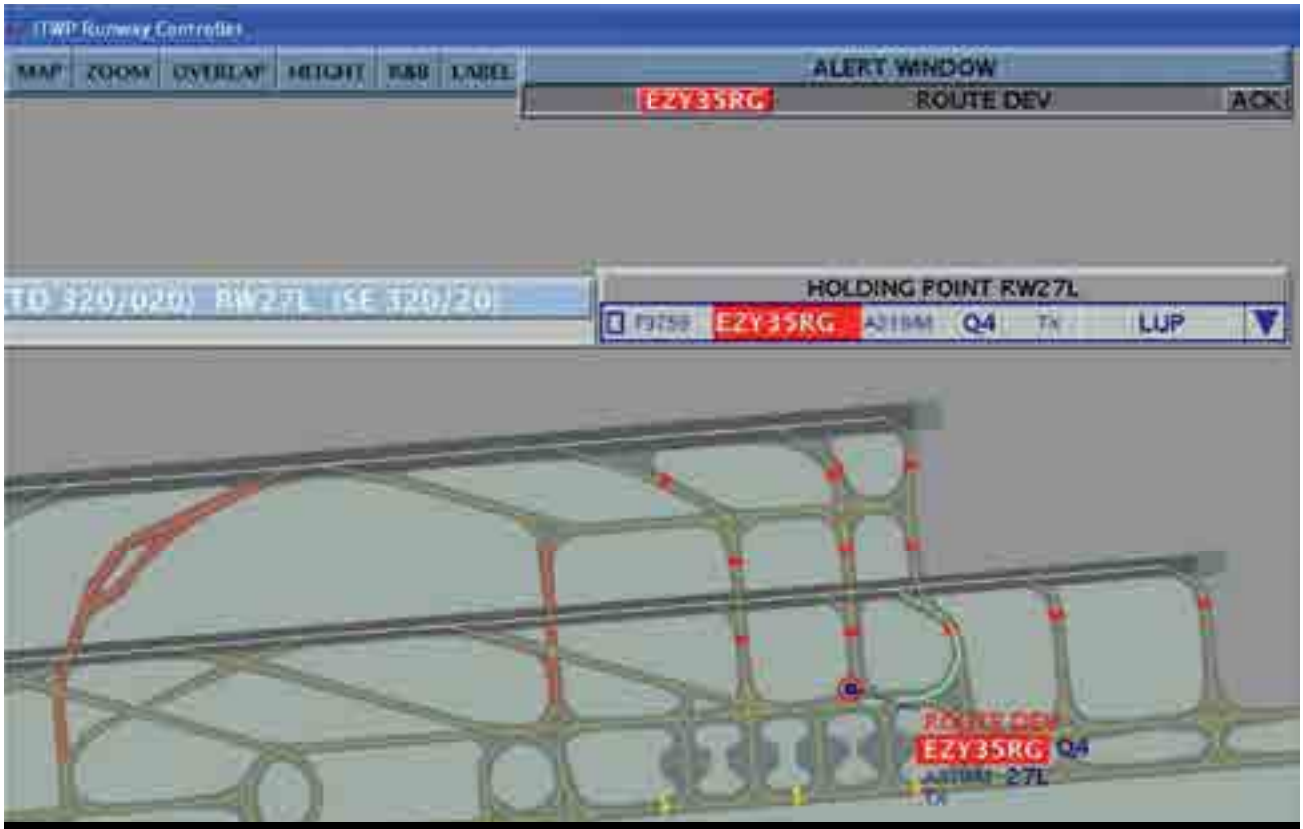


Figure 2: A Route Deviation Alert where the aircraft has turned too early; this triggers an ALARM because it's close to an active runway

THE NEW KID ON THE BLOCK

by Stanislaw Drozdowski

We all probably remember from our schooldays the tension in our group of friends when, at the beginning of a new school year, we saw a new face in the class. We all had well-defined roles in our "gang" and with the new arrival we did not quite know what to expect, whether the new one might be stronger or maybe a better football player and thereby threaten our well-established roles.

We are all familiar with TCAS II[1], in fact the only kid on the block in the world of airborne collision avoidance. TCAS II has been with us for over 20 years and we are all familiar with its functions and operations. As much as we may dislike TCAS II for its shortcomings (like nuisance Resolution Advisories in level off situations), its role in ensuring safety and preventing mid-air collisions is well known. But now the status of TCAS II as the only airborne collision avoidance system in use will change with the forthcoming arrival of the new kid – ACAS X[2] which we can expect in the skies above us in less than five years from now.

First of all, the new system is intended to generate optimised Resolution Advisories (e.g. reduce the number of unwanted or nuisance advisories). Secondly, the design of ACAS X logic will provide the flexibility not afforded by TCAS II to adapt relatively easily to any future modes of separation or operations as well as to new sources of surveillance data. Finally, ACAS X will be a family of collision avoidance systems (see the adjacent text box) which, through modification of the baseline system, will enable its extension to new classes of airspace users such as RPAS and general aviation as well as to specific types of operations such as closely-spaced parallel approaches, where TCAS II produces nuisance RAs too often.

ACAS X VARIANTS

ACAS Xa – The general purpose ACAS X that makes active interrogations to detect intruders. ACAS Xa is the baseline system, the successor to TCAS II. The Standards are expected to be ready by 2018.

ACAS Xo – ACAS Xa extensions designed for particular operations, like closely spaced parallel approaches, for which ACAS Xa is less suitable because it might generate a large number of nuisance alerts. The Standards are also expected to ready by 2018.

ACAS Xu – Designed for Remotely Piloted Aircraft Systems (RPAS), incorporating horizontal resolution manoeuvres. Work on Standards will start in 2016.

ACAS Xp – A variant that is expected to solely rely on passive ADS-B data rather than active interrogation to track intruders. It is intended particularly for light aircraft that are not currently required to fit TCAS II. No schedule for the development of Standards yet.

What is ACAS X?

The US Federal Aviation Administration has been driving the development program of ACAS X since 2008. A decision was made to develop a new collision avoidance system to take advantage of recent advances in dynamic programming and other computer science techniques, which were not available when TCAS II was initially conceived over three decades ago.

The key difference between TCAS II and ACAS X is in the design of collision avoidance logic. TCAS II issues alerts against a potential threat on the basis of the time to the closest approach using a set of hard-coded rules.

Instead of using a set of rules, ACAS X will use alerting logic that is based upon a lookup table. The current state of the own aircraft in relation to a threat aircraft is used to look up the best course of action in the table, whilst also taking into account predefined safety and operational objectives.

The best course of action is the one with the lowest 'cost'. This 'cost' increases in the order 'do nothing', 'generate a TA', 'generate a simple RA' and 'generate a complex RA'. An RA is complex rather than simple if it results in reversals or intruder's altitude crossings, as such RAs are generally considered operationally undesirable because they are sometimes not

1- TCAS II ("tee-cas two") – Traffic alert and Collision Avoidance System, also referred to as ACAS II – Airborne Collision Avoidance System.
2- ACAS X – Airborne Collision Avoidance System. Pronounced "Ay-cas eks" rather than "Ay-cas ten"

followed correctly. ACAS X will use the same hardware (antennas and displays) as the current TCAS II system and the same range of RAs as in TCAS II version 7.1. Although the timing of alerts may change, it is expected that pilots and controllers will not perceive any change with the transition to the new system. ACAS X will be fully backwards-compatible with current TCAS II systems (e.g. using the same coordination protocols between two units).

Previously, it was assumed that ACAS III (or TCAS III) would be the successor to TCAS II. ACAS III was foreseen as also generating horizontal RAs. However, the idea of ACAS III has been abandoned and it is now highly unlikely to ever materialise – although horizontal avoiding manoeuvres are expected to be used in ACAS Xu.

Putting the new kid through the stress test

So what did we do at school with new kids? We tested their strength, speed or resilience in their new environment. We did not always know what kind of tests the new kids needed to be subjected to and so we invented new tests whilst getting acquainted with them.

It is a bit easier with ACAS X given that we have several years to prepare for its arrival and conduct testing. Currently, ACAS X logic is undergoing a process of optimisation during which the lookup tables are fine-tuned to address any undesirable results found during testing.

The data used for testing comprise of recorded real-life encounters and radar data as well as millions of computer-generated encounters.

What do we look at specifically? First of all, we need to make sure that ACAS X will perform satisfactorily in critical conflict geometries, those where without an airborne collision avoidance system there would be a high probability of a midair collision. We also need to make sure that there is no degradation of existing safety standards when using the new system.

Secondly, through comparison of a large number of encounters, the types, timings and numbers of RAs generated are analysed. The goal is reduce the number of nuisance or other operationally undesirable RAs whilst also ensuring that RAs are issued correctly and timely when needed. Moreover, we would like to confirm (as much as it is possible in the simulation environment) that ACAS X will not create new problems, e.g. it will not generate nuisance alerts in situations in which even TCAS II is not generating any alerts. To the surprise of ACAS X developers, early testing has shown that within the airspace of one major European ANSP, the number of alerts generated by ACAS X compared to those generated by TCAS II has shown a significant increase. However, this mainly happened in encounters where there was adequate horizontal spacing between the aircraft involved and, therefore, a low risk of collision.

Finally, testing is looking at the interoperability of ACAS X with TCAS II to make sure that the new kid will fit into today's world of collision avoidance. ACAS X will have to co-exist with TCAS II for many years (if not decades) to come. But whilst it is expected that after 2020, most newly-manufactured aircraft will leave the assembly lines already fitted with ACAS X, many existing aircraft will largely remain TCAS II-equipped even if some operators upgrade to ACAS X to benefit from the new functionalities offered by ACAS Xo.

Sometimes, testing produces results which present the developers with difficult choices. For example, it may be possible to achieve a reduction in one type of nuisance RA but this may then result in an increase in another type of unwanted RAs. How do we balance which is better and which is worse? In these cases, the developers seek advice from the pilot and controller communities through specially-established working groups made up of representatives from major and regional airlines, ANSPs and the professional bodies representing pilots and controllers.

When the development of ACAS X is complete, the regulators will need to be satisfied that its design is sound and that the results of testing are acceptable. While testing and the data used for tests covers a wide array of situations and airspace environments, it is inevitable that some unusual cases will not be covered – a new kid can always cause surprises. ACAS X will be closely watched when it arrives. One always needs to keep a careful eye on the new kid.

Lastly, you are probably curious as to why the new version of ACAS got the suffix X, rather than sequential III or perhaps IV. I am not sure myself why the term X was coined and whether there is any relation to X Factor or X Files, as some people speculate. Most likely, ACAS X, like any new kid on the block, wants to come surrounded by a bit of mystery.

STANISLAW **DROZDOWSKI**

is a Senior ATM Expert at EUROCONTROL HQ in Brussels, working in the area of ground and airborne safety nets. Previously, he worked as a system engineer with Northrop Grumman and as an Air Traffic Controller in Poland and New Zealand. He is currently involved in ACAS X standardisation and validation.

THE CONTINUAL IMPROVEMENT OF SAFETY NETS

by Rod Howell

Over the last twenty years or so, I have had the privilege of helping to improve the performance of numerous ground–based Safety Net systems, through design improvements and optimisations. This article draws on my experiences and explains some crucial analysis activities that should be undertaken to achieve continuous improvement. Following the advice offered here will save you time and money in the long run, and lead to better performing Safety Nets.

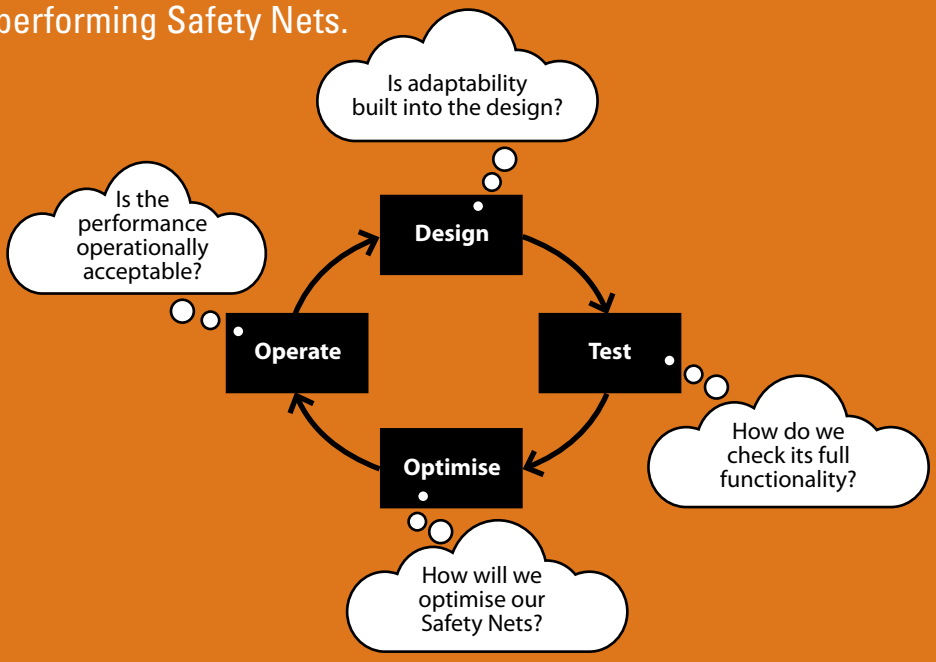
The four classic ground-based safety nets are:

Short Term Conflict Alert (STCA) - STCA assists the controller in preventing collision between aircraft by generating, in a timely manner, an alert of a potential or actual infringement of separation minima.

Minimum Safe Altitude Warning (MSAW) - MSAW warns the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of aircraft proximity to terrain or obstacles.

Approach Path Monitor (APM) - APM warns the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of unsafe aircraft altitude during final approach.

Area Proximity Warning (APW) - APW warns the controller about unauthorised penetration of an airspace volume by generating, in a timely manner, an alert of a potential or actual infringement of the required spacing to that airspace volume.



The "Continual Improvement" loop shows how the performance of Safety Nets should evolve – primarily as a result of testing, optimising and operational use of Safety Nets. For senior management, the procurement of a Safety Nets system should be seen not as a one-off event but as the beginning of an ongoing process of adaptation and improvement.

The 'Continual Improvement' loop shows that effective management of a Safety Net system requires regular monitoring of performance and the making improvements to design and parameter optimisations as necessary to maintain operational acceptability. There are numerous questions to ask at each stage of the process, some of which are shown in the diagram.

Is the Performance OK?

One thing that has become clear to me is that many ANSPs still do not have a clear understanding of how well a Safety Net system is performing or should perform. Performance figures are not generally widely published. Those that are can be very context specific, making them difficult to apply to somebody else's airspace.

Questions have been raised on numerous occasions over how many nuisance alerts are too many, and how much warning should a Safety Net provide. Precise numbers are impossible to provide because they depend so much on multiple local factors (including traffic levels and complexity, technical systems and HMIs), and the effect of these in concert with Safety Nets alerts on controller performance are not eadily quantifiable.

I therefore make a plea: If you have any concerns about the performance of a Safety Net, make sure that they are raised within your organisation. There are two very good reasons for this: firstly, these systems are there to add an additional layer of safety to Air Traffic Control. An underperforming Safety Net system (as well as being potentially annoying for controllers) is not providing the safety benefit that it should and secondly, virtually all of the operational issues that I have seen can be overcome either through algorithm improvements or through careful tuning of parameters.

Too many Tracks

The 'split tracks' issue can be a problem. The displayed system tracks are the fundamental data that the controller uses for Air Traffic Control, and that the Safety Nets use to determine if alerting conditions exist. A split track is essentially the occurrence of two (or sometimes more) tracks for only one actual aircraft. Surveillance errors are the main reason that split tracks occur, and whilst they can slightly clutter the controller's display, they can be much more distracting if they result in false STCA alerts.

There are a number of reasons for split tracks. Whilst the Surveillance Data Processing System creates a split track, the root cause is usually due to erroneous radar data. These errors can include position errors, poorly extracted Mode A or Mode C (SSR data), or split plots (two radar plots where only one should exist).

As a case in point, an ANSP from an ECAC member state recently reported to EUROCONTROL's Safety Nets Performance Improvement Network (SPIN) Sub Group that it was experiencing a large number of nuisance STCA alerts in part of their airspace. Their own evaluations indicated that half of the alerts were from split tracks. Having verified their analysis, a novel and highly adaptable split track detection algorithm was designed, which the system supplier implemented in the STCA function. The result was a resounding success – halving the overall STCA alert rate overnight. Although removing split tracks themselves from the screen would inevitably take some considerable effort, modifying STCA to suppress the resultant false alerts was a quick and effective solution. In this particular airspace, some further suggested parameter tuning would then reduce the STCA alert rate to one third of its original value.

There have been a number of instances where ANSPs have reported issues which, on analysis, turn out to be due to inappropriate design of a Safety Net, either generally or which make it unsuitable for specific airspace. These cases are fortunately not common and, as Safety Nets gradually improve, the trend is for them to become increasingly so. In order to overcome such issues, it is of paramount importance that ANSP and ATC system suppliers work hand-in-hand to ensure that a Safety Net will be appropriate for the local operational environment by sharing information (including local procedures and system specifications), and by ensuring that full validation and verification are carried out before the Safety Net system goes into operational use. In my experience, the very best systems are produced when ANSP and manufacturer work collaboratively and are fully committed to achieving a common goal.

Good by Design

A good Safety Net design will typically incorporate a number of key features:

- Alerting rules (including prediction algorithms) appropriate for the operational and surveillance environment which should assess actual risk;
- Some protection against surveillance errors (especially split tracks);
- Protection against surveillance data items being missing (e.g. sudden drop of Mode A or Mode C);
- Flexibility for different parameters to be easily set in various types of airspace or for different types of flight;

SURVEILLANCE ERROR DETECTION	✔
ELIGIBILITY CRITERIA	✔
AIRSPACE DEFINITION	✔
ALERTING RULES	✔

There are a number of elements to consider in the design of a Safety Nets system. The design involves considerably more than just the rules for generating an alert. It includes testing whether input data is valid (including surveillance error detection), the determination of which tracks will be processed (eligibility criteria) and potentially the flexibility to allow different parameters to be applied in various types of airspace.

Much of the above will seem quite obvious. Nevertheless, I have found a number of problems with operational Safety Net systems which cannot be overcome by parameter tuning, and therefore require a modification to the Safety Net system itself. To mitigate this, the simplest and most cost-effective thing for an ANSP to do is to carefully examine all the available documentation including any system specifications and user manuals as early as possible in the procurement process. Some potential problems can be identified by having suitably-qualified staff check that the design of the Safety Net will be appropriate for the target operational environment. However, some issues may not be discovered until the system is trialled using real traffic data and an operationally realistic parameter adaptation.

It follows therefore that a completely off-the-shelf solution may not be appropriate in many cases, and it may be in an ANSP's interest to seek a flexible contracting mechanism which will allow some changes to be made to the supplier's standard product.

Testing Times

ANSPs will want to undertake some testing of any new Safety Net system to satisfy themselves firstly that it is functioning as specified and secondly that it's performance will be operationally acceptable.

In an ideal situation this testing and operational tuning will be undertaken in a similar time frame, so that a reasonable adaptation is already available on the day that the Safety Nets system is put into operational use, or perhaps earlier for pre-operational controller training.

For the purposes of system verification, the parameter adaptations (STCA volumes, MSAW alerting surfaces etc.) and the traffic scenarios do not have to be realistic; in fact they should be contrived in order to test as many aspects of the intended functionality as possible.

Separate parameter tuning will be required to assess the new system for operational acceptability. Airspace volumes and alerting thresholds must be set to operationally realistic values in order to make this assessment and parameter optimisation can only really be considered complete once the operational acceptability requirements have been met.

Optimisation Techniques

In the past, some ANSPs have activated Safety Net systems and expected them to be 'plug-and-play' by relying on the manufacturers default settings only to have to switch them off again for adjustment Nowadays, ANSPs and manufacturers alike understand that Safety Nets have to be configured for the local airspace and procedures before going into operation. Nevertheless, full optimisation can still take considerably more effort than many people realise.

Optimisation requires data and, ideally, plenty of it. The techniques used will vary depending on the particular Safety Net. Of significance will be whether or not the system relies on controller interaction to determine when an aircraft is under ATC and hence must participate in the system If controller interaction is necessary, then this can place a practical constraint on how much data can be realistically made available for alert analysis and tuning before the system goes operational. In this case, maximum benefit needs to be leveraged from whatever system track recordings and alert log files can be made available.

In my experience, the most powerful methods of optimisation involve the use of off-line models of Safety Nets – versions of the system which can be run repeatedly with different parameter sets. However, either way a full understanding of the algorithms and the role that each parameter plays in the alerting decision will make the optimisation process very much faster.

All optimisation starts with defining appropriate airspace volumes. These may be STCA volumes (where different conflict thresholds are used), MSAW volumes describing the alert surface, APW volumes describing danger areas and restricted airspace or APM approach funnels.

For some Safety Nets, such as MSAW and APM, the overall alerting performance is dictated by appropriate definition of these airspace volumes by the user. MSAW relies hugely on having a sufficiently fine resolution of the alerting surface combined with carefully-crafted inhibited areas which take account of the standard arrival routes. APM relies on having approach funnels defined to take account of all the various types of approach to and in the vicinity of each APM-protected runway. APM performance in particular benefits from some detailed technical and operational input and it is hard to imagine how one could easily optimise an APM system without recourse to an off-line model and analysis/visualisation tools.

One important thing to bear in mind is that it is very easy to tune Safety Net performance to match a particular set of traffic data. After a tuning exercise, it is important to compare the new tuning against the original parameters on a fresh traffic recording. This will provide confidence that the new parameters provide a benefit generally, rather than just for the traffic sample against which the Safety Net was tuned.

Closing the Loop

Once an optimisation is considered complete, an ANSP should be in 'monitoring' mode, making regular measurements to check that the performance of the new system has not degraded due to operational changes. They should also be seeking feedback from their controllers to help understand whether there are specific concerns or issues which might be grounds for restarting the 'Continual Improvement' loop.

In summary, the most effective Safety Net systems have been implemented when an ANSP and a supplier have worked collaboratively. This is not trivial and needs commitment from senior management on both sides, but it brings demonstrable safety benefits.

ROD **HOWELL**

is an expert in ground-based safety nets and surveillance tracking at QinetiQ (UK). His work has included R&D and design for the NATS' Enhanced STCA system, technical advice to the EUROCONTROL SPIN Sub Group, and technical support to help a number of ANSPs optimise their safety nets systems. He is the primary developer of an AV tool (STRACK), which is used for tracking analysis, and PolyGen which is used in the production of MSAW surfaces.

HOW TO SYNCHRONISE **DIFFERENT SAFETY NETS**

by Captain Wolfgang Starke

Today's technology is delivering opportunities for safety nets covering nearly every possible scenario from different points of view. These features can be ground-based or airborne applications; they can be directive or informative and adherence can be mandated or the indication can be on a "for information only" basis. Most of these systems do work well, are pretty reliable and serve their purpose – enhancing flight safety. However, there is one big problem, what to do if several of these systems generate an alert at the same time, providing different ways of resolving the problem?

Looking back to the early years of aviation, flight safety was hardly comparable to the high standard of today. The only safety net known at that time was the brain of the pilot. Later, when air traffic control was introduced, a second safety net was added - the brain of the air traffic controller.

Today we have numerous systems assisting our brains and organs of perception in order to guarantee high levels of flight safety. Still, one very basic problem remains. Once there were air traffic controllers, there was the chance of having two solutions to one problem at the same time based on the intent of the controller and the intent of the pilot. Both might be adequate ways of solving the problem as all roads lead to Rome but we need to decide which road to follow.

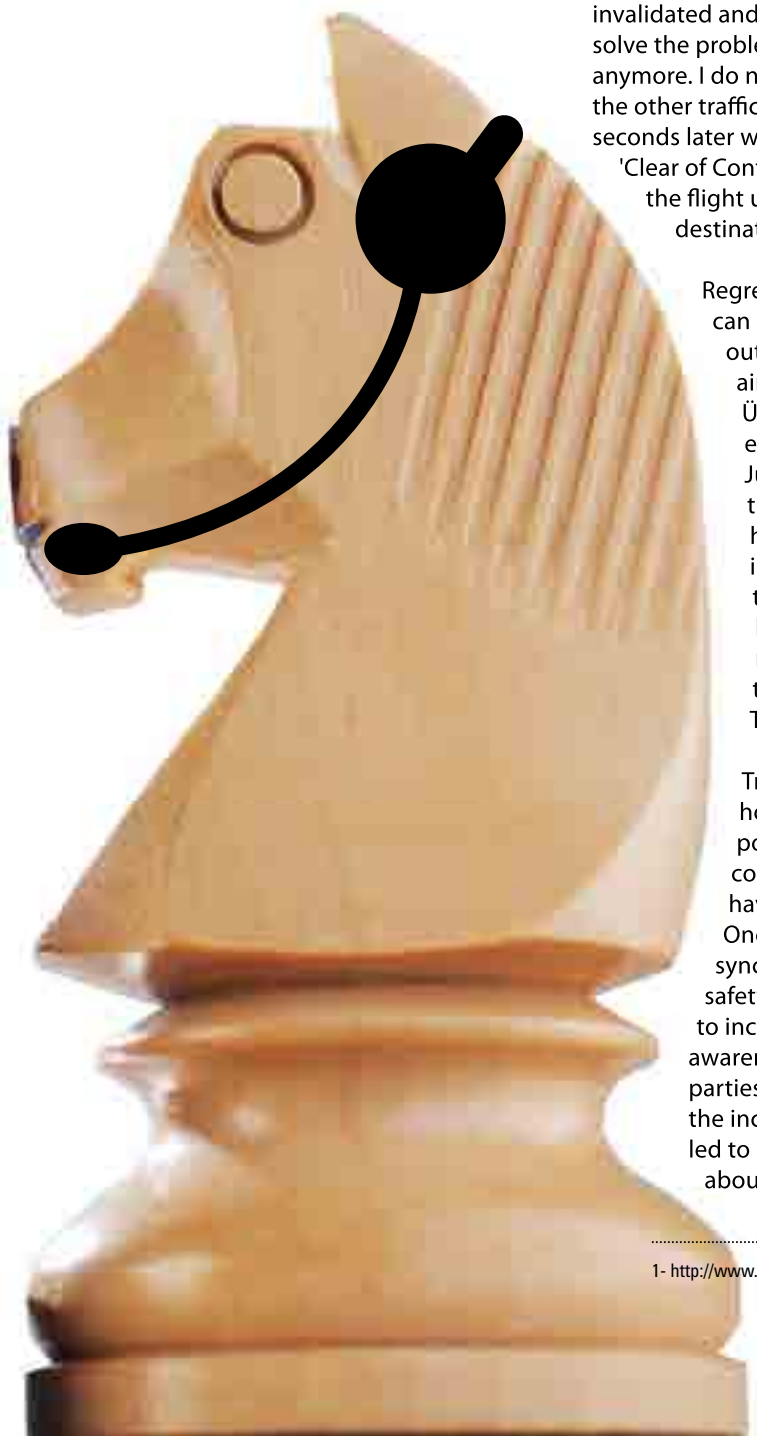
Being faced with a problem - say an airborne conflict - today, there may be several solutions presented to the actors. We have the basic reactions of pilots and controllers such as see and avoid, the mental picture or influences originating from experience, expectations or somewhere else. On top of this there are safety nets such as medium or short term conflict alerts as well as the airborne safety net called ACAS (airborne collision avoidance system). These systems all work independently from each other for good reasons. Still, if the solutions presented are contradictory, the consequence may be confusion.

Such a confusing situation happened to me on a short haul flight during climb out in low traffic density. We had been cleared to climb to flight level 190 on a northerly heading. All of a sudden, the

air traffic controller instructed us to immediately turn right onto heading 090 degrees. While we initiated our turn with the autopilot engaged, climbing through flight level 170, the air traffic controller instructed other traffic, cruising at flight level 180 on a southerly heading to immediately turn right onto a westerly heading. Almost immediately thereafter he asked us whether we could level off at flight level 170. So far this was the mental plan of the air traffic controller, probably assisted by a safety net.

We were already climbing through FL178 when we were asked to maintain flight level 170 by the controller. Therefore we asked the controller whether he wanted us to descend back flight level 170 or level off flight level 180. Just one second later, our TCAS (traffic alert and collision avoidance system) provided a "climb" resolution advisory. As we could not maintain the required climb rate of 1500 ft/min during the turn, we needed to stop the turn on a heading of around 045 degrees in order to comply with our TCAS RA.

The controller now saw us tracking in a direction we had not been instructed to and climbing instead of levelling off as being asked to. His whole mental picture had been invalidated and his approach to solve the problem might not work anymore. I do not remember what the other traffic did, but several seconds later we eventually got a 'Clear of Conflict' and continued the flight uneventfully to our destination.



Regrettably, such conflicts can lead to disastrous outcomes like the mid-air collision overhead Überlingen in the late evening hours of 1st July 2002[1]. The air traffic controller then had a different way in mind how to solve the conflict than TCAS had, as happened to me. The difference is that we followed the TCAS RA.

Trying to find solutions how to prevent this potentially deadly confusion, two ways have been researched: One is to harmonise and synchronise the different safety nets, the other is to increase situational awareness of all involved parties. The second way, the increase of awareness, led to extensive research about possible ways of displaying TCAS RAs to controller working positions. There are ATC centres where such a display is already available, but there is a lack of worldwide standardisation on this feature and no harmonised procedures on the use of such alerts.

A major problem of this so called TCAS RA downlink, besides the legal liability question, is how to deal with a situation where a TCAS RA alert is displayed to the controller but compliance to an RA is not apparent on the radar screen. What would you do as a controller? Intervene and possibly create confusion by giving potentially contradictory instructions, knowing that this kind of confusion can be very dangerous? Or would you keep quiet and trust the pilots of both aircraft to follow their TCAS, risking a mid-air collision destroying both the aircraft involved? An answer to this question has not been found yet.

Looking at the first way of solving this problem of contradictory advisories from different safety nets, it seems to be a good idea to connect all these safety nets with each other to get just one resolution.

Unfortunately the solution is not that simple. As often in life, we sometimes have to accept that nothing is perfect and this is also true for safety nets. Be it STCA (short term conflict alert), ACAS (airborne collision avoidance system), RIMCAS (Runway Incursion Monitoring and Collision Avoidance System), MSAW (Minimum Safe Altitude Warning) or whatever tool you like to examine, none of these safety nets is perfect. All these systems have in common that they have their minor, little bugs. Fortunately, the basic design and parameters of complementary systems is often very different. The chances are small that a conflict that is, for example, not detected by TCAS due to a little bug in the TCAS logic is also not detected by STCA.

1- http://www.skybrary.aero/index.php/T154_/_B752,_en-route,_Uberlingen_Germany,_2002_(LOS_HF)

The same works the other way round, if STCA does not detect a conflict due to a little bug, TCAS will probably do so.

If you connect these two systems and harmonise the alerts, the risk arises that an alert may be suppressed when one of the systems does not detect a conflict. The safety achieved through several levels of conflict detection[2] can only be maintained if the various safety nets work independently of each other.

What needs to be done is to create an order of priority for the different systems and their alerts. aircraft systems already have such priorities. For example, a terrain avoidance alert will always take priority over a traffic alert. This is supported by ICAO provisions that an ACAS resolution advisory should not be followed in preference to terrain avoidance manoeuvre, a wind shear escape or a stall recovery occurring at the same time.

This prioritisation is already in place for the case of a controller trying to resolve a conflict when the ACAS provides solutions at the same time.

WOLFGANG **STARKE**

is a Bombardier Dash8-Q400 check captain and type-rating instructor with the Air Berlin group. He chairs the Air Traffic Management and Aerodromes Working Group of European Cockpit Association (ECA) and serves on committees for the Vereinigung Cockpit (German Air Line Pilots' Association) and for IFALPA (International Federation of Air Line Pilots' Associations). He is an IFALPA representative member of ICAO's Surveillance Panel.

ICAO clearly says that controllers shall not try to alter an aircraft flight path in the event of a TCAS RA until that aircraft reports clear of conflict. But again we end up with the situational awareness-problem stated above, as the air traffic controller needs to be aware of the TCAS RA before ceasing his own efforts to resolve a conflict. As pilots need - and are trained - to fly their aircraft first before making radio calls, the chances are high that controller awareness of a TCAS RA will be delayed. Even if the task sharing on the flight deck is at its best, frequency congestion can make it impossible to notify ATC promptly.

Looking at ground-based safety nets and the possibility of instructing a rejection of a take off the situation can get even more complicated. An aircraft may not be able to safely reject its take off once the indicated speed exceeds V1 (the highest speed at which a take-off can be rejected with the aircraft still able to guarantee stopping on the runway). Neither the safety net nor the controller knows what the V1 of any particular aircraft on any particular day is given that it is dependent on the weight of the aircraft, environmental factors and actual runway conditions.

In the event of a runway incursion at the far end of the take off runway, two alternatives may be considered by a pilot. Continue the take-off, rotating ahead of the incursion and passing overhead of the vehicle or rejecting the take off and stopping ahead of the obstruction. As noted above, neither the controller nor the safety net can take this decision and even for pilots, it can sometimes be hard to judge which is best. An option that is definitely worse is to instruct contradictory to the judgement of each other (i.e. instruct an abort while the pilots judge the go-case to be better).

It is a pity but at the end of this article hardly any answer to the questions raised can be given. The best options still need to be researched; procedures need to be designed accordingly. The good news is that on the ICAO-level, within SESAR as well as within other regions and organisations, research and development is in progress which may lead to action plans for implementation and ultimately to appropriate manuals. However, we must not repeat the same mistakes again that we have already done, building single and additional safety nets without looking at the overall picture.

First of all, a safety net does not automatically mean additional safety. Why? Because more and more alerts can on one hand reduce the attention of operational staff to single alerts, on the other hand possible nuisance alerts can draw attention away from urgent and useful alerts. A safety analysis of the whole system before and after the implementation of the new safety net is required. Further, a decision must be made how to proceed. Do we want to build drones with all the safety nets included but without pilots and possibly even without controllers, or do we still want ATC and aircraft being operated by human beings? In the latter case, I think it is a bad idea to place thousands of "safety robots" around the operational staff telling the human what to do. The less advice is sometimes best as long as all the humans involved are properly trained.

This task of harmonising safety nets and properly training operational staff would be a long and winding but could lead to better flight safety in the future. Extensive consideration of human factors and of technical limitations is necessary; all future users of these systems need to be on board. Lastly, there needs to be good trust of the newly designed and harmonised safety nets so that operational users do not hesitate to accept them.

Certainly challenging, but the destination seems tempting.

2- The Swiss Cheese Model: http://www.skybrary.aero/index.php/James_Reason_HF_Model

WHY TCAS DOWNLINKING **IS A BAD IDEA**

by Duncan Auld

People are often surprised if they learn of IFATCA's objections to downlinking TCAS RAs to controller working positions. Yet it's true, it is one of the Federation's most outspoken policies. It is worded as follows in our manual:

IFATCA is opposed to down linking of any advisories generated by ACAS. If downlinking of ACAS Resolution Advisories becomes mandated, then IFATCA can only accept this provided that the following criteria are met: Clear and unambiguous controller legal responsibilities; Downlink should be without delay; ATC systems to be able to receive, process and display the down link to the appropriate control positions; compatibility with all ground based safety nets; nuisance and false alerts must be kept to an absolute minimum; and ACAS should only be considered as a 'safety net'.

Let's analyse this in a bit more detail. The policy firstly demands that clear and unambiguous controller legal responsibilities are defined before such a system should be implemented. If Überlingen has taught us anything, it is that vague and incomplete statements of who does what when a TCAS RA is triggered can be a recipe for disaster. In a Review of ICAO Procedures, the 2007 RA Downlink Safety Assessment concluded that *"the existing ICAO procedures are inconsistent and should be reviewed. The issue of unclear controller responsibilities before and – even more – after the potential implementation of RA Downlink was also discussed (…) Current ICAO procedures do not contain provision for operational use of RA downlink."* [1]

Yet proponents of downlinking RAs, and ANSPs who have 'jumped the gun' and implemented it, are doing just that by not clarifying either where the controller's responsibility for separation ceases or where this responsibility is handed back. If a controller sees that a corrective TCAS RA has been triggered but a pilot contrary to TCAS procedures, should he or she do or say something? An even greater concern is that even though the ATM system can show that there's an RA active, this is not a confirmation that the pilot is reacting. In the current ICAO documentation the controller clearly remains responsible for

1- FARADS (Feasibility of ACAS RA Downlink Study) Close-out Report, EUROCONTROL, 2007, p7. https://www.eurocontrol.int/sites/default/files/publication/files/farads-close-out-report-version-10-20070514.pdf Accessed 15/09/2015

separation provision until the pilot verbally reports the TCAS RA to ATC.

The verbal report of a TCAS RA by a crew conveys the following three points to the ATCOs:

1) Yes, a TCAS RA is present;
2) Yes, we are following the RA;
3) Our manoeuvre makes us deviate from the current ATC-clearance.

Currently, the automatic downlink of a TCAS RA to ATC does not confirm any of the three points. Until all the above-mentioned issues are explicitly standardised at the ICAO level, IFATCA has no other option but to reject the idea of downlinking RAs to the controller.

Downlink should be without delay, as the more latency (delay) we have until the RA-messages reach the ATM-System and the operators, the less these messages are operationally relevant. ANSPs, such as DFS in Germany have proven that it is technically feasible to transmit TCAS downlink messages with almost no delay. In order to achieve this, extensive ground-infrastructure adaptations and developments are required (e.g. using Mode-S and listening to the various TCAS-transmissions). False or ghost TCAS squitter continues to be a serious concern, even if a lot of progress has been made to filter them out. It will be up to ANSPs to establish their own methods to differentiate bogus RAs from the real ones. While engineers tell us it's no problem to filter these out, there is a clear legal (and technical) dilemma: filter too much and risk missing a real one, or filter too little and risk overloading the controller with RAs that are simply not present in the cockpit!

That the down-linked TCAS RAs should be processed and displayed at the appropriate Controller Working positions speaks for itself. In order to achieve this the ATM system must be adapted to make sure that the addressing of the RA-messages to the correct Controller Working Positions (CWP) is achieved.

This task will generate delays or latency within the ATM System, but this is the price to be paid to avoid ATCO overloads, de-sensitisation and a loss of operator confidence in system warnings.

Even trickier will be the interaction with ground-based safety nets such as, for instance, with STCA (Short Term Conflict Alert). Which alerts should get precedence if they sound at approximately the same time? How can an HMI ensure that the different alerts are not interfering with each other and that they are clearly understood as such by the ATCOs working the affected flights? How will a controller prioritise them and make sure that all relevant procedures are followed correctly? What happens in cross-border cases, where one controller sees the RA-information but the colleagues in an adjacent centre or sector don't? Given the multitude of different ATC systems and HMIs, all this will require a tailored approach in each instance to ensure that these alerts are placed in the correct operational context. If this is not done correctly, it clearly will increase the safety risks dramatically – including confusing and/or contradictory ATC instructions reaching the crew.

And lastly, ACAS/TCAS was considered from inception to be a Safety Net that was completely and totally independent, in particular of all ground systems (TCAS was designed as a stand-alone airborne Safety Net). The downlinking of TCAS RAs, even if only meant to increase the situational awareness of controllers, clearly violates this principle. To show the alerts of the independent airborne Safety Net on-ground can create more hazards and may lead to uncertainties - worse even - it could create confusion. The more players and parties get informed about a last-chance safety warning, the more risk and possibilities for confusion, unexpected actions or even contradictions are created.

Experience, as well as TCAS-monitoring has shown that the existing TCAS procedures are working quite well; that controllers have become far less inclined to interfere with an announced TCAS RA and that pilots have also become less inclined to react to a controller's instruction (when this interferes or contradicts) with a TCAS RA shown in the cockpit. This implies that the strongest argument used by proponents of such a system is no longer valid. It was much more so when TCAS was introduced… but not anymore…. Current monitoring shows too that crew reactions to TCAS RAs are not yet totally flawless and manoeuvres are not always performed as required by procedure. The same can be said for ATCO-reactions: ATC-operators don't always stay hands off as required once a TCAS RA is announced on the frequency. So there is a clear need for much more TCAS-training for pilots, but also ATCO-training must be maintained or even enhanced (including simulator based training).

Another approach to 'TCAS improvement' is the Airbus initiative of coupling TCAS RAs with the autopilot. This in itself is much more beneficial than downlinking RAs - the former clearly makes quicker reactions and more accurate compliance much more likely, thereby limiting the impact on the ATC system and ATC provision of separation. Generally speaking the Airbus solution makes sure that all TCAS RA assumptions and requirements are met. That all TCAS RAs are followed correctly, meaning within the time frame allotted and within the commanded vertical constraints. This is a huge safety improvement!

Another system, also developed and certified by Airbus is called TCAP – TCAS Alert Prevention. It imposes new altitude capture laws on autopilots or Flight Directors (FD) by automatically reducing the rate of climb/descent before a level off. TCAP is reducing the vertical rate in the final 1000 feet before level-off and, by doing so, is reducing in a significant manner the number of TCAS RAs. Such level-off encounters, which are usually preventive TCAS RAs (where no deviation from the current ATC-clearance is required) make up about two-thirds of all monitored TCAS RAs in busy European and North American continental airspace. The TCAP system is another very promising safety enhancement that is improving the overall safety of the aviation system. A TCAS RA shown or reported to ATC is always a critical situation. The ATCO must remain hands-off for the duration of the TCAS RA event and this is clearly a loss of control and a serious limiting factor for ATC service provision.

And for the ground based ATM-systems, there would be a far greater safety benefit if every ATC system had a functioning and well-tuned HMI that included a predictive conflict alert system. This way, emphasis would be given to addressing the cause rather than trying to fight the symptoms. IFATCA believes that efforts should be concentrated on all the above-mentioned safety improvements, instead of running for risky short-term patches that will bring much more complexity into the system and have unintended or unexpected consequences that could have a tragic outcome …

DUCAN **AULD**

is the Executive Vice President Technical for IFATCA. In addition to his current work as an operational air traffic controller in Sydney terminal control, he has operated as an oceanic and area (both radar and non-radar) controller. He holds a Masters Degree in Aviation Management and serves as a technical expert on some ICAO Panels.

EMAS - A PASSIVE SAFETY NET FOR RUNWAY OVERRUNS

by Stan Koczkodaj

When addressing the area of ground-based or airborne safety nets, one subject that is often absent from discussions is that of an EMAS (Engineered Material Arresting System). Why is that so? After all, an EMAS certainly "prevents imminent or hazardous situations from developing into major incidents or accidents." The answer may stem from the fact that an EMAS is a passive system. Unlike most safety nets, an EMAS does not analyze and generate streams of data to a computer or relay that information to an air traffic controller, cockpit crew or other responsible party. There are no warnings, surveillance alerts, nor advisories.

I think that the retention material works a little bit too well...

The EMAS sits in a perpetual state of readiness, to be called upon to stop an aircraft on an airport runway when there is an overrun due to an aborted take-off or an anomaly in landing. It is a low-profile gray monument to the data and analysis gathered and processed months before the system was designed, manufactured, and installed. An EMAS directly addresses what is usually an unexpected and sudden emergency and delivers predictable performance and energy control that prevents a potentially catastrophic situation from occurring.

At one time, upon first hearing of an EMAS, the first question that may have been posed was: "What is an EMAS?" Thanks to evolving aviation policies, education, and word-of-mouth in the airport community, most aviation personnel know that an EMAS is an arrestor bed situated at the end of an airport runway and that it is designed to safely stop airplanes that overshoot runways. Over-simplification in descriptions by the media often compare/describe an EMAS to highway run-off gravel beds. The product is much more sophisticated.

The overall bed design and strength is based on an FAA-validated computer model that integrates the key elements of an airport's runway characteristics with the full range of their aircraft fleet mix. This model factors in over 100 data points, including airport fleet mix, available real estate, and a performance target of 70 knots as a standard or less when necessary. Because the main requirement upon calculation is to preserve the physical integrity of an aircraft, the design and performance takes into account all aircraft considered as critical, as one may have a weaker nose gear, a low engine clearance or specific gear configuration that would pose the greatest demand on the arresting system.

How does it work?

The EMAS predictably and reliably crushes under the weight of an aircraft, providing deceleration and a safe stop. It is FAA-accepted as an equivalent to a standard Runway End Safety Area (aka Runway Safety Area) and is an acceptable alternative for preventing overrun catastrophes at airports where RESAs/RSAs do not exist or are impractical due to environmental or other issues.

An EMAS bed is designed to stop an overrunning aircraft by exerting predictable deceleration forces on its landing gear as the EMAS material crushes without causing structural failure to the landing gear. The system operates independently of runway friction or braking action because the landing gear gradually sinks into the specially designed crushable material.

An EMAS may literally be the last line of defence against very dire consequences, which makes a very strong case for the system as a "safety net." The 243 passengers and crew that were on board the 9 aircraft, ranging from a Cessna Citation to a Boeing 747, that have been saved over the years by this technology would certainly provide a vote of confidence in agreement with that terminology. The 9 "saves" occurred in 9 attempts, with no failed arrestments, a perfect safety record: a safety net with flawless performance! After removal from the EMAS bed, every aircraft was able to return to service.

Air travel has never been safer than it is today. When justifying factors for not installing an EMAS, quite often statistics are cited to justify what could be perceived as a low percentage of runway excursions versus successful landings and take-offs. To put this in perspective:

STAN
KOCZKODAJ

is Marketing Creative Director for Zodiac Arresting Systems, a subsidiary of Zodiac Aerospace. An Art Institute of Philadelphia graduate, he has more than 30 years experience in marketing communications, conferences, public relations and multi-media relating to aviation safety. His most recent written work has appeared in Airport, Global Airports, and Airports International magazines.

runway safety related accidents where excursions occurred accounted for 83% of all fatal runway accidents (according to Flight Safety Foundation analysis, 1995-2008.) All it takes is one disastrous overrun to result in significant loss of life and high value assets, as well as loss of revenue due to an inactive runway.

When "lightning struck twice" at the same location.

Speaking of statistics, unusual anomalies do occur. The odds of an aircraft overrun occurring on one end of an airport runway may be remote, but certainly in the realm of possibility. Even more unlikely is the concept that two of these incidents would occur on the opposite ends of the same runway, at the same airport. But the likelihood that two overruns would occur on the opposite ends of the same runway, at the same airport, during the same week, are highly improbable. Yet that is exactly what happened in Key West, Florida USA in October, 2011.

On Monday, Oct. 31 at 7:45 PM, a Gulfstream 150 business jet was landing on Runway 27 when the aircraft overran the runway. It passed through an unpaved 180 meter (600 ft). runway safety area and travelled an additional 70m (220 ft), stopping at the end of the airfield, 1m (3 ft) away from an airport perimeter fence. There was substantial damage to the wings, nose, landing gear and body. The left side and wing of the aircraft were partially submerged in a shallow salt pond, with some fuel leakage. One passenger was hospitalized with a broken clavicle and ribs, while another suffered minor cuts and bruises.

Four days later, on Thursday, Nov. 3 at 12:15 PM, a Cessna Citation 550 touched down for a landing on Runway 09 of the same 1,464m (4,800 ft) runway. Unable to stop, the aircraft passed over an 11m (35-ft) setback area then engaged an EMAS. The aircraft continued 45 m (148 ft) into the energy-absorbing arrestor bed and coasted to a safe, controlled stop. As the dust was still in the air, the pilot, co-pilot and three passengers quickly exited the aircraft with no injuries. The aircraft suffered only minimal damage to its belly and front landing gear, with no fuel leakage. By 2:00 PM, the aircraft had been towed to a hangar and the runway reopened at 2:06 PM.

Airport Director Peter Horton observed that the safety material worked perfectly: "Not even a bruise or a scratch." And further: ". . . I have never seen a more effective safety device than EMAS to minimize aircraft damage or passenger injury in the event of an over-run incident. And as recent events have proven, it works exactly as advertised." Key West installed a second EMAS at the end of Runway 27 in early 2015. Aircraft overruns seem to happen when you least expect it. Although the circumstances in these two were similar, the outcome in each situation was remarkably different.

The EMAS safety net and aborted take-off: "We made the investment and we saved lives."

January 19, 2010 at Yeager Airport, Charleston, West Virginia USA, at 4:20 PM, when US Airways Express Flight 2495, a Bombardier CRJ-200 regional jet carrying 34 passengers and crew onboard, rejected take off 4 seconds after V1 due to an incorrect flap setting and was safely stopped by an EMAS arrestor bed. This save was unique due to the circumstance of the aborted takeoff, as the five previous successful EMAS aircraft arrestments had all taken place during aircraft landings.

The aircraft had reached a speed of 143 knots before braking aggressively, leaving skid marks on the runway before entering a sub¬stantial distance into the length of the EMAS bed, safely and dramatically stopping short of a steep 136m (446 ft) drop at the end of the airport runway, which overlooks a valley near the Kanawha River and the city of Charleston. Thanks to the EMAS, the passengers and crew walked away unharmed. After a brief shutdown, the runway was reopened by 10:15 PM, less than six hours after the arrestment.

For Aircraft Operators: Engaging an EMAS

As the manufacturer of EMASMAX, Zodiac Arresting Systems (ZASA) cannot dictate procedures for aircraft operators. However, following the guidance below ensures that the aircraft engages the EMAS according to the design entry parameters.

During the takeoff or landing phase, if a pilot determines that the aircraft will exit the runway end and enter the EMAS, the following protocol should be adhered to:

1. Continue deceleration - Regardless of aircraft speed upon exiting the runway, continue to follow Rejected/Aborted Takeoff procedures, or if landing, Maximum Braking procedures outlined in the Flight Manual.

2. Maintain runway centreline - Not veering left or right of the bed and continuing straight ahead will maximize stopping capability of the EMAS bed. The quality of deceleration will be best within the confines of the bed.

3. Maintain deceleration efforts - The arrestor bed is a passive system, so this is the only action required by the pilot.

4. Once stopped, do not attempt to taxi or otherwise move the aircraft.

An arrestment by itself does not by default require an emergency ground egress, but it may be impractical to offload passengers and crew via an air stair truck, thus necessitating the use of slides or internal aircraft stairs. However, should an emergency egress be required, use published aircraft emergency ground egress procedures.

The certification process from the FAA extensively tested successful aircraft evacuation and fire fighting and rescue vehicle response. Where the surface of the bed has been breached, the loose material will crush under foot. There are continuous steps built into the back and sides of the bed to help provide easy access for responding fire fighting vehicles and to enable passengers to safely step off of the bed.

Yeager Airport officials and the FAA installed the EMAS system as part of an overall airport safety upgrade in April-May 2007. At a post-event press conference, Kanawha County Commission President Ken Carper commented: "If it hadn't been for the EMAS, I'm convinced a catastrophe would have occurred." Mr. Carper, to Charleston radio station WCHS: "This is what is important. The Board of Yeager Airport, Senator Byrd, Senator Rockefeller, Governor Manchin, and others felt that we had to do this. We made the investment, and we saved lives."

EMAS safety net: aviation community acceptance

In early 2014, EASA adopted a stance similar to that of ICAO's "Annex 14, Volume I, Aerodrome Design and Operations to the Convention on International Civil Aviation", which included the use of aircraft arresting systems, as an Alternative Means of Compliance to meet runway end safety area (RESA) requirements. Many airports have no space or only a very minimal area in which a RESA could be established. ICAO's allowance for an EMAS to be installed within the runway strip provides flexibility to improve safety for a runway with a severely constrained RESA/RSA. IFALPA, IATA, ACI and civil aviation authorities have also recommended the deployment of arresting systems such as an EMAS when it is impractical to build out to meet ICAO-required RESA lengths.

A Safety Net That can also Gain Runway Space

Runways with adequate RESA/RSA space can also benefit from the installation of an EMAS as a means of reducing the length of a safety area, based on the design specifications of the arrestor bed. This can potentially free up valuable RESA real estate for other airport planning purposes, such as runway extensions.

Such was the case at San Luis Obispo County Regional Airport, San Luis Obispo, California USA who implemented EMAS systems in a creative fashion that earned the airport the distinction of being the first to use the product to gain sizable runway extension within airport property.

The dilemma in San Luis Obispo: a primary runway needed an extension from 5,300 feet to 6,100 feet to meet airline requirements for regional jets. The airport did not have the necessary geographic flexibility to expand the runway and keep the required 1,000 feet of runway safety area on each end. The solution: By physically shifting their runway north and installing two approximately 100 metre (300 feet) long arrestor beds at both ends of runway 11-29, the airport gained 245 metres (800 feet) of runway length (112metres or 400 feet at each end), eliminating the need to purchase expensive real estate or deal with protected areas and environmental issues.

Safety net and more?

A safety net in a circus will not prevent an acrobat from falling, but it will save him from injuries, in case of a fall. Similarly, an EMAS is there when all other measures have failed to reduce the severity of an excursion and transform an accident into an incident. With the presentation of all of the information so far, I hope that I have shed some light on EMAS, the sometimes forgotten safety net, so that it can be included with the full array of safety nets in place at airports that ensure the safety and reliable transit of passengers, crew and ground support personnel throughout the world.

The next time you fly in or out of a particular airport, and you see a flat gray, stepped checkerboard bed with chevrons at the end of a runway, don't be alarmed – that is your safety net!

ROPS - AN ACTIVE SAFETY NET FOR RUNWAY OVERRUNS

LOGAN
JONES

is an aircraft performance engineer working at Airbus. He was part of the team that worked on the development and certification of Airbus ROPS. He gained his PhD from ISAE in Toulouse, France for modeling the friction between an aircraft tyre and the runway.

by Logan Jones

Among incident and accident statistics, runway overruns continue to stand out. And now with the advances made on Airline Safety Management Systems reporting, we are able to track the number of events which did not result in an incident or accident but which showed minimal safety margins that could have ended much worse. How can we better understand what leads to these events and how to prevent them? When the aircraft is dispatched, a first calculation is made to ensure that the destination airport and preferred runway are indeed long enough for the conditions expected at landing. This is called the Required Landing Distance check or Dispatch check.

As the dispatch calculation is based on a set of regulatory assumptions, authorities around the world (and aircraft manufacturers) have started to recommend that the flight crew calculate an In-Flight Landing Distance during the descent preparation. This In-Flight Landing Distance check uses more operational assumptions of the aircraft performance and the most current conditions expected at landing (runway state, temperature, wind conditions etc…). The recommended safety factor to be added to the In-Flight Landing distance is 15%[1].

Why is that not always enough to prevent a runway overrun? From an aircraft performance point of view, small changes can have a surprisingly large impact on the landing distance. We have to remember that a 60 ton aircraft travelling at a typical approach speed of 135 knots (250km/hr) represents a lot of energy that needs to be dissipated.

To give you some examples (based on an A320 aircraft):

Whilst in the air:

- If the tail-wind increases by 5kt, aircraft speed over the ground will increase which can add 5% to the landing distance;
- Crossing the threshold at 60ft instead of 50ft can add 6% to the landing distance;
- A nominal touchdown from threshold is calculated as 7 seconds. Each additional second over 7 seconds can add 7% to the landing distance.

Once on the ground:

- Every one second of delay on applying pedal braking will add 7% to the landing distance;
- A delay of three seconds in selecting maximum reverse on a wet runway can add 4% to the landing distance;
- If the runway friction is 10% worse than predicted the landing distance will be 5% longer;
- Note: a failure of the spoilers to deploy can increase the landing distance by over 25%.

The end result is that, whereas during approach preparation the runway seemed sufficiently long, just a couple of small deviations can quickly put the flight crew into a situation where they are right on the edge of the capability of the aircraft to stop in the available runway length.

This is at the heart of why Airbus developed the Runway Overrun Prevention System (ROPS). ROPS is a safety net designed to continuously calculate whether the aircraft can safely stop in the runway length remaining ahead of the aircraft. If at any point the system detects there is a risk of a runway overrun, flight deck alerts are generated to help the crew in their decision making.

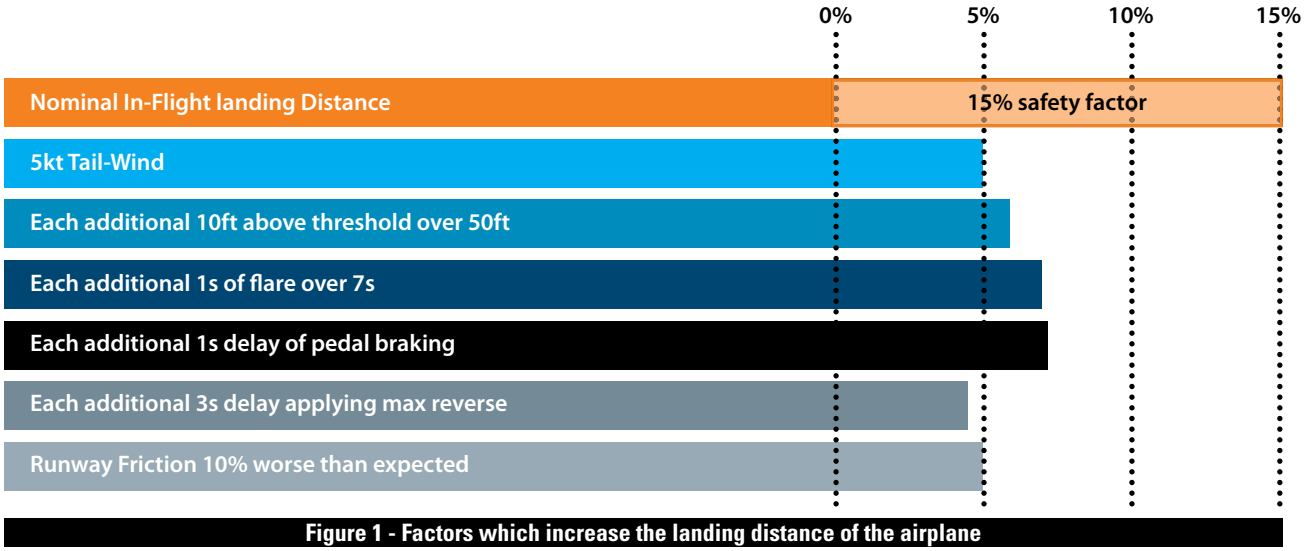


Figure 1 - Factors which increase the landing distance of the airplane

1- FAA AC No: 91-79A – Mitigating the Risks of a Runway Overrun Upon Landing

Research into ROPS began in 1998. In 2006, the system was officially launched and was certified for the first time on the A380 in 2009. Since then Airbus has achieved certification on the A320 family in 2013, the A350 in 2014 and lastly the A330 in 2015.

So how does ROPS work?

ROPS is embedded in the aircraft avionics and has access to all of the parameters that may affect the landing distance of the aircraft such as: aircraft weight, slat/flap configuration, ground speed, wind velocity, outside air temperature and the aircraft current vertical and horizontal position. ROPS also has access to a runway database on-board the aircraft which contains the runway characteristics. With the runway database, ROPS will auto-detect which runway the aircraft is approaching. In fact, all the information that ROPS uses is contained on-board the aircraft; no additional information is received from the ground (ILS, weather etc…). The current version of ROPS is certified for Dry and Wet runways only. However Airbus has already begun work on extending the system to cover contaminated runways based on the flight crews input of the reported runway state.

With the available onboard information, ROPS can instantly calculate (8 times per second) the amount of runway the aircraft needs to stop and compare this to how much runway remains ahead of the aircraft. The system begins active monitoring during final approach at 500ft above ground and continues throughout the flare, touchdown and roll-out.

The visual and audio alerts that the system generates change between the in-air phase and the on-ground phase. In-Air, the system will generate an alert "RUNWAY TOO SHORT". The procedure associated with this alert is to perform a Go-Around. Once on the ground, with the spoilers selected and the Go-Around no longer a safe option, ROPS will generate alerts which incite the crew to use all available deceleration means. These alerts may be "BRAKE, MAX BRAKING" and/or "SET MAX REVERSE" depending on the pilot actions. An additional functionality provided on Airbus A380 and A350 is that, when in autobrake mode, ROPS will also automatically activate maximum braking. Even after an alert is generated, the system continues to calculate the aircraft deceleration capability and if the aircraft is no longer at risk, the alerts are cancelled.

The design goals of ROPS were two-fold:

- ensure that the system alerted the pilot in a timely manner if there was an overrun risk
- ensure the system did not unnecessarily increase the number of go-arounds

The nature of the achieved design ensures both. The system is based on the actual capability of the aircraft to stop so that if the system triggers an alert, it is directly related to an imminent runway overrun risk.

Thus far the system has fully met its design goals. In years of in-service experience, Airbus has not been advised of any unjustified in-air alerts. In addition, ROPS has already shown its worth on several

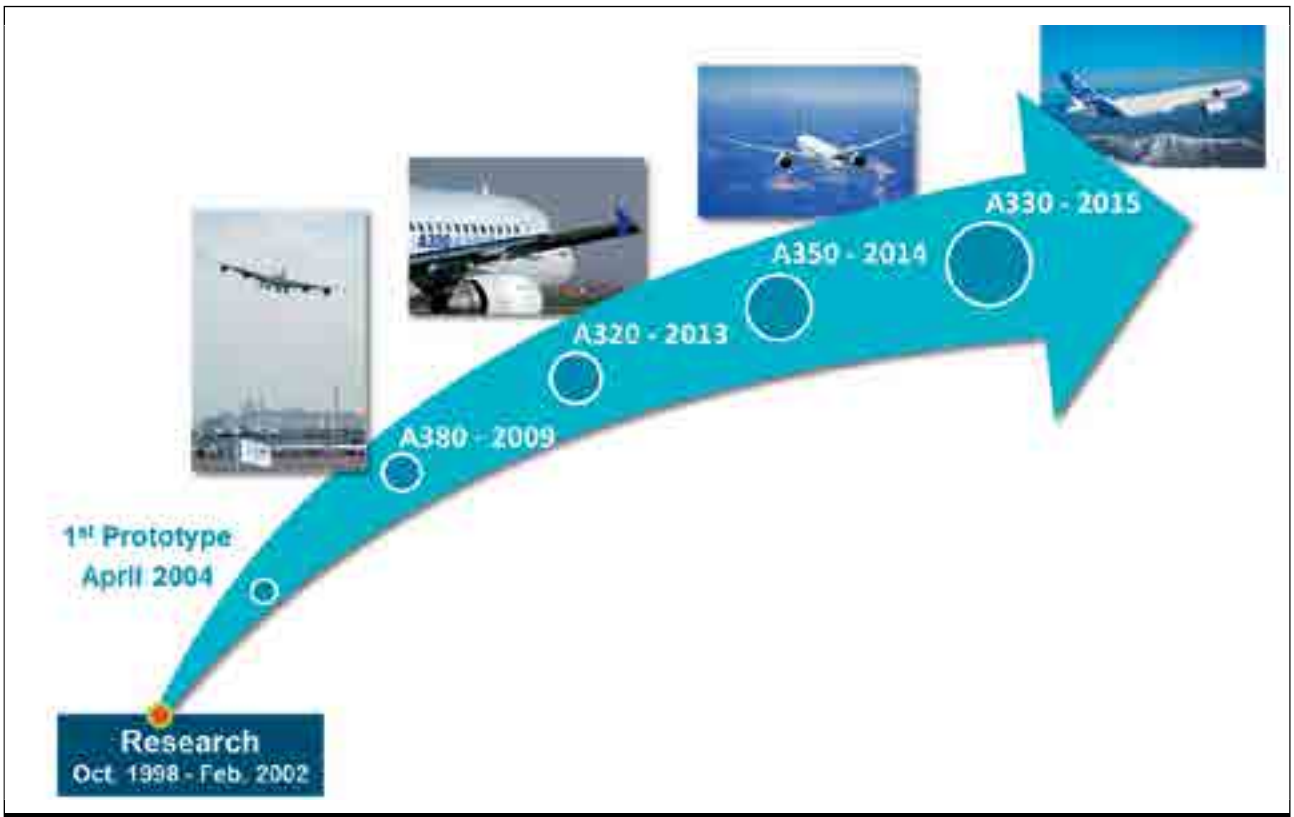


Figure 2 - Timeline of ROPS implementation in Airbus aircraft

Figure 3 - ROPS In-Air alerts for runway overrun risk

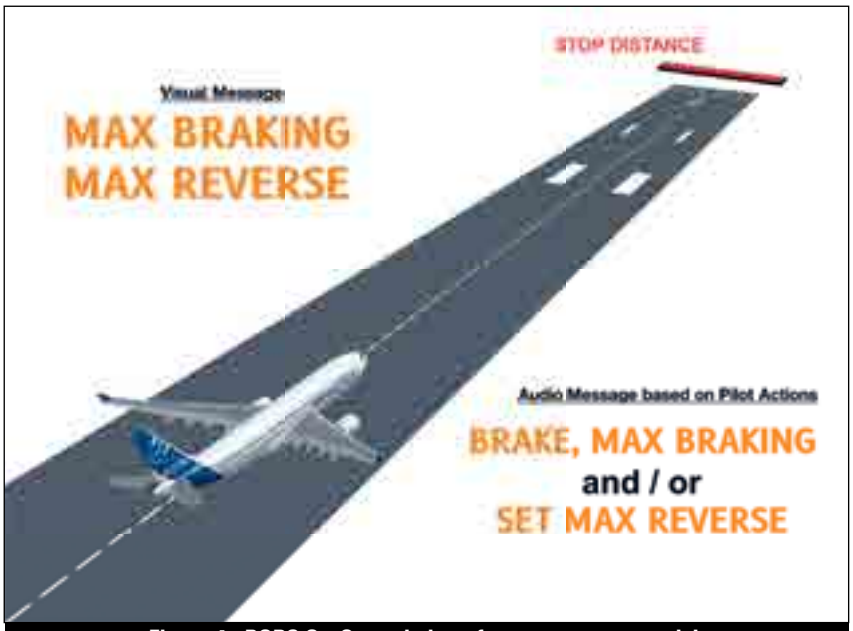


Figure 4 - ROPS On-Ground alerts for runway overrun risk

occasions, correctly alerting the flight crew that, due to rapidly changing conditions, the aircraft was now at a risk of a runway overrun. In all of these cases, the flight crews promptly followed procedures: one of these cases involved a low altitude Go-Around after the tail-wind increased by 10kt during short final, another case prompted the crew to Set Max Reverse on a slippery runway (even though ROPS is only currently certified on dry and wet runways) and another case prompted the crew to override 'Autobrake Low' and apply max manual braking.

The market response to ROPS so far has been remarkable. Nearly every A380 operator has selected ROPS, the system is standard equipment on every A350, ROPS has recently been certified for the A330 and is now entering into service and 150 Airbus A320 family in-service aircraft are already equipped.1 in 4 Airbus aircraft being delivered now have ROPS installed. Development has started on A350 to extend ROPS to contaminated runways.

Nevertheless, it is important to remember that ROPS is only one link in the global runway safety chain. As described in the European Action Plan for the Prevention of Runway Excursions (EAPPRE), each entity has a part to play in reducing runway excursions.

For aircraft operators, training and procedures remain fundamental to mitigate the risk of runway overruns. Whether an aircraft is equipped with ROPS or not, strict adherence to airline standard operating procedures (SOPs) and maintaining a stabilised approach are key components for a safe landing. Reviews of past overruns show that many runway excursions occurred despite aircraft meeting the stabilised approach criteria at the specified (e.g.1000ft/500ft) gates. For this reason, it is important to continuously monitor aircraft parameters and the aircraft's current position throughout the final approach, flare, touchdown and rollout. Once on the ground, timely application of deceleration devices will ensure the aircraft can stop in the planned and expected distance. ROPS, even if important, is only a last safety net before a major overrun risk.

For the civil aviation authorities, up-to-date information in the Aeronautical Information Publications (AIPs) is a key component to runway safety. ROPS uses an onboard runway database whose original source of information is the AIPs. Thus if ROPS is expected to correctly issues alerts to the flight crew, then the integrity of the runway database is essential.

For aerodromes, properly maintained runways play a key-role in ensuring that the aircraft can indeed achieve the stopping distance predicted. During contaminated runway conditions, it is essential to monitor changing conditions, report significant changes and clean the runway when necessary. A safe landing distance calculation is dependent on the flight crew knowing the actual runway state they will be landing on.

Together we can reverse the trend of runway overruns and improve safety during landing.

EDITOR'S NOTE:

More on the European Action Plan for the Prevention of Runway Excursions (EAPPRE) referred to above can be found at:

http://www.skybrary.aero/index.php/European_Action_Plan_for_the_Prevention_of_Runway_Excursions_(EAPPRE)

SHORT TERM CONFLICT ALERT (STCA) OPTIMIZATION FOR TMAS

If by any chance you can't find what you want, please remember that SKYbrary is a dynamic work-in- progress which needs continuous user feedback and benefits from user support. Be sure to tell the SKYbrary Editor about any difficulty you may have had making it work for you. If you can directly help us by identifying material we could use or even fill a gap by writing some content yourself then please tell us too!

We aim to provide wide coverage through both original articles and, especially, by hosting the best of what's already been written so that a wider audience can access it more easily in one place.

SKYbrary is also the place where you can access:

- all the documents of the **Flight Safety Foundation Operator's Guide to Human Factors in Aviation**
- the largest collection of selected **official accident & serious incident reports** from around the world anywhere in one place online

An article taken from **SKYbrary** is reprinted in each **HINDSIGHT**. For this issue, we have chosen **"Short Term Conflict Alert (STCA) optimisation for TMAs"**.

Description

STCA is a ground-based safety net intended to assist the controller in preventing collision between aircraft by generating, in a timely manner, an alert of a potential or actual infringement of separation minima. Generally, it is more difficult to optimise Short Term Conflict Alert (STCA) for Terminal Control Areas (TMAs) than for en-route airspace. This is because the nature of TMA operations makes it hard to tune the look-ahead parameters used by STCA to predict potential conflicts.

The reason for this is two-fold:

- TMA traffic is more closely spaced than traffic in en-route airspace; and
- TMA traffic undergoes far more turns in comparison to en-route traffic – often for much shorter periods of time and at higher rates of turn.

These two factors can result in relatively poor warning time performance and a relatively high number of STCA nuisance alerts in the TMA.

Solutions

With respect to the use of STCA in TMA airspace, the following avenues can be explored:

- improve the prediction law (e.g. reducing linear prediction parameters and use of standard turning prediction)
- optimise the filtering processes (e.g. implementing prediction filters which 'know' the traffic patterns associated with approach procedures)
- optimise parameters and sensitivity, possibly under the control of the user (e.g. defining STCA volumes at recognised hotspots, with specific parameters).

The key to a STCA system that performs well is to apply the conflict thresholds and prediction times that are most appropriate to each volume of airspace. This might mean defining some quite small STCA volumes in the TMA where very specific parameters will apply. For example, aircraft in stacks (holding patterns) rarely fly straight for more than a minute. Therefore, a linear prediction time set at two minutes is entirely inappropriate for holding aircraft and is, in fact, generally inappropriate for most of the TMA.

We have another case of Systems Alerts Overdose...
I wonder if keeping plain old STCA have been prevented this epidemic...

STCA volumes for different parts of the TMA should use different parameters. For example, an outer TMA zone can provide for a gradual change in the STCA parameters between en-route airspace and the busiest part of the TMA. The outer TMA zone provides a buffer between the en-route corridor and the busy inner TMA. Further consideration may also be given to setting up specific STCA volumes for lower parts of the airspace, for example, to address potential nuisance alerts between IFR and VFR traffic.

In some parts of airspace the future course of an aircraft is not predictable without specific additional information that only the controller or the pilot could disclose. However, there are some segments of certain flights when the aircraft trajectory is predictable based upon the approach procedures.

The most common STCA prediction filter is the linear prediction filter, which makes a straight-line prediction of the aircraft's trajectory. In the TMA, where turns are common (sometimes at high rates), the linear prediction assumption can be very inaccurate. If one aircraft starts to manoeuvre towards another the linear prediction may not detect a conflict in time. As a result, in addition to the usual linear prediction, some STCA systems use a turning prediction which activates when an aircraft is detected as turning by the tracker.

Related Articles

- STCA
- Level Bust in Holding Patterns
- Barometric Pressure Setting Advisory Tool (BAT)
- Radar Control – Collision Avoidance Concepts

Further Reading

- EUROCONTROL Safety Nets Guide, 21 May 2011
- NETALERT Newsletter no. 12 – "Short Term Conflict Alert in the TMA"

If you are interested in downloading back numbers of the **HindSight collection**
http://www.skybrary.aero/index.php/HindSight_-_EUROCONTROL

In the next issue of HindSight:
"Situational Awareness!?"

EUROCONTROL

Putting Safety First in Air Traffic Management

This publication has been prepared under the auspices of the Safety Improvement Sub-Group (SISG) of EUROCONTROL.
The Editor in Chief acknowledges the assistance given by many sources in its preparation.

This edition is printed in 5500 copies