Chapter Three: The Overview of Mathematical Models of Risk in Aviation

Rabiah binti Tukiman

October 17, 2018

1 Introduction

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.

2 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. Some of the methods/models are as follows:

1. Fault Tree Analysis (FTA) is method developed by Bell Telephone Laboratories, US in 1961 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;

2. 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;

3. 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;

4. 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. 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.

Increasingly interesting causal methods/models have mainly been used for:

1. better understanding of effects of different influencing factors on level of risk;

2. evaluation of overall risk, risk communication, and cost-benefit analysis of new technologies;

3. training of aviation staff and identification of system components that could be improved; and

4. 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. 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.

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. Consequently, in some cases it has been rather difficult to express results from these methods/models in a transparent and comprehensible way.

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.

3 Collision Risk Methods/Model

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:

1. The Reich-Marks model is developed in early 1960's by Royal Aircraft Establishment, UK. 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. 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;

2. 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;

3. 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;

4. 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).

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.

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:

1. Complexity and cost of collecting the enormous amount of data on aircraft three-dimensional positions necessary to define the related statistical distributions;

2. 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.);

3. 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;

4. 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;

5. 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;

6. 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.

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.

4 Human Factor Error Methods/Model

Investigation of causes of particular air traffic accidents has identified "human error" as one of the most frequent causes. 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. 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:

1. 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);

2. 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;

3. 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;

4. 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;

5. 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.

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.

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

1. 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;

2. 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;

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

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.

5 Third-Party Risk Method/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%) 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. Three cases of assessment of the third-party risk are illustrated as follows:

1. ***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;

2. ***Netherland 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:

   (a) 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;

   (b) 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

   (c) 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. Societal risk applies to the entire area around a given airport and actually exists only when people are actually present in the area;

3. ***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". 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.

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).

The third-party methods/models have been permanently improved and updated. The main problems identified during that process have been as follows: *(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.

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.