Review of risk assessment status for air traffic

Henk Blom, Jaroslav Krystul, Pascal Lezaud, G.J. (bert) Bakker, Margriet B.
Klompstra, Bart Klein Obbing, Sybert H. Stroeve, Hans H. de Jong

Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

iFly

Safety, Complexity and Responsibility based design and
validation of highly automated Air Traffic Management

Specific Targeted Research Projects (STREP)

Thematic Priority 1.3.1.4.g Aeronautics and Space

iFly Deliverable D7.2.a

Review of risk assessment status for air traffic

Due date of deliverable: 22 November 2007
Actual submission date: 8 November 2007

Start date of project: 22 May 2007   Duration: 39 months

Version: Draft 0.3

DOCUMENT CONTROL SHEET

Title of document:	*Review of risk assessment status for air traffic*
Authors of document:	
Deliverable number:	*D7.2.a*
Project acronym:	*iFly*
Project title:	*Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management*
Project no.:	*TREN/07/FP6AE/S07.71574/037180 IFLY*
Instrument:	*Specific Targeted Research Projects (STREP)*
Thematic Priority:	*1.3.1.4.g Aeronautics and Space*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
0.1	14 June 2007	All	1st draft
0.2	18 October 2007	All	2nd draft
0.3	8 Nov. 2007	All	3rd draft
…			
1.0			

Version 0.3		Organisation	Signature/Date
Authors			
Henk A.P. Blom		NLR	
Jaroslav Krystul		TWEN	
Pascal Lezaud		DTI/SDER	
G.J. (Bert) Bakker		NLR	
Margriet B. Klompstra		NLR	
Bart Klein Obbing		NLR	
Sybert H. Stroeve		NLR	
Hans H. de Jong		NLR	
Internal reviewers			
External reviewers			

Contents

Contents

1 Introduction

1.1 Objectives

The objective of work package WP7 is to assess the A^3 operations developed by work packages WP1 and WP2, through hazard identification and Monte Carlo simulation on accident risk as a function of traffic demand, to assess what traffic demand can safely be accommodated by this advanced operational concept, and to assess the efficiency of the flights. The accident risk levels assessed should be in the form of an expected value, a 95% uncertainty area, and a decomposition of the risk level over the main risk contributing sources. The latter verifies which of these sources should have been mitigated during the 2nd design cycle by the A^4 concept. In order to accomplish this assessment through Monte Carlo simulation, the complementary aim of this WP is to further develop the innovative HYBRIDGE speed up approaches in rare event Monte Carlo simulation.

The aim of the current report is to give a thorough review of risk assessment status for advanced air traffic operations.

1.2 Accident risk assessment in ATM

Among the class of complex and safety critical industries, air traffic is an interesting example that poses exceptional challenges to advanced design. By its very nature, each aircraft has its own crew, and each crew is communicating with several human operators in different air traffic management (ATM) and airline operational control (AOC) centres on the ground in order to timely receive instructions critical to a safe flight. In addition, from an organisational perspective, air traffic involves interactions between many stake holders: pilots, air traffic controllers, airline operation centres, airport authorities, government regulators and the public travelling. Figure 1.2 highlights this characteristic feature of interplay between distributed decision making and safety criticality both for air traffic and for other complex or safety-critical industries, such as finance and nuclear and chemical plants. Among the safety critical industries, air traffic stands out regarding the many distributed levels of interactions in control and decision making.

The implication is that safety of air traffic is the result of interactions between multiple human operators, procedures (including spacing and separation criteria), and technical systems (hardware and software) all of which are highly distributed. Since safety depends crucially on the interactions between the various elements of a system, providing safety is more than making sure that each of these elements function properly. It is imperative
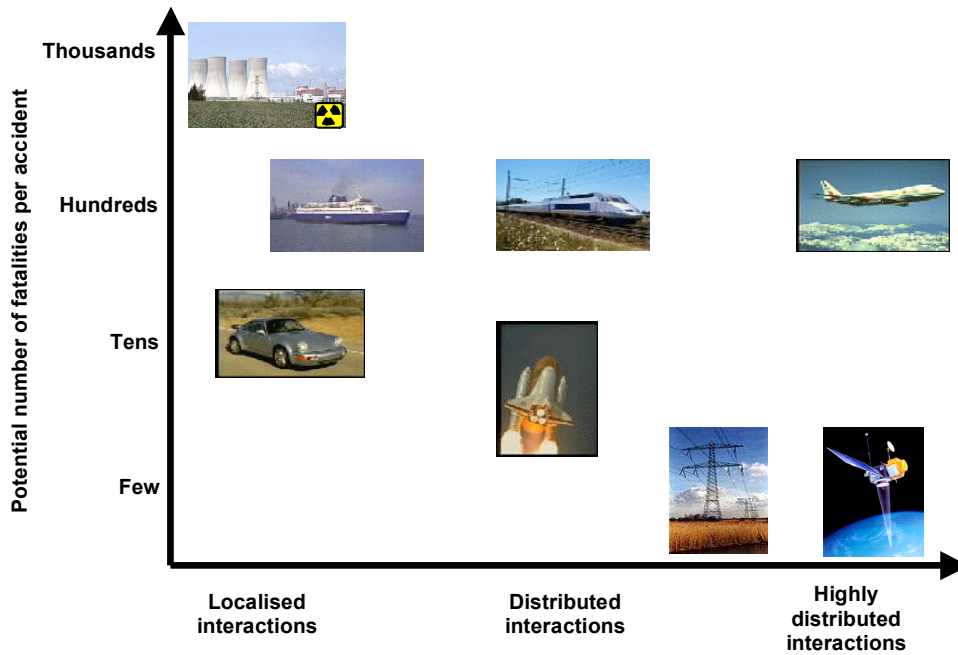
Figure 1.1: Air traffic compared with other complex and/or safety-critical industries in terms of potential number of fatalities per accident and the level of distributed interactions

to understand the safety impact of these interactions, particularly in relation to non-nominal situations.

Traditional ATM design approaches tend to be bottom-up, that is starting from developing concept elements aimed at increasing capacity, and next to extend the design with safety features. The advantage of the traditional approach is that advanced design developments can be organised around the clusters of individual elements, i.e., the communication cluster, the navigation cluster, the surveillance cluster, the automation tools cluster, the controllers/pilots and their human machine interfaces (HMIs), the advanced procedures, etcetera. The disadvantage of this traditional approach is that it fails to fully address the impact of interactions between controllers, pilots and ATM systems on safety.

A goal oriented approach would be to design ATM such that safety has been built in at the capacity-level required. From this perspective, safety assessment forms a primary source of feedback (Figure 1.2) in the development of advanced ATM designs. An early guidance of ATM design development on safety grounds can potentially avoid a costly redevelopment program, or an implementation program that turns out to be ineffective. Although understanding this idea is principally not very difficult, it can be brought into practice only when an ATM safety assessment approach is available that provides appropriate feedback to the ATM designers from an early stage of the concept development

(Figure 1.2). This feedback should provide information on which safety-capacity issues are the main contributor to unsafety.
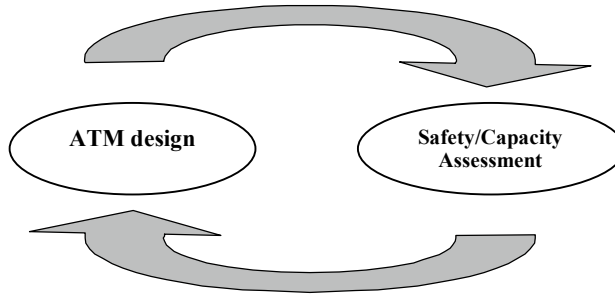
Figure 1.2: Safety feedback based ATM design

Collision risk modelling for air transportation was initially developed in the 1960s to address the safety of proposed separation standard reductions in the North Atlantic Organized Track Structure. The civil aviation community has developed a mathematical model to estimate mid-air collision risk levels as a function of spacing values in route structures [56]. This model is known as the Reich collision risk model; it assumes that the physical shape of each aircraft is a box, having a fixed orientation, and the collision risk between two aircraft is approximated by an expression that has proven to be of practical use in designing route structures [54]. Apart from the approximation, the most severe shortcoming is that the Reich model does not adequately cover situations where interaction between pilots and controllers play a crucial role, e.g. when controllers monitor the air traffic through surveillance systems and provide tactical instructions to the aircraft crews. These shortcomings of the methodology have led to the development of new approaches and relevant tools for the safe separation assessment of advanced procedures in air traffic, e.g Analytic Blunder Risk Model (ABRM), Airspace Simulation and Analysis for Terminal instrument procedures (ASAT), ICAO's Collision Risk Model (CRM), Reduced Aircraft Separation Risk Assessment Model (RASRAM) [89] and Traffic Organization and Perturbation AnalyZer (TOPAZ) [9]. An extensive overview of these approaches can be found in [26]. TOPAZ appeared to be the most advanced in going beyond established approaches. It was developed by National Aerospace Laboratory NLR as a safety risk assessment methodology which provides safety risk feedback to advanced air traffic operation design. Within TOPAZ, Petri net modelling and Monte Carlo simulation has proven to deserve a key role in modelling and assessment of advanced air traffic operations on safety risk [5, 10, 13, 14, 15, 16, 38, 39, 41, 90]. In this respect it is relevant to notice that the use of Petri nets has been shown to work well in modelling safety critical operations in nuclear and chemical industries (e.g. [72]).

In this report we will explain in details the TOPAZ methodology and present recent extensions which were developed during the HYBRIDGE project.

1.3 Organisation of this report

This report is organized as follows.

The aim of Chapter 2 is to explain how the TOPAZ methodology effectively uses Monte Carlo simulation in safety risk assessment of an advanced air traffic operation. Emphasis is on how Monte Carlo simulation of safety risk works and how this is embedded within a complete safety risk assessment cycle. First, Section 2.2 provides an overview of the steps of the TOPAZ safety risk assessment cycle and for which step Monte Carlo simulation is of direct use. Next, Section 2.3 provides an overview of how to develop a Monte Carlo simulation model of a given operation. In order to keep the explanation concrete, a particular example is introduced first. Subsequently, Section 2.4 provides an overview of key issues that have to be taken into account when using a Monte Carlo simulation supported safety risk assessment. Section 2.5 presents Monte Carlo simulation results for the particular example identified in Section 2.3. Finally, conclusions are drawn in Section 2.6.

Chapter 3 presents novel sequential Monte Carlo simulation methods which were developed within HYBRIDGE project for a much efficient estimation of collision risk in advanced ATM scenarios. The approach is demonstrated on application of these novel Monte Carlo techniques to a free flight air traffic concept of operations. Section 3.2 develops the sequential Monte Carlo simulation approach toward probabilistic reachability analysis of a Generalised Stochastic Hybrid System (GSHS) model of free flight air traffic. Section 3.3 explains how an initial GSHS model has been developed for a specific free flight air traffic concept of operation. Section 3.4 applies the sequential Monte Carlo simulation approach of Section 3.2 to the GSHS model of Section 3.3. Section 3.5 draws conclusions.

2 Safety Risk Assessment by Monte Carlo Simulation of Complex Safety Critical Operations

2.1 Introduction

This chapter gives an overview of performing safety risk assessment of a safety critical operation with support of Monte Carlo simulation. The approach is outlined for an air traffic example involving aircraft departing from a runway, which is occasionally crossed by taxiing aircraft. At the airport considered, a Runway Incursion Alert System (RIAS) is installed to warn the air traffic controller in case of impending runway incursions. The chapter explains the key issues to be mastered in performing a Monte Carlo simulation supported safety risk assessment of this kind of operation. To begin with, one has to develop an appropriate simulation model, and a sound way to speed up the Monte Carlo simulation based on this model. Complementary, one has to validate the simulation model versus the real operation, and the simulation supported approach has to be embedded within the safety risk assessment of the total operation. For this application example Monte Carlo simulation results are given and the way of feedback to the design of the operation is outlined.

2.2 Safety Risk Assessment Steps

An overview of the steps in a TOPAZ safety risk assessment cycle is given in Figure 2.1. Although the cycle itself is very much in line with the established risk assessment steps (e.g. [70]), some of these steps differ significantly.

In step 0, the objective of the assessment is determined, as well as the safety context, the scope and the level of detail of the assessment. The actual safety assessment starts by determining the operation that is assessed (step 1). Next, hazards associated with the operation are identified (step 2), and aggregated into safety relevant scenarios (step 3). Using severity and frequency assessments (steps 4 and 5), the safety risk associated with each safety relevant scenario is classified (step 6). For each safety relevant scenario with a (possibly) unacceptable safety risk, the main sources contributing to unsafety (safety bottlenecks) are identified (step 7), which help operational concept developers to learn for which safety issues they should develop improvements in the ATM design. If the
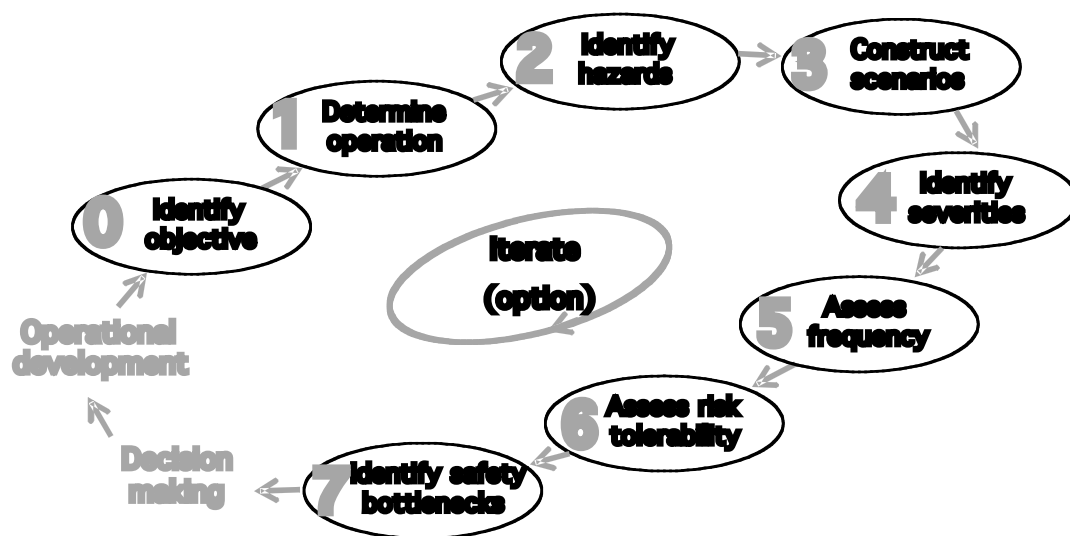
Figure 2.1: Steps in TOPAZ safety risk assessment cycle

ATM design is changed, a new safety risk assessment cycle of the operation should be performed in order to investigate how much the risk posed by previous safety issues has been decreased, but also to assess any new safety issues that may have been introduced by the enhancements themselves.

The following subsections present the risk assessment steps of a TOPAZ cycle in more detail. Then it also becomes clear that Monte Carlo simulation plays a key role in step 5: assess frequency.

Step 0: Identify objective

Before starting the actual safety assessment, the objective and scope of the assessment are set. This should be done in close co-operation with the decision makers and designers of the advanced operation. Also, the safety context must be made clear, such that the assessment is performed in line with the appropriate safety regulatory framework.

An important issue for setting the safety context is the choice of safety criteria with respect to which the assessment is performed. Depending of the application, such criteria are defined for particular flight condition categories (e.g. flight phases or sub-phases) and for particular severity categories (e.g. accident, serious incident). Typically, within the chosen context, these criteria define which flight condition/severity categories have to be evaluated and which frequency level forms the Target Level of Safety (TLS) threshold per flight condition/severity category.

Step 1: Determine operation

Step 1 serves for the safety assessors to obtain a complete and concise overview of the operation, and to freeze this description during each safety assessment cycle. Main input to step 1 is a description of the operational concept from the designers, while its output is a sufficiently complete, structured, consistent and concise description of the operation considered. The operation should be described in generic terms, the description should provide any particular operational assumption to be used in the safety assessment, and the description has to be verified by the operational concept designers. Typically during this step, holes and inconsistencies in the concept as developed are also identified and immediately fed back to the design team.

Step 2: Identify hazards

The term hazard is used in the wide sense; i.e. an event or situation with possibly negative effects on safety. Such a non-nominal event or situation may evolve into danger, or may hamper the resolution of the danger, possibly in combination with other hazards or under certain conditions. The goal of step 2 is to identify as many and diverse hazards as possible. Hazard identification brainstorming sessions are used as primary means to identify (novel) hazards.

In system engineering, the functional approach to hazard identification is well-known. In this approach it is attempted to determine all possible failure conditions and their effects, for each function that plays a role in the operation, including the human operator tasks. Unfortunately, the approach cannot identify all hazards related to an operation that involves human operators. An important reason for this is that the performance of air traffic controllers and pilots depend on their (subjective) situational awareness. From a human cognition perspective a particular act by an air traffic controller or pilot can be logical, while from a function allocation perspective the particular act may be incorrect. Such incidents are often called "errors of commission" [91]. An example of error of commission in the crossing operation is that because of the complicated taxiway structure, the pilot thinks to be taxiing far from the runway, while in reality, he starts crossing the runway without noticing any of the runway signs.

Another well-known technique of hazard identification is the HAZOP (HAZard and OP-erability) method. With this method, hazards are identified and analyzed using sessions with operational experts. At the same time, the experts come up with potential solutions and measures to cope with the identified hazards [63]. The advantage of HAZOP with respect to the functional approach is that also non-functional hazards are identified during the brainstorm with operational experts. However, in applying HAZOP, one needs to take care that hazard analysis and solution activities do not disturb the hazard identification process, which could leave certain hazards unidentified or inappropriately "solved". Leaving such latent hazards in a design typically is known to be very costly in safety critical operation.

Based on the experience gained in using the hazard identification part of HAZOP in a large number of safety analyses and on scientific studies of brainstorming, NLR has developed a method of hazard identification for air traffic operations – by means of pure brainstorming sessions [60]. In such a session no analysis is done and solutions are explicitly not considered. An important complementary source is formed by hazards identified in previous studies on related operations. For this purpose, hazards identified in earlier studies are collected in a TOPAZ database.

Step 3: Construct scenarios

When the list of hazards is as complete as reasonably practicable, it is processed to deal with duplicate, overlapping, similar and ambiguously described hazards. First, per flight condition selected in Step 0, the relevant scenarios which may result from the hazards are to be identified using a full list of potentially relevant scenarios, such as for instance 'conflict between two aircraft merging onto one route' or 'aircraft encounters wake vortex of parallel departure'. Per flight condition, each potentially relevant scenario is subsequently used as crystallisation point upon which all applicable hazards and their combined effects are fitted. If hazards are not appropriately addressed by the crystals developed so far, then additional crystallisation points are defined. The output of such crystallisation process is a bundle of event/condition sequences and effects per crystallisation point, and these are referred to as a safety relevant scenario. This way of constructing scenarios aims to bring into account all relevant ways in which a hazard can play a role in each flight condition/severity category.

In order to cope with the complexity of the various possible causes and results, clusters of similarly crystallised hazards are identified. A cluster of hazards could for instance be the set of 'events causing a missed approach to deviate from the normal path'. An example is given in Figure 2.2. It should also be noticed that the same cluster of hazards may play a role in one or more safety relevant scenarios.

Each of the identified hazards can be of the following types:

- a root hazard (cluster), which may cause a safety relevant scenario; or
- a resolution hazard (cluster), which may complicate the resolution of a safety relevant scenario.

For an appropriate safety risk assessment, all combinations of root and resolution hazards have to be evaluated in the next steps.

Step 4: Identify severities

For each of the safety relevant scenarios identified in step 3, it is determined which of the severity categories selected in step 0 are applicable to its possible effects. Safety experts should assess which of the severities are applicable for each safety relevant scenario, by
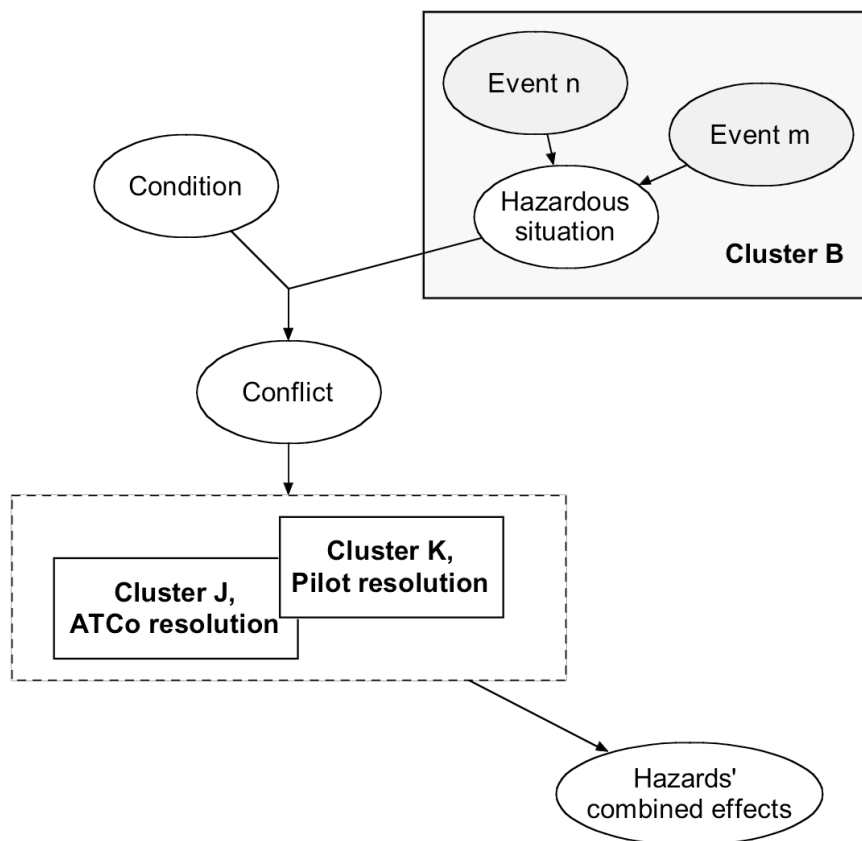
Figure 2.2: Example of a safety relevant scenario diagram

consultation of and review by operational experts. For each safety relevant scenario the effects and their severities depend on many factors, such as the conditions under which the scenario starts and evolves, the geometry of the scenario, and the possibilities of (timely) resolution of the conflict. Therefore, a range of severities may apply to a safety relevant scenario. If necessary, the structuring of the events in the safety relevant scenarios of step 3 are updated such that each applicable severity category is linked to the occurrence of specific event sequences.

Step 5: Assess frequency

Next, for each possible severity outcome of each safety relevant scenario, the occurrence frequency is evaluated by making use of an appropriate tree per safety relevant scenario. The probability of the top event in the tree is expressed as a sum of a product of probabilities of applicable conditional events. For assessing the factors in these trees, primary sources of data are operational experts and databases. Examples of databases are aviation safety databases, local controller reporting system(s), et cetera. For appro-

priate use of such data dedicated operational expertise is taken into account. Hence, important input for the frequency assessments is always formed by interviews with operational experts (including experienced pilots and controllers) who are as much as is possible familiar with the operation under consideration. Qualitative expressions are to be translated in quantitative numbers when the selected safety criteria of step 0 also are expressed in numbers. Complicating factors in assessing at once the frequency of a conflict ending in a given severity can be that there is often little or no experience with the new operation, and that the situation may involve several variables. This holds especially for the more severe outcomes of a safety relevant scenario, since these situations occur rarely, and consequently little information is at hands about the behaviour of air traffic controllers and pilots in such situations. For these difficult safety relevant scenarios it is logical to make use of Monte Carlo simulation of safety risk. This approach has three clear advantages: 1) the quality of the risk estimate improves; 2) it is possible to estimate a 95% confidence interval; and 3) once a Monte Carlo simulation tool for a particular application has been developed it can be re-used for assessing safety risk for similar applications. The next sections explain for an example safety risk assessment by Monte Carlo simulation.

Step 6: Assess risk tolerability

The aim of this step is to assess the tolerability of the risk for each of the flight condition/severity categories selected in step 0. First the total risk per flight condition/severity category is determined by summing over the assessed risk contributions per safety relevant scenario for that flight condition/severity category. This summation takes into account both the expected value and the 95% confidence interval of the risk summation. Next for each flight condition/severity category the total risk expected value and the 95% confidence interval are compared against the TLS selected in step 0.

Step 7: Identify safety bottlenecks

From the risk tolerability assessment, it follows which safety relevant scenario(s) contribute(s) most to the expected value and the 95% confidence interval of the risks that has been qualified as being not below the TLS. For each safety relevant scenario the hazards or conditions that contribute most to the high risk level or confidence interval are identified and localised during step 7. These are referred to as the safety bottlenecks. If desired, this may also be done for assessed risk levels that are just below the TLS. The identification and localisation of safety bottlenecks is important as it gives operational concept designers directions for searching potential risk mitigating measures of the operation, and it gives the safety assessment experts the hazards and conditions for which the reduction of uncertainty has priority.

2.3 Monte Carlo Simulation Model

2.3.1 Active Runway Crossing Example

The Monte Carlo simulation-based risk assessment approach will be illustrated for an active runway crossing operation. This example accounts for a number of interacting human agents (pilots and controllers). The runway configuration of the active runway crossing operation considered is shown in Figure 2.3. The configuration takes into account one runway, named runway A, with holdings for using the runway from two sides (A1 and A2) and with crossings (C1, C2, D1 and D2) and exits (E1, E2, E3 and E4). The crossings enable traffic between the aprons and a second runway, named runway B. Each crossing has remotely controlled stopbars on both sides of the runway. Also the holdings have remotely controlled stopbars and each exit has a fixed stopbar.
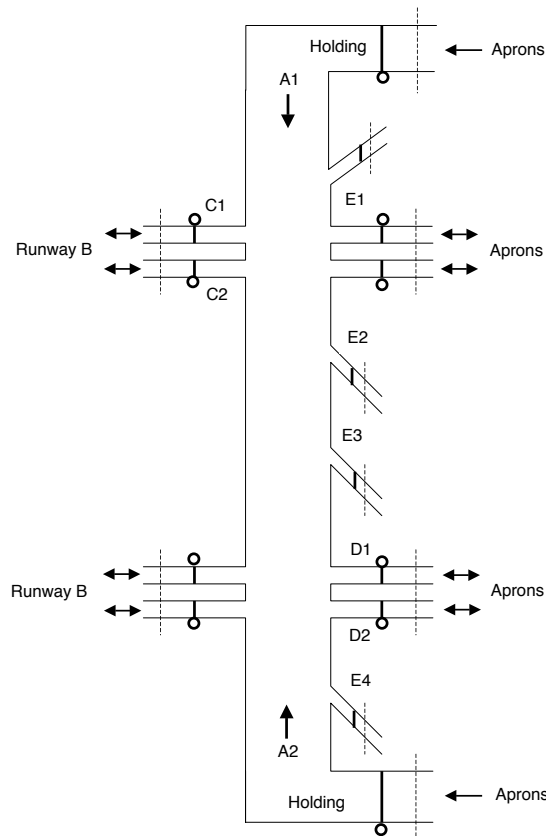
Figure 2.3: Runway configuration of active runway crossing procedure

The involved human operators include the start-up controller, the ground controller, the runway A controller, the runway B controller, the departure controller, and the pilots flying (PF's) and pilots not flying (PNF's) of aircraft taking off and aircraft crossing. Communication between controllers and aircraft crews is via standard VHF R/T (Very High Frequency Receiver/Transmitter). Monitoring by the controllers can be by direct visual observation under sufficiently good visibility conditions; it is supported by ground radar surveillance. The runway A controller is supported by a runway incursion alert system and a stopbar violation alert system. The runway A controller manages the remotely controlled stopbars and the runway lighting. Monitoring by the aircraft crews is by visual observation, supported by the VHF R/T party-line effect.

In the runway crossing operation considered, the control over the crossing aircraft is transferred from the ground controller or the runway B controller (depending on the direction of the runway crossing operation) to the runway A controller. If the runway A controller is aware that the runway is not used for a take-off, the crew of an aircraft intending to cross is cleared to do so and subsequently the appropriate remotely controlled stopbar is switched off. The PNF of the crossing aircraft acknowledges the clearance and the PF subsequently initiates the runway crossing. When the crossing aircraft has vacated the runway, then the PNF reports this to the runway A Controller. Finally, the control over the aircraft is transferred from the runway A controller to either the runway B controller or the ground controller.

2.3.2 Safety Relevant Scenarios

Prior to the development of a quantitative accident risk model for the active runway crossing operation considered, all risk assessment steps had been performed using an expert-based approach. In this study the following safety relevant scenarios were found:

- Scenario I: Aircraft erroneously in take-off and crossing aircraft on runway;
- Scenario II: Aircraft erroneously crossing and other aircraft in take-off;
- Scenario III: Aircraft taking off and runway unexpectedly occupied;
- Scenario IV: Aircraft crossing and runway unexpectedly occupied by aircraft;
- Scenario V: Aircraft crossing and vehicle on runway;
- Scenario VI: Collision between aircraft sliding off runway and aircraft near crossing;
- Scenario VII: Aircraft taking off and vehicle crossing;
- Scenario VIII: Jet-blast from one aircraft to another;
- Scenario IX: Conflict between aircraft overrunning/climbing out low and aircraft using a nearby taxiway.

From this expert-based study it followed that of all identified safety relevant scenarios, for scenarios I, II and III it was difficult to assess the risk sufficiently accurate using an

expert based approach. For these three scenarios it is therefore useful to assess the risk through performing Monte Carlo simulations.

In this chapter, we focus on the details of a Monte Carlo simulation accident risk model for scenario II. In this scenario there is one aircraft that takes off and has been allowed to do so and there is one aircraft that crosses the runway while it should not. Taxiing along a straight line over one of the standard runway crossings (i.e., via C1, C2, D1 or D2 in Figure 2.3) is considered.

2.3.3 Multi-Agent Situation Awareness in the Simulation Model

The safe organisation of co-operation between pilots and controllers in air traffic depends to a large extent on the "picture" or situation awareness (SA) maintained by each of the pilots and controllers. When a difference, even a small one, sneaks into the individual pictures and remains unrecognised, this may create unnoticed miscommunication and a subsequent propagation and increase in differences between the individual pictures. Eventually the situation may spiral out of control, with potentially catastrophic results. Hence any mismatch between individual pictures forms a serious hazardous condition in maintaining a safe organisation. Many hazards identified for the runway crossing operation were of this type.

Endsley [36] has defined human SA as the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. Stroeve et al. [90] and Blom and Stroeve [15] have captured these perception, comprehension and projection notions of SA mathematically in terms of three components: State SA, Mode SA and Intent SA. They also extended this single (human) agent SA concept to a multi-agent SA concept for operations involving multiple humans and systems, inclusive the basic updating mechanisms of such multi-agent SA.

As depicted in Figure 2.4, for the active runway crossing operation we identified a need to model 10 agent types (7 humans and 3 systems) and their interactions:

- Pilots flying;
- Pilots not flying;
- (Each) aircraft;
- Aircraft's flight management systems (FMS);
- Runway A controller;
- Runway B controller;
- Ground controller;
- Departure controller;
- Start-up controller;
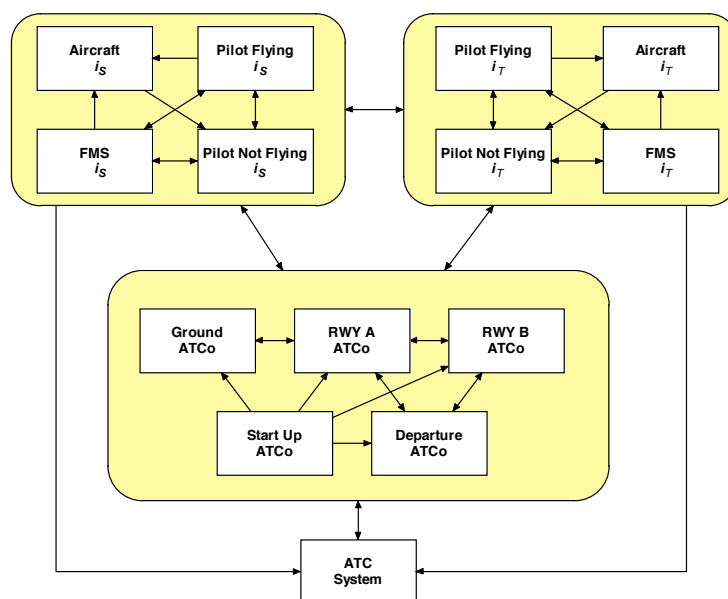
Figure 2.4: Relations between agents identified for the active runway crossing operation

- ATC system, which we broadly define to include airport manoeuvre control systems, air traffic communication and surveillance systems, airport configuration and environmental conditions.

2.3.4 Dynamic Stochastic Modelling

The Monte Carlo simulations are based on dynamic stochastic models of all relevant agents. These simulation models are mathematically specified using the Dynamically Coloured Petri Net (DCPN) formalism [39, 41]. A high-level overview of the agents modelled is provided next.

Taking-off Aircraft

The model of the taking-off aircraft represents the ground run, airborne transition and airborne climb-out phases and includes the possibility of a rejected take-off. The taking-off aircraft initiates its take-off from a position near the runway threshold and may have a small initial velocity. The aircraft may have diminished acceleration or deceleration power. Two types of aircraft are included in the model: medium-weight aircraft and heavy-weight aircraft.

Taxiing Aircraft

The model of the taxiing aircraft represents aircraft movements (hold, acceleration, constant speed, deceleration) during taxiing. The taxiing aircraft enters the taxiway

leading to a runway crossing at a position close to the remotely controlled stopbar, with a normal taxiing speed or initiates taxiing from stance. The entrance time of the crossing aircraft is uniformly distributed around the take-off start time. The taxiing aircraft may have diminished deceleration power. Two types of aircraft are included in the model: medium-weight aircraft and heavy-weight aircraft.

Pilot Flying of Taking-off Aircraft

Initially, the pilot flying (PF) of a taking-off aircraft has the SA that taking-off is allowed and initiates a take-off. During the take-off the PF monitors the traffic situation on the runway visually and via the VHF communication channel. The PF starts a collision avoiding braking action if a crossing aircraft is observed within a critical distance from the runway centre-line or in reaction to a call of the controller, and if it is decided that braking will stop the aircraft in front of the crossing aircraft. Further details of taking-off aircraft PF model are given by [90].

Pilot Flying of Taxiing Aircraft

Initially, the PF expects that the next airport way-point is either a regular taxiway or a runway crossing. In the former case the PF proceeds taxiing and in the latter case the PF may have the SA that crossing is allowed. The characteristics of the visual monitoring process of the PF depend on the intent SA. In case of awareness of a conflict, either due to own visual observation or due to a controller call, the PF stops the aircraft, unless it is already within a critical distance from the runway centre-line. Further details of taxiing aircraft PF model are given by [90].

Runway Controller

The runway A controller visually monitors the traffic and has support from a stopbar violation alert and a runway incursion alert. If the controller is aware that a taxiing aircraft has passed the stopbar, a hold clearance is given to both taxiing and taking off aircraft. Further details of the runway controller model are given by [90].

Radar Surveillance System

The model of the radar surveillance system represents position and velocity estimates for both aircraft. There is a probability that radar surveillance is not available, resulting in track loss. Radar surveillance data is used as basis for ATC stopbar violation alerting and ATC runway incursion alerting.

ATC Alerts

Two types of ATC alerts are included in the model: a stopbar violation alert and a runway incursion alert. A stopbar violation alert is presented to the controller if surveillance data indicates that an aircraft has passed an active stopbar. There is a probability that the stopbar violation alert system does not function, implying that there will be no alert. A runway incursion alert is presented to the controller if radar surveillance data indicates that the taxiing aircraft is within a critical distance of the runway centre-line and the taking-off aircraft has exceeded a velocity threshold in front of the runway crossing. There is a probability that the runway incursion alert system does not function, implying that there will be no alert.

VHF Communication Systems

The model for the VHF communication system between the runway controller and the aircraft crews accounts for the communication system of the aircraft, the communication system of the controller, the tower communication system, the frequency selection of aircraft communication system and the VHF communication medium. The nominal status of these communication systems accounts for direct non-delaying communication. The model accounts for a probability of delay in or failure of the communication systems.

2.4 Use of Simulation Model in Risk Assessment

Once the simulation model has been specified, there are several important aspects that have to be taken into account during the preparation, execution and interpretation of the Monte Carlo simulations. This section explains these aspects.

2.4.1 Does the Simulation Model Cover the Identified Hazards?

During step 2 of the safety assessment cycle, a lengthy list of hazards, including non-nominal situations, has been identified. These hazards contribute individually and possibly in combination with other hazards to the safety risk of the operation considered. Hence it is quite important to verify prior to performing the simulations that the hazards identified in step 2 of the assessment cycle are covered by the model. The verification process consists of specifying per hazard how it is captured by the simulation model. A special class of hazards is formed by the situation awareness related hazards. Table 2.1 shows three of such situation awareness related hazards and includes a short explanation how these hazards are covered by the simulation model.

Table 2.1: Examples of situation awareness related hazards and their simulation model.

Hazard	Simulation model
Pilots become confused about their location at the airport because of complexity of the airport layout.	State SA of the PF of a taxiing aircraft is that its aircraft is at a location that differs from the actual location.
Crew of taxiing aircraft is lost and therefore not aware of starting to cross a runway.	Intent SA of PF is and stays taxiing while PF starts crossing the runway.
RIAS is switched off by maintenance and controllers are not informed.	RIAS working or not is not connected to Mode SA of controllers.

Inevitably this verification of each hazard against the model will lead to the identification of hazards that are not (yet) covered by the simulation model. For non-covered hazards the simulation model developers should consider to further extend the simulation model prior to performing Monte Carlo simulations.

2.4.2 Parametrisation of the Simulation Model

During the mathematical specification of the simulation model there is no need to bother about the correct parameter values to be used during the Monte Carlo simulation. Of course, this is addressed prior to running the simulations. In principle there are three kinds of sources for parameter values. The ideal source would consist of sufficient statistical data that has been gathered under the various contextual conditions for which the risk assessment has to be performed. In practice such ideal sources almost never exist. Instead one typically has to work with limited statistical data that has been gathered under different conditions. Fortunately there often are two complementary sources: domain expertise and scientific expertise (on safety and human factors). In the context of Monte Carlo simulation this means one fuses statistical and expertise sources into a probability density function for the possible values of each parameter. Typically the mean or mode of such a density function is then used as the best estimate of the parameter value to be used when running the Monte Carlo simulation.

2.4.3 Speeding up Monte Carlo Simulations

Air traffic is a very safe means of transport. Consequently, the risk of collision between two aircraft is extremely low. The assessment of such low collision risk values through straightforward Monte Carlo simulation would need extremely lengthy computer simulation periods. In order to reduce this to practicable periods, five to six orders of magnitude in speeding up the Monte Carlo simulation are needed. The basis for realizing such speed-up factors in Monte Carlo simulation consists of decomposing accident risk simulations in a sequence of conditional Monte Carlo simulations, and then to combine the results of these conditional simulations into the assessed collision risk value. For the evaluation of logical systems good decomposition methods can often be obtained by Fault and Event Tree Analysis. Because air traffic operations involve all kinds of dependent, dynamic and concurrent feedback loops, these logic-based risk decomposition methods cannot be applied without adopting severe approximations, typically by assuming that events/entities happen/act independent of each other.

The stochastic analysis framework, that has shown its value in many applications (e.g. in financial mathematics [50]), is exploited by the TOPAZ methodology to develop Monte Carlo simulation models and appropriate speed-up factors by risk decomposition. The power of these stochastic analysis tools lies in their capability to model and analyse in a proper way the arbitrary stochastic event sequences (including dependent events) and the conditional probabilities of such event sequences in stochastic dynamic processes [10, 65]. By using these tools from stochastic analysis, a Monte Carlo simulation based risk assessment can mathematically be decomposed into a well-defined sequence of conditional Monte Carlo simulations together with a subsequent composition of the total risk out of these conditional simulation results. The latter composition typically consists of a tree with conditional probabilities to be assessed at the leaves, and nodes which either

add or multiply the probabilities coming from the subbranches of that node. Within TOPAZ such a tree is referred to as a collision risk tree [9, 10].

For the active runway crossing example, the particular conditions taken into account for this risk decomposition are:

- The type of each aircraft (either a medium-weight or a heavy-weight);
- The intent SA of the PF of a crossing aircraft concerning the next way-point (Taxiway/Crossing) and concerning allowance of runway crossing (Allowed/Not Allowed);
- The alert systems (functioning well or not);
- The remotely controlled stopbar (functioning well or not); and
- The communication systems (functioning well or not).

Based on the simulation model and the accident risk decomposition, Monte Carlo simulation software is developed to evaluate the event probabilities and the conditional collision risks, and to compose this with the help of the collision risk tree into the collision risk value assessed for the simulation model.

2.4.4 Validation of the assessed risk level

For operations as complex as the active runway example considered, a simulation model will always differ from reality. Hence, validation of the Monte Carlo simulation results does not mean that one should try to show that the model is perfect. Rather one should identify the differences between the simulation model and reality, and subsequently analyse what the effects of these differences are in terms of bias and uncertainty at the assessed risk level of the model. If the bias and uncertainty fall within acceptable bounds, then the assesed risk levels are valid for the specified application. Otherwise one should improve the Monte Carlo simulation model on those aspects causing the largest bias and uncertainty influence on the assessed risk level.

Five types of differences between simulation model and the real operation can be distinguished [38]:

- Numerical approximations;
- Parameter values;
- Assumptions on the model structure;
- Non-covered hazards;
- Differences between the real operational concept and the operational concept modelled.

Thinking in terms of these differences makes it possible to consider the validation problem as a problem of making the differences specific, assessing each difference and its effect

on the collision risk, and subsequently decide if this is accurate enough (valid) or not (invalid) for the purpose aimed at. The effects of differences on the collision risk can mathematically be expressed in terms of bias and uncertainty that has to be taken into account when using the simulation model assessed risk value for decisions about reality:

- *Bias.* The accident risk as defined by the simulation model is systematically higher or lower than it is for the real operation.
- *Uncertainty.* In addition to a systematic bias, the differences between simulation model and reality may induce uncertainty in the difference between the safety risk of the real operation and the safety risk resulting from the simulation model.

With this, the validation of a simulation based accident risk assessment has largely become a bias and uncertainty assessment process. Within TOPAZ, a bias and uncertainty assessment method has been developed which consists of the following steps:

- Identify all differences between the simulation model and reality;
- Assess how large these differences are, or how often they happen;
- Assess the sensitivity (or elasticity) of the risk outcome of the simulation model to changes in parameter values;
- Assess the effect of each difference on the risk outcome, using model sensitivity knowledge and complementary statistical and/or expert knowledge;
- Combine the joint effects of all differences in bias and uncertainty factors, and compensate the risk value of the model with these bias and uncertainty factors.

The result is an expected value of risk for the real operation, including a 95% confidence interval of other possible risk values. If the bias or the 95% confidence interval of the combined effects, or the bias and uncertainty of individual differences is too large, then these differences have to be taken into account in the decision making process regarding the acceptability and/or further design of the operation considered.

2.5 Monte Carlo Simulation Results

This section presents collision risk results obtained by Monte Carlo simulation with a computer implementation of the mathematical model of the active runway example of Section 2.3. In order to relate these results to an actual operation, a bias and uncertainty assessment remains to be performed; however, this falls outside the scope of this chapter.

2.5.1 Assessed risk levels

Figure 2.5 shows the accident risk as function of the position of the runway crossing with respect to the runway threshold. The probability of a collision decreases for positions
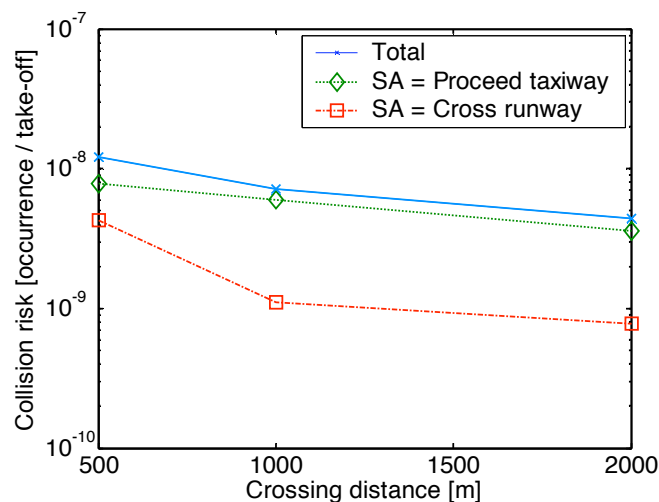
Figure 2.5: Contributions to the total collision risk by the simulation model for the cases that the SA of the PF of the taxiing aircraft is to proceed on a taxiway, or to cross the runway

of the crossing distances further from the threshold. Figure 2.5 also shows the decomposition of the total risk for the cases that the pilot flying of the taxiing aircraft either thinks to be proceeding on a normal taxiway (without being aware to be heading to a runway crossing) or where the pilot intends to cross the runway (without being aware that crossing is currently not allowed). The largest contribution to the risk is from the situation that the pilot thinks to be proceeding on a normal taxiway. The relative size of this contribution depends on the crossing distance and varies from 64% for crossing at 500 m to about 83% for crossing at 1000 or 2000 m.

A more complete overview of the contributions to the collision risk is provided by a projected version of the collision risk tree in Figure 2.6. It shows the contributions of events related to the situation awareness of the pilot of the taxiing aircraft (Cross runway/Proceed runway) and the functioning of ATC alert and communication systems (Up/Down). The collision risk results in the leaves of the tree are the product of the probability of the event combination indicated and the Monte Carlo simulation based collision risk given the event combination. The results in Figure 2.6 show that the risk is dominated by situations with a pilot flying of a taxiing aircraft having an erroneous situation awareness and the ATC alert and communication systems working nominally.

2.5.2 Who contributes to safety risk reduction?

Based on results of the accident risk model, it is possible to attain insight in the accident risk reducing performance of involved human operators and technical systems. Table 2.2 shows conditional collision risks for the situation that an aircraft taxies towards a runway crossing at a distance of 1000 m from the runway threshold while the pilot has
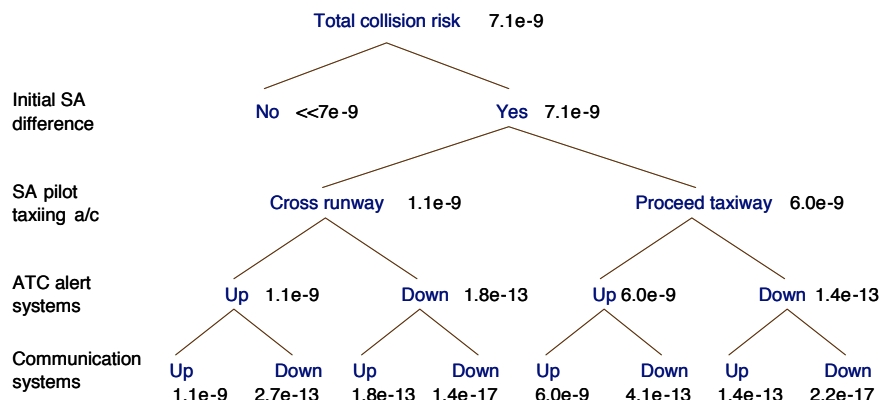
Figure 2.6: Projected version of the collision risk tree for the active runway crossing example, showing the contributions to the collision risk for various combinations of events related to pilot situation awareness and functioning of ATC alert and communication systems. The values are for a crossing distance of 1000 m

the situation awareness to taxi on a normal taxiway. The conditional collision risks in Table 2.2 refer to cases where the model either does ('yes') or does not ('no') involve the indicated human operators actively monitoring for traffic conflicts. A risk reduction percentage is determined by comparing the conditional collision risk with the situation in which none of the human operators is actively monitoring. In this case, a collision is only avoided by the lucky circumstances that the taxiing aircraft just passes in front of or behind the taking-off aircraft (case 0 in Table 2.2). From the results in Table 2.2 a number of model-based insights into the operation can be attained:

- It follows from case 1 that 99.8% of the accidents can be prevented by the combined effort of all human operators and alert systems.

- It follows from a comparison of cases 1 and 5 that in the normal situation that all human operators are actively monitoring, ATC alert systems (runway incursion or stopbar violation) have a modest effect on the achieved risk.

- It follows from a comparison of cases 1 and 4, and cases 5 and 8, that the risk reduction that can be achieved by the tower controller in addition to the risk reduction of both pilots is very small.

- It follows from comparison of cases 1 and 3, and cases 5 and 7 that the pilot of the taxiing aircraft has the largest capability to prevent a collision in this context. Thus, resolution of the conflict is most likely to be by the human operator whose wrong situation awareness initiated the conflict.

Table 2.2: Risk reduction achieved in the simulation model by various combinations of involved human operators when the PF of a taxiing aircraft intends to proceed on a normal taxiway under good visibility (crossing is at 1000 m from runway threshold.)

Case	PF taxiing aircraft	PF taking-off aircraft	Runway controller	Conditional collision risk	Risk reduction
0	no	no	no	8.9 10-2	-
ATC alert systems on					
1	yes	yes	yes	1.7 10-4	99.8%
2	yes	no	yes	4.0 10-4	99.6%
3	no	yes	yes	9.4 10-3	89.4%
4	yes	yes	no	2.3 10-4	99.7%
ATC alert systems down					
5	yes	yes	yes	2.2 10-4	99.8%
6	yes	no	yes	1.7 10-3	98.1%
7	no	yes	yes	1.1 10-2	87.9%
8	yes	yes	no	2.3 10-4	99.7%

2.5.3 Comparison against expert based results

In the earlier conducted expert based safety risk assessment of the active runway crossing operation, it was concluded that both the pilots and the runway controller make large contributions to the prevention of a collision in the scenario aircraft erroneously crossing and other aircraft in take-off. In hindsight, it can be concluded that in the expert based safety risk assessment, the total effect of the pilots and the runway controller in preventing a collision turns out to be overestimated under good visibility condition. It is the simulation based approach that makes clear that although the runway controller identifies a good share of the conflicts, its contribution to timely conflict resolution is relatively small. One significant part of the instruction issued by the runway controller appears to concern conflicts that are already solved by the pilots. And another significant part of the instructions issued by the runway controller appear to arrive too late for the pilots to successfully avoid a collision. Because of this, the effective contribution by the runway controller towards reducing collision risk is relatively small.

2.6 Concluding remarks

This chapter has given an overview of performing safety risk assessment and providing feedback to the design of advanced air traffic operations with support of Monte Carlo simulation. The motivation for developing such a Monte Carlo simulation approach towards safety risk assessment was the identified need for modelling stochastic dynamic

events and interactions between multiple agents (humans and systems) in advanced air traffic operations. The distributed and dynamical interactions pose even greater challenges than those seen in, for instance, nuclear and chemical industries (e.g. [72]). The chapter has explained the key issues to be mastered in performing a Monte Carlo simulation supported safety risk assessment of air traffic operations, and how this fits within a full safety risk assessment cycle. The steps to be followed in developing an appropriate Monte Carlo simulation model has been outlined, including a short overview of multi-agent situation awareness modelling, which plays a key role in the safe organization of cooperation between many pilots and controllers in air traffic. The chapter also has explained the need for using stochastic analysis tools in order to develop the necessary speed-up of the Monte Carlo simulations, and has shown a feasible way to validate the simulation model versus the real operation. This assessment approach has been applied to an air traffic example involving aircraft departing from a runway that is occasionally crossed by taxiing aircraft. The results obtained demonstrate the feasibility and value of performing Monte Carlo simulation in accident risk assessment for safety relevant scenarios that are difficult to assess expert based, because of many interacting agents.

3 Free Flight Collision Risk Estimation by Sequential Monte Carlo Simulation

3.1 Introduction

3.1.1 Safety verification of free flight air traffic

Technology allows aircraft to broadcast information about its own-ship position and velocity to surrounding aircraft, and to receive similar information from surrounding aircraft. This development has stimulated the rethinking of the overall concept for today's Air Traffic Management (ATM), e.g., to transfer responsibility for conflict prevention from ground to air. As the aircrews thus obtain the freedom to select their trajectory, this conceptual idea is called free flight [87]. It changes ATM in such a fundamental way, that one could speak of a paradigm shift: centralized control becomes distributed, responsibilities transfer from ground to air, fixed air traffic routes are removed, and appropriate new technologies are brought in. Each aircrew has the responsibility to timely detect and solve conflicts, thereby assisted by navigation means, surveillance processing, and conflict resolution systems. Due to the potentially many aircraft involved, the system is highly distributed. This free flight concept idea has motivated the study of multiple operational concepts and implementation choices [47, 52, 58, 64, 78]. One of the key outstanding issues is the safety verification of free flight design, and in particular when air traffic demand is high.

For en-route traffic, the International Civil Aviation Organization (ICAO) has established thresholds on the acceptable probability of a mid-air collision. Hence, the en-route free flight safety verification problem consists of estimating the collision probability of free flight operations, and subsequently comparing this estimated level with the ICAO established thresholds [48]. The civil aviation community also has established some approximate models to estimate (an upperbound of) the risk of collision between aircraft flying within a given parallel route structure [46, 54, 57]. Additional methods have been exploited to develop some valuable extensions of this approach, e.g., using fault trees see [34] and using stochastic analysis and Monte Carlo simulation [8, 10, 43]. Andrews et al. [2] have shown how statistical data in combination with a fault tree of the functionalities of the advanced operation can serve to predict how reliability of free flight supported systems impact contributions to collision risk of an advanced operation [37], neglecting other contributions to collision risk. The challenge is to analyze the risk of collision between aircraft in free flight without the limitation of a fixed route structure. We aim

to improve this situation by developing a novel approach toward collision risk assessment for advanced air traffic designs. An initial shorter paper on this development is [11].

3.1.2 Probabilistic reachability analysis

In air traffic, a mid-air collision event happens at the moment in time that the physical shapes of two airborne aircraft hit each other. Such event can be represented as a moment in time that the joint state of aircraft involved hit a certain subset of their joint state space. With this, the problem to estimate the probability of collision between two aircraft within a finite time period is to analyze the probability that this collision subset is reached by their joint aircraft state within that time period. In systems theory, the estimation of the probability of reaching a given subset of the state space within a given time period is known as a problem of probabilistic reachability analysis, e.g., see [71].

Hu et al. [55] and Prandini and Hu [82, 83] apply probabilistic reachability analysis for the development of a grid based computation to evaluate the probability that two aircraft come closer to each other than some established minimum separation criteria. The numerical challenge of this problem, however, differs from the free flight collision risk estimation problem on the following aspects:

- The collision subset is more than three orders smaller in volume than the conflict subset is.

- A safety directed model of a free flight operation includes per aircraft also the states of the technical systems and the pilot models, which increases the size of the state space by many orders in magnitude.

- In free flight there are multiple aircraft, not just two, that can trigger domino effects.

If we would follow the numerical approach of Prandini and Hu [83] to estimate collision risk in free flight operations, then these aspects would imply a blow up of the number of grid points to a practically unmanageably large number.

In most safety critical industries, e.g., nuclear, chemical, etc., reachability analysis is addressed by methods that are known as dynamical approaches towards Probabilistic Risk Analysis (PRA). For an overview of these dynamical methods in PRA, see [72]. These dynamical PRA methods make explicitly use of the fact that between two discrete events the dynamical evolution satisfies an ordinary differential equation. Essentially this means that these dynamical PRA methods apply to the class of stochastic hybrid system models that do not involve Brownian motion. In the hybrid systems control community these are known as piecewise deterministic Markov process [18, 29].

For proper safety modeling of air traffic operations, however, it is needed to incorporate Brownian motion in the piecewise deterministic Markov process models, e.g., to represent the effect of random wind disturbances on aircraft trajectories [81]. The class of systems which incorporates Brownian motion within piecewise deterministic Markov processes,

has been defined as a Generalized Stochastic Hybrid System (GSHS) [17]. GSHS is the class of non-linear stochastic continuous-time hybrid dynamical systems, having a hybrid state consisting of two components: a continuous valued state component and a discrete valued state component. The continuous state evolves according to an SDE whose vector field and drift factor depend on both hybrid state components. Switching from one discrete state to another discrete state is governed by a probability law or occurs when the continuous state hits a pre-specified boundary. Whenever a switching occurs, the hybrid state is reset instantly to a new state according to a probability measure which depends itself on the past hybrid state. GSHS contain, as a subclass, the switching diffusion process, the probabilistic reachability of which is studied in [83]. Important complementary dynamics is induced by the interaction between the hybrid state components.

3.1.3 Sequential Monte Carlo simulation

Shah et al. [88] explain very well that the advantage of using Monte Carlo simulation in evaluating advanced operations is its capability to identify and evaluate emergent behavior, i.e., novel behavior which is exhibited by complex safety critical systems and emerges from the combined dynamical actions and reactions by individual systems and humans within the system. This emergent behavior typically cannot be foreseen and evaluated by examining the individuals' behavior alone. Shah et al.[88] explain that agent based Monte Carlo simulation is able to predict the impact of revolutionary changes in air transportation; it integrates cognitive models of technology behavior and description of their operating environment. Simulation of these individual models acting together can predict the results of completely new transformations in procedures and technology. Their Monte Carlo simulations reach up to the level of novel emerging hazardous events. For safety risk assessment however, it is required to go further with the Monte Carlo simulations up to the level of emerging catastrophic events. In en-route air traffic these catastrophic events are mid-air collisions.

A seemingly simple approach toward the estimation of mid-air collision probability is to run many Monte Carlo simulations with a free flight stochastic hybrid model and count the fraction of runs for which a collision occurs. The advantage of a Monte Carlo simulation approach is that this does not require specific assumptions or limitations regarding the behavior of the system under consideration. A key problem is that in order to obtain accurate estimates of rare event probabilities, say about 10^{-9} per flying hour, it is required to simulate 10^{11} flying hours or more. Taking into account that an appropriate free flight model is large, this would require an impractically huge simulation time.

Del Moral and co-workers [23, 25, 31] developed a sequential Monte Carlo simulation approach for estimating small reachability probabilities, including a characterization of convergence behaviour. The idea behind this approach is to express the small probability to be estimated as the product of a certain number of larger probabilities, which can be

efficiently estimated by the Monte Carlo approach. This can be achieved by introducing sets of intermediate states that are visited one set after the other, in an ordered sequence, before reaching the final set of states of interest. The reachability probability of interest is then given by the product of the conditional probabilities of reaching a set of intermediate states given that the previous set of intermediate states has been reached. Each conditional probability is estimated by simulating in parallel several copies of the system, i.e., each copy is considered as a particle following the trajectory generated through the system dynamics. To ensure unbiased estimation, the simulated process must have the strong Markov property. Hence, we extend the approach of [23, 25] for application to free flight, and illustrate its application to free flight scenarios.

3.1.4 Development of Monte Carlo simulation model

For the modeling of accident risk of safety-critical operations in nuclear and chemical industries, the most advanced approaches use Petri nets as model specification formalism, and stochastic analysis and Monte Carlo simulation to evaluate the specified model, e.g., see [72]. Since their introduction as a systematic way to specify large discrete event systems that one meets in computer science, Petri nets have shown their usefulness for many practical applications in different industries, e.g., see [28]. Various Petri net extensions and generalisations and numerous supporting computer tools have been developed, which further increased their modeling opportunities. Nevertheless, literature on Petri nets appeared to fall short for modeling the class of GSHS [17] that was needed to model air traffic safety aspects well [81].

Cassandras and Lafortune [22] provide a control systems introduction to Petri nets and a comparison with other discrete event modeling formalisms like automata. Both Petri nets and automata have their specific advantages. Petri net is more powerful in the development of a model of a complex system, whereas automata are more powerful in supporting analysis. In order to combine the advantages offered by both approaches, there is need for a systematic way of transforming a Petri net model into an automata model. Such a transformation would allow using Petri nets for the specification and automata for the analysis. For a timed or stochastic Petri net with a bounded number of tokens and deterministic or Poisson process firing, such a transformation exists [22]. In order to make the Petri net formalism useful in modeling air traffic operations, we need an extension of the Petri net formalism including a one-to-one transformation to and from GSHS. Everdij and Blom [40, 42] have developed such extension in the form of (Stochastically and) Dynamically Coloured Petri Net, or for short (S)DCPN.

Jensen [59] introduced the idea of attaching to each token in a basic Petri net (i.e., with logic transitions only), a color which assumes values from a finite set. Tokens and the attached colors determine which transitions are enabled. Upon firing by a transition, new tokens and attached colors are produced as a function of the removed tokens and colors. Haas [51] extended this color idea to (stochastically) timed Petri nets where the time period between enabling and firing depends of the input tokens and their attached colors.

In [51, 59] a color does not change as long as the token to which it is attached remains at its place. Everdij and Blom [40, 41] defined a Dyamically Coloured Petri Net (DCPN) by incorporating the following extensions: (1) a color assumes values from a Euclidean state space, its value evolves as solution of a differential equation and influences the time period between enabling and firing; (2) the new tokens and attached colors are produced as random functions of the removed tokens and colors. An SDCPN extends an DCPN in the sense that colors evolve as solutions of a stochastic differential equation [42].

3.2 Sequential Monte Carlo estimation of collision risk

3.2.1 Stochastic hybrid process considered

Throughout this and the following sections, all stochastic processes are defined on a complete stochastic basis $(\Omega, \mathcal{F}, \mathbb{F}, \mathsf{P}, \mathsf{T})$ with $(\Omega, \mathcal{F}, \mathsf{P})$ a complete probability space, and $\mathbb{F}$ an increasing sequence of sub-σ-algebra's on the positive time line $\mathsf{T} = \mathbb{R}_+$, i.e., $\mathbb{F} \triangleq \{\mathcal{J}, (\mathcal{F}_t, t \in \mathsf{T}), \mathcal{F}\}$, $\mathcal{J}$ containing all P-null sets of $\mathcal{F}$ and $\mathcal{J} \subset \mathcal{F}_s \subset \mathcal{F}_t \subset \mathcal{F}$ for every $s < t$.

We assume that air traffic operations are represented by a stochastic hybrid process $\{x_t, \theta_t\}$ which satisfies the strong Markov property. In [17, 19, 68, 69], this property has been shown to hold true for the processes generated as execution of a GSHS. For an N-aircraft free flight traffic scenario the stochastic hybrid process $\{x_t, \theta_t\}$ consists of Euclidean valued components $x_t \triangleq \mathrm{Col}\{x_t^0, x_t^1, \ldots, x_t^N\}$ and discrete valued components $\theta_t \triangleq \mathrm{Col}\{\theta_t^0, \theta_t^1, \ldots, \theta_t^N\}$, where x_t^i assumes values from $\mathbb{R}^{n_i}$, and θ_t^i assumes values from a finite set (M^i). Physically, $\{x_t^i, \theta_t^i\}$, $i = 1, \ldots, N$, is the hybrid state process related to the i-th aircraft, and $\{x_t^0, \theta_t^0\}$ is a hybrid state process of all non-aircraft components. The process $\{x_t, \theta_t\}$ is $\mathbb{R}^n \times M$-valued with $n = \sum_{i=0}^N n_i$ and $M = \bigotimes_{i=0}^N M_i$. In order to model collisions between aircraft, we introduce mappings from the Euclidean valued process $\{x_t\}$ into the relative position and velocity between a pair of two aircraft (i, j). The relative horizontal position is obtained through the mapping $y^{ij}(x_t)$, the relative horizontal velocity is obtained through the mapping $v^{ij}(x_t)$. The relative vertical position is obtained through the mapping $z^{ij}(x_t)$, and relative vertical rate of climb is obtained through the mapping $r^{ij}(x_t)$. The relation between the position and velocity mappings satisfies:

$$
\begin{aligned}
dy^{ij}(x_t) &= v^{ij}(x_t)\,dt & (3.2.1)\\
dz^{ij}(x_t) &= r^{ij}(x_t)\,dt. & (3.2.2)
\end{aligned}
$$

A collision between aircraft (i, j) means that the process $\{y^{ij}(x_t), z^{ij}(x_t)\}$ hits the boundary of an area where the distance between aircraft i and j is smaller than their physical size. Under the assumption that the length of an aircraft equals the width of an aircraft, and that the volume of an aircraft is represented by a cylinder the orientation of which

does not change in time, then aircraft (i, j) have zero separation if $x_t \in D^{ij}$ with:

$$D^{ij} = \left\{ x \in \mathbb{R}^n ; |y^{ij}(x)| \leq (l_i + l_j)/2 \;\; \text{AND} \;\; |z^{ij}(x)| \leq (s_i + s_j)/2 \right\}, \quad i \neq j \quad (3.2.3)$$

where l_j and s_j are length and height of aircraft j. For simplicity we assume that all aircraft have the same size, by which (3.2.3) becomes:

$$D^{ij} = \left\{ x \in \mathbb{R}^n ; |y^{ij}(x)| \leq l \;\; \text{AND} \;\; |z^{ij}(x)| \leq s \right\}, \quad i \neq j \quad (3.2.4)$$

Although all aircraft have the same size, notice that in (3.2.4), D^{ij} still depends of (i, j). If x_t hits D^{ij} at time τ^{ij}, then we say a collision event between aircraft (i, j) occurs at τ^{ij}, i.e.,

$$\tau^{ij} = \inf\{t > 0 \; ; \; x_t \in D^{ij}\}, \quad i \neq j \quad (3.2.5)$$

Next we define the first moment τ^i of collision with any other aircraft, i.e.,

$$\tau^i = \inf_{j \neq i}\{\tau^{ij}\} = \inf_{j \neq i}\{t > 0 \; ; \; x_t \in D^{ij}\} = \inf\{t > 0 \; ; \; x_t \in D^i\}, \quad (3.2.6)$$

with $D^i \triangleq \cup_{j \neq i} D^{ij}$. From this moment τ^i on, we assume that the differential equations for $\{x_t^i, \theta_t^i\}$ stop evolving. An unbiased estimation procedure of the risk would be to simulate many times aircraft i amidst other aircraft over a period of length T and count all cases in which the realization of the moment τ^i is smaller than T. An estimator for the collision risk of aircraft i per unit T of time then is the fraction of simulations for which $\tau^i < T$.

3.2.2 Risk factorization using multiple conflict levels

Cérou et al. [23, 25] developed a novel way of speeding up Monte Carlo simulation to estimate the probability that an $\mathbb{R}^n$-valued strong Markov process x_t hits a given "small" subset $D \in \mathbb{R}^n$ within a given time period $(0, T)$. This method essentially consists of taking advantage of an appropriately nested sequence of closed subsets of $\mathbb{R}^n$: $D = D_m \subset D_{m-1} \subset \ldots \subset D_1$, and then start simulation from outside D_1, and subsequently simulate from D_1 to D_2, from D_2 to D_3, ..., and finally from D_{m-1} to D_m. Krystul and Blom [65, 66] extended this Interacting Particle System (IPS) approach to hybrid state strong Markov processes, and illustrated the effectiveness for a simple example. In order to apply this IPS approach to air traffic we first have to develop an appropriate sequence of nested subsets.

Prior to a collision of aircraft i with aircraft j, a sequence of conflicts ranging from long term to short term always occurs. In order to incorporate this explicitly in the Monte Carlo simulation, we formalize this sequence of conflict levels through a sequence of closed subsets of $\mathbb{R}^n$: $D^{ij} = D_m^{ij} \subset D_{m-1}^{ij} \subset \ldots \subset D_1^{ij}$ with for $k = 1, \ldots, m$:

$$\begin{aligned} D_k^{ij} \;\; = \;\; & \{ x \in \mathbb{R}^n ; |y^{ij}(x) + \Delta v^{ij}(x)| \leq d_k \;\; \text{AND} \\ & |z^{ij}(x) + \Delta r^{ij}(x)| \leq h_k, \;\; \text{for some } \Delta \in [0, \Delta_k] \}, \quad (3.2.7) \end{aligned}$$

for $i \neq j$, with d_k, h_k and Δ_k the parameters of the conflict definition at level k, and with $d_m = l$, $h_m = s$ and $\Delta_m = 0$, and with $d_{k+1} \leq d_k$, $h_{k+1} \leq h_k$ and $\Delta_{k+1} \leq \Delta_k$. If x_t hits D_k^{ij} at time τ_k^{ij}, then we say the first level k conflict event between aircraft (i, j) occurs at moment τ_k^{ij}, i.e.,

$$\tau_k^{ij} = \inf\{t > 0 \ ; \ x_t \in D_k^{ij}\}. \tag{3.2.8}$$

Similarly as we did for reaching the collision level by aircraft i, we consider the first moment τ_k^i that aircraft i reaches conflict level k with any of the other aircraft, i.e.,

$$\tau_k^i = \inf_{j \neq i}\{\tau_k^{ij}\} = \inf_{j \neq i}\{t > 0 \ ; \ x_t \in D_k^{ij}\} = \inf\{t > 0 \ ; \ x_t \in D_k^i\}, \tag{3.2.9}$$

with $D_k^i \triangleq \cup_{j \neq i} D_k^{ij}$.

Next, we define $\{0, 1\}$-valued random variables $\{\chi_k^i, k = 0, 1, \ldots, m\}$ as follows:

$$\begin{aligned} \chi_k^i &= 1, \text{ if } \tau_k^i < T \text{ or } k = 0 \\ &= 0, \text{ else.} \end{aligned}$$

By using this χ_k^i definition we can write the probability of collision of aircraft i with any of the other aircraft as a product of conditional probabilities of reaching the next conflict level given the current conflict level has been reached:

$$\begin{aligned} \mathbb{P}\left(\tau_m^i < T\right) &= \mathbb{E}\left[\chi_m^i\right] = \mathbb{E}\left[\prod_{k=1}^m \chi_k^i\right] = \prod_{k=1}^m \mathbb{E}\left[\chi_k^i \,|\, \chi_{k-1}^i = 1\right] \\ &= \prod_{k=1}^m \mathbb{P}\left(\tau_k^i < T \,|\, \tau_{k-1}^i < T\right) = \prod_{k=1}^m \gamma_k^i, \end{aligned} \tag{3.2.10}$$

with $\gamma_k^i \triangleq \mathbb{P}\left(\tau_k^i < T \,|\, \tau_{k-1}^i < T\right)$.

With this, the problem can be seen as one to estimate the conditional probabilities γ_k^i in such a way that the product of these estimators is unbiased. Because of the multiplication of the various individual γ_k^i estimators, which depend on each other, in general such a product may be heavily biased. The key novelty in [25] was to show that such a product may be evaluated in an unbiased way when $\{x_t\}$ makes part of a larger stochastic process that satisfies the strong Markov property. This approach is explained next.

3.2.3 Characterization of the risk factors

Let us denote $E' = \mathbb{R}^{n+1} \times M$, and let $\mathcal{E}'$ be the Borel σ-algebra of E'. For any $B \in \mathcal{E}'$, $\pi_k^i(B)$ denotes the conditional probability of $\xi_k \triangleq (\tau_k, x_{\tau_k}, \theta_{\tau_k}) \in B$ given $\chi_l^i = 1$ for $1 \leq l \leq k$.

Define $Q_k^i = (0, T) \times D_k^i \times M$, $k = 1, \ldots, m$. Then the estimation of the probability for ξ_k to arrive at the k-th nested Borel set Q_k^i is characterized through the following recursive set of transformations

$$\pi_{k-1}^i(\cdot) \quad \overset{\text{prediction}}{\longrightarrow} \quad p_k^i(\cdot) \quad \overset{\text{conditioning}}{\longrightarrow} \quad \pi_k^i(\cdot)$$

$$\downarrow$$

$$\gamma_k^i$$

where $p_k^i(B)$ is the conditional probability of $\xi_k \in B$ given $\chi_l^i = 1$ for $0 \leq l \leq k - 1$.

Because $\{x_t, \theta_t\}$ is a strong Markov process, $\{\xi_k\}$ is a Markov sequence. Hence the one step prediction of ξ_k satisfies a Chapman-Kolmogorov equation:

$$p_k^i(B) = \int_{E'} p_{\xi_k \mid \xi_{k-1}}(B|\xi) \, \pi_{k-1}^i(d\xi) \text{ for all } B \in \mathcal{E}'. \tag{3.2.11}$$

Next we characterize the conditional probability of reaching the next level

$$\begin{aligned}
\gamma_k^i &= \mathbb{P}\left(\tau_k^i < T \mid \tau_{k-1}^i < T\right) \\
&= \mathbb{E}\left[\chi_k^i \mid \chi_{k-1}^i = 1\right] \\
&= \int_{E'} 1_{\{\xi \in Q_k^i\}} \, p_k^i(d\xi),
\end{aligned} \tag{3.2.12}$$

and the conditioning satisfies:

$$\pi_k^i(B) = \frac{\int_B 1_{\{\xi \in Q_k^i\}} \, p_k^i(d\xi)}{\int_{E'} 1_{\{\xi' \in Q_k^i\}} \, p_k^i(d\xi')} \text{ for all } B \in \mathcal{E}'. \tag{3.2.13}$$

With this, each of the m terms γ_k^i in (3.2.10) is characterized as a solution of a sequence of "filtering" kind of equations (3.2.11)–(3.2.13). However, an important difference with "filtering" equations is that (3.2.11)–(3.2.13) are ordinary integral equations, i.e., they have no stochastic term entering them.

3.2.4 Interacting Particle System based risk estimation

Based on this theory, an Interacting Particle System (IPS) simulation algorithm is explained next for an arbitrary hybrid state strong Markov process model of air traffic. The transformations (3.2.11)–(3.2.13) lead to the IPS algorithm of [25] to estimate $\mathbb{P}(\tau_m^i < T)$, where $\bar{\gamma}_k^i$, $\bar{p}_k^i$ and $\bar{\pi}_k^i$ denote the numerical approximations of γ_k^i, p_k^i and π_k^i respectively. When simulating from D_{k-1}^i to D_k^i, a fraction $\bar{\gamma}_k^i$ of the Monte Carlo simulated trajectories only will reach D_k^i within the time period $(0, T)$.

IPS Step 0. Initial sampling for $k = 0$.

- For $l = 1, \ldots, N_p$ generate initial state value outside Q_1^i by independent drawings (x_0^l, θ_0^l) from $p_{x_0, \theta_0}(\cdot)$ and set $\xi_0^l = (0, x_0^l, \theta_0^l)$.
- For $l = 1, \ldots, N_p$, set the initial weights: $\omega_0^l = 1/N_p$.
- Then $\bar{\pi}_0^i = \sum_{l=1}^{N_p} \omega_0^l \, \delta_{\{\xi_0^l\}}$.

IPS Iteration cycle: For $k = 1, \ldots, m$ perform step 1 (prediction), step 2 (assess fraction), step 3 (conditioning), and step 4 (resampling).

IPS Step 1. Prediction of $\pi_{k-1}^i \longrightarrow p_k^i$, based on (3.2.11);

- For $l = 1, \ldots, N_p$ simulate a new path of the hybrid state Markov process, starting at ξ_{k-1}^l until the k-th set Q_k^i is hit or $t = T$ (the first component of ξ_k^l counts time).
- This yields new particles $\{\hat{\xi}_k^l, \omega_{k-1}^l\}_{l=1}^{N_p}$.
- $\bar{p}_k^i$ is the empirical distribution associated with the new cloud of particles: $\bar{p}_k^i = \sum_{l=1}^{N_p} \omega_{k-1}^l \delta_{\hat{\xi}_k^l}$.

IPS Step 2. Assess fraction γ_k^i, based on (3.2.12);

- The particles that do not reach the set Q_k^i are killed, i.e., we set $\hat{\omega}_k^l = 0$ if $\hat{\xi}_k^l \notin Q_k^i$ and $\hat{\omega}_k^l = \omega_{k-1}^l$ if $\hat{\xi}_k^l \in Q_k^i$.
- Approximation: $\gamma_k^i \approx \bar{\gamma}_k^i = \sum_{l=1}^{N_p} \hat{\omega}_k^l$. If all particles are killed, i.e., $\bar{\gamma}_k^i = 0$, then the algorithm stops without $\mathbb{P}(\tau^i < T)$ estimate.

IPS Step 3. Conditioning of $p_k^i \longrightarrow \pi_k^i$, based on (3.2.13);

The non-killed particles form a set S_k^i, i.e., iff $\hat{\xi}_k^l \in Q_k^i$, then particle $\{\hat{\xi}_k^l, \hat{\omega}_k^l\}$ is stored in S_k^i.

Renumbering the particles in S_k^i yields a set of particles $\{\tilde{\xi}_k^l, \tilde{\omega}_k^l\}_{l=1}^{N_{S_k}}$ with N_{S_k} the number of particles in S_k^i. Hence, we also have $\bar{\gamma}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l$.

IPS Step 4. Resampling of π_k^i

Draw N_p particles ξ_k^l independently from the empirical measure $\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \, \delta_{\{\tilde{\xi}_k^l\}}$ each of which gets weight $\omega_k^l = \frac{1}{N_p}$.

After step 4, the new set of particles is $\{\xi_k^l, \omega_k^l\}_{l=1}^{N_p}$. If $k < m$ then repeat steps 1, 2, 3, 4 for $k := k + 1$. Otherwise, stop with $\mathbb{P}(\tau^i < T) \approx \prod_{k=1}^m \bar{\gamma}_k^i$.

Remark 3.2.1 *Cérou et al. [23, 25] have proven, under certain conditions, how to manage the simulations from D_{k-1}^i to D_k^i, such that the product of these fractions $\bar{\gamma}_k^i$ forms an unbiased estimate of the probability of x_t to hit the set D^i within the time period $(0, T)$, i.e.,*

$$\mathbb{E}\left[\prod_{k=1}^m \bar{\gamma}_k^i\right] = \prod_{k=1}^m \gamma_k^i = \mathbb{P}(\tau^i < T),$$

and there also is some bound on the expected estimation error, i.e.,

$$\left(\mathbb{E}(\prod_{k=1}^{m} \bar{\gamma}_k^{\,i} - \prod_{k=1}^{m} \gamma_k^{\,i})^q \right)^{\frac{1}{q}} \leq \frac{a_q \, b_q}{\sqrt{N_p}},$$

for some finite constants a_q and b_q, which depend on the simulated scenario and the sequence of intermediate levels adopted.

3.2.5 Modification of IPS resampling step 4

A well known problem with particle systems is the possibility of particle depletion or impoverishment. In order to reduce the sensitivity of the above algorithm on these points, we modify step 4 in two ways: (1) we reduce the chance of impoverishment by not throwing away any particle; and (2) we make copies of particles, but avoid that these copies take away too much weight from the original particles.

Modified IPS Step 4

Resample N_p particles from S_k^i as follows:

If $\frac{1}{2}N_p \leq N_{S_k} \leq N_p$, then copy the N_{S_k} particles, i.e., $\xi_k^l = \tilde{\xi}_k^l$ and set $\omega_k^l = \tilde{\omega}_k^l \dfrac{N_{S_k}}{\bar{\gamma}_k^{\,i} \, N_p}$ for $l = 1, \ldots, N_{S_k}$; the total weight of these particles is $\frac{N_{S_k}}{N_p}$. Subsequently, draw $N_p - N_{S_k}$ particles ξ_k^l independently from the empirical measure $\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \, \delta_{\{\tilde{\xi}_k^l\}}$ and set $\omega_k^l = \dfrac{\sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l}{\bar{\gamma}_k^{\,i} \, N_p} = \dfrac{1}{N_p}$; the total weight of this is $1 - \frac{N_{S_k}}{N_p}$.

Else, i.e., if $N_{S_k} < \frac{1}{2}N_p$, then copy the N_{S_k} particles, i.e., $\xi_k^l = \tilde{\xi}_k^l$, and set $\omega_k^l = \frac{1}{2}\tilde{\omega}_k^l / \bar{\gamma}_k^{\,i}$ for $l = 1, \ldots, N_{S_k}$; the total weight of these particles is $\frac{1}{2}$. For the remaining weight of $\frac{1}{2}$, we independently draw $N_p - N_{S_k}$ particles ξ_k^l from the empirical measure $\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \, \delta_{\{\xi_k^l\}}$ and set $\omega_k^l = \dfrac{\frac{1}{2} \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l}{\bar{\gamma}_k^{\,i} \, (N_p - N_{S_k})} = \dfrac{\frac{1}{2}}{N_p - N_{S_k}}$.

3.3 Development of a Petri net model of free flight

In order to apply the IPS algorithm toward the assessment of collision risk of free flight, we need to develop a Monte Carlo simulator of these operations such that the simulated trajectories constitute realizations of a hybrid state strong Markov process. Everdij

and Blom [40, 42] have developed a Stochastically and Dynamically Coloured Petri Net (SDCPN) formalism that ensures the specification of a free flight Monte Carlo simulation model which is of the appropriate class. This section explains how the SDCPN formalism has been used to develop a Monte Carlo simulation model of a particular free flight design.

The specific free flight design for which we wish to estimate the collision risk by sequential Monte Carlo simulation is the Autonomous Mediterranean Free Flight (AMFF) operation [79]. AMFF has been developed to study the introduction of autonomous free flight operation in Mediterranean airspace. In parallel to the current study, the safety of the AMFF operation has been addressed in [77], following a fault tree analysis approach. These results show that application of AMFF seems feasible to accommodate low en-route traffic conditions over the Mediterranean. However, this study also concludes that the fault tree approach has limited analysis capabilities in showing whether AMFF can safely accommodate a higher traffic density. For this, a need was identified to use a more advanced safety risk assessment approach that considers complex situations involving dynamic interactions between multiple human and systems. The current study addresses this for AMFF under relatively high traffic densities.

For the development of a Petri net model of the AMFF operation, two key challenges have to be addressed: a syntactical challenge of developing a model that is consistent, complete, and unambiguous; and a semantics challenge of representing the AMFF operation sufficiently well. This section shows how the SDCPN formalism has been used to address the syntactical challenge. Addressing the semantics challenge falls outside the scope of this study.

3.3.1 Specification of Petri net model

In using the (S)DCPN formalism [40, 41, 42] in modeling more and more complex multi-agent hybrid systems, it was found that the compositional specification power of Petri nets reaches its limitations. More specifically, the following problems were identified:

1. For the modeling of a complete Petri net for complex systems, a hierarchical approach is necessary in order to be able to separate local modeling issues from global or interaction modeling issues.

2. Often the addition of an interconnection between two low-level Petri nets leads to a duplication of transitions and arcs in the receiving Petri net.

3. The number of interconnections between the different low level Petri nets tends to grow quadratically with the size of the Petri net.

Everdij et al. [45] explained which Petri net model specification approaches from literature solve problem 1, and developed novel approaches to solve problems 2 and 3. Together, these approaches are integrated into a compositional specification approach for SDCPN, which is explained below.

In order to avoid problem 1, the compositional specification of an SDCPN for a complex process or operation starts with developing a Local Petri Net (LPN) for each agent

that exists in the process or operation (e.g., air traffic controller, pilot, navigation and surveillance equipment). Essential is that these LPNs are allowed to be connected with other Petri net parts in such a way that the number of tokens residing in an LPN is not influenced by these interconnections. We use two types of interconnections between nodes and arcs in different LPNs:

- Enabling arc (or inhibitor arc) from one place in one LPN to one transition in another LPN. These types of arcs have been used widely in Petri net literature.
- Interaction Petri Net (IPN) from one (or more) transition(s) in one LPN to one (or more) transition(s) in another LPN.

In order to avoid problems 2 and 3, high level interconnection arcs have been introduced that allow, with well-defined meanings, arcs to initiate and/or to end on the edge of the box surrounding an LPN [45]. The meaning of these interconnections from or to an edge of a box allows several arcs or transitions to be represented by only one arc or transition.

3.3.2 High level interconnection arcs

As an illustration of how high level interconnection arcs avoid duplication of arcs and transitions within an LPN and duplication of arcs between LPNs, we give three examples of these high level interconnection arcs. See [45] for a complete overview of these high level interconnection arcs.

In the first example, Figure 3.1, an enabling arc starts on the edge of an LPN box and ends on a transition in another LPN box, means that enabling arcs initiate from all places in the first LPN and end on duplications of this transition in the second LPN. The duplicated transitions should have the same guard or delay function and the same firing function and their input places should have the same color type. This high level interconnection arc is not defined for inhibitor or ordinary arcs instead of enabling arcs.
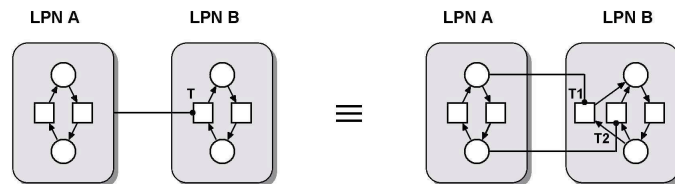
Figure 3.1: High level enabling arc starts at the edge of an LPN box.

In the second example, Figure 3.2, an enabling arc ends on the edge of an LPN box.[1] This means that for each transition in the receiving LPN a copy of this enabling arc should be in place. Figure 3.2 shows an example of this high level interconnection arc. This type of high level arc can also be used with inhibitor arcs instead of enabling arcs.

---

[1] Figures 3.2, 3.3, 3.4, and 3.5 are from [7], with can kind permission of Springer Science and Business Media.

It cannot be used with ordinary arcs, due to the restriction that the number of tokens in an LPN should remain the same.

In the third example, Figure 3.3, an ordinary arc starts on the edge of an LPN box and ends on a transition inside the same box. This means that ordinary arcs start from all places in the LPN box to duplications of this transition. The duplicated transitions should have the same guard or delay function and the same firing function and their set of input places should have the same set of color types. Figure 3.3 illustrates how this avoids both the duplication of transitions and arcs within an LPN, and the duplication of arcs between LPNs.
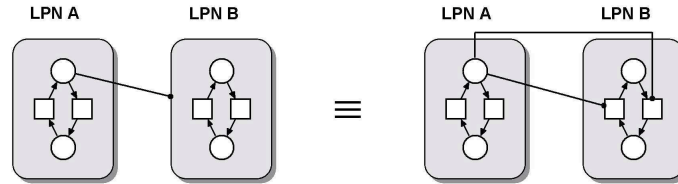
Figure 3.2: High level enabling arc ends at the edge of an LPN box.
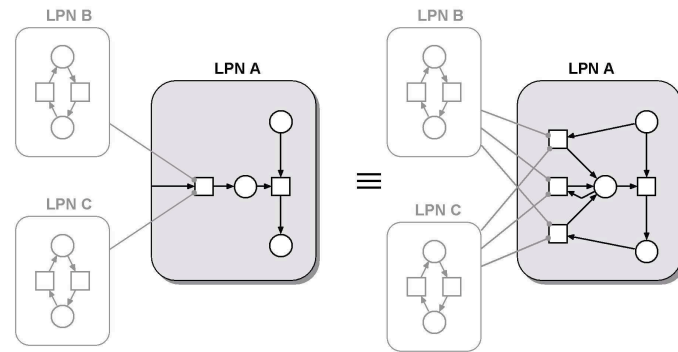
Figure 3.3: High level ordinary arc starts on the edge of an LPN box and ends on a transition inside the same LPN box.

3.3.3 Agents and LPNs to represent AMFF operations

In the Petri net modeling of AMFF operations for the purpose of an initial collision risk assessment, the following agents are taken into account:

- Aircraft
- Pilot-Flying (PF)
- Pilot-Not-Flying (PNF)
- Airborne Guidance, Navigation and Control (AGNC)
- Airborne Separation Assistance System (ASAS)

- Communication, Navigation and Surveillance (CNS)

It should be noticed that our initial model representing AMFF operations, does not yet incorporate other relevant agents such as Airborne Collision Avoidance System (ACAS), Airline Operations Centre (AOC), Air Traffic Control (ATC), or an environmental model. This should be taken into account when interpreting the simulation results obtained with this initial model.

Per agent, particular LPNs and IPNs have been developed and subsequently the interactions between these LPNs and IPNs have been specified. A listing of LPNs per agent reads as follows:

- Aircraft LPNs:

  - Type
  - Evolution mode
  - Systems mode
  - Emergency mode

- Pilot-Flying (PF) LPNs:

  - State situation awareness
  - Intent situation awareness
  - Goal memory
  - Current goal
  - Task performance
  - Cognitive mode

- Pilot-Not-Flying (PNF) LPNs:

  - Current goal
  - Task performance

- Airborne Separation Assistance System (ASAS) LPNs:

  - Processing
  - Alerting
  - Audio alerting
  - Surveillance
  - System mode
  - Priority switch mode
  - Anti-priority switch mode
  - Predictive alerting (of other aircraft)

- Airborne Guidance, Navigation and Control (AGNC) LPNs:

  - Indicators failure mode for PF

- Engine failure mode for PF
- Navigation failure indicator for PF
- ASAS failure indicator for PF
- Automatic Dependent Surveillance-Broadcast (ADS-B) receiver failure indicator for PF
- ADS-B transmitter failure indicator for PF
- Indicator failure mode for PNF
- Guidance mode
- Horizontal guidance configuration mode
- Vertical guidance configuration mode
- Flight Management System (FMS) flightplan
- Airborne Global Positioning System (GPS) receiver
- Airborne Inertial Reference System (IRS)
- Altimeter
- Horizontal position processing
- Vertical position processing
- ADS-B transmission
- ADS-B receiver

- Communication, Navigation and Surveillance (CNS) LPNs:

  - Global GPS / satellites
  - Global ADS-B ether frequency
  - Secondary Surveillance Radar (SSR) mode-S frequency

The actual number of LPNs in the whole model then equals $38N + 3$, where N is the number of aircraft. In addition there are 35 IPNs per aircraft; hence the number of IPNs equals $35N$. Brownian motion enters in each of the aircraft evolution mode LNPs. In this initial model these Brownian motions are assumed to be independent.

3.3.4 Interconnected LPNs of ASAS

The approach taken in developing the AMFF concept of operation [79] is to avoid much information exchange between aircraft and to avoid dedicated decision-making by artificial intelligent machines. Although the conflict detection and resolution approach developed for AMFF has its roots in the modified potential field approach [52], it has some significant deviations from this. The main deviation is that conflict resolution in AMFF is intentionally designed not to take the potential field of all aircraft into account. The resulting AMFF design can be summarized as follows:

- All aircraft are supposed to be equipped with Automatic Dependent Surveillance-Broadcast (ADS-B), which is a system that periodically broadcasts own aircraft state information, and continuously receives the state information messages broadcasted by aircraft that fly within broadcasting range (~ 100 Nm).

- To comply with pilot preferences, conflict resolution algorithms are designed to solve multiple conflicts one by one rather than according to a full concurrent way, e.g., see [52].

- Conflict detection and resolution are state-based, i.e., intent information, such as information at which point surrounding aircraft will change course or height, is supposed to be unknown.

- The vertical separation minimum is 1000 ft and the horizontal separation minimum is 5 Nm. A conflict is detected if these separation minima will be violated within 6 minutes.

- The conflict resolution process consists of two phases. During the first phase, one of the aircraft crews should make a resolution maneuver. If this does not work, then during the second phase, both crews should make a resolution maneuver.

- Prior to the first phase, the crew is warned when an ASAS alert is expected to occur if no preventive action would be timely implemented; this prediction is done by a system referred to as P-ASAS (Predictive ASAS).

- Conflict co-ordination does not take place explicitly, i.e., there is no communication on when and how a resolution maneuver will be executed.

- All aircraft are supposed to use the same resolution algorithm, and all crew are assumed to use ASAS and to collaborate in line with the procedures.

- Two conflict resolution maneuver options are presented: one in vertical and one in horizontal direction. The pilot decides which option to execute.

- ASAS related information is presented to the crew through a Cockpit Display of Traffic Information (CDTI).

ASAS is modeled through the SDCPN depicted in Figure 3.4. The ADS-B information received from other aircraft is processed by the *LPN ASAS surveillance*. Together with the information about its own aircraft state information (from AGNC), the *LPN ASAS processing* uses this information to perform conflict detection and resolution functionalities. Subsequently, the *LPN ASAS alerting* and the *LPN P-ASAS processing* informs the PF and PNF through *ASAS audio alerting* about any aircraft that is in potential ASAS conflict with its own aircraft, and suggests resolution options including a prioritization. Three complementary LPNs represent non-nominal behavior modes, each combination of which has a specific influence on the ASAS alerting LPN:

- *ASAS system mode* may be working, failed, or corrupted (failed or corrupted mode also influences the ASAS processing LPN).

- *ASAS priority switching mode*; under emergency, the PF switches this from "off" to "on."

- *ASAS anti-priority switch*; this is switched from "off" to "on" when own ADS-B is not working.
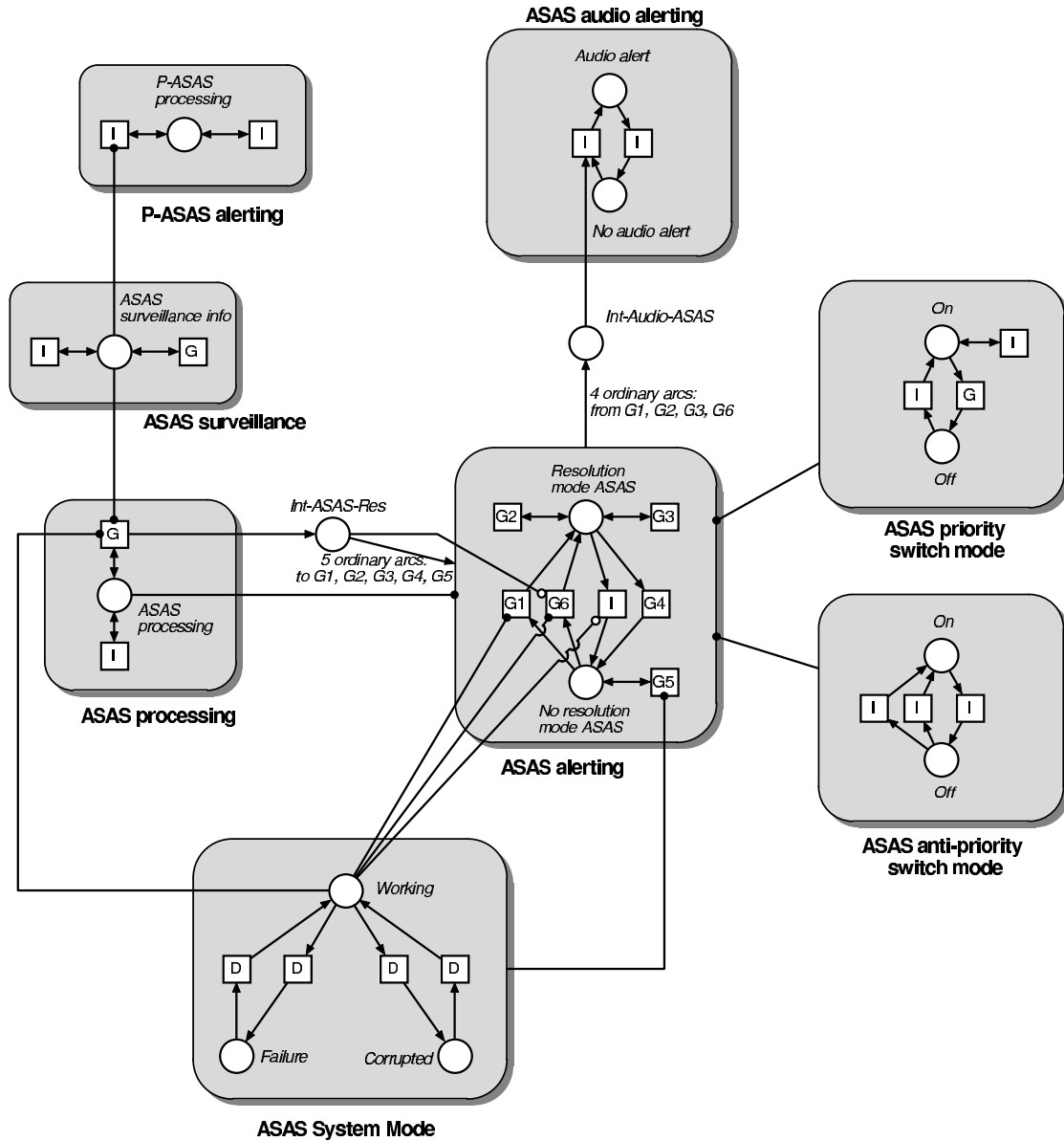
Figure 3.4: The agent ASAS in AMFF is modelled by eight LPNs, a number of ordinary and enabling arcs, and two IPNs (with one place each).

3.3.5 Interconnected LPNs of "Pilot Flying"

This subsection illustrates the specific Petri net model developed for the Pilot Flying. For the semantical basis behind this type of model, see [12, 13, 16, 27, 90]. A graphical representation of all LPNs the Pilot-Flying consists of, is given in Figure 3.5.
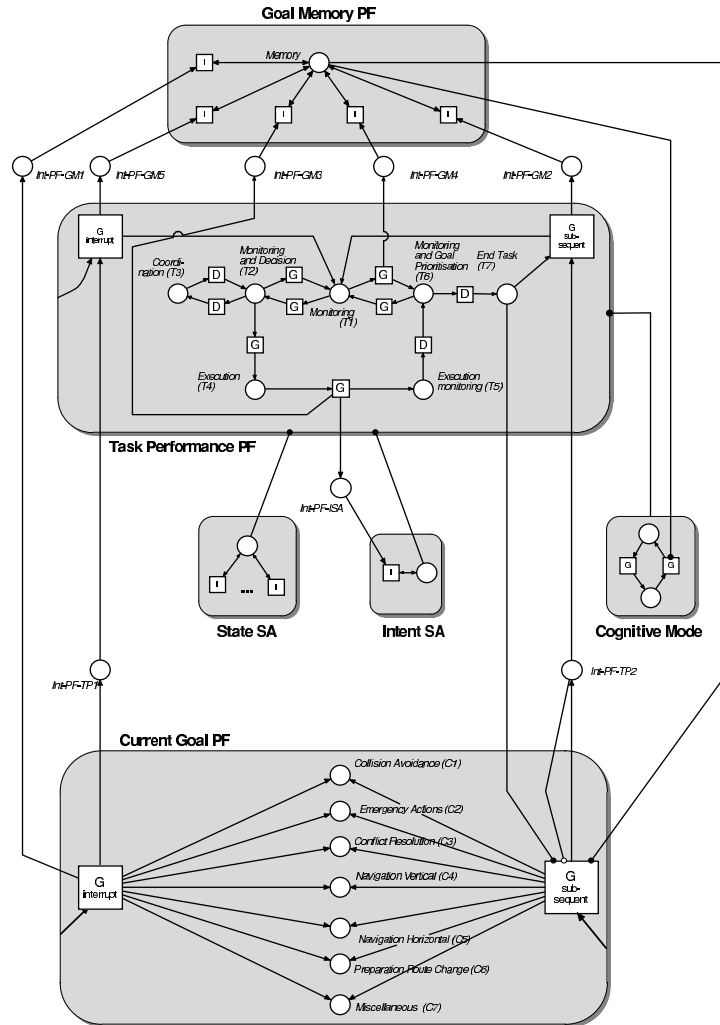
Figure 3.5: The agent Pilot-Flying in AMFF is modelled by six LPNs, and a number of ordinary and enabling arcs and some IPNs, consisting of one place and input and output arcs. The interconnections with other agents are not shown.

The Human-Machine-Interface where sound or visual clues might indicate that attention should be paid to a particular issue, is represented by a LPN that does not belong to the Pilot-Flying as agent and is therefore not depicted in the figure. Similarly, the arcs to or from any other agent are not shown in Figure 3.5. Because of the very nature of Petri nets, these arcs can easily be added during the follow-up specification cycle. To get an understanding of the different LPNs, a good starting point might be the LPN "Current Goal" (at the bottom of the figure) as it represents the objective the Pilot-Flying is currently working on. Examples of such goals are "Collision Avoidance," "Conflict Resolution," and "Horizontal Navigation." For each of these goals, the pilot executes a number of tasks in a prescribed or conditional order, represented in the LPN "Task

Performance." Examples of such tasks are "Monitoring and Decision," "Execution," and "Execution Monitoring." If all relevant tasks for the current goal are considered executed, the pilot chooses another goal, thereby using his memory (where goals deserving attention might be stored, represented by the LPN "Goal Memory") and the Human-Machine-Interface. His memory where goals deserving attention might be stored is represented as the LPN "Goal Memory" in Figure 3.5.

So, the LPNs "Current Goal," "Task Performance," and "Goal Memory" are important in the modeling of which task the Pilot-Flying is executing. The other three LPNs are important in the modeling on how the Pilot-Flying is executing the tasks. The LPN "State SA", where SA stands for Situation Awareness, represents the relevant perception of the pilot about the states of elements in his environment, e.g., whether he is aware of an engine failure. The LPN "Intent SA" represents the intent, e.g., whether he intends to leave the free flight airspace. The LPN "Cognitive mode" represents whether the pilot is in an opportunistic mode, leading to a high but error-prone throughput, or in a tactical mode, leading to a moderate throughput with a low error probability.

3.3.6 Verification, parameterization, and validation of simulation model

The compositionally specified SDCPN model enables a systematic implementation, verification and validation of the resulting Monte Carlo simulator. This is done through the following systematic steps:

- Software code testing. This is done through conducting the following sequence of testing: random number generation, statistical distributions, common functions, each LPN implementation, each agent implementation, interactions between all agents, full Monte Carlo simulation.

- Numerical approximation testing. This is needed to learn choosing an appropriate numerical integration step size and an appropriate number of particular Monte Carlo simulations.

- Graphical user interface testing. This is to verify that the input and output of data works well.

- Parameterization. This is done through a search for literature and statistical sources, and complemented by expert interviews. The fusion of these different pieces of information is accomplished following a Bayesian approach.

- Initial model validation through studying Monte Carlo simulator behavior and sensitivities to parameter changes under dedicated scenarios.

- Overall validation, which is directed to the evaluation of differences between model and reality and what effect these differences have at the assessed risk level.

The last validation step typically is done at a later stage in the risk assessment process, with the help of active participation of operational experts [38, 44].

Table 3.1: Dimensional analysis of agent PF.

Pilot-Flying (PF) LPNs and IPNs	Number of places	Maximum color state space
Pilot Flying (PF) LPNs:		
State Situation Awareness	1	$\mathbb{R}^3$
Intent Situation Awareness	1	$\mathbb{R}^5$
Goal memory	1	$\mathbb{R}$
Current goal	7	$\mathbb{R}$
Task performance	7	$\mathbb{R}^2$
Cognitive mode	2	$\mathbb{R}$
Pilot Flying (PF) internal IPNs:		
Int-PF-GM1	1	$\mathbb{R}$
Int-PF-GM2	1	$\mathbb{R}$
Int-PF-GM3	1	$\mathbb{R}$
Int-PF-GM4	1	$\mathbb{R}$
Int-PF-GM5	1	$\mathbb{R}$
Int-PF-TP1	1	$\mathbb{R}^2$
Int-PF-TP2	1	$\mathbb{R}$
Int-PF-ISA	1	$\mathbb{R}$
Pilot Flying (PF) external IPNs:		
Ext-PF-Audio-PF	5	
Ext-PF-PNF	1	$\mathbb{R}$
Ext-PF-PASAS	1	$\emptyset$
Ext-PF-SSA-1	1	$\emptyset$
Ext-PF-SSA-2	1	$\mathbb{R}$
Ext-PF-SSA-3	1	$\mathbb{R}$
Ext-PF-SSA-4	1	$\mathbb{R}$
Ext-PF-SSA-5	1	$\mathbb{R}$
PRODUCT	490	$\mathbb{R}^{28}$

3.3.7 Dimensions of Monte Carlo simulation model

Now, we analyze the dimensions of the joint state space of the resulting Monte Carlo simulation model. In Table 3.1 and Table 3.2, this is done for the agents PF and ASAS respectively, including all LPNs and all IPNs that end on one of these LPNs. The second column gives the number of places in the LPN or IPN. The third column gives the maximum state space of the color used within an LPN or IPN. We also perform this analysis to the LPNs and IPNs of the other agents. The resulting number of product places and product state spaces is given in Table 3.3. This table brings into account that of each agent, except global CNS, there is one per aircraft.

Table 3.2: Dimensional analysis of agent ASAS.

ASAS LPNs and IPNs	Number of places	Maximum color state space
ASAS LPNs:		
Processing	1	$\mathbb{R}^{13+12N}$
Alerting	2	$\mathbb{R}^7$
Audio alerting	2	$\emptyset$
Surveillance	1	$\mathbb{R}^{11+9N}$
System mode	3	$\emptyset$
Priority switch mode	2	$\emptyset$
Anti-priority switch mode	2	$\emptyset$
Predictive alerting	1	$\mathbb{R}^3$
ASAS internal IPNs:		
Int-ASAS-Resolution	1	$\emptyset$
Int-ASAS-Audio	1	$\emptyset$
ASAS external IPNs:		
Ext-ASAS-PF	1	$\mathbb{R}^3$
Ext-PASAS-PNF	1	$\emptyset$
Ext-ASASProc-PNF	1	$\emptyset$
Ext-ASASurv-ADSB-Global	1	$\mathbb{R}$
Ext-ASASprio-PNF PRODUCT	1	$\emptyset$
PRODUCT	48	$\mathbb{R}^{38+21N}$

The product places of the global CNS agent form the θ_t^0 state space M^0. The corresponding state space is empty, which means that there is no x_t^0. The product places of the other agents form the state space $\bigotimes_{i=1}^N M^i$ of the proces components θ_t^i, $i = 1, \ldots, N$. Per aircraft, the number of product places is $|M^i| \approx 0.777 \times 10^{12}$. The colors attached to the places in the other agents form the process components x_t^i, $i = 1, \ldots, N$, each of which assumes values in $\mathbb{R}^{126+21N}$.

Each of the scenarios considered in the next subsection has eight aircraft, so $N = 8$. This means that the number of product places equals $\approx 16 \times (0.777 \times 10^{12})^8 \approx 2.13 \times 10^{96}$, and that the product of the color state spaces equals $\mathbb{R}^{2352}$.

3.4 Simulated scenarios and collision risk estimates

The IPS algorithm of Section 3.2 is now applied to three hypothetical AMFF air traffic scenarios. The first scenario has eight aircraft that fly at the same flight level and their flight plans cause them to fly through the same point in airspace at the same moment in time. The second scenario has one aircraft flying through a virtual infinite airspace

Table 3.3: Dimensional analysis of complete SDCPN.

Agent	Number of product places	Maximum color product state space
Aircraft	24^N	$\mathbb{R}^{13N}$
Pilot Flying (PF)	490^N	$\mathbb{R}^{28N}$
Pilot-not-Flying (PNF)	7^N	$\mathbb{R}^{3N}$
AGNC	$(15 \times 2^{16})^N$	$\mathbb{R}^{45N}$
ASAS	48^N	$\mathbb{R}^{37N+21N^2}$
Global CNS	16	$\emptyset$
PRODUCT	$\approx 16 \times (0.777 \times 10^{12})^N$	$\mathbb{R}^{126N+21N^2}$

of randomly distributed aircraft, with a density 3 times as high as in a current high capacity en route area. The third scenario is the same as the second, except that the aircraft density is four times lower. Prior to describing these scenarios and simulation results, we explain the parametrization of the IPS algorithm used.

Table 3.4: Parameter values of free flight enabling technical systems.

Model Parameter	Probability
Global GPS down	1.0×10^{-5}
Global ADS-B down	1.0×10^{-6}
Aircraft ADS-B receiver down	5.0×10^{-5}
Aircraft ADS-B transmitter down	5.0×10^{-5}
Aircraft ASAS system mode corrupted	5.0×10^{-5}
Aircraft ASAS system mode failure	5.0×10^{-5}

3.4.1 Parameterization of the IPS simulations

The main safety critical parameter settings of the free flight enabling technical systems (GPS, ADS-B and ASAS) are given in Table 3.4; in the table, global ADS-B down refers to frequency congestion/overload of the data transfer technology used for ADS-B. The IPS conflict levels k are defined by parameter values for lateral conflict distance d_k, conflict height h_k, and time to conflict Δ_k. These values have been determined through two steps. The first was to let an operational expert make a best guess of proper parameter values. Next, during initial simulations with the IPS some fine tuning of the number of levels and of parameter values per level has been done. The resulting values are given in Table 3.5.

Table 3.5: IPS conflict level parameter values.

k	1	2	3	4	5	6	7	8
d_k (Nm)	4.5	4.5	4.5	4.5	2.5	1.25	0.5	0.054
h_k (ft)	900	900	900	900	900	500	250	131
Δ_k (min)	8	2.5	1.5	0	0	0	0	0

3.4.2 Eight aircraft on collision course

In this simulation eight aircraft start at the same flight level, some 135 Nm (250 km) out of each other, and fly in eight 45 degrees differing directions with a ground speed of 466 knots (= 240 m/s), all aiming to pass through the same point in airspace. By running ten times the IPS algorithm the collision risk is estimated ten times. The number of particles per IPS simulation run is 12,000. The total simulation time took about 20 hours on two machines, and the load of computer memory per machine was about 2.0 gigabyte. For the first eight IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table 3.6 for each of the conflict levels, $k = 1, \ldots, 8$, and aircraft $i = 1$. It can be seen that the first and sixth IPS runs have zero particles that reach the last (8th level). Hence the first and sixth IPS runs yield $\bar{\gamma}_8^i = 0$. This is a clear example of particle depletion.

The IPS estimated mean probability for one aircraft to collide with any of the other seven aircraft equals 2.2×10^{-5}. The minimum and maximum values now are respectively a factor 250 lower and a factor 4 higher than the mean value. We also verified that this risk value was not sensitive at all to the failure rates of the ASAS related technical systems.

In [52] a similar eight aircraft encounter scenario has been simulated some thousand times, without experiencing any collision event. At a collision probability value of 2.2×10^{-5}, the chance to count at least one collision would be in the order of 5 %. As such the current results agree quite well with the fact that in these earlier simulations for the eight aircraft scenario no collision has been observed. We also verified that the novel simulation results for the eight aircraft scenario agreed quite well with the expectation of the designers of the AMFF operational concept.

3.4.3 Free flight through an artificially constructed airspace

In this simulation the complete airspace is divided into packed containers. Within each container a fixed number of seven aircraft ($i = 2, \ldots, 8$) fly at arbitrary position and in arbitrary direction at a ground speed of 466 Nm/hr. One additional aircraft ($i = 1$) aims to fly straight through a sequence of connected containers, at the same speed, and the aim is to estimate its probability of collision with any of the other aircraft per unit time of flying.

Per container, the aircraft within it behave the same. This means that we have to simulate each aircraft in one container only, as long as we apply the ASAS conflict prediction

Table 3.6: Fractions counted during eight IPS runs of scenario 1.

Level	1st IPS	2nd IPS	3rd IPS	4th IPS	5th IPS	6th IPS	7th IPS	8th IPS
1	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
2	0.528	0.529	0.539	0.533	0.537	0.538	0.536	0.539
3	0.426	0.429	0.424	0.431	0.421	0.428	0.426	0.418
4	0.033	0.036	0.035	0.037	0.039	0.031	0.044	0.039
5	0.175	0.180	0.183	0.181	0.142	0.157	0.181	0.147
6	0.267	0.158	0.177	0.144	0.255	0.138	0.295	0.146
7	0.150	0.268	0.281	0.427	0.645	0.208	0.253	0.295
8	0.000	0.009	0.233	0.043	0.455	0.000	0.006	0.815
Product of fractions	0.0	5.58×10^{-7}	1.67×10^{-5}	4.01×10^{-6}	9.33×10^{-5}	0.0	8.00×10^{-7}	4.48×10^{-5}

and resolution also to aircraft copies in the neighboring containers. In principle this can mean that an aircraft experiences a conflict with its own copy in a neighboring container. This also means that the size of a container should not go below a certain minimum size.

By changing container size we can vary traffic density. To choose the appropriate traffic density, our reference point is the highest number (17) of aircraft counted at 23rd July 1999 in an en-route area near Frankfurt of size 1 degree × 1 degree × FL290-FL420. This comes down to 0.0032 a/c per Nm^3. For our simulation we assume a 3 times higher traffic density, i.e., 0.01 a/c per Nm^3. This resulted in choosing containers having a length of 40 Nm, a width of 40 Nm, and a height of 3000 feet and with 8 aircraft flying in such a container.

By running the IPS algorithm ten times (+ one extra later on) over 25 minutes (5 minutes to allow convergence and 20 minutes to estimate collision probability) the collision probability per unit time of flying has been estimated. The number of particles per IPS simulation run is 10,000. The total simulation time took about 300 hours on two machines, and the load of computer memory per machine was about 2.0 gigabyte. For the first eight IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table 3.7 for each of the conflict levels, $k = 1, \ldots, 8$, for aircraft $i = 1$.

The estimated mean probability of collisions per 20 minutes of aircraft flight equals 5.22×10^{-5}, which is equal to a probability of collisions per aircraft flight hour of 1.6×10^{-4}, with minimum and maximum values respectively a factor four lower and higher. We also verified that this risk value was not sensitive at all to the failure rates of the ASAS related technical systems.

One should be aware that this value has been estimated for the simulation model of the intended AMFF operation. Hence the question is what this means for the intended AMFF operation itself? By definition a simulation model of AMFF differs from the intended AMFF operation. If it can be shown that the combined effect of these differences on the risk level is small, then the results obtained for the simulation model may be

Table 3.7: Fractions counted during eight IPS runs of scenario 2.

Level	1st IPS	2nd IPS	3rd IPS	4th IPS	5th IPS	6th IPS	7th IPS	8th IPS
1	0.922	0.917	0.929	0.926	0.925	0.925	0.925	0.921
2	0.567	0.551	0.560	0.559	0.554	0.551	0.561	0.556
3	0.665	0.666	0.674	0.676	0.672	0.673	0.664	0.670
4	0.319	0.331	0.323	0.321	0.328	0.321	0.334	0.331
5	0.370	0.367	0.371	0.379	0.363	0.345	0.366	0.343
6	0.181	0.158	0.162	0.171	0.164	0.181	0.148	0.191
7	0.130	0.209	0.174	0.145	0.162	0.170	0.214	0.215
8	0.067	0.005	0.094	0.066	0.002	0.150	0.015	0.019
Product of fractions	6.42×10^{-5}	6.76×10^{-6}	1.11×10^{-4}	6.99×10^{-5}	2.57×10^{-6}	1.75×10^{-4}	1.99×10^{-5}	2.98×10^{-5}

considered as a good representation of the accident risk of the intended operation. In order to assess the combined effect of these differences there is need to perform a bias and uncertainty assessment [38].

In order to better learn understanding of what causes the collision risk of the simulation model to be relatively high, we performed an extra IPS run, and memorized in static memory for each particle the ancestor history at each of the eight levels. This allowed us to trace back what happened for the particles that hit the last level set (i.e., collision). There appeared to be five different collision events. Evaluation of these five collision events showed that all five happened under nominal safety critical conditions. Four of the five collisions were due to a growing number of multiple conflicts that could not be solved in time under the operational concept adopted. The fifth collision was of another type: at quite a late moment finally a conflict between two aircraft was solved with a maneuver by one of the two aircraft. However because of this maneuver there was a sudden collision with a third nearby aircraft.

These detailed evaluations of the five collision events of the 11th IPS run also showed that a significant increase of collision risk is caused by the relatively small height (4000 ft) of a container. Because of this small height it happened that an aircraft in one container came in conflict with a copy of its own in a neighboring container, and in such a situation there was an undesired limitation in conflict resolution options, and thus an undesired artificial increase in collision risk.

The results in this section seem to indicate that the key factor in the increased risk of collision for encounters with homogeneous traffic in the background — as opposed to the eight encountering aircraft only scenario — are the multiple conflicts. Under the far higher traffic densities than what the AMFF operational concept was designed for, it is not always possible to timely solve a sufficiently high fraction of those multiple conflicts. On the basis of this finding one would expect that the collision risk would decrease faster than linear with a decrease in traffic density. The validity of this expectation is verified by the next scenario.

3.4.4 Reduction of the aircraft density by a factor four

Now we enlarge the length and width of each container by a factor two. This means that the traffic density has gone down by a factor four. Hence the density is now $\frac{3}{4}$ of the density counted on 23rd July 1999 in the en-route area near Frankfurt. This still is a factor 2.5 higher than current average density above Europe. At the same time simulated flying time has been increased to 60 minutes (with 10 minutes prior flying to guarantee convergence).

By running four times the IPS algorithm the collision risk is estimated four times. The number of particles per IPS simulation run is 10,000. The total simulation time took about 280 hours on two machines, and the load of computer memory per machine was about 2.0 gigabyte. For these IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table 3.8 for each of the conflict levels, $k = 1, \ldots, 8$, for aircraft $i = 1$.

Table 3.8: Fractions counted during four IPS runs of scenario 3.

Level	1$^{\text{st}}$ IPS	2$^{\text{nd}}$ IPS	3$^{\text{rd}}$ IPS	4$^{\text{th}}$ IPS
1	0.755	0.750	0.752	0.749
2	0.295	0.292	0.286	0.285
3	0.476	0.475	0.497	0.487
4	0.263	0.258	0.266	0.267
5	0.321	0.315	0.300	0.328
6	0.068	0.088	0.082	0.096
7	0.156	0.367	0.290	0.254
8	0.011	0.059	0.021	0.005
Product of fractions	1.07×10^{-6}	1.61×10^{-5}	4.31×10^{-6}	1.07×10^{-6}

The estimated mean probability of collision per aircraft flight hour equals 5.64×10^{-6}, with minimum and maximum values respectively a factor five lower and higher. This is about a factor 30 lower than the previous scenario with a four times higher aircraft density. Thus, for the model there is a steep decrease of collision probability with decrease of traffic density, and this agrees well with the expectation at the end of the previous section.

3.4.5 Discussion of IPS simulation results

Because of the IPS simulation approach we were able to estimate collision risk for complex multiple aircraft scenarios. The large increase in handling complexity of multiple aircraft encounter situations is a major improvement over what was feasible before for two aircraft flying in a parallel route structure [10, 43]. Inherent to the IPS way of simulation, the dynamic memory of the computers used appeared to pose the main limitation on the full exploitation of the novel sequential Monte Carlo simulation approach. This also prevented performing a bias and uncertainty assessment for the differences between

the simulation model and the AMFF operation. As long as such a bias and uncertainty assessment has not been performed, any conclusion drawn from the simulation apply to the simulation model only, and need not apply to the intended AMFF operation.

The simulations performed for a model of AMFF allow free flight operational concept developers to learn characteristics of the simulation model. Because of the sequential Monte Carlo simulation based speed up, these simulations can show events that have not been observed before in Monte Carlo simulations of an AMFF model. Under far higher traffic densities than what the AMFF operational concept has been designed for, the simulations of the model shows it is not always possible to timely solve multiple conflicts. As a result of this, at high traffic levels there is a significant chance that multiple conflicts are clogging together, and this eventually may cause a non-negligible chance of collision between aircraft in the simulation model. It has also been shown that by lowering traffic density, the chance of collision for the model rapidly goes down.

3.5 Concluding remarks

We studied collision risk estimation of a free flight operation through a sequential Monte Carlo simulation. First a Monte Carlo simulation model of this free flight operational concept has been specified in a compositional way using the Stochastically and Dynamically Coloured Petri Net (SDCPN). Subsequently a novel sequential Monte Carlo simulation method [23, 25] has been extended for application to collision risk estimation in air traffic, and has subsequently been applied to an SDCPN model of free flight.

The results obtained show that the novel simulation model specification and collision risk estimation method allow to speed up the Monte Carlo simulations for much more complex air traffic encounter situations than what was possible before, e.g., [10, 43]. Moreover, for the simulation model of the free flight operational concept considered, behavior has been made visible that was expected by free flight concept designers, but could not be observed in straightforward Monte Carlo simulations of free flight concepts (e.g., [52]): the rare chance of clogging multiple conflicts at far higher traffic density levels than where the particular concept has been designed for. Hence, further attention has to be drawn toward the development and incorporation in the particular operational concept design of advanced methods in handling multiple conflicts. For example, Hoekstra [52] studied a conflict resolution approach that performs better than the one adopted in the AMFF concept. In addition, there are some complementary developments that aim to develop complex conflict resolution solvers with some guaranteed level of performance [33, 76] under nominal conditions, and ways to incorporate situation awareness views by human operators (pilots and/or controllers) in these combinatorial conflict resolution problems [30].

The initial collision risk estimation results obtained with our sequential Monte Carlo simulation of free flight provides valuable feedback to the design team and allows them to learn from Monte Carlo simulation results they have never seen before. This allows

them to significantly improve their understanding of when and why multiple conflicts are not solved in time anymore in the simulation model. Subsequently the operational concept designers can use their better understanding for adapting the free flight design such that it can better bring into account future high traffic levels.

In its current form the sequential Monte Carlo simulation approach works well, but at the same time poses very high requirements on the availability of dynamic computer memory and simulation time. The good message is that in literature on sequential Monte Carlo simulation, e.g., see [31, 32, 35, 50, 67, 74], complementary directions have been developed which remain to be explored for application to free flight collision risk estimation. These potential improvements of sequential Monte Carlo simulation will be studied in the work package WP7.

A Mathematical Background

A.1 Stationary Point Processes, Palm measure and applications to collision risk

A.1.1 Point process

In many applications, we observe some discrete events occurring at times T_0, $T_1, \cdots , T_n$; more formally these observations can be encompassed in the sequence $(T_n, n \in \mathbb{Z})$, where the $T_n \leq T_{n+1}$ are random variables. We call this process a *point process* on $\mathbb{R}^+$, and we say that the point process is *simple* if $T_n < T_{n+1}$ for each n. Another point of view consists in counting the number $N((a, b])$ of events observed during the time interval $(a, b]$; then $N((a, b]) = \sum_{n \in \mathbb{Z}} 1_{(a,b]}(T_n)$ and $T_n = \inf\{t : N(-\infty, t]) = n\}$. We say that the point process is *stationary* if the joint probability of the number of events in m disjoint intervals $I_1, \cdots , I_m$ is invariant by translation, ie for all $m \in \mathbb{N}$ and all $t \in \mathbb{R}$

$$\mathbb{P}(N(I_1) = k_1, \cdots , N(I_m) = k_m) = \mathbb{P}(N(I_1 + t) = k_1, \cdots , N(I_m + t) = k_m).$$

Let introduce for each t, the shift mapping θ_t defined on the probability space by $N(\theta_t\omega, I) = N(\omega, I + t)$. Therefore, the point process should be stationary if and only if $\mathbb{P} \circ \theta_t = \mathbb{P}$. These mappings satisfy the following properties: $\theta_t \circ \theta_s = \theta_{t+s}$, $\theta_t^{-1} = \theta_{-t}$ and for each $T_n \leq t < T_{n+1}$, $\theta_t T_n = T_0$ and $\theta_{T_{n+1}} = T_1$ with the convention that $T_0 \leq 0$ (see Figure (A.1)).
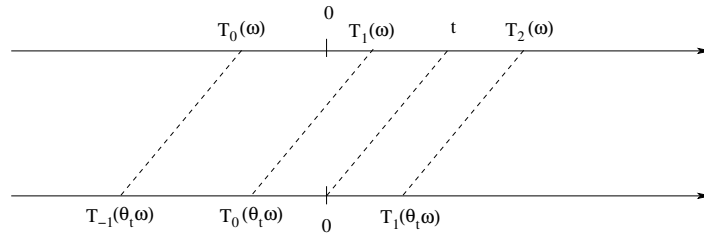
Figure A.1: The shift. Note the numbering of the points T_i

In the following, we will consider only stationary point processes. The positive number $\lambda = \mathbb{E}(N((0, 1]))$ is called the *intensity* of the point process; this number can be infinite, so we assume now that $\lambda > 0$ and is finite. Since the stationarity, for all interval I, the measure $\lambda(I) := \mathbb{E}(N(I))$ is invariant by translation, so it is proportional to the Lebesgue measure l on $\mathbb{R}$ and we deduce that $\lambda(I) = \lambda l(I)$, with $\lambda > 0$.

A.1.2 Palm measure

An important area in which point processes are used is queueing theory. For example, the number of clients at a bank counter is a point process and the study of the counting process N is useful to decide to open another counter or not. Nevertheless, the point of view of the client is different, since the more pertinent for him is the waiting time at the instant he arrives in the queue or more generally all information related to the counting process given its arrival time.

This suggests us to introduce a new probability P_N^0, called Palm measure, defined only on the event $T_0 = 0$, i.e. $P_N^0(T_0 = 0) = 1$. Due to the stationarity of the point process, the random variables $S_n = T_n - T_0$ are identically distributed, therefore we could define the empirical function $F_0(t)$ of $T_1 = S_0$ and we will have $F_0(t) = P_N^0(S_n \leq t)$ for all n. Thus, the Palm measure need to be a measure P_N^0 such that $P_N^0(A) = 0$ for all measurable sets A such $A \cap \{T_0 = 0\} = \emptyset$. For that, we need to count the number of events in A, not by observing all the process but by shifting successively all the T_n at the origin of the time, and so we consider the sum $\sum_{n \in \mathbb{Z}} 1_A \circ \theta_{T_n}$. Nevertheless, the Palm measure being a probability we have to normalize the sum, from which the probability

$$P_N^0(A) = \frac{1}{\lambda l(C)} \mathbb{E}\left[(1_A \circ \theta_{T_n}) 1_C(T_n)\right] := \frac{1}{\lambda l(C)} \mathbb{E}\left[\int_C (1_A \circ \theta_s) N(ds)\right].$$

It can be proved that this probability is independent of C and is supported by the event $\{T_0 = 0\}$, so we adopt the following definition

$$P_N^0(A) = \frac{1}{\lambda} \mathbb{E}\left[(1_A \circ \theta_{T_n}) 1_{(0,1]}(T_n)\right].$$

Knowing the Palm probability, it is also possible to obtain the law of the Point process by the following relation

$$\mathbb{P}(A) = \lambda \int_0^\infty P_N^0(T_1 > t, \theta_t \in A) dt. \tag{A.1.1}$$

A.1.3 Residual waiting time and spent waiting time

Let us come back to the empirical function $F_0(t)$ of the S_n under the probability P_N^0, i.e.

$$F_0(t) = P_N^0(S_n \leq t)$$

and introduce the residual waiting time at time $t \geq 0$ defined by

$$W(t) = T_{N(t)+1} - t$$

and the spent waiting time at time t

$$A(t) = t - T_{N(t)}.$$

For a stationary point process, you can take $t = 0$, in that case $W(0) = T_1$ and $A(0) = -T_0$. Using (A.1.1) we get for $A = \{T_1 > v, -T_0 > u\}$ with $u, v \geq 0$,

$$\mathbb{P}(T_1 > v, -T_0 > u) = \lambda \int_{v+u}^{\infty} (1 - F_0(s))ds,$$

from which we derive

$$\mathbb{P}(T_1 > v) = \lambda \int_{v}^{\infty} (1 - F_0(s))ds, \quad \mathbb{P}(-T_0 > u) = \lambda \int_{u}^{\infty} (1 - F_0(s))ds.$$

We conclude that $-T_0$ and T_1 are identically distributed for the probability P. Moreover, the law of S_0 under P is given by

$$\mathbb{P}(-T_0 + T_1 \leq x) = \int_{[0,x]} \lambda y F_0(dy),$$

which is in general different from $F_0(x)$. For instance,

$$E(S_0) = \int_0^{\infty} \lambda y^2 F_0(dy) = E_N^0(S_0) \left(1 + \frac{\text{Var}_N^0(S_0)}{(E_N^0(S_0))^2} \right),$$

since $E_N^0(S_0) = 1/\lambda$, so $E(S_0) = E_N^0(S_0)$ iff under the Palm probability, the variance of S_0 is zero, therefore iff S_0 is a constant and thus also all the S_n.

A.1.4 Application to the collision risk

We consider two aircraft A_1 and A_2, each flying on straight-line paths at constant velocity $\mathbf{v_1}$ and $\mathbf{v_2}$ respectively. If the aircraft A_1 is considered fixed, the aircraft A_2 can be considered having a velocity $\mathbf{v_r} = \mathbf{v_2} - \mathbf{v_1}$ relative to the aircraft A_2 and a relative position $\mathbf{r(t)}$ at time t given by, $\mathbf{r(t)} = \mathbf{r(0)} + \mathbf{v_r t}$.

A conflict is declared when the predicted position of the two aircraft are such that both horizontal and vertical separation parameters are infringed. Therefore, we associate a conflict volume to the aircraft A_1 which is an airspace formed around aircraft A_1 into which, if aircraft A_2 enters, a conflict is signalled. When this volume is a sphere a radius R, a conflict occurs when the predictive distance at the Closest Point of Approach (CPA) is smaller than or equal to R. The CPA is determined by the condition $\frac{d}{dt}(\mathbf{r(t)} \cdot \mathbf{r(t)}) = \mathbf{0}$ or

$$\mathbf{r(t)} \cdot \mathbf{v_r} = \mathbf{0},$$

that means the relative distance $\mathbf{r}$ is orthogonal to the relative velocity $\mathbf{v_r}$. The time t_{CPA} of the CPA and the distance d_{CPA} at CPA are given respectively by

$$t_{\text{CPA}} = -\frac{\mathbf{r(0)} \cdot \mathbf{v_r}}{\mathbf{v_r} \cdot \mathbf{v_r}}, \qquad d_{\text{CPA}}^2 = \mathbf{r(0)} \cdot \mathbf{r(0)} - \frac{(\mathbf{r(0)} \cdot \mathbf{v_r})^2}{\mathbf{v_r} \cdot \mathbf{v_r}}.$$

Let $\theta_r \in [0, 2\pi[$ be the angle between $\mathbf{v_r}$ and $\mathbf{r(0)}$, i.e. $\mathbf{r(0)} \cdot \mathbf{v_r} = \mathbf{r}(0)\mathbf{v_r} \cos \theta_r$, with $r(0) = \|\mathbf{r(0)}\|$ and $v_r = \|\mathbf{v_r}\|$. If $\theta_r = 0$ then the aircraft A_2 is passing from the aircraft A_1 an this situation is not relevant, so by now we assume that $\theta_r \neq 0$. Introducing the distance $a = R/(|\sin \theta_r|)$, a conflict will occur if $r(0) \leq a$.

We consider now an aircraft A_2 whose the straight-line path crosses a flow of aircraft each of which are flying on straight-line path too. Moreover, we assume that aircraft A_1 of the flow are distributed according to a stationary point process with intensity λ. Let choose the time zero as the moment the aircraft A_2 crosses the flow and let T_0 and T_1 the time separations between the two closest aircraft A_1 of the flow to the aircraft A_2. That means, at time $t = 0$, an aircraft A_1 will arrive at the crossing point at time $-T_0$ and the other crossed this same point T_1 time units ago. If F_0 is the distributed function of T_1 under the Palm measure of the point process, the probability P_c to have a conflict between the aircraft A_2 and one of aircraft A_1 is given by

$$P_c = 1 - \mathbb{P}(-T_0 > a/v_1, T_1 > a/v_1) = 1 - \lambda \int_{2a/v_1}^{\infty} (1 - F_0(u))du$$

$$= \lambda \int_0^{2a/v_1} (1 - F_0(u))du,$$

since $\int_0^{\infty}(1 - F_0(u))du = \mathbb{E}_N^0(T_1) = 1/\lambda$.

The quantity $2a/v_1$ being very small, we obtain the first order approximation $P_c \approx (2\lambda a)/v_1$ and if in addition, F_0 has a density f_0, we obtain a second order approximation

$$P_c \approx \frac{2\lambda a}{v_1}\left(1 - \frac{a}{v_1}f_0(0)\right).$$

Poisson Process

The Poisson process corresponds to the case $F_0(t) = 1 - e^{-\lambda t}$; so

$$P_c = 1 - e^{-2\lambda a/v_1} \approx \frac{2\lambda a}{v_1}\left(1 - \frac{\lambda a}{v_1}\right).$$

As $v_r \sin \theta_r = v_2 \sin \theta$ with θ the crossing angle between the two trajectories, we obtain the well-known formula

$$P_c \approx \frac{2\lambda a}{v_1}.$$

Gamma Law

Now, we assume that F_0 is a Gamma Law with parameters $p > 0$ and $\theta > 0$ whose the density is given by

$$f_0(u) = \frac{\theta^p}{\Gamma(p)}e^{-\theta u}u^{p-1} \qquad u \geq 0.$$

The expectation of this law being p/θ, we have to set $\lambda = \theta/p$, therefore

$$
\begin{aligned}
P_c &= \frac{\lambda 2a}{v_1} - \lambda \int_0^{2a/v_1} dt \int_0^t \frac{\theta^p}{\Gamma(p)} e^{-\theta u} u^{p-1} du \\
&= \frac{\lambda 2a}{v_1} - \lambda \int_0^{2a/v_1} \frac{\theta^p}{\Gamma(p)} e^{-\theta u} u^{p-1} du \int_u^{2a/v_1} dt \\
&= \frac{\lambda 2a}{v_1} \left[1 - \left(\frac{\lambda 2a\theta}{v_1}\right)^p \frac{1}{\Gamma(p)} \int_0^1 (1-v) v^{p-1} e^{-\frac{2a\theta}{v_1} v} dv \right] \\
&= \frac{\lambda 2a}{v_1} \left[1 - \left(\frac{\lambda 2a\theta}{v_1}\right)^p \frac{1}{\Gamma(p)} \sum_{n=0}^\infty (-1)^n \left(\frac{\lambda 2a}{v_1}\right)^n \frac{1}{n!} B(p+n, 2) \right] \\
&= \frac{\lambda 2a}{v_1} \left[1 - \sum_{n=0}^\infty (-1)^n \left(\frac{\lambda 2a\theta}{v_1}\right)^{n+p} \frac{1}{n!(p+n+1)(p+n)\Gamma(p)} \right].
\end{aligned}
$$

where $B(x,y) = \int_0^1 (1-v)^{y-1} v^{x-1} dv = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$. Thus the second order approximation is given by

$$
P_c \approx \frac{2a\theta}{p v_1} \left[1 - \left(\frac{2a\theta}{p v_1}\right)^p \frac{1}{\Gamma(p+2)} \right].
$$

Regular events with random translatories

Here, we consider events which are regularly spaced out but with a possibly random translatory. So, the i-th event occurs at time

$$
t_i = a_0 + ic + b_i, \qquad i = \cdot, -1, 0, 1, \cdots,
$$

where c is spacing between the events in absence of random perturbations and the b_i are independent and identically distributed random variable whose the empirical function, under the Palm measure, will be denoted by F_B. Then the i-th event is planned at time $a_0 + ic$, but its real time is moved by b_i. This type of process has been studied by T. Lewis and Govier (1960,1963) about the arrivals of tankers at a terminal.

We choose the event with indix $i = 0$ as initial time ; this event being planned at time $-b_0$ with regard to the origin of time, we deduce that, given b_0, the i-th event occurs at time $ic + b_i - b_0$, so

$$
\mathbb{P}_N^0(t_i \le t | b_0) = F_B(t + b_0 - ic) - F_B(b_0 - ic).
$$

It is important to note that the times t_i are not the times T_i of the point process induced by the events considered, since the j-th event can occur before the i-th event, even if $i < j$.

To obtain $F_0(t)$, it is enough to observe that $P_N^0(T_1 > t) = P_N^0(N(0, t] = 0)$, that means no event, except the 0-th event, has occurred during the time interval $(0, t]$. Thus

$$\mathbb{P}_N^0(T_1 > t | b_0) = \prod_{i=-\infty}^{\infty}{}' \left[1 - (F_B(t + b_0 - ic) - F_B(b_0 - ic))\right],$$

$$F_0(t) = 1 - \int_{-\infty}^{\infty} \prod_{i=-\infty}^{\infty}{}' \left[1 - (F_B(t + b_0 - ic) - F_B(b_0 - ic))\right] F_B(db_0),$$

where $\prod_{i=-\infty}^{\infty}{}'$ denotes the product over all the indices i except $i = 0$.

Let assume now, that F_B has a density f_B with a finite value in zero. Then, for t small enough we get the following approximation

$$F_0(t) \approx_{t=0} 1 - \int_{-\infty}^{\infty} \prod_{i=-\infty}^{\infty}{}' \left[1 - t f_B(b_0 - ic)\right] f_B(b_0) db_0$$

$$\approx_{t=0} 1 - \int_{-\infty}^{\infty} \left[1 - t \sum_{i=-\infty}^{\infty}{}' f_B(b_0 - i)\right] f_B(b_0) db_0$$

$$= t \sum_{i=-\infty}^{\infty} \int_{-\infty}^{\infty} f_B(b_0 - i) f_B(b_0) db_0 - t \int_{-\infty}^{\infty} f_B^2(b_0) db_0$$

$$= t \sum_{i=-\infty}^{\infty} f_Z(-ic) - t f_Z(0),$$

where f_Z is the density of a random variable Z with same law that the difference of two random variables i.i.d. with density f_B.

We deduce that

$$F_0(t) \approx t \left[c^{-1} \int_{-\infty}^{\infty} f_Z(u) du - f_Z(0)\right]$$

$$= t \left(\frac{1}{c} - f_Z(0)\right).$$

Therefore, the probability P_c can be approximated by

$$P_c \approx \lambda \int_0^{2a/v_1} \left[1 - u(c^{-1} - f_Z(0))\right] du = \frac{2\lambda a}{v_1} \left[1 - \frac{a}{v_1}\left(\frac{1}{c} - f_Z(0)\right)\right].$$

For instance, if the B is distributed as a centered Gaussian variable with variance σ_b^2, then

$$f_Z(x) = \frac{1}{2\sigma_b \pi^{1/2}} \exp\left(-\frac{x^2}{4\sigma_b^2}\right),$$

and

$$P_c \approx \frac{2\lambda a}{v_1} \left[1 - \frac{a}{v_1} \left(\frac{1}{c} - \frac{1}{2\sigma_b \pi^{1/2}} \right) \right].$$

It remains to estimate the parameter λ, nevertheless, the process being stationary the mean number of events, during a period of t unit of time, is t/c, so λ is approximatively equal to $1/c$.

A.2 Stochastic approach of the collision risk

In the previous section we have taken into account only random perturbations along the trajectory; now we generalize our approach by considering three-dimensional perturbations.

A.2.1 Introduction

In safety requirement, risk assessment and conflict prediction studies, the need to model and estimate the deviation of an aircraft from its assigned trajectory, leads to implement a probabilistic approach often based on Gaussian deviations from the predicted aircraft trajectories. We would like to mention two approaches: the geometric approach developed for conflict prediction [80] and the National Aerospace Laboratory (NLR) approach developed for collision risk evaluation [4]. In [80], the authors try to estimate the conflict probability from a modelling of lateral, longitudinal and vertical deviations. They approximate the prediction errors by a Gaussian distribution and use a geometric approach, based on uncertainty ellipsoid. However, this model does not take into account the time evolution of the uncertainty in the lateral and vertical direction while it assumes in the longitudinal direction a linear increasing standard deviation with time (i.e. 0.25NM/min in cruise situations).

The other approach is the NLR approach which is used in their simulation tool TOPAZ [6] but also in probabilistic conflict probe applications [4]. The aim there is to evaluate collision risk. Therefore the deviations are modelled by a certain type of stochastic differential equations (SDE's), the so-called Kramers' equation in Physics. Initially linear SDE's were used for modeling Gaussian deviations [4]. With the further development of TOPAZ the extension to non-linear SDE's was made and implemented in the TOPAZ tool. These non-linear SDE's result in non-Gaussian deviation distributions (like the Double Exponential stationary distribution, the Double-Double Exponential stationary distribution and the Gaussian Double Exponential stationary distribution, etc). These types of distributions are often used in fitting observed data for modelling the tails of data. More precisely, the two common stationary densities adopted for modeling errors (see [20, 21, 56, 86]) are a stationary Gaussian Double Exponential density

$$f(d) = (1 - \alpha) \left\{ \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{d^2}{2\sigma^2}\right) \right\} + \alpha \left\{ \frac{1}{2\lambda} \exp\left(-\frac{|d|}{\lambda}\right) \right\},$$

or a stationary Double-Double Exponential density

$$f(d) = (1 - \alpha)\Big\{\frac{1}{2\kappa}\exp\big(-\frac{|d|}{\kappa}\big)\Big\} + \alpha\Big\{\frac{1}{2\lambda}\exp\big(-\frac{|d|}{\lambda}\big)\Big\},$$

where the parameter α determines the relative importance of each of the functions, α is usually small, so in case of the Gaussian-Double Exponential density, the Gaussian density models the core of the data, while the Double Exponential density models the tails of the data. The context of the NLR's approach being the collision risk evaluation, all the 4 mentioned densities can be taken into account depending on which scenario is evaluated within TOPAZ. Hence, it is possible to use the NLR's approach to obtain a Gaussian (stationary) density or to obtain a Gaussian Double Exponential stationary density. One of the advantages of this approach is its time evolution formulation, by using stochastic differential equations. A SDE is a differential equation with a random term and hence whose the solution is, in some sense, a random function. Thus, each solution of a SDE represents a different random trajectory.

When the relative position x_t between two aircraft is modelled by a stochastic process, or more exactly a diffusion, the probability of conflict during a time interval $[0, T]$ is given by $P_c(T) = \mathbb{P}(\exists t \in [0, T] : x_t \in D)$, where D is the volume of conflict. This probability is very difficult to evaluate in general; but let us introduce the first hitting time of D, defined by $T_D = \inf\{t > 0 : x_t \in D\}$, then $P_c(T) = \mathbb{P}(T_D \leq T)$. Thus, it is enough to known the law of T_D; of course this law is also difficult to estimate, but it is easier to study, mainly by the so-called stochastic potential theory which allows to obtain lower and upper bounds of P_c in terms of a particular measure of D.

In [5], the authors introduces two another approaches : the absorbing or the transient boundary situation. In the absorbing boundary approach, instead of considering the process x_t, the authors study the absorbed process $\tilde{x}_t$ defined by $\tilde{x}_t = x_t$ for all $t \leq T_D$ and $\tilde{x}_t = x_{T_D}$ for all $t \geq T_D$. Thus $\mathbb{P}_x(T_D \leq t) = \mathbb{P}_x(\tilde{x}_t \in D)$, where $x = x_0$. We assume that the Kolmogorov backward equation is satisfied by $\mathbb{P}_x(\tilde{x}_t \in D)$, that means

$$\frac{\partial \mathbb{P}_x(\tilde{x}_t \in D)}{\partial t} = L\mathbb{P}_x(\tilde{x}_t \in D),$$

where L is a second order differential operator ; the two boundary conditions being

$$\lim_{x \to \partial D} \mathbb{P}_x(\tilde{x}_t \in D) = 1 \quad \text{for } t > 0, \ x \in D^c, \qquad \lim_{t \downarrow 0} \mathbb{P}_x(\tilde{x}_t \in D) = 0 \quad \text{for } x \in D^c.$$

If the initial position of x_t is not deterministic, but distributed according to the initial law $\pi_0(x)$, then the probability of collision in time period $(t_1, t_2]$ is given by

$$\mathbb{P}(\tilde{x}_{t_1} \in D^c, \tilde{x}_{t_2} \in D) = \int_{t_1}^{t_2} \int_{D^c} \frac{\partial \mathbb{P}_x(\tilde{x}_t \in D)}{\partial t} \pi_0(x) dx dt.$$

The coefficient

$$\mu(t) = \int_{D^c} \frac{\partial \mathbb{P}_x(\tilde{x}_t \in D)}{\partial t} \pi_0(x) dx,$$

is called in [5] *the conditional collision rate at time t.*

Let us notice that under good hypothesis, we get

$$\mu(t) = \int_{D^c} \lim_{\Delta \downarrow 0} \frac{\mathbb{P}_x(\tilde{x}_t \in D) - \mathbb{P}_x(\tilde{x}_{t-\Delta} \in D)}{\Delta} \pi_0(x) dx$$
$$= \int_{D^c} \lim_{\Delta \downarrow 0} \frac{\mathbb{P}_x(\tilde{x}_t \in D, x_{t-\Delta} \in D^c)}{\Delta} \pi_0(x) dx,$$
$$= \lim_{\Delta \downarrow 0} \frac{\mathbb{P}(\tilde{x}_t \in D, \tilde{x}_{t-\Delta} \in D^c)}{\Delta}.$$

In the transient boundary situation, the authors introduce the *in-crossing* rate $\varphi(t)$ at time t defined by

$$\varphi(t) = \lim_{\Delta \downarrow 0} \frac{\mathbb{P}(x_t \in D, x_{t-\Delta} \in D^c)}{\Delta}.$$

We notice that the conditional collision rate at time t of the process x_t is the in-crossing rate at time t of the absorbed process $\tilde{x}_t$. In fact, the existence de $\varphi(t)$ needs the differentiability of x_t, that means we must consider the diffusion (x_t, v_t) with $v_t = dx_t/dt$. Now, let $x \in \partial D$, we introduce the in-crossing rate $\varphi(x,t)$ at x, given by

$$\varphi(t,x)|dB|dt = \mathbb{P}(\text{ the process } x_t \text{ enters in } D \text{ during } [t, t+dt] \text{ through } dB),$$

where dB is some domain in ∂D whose area is $|dB|$. If ∂D is smooth, we obtain that

$$\varphi(t) = \int_{\partial D} \varphi(t,x) dx.$$

Under some assumptions [5] about the stochastic process (x_t, v_t), the Rice formula [75] can be applied and gives

$$\varphi(t,x) = \mathbb{E}\left[\langle n_x, v_t \rangle^- | x_t = x \right] f_t^X(x),$$

where n_x is the outwards normal in x at ∂D, f_t^X is the density of the x_t and $\langle n_x, v_t \rangle^- = 0$ if $\langle n_x, v_t \rangle \geq 0$ and $\langle n_x, v_t \rangle^- = \langle n_x, v_t \rangle$ otherwise. In [5], an explicit derivation of $\varphi(t)$ is obtained for a domain $D = [-s_1, s_1] \times [-s_2, s_2] \times [-s_3, s_3]$ in terms of $f_t^X(x)$.

A.2.2 Errors Modelling

In this section, we describe a model of perturbation introduced by Bakker and Blom. Let consider an aircraft following a straight-line path and denote by $x(t)$ and $v(t)$ its position and velocity; the couple $(x(t), v(t))$ is a 6-components vector called the state of the aircraft. For simplicity, we use a referential oriented according its trajectory: so the current state of the aircraft is $(x_{//}, v_{//}, x_{\vdash}, v_{\vdash}, x_{\perp}, v_{\perp})$, where $(x_{//}(t), v_{//}(t))$ is the longitudinal component, $(x_{\vdash}(t), v_{\vdash}(t))$ the lateral one and $(x_{\perp}(t), v_{\perp}(t))$ the vertical one. Denote by $\bar{\chi}$ the reference course and by $\bar{v}_G$ the reference ground speed. The deviations

of the aircraft from its trajectory is modelled by random perturbations of the course and the ground speed. Nevertheless, modelling the deviations of the course seems difficult; but we assume that we know the stationary distribution of the lateral deviations from the assigned trajectory. This distribution is a mixture between a Gaussian distribution and a Double Exponential one. So, instead of modelling the deviations of the course, it seems easier to model the lateral deviations, since by using a certain SDE, called Kramers' equation, we can obtain any stationary distribution for the lateral deviation (for instance a stationary Double Exponential distribution or a Gaussian distribution for the lateral deviation).
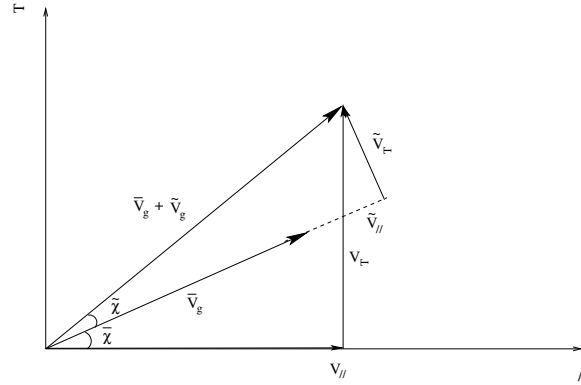

Figure A.2: Description of deviations from the trajectory in the plane

Let us introduce now the state vector $(\tilde{\chi}, \tilde{v}_G, \tilde{x}_\vdash, \tilde{v}_\vdash, \tilde{x}_\perp, \tilde{v}_\perp)$ that describes the deviations from the trajectory. The lateral deviations $(\tilde{x}_\vdash, \tilde{v}_\vdash)$ are taken relatively to the assigned trajectory (see Figure A.2). We have the following identities:

$$\begin{cases} v_{//} & = \cos(\bar{\chi} + \tilde{\chi})(\bar{v}_G + \tilde{v}_G) \\ v_\vdash & = \sin(\bar{\chi} + \tilde{\chi})(\bar{v}_G + \tilde{v}_G) \\ v_\perp & = \bar{v}_\perp + \tilde{v}_\perp \\ \tilde{\chi} & = \arctan\left(\frac{\tilde{v}_\vdash}{\sqrt{(\bar{v}_G + \tilde{v}_G)^2 - \tilde{v}_\vdash^2}}\right) \end{cases}$$

We do not get into the aircraft performance modelling, since for simplicity, we consider only a horizontal straight-line path, with a constant reference course $(d\bar{\chi}(t) = 0)$, a constant reference ground speed $(d\bar{v}_G(t) = 0)$ and a vertical reference speed zero $(\bar{v}_\perp(t) = 0)$. Hence, $\bar{\chi}$ may be fixed to zero, so we see that the deterministic motion (i.e. without random perturbations) is described by the following equations:

$$\begin{cases} d\bar{\chi}(t) & = 0, \quad d\bar{v}_G(t) = 0, \\ v_\vdash(t) & = 0, \quad v_\perp(t) = 0, \quad v_{//}(t) = \bar{v}_G, \end{cases}$$

where the origin of the referential is assumed to be the location of the aircraft, at time $t = 0$. For more details on aircraft performance modelling, see [53] for example. To

obtain the actual position of the aircraft, we must add the random effects, whence the use of the stochastic differential equations. Considering the NLR's approach, we have the following SDE for the lateral deviations (which result in the stationary Double Exponential distribution):

$$\begin{cases} d\tilde{x}_\vdash & = \tilde{v}_\vdash dt \\ d\tilde{v}_\vdash & = -a_1\mathrm{sign}(\tilde{x}_\vdash)dt - a_2\tilde{v}_\vdash dt + \text{ noise} \end{cases}$$

To understand these equations, we can think about the motion of a particle suspended in a fluid, which is influenced by two principal forces. First, a nonrandom (deterministic) motion which is engendered by an external force derived of the potential function $-a_1\mathrm{sign}(\tilde{x}_\vdash(t))$ and by the nature of the underlying fluid flow with the friction coefficient a_2. Second, collisions and more general interaction relationships with the fluid cause generally random perturbations of the velocity. Over a short time, these perturbations are often well described by Brownian fluctuations. Thus for a small duration from time t to $t + \Delta t$, the variation of the velocity is approximated by

$$\tilde{v}_\vdash(t + \Delta t) - \tilde{v}_\vdash(t) \approx -a_1\mathrm{sign}(\tilde{x}_\vdash(t))\Delta t - a_2\tilde{v}_\vdash(t)\Delta t$$
$$+ b_1 \text{ Normal}(0, \Delta t),$$

where Normal$(0, \Delta t)$ is a Gaussian distributed noise with expectation 0 and variance Δt. Following [62], we state that $\tilde{x}_\vdash(t)$ is a continuous-path Markov process such that the velocity $\tilde{v}_\vdash(t)$ exists and is continuous. Moreover, $(\tilde{x}_\vdash(t), \tilde{v}_\vdash(t))$ has a joint density $p(x, v, t)$, so the probability of finding $\tilde{x}_\vdash(t)$ in $]x, x + \Delta X]$ and $\tilde{v}_\vdash(t)$ in $]v, v + \Delta v]$ is $p(x, v, t)\Delta x\Delta v$ as $\Delta x \to 0$ and $\Delta v \to 0$. It is remarkable that this density converges as $t \to \infty$ to a simple stationary distribution

$$\pi(x, v) = K \exp(-\frac{2a_2a_1|x|}{b_1^2}) \exp(-\frac{a_2v^2}{b_1^2}),$$

in which position and velocity are independent; velocity is Normally distributed, and position deviation is distributed according as a Double Exponential density with variance $b_1^4/(2a_1^2a_2^2)$. Denote respectively $\sigma_{\tilde{x}_\vdash}^2$ and $\sigma_{\tilde{v}_\vdash}^2$ the variance of $\tilde{x}_\vdash$ and $\tilde{v}_\vdash$; these quantities can be estimated using statistical data or expert judgement. So, we obtain

$$a_1 = \sqrt{2}\frac{\sigma_{\tilde{v}_\vdash}^2}{\sigma_{\tilde{x}_\vdash}}, \quad a_2 = \frac{1}{2}\Big(\frac{b_1}{\sigma_{\tilde{v}_\vdash}}\Big)^2.$$

Nevertheless, we note that the model depends on three parameters a_1, a_2, b_1 linked together by two equations; thus one of these parameters remains undetermined by the only one observation of the stationary measure. In fact, the friction coefficient a_2 influences only on the convergence speed to equilibrium and not on the stationary measure.

A drawback of this model is the singular character of the function sign which is not derivable at the origin. The choice of this function has been guided by the form of the stationary measure you desired, despite its non physical aspect. Nevertheless, it

seems possible to overcome this drawback using the remark, already mentioned by J. B. Parker, that the Laplace distribution with parameter a can be obtain from a centered Gaussian distribution whose the variance is distributed according to an exponential law with parameter $a^2/2$, i.e.

$$\mathbb{P}(u < \sigma^2 \leq u + du) = \frac{a^2}{2} e^{-\frac{a^2}{2}u} du. \tag{A.2.1}$$

This follows from the identity

$$\int_0^\infty \frac{a^2}{2} e^{-\frac{a^2}{2}u} e^{-\frac{x^2}{2u}} \frac{du}{\sqrt{2\pi u}} = \frac{a}{2} e^{-a|x|}.$$

This situation can be regarded as representing a population of errors made by different aircraft with varying degrees of proficiency (different σ) and perhaps under different operating conditions (again, different σ).

A.2.3 The Kramers equation

Many stochastic approaches of the collision risk are based on a brownian perturbation of the position or more generally on diffusions under a potential function (see for example [84, 85]).

Nevertheless diffusions under a potential function are physically unrealistic because, recalling Newton's laws of motion, a potential really acts to cause a change in velocity rather than in position. We now describe a more realistic model; the Kramers equation, which describes the motion of a particle under the influence of the external force potential H, of viscosity, and of random perturbations of velocity. Let consider only the case of one dimensional motion and denote by X_t the position, V_t the velocity of the particle and $H'(x)$ the derivative of the potential H. The Kramers equation is a stochastic differential equation of the form

$$\begin{cases} dX_t &= V_t dt \\ dV_t &= -H'(X_t)dt - \gamma V_t dt + \sqrt{2\gamma} v_{th} dB_t, \end{cases} \tag{A.2.2}$$

where B_t is a standard Brownian motion. Thus, the pair (X_t, V_t) is a 2-dimensional diffusion and the position is a smoothed stochastic process, since the Brownian component, which is not differentiable, acts upon the velocity of the particle only. In other terms, the particle possesses a velocity though in general no acceleration.

This 2-dimensional diffusion process (X_t, V_t) has a simple stationary distribution

$$\pi(x, v) = K \exp(-\frac{H(x)}{v_{th}^2}) \exp(-\frac{v^2}{2v_{th}^2}),$$

in which position and velocity are independent.

Example 1 *[Laplace stationary distribution]*

Let $H(x) = a|x|$, where a is a positive real constant. This potential function satisfies the conditions that ensure existence and uniqueness of a solution. Here, the position has a bilateral exponential stationary distribution, $\pi(x) = K \exp(-a|x|/v_{th}^2)$. This example is interesting, since it leads to a stationary Laplace distribution, which is used in modelling the tails of the deviation errors in the air traffic data.

A.2.4 Solution for a linear force

For a linear force $H'(x) = \omega^2 x$, the Kramers equation may be written in the form

$$d \begin{pmatrix} x \\ v \end{pmatrix} = -A \begin{pmatrix} x \\ v \end{pmatrix} dt + \sqrt{2\gamma} v_{th} \begin{pmatrix} 0 \\ 1 \end{pmatrix} dB_t,$$

where

$$A = \begin{pmatrix} 0 & -1 \\ \omega^2 & \gamma \end{pmatrix}$$

The general solution, given X_0, V_0 is

$$\begin{pmatrix} X_t \\ V_t \end{pmatrix} = e^{-At} \begin{pmatrix} X_0 \\ V_0 \end{pmatrix} + \sqrt{2\gamma} v_{th} \int_0^t e^{-A(t-s)} \begin{pmatrix} 0 \\ 1 \end{pmatrix} dB_s.$$

Furthermore the exponential matrix e^{-At} is given by

$$e^{-At} = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} -\lambda_2 e^{-\lambda_1 t} + \lambda_1 e^{-\lambda_2 t} & e^{-\lambda_2 t} - e^{-\lambda_1 t} \\ \omega^2(e^{-\lambda_1 t} - e^{-\lambda_2 t}) & \lambda_1 e^{-\lambda_1 t} - \lambda_2 e^{-\lambda_2 t} \end{pmatrix}.$$

Thus, the transition probability $P(x, v, t|x', v', 0)$ is given by the two-variable gaussian distribution with means values $m(t) = (x(t), v(t))$ and covariance matrix

$$\Sigma(t) = \begin{pmatrix} \Sigma_{xx}(t) & \Sigma_{xv}(t) \\ \Sigma_{xv}(t) & \Sigma_{vv}(t) \end{pmatrix},$$

where

$$x(t) = \frac{x'}{\lambda_1 - \lambda_2}(\lambda_1 e^{-\lambda_2 t} - \lambda_2 e^{-\lambda_1 t}) + \frac{v'}{\lambda_1 - \lambda_2}(e^{-\lambda_2 t} - e^{-\lambda_1 t}),$$

$$v(t) = \frac{x'\omega^2}{\lambda_1 - \lambda_2}(e^{-\lambda_1 t} - e^{-\lambda_2 t}) + \frac{v'}{\lambda_1 - \lambda_2}(\lambda_1 e^{-\lambda_1 t} - \lambda_2 e^{-\lambda_2 t}),$$

$$\Sigma_{xx}(t) = \frac{\gamma v_{th}^2}{(\lambda_1 - \lambda_2)^2}\left[\frac{\lambda_1 + \lambda_2}{\lambda_1 \lambda_2} + \frac{4}{\lambda_1 + \lambda_2}\left(e^{-(\lambda_1 + \lambda_2)t} - 1\right) - \frac{1}{\lambda_1}e^{-2\lambda_1 t} - \frac{1}{\lambda_2}e^{-2\lambda_2 t}\right],$$

$$\text{(A.2.3)}$$

$$\Sigma_{xv}(t) = \frac{\gamma v_{th}^2}{(\lambda_1 - \lambda_2)^2}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)^2,$$

$$\Sigma_{vv}(t) = \frac{\gamma v_{th}^2}{(\lambda_1 - \lambda_2)^2}\left[\lambda_1 + \lambda_2 + \frac{4\lambda_1 \lambda_2}{\lambda_1 + \lambda_2}\left(e^{-(\lambda_1 + \lambda_2)t} - 1\right) - \lambda_1 e^{-2\lambda_1 t} - \lambda_2 e^{-2\lambda_2 t}\right],$$

with $\lambda_{1,2} = \frac{1}{2}(\gamma \pm \sqrt{\gamma^2 - 4\omega^2})$.

For $\omega^2 > \gamma^2/4$ the real parts of the eigenvalues $\lambda_{1,2}$, and for $\omega^2 \leq \gamma^2/4$ the eigenvalues $\lambda_{1,2}$ are larger than zero. Therefore, the covariance matrix converges for $t \to \infty$ to

$$\Sigma(\infty) = \begin{pmatrix} \frac{v_{th}^2}{\omega^2} & 0 \\ 0 & v_{th}^2 \end{pmatrix} \overset{def}{=} \begin{pmatrix} \sigma_x^2 & 0 \\ 0 & \sigma_v^2 \end{pmatrix}.$$

For $t \sim 0$, we obtain with $\eta = \sqrt{2\gamma}v_{th}$

$$\Sigma_{xx}(t) \sim \eta^2 t^3/3, \quad \Sigma_{xv}(t) \sim \eta^2 t^2/2, \quad \Sigma_{vv}(t) \sim \eta^2 t.$$

Initial Gaussian velocity

We assume now that $X_0 = 0$ and V_0 is a Gaussian centered random variable with variance v_{th}^2, independent of the Brownian motion. The solution is now the sum of the previous solution with $x' = v' = 0$ and the centered Gaussian vector

$$e^{-At}\begin{pmatrix} 0 \\ V_0 \end{pmatrix} = \frac{1}{\lambda_1 - \lambda_2}\begin{pmatrix} (e^{-\lambda_2 t} - e^{-\lambda_1 t})V_0 \\ (\lambda_1 e^{-\lambda_1 t} - \lambda_2 e^{-\lambda_2 t})V_0 \end{pmatrix}.$$

So the solution is always a centered Gaussian vector whose the covariance matrix is now given by

$$\begin{pmatrix} \frac{v_{th}^2}{\omega^2}(1 - y^2(t)) & v_{th}^2 y(t)z(t) \\ \\ v_{th}^2 y(t)z(t) & v_{th}^2(1 - \omega^2 z^2(t)) \end{pmatrix}$$

where

$$y(t) = (\lambda_2 e^{-\lambda_1 t} - \lambda_1 e^{-\lambda_2 t})/(\lambda_1 - \lambda_2)$$
$$z(t) = (e^{-\lambda_1 t} - e^{-\lambda_2 t})/(\lambda_1 - \lambda_2).$$

A.2.5 Randomization approach

As mentioned previously, to obtain an asymptotic Laplace distribution, instead of considering the Kramers' equation with the potential function $H(x) = a|x|$ order to obtain an asymptotic Laplace distribution, we can use a parabolic potential $H(x) = \omega^2 x^2/2$ and randomize the parameter ω^2. Since the asymptotic distribution of the position is Gaussian with variance v_{th}^2/ω^2, we consider a random potential such that the law of $1/\omega^2$ is an Exponential distribution with parameter $a^2/(2v_{th}^2)$ (A.2.1). Of course, we does not obtain necessarily the same transition density than in the previous model, and so the same transient behavior. The transition density $\tilde{p}(x, v, t)$ of this model, called the "annealed" transition density may be obtained by integrating the Gaussian density (so called the "quenched" transition density) with the Exponential density,

$$\tilde{p}(x, v, t) = \int_0^\infty \frac{a^2}{2v_{th}^2} e^{-\frac{a^2}{2v_{th}^2}u} p(x, v, t; u)du, \text{ where } u = \omega^{-2}.$$

A.2.6 Extreme cases

We consider the two extreme cases corresponding to large and low friction constant γ (see [1][§I14].

For large γ, let

$$Z_t = X_t + \gamma^{-1}V_t.$$

Then equations (A.2.2) yield

$$dZ_t = -\gamma^{-1}H'(X_t)dt + \sqrt{2/\gamma}v_{th}dB_t.$$

By using the scaling property of Brownian motion, which states that cB_{t/c^2} is a Brownian motion for every $c > 0$, we obtain that the time-changed process $Z_{t\gamma}$ of Z_t is solution of

$$dZ_u = -H'(X_u)du + \sqrt{2}v_{th}dB_u.$$

Thus, as $\gamma \to \infty$, the speeded-up process $X_{\gamma t}$ converges to the diffusion with drift $\mu(x) = -H'(x)$ and $\sigma^2(x) = 2v_{th}^2$.

As $\gamma \to 0$, the motion approximates that of deterministic frictionless motion under a potential. For instance, assume that $H(x)$ attains its minimum at a unique point x_0. If $\gamma = 0$, starting from $x_1 > x_0$ with velocity 0, the particle moves to $\hat{x}_1 < x_0$ such that $H(\hat{x}_1) = H(x_1)$ and then returns to x_1 : call this a x_1-cycle. As the energy

$$E_t = H(X_t) + \frac{1}{2}V_t^2, \tag{A.2.4}$$

is conserved, we can calculate the duration of this x_1-cycle (i.e. the trajectory on the level set $E_t \equiv H(\hat{x}_1)$)

$$D(x_1) = 2\int_{\hat{x}_1}^{x_1} (\text{ velocity at } x)^{-1}dx = 2\int_{\hat{x}_1}^{x_1} (2(H(x_1) - H(x))^{-1/2}dx.$$

In the stochastic case $(\gamma > 0)$, by using It calculus, we obtain the following SDE satisfied by the energy

$$dE_t = \gamma(v_{th}^2 - V_t^2)dt + \sqrt{2\gamma}v_{th}V_tdB_t. \tag{A.2.5}$$

Let $\hat{X}_1, \hat{X}_2, \cdots$, the right-most extremes of successive cycles, then integrating (A.2.5) over a cycle gives

$$H(\hat{X}_{n+1}) \approx H(\hat{X}_n) + \gamma(v_{th}^2D(\hat{X}_n) - I(\hat{X}_n)) + \text{Normal } (0, 4\gamma v_{th}^2I(\hat{X}_n)),$$

where

$$I(x_1) = \int V(t)dt \text{ over a } x_1 - \text{cycle} = 2\int_{\hat{x}_1}^{x_1} (2(H(x_1) - H(x))^{1/2}dx.$$

This approximation is the starting point of the heuristic developed in [1] to estimate the hitting time by X_t of a high level.

A.2.7 Low-Friction Limit

For the limit $\gamma = 0$, the motion of the particle is described by the trajectories of the dynamical system in the phase space (x, v), corresponding to the energy level curves. For very small friction, the energy varies slowly in the course of time (cf. (A.2.4)). So the random motion consists of fast rotations along the unperturbed trajectories of the deterministic system and slow motion across these trajectories. The nature of this motion thus suggests a set of new coordinates which splits the two components of motion: the so-called *action-angle coordinates*. The *action* part is defined by the area enclosed by the level curves of the energy, hence, it captures the slow component of the motion. Whereas the *angle* describes the uniform motion along the level curves, and is therefore related with the fast motion [3]. With these new coordinates (I, ϕ), the new energy or Hamiltonian is a constant $h(I)$ and the angle coordinate ϕ increases by 2π after each complete period $T(x, v) = T(I)$ of the motion on the level curve corresponding to the energy $h(I)$. Let assume that $H(0) = 0$ and $H(x) = H(-x)$, so, we obtain the following:

$$I = \frac{1}{\pi} \int_{-x_0(I)}^{x_0(I)} \sqrt{2(h(I) - H(\xi))} d\xi \tag{A.2.6}$$

$$\phi = \frac{\partial}{\partial I} \int_{-x_0(I)}^{x} \sqrt{2(h(I) - H(\xi))} d\xi$$

$$= h'(I) \frac{\partial}{\partial h} \int_{-x_0(I)}^{x} \sqrt{2(h - H(\xi))} d\xi$$

$$= \omega(I) \int_{-x_0(I)}^{x} \frac{1}{\sqrt{2(h - H(\xi))}} d\xi \tag{A.2.7}$$

The unperturbed Hamiltonian equations give that for $I > 0$

$$\frac{dI}{dt} = 0, \qquad \frac{d\phi}{dt} = \omega(I);$$

thus I is constant and $\phi(t) = \omega(I)t + \phi(0)$.

For $I > 0$ and $\phi \in\,] - \pi, \pi[$, the Jacobian of this transformation is given by [3]

$$\frac{(\partial x, v)}{(\partial \phi, I)} := \begin{pmatrix} \frac{\partial x}{\partial \phi} & \frac{\partial x}{\partial I} \\ \frac{\partial v}{\partial \phi} & \frac{\partial v}{\partial I} \end{pmatrix} = \begin{pmatrix} \frac{v}{\omega(I)} & v\beta(\phi, I) \\ -\frac{H'(x)}{\omega(I)} & \frac{\omega(I)}{v} - H'(x)\beta(\phi, I) \end{pmatrix}$$

where

$$\beta(\phi, I) = \begin{cases} \int_{\frac{\pi}{2}}^{\phi} \left[\frac{1}{v^2(\xi, I)} - \frac{\omega'(I)}{\omega(I)} \right] d\xi, & \text{for } I > 0, \phi \in 0, \pi[\\ -\beta(-\phi, I) & \text{for } I > 0, \phi \in 0, \pi[\end{cases}$$

The inverse of the Jacobian may be immediately obtained by using the identity

$$\frac{\partial x}{\partial \phi} \frac{\partial v}{\partial I} - \frac{\partial x}{\partial I} \frac{\partial v}{\partial \phi} = 1.$$

We obtain [3]

$$\frac{(\partial \phi, I)}{(\partial x, v)} := \begin{pmatrix} \frac{\partial \phi}{\partial x} & \frac{\partial phi}{\partial v} \\ \frac{\partial I}{\partial x} & \frac{\partial I}{\partial v} \end{pmatrix} = \begin{pmatrix} \frac{\omega}{v} - H'(x)\beta & -v\beta \\ \frac{H'(x)}{\omega} & \frac{v}{\omega}v \end{pmatrix}$$

Finally, the Kramers'equation in action-angle variables is given by

$$dI_t = \frac{H'(X_t)}{\omega(I_t)}V_t dt + \frac{V_t}{\omega(I_t)}[-\gamma V_t - H'(X_t)]dt + \gamma v_{th}^2 \left(\frac{\partial^2 I_t}{\partial V_t^2}\right)dt$$
$$+ \sqrt{2\gamma}v_{th}\frac{V_t}{\omega(I_t)}dB_t$$
$$\stackrel{def}{=} \gamma f_I(\phi_t, I_t)dt + \sqrt{2\gamma}v_{th}g_I(\phi_t, I_t)dB_t$$
$$d\phi_t = \omega(I_t)dt - H'(X_t)\beta(\phi_t, I_t)V_t dt - V_t\beta(\phi_t, I_t)[-\gamma V_t - H'(X_t)]dt$$
$$+ \gamma v_{th}^2\left(\frac{\partial^2 \phi_t}{\partial V_t^2}\right)dt - \sqrt{2\gamma}v_{th}V_t\beta(\phi_t, I_t)dB_t$$
$$\stackrel{def}{=} \omega(I_t)dt + \gamma f_\phi(\phi_t, I_t)dt + \sqrt{2\gamma}v_{th}g_\phi(\phi_t, I_t)dB_t$$

where

$$f_I(\phi, I) = -\frac{V_t^2(\phi, I)}{\omega(I)} + v_{th}^2\left(\frac{\partial^2 I_t}{\partial V_t^2}\right), \quad f_\phi(\phi, I) = V_t^2(\phi, I)\beta(\phi, I) + v_{th}^2\left(\frac{\partial^2 \phi_t}{\partial V_t^2}\right)$$
$$g_I(\phi, I) = \frac{V_t(\phi, I)}{\omega(I_t)}, \qquad\qquad g_\phi(\phi, I) = -V_t\beta(\phi_t, I_t).$$

Accordingly, as $\gamma \downarrow 0$, we see that the first motion is slow since its speed is of order γ whereas the second motion is relatively fast. Thus before the diffusing particle makes a small displacement transversally to the level sets direction it makes many rotation along the periodic trajectories. We now apply the "averaging principle" in [49][§7.9] consisting in averaging the slow motion over a period of the fast motion, giving an averaged system

$$d\bar{I}_t = \gamma \bar{f}_I(\bar{I}_t)dt + \sqrt{2\gamma}v_{th}\bar{g}_I(\bar{I}_t)dB_t,$$

where

$$\bar{f}_I(I) = \frac{1}{\pi}\int_0^\pi f_I(\phi, I)d\phi = -I - \frac{v_{th}^2}{\omega(I)}\left(\frac{I\omega'(I)}{\omega(I)} - 1\right)$$
$$\bar{g}_I^2(I) = \frac{1}{\pi}\int_0^\pi g_I^2(\phi, I)d\phi = \frac{I}{\omega(I)}$$

We used the following identity

$$\frac{1}{\pi}\int_0^\pi V^2(\phi, I)d\phi = \omega(I)\frac{1}{\pi}\int_0^\pi \sqrt{2(h(I) - H(\xi))}d\xi = I\omega(I).$$

The main result proved in [49] is that with probability 1 the process I_t converges to the process $\bar{I}_t$ when $\gamma \to 0$. So, if γ is so small that the effect of the perturbative term in

γ has a negligible effect during a period, the trajectory I_t can be approximated by the averaged system $\bar{I}_t$. Finally, we get the new Fokker-Planck equation for the probability density $p(I, t)$ (for convenience, we use the notation I_t)

$$\frac{\partial p(I, t)}{\partial t} = \gamma \frac{\partial}{\partial I}(Ip) + \gamma v_{th}^2 \frac{\partial}{\partial I} \frac{I}{\omega(I)} \frac{\partial p}{\partial I}.$$

Let remark that $h(\bar{I}_t)$ is a one-dimensional diffusion with drift $\gamma(v_{th}^2 - \bar{I}\omega(\bar{I}))$ and variance $2\gamma v_{th}^2 \bar{I}\omega(\bar{I})$, which corresponds to the averaged equation (A.2.5).

Example 2 *When the potential is parabolic, i.e. $H(x) = \omega^2 x^2/2$, the level curve $h(I) = E$ is an ellipse with axis $\sqrt{2E}$ and $(\sqrt{2E})/\omega$. Accordingly, the area of this ellipse being $(2\pi E)/\omega$, we get $I = E/\omega$ and $\omega(I) = \omega$. So, for small γ we obtain the averaged system*

$$\frac{\partial p(I, t)}{\partial t} = \gamma \frac{\partial}{\partial I}(Ip) + \gamma v_{th}^2 \omega^{-1} \frac{\partial}{\partial I} I \frac{\partial p}{\partial I}. \tag{A.2.8}$$

Introducing the new variable $\tilde{I} = (2\omega/v_{th}^2)I$ in (A.2.8), we get

$$\frac{\partial p(\tilde{I}, t)}{\partial t} = \gamma \frac{\partial}{\partial \tilde{I}}(\tilde{I}p) + 2\gamma \frac{\partial}{\partial \tilde{I}} \tilde{I} \frac{\partial p}{\partial \tilde{I}}.$$

So, a straightforward computation gives that the stationary distribution of $\tilde{I}$ is the Exponential law with parameter $1/2$. This is the exact distribution, since following Section A.2.4, the stationary state of the scaled energy $2E/v_{th}^2$ is distributed as the sum of two squares of independent standard Gaussian variables, whose the law is precisely the Exponential law of parameter $1/2$.

The transition density $p(x, y, t)$ of the averaged diffusion $\bar{I}_t$ satisfies the Kolmogorov backward equation

$$\frac{\partial p}{\partial t} = \gamma(\frac{v_{th}^2}{\omega} - x)\frac{\partial p}{\partial x} + \gamma \frac{v_{th}^2}{\omega} x \frac{\partial^2 p}{\partial x^2}.$$

By the method of separation of variables, we attempt a solution of the form

$$p(x, y, t) = e^{-\lambda \gamma t}\varphi(x).$$

We obtain the following equation (we omit the fixed variable y)

$$x\varphi''(x) + (1 - \frac{\omega}{v_{th}^2}x)\varphi'(x) + \lambda \frac{\omega}{v_{th}^2}\varphi(x) = 0. \tag{A.2.9}$$

As the Laguerre polynomials $L_n(x)$ satisfy the differential equation

$$xL_n''(x) + (1 - x)L_n'(x) + nL(x) = 0, \qquad 0 \le x < \infty,$$

the transformation $x \to \frac{\omega}{v_{th}^2}x$ shows that the solutions of the equation (A.2.9) are given by $\lambda = n$ and $\varphi_n(x) = L_n(\frac{\omega}{v_{th}^2}x)$. So

$$p(t,x,y) = \left(\frac{\omega}{v_{th}^2}\right)\exp\left[-\left(\frac{\omega}{v_{th}^2}\right)y\right]\sum_{n=0}^{\infty}e^{-n\gamma t}L_n\left(\frac{\omega}{v_{th}^2}x\right)L_n\left(\frac{\omega}{v_{th}^2}y\right).$$

It turns out that the density of the averaged squared velocity $\overline{V_t^2}$ is $\omega p(t, v_0, \omega v)$, hence the expectation $\mathbb{E}_0(\overline{V_t^2}) = v_{th}^2(1 - e^{-\gamma t})$. Let compare with the exact variance $\Sigma_{vv}(t)$ (cf. Section A.2.4). Let assume that $\gamma \ll 4\omega^2$, so the first order approximation of $\Sigma_{vv}(t)$ gives

$$\Sigma_{vv}(t) \sim v_{th}^2(1 - e^{-\gamma t}) + \frac{\gamma v_{th}^2}{2\omega}e^{-\gamma t}\sin(2\omega t),$$

hence, the same value by averaging. Finally, we get $\mathbb{E}_0(\overline{X_t^2}) = (v_{th}^2/\omega^2)(1 - e^{-\gamma t})$.

Example 3 *Now, let consider the potential function $H(x) = a|x|$. The action-angle coordinates may be obtained directly by (A.2.6, A.2.7)*

$$I = \left(\frac{2}{3a\pi}\right)(2E)^{3/2}, \qquad \omega(I) = \left(\frac{\pi a}{2}\right)^{2/3}(3I)^{-1/3},$$

hence the following Fokker-Planck equation

$$\frac{\partial p(I,t)}{\partial t} = \gamma\frac{\partial}{\partial I}(Ip) + \gamma v_{th}^2\left(\frac{2\sqrt{3}}{a\pi}\right)^{2/3}\frac{\partial}{\partial I}I^{4/3}\frac{\partial p}{\partial I}.$$

The stationary distribution is given by

$$p(I) = \frac{\beta}{2^{3/2}\sqrt{\pi}v_{th}^3}\exp\left(-\frac{(3\beta)^{2/3}}{2v_{th}^2}I^{2/3}\right), \qquad \text{with } \beta = \frac{a\pi}{2},$$

which means that the distribution of the random variable $(3\beta I)^{2/3}/v_{th}^2$ has a chi-squared density with 3 degrees of freedom.

Accordingly, let consider the transformation $x = (3\beta)^{2/3}v_{th}^{-2}I^{2/3}$, the function $u_t(x,y) = x^{1/2}p(t,x,y)$ satisfies the following equation

$$\left(\frac{3}{2\gamma}\right)\frac{\partial u}{\partial t} = -\frac{\partial}{\partial x}(3-x)u + \frac{1}{2}\frac{\partial^2}{\partial x^2}(4xu),$$

whose the adjoint form is

$$\left(\frac{3}{2\gamma}\right)\frac{\partial u}{\partial t} = (3-x)\frac{\partial u}{\partial x} + 2x\frac{\partial^2 u}{\partial x^2}.$$

A Mathematical Background

As previously, we attempt a solution of the form

$$u(x, y, t) = e^{-\frac{2\gamma\lambda}{3}t}\varphi(x, y).$$

We get the following equation

$$x\varphi''(x) + (3/2 - z/2)\varphi'(x) + \lambda/2\varphi(x) = 0. \qquad (A.2.10)$$

By substituting $x/2$ for x, the equation (A.2.10) becomes an equation of the form

$$z\varphi''(z) + (3/2 - z)\varphi'(z) + \lambda\varphi(z) = 0.$$

A corresponding solution is for $\lambda = n$

$$\varphi(x) = c_1 L_n^{1/2}(z) + c_2 F(-n, 3/2, z),$$

where $L_n^\alpha(z)$ are the generalized Laguerre polynomials

$$L_n^\alpha(z) = \frac{\Gamma(\alpha + n + 1)}{\Gamma(n + 1)} \sum_{k=0}^n \binom{n}{k} \frac{(-1)^k}{\Gamma(\lambda + k + 1)} z^k,$$

and $F(\alpha, \gamma, z)$ is the degenerated hypergeometric function

$$F(\alpha, \gamma, z) = 1 + \frac{\alpha}{\gamma}\frac{z}{1!} + \frac{\alpha(\alpha+1)}{\gamma(\gamma+1)}\frac{z^2}{2!} + \cdots.$$

As $F(-n, b, z) \propto z^n$ as $z \to \infty$, we have $c_2 = 0$.

The Laguerre system $L_n^\alpha(z)$ comprises the unique orthogonal polynomials with respect the weight function $w(z) = z^\alpha e^{-z}/\Gamma(\alpha + 1)$, pour $z > 0$; $w(0) = 0$ for $z < 0$, since the identity

$$\int_0^\infty L_n^\alpha(z)L_m^\alpha(z)w(z)dz = \binom{n + \alpha}{n}\delta_{nm}.$$

For example, we have

$$L_n^\alpha(0) = \binom{n + \alpha}{\alpha}, \quad L_0^\alpha(z) = 1, \quad L_1^\alpha(z) = -z + \alpha + 1.$$

Finally, the transition density of the diffusion $Z_t = (3\beta I_t)^{2/3}/v_{th}^2 = (2\overline{E}_t)/v_{th}^2$ is given by

$$p(t, x, y) = \frac{1}{2^{3/2}\Gamma(3/2)}y^{1/2}e^{-y/2} \sum_{n=0}^\infty e^{-\frac{2\gamma nt}{3}} L_n^{1/2}(x/2)L_n^{1/2}(y/2)w_n,$$

with $w_n^{-1} = \binom{n+1/2}{n}$.

A straightforward but arduous separation of variables [62][§15.13] leads to

$$p(t, x, y) = \frac{y^{1/2}e^{-y/2}}{2^{3/2}\Gamma(3/2)(1 - e^{-bt})} \exp\left\{-\frac{(x + y)e^{-bt}}{1 - e^{-bt}}\right\}\left(\frac{1}{4}e^{-bt}xy\right)^{-1/4}I_{1/2}\left(\frac{\sqrt{xye^{-bt}}}{1 - e^{-bt}}\right),$$

where $b = 2\gamma/3$ and $I_{1/2}$ is the modified Bessel function of order $1/2$.

It follows that given $\overline{E}_0 = e$

$$\mathbb{E}_e(\overline{E}_t) = \frac{3v_{th}^2}{2}\left(1 - e^{-\frac{2\gamma t}{3}}\left(1 - \frac{2e}{3v_{th}^2}\right)\right).$$

Furthermore, let notice that $\overline{V^2}_t = \omega(I_t)I_t = (2/3)\overline{E}_t$, so $a\overline{|X_t|} = (2/3)\overline{E}_t = 2\overline{V^2}_t$. We deduce that

$$\mathbb{E}_e(\overline{V^2}_t) = v_{th}^2\left[1 - e^{-\frac{2\gamma t}{3}}\left(1 - \frac{2e}{3v_{th}^2}\right)\right], \quad \mathbb{E}_e(\overline{|X|}_t) = \frac{v_{th}^2}{a}\left(1 - e^{-\frac{2\gamma t}{3}}\left(1 - \frac{2e}{3v_{th}^2}\right)\right).$$

A.2.8 High Friction

In Section A.2.6, we have seen that for large γ the diffusion $Z_t = X_t + \gamma^{-1}V_t \approx X_t$ was a solution of

$$dZ_t = -\gamma^{-1}H'(X_t)dt + \sqrt{2\gamma^{-1}}dB_t.$$

By using scaling property of Brownian motion, we obtain that the time-changed process $Z_{t\gamma/2v_{th}^2}$ is solution of

$$dZ_u = -\frac{a}{2v_{th}^2}\,\text{sgn}(Z_u)du + dB_u, \tag{A.2.11}$$

and accordingly, for large γ, we can approximate X_u by Z_u. To obtain the transition density, we follow [61][§6.5]. Firstly, we consider the new function sgn defined by

$$\text{sgn}(x) = \begin{cases} 1\,; & x > 0 \\ -1\,; & x \le 0 \end{cases},$$

which is left continuous (this is nothing else that the left-derivative of $|x|$). Let introduce the notation $u(x) = -\theta\,\text{sgn}(x)$, with $\theta = a/(2v_{th}^2)$. By Girsanov transformation, equation (A.2.11) has a weak solution $(Z, B), (\Omega, \mathcal{F}_t, \tilde{P}_x)$ which is unique in the sense of probability law, with finite-dimensional distribution given by

$$\tilde{P}_x[(X_{t_1}, \cdots, X_{t_n}) \in \Gamma]$$
$$= \mathbb{E}_x\left[1_{\{(B_{t_1}, \cdots, B_{t_n}) \in \Gamma\}}\exp\left\{\int_0^t u(B_s)dB_s - \frac{1}{2}\int_0^t u^2(B_s)ds\right\}\right],$$

where $\mathbb{E}_x$ is the expectation with respect the Brownian probability P_x. The transition density $\tilde{p}(x, z, t)$ takes the form

$$\tilde{p}(x, z, t) = \mathbb{E}_x\left[1_{\{B_t \in dz\}}\exp\left\{\int_0^t u(B_s)dB_s - \frac{1}{2}\int_0^t u^2(B_s)ds\right\}\right]. \tag{A.2.12}$$

To eliminate the stochastic integral in (A.2.12), let set

$$f(z) = \int_0^z u(y)dy = \begin{cases} \theta z; & z < 0 \\ -\theta z; & z \ge 0 \end{cases}$$

A Mathematical Background

The It formula generalized for convex functions [61][Th 3.6.22] gives

$$f(B_t) = f(B_0) + \int_0^t u(B_s)dB_s + \frac{a}{v_{th}^2}L(t),$$

where $L(t)$ is the local time of B at the origin

$$L_t(0) = \lim_{\epsilon \downarrow 0} \frac{1}{4\epsilon}\text{meas}\{0 \le s \le t; |B_t| \le \epsilon\},$$

where $\text{meas}(A)$ denotes the Lebesgue measure of the set A. On the other hand,

$$\int_0^t u^2(B_s)ds = \frac{a^2}{4v_{th}^4}t,$$

and (A.2.12) becomes

$$\tilde{p}(x,z,t) = \exp\left[f(z) - f(x) - \frac{t}{2}\frac{a^2}{4v_{th}^4}\right]\int_{b=0}^\infty \exp\{b\frac{a}{v_{th}^2}\}P_x[B_t \in dz; L(t) \in db] \quad (A.2.13)$$

Finally, we get [61][Remark 6.5.2]

$$\tilde{p}(x,z,t) = \begin{cases} \frac{1}{\sqrt{2\pi t}}\left[\exp\left\{-\frac{(x-z-\theta t)^2}{2t}\right\}+\theta e^{-2\theta z}\int_{x+z}^\infty \exp\left\{-\frac{(v-\theta t)^2}{2t}\right\}dv\right]; \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x \ge 0, z > 0 \\ \frac{1}{\sqrt{2\pi t}}\left[\exp\left\{2\theta x - \frac{(x-z+\theta t)^2}{2t}\right\}+\theta e^{2\theta z}\int_{x-z}^\infty \exp\left\{-\frac{(v-\theta t)^2}{2t}\right\}dv\right]; \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x \ge 0, z \le 0 \end{cases}$$

and for $x \le 0$, we use the relation $\tilde{p}(x,z,t) = \tilde{p}(-x,-z,t)$.

Accordingly a tedious computations gives for the function $v(t,x) = \tilde{\mathbb{E}}_x(Z_t^2)$

$$\begin{aligned} v(t,x) =& \frac{1}{2\theta^2} + \sqrt{\frac{t}{2\pi}}(|x| - \theta t - \frac{1}{\theta})\exp\left\{-\frac{(|x| - \theta t)^2}{2t}\right\} \\ &+ \left\{(|x| - \theta t)^2 + t - \frac{1}{2\theta^2}\right\}\Phi\left(\frac{|x| - \theta t}{\sqrt{t}}\right) \\ &+ e^{2\theta|x|}\left(\frac{|x|}{\theta} + t - \frac{1}{2\theta^2}\right)\left[1 - \Phi\left(\frac{|x| + \theta t}{\sqrt{t}}\right)\right] \end{aligned}$$

where

$$\Phi(x) := \int_{-\infty}^x e^{-y^2/2}\frac{dy}{\sqrt{2\pi}}.$$

We can verify that

$$\lim_{t \downarrow 0} v(t,x) = x^2, \quad \lim_{t \to \infty} v(t,x) = \frac{1}{2\theta^2} = \frac{2v_{th}^4}{a^2}.$$

On the other hand $v(t,x)$ satisfies the equation

$$\frac{\partial v}{\partial t} = \frac{1}{2}\frac{\partial^2 v}{\partial x^2} - \theta\text{sgn}(x)\frac{\partial v}{\partial x}.$$

A.3 Rare Event Simulations

Let assume that the dynamic of the studied system is well described by a continuous-time strong Markov process $X = (X_t)_{t \geq 0}$ with values in $\mathbb{R}^d$ for some $d > 0$. We suppose that the paths of X are cdlg (i.e. right-continuous with left-hand limits). Let $B \subset \mathbb{R}^d$ be some closed critical region, in which the system could enters but with a very small probability, say about 10^{-9}. Let

$$T_B = \inf\{t \geq 0 : X_t \in B\}$$

the entrance time into B, our objective is to compute the probability of the critical event B and the probability distribution of the critical paths

$$P_B = \mathbb{P}[T_B \leq T], \qquad \mathbb{E}[f(X_t; 0 \leq t \leq T_B)|T_B \leq T],$$

where T is a finite deterministic time, or an a.s. finite stopping time.

In practice, none of the simulated trajectories will ever reach B, hence a crude Monte Carlo simulation fails. To speed-up the simulations, there exists two main methods: Importance Sampling and Importance Splitting.

Importance Sampling works by changing the stochastic process X into a new process for which the set B has a high probability; this makes the Monte-Carlo estimator of the probability more efficient, mainly by decreasing its variance. Nevertheless, this estimator is biased, so to unbiased it we need to weight the sample values to get to account for the change in stochastic process we are simulating. The well-know problem to Importance Sampling method is that it is hard to derive the optimal change and in practice usually this optimal change cannot be found analytically and/or adaptively.

In contrast to importance sampling type algorithms, in the trajectory splitting methodology, the step-by-step evolution of the system follows the original probability measure. Entering the intermediate states, which is usually characterized by crossing a threshold by a control parameter, triggers the splitting of the trajectory. The current system state is held, and a number of independent subtrajectories are simulated from that state.

For example, let us consider $(n+1)$ sets B_i such that

$$B_n \subset B_{n-1} \subset \cdots \subset B_0.$$

When the rare event B coincide with B_n, we have the product formula

$$\mathbb{P}(B) = \mathbb{P}(B|B_{n-1})\mathbb{P}(B_{n-1}|B_{n-2}) \cdots \mathbb{P}(B_1|B_0)\mathbb{P}(B_0). \qquad (A.3.1)$$

On the right hand side of (A.3.1), each conditioning event is "not rare". The branching splitting technique proceeds as follows. Make a $\{0,1\}$ Bernoulli trial to check whether or not the set event B_1 has occurred. If B_1 has occurred, then we split this trial in R_1 Bernoulli additional trials, and for each of them we check again wether or not the event B_2 has occurred. This procedure is repeated at each level. More precisely, each time

the event B_i has occurred, we sample R_i trials and we repeat this splitting technique each time B_{i+1} has occurred. If an event level is not reached, neither is B, then we stop the current retrial. Using R_0 independent replications of this procedure, we have then considered $R_0 R_1 \cdots R_m$ trials, taking into account for example, that if we have failed to reach a level B_i at the i-th step, the $R_i \cdots R_m$ possible retrials have failed. An unbiased estimator of $\mathbb{P}(B)$ is clearly given by the quantity

$$\widehat{P} = \frac{N_B}{R_0 \prod_{i=1}^{m} R_i},$$

where N_B is the total number of trajectories having reached the set B. It can be proven [73] that in some sense the optimal simulation is obtained if

$$m = \lfloor -0.6275 \log P(B) - 1 \rfloor, \quad \mathbb{P}(B_i | B_{i-1}) \approx 1/5, \quad R_i = 5.$$

Nevertheless, in practice the trajectory splitting method may be difficult to apply. For example, the case of the estimation of the probability of a rare event in dynamical system is more complex, since the difficulty to find theoretically the optimal B_i, and R_i for each level i. Furthermore, the probability to reach B_i varies generally with the state of entrance in level B_{i-1}. Finally, but not the least, the conditional probabilities $\mathbb{P}(B_i | B_{i-1})$ are of course generally unknown!

Hence, the random evolution of the process must be taken into account; and for that a well adapted tool is the so-called Feynman-Kac models.

A.3.1 Multilevel Feynman-Kac distributions

We consider a continuous-time strong Markov process $X = \{X(t); t \geq 0\}$ with value in $\mathbb{R}^d$ for some $d > 0$ and with cdlg trajectories. Let introduce an embedded sequence of closed regions

$$[0, \infty) \times B = A_n \subset \cdots \subset A_1 \subset A_0 = [0, \infty) \times \mathbb{R}^d,$$

which are defined by

$$A_k = \{(t, x) \in [0, \infty) \times \mathbb{R}^d : F_k(t, x) \leq c_k\},$$

where F_k is some lower semi-continuous function. Let the corresponding hitting times

$$T_k = \inf\{t \geq 0 : (t, X(t)) \in A_k\},$$

which satisfy

$$0 = T_0 \leq T_1 \leq \cdots \leq T_n = T_B.$$

To capture the precise behavior of the process X in each region, we consider the random excursions $\mathcal{X}_k$ of X between the successive random times T_{k-1} and T_k. More precisely,

we introduce the discrete-time Markov chain $\mathcal{X} = \{\mathcal{X}_k, k = 1, \cdots, n\}$ with value in the excursion set E, defined by

$$\mathcal{X}_k = ((t, X(t)), T_{k-1} \wedge T \leq t \leq T_k \wedge T),$$

with $t \wedge T = \inf\{T, t\}$. We observe that these excursions may have different random lengths. To check wether or not a given path $e = ((t, X(t)), t' \leq t \leq t'')$, starting at $X(t') \in B_{k-1}$ at time t', has succeeded to reach the level B_k at time t'', it is convenient to introduce the terminal point $\pi(e) = (t'', X(t''))$ of the excursion and the indicator functions g_k defined by

$$g_k(e) = 1_{\{\pi(e) \in A_k\}}.$$

With this notation, and for each k, we have $T_k \leq T$ iff $g_k(\mathcal{X}_k) = 1$, hence

$$1_{\{T_k \leq T\}} = g_k(\mathcal{X}_k) = \prod_{p=1}^{k} g_p(\mathcal{X}_p).$$

Now, let us introduce the so-called Feynman-Kac distributions γ_k on the path space E defined in such a way that the integral of all bounded measurable functions f relatively to this measure, denoted by $\gamma_k(f)$ is defined by the formula

$$\gamma_k(f) = \mathbb{E}\left[f(\mathcal{X}_k) \prod_{p=1}^{k} g_p(\mathcal{X}_p)\right] = \mathbb{E}\left[f((t, X(t)), T_{k-1} \leq t \leq T_k)1_{\{T_k \leq T\}}\right].$$

This measure is not a probability, since its normalizing constant is given by

$$\gamma_k(1) = \mathbb{P}[T_k \leq T].$$

Therefore, the corresponding probability μ_k is given by

$$\mu_k(f) = \frac{\gamma_k(f)}{\gamma_k(1)} = \mathbb{E}\left[f((t, X(t)), T_{k-1} \leq t \leq T_k)|T_k \leq T\right].$$

The entrance distribution with support included in A_k is the image of μ_k under π, i.e. the measure $\pi_k \circ \pi^{-1}$ defined by

$$\mu_k \circ \pi^{-1}(dt, dx) = \mathbb{P}\left[T_k \in dt, X(T_k) \in dx)\right].$$

Thus, for any bounded measurable function ϕ defined on A_k, we get

$$\mu_k \circ \pi^{-1}(\phi) = \mu_k(\phi \circ \pi) = \mathbb{E}\left[\phi(T_k, X(T_k))|T_k \leq T\right].$$

Similarly, introducing the measure γ_k^- defined by

$$\gamma_k^-(f) = \mathbb{E}\left[f(\mathcal{X}_k) \prod_{p=1}^{k-1} g_p(\mathcal{X}_p)\right] = \mathbb{E}\left[f((t, X(t)), T_{k-1} \leq t \leq T_k \wedge T)1_{\{T_{k-1} \leq T\}}\right],$$

leads us to define the so-called Feynman-Kac distributions η_k obtained by normalizing γ_k^-, and so given by

$$\eta_k(f) = \mathbb{E}\left[f((t, X(t)), \ T_{k-1} \leq t \leq T_k \wedge T)|T_{k-1} \leq T\right].$$

In particular for $f = g_k$,

$$\eta_k(g_k) = \mathbb{P}[T_k \leq T|T_{k-1} \leq T] := P_k,$$

hence

$$\mathbb{P}[T_k \leq T] = \gamma_k(1) = \prod_{p=1}^{k} \eta_p(g_p) = \prod_{p=1}^{k} P_p.$$

The interacting particles methods, we will discuss hereafter, provide numerical approximation for the rare event probability

$$P_B = \mathbb{P}[T_B \leq T] = \gamma_n(1),$$

the transition probabilities from one level to the next P_k and the entrance distribution in one level $\mu_k \circ \pi^{-1}$.

A.3.2 Interacting particle system approximations

The idea of the Interacting Particle Systems (IPS) is derived from the following remarks. First at all, the so-called Feynman-Kac flow $(\eta_k; \ 0 \leq k \leq n)$ is the solution of a nonlinear measure-valued dynamical system

$$\eta_k = \Phi_k(\eta_{k-1}). \tag{A.3.2}$$

The mappings Φ_k from the set of measures

$$\mathcal{P}_k(E) = \{\eta : \eta(g_k) > 0\}$$

into the set $\mathcal{P}(E)$ of measure on E are defined by

$$\Phi_k(\eta)(f) = \Psi_{k-1}(\eta)\left(\mathcal{M}_k f\right),$$

where the non-homogeneous Markov kernels $\mathcal{M}_k$, which describe the Markovian transitions of the Markov chain $\mathcal{X}$, are defined for all excursion e by

$$\mathcal{M}_k f(e) = \mathbb{E}\left[f(\mathcal{X}_k)|\mathcal{X}_{k-1} = e\right],$$

and the updating mappings Ψ_k from $\mathcal{P}_k(E)$ into $\mathcal{P}_k(E)$ are defined for any bounded function f by

$$\Psi_k(\eta)(f) = \eta(fg_k)/\eta(g_k).$$

All these follow from

$$\gamma_k^-(f) = \mathbb{E}\left[g_{k-1}(\mathcal{X}_{k-1})\prod_{p=1}^{k-2} g_p(\mathcal{X}_p)\mathbb{E}\left[f(\mathcal{X}_k)|\mathcal{X}_{k-1}\right]\right] = \gamma_{k-1}^-(g_{k-1}\mathcal{M}_k f).$$

Thus, we see that the recursion (A.3.2) involves two separate selection/mutation transitions

$$\eta_k \in \mathcal{P}_k(E) \xrightarrow{\text{selection}} \widehat{\eta}_k := \Psi_k(\eta_k) \in \mathcal{P}(E) \xrightarrow{\text{mutation}} \eta_{k+1} = \widehat{\eta}_k\mathcal{M}_{k+1} \in \mathcal{P}(E).$$

Secondly, from a pure mathematical point of view, particles methods can be interpreted as a kind of stochastic linearization technique for solving nonlinear equations in measure space. The idea is to associate to (A.3.2) a sequence $\xi = (\xi^1, \cdots, \xi^N)$ of N E-valued Markov chains such that the empirical measures

$$\eta^N = \frac{1}{N}\sum_{i=1}^{N}\delta_{\xi^i}$$

converge as $N \to \infty$ to the desired distribution η. The state components of the E^N-valued Markov chains are called particles.

Now, we describe in more details the evolution of the particles according to the diagram

$$\xi_k = (\xi_k^1, \cdots, \xi_k^N) \xrightarrow{\text{selection}} \widehat{\xi}_k = (\widehat{\xi}_k^1, \cdots, \widehat{\xi}_k^N) \xrightarrow{\text{mutation}} \xi_{k+1} = (\xi_{k+1}^1, \cdots, \xi_{k+1}^N).$$

At time $k = 0$, the initial configuration consists in N independent and identically distributed random variables ξ_0^i, $i = 1, \cdots, N$ with common law η_0. Since we have $g_0(x) = 1$ for η_0-almost every x, we may discard the selection at time $k = 0$ and set $\widehat{\xi}_0^i = \xi_0^i$ for each i. We use the conventions $T_{-1}^i = T_0^i = 0$ and we introduce a cemetery point Δ which takes into account the possible stopping of the algorithm..

The **mutation transition** $\widehat{\xi}_k \to \xi_{k+1}$ at time $k + 1$ is defined as follows. If $\widehat{\xi}_k = \Delta$, we set $\widehat{\xi}_{k+1} = \Delta$. Otherwise during mutation, independently of each other, each selected particle
$$\widehat{\xi}_k^i = \left((t, X^i(t)), T_{k-1}^i \wedge T \leq t \leq T_k^i \wedge T\right)$$
evolves randomly according to the Markov transition $\mathcal{M}_{k+1}$, so that
$$\xi_{k+1}^i = \left((t, X^i(t)), T_k^i \wedge T \leq t \leq T_{k+1}^i \wedge T\right),$$

where
$$T_{k+1}^i = \inf\{t \geq T_k^i; \xi_{k+1}^i \in A_{k+1}\}.$$

Thus, for each particle i, we start a trajectory from $\widehat{\xi}_k^i$ at time T_k^i, and let it evolve randomly as a copy of the process $\{X_s, s \geq T_k^i\}$, until the stopping time T_{k+1}^i.

The **selection transition** $\xi_k \to \widehat{\xi}_k$ is defined as follows. From the N particles ξ_k^i only some of these have succeeded to reach the desired set A_k; we denote by I_k^N the set of their labels. If $I_k^N = \emptyset$, then none of the particles have succeeded to reach the desired region; the algorithm is stopped and $\widehat{\xi}_k = \Delta$. Otherwise, we draw N particles $\widehat{\xi}_k^i$ uniformly among the $|I_k^N|$ pieces of trajectories $\{\xi_k^i, i \in I_k^N\}$. Consequently, we obtain N independent random variables $\widehat{\xi}_k^i$ with common distribution

$$\Psi_k\left(\eta_k^N\right) = \sum_{i=1}^{N} \frac{g_k(\xi_k^i)}{\sum_{j=1}^{N} g_k(\xi_k^j)} \delta_{\xi_k^i},$$

$$= \frac{1}{|I_k^N|} \sum_{i \in I_k^N} \delta_{\xi_k^i}.$$

where

$$\eta_k^N = \frac{1}{N} \sum_{i=1}^{N} \delta_{\xi_k^i}.$$

An alternate scheme for the selection step, with less randomness in some sense, can be proposed. The key idea is to notice that the updating mapping Ψ_k can be rewritten in the following form

$$\Psi_k(\eta)(de') = (\eta \mathcal{S}_k(\eta))(dx') := \int \eta(de)\mathcal{S}_k(\eta)(e, de'),$$

where

$$\mathcal{S}_k(\eta)(e, de') = (1 - g_k(e))\Psi_k(\eta)(de') + g_k(e)\delta_e(de').$$

We easily verify that

$$(\eta \mathcal{S}_k(\eta))(f) = (1 - \eta(g_k))\Psi_k(\eta)(f) + \eta(fg_k) = \Psi_k(\eta)(f).$$

In this notation, (A.3.2) can be rewritten as

$$\eta_{k+1} = \eta_k \mathcal{K}_{k+1}(\eta_k),$$

with the composite Markov kernel $\mathcal{K}_{k+1}(\eta)$ defined by

$$\mathcal{K}_{k+1}(\eta)(e, de') = (\mathcal{S}_k(\eta)\mathcal{M}_{k+1})(e, de') = \int_E \mathcal{S}_k(\eta)(e, de'')\mathcal{M}(e'', de').$$

Note that the corresponding evolution equation is now decomposed into two separate transitions

$$\eta_k \xrightarrow{selection} \widehat{\eta}_k = \eta_k \mathcal{S}_k(\eta_k) \xrightarrow{mutation} \eta_{k+1} = \widehat{\eta}_k M_{k+1}, \tag{A.3.3}$$

In the alternative N-particle model associated with this new description each particle $\widehat{\xi}_k^i$ is sampled according to the selection distribution

$$\mathcal{S}_k\left(\eta_k^N\right)(\xi_k^i, de)$$
$$= 1_{\{X^i(T_k^i) \in B_k\}} \delta_{\xi_k^i}(de) + 1_{\{X^i(T_k^i) \notin B_k\}} \Psi_n\left(\eta_k^N\right)(de).$$

More precisely, if the i-th particle has reached the desired region, then we set $\widehat{\xi}_k^i = \xi_k^i$. In the opposite case, the particle has not reached the k-th region. In this case, $\widehat{\xi}_k^i$ is chosen randomly and uniformly in the set $\{\xi_k^j; j \in I_k^N\}$ of all excursions having entered into B_k. In other words, each particle that doesn't enter into the k-th level is killed, and instantly a different particle in the B_{k+1} level splits into two offsprings.

We denote by τ^N the lifetime of the N-particle algorithm, i.e. $\tau^N = \infty$ or τ^N is the first time all the particles are killed. For each $k < \tau^N$, the N-particle approximating measure γ_k^N defined by

$$\gamma_k^N(f) = \eta_k^N(f) \prod_{p=0}^{k-1} \eta_p^N(g_p),$$

when applied to the constant function 1 gives

$$\gamma_{k+1}^N(1) = \gamma_k^N(g_k) = \prod_{p=1}^{k} \frac{|I_p^N|}{N}.$$

Therefore, if $\tau^N > n$, we obtain the following approximation of the rare event probability

$$P_B = \mathbb{P}[T_B \leq T] = \gamma_n(1) \approx \gamma_n^N(1) = \prod_{p=1}^{n} \frac{|I_p^N|}{N}.$$

This estimator is unbiased and the central limit theorem applies [31]: as $N \to \infty$

$$\sqrt{N} \left(\frac{\gamma_n^N(1)}{P_B} - 1 \right) \Longrightarrow \mathcal{N}(0, \sigma_n^2),$$

where the asymptotic variance of the estimator is given by

$$\sigma_n^2 = \sum_{k=1}^{n} \left(\frac{1}{P_k} - 1 \right) + \sum_{k=1}^{n} \frac{1}{P_k} \frac{\mathrm{Var}_{\mu_k \circ \pi^{-1}}(\Delta_k^n)}{\mathbb{E}_{\mu_k \circ \pi^{-1}}^2(\Delta_k^n)},$$

for the first algorithm, and

$$\sigma_n^2 = \sum_{k=1}^{n} \left(\frac{1}{P_k} - 1 \right) + \sum_{k=1}^{n} \frac{1}{P_k} \frac{\mathrm{Var}_{\mu_k \circ \pi^{-1}}(\Delta_k^n)}{\mathbb{E}_{\mu_k \circ \pi^{-1}}^2(\Delta_k^n)} (1 - P_k^2),$$

for the alternate one, where

$$\Delta_k^n(t, x) = \mathbb{P}\left[T_B \leq T | T_k = t, X(T_k) = x \right].$$

In particular, if for each k the function Δ_k^n is constant, i.e. $\mathbb{P}\left[T_B \leq T | T_k, X(T_k) \right]$ does not depend on the hitting time and point of the level set A_k, given $T_k \leq T$, then the second right-hand term is null and the asymptotic variance reduces to the expression

$$\sigma_n^2 = \sum_{k=1}^{n} \left(\frac{1}{P_k} - 1 \right),$$

as given in [73]. Ideally, the level set A_k should be chosen such that the functions Δ_k^n are constant; even if this is clearly unrealistic for most practical problems, this observation gives an insight on how to choose them.

To see that the asymptotic variance is better than the one obtained with a crude Monte Carlo simulation, let us consider the simplified framework of a one dimensional Markov process and of a N-particle model in which all the probabilities P_k are equal to the same P. In this case, the asymptotic variance of the estimator is $nP_B^2(1 - P)/P$, whereas in naive Monte Carlo the variance of the estimator is $P_B(1 - P_B)$. It is also worth noting that the n factor does not mean that the variance increases with n, since for a given problem the rare event probability P_B is fixed. So $P \approx P_B^{1/n}$, and we have

$$n\frac{1 - P}{P} \approx n\exp\{-\frac{1}{n}\log P_B - 1\} \approx -\log P_B + \frac{1}{2n}\log^2 P_B + o(\frac{1}{n^2}),$$

which means that as $n \to \infty$, the variance is decreasing to $-P_B^2 \log P_B$.

Finally, let us mention the two adaptive algorithms [24, 74] developed to cope with the possible extinction of the particle system and the difficulty in determining the splitting levels at hand.

Bibliography

[1] D Aldous. *Probability Approximations via the Poisson Clumping Heuristic*, volume 77 of *Applied Mathematical Sciences*. Springer Verlag, 1989.

[2] J.W. Andrews, J.D. Welch, and H. Erzberger. Safety analysis for advanced separation concepts. In *Proceedings of USA/Europe ATM R&D Seminar*, Baltimore, MD, 27–30 June 2005.

[3] L. Arnold, P. Imkeller, and N. Sri Namachchivaya. The Asymptotic Stability of weakly perturbed two dimensional Hamiltonian Systems. In *Proceedings of the 18-th Biennal of Conference on Mechanical Vibration and Noise ASME Design Engineering Technical Conferences*, Pittsburgh, Pennsylvania, September 9-12 2001.

[4] B. G. J. Bakker, H. Kremer, and H. A. P Blom. Geometric and probabilistic approach towards conflict prediction in free flight, 1999.

[5] G.J. Bakker and H.A.P Blom. Air traffic collision risk modelling. In *Proceedings of the 32nd Conference on Decision and Control*, volume 2, pages 1464–1469, San Antonio, Texas, December 1993.

[6] H. A. P. Blom, G. J. Bakker, P. J. G. Blanker, J. Daams, M. H. C. Everdij, and M.B. Klompstra. Accident risk assessment for advanced atm. In *Proceedings of the 2nd U.S.A/Europe Air Traffic Management R&D seminar*, Orlando, December 1998.

[7] H. A. P. Blom and J. Lygeros, editors. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*. LNCIS series. Springer, Berlin, July 2006.

[8] H.A.P. Blom and G.J. Bakker. Conflict probability and incrossing probability in air traffic management. In *Proceedings IEEE Conference on Decision and Control*, pages 2421–2426, Las Vegas, NV, December 2002.

[9] H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij, and M.B. Klompstra. *Air Transport Systems Engineering*, chapter Accident risk assessment for advanced air traffic management, pages 463–480. AIAA, 2001.

[10] H.A.P. Blom, G.J. Bakker, M.H.C. Everdij, and M.N.J. van der Park. Collision risk modeling of air traffic. In *Proc. European Control Conf.*, Cambridge, UK, 2003.

[11] H.A.P. Blom, G.J. Bakker, B. Klein Obbink, and M.B. Klompstra. Free flight safety risk modelling and simulation. In *Proceedings of International Conference on Research in Air Transportation (ICRAT)*, Belgrade, 26–28 June 2006.

[12] H.A.P. Blom, K.M. Corker, and S.H. Stroeve. On the integration of human performance and collision risk simulation models of runway operation. In *Proceedings of the 6th USA/Europe Air Traffic Management R&D Seminar*, pages 27–30, Baltimore, MD, June 2005.

[13] H.A.P. Blom, J. Daams, and H.B. Nijhuis. *Air Transportation Systems Engineering*, volume 193 of *Progress in Astronautics and Aeronautics*, chapter Human cognition modeling in Air Traffic Management safety assessment, pages 481–511. 2001.

[14] H.A.P. Blom, M.B. Klompstra, and G.J. Bakker. Accident risk assessment of simultaneous converging instrument approaches. *Air Traffic Control Quarterly*, 11:123–155, 2003.

[15] H.A.P. Blom and S.H. Stroeve. Multi-agent situation awareness error evolution in air traffic. In *Proc. 7th Conference on Probabilistic Safety Assessment & Management*, Berlin, Germany, 2004.

[16] H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij, and M.N.J. Van der Park. Human cognition performance model to evaluate safe spacing in air traffic. *Human Factors and Aerospace Safety*, 2:59–82, 2003.

[17] M. L. Bujorianu. Extended stochastic hybrid systems. In O. Mahler and A. Pnuelli, editors, *Proceedings of Hybrid Systems Computation and Control*, LNCIS number 2993, pages 234–249, Berlin, 2004. Springer.

[18] M. L. Bujorianu and J. Lygeros. Reachability questions in piecewise deterministic markov processes. In O. Mahler and A. Pnuelli, editors, *Proceedings of Hybrid Systems Computation and Control*, LNCIS number 2623, pages 126–140, Berlin, 2003. Springer.

[19] M. L. Bujorianu and J. Lygeros. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Towards a general theory of stochastic hybrid systems, pages 3–30. LNCIS series. Springer, Berlin, 2006.

[20] L Burt. Results of route space calculations, progress report. Eurocontrol report NSSG/22-DP/5, Brussels, December, 1995.

[21] CAA. Outline of a method for the determination of separation standards for future air traffic systems. CAA paper 91010, DORA report 9111, CAA London, June 1991.

[22] C. G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, Boston, 1999.

[23] F. Cérou, P. Del Moral, F. Le Gland, and P. Lezaud. Limit theorems for the multilevel splitting algorithm in the simulation of rare events. In M.E. Kuhl, N.M. Steiger, F.B. Armstrong, and J.A. Joines, editors, *Proceedings of the 2005 Winter Simulation Conference*, Orlando, December 2005.

[24] F. Cérou and A. Guyader. Adaptive multilevel splitting for rare event analysis. To appear in Stochastic Analysis and its Applications, 2007.

[25] F. P. Cérou, P. Del Moral, F. Le Gland, and P. Lezaud. Genetic genealogical models in rare event analysis. Publications du Laboratoire de Statistiques et Probabilites, Toulouse III, 2002.

[26] S. Cohen and S. Hockaday. A Concept Paper for Separation Safety Modeling, an FAA/EUROCONTROL Cooperative Effort on Air Traffic Modeling for Separation Standards. FAA and EUROCONTROL, Brussels, May 1998.

[27] K. Corker. *Cognitive Engineering in the Aviation Domain*, chapter Cognitive Models & Control: Human & System Dynamics in Advanced Airspace Operations. Lawrence Earlbaum Associates, Hillsdale, New Jersey, 2000.

[28] R. David and H. Alla. Petri nets for the modeling of dynamic systems - a survey. *Automatica*, 30(2):175–202, 1994.

[29] M.H.A. Davis. *Markov models and optimization*. Chapman & Hall, London, 1993.

[30] E. De Santis, M. D. Di Benedetto, S. Di Gennaro, A. D. 'Innocenzo, and G. Pola. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Critical observability of a class of hybrid systems and application to air traffic management, pages 141–170. LNCIS series. Springer, Berlin, 2006.

[31] P. Del Moral. *Feynman-Kac Formulae. Genealogical and Interacting Particle Systems with Applications*. Probability and its Applications. Springer-Verlag, New York, 2004.

[32] P. Del Moral and P. Lezaud. Branching and interacting particle interpretation of rare event probabilities. In H. A. P. Blom and J. Lygeros, editors, *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, LNCIS series, pages 351–389. Springer-Verlag, Berlin, 2006.

[33] D. V. Dimarogonas, S. G. Loizou, and K. J. Kyriapoulos. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Multirobot navigation functions II: towards decentralization, pages 209–256. LNCIS series. Springer, Berlin, 2006.

[34] DNV. Safety assessment of P-RNAV route spacing and aircraft separation. Final report TRS 052/01, Eurocontrol, 2003.

[35] A. Doucet, N. de Freitas, and N. Gordon. *Sequential Monte Carlo Methods in Practice*. Springer-Verlag, 2001.

[36] M.R. Endsley. Towards a theory of situation awareness in dynamic systems. *Human Factors*, 37(1):32–64, 1995.

[37] H. Erzberger. Transforming the NAS: The next generation air traffic control system. In *Proceedings of the 24th Int. Congress of the Aeronautical Sciences (ICAS)*, Yokohoma, Japan, 2004.

[38] M. H. C. Everdij and H. A. P. Blom. Bias and uncertainty in accident risk assessment. NLR report CR-2002-137, National Aerospace Laboratory NLR, 2002.

[39] M. H. C. Everdij and H. A. P. Blom. *Analysis and design of hybrid systems*, chapter Petri-nets and hybrid-state Markov processes in a power-hierarchy of dependability models, pages 313–318. Elsevier, 2003.

[40] M. H. C. Everdij and H. A. P. Blom. Petri nets and hybrid state Markov processes in a power-hierarchy of dependability models. In *Proceedings of IFAC Conference on Analysis and Design of Hybrid Systems*, pages 355–360, Saint-Malo Brittany, France, June 2003.

[41] M. H. C. Everdij and H. A. P. Blom. Piecewise deterministic markov processes represented by dynamically coloured petri nets. *Stochastics*, 77:1–29, 2005.

[42] M. H. C. Everdij and H. A. P. Blom. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Hybrid Petri nets with diffusion that have into-mappings with generalised stochastic hybrid processes, pages 31–64. LNCIS series. Springer, Berlin, 2006.

[43] M. H. C. Everdij, H. A. P. Blom, and G. J. (Bert) Bakker. Modeling lateral spacing and separation for airborne separation assurance using petri nets. *Simulation, Transactions of the Society for Modeling and Simulation International*, 82, 2006.

[44] M. H. C. Everdij, H. A. P. Blom, and S. H. Stroeve. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. In *Proceedings of the 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8)*, New Orleans, LA, May 2006.

[45] M. H. C. Everdij, M. B. Klompstra, H. A. P. Blom, and B. Klein Obbink. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Compositional specification of a multi-agent system by stochastically and Dynamically Coloured Petri Nets, pages 325–350. LNCIS series. Springer, Berlin, 2006.

[46] FAA/Eurocontrol. A concept paper for separation safety modeling. Cooperative R&D Action Plan 3 report. Available at http://www.faa.gov/asd/ia-or/pdf/cpcomplete.pdf, 20 May 1998.

[47] FAA/Eurocontrol. Principles of operations for the use of asas. Cooperative R&D Action Plan 1 report, Version 7.1, 2001.

[48] FAA/Eurocontrol. Safety and asas applications. Co-operative R&D Action Plan 1 report, version 4.1, 2004.

[49] M.I. Freidlin and A.D. Wentzell. *Random perturbations of dynamical systems.* Springer-Verlag, New-York, 1984.

[50] P. Glasserman. *Monte Carlo methods in financial engineering*, volume 53 of *Stochastic Modeling and Applied Probability.* Springer, New York, NY, 2003.

[51] P.J. Haas. *Stochastic Petri Nets, Modeling, Stability, Simulation.* Springer-Verlag, New York, Simulation.

[52] J. Hoekstra. *Designing for Safety, the Free Flight Air Traffic Management concept.* PhD thesis, Delft University of Technology, November 2001.

[53] E Hoffman. Contribution to Aircraft Performance Modeling for ATC. *Air Traffic Control Quaterly*, 2(2):103 –130, 1994.

[54] D.A. Hsu. The evaluation of aircraft collision probabilities at intersecting air routes. *J. of Navigation*, 34:78–102, 1981.

[55] J. Hu, M. Prandini, and S. Sastry. Probabilistic safety analysis in three-dimensional aircraft flight. In *Proc. 42nd IEEE CDC*, Maui, USA, December 2003.

[56] ICAO. Review of the general concept separation panel. 6th meeting, 28 November-15 December, Montreal. Doc 9536, RGCSP/6 Volume1, December 1988.

[57] ICAO. Manual on airspace planning methodology for the determination of separation minima. ICAO Doc. 9689-AN/953, 1998.

[58] ICAO. Airborne separation assistance system (asas) circular. Draft, version 3, SCRSP, WGW/1 WP/5.0, International Civil Aviation Organization, May 2003.

[59] K. Jensen. *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use*, volume 1. Springer, London, UK, 1992.

[60] H.H. De Jong. Guidelines for the identification of hazards; how to make unimaginable hazards imaginable? National Aerospace Laboratory NLR, Contract report for Eurocontrol, NLR-CR-2004-094, 2004.

[61] I. Karatzas and S. Shreve. *Brownian Motion and Stochastic Calculus.* Springer, 2000.

[62] S. Karlin and H. Taylor. *A Second Course in Stochastic Processes.* Academic Press, New York, 1982.

[63] T. Kletz. *Hazop and Hazan; identifying and assessing process industry hazards.* The Institution of Chemical Engineers, 4th edition, 1999.

[64] J. Krozel. Free flight research issues and literature search. Under NASA contract NAS2-98005, 2000.

[65] J. Krystul and H. A. P. Blom. Monte Carlo simulation of rare events in hybrid system. Hybridge Report D8.3. Available at http://www.nlr.nl/public/hosted-sites/hybridge, June 2004.

[66] J. Krystul and H. A. P. Blom. Sequential Monte Carlo simulation of rare event probability in stochastic hybrid systems. In *Proceedings of the 16th IFAC World Congress*, Prague, Czech Republic, June 4-8 2005.

[67] J. Krystul and H. A. P. Blom. Sequential Monte Carlo simulation for the estimation of small reachability probabilities for stochastic hybrid systems. In *Proceedings of IEEE-EURASIP Int. Proceedings of IEEE-EURASIP Int. Symposium on Control, Communications and Signal Processing*, Marrakech, Morocco, March 13-15 2006.

[68] J. Krystul, H. A. P. Blom, and A. Bagchi. Stochastic hybrid processes as solutions to stochastic differential equations. In C. G. Cassandras and J. Lygeros, editors, *Stochastic Hybrid Systems: Recent Developments and Research Trends*. CRC Press, 2006.

[69] J. Krystul and H.A.P. Blom. Generalized stochastic hybrid processes as strong solutions of stochastic differential equations. Hybridge Report D2.3. `http://www.nlr.nl/public/hosted-sites/hybridge/`, June 2005.

[70] H. Kumamoto and E.J. Henley. *Probabilistic Risk Assessment and management for engineers and scientists*. IEEE Press, 1996.

[71] A. B. Kurzhanski and P. Varaiya. On reachability under uncertainty. *SIAM Journal on Control and Optimization*, 41:181–216, 2002.

[72] P. E. Labeau, C. Smidts, and S. Swaminathan. Dynamic reliability: Towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, 68:219–254, 2000.

[73] A. Lagnoux. Rare Events Simulation. *PEIS*, 20(01):45–66, January 2006.

[74] F. Le Gland and N. Oudjane. A sequential algorithm that keeps the particle system alive. In H. A. P. Blom and J. Lygeros, editors, *Stochastic Hybrid Systems : Theory and Safety Critical Applications*, LNCIS series, pages 351–400. Springer, Berlin, 2006.

[75] M. R. Leadbetter, G. Lindgren, and H. Rootzen. *Extremes and Related Properties of Random Sequences and Processes*. Springer-Verlag, New-York, 1983.

[76] A. Lecchini, W. Glover, J. Lygeros, and J. Maciejowski. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter Monte Carlo optimisation for conflcit resolution in air traffic control, pages 257–276. LNCIS series. Springer, Berlin, 2006.

[77] MFF. MFF Final safety case. Report MFF D734, ed. 1.0. Available at http://www.medff.it/public/index.asp, November 2005.

[78] NASA. Concept definition for distributed air-/ground traffic management (DAG-TM). Version 1.0, Advanced Air Transportation Technologies project, Aviation System Capacity Program, National Aeronautics and Space Administration, NASA, 1999.

[79] B. Klein Obbink. MFF airborne self separation assurance OSED. Report MFF R733D. Available at http://www.medff.it/public/index.asp, April 2005.

[80] R. A. Paielli and H. Erzberger. Conflict Probability Estimation For Free Flight. *AIAA Journal of Guidance, Control and Dynamics*, 20(3):588–596, 1997.

[81] G. Pola, M. Bujorianu, J. Lygeros, and M. D. Di Benedetto. Stochastic hybrid models: an overview with applications to air traffic management. In *Proceedings of IFAC Conf. Analysis and Design of Hybrid Systems (ADHS)*, Saint Malo, Brittany, France, 2003.

[82] M. Prandini and J. Hu. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, chapter A stochastic approxmation method for reachability computations, pages 107–139. LNCIS series. Springer, Berlin, 2006.

[83] M. Prandini and J. Hu. Stochastic reachability: Theory and numerical approximation. In C.G. Cassandras and J. Lygeros, editors, *Stochastic Hybrid Systems: Recent Developments and Research Trends*. CRC Press, 2006.

[84] M. Prandini, J. Hu, and S. Lygeros, J. amd Sastry. A probabilistic approach to aircarft conflict detection. *IEEE Tr. on Intelligent Transportation Systems*, 1(4):199–220, 2000.

[85] M. Prandini, J. Lygeros, A. Nilim, and S. Sastry. A Probabilistic Framework for Aircraft Conflict Detection. In *AIAA Guidance Navigation and Control Conference*, 1999.

[86] H. J. Rome and V. Krishnan. Causal probabilistic model for evaluating future transoceanic airline separation. In *IEEE Transactions on Aerospace and Electronics Systems*, volume 26, pages 804–817, September 1990.

[87] RTCA. Free Flight Implementation. Task Force 3 Final Technical Report, Washington DC, 1995.

[88] A. P. Shah, A. R. Pritchett, K. M. Feigh, S. A. Kalarev, A. Jadhav, K. M. Corker, D. M. Holl, and R. C. Bea. Analyzing air traffic management systems using agent-based modeling and simulation. In *Proceedings of the 6th USA/Europe Seminar on Air Traffic Management Research and Development*, Baltimore, MD, 27-30 June 2005.

[89] R. Sheperd, R. Cassell, R. Thava, and D. Lee. A reduced aircraft separation risk assessment model. In *Proceedings of the AIAA Guidance, Navigation and Control Conference*, AIAA, Reston, VA,, August 1997.

[90] S. H. Stroeve, H. A. P. Blom, and M. N. van der Park. Multi-agent situation aware-
ness error evolution in accident risk modeling. In *Proceedings of the 5th USA/Europe
Seminar on Air Traffic Management Research and Development*, Budapest, Hun-
gary, 23-27 June 2003.

[91] O. Strter, V. Dang, B. Kaufer, and A. Daniels. On the way to assess errors of
commission. *Reliability Engineering and System Safety*, 83:129–138, 2004.