Innovative Methods for Safety Assessments SAF

Rapporteur: Henk Blom, NLR
Session Chair: Dres Zellweger

Papers & Analysis

Paper 19, A systems-engineering approach to assessing the safety of the SESAR Operational Concept, presented by Eric Perrin, EUROCONTROL.

The paper continues the EUROCONTROL work that has been presented at ATM2007 in Barcelona. Both their ATM2007 paper as well as the current paper explains in a very elegant way why the traditional engineering directed safety assessment approaches that are widely used in the aviation industry, are well suited to evaluate the reliability of new systems but fall short in assessing how such new systems impact the safety of an advanced ATM concept of operation. This omission has been explained for the example of using ADS-B for areas that are not covered by radar surveillance. The traditional safety assessment points out that ADS-B brings with it hazards that pose certain safety risks that have to be mitigated, but it does not show by what factor (referred to as Success Factor) the safety risk of flights under control by ATC using ADS-B would be in comparison to the safety risk of flights under procedural control. Motivated by this clear finding, the authors propose to broaden the traditional Functional Hazard Assessment (FHA) and the traditional Preliminary System Safety Assessment (PSSA). The broader approach is proposed for application to SESAR 2020 high level concept of operation, under the explicit assumption that current minimum separation minima remain unchanged. The broader FHA aims to translate future safety Targets (T) that apply to aircraft flights under the operational environment Properties (P) of SESAR 2020, to a high level Specification (S) of ATM services and their safety objectives. To accomplish this, the broader FHA makes use of a barrier model and of a 2020 predicted Integrated Risk Picture (IRP), the exact details of which are not given in the paper/presentation. The S forms the starting point for the broadened PSSA, which aims to refine the SESAR 2020 high level design using functional modelling, logical modelling and thread analysis for normal and abnormal (external and internal) conditions respectively. The power of broadening the FHA and PSSA is that it allows using established system engineering methods, which for example are widely used within the aviation systems industry. In order for the proposed approach to work well, however, humans and procedures have to be represented well in the system engineering model. Because the system engineering approach tends to spread out cognitive activities of one human over various sub-systems, it is not yet clear how the methodology deals with activities in which human are so good, such as maintaining situation awareness and coordination with other humans in case of unforeseen problems. The authors claim in the paper that the proposed approach has been validated appears to mean that the proposed approach has been applied. References to any corresponding reports are not provided. The paper does not explain how the proposed approach relates to state-of-the-art in safety risk analysis research.

Paper 130, Risk-benefit analysis of advanced air transportation technologies using logic gate models, presented by Terry Bott, Logic Evolved Technologies.

The paper addresses the highly relevant problem that both NEXTGEN and SESAR concept designers have in assessing the many alternatives and selecting the most promising during the development of their advanced ConOps. The innovative approach proposed in this paper is to use Logic Gate Model (LGM) to systematically capture all these ConOps design options in one model. The proposed approach has previously been developed by Los Alamos National Laboratory for application to safety critical applications outside air transport. An LGM is a hierarchical, tree-like structure where a specific set of alternatives is represented using OR and AND type logic gates. Once an LGM has been specified for the ATM application considered, then the combinatorially many ConOps alternatives are systematically evaluated and rank ordered. The paper shows how this novel approach is applied to modelling and evaluating the alternatives of a Flight Deck Merging and Spacing (FDMS) tool that is aimed to support Airborne Precision Spacing (APS). The resulting logical model includes aspects ranging from initial APS conditions, such as type of spacing operations and meteorological conditions, through the various aspects of the merging and spacing process, such as issuing APS clearances and the impact of various non-nominal conditions. The proposed metrics to be evaluated using this modelling approach are incident probability and the aircraft arrival delay. The paper provides initial results for four scenarios:

- a current Metering and Spacing (M&S) scenario at baseline traffic demand,
- an initial FDMS based M&S at 1.5 times traffic demand,
- a full FDMS based M&S at 1.5 times traffic demand, and
- a full FDMS based M&S at 3 times traffic demand.

The results show that for all three FDMS based scenarios both incident probabilities and arrival delays reduce significantly over those for the current M&S scenario. The paper also shows what the reductions in arrival delays mean in terms of capacity improvements. The paper does not address the question of how incident probabilities impact accident risk under the different scenarios considered. The paper does not show how the LGM modelling approach is able to overcome the serious limitations of using fault/event tree based hazard analysis for ATM safety assessment. As a consequences of these limitations, it is quite well possible that unintentionally a potentially unsafe alternative is being selected.

Paper 12, Airspace encounter models for conventional and unconventional aircraft, presented by Matt Edwards, MIT.

The paper explains an innovative approach in developing Bayesian network based encounter models for the evaluation of TCAS and future collision avoidance systems. The motivation for this development stems from two identified needs. The first need is that current TCAS encounter models do not cover aircraft not receiving ATC services. The second need is that the current models do not yet reflect last decade changes such as reduced vertical separation and the rise of regional jet fleets. The paper first introduces an elegant classification of aircraft which do not receive ATC services, ranging from conventional aircraft to unmanned aircraft, gliders and balloons. Because of the large variation in characteristics over these classes, the authors have chosen to develop the novel encounter model in the form of a dynamic Bayesian network model, which can learn its parameter values by applying Bayesian feature extraction to a large set of data. In November 2007 a systematic collection began of real-time radar data from Air Force 84th Radar Evaluation Squadron (RADES). In addition, pilot-uploaded GNSS data has been collected for classes that are not well observable by RADES. This data has been used to develop three basic models: 1) a correlated model for aircraft receiving ATS services; 2) an uncorrelated model for conventional aircraft not receiving ATS services; and 3) an unconventional model for aircraft not observable by RADES. The number of parameters in each of these models equals 16, 6 and 5 respectively. The parameterised Bayesian network models have subsequently been used to simulate encounters, and to compare these simulation results with true encounters observed. The initial results of this comparison are promising. Each of the three Bayesian network models is documented well in a publicly available Lincoln Laboratory report. These models are currently in use for the evaluation of TCAS and unmanned collision avoidance systems. For TCAS evaluation of encounters between conventional aircraft it has not (yet) been investigated how the TCAS evaluation results using the new model compares to those obtained using the old established model. The main achievement is that the new TCAS evaluation models developed also apply to aircraft not receiving ATC services. Although some initial validation has been performed, much remains to be done in order for the newly developed models to reach the desired level of maturity. An issue for further research is that the data used to develop the Bayesian network models do not cover contextual information, such as weather information and controller-pilot communication, which may have significant impact on the evaluation of collision avoidance behaviour.

General Aspects

There were two US and one European paper in this session; the estimated average number of participation was 40-50.

Overall the quality of the papers/presentations are fine. Paper 19 is missing references to related research by others. Paper 130 asks significant effort from a reader in understanding and following the argumentation of the authors throughout the paper. This was solved by the presentations given at the conference. Scientifically, paper 12 is the best of the three. In hindsight, paper 130 is focussing on the application of the methodology rather than methodology and might as well have been scheduled outside the safety methodology development track.

No statistically significant differences in scientific culture can be observed from three papers.

High-level Recommendations

All three papers identify and address research questions that are of relevance for NEXTGEN and SESAR.

The above report can be summarised as follows:

Safety assessment research is drawing its attention to research issues that have not been addressed before, i.e. (1) NextGen/SESAR are in need of a macroscopic approach towards safety assessment; (2) NextGen/SESAR safety assessment needs to find its way in the combinatorially many possible alternatives of NextGen/SESAR ConOps; (3) Established aircraft behaviour models for use within safety analysis need to be adapted to recent and forthcoming NextGen/SESAR changes.

For future seminars, a critical link in safety analysis is to take human factors, organizational aspects and emergent behaviour well into account. There is need to focus on approaches that evaluate the effect of interactions between technical and human agents that are distributed over so many aircraft and ground centres (ATC, AOC and airports). This asks for effective collaboration over distant research disciplines It is suggested that for ATM2011, the call for papers explicitly invite research papers on multi-disciplinary approaches towards safety that address the above mentioned aspects.

The research issues for the US and Europe are:

1. To perform independent critical analysis of documented safety cases that have been produced during the last decade both within Europe and within USA. A prerequisite for making these studies possible is that these documented safety cases have to be made publicly available, both by FAA and by EUROCONTROL.

2. To study approaches on how to evaluate the effect of interactions between human and technical agents that are by the very nature of air transport distributed over so many aircraft and ground centres (AOC, ATC and airports).

3. To study extension of ATC directed approaches to safety analysis to approaches that take an integrated approach towards the safety analysis of the joint contributions of all stakeholders involved (ATC, airlines, airports) to air traffic safety.

4. To study approaches which address the issue of validation of safety analysis results under uncertainty and limited availability of statistical data.

5. To study approaches in performing safety assessment studies when the NextGen and SESAR concepts of operation are defined at a high general level only.