Journal of Air Transport Management 14 (2008) 213–220

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

A review of research on risk and safety modelling in civil aviation

Fedja Netjasov [a], Milan Janic [b,*]

[a] Faculty of Transport and Traffic Engineering, University of Belgrade, Division of Airports and Air Traffic Safety, Vojvode Stepe 305, Belgrade, Republic of Serbia
[b] OTB Research Institute, Delft University of Technology, Jaffalaan 9, 2628 BX Delft, The Netherlands

ARTICLE INFO

Keywords:
Civil aviation
Risk and safety
New technologies

ABSTRACT

Safety is considered as some of the most important operational characteristics of contemporary civil aviation. An extensive regulatory structure has been established to supplement the private airline, airport and air navigation systems, incentives to limit the risks of flying. This paper reviews the research on risk and safety modelling in civil aviation. In such a context, the basic concepts and definitions of risk, safety and their evaluation are described. The review focuses on four categories of models for safety assessment: causal for aircraft and air traffic control/management operations, collision risk, human factor error and third-party risk.

1. Introduction

Air transport is one of the fastest growing modes of transport, and is forecast to grow at an annual rate of between 5% and 6% over the next two decades. Growth rates in international markets are expected to be about twice those in domestic markets, and faster in developing countries. The system's infrastructure—airports and air traffic control/management (ATC/ATM)—has the objective of supporting this growth safely, efficiently and effectively. Air transport, however, is a complex system involving a complicated, interlinking distributed network of human operators, procedures and technical/technological systems. These factors make the provision of a socially acceptable level of safety difficult (Blom et al., 1998; European Commission, 1999). Due to the potentially severe consequences of accidents, safety has always been considered an issue of greatest importance in the sector (Janic, 2000). This paper focuses on the methods and models used for the assessment of risk for individual aircraft and for ATC/ATM operations.

For a long time, the interpretation of safety depended on the system involved and the purpose of the analysis (Kumamoto and Henley, 1996). For technical systems, risk is related to the probability of failure of components or of an entire system causing exposure to hazard and related consequences. In commercial systems, risk is the chance of being exposed to the hazard of losing business opportunities by making inappropriate decisions when there is a known probability of failure. In terms of safety, risk can be considered as a combination of the probability or frequency of occurrence and the magnitude of consequences or severity of a hazardous event (Bahr, 1997).[1]

In air transport, risk has traditionally been related to air traffic accidents resulting in the significant loss of life and property. Assuming that flying is an individual's choice and that the system deploys some resources to satisfy such choice, four types of risks can be identified: risk to an individual, statistical risk of the occurrence of an accident, predicted risk and perceived risk. While these types of risk, albeit with particular nuances, are common across transport modes, air traffic accidents have some distinguishing features. For example, they can occur at any point in time and space because flights are not limited by "roadways" and they are relatively rare events but often have severe consequences. Additionally while the main target groups exposed to the risk are air passengers and crew, "third-party" individuals on the ground may be exposed, but with generally lower probability of losing life or property.

2. Models for assessment of the risk and safety

Fig. 1 offers a generic scheme for analysing air traffic accidents and their consequences (Federal Aviation Administration and European Organization for Safety of Air Navigation, 2005). The first group of models deals with assessment of risk and safety of aircraft operations supported by ATC/ATM and, in particular, with failures of particular technical systems and components that result in an aircraft crash. The failures can be due to many interrelated causes either in the aircraft or at ATC/

* Corresponding author.
E-mail address: janic@otb.tudelft.nl (M. Janic).

[1] This contrasts, as Frank Knight pointed out over 80 years ago, to uncertainty where there is no calculable probability.

0969-6997/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jairtraman.2008.04.008

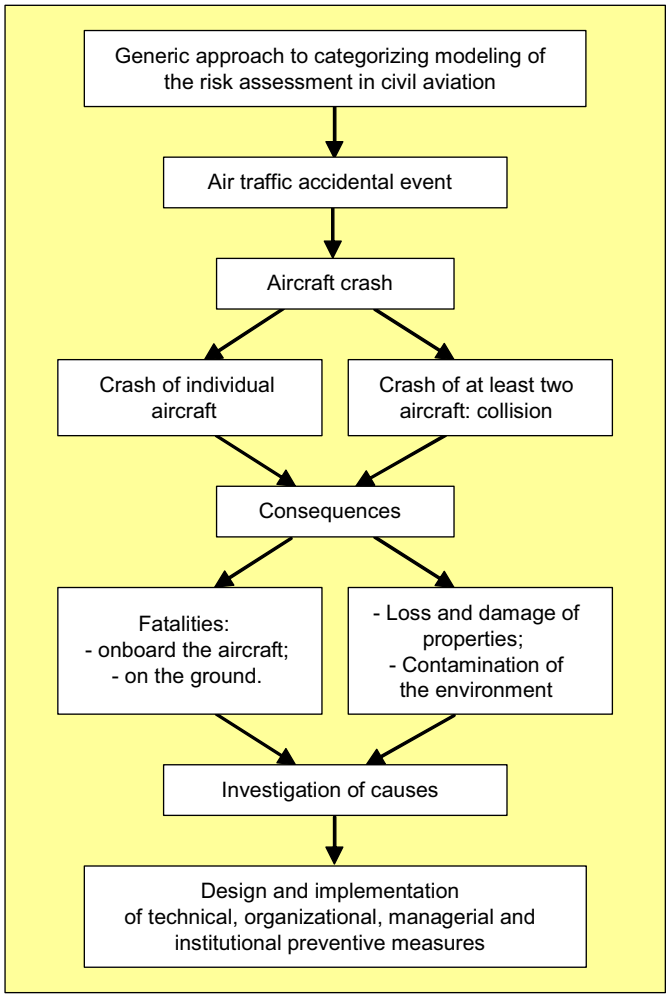

Fig. 1. A generic scheme for analysing air traffic accidents and their consequences.

ATM. The second category deals with assessment of the risk of aircraft collision while airborne and/or on the ground due to deterioration of ATC/ATM separation rules. In addition, it embraces methods for assessment of the risk of collision of an aircraft generally with terrain and particularly during missed approach. The third deals with risk and safety assessment of air traffic incidents and accidents due to human error (mostly of ATC/ATM controllers). The final category considers the risk assessment for people on the ground, who might be affected by the aircraft crash.

The categorisation of models is somewhat arbitrary—there are inevitable overlaps and the dividing lines could have been different. There is a focus on proactive modelling approach—i.e., on models that anticipate the problems due to which the accidents occur. In terms of presentation, the approaches are largely examined in the order they were developed.

3. Causal models for risk and safety assessment

Causal 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. They can be qualitative or quantitative, with the former providing a diagrammatic or hierarchical description of the factors that might cause accidents, which is useful for improving understanding of causes of accidents and proposing means for avoiding them. The latter estimate the probability of occurrence of each cause and thus estimate the risk of accident. This can be restricted to pure statistical analysis based on the available data or it can combine such data with expert judgement on causes. In addition, they can estimate the relative benefits of different interventions aimed at preventing accidents (Spouge, 2004). The methods deployed include the following:

- Fault tree analysis (FTA) was developed by Bell Telephone Laboratories (Kumamoto and Henley, 1996) and has been used for analysing events or combinations of events that might lead to a hazard or an event with serious consequences. Usually, it has involved using a fault tree with paths representing different combinations of instant-direct and intermediate causes described by logical operators (“and” and “or”). At the top of the tree is a hazard event or a serious consequence. Then, for a given tree, the minimum cut set is determined—i.e., the minimal set of failures of which if all occur this is followed by the top event. One fault tree might have several minimal cut sets and if only one happens the top event also happens. The probability of occurrence of a given minimum cut set 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 the sum of probabilities of particular minimum cut sets. The method has been frequently applied to assess safety, as well as reliability of the aircraft and ATC/ATM computer components.
- Common cause analysis (CCA) is a method for identifying sequences of events leading to an aircraft accident. It is useful to extract the common causes of several aircraft accidents. 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. In addition, the method enables identifying and assessing hazard from external causes that might compromise independency between particular systems and components and cause their failures due to the same (common) causes. The US National Aeronautics and Space Administration (NASA) has used this method for a long time (since 1987) although the method itself is probably older than 1975. In addition, it has been recommended for assessment of the risk of failures of aircraft systems and equipment.
- Event tree analysis (ETA) method is used for modelling sequences of events arising from a single hazard and describe the seriousness of the outcomes from these events. ETA was developed in 1980 and is widely used. 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 is applicable in combination with FTA for almost all technical systems including aircraft and ATC/ATM components.
- Bow-Tie analysis presents a combination of ETA and FTA. Origins are from 1970s and 1980s, but since 1999 it has been popularised as a structured approach for risk analysis. The method was recently applied for control flight into terrain (CFIT) accidents (Spouge, 2004). It is complex and incorporates