Reliability Engineering and System Safety 142 (2015) 444–455

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Methodology for collision risk assessment of an airspace flow corridor concept

Yimin Zhang, John Shortle, Lance Sherry

George Mason University, Fairfax, Virginia

ARTICLE INFO

Article history:
Received 17 July 2014
Received in revised form
12 May 2015
Accepted 19 May 2015
Available online 28 May 2015

Keywords:
Dynamic event tree
Fault tree
Monte Carlo simulation
Air traffic management
Flow corridor concept
Autonomous Flight Management

ABSTRACT

This paper presents a methodology to estimate the collision risk associated with a future air-transportation concept called the *flow corridor*. This concept is designed to reduce congestion and increase throughput in en-route airspace by creating dedicated flight corridors across the continent. The methodology is a hybrid collision-risk methodology combining Monte Carlo simulation and dynamic event trees. Monte Carlo simulation is used to model the movement of aircraft within the corridor and to identify potential trajectories that might lead to a collision. Dynamic event trees are used to evaluate the effectiveness of subsequent safety layers that protect against collisions. The overall risk assessment captures the unique characteristics of the flow corridor concept, including self-separation within the corridor, lane change maneuvers, speed adjustments, and the automated separation assurance system. A tradeoff between safety and throughput is conducted, and a sensitivity analysis identifies the most critical parameters in the model.

1. Introduction

Transportation systems coordinate the efficient and safe flow of vehicles. The safety of these systems includes the risk of collision. In transportation systems that operate at high speeds in non-visual conditions, layers of collision assurance automation and procedures are defined to satisfy a required target safety level. To meet this target, collision risk assessments are faced with evaluating the rare-event occurrence of separation violations in vehicles controlled by autonomous agents with complex automation systems.

This paper presents a methodology to estimate the collision risk associated with a future air-transportation concept called the *flow corridor*. While the corridor concept is well studied with respect to concept design and benefits analysis, little has been done to address the safety of the proposed concept. This paper presents a hybrid collision-risk methodology that combines Monte Carlo simulation and dynamic event trees. Monte Carlo simulation is used to model the movement of aircraft within the corridor and to identify potential trajectories that might lead to a collision. The simulation captures unique characteristics of the corridor concept including self-separation, lane change maneuvers, and speed adjustments.

Dynamic event trees are then used to evaluate the effectiveness of subsequent safety layers that protect against collisions. While standard event trees are static, the event trees in this paper are dynamic in the sense that they capture the timing of events. For example, a dynamic event tree captures not just whether or not a conflict is detected (via a branch in the tree, as in a standard event tree), but also *when* the conflict is detected. This is important because conflicts detected later in time are more difficult to resolve, so the timing affects the downstream events in the tree.

Results based on the overall methodology and the associated modeling assumptions indicate that the collision risk is (to a rough order of magnitude) around 10^{-9} collisions per flight hour. A sensitivity analysis identifies the most critical parameters in the model. These parameters include the minimum separation, the transponder failure probability, conflict detection probabilities, and pilot response to the Traffic Collision Avoidance System (TCAS).

1.1. Flow corridor concept

The flow corridor is a Next Generation Air Transportation System (NextGen) concept to reduce congestion in en-route airspace [1]. It has the potential to increase en-route throughput by reducing the controller workload required to manage aircraft outside the corridor and by reducing aircraft separation within corridor [2,3]. A flow corridor consists of several closely-spaced

Abbreviations: ADS-B, Automatic Dependent Surveillance Broadcast; AFM, Autonomous Flight Management; CD&R, conflict detection and resolution; FAA, Federal Aviation Administration; ICAO, international civil aviation organization; LOL, loss of locatability; NextGen, Next Generation Air Transportation System; NMAC, Near Mid-air Collision; RNP, required navigation performance; SICDR, Strategic Intent-based CD&R Function; TICDR, tactical intent-based CD&R function; TIS-B, Traffic Information Service Broadcast; TSCDR, tactical state-based CD&R function; TCAS, Traffic Collision Avoidance System

E-mail addresses: yzhangk.gmu@gmail.com (Y. Zhang), jshortle@gmu.edu (J. Shortle), lsherry@gmu.edu (L. Sherry).

http://dx.doi.org/10.1016/j.ress.2015.05.015
0951-8320/

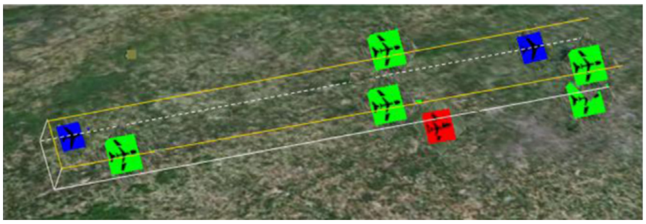

Fig. 1. Example flow corridor consisting of 4 lanes in a 2-by-2 configuration.

lanes in parallel. Fig. 1 shows a notional example with four lanes. The overall path of the corridor can be adjusted based on weather information to follow wind favorable routing. Corridor traffic is procedurally separated from other traffic so that non-corridor traffic does not penetrate the corridor.

Aircraft flying in the corridor are equipped with required navigation performance (RNP). RNP-x is a capability to fly within $\pm x$ nautical miles (nmi) of a centerline 95% of the time and within $\pm 2x$ nmi of a centerline 99.999% of time. In this paper, each lane is assumed to be 4 nmi in width, so an aircraft needs RNP-1 capability to fly in the corridor (that is, to fly within ± 2 nmi of the centerline 99.999% of the time). In the future, tighter RNP capabilities can be used reduce the lateral lane separation.

Within the corridor, pilots are responsible for maintaining separation, rather than controllers. Pilots maintain self-separation by monitoring an onboard display system, which shows the speed and position of nearby aircraft. In the case of a faster aircraft coming from behind and catching up to a slower aircraft, pilots can perform speed adjustments to fly behind the slower aircraft or can pass by changing lanes. Potential losses of separation are detected automatically by an onboard separation assurance system. The onboard system detects conflicts, determines possible resolutions, and displays the resolutions to the pilots, who must then execute one of the suggested resolutions in order to avoid a loss of separation. Examples of resolutions include speed adjustments, lane changes, horizontal turns, and altitude changes. Where possible, resolutions are given to keep aircraft within the flow corridor (e.g., speed adjustments or change lanes). Resolutions are implicitly coordinated in the sense that an aircraft's intended trajectory is broadcast to other aircraft. Thus, other aircraft are aware of the intended resolution maneuver and use this information to predict future conflicts. Due to the latency of broadcasting intent information (on the order of several seconds) it is possible for two aircraft to simultaneously initiate resolution maneuvers – for example, two aircraft simultaneously switching lanes in the corridor. Such a case is considered in this paper, though it turns out not to be a dominating factor in the overall safety estimate, due to the low-probability nature of near-simultaneous resolutions.

The onboard automated separation assurance system is based in part on the Autonomous Flight Management (AFM) concept in [5], though some details are specific to this paper. Suppose that two aircraft are on course for a near mid air collision (NMAC). The separation assurance system is assumed to incorporate four levels of safety, based on the time until the NMAC. The first level, called the strategic intent-based conflict detection and resolution (CD&R) function (SICDR), is designed to resolve conflicts (that is, trajectories that lead to a loss of separation, defined as two aircraft within 5 nmi laterally and 1000 feet vertically) 3–10 min prior to an NMAC. Resolutions at this level take the flight plan into account and provide waypoints back to the original track. The second level, called the tactical intent-based CD&R function (TICDR), is designed to resolve conflicts 2–3 min prior to an NMAC. This function takes advantage of available intent data to predict aircraft trajectories, but does not provide waypoints back to the original track. The third level, called the tactical state-based CD&R function (TSCDR), is designed to resolve conflicts 1–2 min prior to an NMAC. (Roughly speaking, it is still possible to avoid a loss of separation in this time frame, since the time from loss of separation to NMAC is about 1 min, though this estimate is highly dependent on conflict geometry.) This function predicts trajectories based solely on extrapolating future position from the current aircraft state vector. The final safety layer is the Traffic Collision Avoidance System (TCAS), which is mandated for all aircraft with a maximum take-off weight of over 12,600 lbs. TCAS resolutions are explicitly coordinated between the two aircraft – e.g., one aircraft is instructed to climb and the other to descend.

1.2. Related literature

Studies on the flow corridor concept can be summarized into several categories: concept description [6–9], location of candidate routes [10–14], aircraft equipage requirements [15,16], rules and procedures [17], and benefits analysis [2,3]. In general, little has been done to analyze the safety of the corridor concept. One study [18] estimates potential losses of separation in the corridor, but does not directly calculate collision risk or consider failures of the automation.

Other closely related studies are safety analyses of parallel route structures, such as the north Atlantic tracks. These parallel tracks connect the northeast of North America with Western Europe across the Atlantic Ocean. Because of a lack of radar coverage, lateral position errors are significantly increased. The Reich collision risk model [19] is often used to determine the safe lateral and vertical separation of such parallel tracks. However, the model has some limitations with respect to modeling the flow corridor concept. The model mainly emphasizes lateral and vertical navigation performance, but does not account for things like speed adjustments and lane change maneuvers that might occur within the corridor. Also, the Reich model does not account for the safety layers of the onboard CD&R functions and their potential failures. In [20], a generalized Reich collision model is used with hybrid-state Markov processes and Petri nets to model a 2 lane parallel route. The model considers aircraft performance of navigation, communication, and response times in the control loop.

Several papers have investigated the safety of automated separation assurance concepts [21–27]. These papers consider aircraft in an unstructured airspace, but do not consider the specific geometry of the conflicts. A unique feature of this paper is that geometry-specific scenarios are modeled in detail. Because of the simple geometry of the corridor, it is possible to enumerate all critical conflict geometries, which is more difficult to do in an unstructured airspace. A preliminary version of the dynamic event trees that appear in this paper is given in [27].

Free flight is a concept similar to AFM and has been modeled in several papers. Hoekstra et al. [28] discuss the conceptual design and validation of the free-flight concept. Bloom et al. [29] estimate the collision risk of the free flight concept using Monte Carlo simulation with Petri nets. One limitation is that it is time consuming to simulate a collision in terms of the low occurrence rates of failures.

Other related papers on aircraft reliability and safety include the following: Ale et al. [30] develop a method to analyze causal chains and quantify risks. The method combines event sequence diagrams, fault trees and Bayesian belief nets. Shalev et al. [31] discuss the condition-based fault tree analysis that can be used to model a system with sensitive components. Rao et al. [32] combine Monte Carlo simulation with fault tree analysis to address limitations of analytical methods in dealing with complex problems.

2. Methodology to estimate collision probability

This section describes the overall methodology to estimate the collision probability of the flow corridor concept-of-operations. The