PRELIMINARY RESULTS FROM A EUROPEAN SAFETY R&D PROGRAM

Barry Kirwan

EUROCONTROL Experimental Centre, Centre de Bois des Bordes, BP 15, F-91222 CEDEX, France

Abstract

This paper is concerned with safety research and development (R&D) that is necessary to ensure continued safety of air traffic management, given the major changes that will occur in European ATM over the coming years. The program of safety R&D was developed following the two tragic fatal accidents in Europe of the Milan Linate runway collision and the Ueberlingen mid-air collision. Eight high priority safety R&D work areas were defined: organisational (safety) learning; enhanced safety and risk assessment approaches; integration of safety into early ATM system design processes; short term key risk areas; longer term key risk areas; safety culture; development of a safety roadmap towards the European ATM vision of 2012; and enhanced safety R&D coordination. This paper distils key results and achievements from each of these eight areas.

Introduction

Following two severe accidents which involved significant ATM contributions, namely the runway incursion in Milan airport in Italy [1] and the mid-air collision near Ueberlingen in Germany [2], the role of safety received a new focus in its agenda. A High Level European Action Group on ATM Safety (called 'AGAS') was set up to consider the actions needed to prevent recurrence of these and similar accidents. These deliberations, over the period of approximately nine months, yielded eight 'threads' of action, which were put into a Strategic Safety Action Plan [3]. This paper concerns one of these threads, the one concerned with Safety Research and Development (SRD). Whereas the other seven threads were primarily concerned with relatively short-term measures (e.g. guidance on runway safety, safety regulation, safety assessment, safety nets improvement, etc.), the SRD program was more medium-long term in its focus. This paper therefore outlines the safety R&D program and objectives, and the results obtained at this point in time, roughly half-way through its initial timeline.

Background

The Safety R&D Plan [4] that resulted from the AGAS deliberations produced eight threads or work areas for safety R&D – these and their backgrounds are described in the succeeding sections of the paper.

I - ATM must become a learning organisation

Methods to collect data now exist, and data collection is occurring in many ANSPs. Safety learning mechanisms now need development.

II - ATM must have suitable methods with which to anticipate and protect itself against risks

ATM needs to adapt risk assessment and management methods from other industries and develop new ones where required.

III - Safety must be built in at the early stages of ATM system design, right through to implementation

Safety lessons and information need to be fed into the design process throughout the design life cycle, from concept development to transition to operations.

IV - ATM must improve safety in key near-term risk areas

Level busts, runway incursions, safety net interactions, events at low vigilance periods – these are key risks where more understanding is needed to reduce risk.

V - ATM must plan for key longer term risk areas

Airspace and traffic patterns are becoming more complex – ways to support the controller in increasingly complex traffic patterns need to be developed.

VI - ATM must be sure that the systems it is developing will deliver the required safety levels

The broad 'roadmap' in terms of changes is laid out (e.g. ATM 2000+, etc.). However, exactly how each roadmap 'component' adds safety individually and as a part of the whole of the future ATM system, needs to be assessed and assured so we will meet safe capacity targets.

VII - ATM must retain its 'High Reliability' status and its 'safe culture'

Safety culture needs to be assured for proposed fundamental ATM changes such as Single Sky, and delegation of separation tasks to the cockpit.

VIII – The above should be achieved effectively and cost-efficiently

There needs to be co-ordination of a focused effort between different R&D Centres, to avoid duplication of work or following dead ends, and to make best use of combined available resources, facilities and competencies.

This paper describes the results found so far in the projects that aim to serve these principles. Two of the projects described below (ASMT & ACAS Event Analysis) actually date back to a previous safety program, but they overlap with the current one and so have been included in the paper.

I - Organizational Safety Learning

Automatic Safety Monitoring Tool

Learning cannot occur without feedback. Therefore, a cornerstone of any safety program is that of gaining and understanding safety feedback from the operational system. This means in practice that ATM safety-related events can be detected and measured, and associated data collected and analyzed. However, in European ATM there has not generally been a consistent approach to the detection, recording and analysis of such key data. In particular, there has been reliance on self-report of incidents and subsequent documentation. But a safety-related event may be missed by controllers and pilots for a number of reasons, and so it is better to have an automatic radar-data based approach for identifying when a potential safety-related event has occurred. This alone will yield comprehensive and consistent safety data.

Therefore, over the past five years or so a tool has been developed to automatically record safety related events in an operational control centre. The tool is known as Automatic Safety Monitoring Tool (ASMT [5]). This tool records a number of adjustable parameters automatically, and can be used to assist in understanding why incidents such as losses of separation or other safety-related events (e.g. level busts) have occurred. Whilst a few Air Navigation Service Providers (ANSPs: e.g. in the UK and France) already had a form of automatic recording, the aim was to develop a powerful and generic method and tool. The R&D for the development of ASMT was successfully completed at the end of 2003, having undergone implementation and testing in three separate European countries, and the tool transferred to EHQ for wider dissemination throughout Europe. Five countries now have ASMT and several others are considering implementation at this stage.

SAFLEARN

A project called SAFLEARN [6; 7] has been developed to try and help future projects and visions of ATM learn from past and current 'mistakes'. SAFLEARN collects incident information (e.g. loss of minimum separation between aircraft) from participating European member states, and stores the information. It then works with a future ATM project such as CORA (Conflict Resolution Assistant – a tool which advises controllers of conflict avoidance actions) to see whether CORA could overcome certain incident causes. If this is the case, then the project will 'add' safety value to future ATM. Such safety 'propensity' can be recorded so that systems such as CORA retain the elements that make them safe and add safety.

Additionally, there may be aspects of a system like CORA where analysis of past but relevant incidents suggests further areas of concern. For example, in the SAFLEARN analysis of CORA, it was realized that the CORA system could be better 'defended' with respect to military traffic maneuvering within or at the edges of 'Danger Areas' (military practice areas). This type of insight can lead

to the project taking on additional safety requirements.

Lastly, there may be residual incidents that would not be resolved by a system like CORA, unless it was developed with safety in mind together with a related functionality such as Datalink. In fact, in the CORA SAFLEARN study it was noted that CORA + Datalink could resolve certain current incident types, if 'joint' safety requirements for both systems were developed. This requires a non-compartmentalized approach to safety and to design itself, but is feasible.

At present, SAFLEARN is still being developed and explored as a concept, and the incident database is being developed. SAFLEARN has been applied to four projects and will be applied to roughly the same number again in 2005.

ACAS Event Analysis

The second approach in this area is not new to Eurocontrol, and is a joint effort run by EHQ, with the analysis cell located in the EEC. Essentially, ACAS (Airborne Collision Avoidance Systems such as TCAS – Traffic Alert and Collision Avoidance System) related events are analyzed in depth to determine if there are any trends arising, or if there are problems occurring with existing equipment or equipment being updated.

As an example of ACAS event analysis leading to organizational learning, there is the case of the TCAS alert command 'Adjust Vertical Speed Adjust', which means effectively 'reduce the current vertical ascent or descent rate' (i.e. reduce climb rate if climbing; reduce descent rate if descending). Unfortunately, it was revealed a couple of years ago that a number of pilots in Europe were misunderstanding this command and acting contrary to the intention of the instruction, leading to increased risk of collision. This trend was detected, and studied over a period of time before issuing a newsletter to all pilots concerning the issue [8] both to raise awareness and as a preventative measure. Alternative wording to this instruction is now being investigated and considered by the industry.

II - Enhanced Risk Assessment

Adapting risk assessment tools to ATM

Formal risk assessment is relatively new to ATM, and is enshrined in the new Eurocontrol Safety Regulatory Requirement on risk assessment (ESARR 4 [9]) which also embodies the suggested Safety Assessment Methodology (SAM). The SRD program of work has sought to help enhance this SAM to ensure it is able to deal with all related risks.

The first phase of this research was to carry out a study of more than 500 techniques of safety and risk assessment in nine different industries [10]), including techniques dealing with hardware, software, human and environmental contributors to risk in various life cycle stages. These techniques were evaluated and compared to the existing approaches in the SAM, to see which ones could be adapted to ATM, and also where new techniques would need to be developed for ATM specific attributes. The nineteen techniques identified for adaptation are as follows:

- Bias and uncertainty assessment
- *Bow-tie analysis*
- Common cause analysis
- *Event tree analysis*
- External events analysis
- *Fault tree analysis*
- *Hazard & operability study (HAZOP)*
- Human error assessment and reduction technique (HEART)
- *Human error data collection (CORE-DATA)*
- *Hierarchical task analysis*
- *Hazard tracking & risk resolution*
- *Human error data generation*
- *Human factors case*
- Operational readiness review
- Reliability centered maintenance
- Software failure modes and effects analysis
- State machine hazard analysis
- *Technique for the retrospective and cognitive analysis of human errors (TRACER – predictive version)*
- *Use of expert judgments*

So far, those in italics above have been tested at the EEC in the context of safety case work for future ATM systems (e.g. see [11, 12]). In particular, there has been a focus on human elements in safety work, both using qualitative, and more recently quantitative approaches. This work is continuing, and in fact two new areas have been identified. The first concerns the interactions between different future ATM concept elements (requiring an approach dubbed 'cross-boundary HAZOP', currently under research). The second is the development of an approach for identifying and protecting against safety impacts of running a live trial of a prototype new system or tool. This latter approach is called Live Trial HAZOP, and has been applied to the live trials for Medium Term Conflict Detection and Mediterranean Free Flight

procedures. In the MTCD case, the approach developed experimental safety protocols, and 'reversionary' procedures in case of a safety threat to the trial, which were invoked once (and worked) during the trial.

Integrated Risk Picture

Whilst individual risk assessments and safety cases have been proceeding and developing for individual systems, what is ultimately needed is a complete risk 'picture' of the future system to see where risks are adequately addressed an where more safety effort will be needed. Furthermore, in order to realize such an approach, a 'baseline' is needed of the risks now, to compare against those estimated for a future significant date (e.g. 2012, when many currently proposed new systems will be in place).

This area of work has therefore commenced with the development of a total gate-to-gate risk picture for 2004, using a series of data sources and modeling techniques such as fault and event trees, as well as a new approach for modeling the impact of other contributory influences that cannot be modeled using such methods [13, 14]. The overall ATM contribution rate to fatal aviation accidents is around 4%. This figure, although low, can be usefully analyzed further to see how ATM contributes to different types of accident category. Therefore, a number of accident categories have been used, and associated ATM contributions assessed:

- Mid-air collision (72%)
- Controlled flight into terrain (CFIT) (4.3%)
- Runway collision (18.1%)
- Taxiway collision (10%)
- Wake turbulence accident (6.9%)
- Loss of control in flight (-)
- Single aircraft take-off/landing accident (-)
- Structural accident (-)
- Fire/explosion (-)

Not surprisingly, ATM makes a significant contribution to certain accident categories, notably mid-air collisions, which are thankfully very few in number compared to other categories (e.g. CFIT). Furthermore, particular causes can be identified that contribute significantly to each accident category. For example, certain events such as '*controller fails to recognize loss of separation'; 'short-term conflict alert fails to give warning in time'*; and *'no independent controller monitoring'* feature significantly in the risk analyses for mid-air collisions. Such results then lead to potential future safety studies along the following lines:

- Reduction of controller distractions
- Better conflict detection in time
- Improved controller response against conflicts with military aircraft
- Improved detection of terrain conflicts

This work for 2004 already therefore yields some important insights for safety needs for the future. However, it has also opened up a potential avenue for exploring how ATM could help accidents for which it is not a significant contributor, but for which it could be an effective preventive mechanism or safety barrier. For example, whilst ATM is not a major cause of CFIT, the work so far suggests that ATM could nevertheless help reduce significantly the frequency of such accidents. Therefore, if the 'total safety picture' is taken, e.g. from a passenger's perspective, reducing CFIT by 50% would be far more beneficial than reducing mid air collisions by the same amount. At present this is not the scope of the work, but it has certainly opened up some interesting questions.

Further work in 2005 will aim both to further validate the results for 2004 with new data sources, and begin work on the integrated risk picture for 2012. The result will be detailed insights into the main contributions from ATM to risk, across the entire ATM gate-to-gate process, along with well-balanced safety requirements and safety objectives for future systems to achieve.

III - Safety in Design

Design contribution to accidents

When the third principle was first proposed, there was an understandable initial response from some designers / concept developers, that safety should occur later, and was not related to very early design. This prompted a study to determine the contribution of design to accidents. The study looked at several industries and found that the broad contribution was in fact 50 – 60% [15]. Moreover, typical design 'failure modes' were also identified, such as the following:

- Use outside intended design envelope
- Failure of defense in depth
- Misconceptions between designers and operators
- Incorrect functioning leading to mistrust by operators
- Adding or modifying existing system without considering effects on whole system or side-effects
- Unexpected failure mechanisms

This analysis therefore reinforced the need to consider safety early in the design process, leading to the development of a Safety Policy for the EEC [16] and the development (ongoing) of a Safety Management System for the EEC, and a Safety Assessment approach for EEC projects (next sub-section).

Safety Assessments for New Designs

Although as already mentioned earlier there is a Eurocontrol Safety Assessment Methodology (SAM) for future systems, there was a need for a methodology that was more flexible for early concept design projects. Therefore an approach called SAND (Safety Assessment for New Designs) was developed. This process involves a safety plan dictating the scope of the safety work and safety activities for a project, and then a series of activities:

- HAZOP – for hazard identification
- TRACER – for error identification
- Human Factors Case
- SAFLEARN
- Cross-Boundary HAZOP
- SAFSIM (next sub-section)
- Live Trial HAZOP

Some or all of these will be applied to each individual project according to the needs identified in the corresponding safety plan. Additionally, as hazards are identified from whatever source, they are entered into a hazard logging system for that project. The aim is then to evaluate the hazards and decide if changes need to be made to the system concept/design. This leads to specified safety requirements for that project. At the completion of the concept design stage, this information is passed on to recipients, either other Eurocontrol parties who will continue the system development, or other stakeholders who may wish to pursue the concept to design maturity and implementation. In both cases the recipients will continue safety work using the SAM or equivalent approaches as per ESARR 4, but the SAND process ensures that the concept designs come already with a degree of safety input and key safety requirements identified. This should help avoid accidents caused by design.

SAND also interacts with the Integrated Risk Picture (IRP) mentioned earlier. The IRP works top-down, and SAND works 'bottom-up'. At a certain point, they must meet. This means that SAND helps ensure that IRP does not miss any detailed but critical failure modes, and IRP can inform SAND and projects in general of the degree of safety required by each system. This effectively gives individual projects (such as CORA, MTCD, datalink etc.) safety targets which can be translated down into detailed safety requirements.

The SAND work is in progress, but already SAND activities (HAZOP, TRACER, etc.) are being applied to around 10 projects, and some safety requirements have already been identified.

Safety insights from simulations

At the EEC, real-time simulations are often carried out to test new concepts and procedures, using the full-scale simulator at the EEC, or a number of smaller facilities, including a Human Factors Laboratory. Although these are simulations and not reality, there is still a chance to gain insights from such simulations that can inform safety. A project called SAFSIM (Safety insights in simulations) [17] was therefore set up to determine how to do this. The project surveyed a number of safety and human factors measurement approaches that could be adapted to a simulation environment, and catalogued how to use these approaches either singly or in concert. Examples of such approaches are mental workload measurement, situation awareness measurement, communication load monitoring, loss of separation monitoring, error monitoring, team interactions observation techniques, and psycho-physiological measurements. Additionally, the idea of 'seeding' particular hazards or 'non-nominal events' into the simulation was explored in a simulation on Mediterranean Free Flight [18, 19], yielding useful qualitative information for the safety case. SAFSIM is still in early stages in terms of its application, and is currently being integrated as part of the SAND process.

Safety & Requirements Engineering

Another approach being explored is the SPECTRUM approach developed by Leveson [20]. This aims to enhance safety via a formal Requirements Engineering process and hierarchical specification of safety requirements in the design engineering itself. Although this approach appears favorable, it does not appear at the moment to fit with that type of design and conceptualization environment at the EEC – these processes are quite creative and more 'organic' in nature than a formal and more structured requirements engineering process as may occur in industry or later in the design stage. Nevertheless, the approach is still being evaluated, for non-EEC usage.

IV & V - Key Risk Areas

After the accidents and ensuing deliberations, a number of key risk areas that could benefit from safety R&D were identified. These were as follows:

- Level busts
- Interactions between safety nets
- Low Vigilance &Controller Performance
- Airspace Complexity

Level Busts

A level bust is when an aircraft deviates from its assigned flight level. Level busts have been considered a problem particularly around certain airports in Europe, but also level busts can be hazardous in cruise phases of flight if, for example, a pilot mishears an instruction, and the controller fails to detect the mishearing via the pilot read-back. The aircraft may then change its level by one thousand feet for example, which is dangerous if that level is already occupied by another aircraft.

The R&D approach was to try and understand why such events are happening. The method chosen for such study is called SMART [21], and is a detailed barrier analysis approach. It works by building up a detailed 'safety architecture' of all the physical and procedural barriers (e.g. including safety nets such as ACAS and short term conflict alert, and procedures such as listening to read-backs, etc.). This safety architecture is developed as a model, and then incident and accident cases are used to validate the model, and to determine which barriers are working and which are failing. The approach is useful in that it highlights the 'safety value' of each barrier, which may differ from expectations. The safety architecture can also be used to consider the added value of future tools or safety nets or procedures – effectively acting as a simulation to see which barriers will be reinforced or negated, or what new barriers might be added, by new developments.

The safety architecture for level busts has now been developed, and has reinforced the opinion that level busts will not truly be defended against until a non-human-reliant approach to verification of understanding of the instruction and aircraft intent has been established (e.g. via datalink technology – up-linking the command to the pilots, and then down-linking what the pilots have implemented into the onboard Flight Management System). Until such time, other solutions must be explored, and best practice guidance developed by EHQ and others [22] needs to be implemented across Europe.

Interactions between safety nets

The mid-air collision in particular highlighted the potential (although a low probability one) for interactions between safety nets which could increase risk. The adequacy of safety nets (such as Short term conflict alert and TCAS, as well as ground-based altitude warning alerts) is currently therefore being explored using the SMART approach as for level busts. The safety architecture has been developed, and the next step is to simulate the advantage of a potential function which would downlink to the controller the fact that an aircraft has received a TCAS Resolution Advisory (climb/descent instruction). This potential function was identified during the AGAS deliberations following the mid-air collision, and is also recommended in the official accident report [2]. The feasibility of developing such a function (called 'RA Downlink') is also being explored in a series of simulations at the EEC, wherein controllers can experience how it would work and appear on the radar screen. In the longer term it is hoped that the safety architecture can inform design of future safety nets or improvements to existing safety nets.

Low Vigilance

Low vigilance refers to a decrease in controller awareness such as fatigue (e.g. at the end of a demanding work period), time of day (e.g. during the night shift), low workload (leading to boredom or distraction). This study area arose out of the AGAS deliberations, but is also recognizable to many controllers. However, finding hard evidence for it is not so easy, as often such contributory factors are not recorded in incident reports (e.g. a report may say the controller was not busy at the time of the incident, but is unlikely to say that 10 minutes earlier he was very busy).

The initial approach has therefore been to canvas controllers in several operational centers around Europe, to see if there is a perception that this is indeed a real problem. Results from the first Center have indeed confirmed the importance of this area:

<u>Main Statistics (47 controllers):</u>

- 30% experience low density traffic 'often' or 'very often'
- 77% less alert during low density traffic periods
- 24% thought there was a high risk of an incident during low vigilance periods

- 57% can detect when they are 'low vigilant'

Typical Causes:

- Low traffic; fatigue; distractions; boredom

Safety-Relevant Outcomes:

- Slow reactions; missing conflicts & readbacks

These initial results do suggest that this area needs further investigation. The results from two other operational centers are currently being analyzed. The next step will be to integrate the results and begin to explore compensatory measures to defend against the impacts of low vigilance.

Airspace Complexity & Safety

A longer term key risk area identified concerns increasingly complex airspace in some parts of Europe and its impact on safe controller performance [23]. This is being investigated from several quarters. First, a set of incidents available from the SAFLEARN database have been studied to see what types of issue lead to complexity. This analysis has identified certain potential pre-disposing factors, including some combinations of factors (usually in pairs) that appear to lead to safety-related complexity:

- Short-sector & vertically changing traffic
- Volume of traffic & high communication load
- Ongoing training & no controller 'plan B'
- Direct routes & only 'one pair of eyes'

Secondly, an approach called 'Complexity HAZOP' has been tested to see if, at the airspace design stage, potential complexity-related problems can be identified and resolved before the airspace re-design becomes operational. HAZOP appeared to work in one case (airport) but not in another (en route), so this work is inconclusive at this stage, and requires a further trial of the approach. Thirdly, UK NATS (National Air Traffic Services) has carried out promising work entailing extensive analysis of incidents correlated to certain measures of procedural complexity. Via the FAA-Eurocontrol Action Plan on Safety (see VIII below), Eurocontrol, NATS, FAA and NASA are in the process of sharing information to try and better understand this area with respect to safety, and to develop safety assurance processes.

VI – Safety Roadmap

Since European ATM will change significantly over the coming years, it is important that safety is assured in the transition and evolution process. The changes will not necessarily happen all at once, and so there is an opportunity to measure the safety impact of changes as they assure. The idea of the safety roadmap is therefore quite straightforward. The Integrated Risk Picture project identifies the baseline picture for 2004 and for 2012 (and incidentally for 2017, the next major change period). These two 'pictures' show what will be implemented, and how much safety should change as a result. This will lead to the development of a safety evolution plan, showing that at each step change there should be a certain increase in safety. This then is the roadmap. It then requires monitoring of key safety parameters (e.g. losses of separation, etc.) throughout the evolution period to determine if the system changes being implemented are in fact delivering the required safety. This is the Safety Roadmap concept.

The roadmap itself is not yet devised, as it needs first both 2004 and 2012 Integrated Risk Pictures. The Roadmap however should be available by 2006. At this point, safety monitoring parameters and processes need also to be implemented. This will enable true safety management of the evolution of ATM safety in Europe. It should also be noted that certain Air Navigation Service Providers (ANSPs) have already developed their own Roadmaps (e.g. in NATS UK's case, this is called the 'Safety Staircase').

VII - Safety Culture

EEC Safety Culture Measurement

Safety culture [24] concerns the priority given to safety in an organization or organizational unit. Effectively, having rules and procedures alone will never be enough to assure safety. Without a positive attitude towards safety, and importance given to it throughout an organization from the top down, an organization is unlikely to allocate appropriate and sufficient resources to safety, and in many cases will not even have the right procedures, or else will only pay 'lip service' to them. Given such considerations, it was decided that the EEC should examine its own safety culture before setting out to measure that of others.

Due to the recognized importance of safety and safety culture in the EEC itself, a safety culture survey was carried out in the EEC to measure its own safety culture level [25]. On a maturity level of 1 – 5 the EEC in 2003 scored 2.3, suggesting that there is certainly room for improvement. This survey was followed up by a Safety Management System (SMS) analysis, to develop and implement a research-oriented SMS for the EEC by 2006 [26]. In parallel, an internal group to foster safety culture has been in operation (called SAGE – Safety Awareness Group at the EEC), which helps to coordinate safety

awareness, training, safety policy, and SMS development.

EEC Safety Management System (SMS)

As mentioned above, a SMS is being developed for the EEC. This entails defining work processes and procedures for integration of safety into projects. These projects as a whole will integrate to form the future ATM operational concepts for 2012 and beyond, so it is important that the appropriate safety studies are carried out for projects individually (via SAND) and integrally (via the Integrated Risk Picture). The SMS will integrate many of the methods being developed and referred to in this paper (e.g. SAFLEARN, SAND, IRP, SAFSIM, and others) to enable this future vision of ATM to deliver a safe operating system. The SMS also links with some of the EEC safety culture activities such as training in safety so that it is properly understood (at project manager level, practitioner level, and at a general level amongst all staff at the EEC), and assuring safety resources are sufficient and allocated appropriately.

Future Systems Safety Culture

ATM is usually considered a very reliable and safe system, compared to many other industrial sectors, and this is in no doubt greatly attributable to the controllers themselves and their professionalism and attitudes towards safety. However, the various changes that are going to happen could change the nature of the controllers' job, and thus could directly or indirectly affect their skills and attitudes. It is therefore advisable to try and predict the impacts of future changes on controller performance well before such impacts may arise. Unfortunately, predictive safety culture approaches are rare or non-existent. Therefore, a survey method was developed to interview controllers themselves about future and also past changes with respect to safety culture. Past changes include short term conflict alert, reduction of vertical separation minima, and certain automated tools that are now available, as well as changes such as new operational environments (new radar screens and functionality etc.).

Four European operational ATM centers participated in the study. At each of these centers, the controllers had experienced changes in level of automation etc. over the past few years.

During a literature review for the study, the following nine dimensions were identified with which to structure the interviews:

- Teamwork
- Communication
- Trust in people
- Trust in equipment
- Understanding of others' competence
- Personal responsibility for safety
- Understanding of risk
- Job pressure
- Job satisfaction

The first main result was that the controllers generally did not feel their attitudes towards safety (i.e. perceived responsibility and perceptions of risks) had been affected by past changes. However two of the dimensions in particular (teamwork and communications) were perceived as vulnerable to change.

The controllers were then asked about the likely impact of proposed future systems such as datalink, medium term conflict detection and resolution tools, temporary delegation of separation responsibility to the cockpit, etc. The results [27] suggest that the two main factors most sensitive to change will still be teamwork and communications. Additionally, understanding of risk, personal responsibility, and job satisfaction were thought to be sensitive to future changes. However, two controller comments are worth citing with respect to such results. The first is that the controllers recognized that changes in such dimensions could be positive as well as negative. The second is that, with respect to job satisfaction, the controllers recognized that concerns they have at this stage may not be realized in practice (based on experiences with introduction of tools in the recent past). The next phase of this work will feed back the information to the various projects to consider a way forward.

VIII – Safety Coordination

Safety R&D needs to be communicated beyond the EEC itself. Also, the EEC's resources for safety studies and assessments are themselves limited. It is therefore necessary to communicate and coordinate with other parties concerned with safety R&D. Initially such coordination has occurred with other safety departments in Eurocontrol itself, such as those concerned with near-term and longer term safety, and with safety regulation, as well as Eurocontrol's operational safety manager at the Maastricht Control center, and the safety training people in Luxembourg. This coordination has been followed by coordination with certain European countries who participate in some of the research projects, as already mentioned in several places above.

Additionally, a FAA-Eurocontrol Action Plan (AP15) has been developed and enacted, which entails working on a number of safety issues of common interest to the US and Europe. One notable example has been the development of a comprehensive toolkit of safety assessment methods [28], building on the survey of techniques mentioned earlier, but with some additional techniques used in the aviation domain. AP15 is also working on the definition of a logical set of safety principles, as well as the relation between Human Factors and safety, and specific issues such as complexity and safety.

The current focus in terms of coordination relates to a survey of different European States in terms of their safety R&D programs and aspirations. Over twenty countries have recently participated in the survey, which aims (in Autumn 2005 via an international workshop) to determine ATM safety R&D priorities across Europe, as well as potential partnerships to tackle key issues. This survey and workshop are being sponsored by the European Commission [29].

More generally, dissemination of EEC safety R&D activities is now achieved via the Eurocontrol website [30], where reports and safety R&D plans etc. are now publicly available.

Conclusions

This paper has aimed to give a snapshot of an ATM safety R&D program, and to highlight some key results. Although these results are to an extent preliminary in nature, in that the program of work is at the half way point, there have already been some useful results and insights gained from work so far. Over the next eighteen months it is hoped that the work will consolidate, delivering a safety roadmap, future ATM concepts with associated safety requirements, and insights into how to resolve key risk areas. At the same time it is hoped that ATM becomes more of a 'safety learning' industry, and improves its own safety culture in a way that continues its current high safe performance into the future.

Disclaimer

The opinions expressed in this paper are those of the authors and do not necessarily represent those of the parent organization or its affiliates.

Acknowledgements

The author wishes firstly to acknowledge the Safety Research Team: Veronique Begault, Garfield Dean, Fabrice Drogoul, Catherine Gandolfi, Adrian Gizdavu, Rachael Gordon, Brian Hickling, Paul Humphreys, Tony Joyce, Yann Kermarquer, Andrea Pechhacker, and Eric Perrin.

Also the author wishes to acknowledge the following: Andrea Antonini, Corinne Bieder, Henk Blom, Laurent Bocquet, Deirdre Bonini, Mete Celiktin, Matt Clear, Mirna Daouk, Marc Durasse, Mariken Everdij, Grant Foster, Huw Gibson, Jamie Henderson, Alistair Jackson, Richard Kennedy, Steve Kinnersley, Patrick Mana, Jean Paries, Alfred Roelen, Ed Smith, John Spouge, Oliver Straeter, and Appie van der Welle.

References

[1] ANSV 2001, Final Report: Accident Involved Aircraft Boeing MD-87, registration SE-DMA and Cessna 525-A, registration D-IEVX, Milano Linate airport October 8, 2001. ANSV 20/01/04 - N.A/1/04 www.ansv.it

[2] BFU Report 2004, Investigation report AX001-1-2/02. Bundesstelle fur Flugunfalluntersuchung (BFU), http://www.bfu-web.de, May.

[3] Eurocontrol 2003, Strategic Safety Action Plan: http://www.eurocontrol.int/ssap/public/standard_page/agas.html

[4] Kirwan, B. 2003, Safety Research & Development Plan, *March* 2004*,* EEC Publication, Brétigny, France.

[5] Bocquet, L. 2003, Automatic Safety Monitoring Tool ASMT – HMI User Guide, EUROCONTROL Experimental Centre, EEC/SAF-M-E1/ASMT/V2.3/HMI/UserGuide, February 2003

[6] Bonini, D., Joyce, A. 2004, *Designing Safety into future Air traffic Control system by Learning from operational*, Human Factors and Ergonomic Society Conference, Delft, Netherlands.

[7] Joyce, A. 2005, (in prep) Final Report on the SAFLEARN Process. EEC Note.

[8] Eurocontrol 2004, Adjust vertical speed adjust – Safety Bulletin on: http://www.eurocontrol.int/acas/

[9] Eurocontrol 2003, ESARR 4 & Safety Assessment Methodology: http://www.eurocontrol.int/src/public/standard_page/esarr4.html

[10] Everdij, M. 2004, *Review of techniques to Support the EATMP Safety Assessment Methodology,* EEC Note 2004-1, Brétigny, France.

[11] Callan, K., Siemieniuch, C., Sinclair, M., Rognin, L., Kirwan, B., and Gordon, R. 2004, *Review of Task Analysis for Use with Human Error Assessment techniques within ATC Domain*, Contemporary Ergonomics, Swansea, UK, pp.293-297.

[12] Shorrock, S. 2003, Individual and Group Approaches to human error identification, Eurocontrol Note 2003-8, Brétigny, France.

[13] Perrin, E. and Spouge, J. 2005, Safety Management Coping with Complexity in Air Traffic Management 27 – 30 June, ESREL 2005, Poland.

[14] Perrin, E. 2005, (in prep) First step towards a uniform and system wide approach to safety: the Integrated Risk Picture for European Air Traffic Management in 2004. EEC Report.

[15] Roelen, A., Kinnersley, S., and Drogoul, F. 2004 Review of root causes of accidents due to design. EEC Note 14/04.

[16] Garot, J-M., Andribet, P. and Kirwan, B. 2004, *Safety Policy*, EEC Publication, Brétigny, France. Website address: http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_safety_documents/EEC_Safety_Policy_001.pdf

[17] Antonini, A. and Kermarquer, Y. 2004, *HITL (Human in the loop) Safety Experiments guide,*, EEC publications, Brétigny, France. (available on web-link [30]).

[18] Gordon, R., Shorrock, S., Pozzi, S. and Boschiero, A. 2004,, *Using human error analysis to help to focus safety analysis in ATM simulation: ASAS separation*, Human Factors & Ergonomics Society Conference, Cairns, Australia,.22- 25 August.

[19] Pozzi, S. and Marinella, L. 2004, Report of the Comparison of the ASMT Data Collected from Real Time Simulations with MFF OHAs (Hazard Analysis) – see website [30]

[20] Leveson, N. 2000, Completeness in formal specification language design for process control systems, proceedings of formal methods in software practice conference, August 2000.

[21] Woldring, M. 2003, The development of a Safety Management Tool within ATM (HERA-SMART). Eurocontrol EATMP/HRS/HSP-002-REP-08 05 2003.

[22] Level bust toolkit – see website: http://www.eurocontrol.int/safety/public/subsite_homepage/homepage.html

[23] Kirwan, B., Scaife, R., and Kennedy, R. 2001, Investigating complexity factors in UK air traffic management. Human Factors & Aerospace Safety, 1, 2, 125 - 144.

[24] International Atomic Energy Authority (IAEA) 1986, Summary report on the post accident review meeting on the Chernobyl accident 75-INSAG-1. IAEA, Vienna.

[25] Gordon, R. and Kirwan, B. 2004, *Developing a Safety Culture in a R&D environment,* Human Factors & Ergonomics Society Conference, Delft, Netherlands, 27-29 October.

[26] Perrin, E. 2005 (*in press*) EEC Safety Work Plan. EEC Note.

[27] Gordon, R. 2005, (*in prep*.) Changes in safety culture due to new technology. EEC Note.

[28] FAA Eurocontrol Action Plan 15 2005, ATM Safety Techniques and Toolbox. On website [30].

[29] CAATS Website: http://www.caats.isdefe.es/

[30] EEC Website on Safety R&D:

http://www.eurocontrol.int/eec/public/standard_page/safety.html

Key words

Safety, research & development, safety management, safety culture, safety nets, safety assessment, organisational learning, level busts, accidents

Biography

Dr Barry Kirwan trained as a psychologist and then in Human Factors, and gained a PhD in Human Reliability Assessment. He has worked in nuclear power, chemical, offshore petrochemical, marine and air traffic industrial sectors. He has been Head of Human Factors in British Nuclear Fuels, a lecturer in Human Factors in Birmingham University, Head of Human Factors in National Air Traffic Services (UK), and is now Safety R&D Coordinator for Eurocontrol, based at the Eurocontrol Experimental Center in Brétigny, South of Paris.