A Review of the Research on Risk and Safety Modelling in Civil Aviation

Fedja Netjasov
Division of Airports and Air Traffic Safety
The Faculty of Transport and Traffic Engineering,
University of Belgrade
Belgrade, Serbia
f.netjasov@sf.bg.ac.yu

Milan Janic
Department of Transport and Infrastructure
OTB Research Institute,
Delft University of Technology
Delft, The Netherlands
janic@otb.tudelft.nl

Abstract— **Risk and safety are always considered the most important operational characteristics of contemporary civil aviation. Usually, they refer to the potential occurrence of air traffic accidents which might result in loss of life, damage to infrastructure and third party property damage. Consequently, they have been regarded as externalities in addition to other adverse effects such as noise, air pollution, land-use, water/soil pollution, waste, and congestion. Due to their inherent very high importance, risk and safety have been issues of continuous research ranging from purely technical/technological aspects to strictly institutional. These issues warrant the setting up of adequate regulations on system technology designs and operations. This paper deals with a review of part of the research on risk and safety modeling in civil aviation. In such a context, the basic (generic) concepts and definitions of risk, safety and their evaluation are described. A review of the research is focused on four categories of methods/models for risk and safety assessment: causal for aircraft and air traffic control/management (ATC/ATM) operations, collision risk, human factor error and third-party risk. The review is carried out with respect to their purpose, problems, recommendations and relation to new technologies.**

Keywords: civil aviation, risk and safety, models/methods, new technologies

I. Introduction

Nowadays, the air transport system is recognized as one of the fastest growing areas within the transport sector as well as in overall regional and world economies. According to many forecasts this growth will continue at an average rate of 5% in passenger and 6% in freight transport demand over the next two decades. It will primarily be driven by overall economic growth, further globalization of the regional and world's economy, and even further decreasing of airfares thanks to among other factors the growth of the low-cost carrier's market share. The system infrastructure – airports and Air Traffic Control/Management (ATC/ATM) although in many cases acting as temporal "bottlenecks" are expected to be able to support such growth safely, efficiently and effectively.

Physically and operationally, the air transport system is a rather complex system with the main components - airlines, airports and air traffic control services - interacting with each other on different hierarchical levels constituting a very complicated, highly distributed network of human operators, procedures and technical/technological systems. In particular, risk of accidents and related safety in such a complex system is crucially influenced by interactions between the various components and elements. This implies that providing a satisfactory level of safety (i.e., low risk of accident) is more than making sure that each of the components and elements functions safely [1]. Due to such inherent complexity and severe consequences of accidents, risk and safety have always been considered as issues of the greatest importance for the contemporary air transport system [2]. Consequently, they have been a matter of continuous research from different aspects and perspectives ranging from the purely technical/technological to the strictly institutional. In general, the former have dealt with design of safe aircraft and other system facilities and equipment. The later have implied setting up adequate regulations for system design and operations.

The objective of this paper is to present a review of part of the research dealing with risk and safety in the contemporary civil aviation system.

II. Concepts and Definitions of Risk and Safety

For a long time, risk and safety have been differently and ambiguously interpreted depending on the system and purpose [3]. For technical systems, risk is related to the chance of failure of components or of the entire system causing exposure to hazard and related consequences. In economic business systems, risk is a chance of being exposed to the hazard of losing business opportunities and/or money due to making decisions under uncertain circumstances. In social systems, risk is the chance of being exposed to the hazard of injuries and/or losing of life. Consequently, risk could be considered as combination of the probability (or frequency of occurrence) and the magnitude of consequences (or severity) of a hazardous event [4].

In the air transport system, risk and safety have always been related to air traffic accidents which resulted in the significant loss of life and property (aircraft and the property on the ground). Assuming that making an air trip is an individual choice and that the system deploys some resources to satisfy such choice, four types of risks can be identified in the air transport system [2]: i) real risk to an individual (determined on the basis of future circumstances after their full development, frequently incorporated in decisions on introduction of new aerospace technologies in any system component); ii) statistical risk of occurrence of an accident (important for companies providing insurance, determined by the available statistical data on the incidents and accidents); iii) predicted risk (important for air transport authorities while introducing changes in technologies and air traffic patterns, determined from methodologies using some relevant historical research); and iv) perceived risk (important for users of the air transport system and determined by the individual's intuition, feeling and perception).

In addition, air traffic accidents may have some features distinguishing them from accidents in other transport modes as follows [2]: i) they may occur at any point in time and space mainly because flights may take place over large areas; ii) the primal target groups exposed to the risk exposure are passengers and crew; in addition, individuals on the ground may be exposed but generally have a lower probability of losing life or property; iii) they are relatively rare events but usually with severe consequences; iv) conditionally, each of them can be classified as an inherently risky although highly unlikely (but still possible) event; and v) risk of an accident is inherently present during the flight.

Risk implies exposure of an individual to the hazard of an air traffic accidental event (collision between aircraft, and/or collision between the aircraft and terrain). This could result in losing life or getting severe injuries both onboard the aircraft and/or on the ground, damaging and/or destroying property (the aircraft and eventually buildings on the ground), and contamination of the environment (water and soil) by burning and/or leaking fuel and oil, and hazardous cargo.

In the above-mentioned context, assessing the risk of occurrence of an air traffic accident with the associated consequences can be used as a measure of the system safety for people, systems and environment.

III. Overview of the Methods/Models for Assessment of the Risk and Safety

Many developments in aviation are initiated as a direct result from aircraft accidents. One of them is development of risk and safety methods/models at beginning of 1960's. As a reaction on accidents, first causal methods/models are developed with aim to find out their main causes in order to prevent further accidents. In the same time, collision risk methods/models appeared with proactive role in redesigning the air traffic system in order to safely accommodate increasing traffic demand. Since 1970's, aviation community become more concerned in a human roles in accidents, resulting in development of Human factor errors methods/models. Latter on, during 1990's, airports appear to be a bottleneck of an air traffic system, so the general public become aware of severity of accidents in airports vicinity and their influence on surrounding inhabitants and environment. Increased awareness was resulting in development of Third-party risk methods/models. Causal methods/models for risk and safety assessment of aircraft and ATC/ATM operations, in particular, deals with failures of particular technical systems and components resulting in the aircraft crash or collision. The failures can be due to many interrelated causes and happen either in the aircraft or at ATC/ATM. Collision risk methods/models are dealing with assessment of the risk of aircraft collision while airborne and/or on the ground due to deterioration of ATC/ATM separation rules. Human factor error methods/models deals with risk and safety assessment of air traffic incidents and accidents due to human error. Third-party risk methods/models consider the risk assessment for people on the ground, who might be affected by the aircraft crash.

The main criterion for selection of particular methods/models has been the authors' judgment about their both theoretical importance and practical contribution (although authors were well aware of existence of many other models and similar previous studies). Also, authors' are focusing on proactive modeling approach, i.e. on methods/models which are attempting to anticipate problems before accidents occur, presenting their purpose and related problems.

A. Causal methods/models for the risk and safety assessment of aircraft and ATC/ATM operations

Causal methods/models of assessment of risk and safety of aircraft and ATM/ATC operations establish the theoretical framework of causes that might lead to aircraft accidents. These methods/models can be qualitative or quantitative. The former provide a diagrammatic or hierarchical description of the factors that might cause accidents. They are useful for improving understanding of causes of accidents and proposing preventive interventions. The later estimate the probability of occurrence of each cause and hence estimate the risk of accident. They might be restricted to pure statistical analysis based on the available data or combine these data with expert judgment on the accident causes. In addition, they can estimate the relative benefits of different interventions aiming at preventing accidents in the future [5], [6]. Some of the methods/models are as follows:

- Fault Tree Analysis (FTA) is method developed by Bell Telephone Laboratories, US in 1961 [3] and has been used for analyzing events or combinations of events that might lead to a hazard or an event with serious consequences. Usually, the analysis has been carried out using a fault tree with several paths representing different combinations of instant-direct and intermediate causes described with logical operators ("and" and "or"). At the top of the tree there is a hazard event or a serious consequence. Then, for a given tree the minimum cut set has been determined, i.e., the minimal set of failures of which if all happen causes the top event to happen too. One fault tree might have several minimal cut sets, and if only one happens, the top event also happens. The probability of occurrence of given minimum cut sets is equivalent to the product of probabilities of occurrence of each event within the set. Consequently, the probability of the occurrence of the top event is equal to the sum of probabilities of particular minimum cut sets. The method has been frequently applied (as the best recommended) to assessment of risk and safety as well as reliability of the aircraft and ATC/ATM computer (hardware) components;

- Common Cause Analysis (CCA) is the method, which can be used for identifying sequences of events leading to an aircraft accident. In particular, the method appears useful to extract common causes of several aircraft accidents. For such a purpose, it "divides" the aircraft into "zones" implying that the system and components in each zone are ultimately independent. Consequently, it is possible to identify the common causes of failures of particular components of such independent systems. The NASA has used this method for a long time (since 1987) although the method itself is probably older then 1975. In addition, it has been recommended for assessment of the risk of failures of aircraft systems and equipment;

- Event Tree Analyses (ETA) method is developed in 1980 and is used for modeling sequences of events arising from a single hazard and consequently describe seriousness of the outcomes from these events. The hierarchy of presenting a hazard, the sequence of events causing failures of the system components, and their state in terms of functioning and failure, represent the core of the method. Consequently, a tree with branches of events and functioning and failing components displays probabilities of failures along particular branches. These in combination with the probability of the hazardous event enable quantification of the probability of the system or component failure. This method has shown it is applicable in combination with FTA (Fault Tree Analysis) for almost all technical systems including the aircraft and ATC/ATM components. Bow-Tie Analysis presents a combination of ETA and FTA. Origins are from 1970's and 1980s, but since 1999 have been popularized as a structured approach for risk analysis;

- TOPAZ accident risk assessment methodology is a complex method that uses scenario analysis and a Monte Carlo simulation technique for assessment of the risk and safety of ATC/ATM operations modeled as a Petri Nets. It has been developed by NLR (The Netherlands National Aerospace Laboratory) during the 1990's. The method addresses all types of system safety issues such as technical/technological, organizational, environmental, and human-related and other hazards and their combinations. Risk and safety assessment is performed through few steps enabling identification of safety bottlenecks. The method has been widely applied to risk assessment of ATC/ATM operations [5];

- Bayesian Belief Networks (BBN) is a method based on probability theory, which has been developed to improve understanding of the impacts of different causes on the risk of aircraft accidents (originating from mid of 1980's, applied in aviation filed at beginning of 2000's). The method is supposed to capture the wide range of failures of aircraft systems both qualitatively and quantitatively and thus provide rather objective and unambiguous information on the state of system safety relevant for the managerial decisions [7], [8], [9]. The method has been applied as a decision-support tool to calculate effects of specific changes to the aviation system on the overall risk as well as support in developing a proactive policy by providing an insight into the effects of anticipated system changes on risk.

1) *Purpose*

Increasingly interesting causal methods/models have mainly been used for: i) better understanding of effects of different influencing factors on level of risk; ii) evaluation of overall risk, risk communication, and cost-benefit analysis of new technologies; iii) training of aviation staff and identification of system components that could be improved; and iv) identifying "critical" causes of the aircraft accident as well as measures for reducing risk. For example, in order to decide which measures for risk reduction should be adopted; regulators and safety managers need an understanding of causes of accidents and an ability to evaluate benefits of various interventions. These methods/models can support these decisions [6]. All mentioned methods/models are quantitative except the CCA. Related to risk types given in Section II, it could be mentioned that FTA, ETA and CCA are generally used to determine "statistical risk" of occurrence of an accident or failures, while Bow-Ties, TOPAZ and BBN - "predicted risk" of system changes such as introduction of new technologies, procedures, operations, etc.

2) *Problems*

The causal methods/models are data driven and highly dependant in their quality on the one hand and the expert judgment about combinations of particular causal factors of the air traffic accidents on the other. Quantification of these methods/models has appeared extremely difficult and time consuming mainly due to the complexity of combinations of causal factors leading to possible accidents. In addition, calculation of probabilities and conditional probabilities in situations where dependencies between particular causal factors have not completely been known further complicates quantification of the methods/models. As well, one important problem has been the cumulative nature of these methods/models, which could make assessment of particular probabilities difficult due to the large number of causal factors and their combinations [8]. Consequently, in some cases it has been rather difficult to express results from these methods/models in a transparent and comprehensible way [6].

B. *Collision risk methods/models*

One of the principal matters of concern in the daily operation of civil aviation is preventing conflicts between aircraft either while airborne or on the ground, which might escalate to collision. Although aircraft collisions have actually been very rare events contributing to a very small proportion of the total fatalities, they have always caused relatively strong impact mainly due to relatively large number of fatalities per single event and complete destruction of the aircraft involved. In general, separating aircraft using space and time separation standards (minima) has prevented conflicts and collisions. However, due to reduction of this separation in order to increase airspace capacity and thus cope with growing air transport demand, assessment of the risk of conflicts and collisions under such conditions has been investigated using several important methods/models as follows [10], [11]:

- The Reich-Marks model is developed in early 1960's by Royal Aircraft Establishment, UK [12]. It is based on the assumption that there are random deviations of both aircraft positions and speeds from the expected.

The model was developed to estimate the collision risk for flights over the North Atlantic and consequently to specify appropriate separation rules for the flight trajectories [11]. The model computed the probability of aircraft proximity and the conditional probability of collision given the proximity. Aircraft were represented as three-dimensional boxes, i.e., rectangular parallelepipeds, of given length, width and height reflecting the ATC/ATM minimum separation rules. The collision might occur whenever any two boxes intersected. As well, when one aircraft was represented as the dimensionless point, conflict occurred when the point entered the box. In such a context the collision risk with the vertical, lateral and longitudinal neighbor could be determined independently of each other bearing in mind that the position errors of boxes and points representing the aircraft along their tracks were random variables with zero mean and given standard deviations. Consequently, the prescribed lateral distance between aircraft could be specified with given probability of violation reflecting the acceptable collision risk [10], [13];

- The Machol-Reich model was developed after the ICAO had established the NAT SPG (North Atlantic System Planning Group) in 1966 with the idea of creating the Reich-Marks model as the workable tool as well as increase of airspace capacity. The modified model using actual data for the position error (collected for about 14000 flights) enabled prediction with moderate confidence of each of the vertical, horizontal and longitudinal collision risks. Consequently, the ICAO NAT SPG has adopted the threshold for risk of collision of two aircraft due to the loss of planned separation [10], [14];

- The intersection models belong to the simplest collision risk models. They are based on assumptions that aircraft follow pre-determined crossing trajectories at constant speeds. The probability of a collision at the crossing point is computed using the intensities of traffic flows on each trajectory, aircraft speeds, and the airplane geometry [15], [16], [17];

- The geometric conflict models are similar to the intersection models. In these models (developed in 1990's) the speed of any two aircraft is constant, but their initial three-dimensional positions are random. Based on extrapolating their positions in time, it is possible to geometrically describe the set of initial locations that eventually lead to a conflict. The conflict occurs when two aircraft are closer than the prescribed separation rules. After integrating the probability density of the initial aircraft positions over the conflicting region, the conflict probability can be estimated [18], [19], [20];

- Generalized Reich model was developed by removing restrictive assumptions of Reich model based on the fact that Reich model does not adequately cover some real air traffic situations. The model was based on the hybrid-state Markov processes, aiming to cover a larger variety of air traffic situations. The resulting collision risk equals the probability of collision between two aircraft. Such a generalized collision model was developed during 1990's and has been used as part of the TOPAZ methodology (mentioned in Section II, A) [1], [11], [21], [22], [23], [24].

1) *Purpose*

The main driving force for developing collision risk methods/models during the 1960's was the need for increasing airspace capacity over Atlantic through decreasing aircraft separation minima. The methods/models were expected to show if reduction of separation and spacing between the flight tracks would be sufficiently safe, i.e., determine the appropriate spacing between tracks guaranteeing a given level of safety. The collision risk methods/models have gradually been developed from Marks, Reich and Machol to the latest versions used in TOPAZ methodology. The main purpose has always remained to support decision-making processes during system planning and development through evaluation of the risk and safety of proposed changes (either in the existing or new system). Methods/models from this category, according to risk classification from Section II, generally provide an assessment of "predicted risk" and implicitly "real risk to an individual" due to the fact that collisions are usually leading to fatalities.

2) *Problems*

Despite the collision risk methods/models having been successfully used for a long time (more than 40 years), some problems, which could make their further use even more complex have continued to exist as follows:

a) Complexity and cost of collecting the enormous amount of data on aircraft three-dimensional positions necessary to define the related statistical distributions [14], [25];

b) Inherent complexity of the generic collision risk method/model as the result of the modeling approach (closer to the reality). New versions of these methods/models such as those used in TOPAZ are even more complex because they embrace more details when calculating risks, such as possible failure of some technical systems (engine, avionics, etc.) or flight crew awareness or fatigue; and cover complex relationships between elements of the system (flight crew, aircraft, ATC/ATM system, other aircraft, etc.) [26];

c) Inherent danger of misunderstanding or no understanding from the average user's point of view mainly due to complexity. This requires of the specialists a long and costly familiarization time [27];

d) The lack of risk-predicting capability with high degree of confidence and bias and uncertainty of the obtained results. Additional time and expertise for calculation of the credible risk intervals are needed [28];

e) Relying on expert judgment in cases where historical data are not available, or when their collection is very expensive: the experts are used for setting up the value of parameters, value and dispersion of the random variables, and the dependence between variables. In such contexts, there is always the problem of engaging credible experts, especially in cases involving new system concepts;

f) Complexity in validation particularly of new system concepts. In cases of non-existent systems, the ICAO has recommended comparison with the reference system and evaluating risk against its given threshold value.

C. *Human factor error methods/models*

Investigation of causes of particular air traffic accidents has identified "human error" as one of the most frequent causes [29]. Human error is considered as an incorrect execution of a particular task, which as an event, triggers a series of consecutive errors in execution of other tasks, finally resulting in serious consequences – an aircraft accident – crash.

Therefore, monitoring and modeling of human errors in the aircraft and ATC/ATM operations aiming at discovering and preventing them have always been high on the research agenda of both academics and practitioners dealing with civil aviation. Consequently, many methods for detection and prevention of "human errors" have been developed; some of them are [5]:

- HAZOP (Hazard and Operability) method (developed in early 1970's) aims at discovering potential hazards, operability problems, and possible deviations of the actual from the system intended operational conditions (states) including estimating the probability of escalation into a serious event. The method was intended to deal with human errors in complex technical systems such as chemical and nuclear plants having human operator in their control loop. Later on, the UK NATS (National Air Traffic Service) applied the method to different aspects of planning and assessing hazard in operation of the national ATC/ATM, particularly for identification of hazards due to human failures that might develop into risk of air traffic accidents (HAZOP can provide input to FTA and ETA, mentioned in Section III, A);
- HEART (Human Error Assessment and Reduction Techniques) was developed in 1985 for identifying and quantifying errors in an operator's task. It simultaneously considers particular ergonomic and other environmental factors, which might compromise the required operator's performance. The impact of a particular (each) factor on the operator's error while performing particular tasks can be quantified. Then the probability of error in executing a given task (or a series of tasks) can be estimated. The method has been applied by the UK NATS in combination with other methods for identification of the human errors in ATC/ATM;
- TRACER-Lite (Technique for the Retrospective Analysis of Cognitive Errors) was developed in 1999 by NATS, for predicting human errors and deriving error prevention measures in ATC/ATM. The method is retrospective, i.e., it is used for classifying types of errors contributing to the air traffic incidents, which have already happened. The method has a modular structure with three modules: the context; the error discovery; and the error recovery. Hierarchical Task Analysis enabling identification of the "set of critical" tasks, critically influencing safety, usually classifies the human errors;
- HERA (Human Error in ATM) is the retrospective method providing insight into ATC/ATM controllers' cognitive processes while dealing with air traffic incidents (developed at EUROCONTROL at beginning of 2000's). The method consists of two parts: a retrospective part for the incident analysis; and a prospective part using the information collected on the assessment of probability of human error in cases of compromised safety. Consequently, the method enables better understanding of the constraints and conditions under which ATC/ATM controllers operate. These conditions are important for understanding ATC/ATM controllers' incompliance with existing procedures and skill-related errors;
- HFACS (Human Factor Analysis and Classification System) is method developed at beginning of 2000's in USA, as a system to categorize latent and immediate causal factors that have been identified in aviation accidents. It is based on analysis of hundreds of aviation accident reports and main purpose is to provide a framework for accident investigations and to serve as a tool for accident trends assessment. HFACS uses four levels of failure: i) unsafe acts; ii) preconditions for unsafe acts; iii) unsafe supervision and iv) organizational or cultural influences. The method is very promising for analysis of air traffic controller errors and failures in ATC/ATM and is effective for understanding the antecedents of operational errors for air traffic safety analysis.

1) Purpose

The methods/models dealing with human factor errors in civil aviation have been developed to identify and eventually prevent errors (particularly of aircraft crew and ATC/ATM controllers), which could cause aircraft incidents and accidents. In addition, these models have investigated factors from the operational environment, which could cause errors, as well as calculating the probability of making errors in performing given activities. Consequently, it will be expected that they will be applied to both operational and design stages of developing aviation systems. Specific types of methods/models have given insight into the cognitive processes of the ATC/ATM controllers operating in the incidental situations, analyzed these situations, and calculated probability of making errors. In addition, these methods/models have possessed some ability for predicting errors and specifying the error reduction measures. According to risk types in Section II, those methods/models are mostly intended to determine "statistical" and "predicted" risk for given probability of error.

2) Problems

Human factor errors methods/models posses some shortcomings, which might compromise their more efficient and effective application to the ATC/ATM as follows:

a) Most activities in ATC/ATM and in particular, factors influencing human operator performance and possible errors have usually been considered in isolation, i.e., independently on each other; in many cases the quantitative information has exclusively relied on expert judgment;

b) Only specialists in "human factors" have been able to use these methods/models efficiently and effectively; i.e., it has been time consuming and almost impossible to apply these methods/models in an operational environment without specialists;

c) The methods/models have been constrained exclusively to the operational processes and activities in the ATC/ATM.

D. Third-party risk methods/models

Third-party risk implies risk if an individual on the ground to be killed by crashing aircraft. In such a case, the accident is called a "groundling accident" or "groundling crash" and the fatality a "groundling fatality". Since most air traffic accidents (about 70% according to [29]) happen around airports, the concept and assessment of third-party risk has been mainly focused on areas around airports. In a given context, the basic assumption has been that risk always exists, cannot be reduced to zero and should be predictable, transparent, and controllable, as well as quantifiable and measurable. Modeling of third-party risk has shown promise in resolving these problems including setting up thresholds for acceptable risk around airports [30], [31], [32]. Three cases of assessment of the third-party risk are illustrated as follows:

- USA case - generally implies assessment of the risk an individual is exposed to when at some distance from a given airport during the period of a year. For such a purpose, relevant statistics on fatalities from official sources have been collected and the prospective number of ground fatalities estimated. The estimation has been carried out by multiplying two independent variables – the number of crashes around airports and the number of fatalities per individual crash. The model has shown that the probability of being killed by crashing aircraft has decreased more than proportionally with increasing distance from the airport and increased with increase in the volume of the airport traffic at distances up to about two miles. The model has not considered spatial variability of the risk due to changing residence locations and the aircraft flight paths around the airports, which might be considered as its main disadvantage [32];
- The Netherlands case - this method was developed by the NLR, inspired by the crash of cargo aircraft in the Bijlmer district of Amsterdam in 1992. Method contain the following elements [31], [33]: i) the accident probability model, which calculates the probability of an aircraft accident in the vicinity of an airport depending on the probability of an accident per aircraft movement and the annual volume of airport traffic; ii) the accident location probability model, which calculates the probability of a given location becoming an accident scene depending on its position relative to airport runways and the incoming and outgoing aircraft trajectories; and iii) the accident effect model, which combines output from both previous models to calculate the probability of an accident at each location within the area surrounding a given airport. Individual and societal risks have been used as measures of third-party risk. After calculating the individual risks for the entire area around given airport, the risk contours can be plotted on the horizontal plane [31]. Societal risk applies to the entire area around a given airport and actually exists only when people are actually present in the area [31], [33];
- UK case - has become important after Public Safety Zones (PSZs) were introduced in 1958. The PSZ was defined as an area adjacent to the end of a runway in which development of land had to be restricted if it would likely significantly increase the number of "residing, working or congregating people there" [31]. In the 1997 the method for third-party risk assessments around airports and the proposal of the appropriate risk assessment criteria was developed in a NATS. The method was based on distinguishing aircraft regarding their manufacturer, country of origin, type (large, small, jets, turbo-props), and category (passenger, cargo), modeling of the aircraft crash location and the crash consequences both based on a limited sample, and simplified approach, to draw the risk contours around a given airport. In addition, cost-benefit analysis was applied to set up criteria for acceptable (tolerable) risk [31].

1) Purpose

The third-party methods/models have been mainly used for decision-making and policy purposes related to airport development and operations as follows: a) forecasting risk for an individual to be killed by a crashing airplane in the vicinity of given airports. The information has been used for comparing the risk around airports and that around chemical or nuclear plants; b) zoning around airports using individual risk contours and societal risk values, i.e. determining areas, which should be considered dangerous for building houses or other vulnerable infrastructure; c) indicating changes in risk contours arising from airport development or changes in using existing infrastructure (changes of runways in use, arrival or departure trajectories, etc). Relative to the classification of risk given in Section II, it could be mentioned that third-party methods/models are used for assessment of "predicted" and "real risk to an individual".

2) Problems

The third-party methods/models have been permanently improved and updated. The main problems identified during that process have been as follows [33]: a) lack of generality, i.e., the specific method/model has been developed for the specific airport; b) proactive assessment of the risk could not be carried out due to the risk control measures being already in place; c) scarcity of data on real accidents and risk exposure around the airports in the official statistical sources; d) difficulties in setting up threshold values for individual and societal risk; if too high it might compromise the airport operations and development; if too low, it might put individuals at an unacceptable jeopardy.

IV. Recommendations and Relation to New Technologies

The methods/models for assessment of risk and safety in civil aviation described in the previous section have been reviewed aiming at identifying, from the engineering perspective, eventual shortcomings which might significantly compromise their usability, as well as points for their eventual improvements. For such a purpose, based on the available literature, a review framework containing the recommendations (requirements) and relation to new technologies for each method/model type, has been designed (the term "new technology" is referring to the new technologies, systems, procedures, concepts, operations, etc). Finally, some commonalities between them are presented in form of prospective research agenda.

A. Recommendations

1) Causal methods/models for risk and safety assessment of aircraft and ATC/ATM

It is desirable that causal methods/models posses some predictive capabilities, i.e., not only predicting the risk level and causal breakdown but also indicating their variations within changing input assumptions. Such capability would enable these methods/models to reflect better the already adopted safety measures as well as eventual benefits of further improvements. In addition, they should be able to assess the safety bottleneck in the existing system, i.e., its most vulnerable component. Due to the very complex and demanding modeling process; modular development could eventually be a compromise solution for these methods/models. This could imply starting with official statistics on air traffic accidents, and later on, allowing integration of particular modules into more complex networks. In addition, these methods/models could be developed specifically for airports, ATC/ATM, and airlines as components of the civil aviation system.

2) *Collision risk methods/models*

Regarding the purpose and existing structure, certain compromise in terms of obtaining some kind of balance between complexity and usability (due to enormous amount of input data and high level of the necessary expertise) might be recommended. Additional recommendations would be development of the method/models for specific purposes such as collision risk assessment in the en-route and terminal airspace or at the airport as well as devotion to their use at local level particularly while assessing the effects of new equipment on the collision risk. Finally, these methods/models should have better predictive capability because their usage will be more and more related to collision risk assessment when new systems, procedures, concepts and operations are introduced.

3) *Human factor error methods/models*

Further development of these methods/models should focus on dealing with human error at all ultimately interrelated levels of ATC/ATM such as operations, maintenance, organization, and management. They should be able to consider mutual dependency between errors from particular interrelated activities as well as dependability of factors causing particular errors. In addition, the methods/models will have to focus more on dealing with existing and new technologies and systems in their both operational and design stages.

4) *Third-party risk methods/models*

Certainly, development of more general methods/models for assessment of third-party risk could be recommended. They should have flexible structure in order to appropriately handle differences and specificities of traffic, layout and surrounding environment at particular airports. In addition, these methods/models should be able to handle proactive managerial, organizational, technical and/or other changes, and to represent their effects on the overall risk and safety around given airport. As well, they should have some predictive capabilities. Last but not least, there is an increasing need for common frameworks for managing third party risk by developing methodologies and tolerability criteria for comparable risk assessment in order to ensure fair competition between airports (in Europe) [34].

B. *Relation to new technologies*

1) *Causal methods/models for risk and safety assessment of aircraft and ATC/ATM*

The causal methods/models could contribute to the proactive development of policies on implementing changes by providing insight into the effects of changes in existing systems on risk and safety [8]. In particular, under conditions when the system changes due to implementation of new technologies, these methods/models could provide feedback about their contribution to lowering risk and consequently increasing the overall system safety.

2) *Collision risk methods/models*

Used for reduction of aircraft separation for more then 40 years, the collision risk methods/models have proved their viability. However, further reductions in aircraft separation by the use of new technologies will be needed as an option for increasing airspace capacity. Therefore, existing modified and new methods/models will have to be able to assess collision risk under such circumstances [10]. Some models such as TOPAZ are already in place. Use of this method/model is in line with methodology proposed by the ICAO, which points out the necessity for evaluation of risk of new technologies against threshold values and its comparison with the reference system [35]. In cases where there is lack of reference systems or large scale changes in existing systems, expert judgment is recommended. In addition, setting up threshold values for risk while implementing new technologies, which are expected to be of lower risk, is also a matter for further elaboration of existing systems and the development of new collision risk methods/models.

3) *Human factor error methods/models*

Human factor error methods/models with necessary modifications should be applicable to new technologies and systems in ATC/ATM for identifying human errors at all levels of system functioning and they should be able to generate measures for error prevention and/or reduction already at the design stage. For such purposes, they will have to be able to handle careful specification of activities and tasks throughout the system in a way, which will not be highly if not crucially dependent on the highly specialized staff.

4) *Third-party risk methods/models*

Predictive capabilities and flexibility of third-party risk methods/models will be essential to produce new (updated) individual and societal risk estimates based on the expected number of fatalities after introducing new technologies and operational procedures at given airport. On the one hand these are expected to increase airport capacity and on the other they should decrease the accident rate in the vicinity of airports.

C. *Prospective research agenda*

The overview and review of the mentioned methods/models for assessment of risk and safety in civil aviation have uncovered some commonalities between them, which could be, after being summarized, used for generating prospective research agenda. These are as follows:

- Regarding the *purpose* all models have been developed to support decision-making processes during system planning, development and management, through evaluation of the risk and safety of proposed technological, organizational and managerial changes;
- Regarding *problems* that all methods/models have been confronted with: i) Necessity to have a good, statistically significant data bases on air traffic accidents and their causes (the lack of such data has been compensated by the expert judgment inherently containing unreliability and uncertainty); and ii) Complexity in quantification of risk and safety due to dependability of particular air traffic accidents on many interrelated dynamic and stochastic causes;
- Regarding the *recommendations*, all methods/models should have some predictive capabilities, flexibility, and modularity as well as should be generic;
- Regarding *application to new technologies*, all methods/models should be able to investigate their risk and safety under given circumstances. However there might be some limitations in such application due to the inherent limitations of existing models to appropriately handle the risk and safety of new technologies [35].

Mitigating the above-mentioned and other problems in line with recommendations how to improve existing and develop new methods/models for assessment of risk and safety in civil aviation particularly for new still non-existing technologies have been identified as the main research challenge for the prospective research.

V. CONCLUSIONS

The paper has provided a review of some of the methods/models for assessment of risk and safety in civil aviation. The main findings have provided insight into the efforts already carried out in developing these methods/models, their inherent complexity and lack of sufficient flexibility, lack of the available data for calibration and testing, and lack of the sufficient predicting capabilities enabling easier application to the assessment of risk and safety of new technological, procedural and operational concepts. These have aimed at increasing system capacity on the one hand and reducing acceptable risk and safety thresholds on the other. In many cases, the need for developing "specialized" or "dedicated" methods/models for particular parts of the system have been discovered. In addition, difficulties such as the lack of real-life data have been overcome by including expert judgment despite awareness of its uncertainty and biases. The structured need for balance and compromise between methods/models complexity, time and cost of development, and transparency of results have also been pointed out. Prospective research has been considered to further improve existing models in line with recommendations, which have generally implied capability of risk and safety assessment during development and after implementation of new technologies, generality on the one hand and dedication on the other, predictive capabilities, flexibility and easier understood and handled modular system structures.

REFERENCES

[1] H. Blom, G. Bakker, P. Blanker, J. Daams, M. Everdij, M. Klompstra, "Accident risk assessment for advanced ATM", Proceedings of 2nd USA/Europe Air Traffic Management R&D Seminar, USA, 1998.

[2] M. Janic, "An Assessment of Risk and Safety in Civil Aviation", Journal of Air Transport Management, Vol. 6, No. 2, pp 43-50, 2000.

[3] H. Kumamoto, E. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, IEEE Press, USA, 1996.

[4] N. Bahr, System Safety Engineering and Risk Assessment: A Practical Approach, Taylor & Francis, United Kingdom, 1997.

[5] ATM Safety Techniques and Toolbox, Safety Action Plan – 15, Federal Aviation Administration and EUROCONTROL, USA, 2005.

[6] J. Spouge, A Demonstration Causal Model for Controlled Flight into Terrain, Det Norske Veritas, United Kingdom, 2004.

[7] J. Luxhoj, D. Coit, "Modeling Low Probability/High Consequence Events: An Aviation Safety Risk Model", Proceedings of the Reliability & Maintainability Symposium (RAMS), USA, pp. 215 – 220, 2006.

[8] A. Roelen, R. Wever, A. Hale, L. Goossens, R. Cooke, R. Lapuhaa, M. Simons, P. Valk, "Causal Modelling for Integrated Safety at Airports", Proceedings of ESREL 2003 - European Safety and Reliability Conference, The Netherlands, pp. 1321 – 1327, 2003.

[9] A. Roelen, R. Wever, R. Cooke, R. Lapuhaa, A. Hale, L. Goossens, "Aviation Causal Model Using Bayesian Belief Nets to Quantify Management Influence", Proceedings of ESREL 2003 - European Safety and Reliability Conference, The Netherlands, pp. 1315 – 1320, 2003.

[10] R. Machol, "Thirty Years of Modelling Midair Collisions", Interfaces, Vol. 25, No.5, pp. 151-172, 1995.

[11] J. Shortle, Y .Xie, C. Chen, G. Donohue, "Simulating Collision Probabilities of Landing Airplanes at Non-towered Airports", Simulation, Vol. 80, Issue 1, pp. 21-31, 2004.

[12] P. Reich, "Analysis of long range air traffic systems: Separation standards – I, II and III", Journal of the Institute of Navigation, No. 19, pp. 88-96, 169-176, 31-338, 1966.

[13] A Concept Paper for Separation Safety Modelling, Federal Aviation Administration and EUROCONTROL, USA, 1998.

[14] R. Machol, "An Aircraft Collision Model", Management Science, Vol. 21, No. 10, pp. 1089-1101, 1975.

[15] W. Siddiqee, "A mathematical model for predicting the number of potential conflict situations at intersecting air routes", Transportation Science, No. 7, pp. 158-167, 1973.

[16] K. Geisinger, "Airspace Conflict Equations", Transportation Science, No. 19, pp. 139-153, 1985.

[17] A. Barnett, "Free-flight and en route air safety: A first-order analysis", Operations research, No. 48, pp. 833-845, 2000.

[18] R. Paielli, H. Erzberger, "Conflict probability estimation for free flight", Journal of Guidance, Control and Dynamics, No. 20, pp. 588-596, 1997.

[19] R. Paielli, H. Erzberger, "Conflict probability estimation generalized to non-level flight", Air Traffic Control Quarterly, No. 7, pp. 195-222, 1999.

[20] R. Irvine, "A geometrical approach to conflict probability estimation", Air Traffic Control Quarterly, No. 10, pp. 85-113, 2002.

[21] G. Bakker, H. Blom, "Air Traffic Collision Risk Modelling", Proceedings of 32nd IEEE Conference on Decision and Control, USA, pp. 1464-1469, 1993.

[22] H. Blom, G. Bakker, "Conflict probability and In-crossing probability in Air Traffic Management", Proceedings of 41st IEEE Conference on Decision and Control, USA, (preprint), 2002.

[23] G. Bakker, H. Kramer, H. Blom, "Geometric and Probabilistic Approaches towards Conflict Prediction", Proceedings of 3rd USA/Europe Air Traffic Management R&D Seminar, Italy, 2000.

[24] H. Blom, G. Bakker, M. Everdij, M. van der Park, "Collision risk Modelling of Air Traffic", Proceedings of European Control Conference, United Kingdom, (preprint), 2003.

[25] L. Stachtchenko, "An Investigation of Aircraft Collision Risks over the North Atlantic", CORS Journal, Vol. 3, No. 2, pp. 55-71, 1965.

[26] J. Rouvroye, E. van den Bliek, "Comparing safety analysis techniques", Reliability Engineering and System Safety, No. 75, pp. 289-294, 2002.

[27] Guide to Methods & Tools for Safety Analysis in Air Traffic Management, Global Aviation Information Network, USA, 2003.

[28] M. Everdij, H. Blom, S. Stroeve, "Structured Assessment Of Bias And Uncertainty in Monte Carlo Simulated Accident Risk", International Conference On Probabilistic Safety Assessment And Management (PSAM 8), USA, (preprint), 2006.

[29] Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations 1959 – 2005, Boeing Commercial Airplanes, USA, 2006.

[30] B. Ale, "Risk Assessment Practices in the Netherlands", Safety Science, Vol. 40, pp. 105 –126, 2002.

[31] B. Ale, E. Smith, R. Pitblado, Safety around airport – developments in 1990s and future directions, Det Norske Veritas, United Kingdom, 2000.

[32] R. Rabouw, K. Thompson, R. Cooke, "The Aviation Risk to Groundlings with Spatial Variability", Proceedings of ESREL 2001 - European Safety and Reliability Conference, Italy, pp. 1219-1226, 2001.

[33] A. Hale, "Risk Contours and Risk Management Criteria for Safety at Major Airports, with Particular Reference to the Case of Schiphol", Safety Science, Vol. 40, pp. 299–323, 2002.

[34] Safety in and Around Airports, European Transport Safety Council, European Commission, Belgium, 1999.

[35] F. Vismari, B. Camargo "Evaluation of the impact of new technologies on aeronautical safety: an approach through modelling, simulation and comparison with legacy systems", Journal of the Brazilian Air Transportation Research Society, No.1, pp 19-30, 2005.