Risk Analysis and Safety Assessment of Air Traffic Control System

Model of Airborne Collision Avoidance System Operation for Safety Assessment of Air Traffic Control Operational Concepts

Doctoral Thesis

July 2010.
Members of the Committee for evaluation and defense of the doctoral thesis:

Dr Vojin Tošić, Professor at the Faculty of Transport and Traffic Engineering, University of Belgrade, Thesis Advisor

Dr Obrad Babić, Professor at the Faculty of Transport and Traffic Engineering, University of Belgrade

Dr Mirko Vujošević, Professor at the Faculty of Organizational Sciences, University of Belgrade

Dr Milan Janić, Senior Researcher at the Section: Transport & Infrastructure, OTB Research Institute for the Built Environment, Delft University of Technology, Delft, The Netherlands, and Research Professor (Faculty of Transport and Traffic Engineering, University of Belgrade)

Dr Henk Blom, Principal Scientist at the National Aerospace Laboratory NLR, Air Transport Safety Institute, Amsterdam, the Netherlands.

Public defense

July 20, 2010 at 13:00, Faculty of Transport and Traffic Engineering, University of Belgrade, Belgrade, Serbia
This research has been conducted with support from the “RESET - Reduced Separation Minima” project commissioned by European Commission DG TREN under the FP6 Program (2006-2010) and the “Methods for Evaluation of Development Scenarios of the Air Transport System in Serbia (airlines, airports, ATC) - Safety, Efficiency, Economic and Environmental Aspects” project, commissioned by the Ministry of Science and Technological Development of the Republic of Serbia, under the Program for Research in Technology Development in the period 2008-2011.
I dedicate this dissertation to my father
Tomislav Netjasov (March 06, 1953 – October 11, 2006)
who would be proud to see me defending it.
ACKNOWLEDGMENTS

I am indebted to Prof. Vojin Tošić, my teacher and supervisor, who recognised my interests in air traffic safety and who created the opportunity for me to accomplish this research over the years. Especially I’m grateful for his patience and effort in guiding me and for all knowledge he has transferred to me. Also, I am grateful to Prof. Obrad Babić who supported me and this idea from the very beginning.

My foray into air traffic safety started in 2005, when with the selfless help of Prof. Tošić my visit to the Netherlands was organized. The three months collaboration with the National Airspace Laboratory (NLR) in Amsterdam, and Delft University of Technology (TU Delft) in Delft, started at the beginning of 2006. My visit was sponsored by the Division of Airports and Air Traffic Safety (APATC), Faculty of Traffic and Transport Engineering, University of Belgrade, and was approved and hosted by Dr Henk Blom, Principal Scientist at the NLR Air Traffic Safety Institute (ATSI) and Dr Milan Janić, Senior Researcher at the OTB Research Institute for Housing, Urban and Mobility Studies at the TU Delft. I would like to express my gratitude to all of them.

During my stay at TU Delft I learned a lot about research in general and about the fundamentals of risk and safety in air traffic from numerous and long-lasting discussions with Dr Janić. At NLR Dr Blom and his colleagues helped me to understand Petri Nets and to learn about TOPAZ (Traffic Organizer and Perturbation Analyzer) methodology. Later on in 2006, Dr Blom introduced APATC in pan-European project RESET, making it possible for me to work on this dissertation. He carefully followed and evaluated my work on this thesis during the project. My gratitude also goes to Ms. Mariken Everdij, from NLR ATSI, who helped me to better understand the details of Stochastically and Dynamically Coloured Petri Nets (SDCPN) and evaluated my work during the project.

For the validation of the developed model, I am very grateful to Mr. Garfield Dean from the EUROCONTROL Experimental Centre, Bretigny-sur-Orge, France, who provided the InCAS Version 2.6 software as well as some necessary documentation. Also, my gratitude goes to Prof. Peter Form and Jens Gottstein (PhD Student) from the Institut für Eisenbahnwesen und Verkehrssicherung, TU Braunschweig, Braunschweig, Germany for providing real life TCAS encounters data, without which the validation of my research would not be meaningful.

I am also very grateful to my colleague Mr. Andrija Vidosavljević, PhD student at APATC, who worked together with me on the RESET project and who performed the necessary programming for the purpose of my research and patiently reviewed many versions of my reports. Finally, I wish to thank all my current and former colleagues from APATC, especially to my officemates Ms. Tatjana Krstić-Simić and Ms. Bojana Mirković.

I owe my family gratitude for their full support and understanding.

Fedja Netjasov

Belgrade, 2010.
SUMMARY

Existing international regulations and policies in the field of air transport do not consider the effect of an airborne safety net in the analysis of safety risks. This widely accepted practice tends to create significant tension between the realization of the ambitious safety improvement targets of SESAR and NextGen, and the current regulations. In order to close this gap there is need for the systematic development of risk and safety assessment of airborne safety nets within the specific Air Traffic Control/Management (ATC/ATM) context, which may range from current practices to advanced ATC/ATM concepts.

The aim of the research described in this dissertation is to make a contribution through the systematic development of an unambiguous model of ACAS operations, i.e. TCAS II version 7, together with its interactions with pilots and air traffic controllers. The model is intended for risk/safety assessment of ACAS operations, which would allow for the assessment of the possible benefit of ACAS in risk reduction in current and advanced ATC/ATM.

The specific modelling formalism used for this purpose is Stochastically and Dynamically Coloured Petri Nets (SDCPN). It was shown that the SDCPN representation is very powerful and allows the modeller to represent all elements of such a complex system (technical elements, pilots, air traffic controllers, procedures in force), dynamical and stochastic system, as well as interactions between them, in a flexible and modular way. The model is built in a way to be easily added to certain previously developed SDCPN model of existing or future operational concept, enabling for the assessment of the possible benefit of the safety net in it. The model also could be used as standalone.

The fact that the model is stochastic and dynamic enables its use in Monte Carlo simulation of rare events such as aircraft collisions, repeating the experiments many times (order of magnitude $10^{10}$) and tracing back in order to determine the chain of events leading to collision. However, in this research this kind of application, i.e. risk assessment itself was not performed.

Apart from model development, attention was given to model validation in order to build a confidence in the model and to use it as a credible tool for safety assessment purposes of current and future ATM operational concepts. A validation process is proposed in this research and is applied to historical data, in which a set of different real life encounters were compared to simulation outputs of the developed SDCPN-based model. Although the number of real life encounters was not great, this kind of validation was very valuable due to the fact that it is rarely made for such a kind of models. It was concluded that the developed model could be used for the intended purpose, i.e. as part of the models for the risk/safety assessment of operational concepts, although only the first two levels of validation (of proposed four) were evaluated as satisfactory.

The model application is illustrated on a real life accident. Namely, a collision between Inex Adria DC9 and British Airways Trident 3, which occurred on September 10, 1976, over VOR Zagreb (former Yugoslavia) at FL330. ACAS was not in use at the time of collision. The SDCPN model is demonstrated to work well - if TCAS II had existed at the time of the accidents, it could have prevented a collision.

Further research steps are proposed. The developed SDCPN-based model should be applied as standalone in certain characteristic cases (encounters) for risk/safety assessment with the aim of estimating possible benefit of risk reduction in airborne safety nets. Additionally, further improvement of TCAS SDCPN-based model and Conceptual model of TCAS Logic should be considered. Finally, the developed model should be integrated with broader models for risk and safety assessment of existing or future operational concepts, which would show the full benefit of airborne safety nets.
CONTENTS

ACKNOWLEDGMENTS ......................................................................................................................... ix
SUMMARY ............................................................................................................................................. xi
GLOSSARY OF TERMS ........................................................................................................................ xiv

1 INTRODUCTION ................................................................................................................................. 1

2 AIR TRAFFIC CONTROL AND SAFETY ......................................................................................... 3
  2.1 Air Traffic Control and Safety Assessment ................................................................................... 3
  2.2 Target Level of Safety ...................................................................................................................... 3
  2.3 Safety Nets .................................................................................................................................... 4
  2.4 Aircraft Separation and Safety ......................................................................................................... 6

3 OBJECTIVE OF THE RESEARCH .................................................................................................... 7
  3.1 Literature Survey ........................................................................................................................... 7
  3.2 Research Objective ......................................................................................................................... 8
  3.3 TOPAZ Methodology ...................................................................................................................... 8

4 DESCRIPTION OF THE TRAFFIC ALERT AND COLLISION AVOIDANCE SYSTEM .......... 11
  4.1 Components of TCAS .................................................................................................................. 12
  4.2 TCAS Functions ........................................................................................................................... 14
  4.3 Collision Avoidance Concepts and Functions ............................................................................... 16

5 MODEL OF TCAS OPERATIONS IN AIR TRAFFIC CONTROL .................................................... 19
  5.1 Operational use of TCAS II Version 7: Brief Description and Human Roles ............................... 19
  5.2 Conceptual Model of TCAS II Version 7 Logic ........................................................................... 20
    5.2.1 Threat Detection Algorithms ................................................................................................. 22
    5.2.2 Threat Resolution Algorithm ............................................................................................... 25
    5.2.3 Clear of Conflict Annunciation ............................................................................................ 27
  5.3 Hazards Identified ......................................................................................................................... 28
  5.4 Agents and Local Petri Nets for Operational use of TCAS II version 7 ....................................... 30
  5.5 Specification of Local Petri Nets .................................................................................................... 32
    5.6 Local Petri Nets vs. Agents ......................................................................................................... 33
      5.6.1 Own Aircraft as Agent .......................................................................................................... 34
      5.6.2 Intruder Aircraft as Agent .................................................................................................... 35
      5.6.3 Own Aircraft Crew as Agent ............................................................................................... 35
      5.6.4 Air/Ground Communication Link as Agent ......................................................................... 35
      5.6.5 Tactical Air Traffic Controller (ATCo) as Agent ................................................................. 36
  5.6.6 Intruder Aircraft as Agent .................................................................................................... 34

6 VALIDATION OF MODEL OF TCAS OPERATIONS ...................................................................... 37
  6.1 Definition and Principles of Validation ......................................................................................... 37
  6.2 Validation Process ........................................................................................................................ 38
    6.2.1 Level 1 - Is TCAS activated? .................................................................................................. 39
    6.2.2 Level 2 - Are the same TCAS events occurring? .................................................................. 40
    6.2.3 Level 3 - If RA occurs, is resolution manoeuvre similar? ....................................................... 40
    6.2.4 Level 4 - Are corresponding horizontal and vertical separations at CPA great enough following implementation of the issued RA? .............................................................................. 41
    6.2.5 Criteria for passing to the next validation level ..................................................................... 41
  6.3 Historical Data Validation .............................................................................................................. 42
    6.3.1 Real Life Encounter Data ..................................................................................................... 42
    6.3.2 Validation of TCAS SDCPN model vs. Real Life Encounters data ......................................... 42

7 ILLUSTRATION OF THE MODEL APPLICATION ......................................................................... 49
  7.1 Event Validity ............................................................................................................................... 49
  7.2 Illustration .................................................................................................................................... 55

8 CONCLUSION ..................................................................................................................................... 57
# Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACAS</td>
<td>Airborne Collision Avoidance System</td>
</tr>
<tr>
<td>ALIM</td>
<td>Altitude Limit</td>
</tr>
<tr>
<td>ALS</td>
<td>Achieved (actual) level of Safety</td>
</tr>
<tr>
<td>ASARP</td>
<td>ACAS Safety Analysis post-RVSM Project</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATCo</td>
<td>Air Traffic Controller</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>CA</td>
<td>Collision Avoidance</td>
</tr>
<tr>
<td>CAS</td>
<td>Collision Avoidance System</td>
</tr>
<tr>
<td>CDTI</td>
<td>Cockpit Display of Traffic Information</td>
</tr>
<tr>
<td>CoC</td>
<td>Clear of Conflict</td>
</tr>
<tr>
<td>CPA</td>
<td>Closest Point of Approach</td>
</tr>
<tr>
<td>DMOD</td>
<td>Distance Modification</td>
</tr>
<tr>
<td>IAPA</td>
<td>Implications on ACAS Performances due to ASAS implementation</td>
</tr>
<tr>
<td>I-AM-SAFE</td>
<td>IAPA – ASARP Methodology for Safety net Assessment</td>
</tr>
<tr>
<td>InCAS</td>
<td>Interactive Collision Avoidance Simulator</td>
</tr>
<tr>
<td>IPN</td>
<td>Interaction Petri net</td>
</tr>
<tr>
<td>LPN</td>
<td>Local Petri Net</td>
</tr>
<tr>
<td>PF</td>
<td>Pilot Flying</td>
</tr>
<tr>
<td>PNF</td>
<td>Pilot Not Flying</td>
</tr>
<tr>
<td>RA</td>
<td>Resolution Advisory</td>
</tr>
<tr>
<td>SDCPN</td>
<td>Stochastically and Dynamically Coloured Petri Nets</td>
</tr>
<tr>
<td>SL</td>
<td>Sensitivity Level</td>
</tr>
<tr>
<td>STCA</td>
<td>Short Term Conflict Alert</td>
</tr>
<tr>
<td>TA</td>
<td>Traffic Alert</td>
</tr>
<tr>
<td>TLS</td>
<td>Target level of Safety</td>
</tr>
<tr>
<td>TCAS</td>
<td>Traffic alert and Collision Avoidance System</td>
</tr>
<tr>
<td>TMA</td>
<td>Terminal Control Area</td>
</tr>
<tr>
<td>TOPAZ</td>
<td>Traffic Organization and Perturbation AnalyZer</td>
</tr>
<tr>
<td>VOR</td>
<td>Very High Frequency Omni Range Navigation Aid</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

Air Transport is generally growing despite constraints, such as the world economic crisis, but its further increase is expected with an average annual rate of about 4-5% (SESAR, 2006). The increase of air traffic volume in Europe 2020 is forecasted in European Commission (EC) document Vision 2020 (OOPEC, 2001) and The Challenge of Safety (ACARE, 2002) to be up to three times greater relative to the year 2000. At the same time, a higher level of safety is required through a fivefold reduction of accident rates and a significant decrease in human error (OOPEC, 2001). The abovementioned documents were used by the EC as a base for the definition of Single European Sky Air Traffic Management Research (SESAR) initiative, whose role is to define the future of the European Air Traffic Management system (SESAR, 2006).

The facts mentioned in the abovementioned documents are conflicting by nature and present a great challenge for the research and scientific community because an increase in traffic should not lead to a decrease in safety. According to Vision 2020, the development of new operational concepts in air traffic system is planned, as well as development of safety measures and system safety performance indicators.

The Air Traffic Management (ATM) system, whose main task is to enable safe air traffic, should satisfy the mentioned ambitious goals. The basic problem of the ATM system is lack of capacity that would cope with growing air traffic demand. One of many possible solutions for the capacity issue is to change aircraft separation rules, while enhancing the communication, navigation and surveillance (CNS) system. The sharing of separation responsibility between air traffic controllers (ATCos) and pilots is also one of the possible solutions. Important parts of the ATM system are the airborne and ground-based safety nets, which both present a last defence against mid-air collisions, among other things.

Possible changes in the ATM system influence safety. Certain questions arise: Are the proposed solutions valid from a safety point of view? How to assess the level of safety? How to choose the best possible solution? Therefore, for any change in an ATM system prior to operational use, there is a need to perform a safety assessment in order to see whether this change satisfies the given safety criteria.

Due to the fact that separation minima reductions as well as share of separation responsibility are seen as promising solutions for the capacity problem, the role of airborne safety nets is becoming very important. According to Brooker (2004a, 2005), current ICAO risk/safety assessment policy is restrictive relative to ACAS in the sense that maximum values for mid-air collision risks are defined under the explicit assumption that the effect of an airborne safety net is not considered. This is also the case with Eurocontrol policy, which states that safety nets in general (both airborne and ground) should not be taken into account in the risk/safety assessment process (Brooker 2004a, 2005).

In view of the SESAR and USA NextGEN programme objectives of increasing both capacity and safety there simply is a need to conduct safety risk analysis of new operations, including ACAS. And this need exists, even when the inclusion of ACAS in safety regulation would not be taken up. An example is the Airborne Separation Assurance System (ASAS), as one of the new concepts whose interaction with ACAS, has proven to be important from both the procedural and the human factor aspects (Abeloos et al, 2000; Ivanescu et al, 2004; de Oliveira et al, 2007; Blom et al, 2007, 2008). These examples clearly show that the only way to include ACAS in the safety assessment process is through the modelling of ACAS operations.
The aim of the research described in this paper is to develop a model for risk/safety assessment of ACAS operations which would allow for the assessment of the possible benefit of ACAS in risk reduction in current and advanced ATMs. In view of this objective, the specific modelling framework used in this research is the Stochastically and Dynamically Coloured Petri Net (SDCPN) modelling formalism. The SDCPN formalism makes it possible to model a complex distributed operation in a systematic and compositional way (Everdij et al, 2006), and at the same time it brings powerful analysis frameworks within reach (Everdij and Blom, 2008) and is fully embedded in the advanced safety risk assessment methodology TOPAZ (Everdij and Blom, 2003, 2005a, 2005b).

Apart from the Introductory Chapter, this dissertation contains the following chapters. In the second Chapter an ATC/ATM system is briefly described from the capacity and safety increase point of view. A special place is provided for the description of “safety nets” which are intended to increase the system safety as well as the “target level of safety” concept representing the safety criteria that new or modified ATC/ATM system should satisfy.

The third chapter describes the development of a quantitative accident risk assessment model for the Airborne Collision Avoidance System (ACAS) operation in ATC/ATM. This chapter explains the development of an ACAS model using the SDCPN formalism. This ACAS model covers the TCAS II version 7 technical system, as well as the pilots, the ATCo, certain other relevant equipment and the interactions between these model entities. In order to avoid repetition of modelling specification, a detailed specification containing the description of Petri Nets is given in the Appendix, together with the list of modelling assumptions as well as an explanation of how and where the hazards are covered in the Petri Net model.

The forth chapter describes Validation process for the developed SDCPN-based model of ACAS Operation in ATMs. A validation process containing four levels is proposed in this research. After each level there is a possibility to pass on the following validation level or to improve the existing model. The validation is performed using real life TCAS events (historical data) for comparison. This kind of validation is highly valuable due to the fact that it is rarely is performed for such models.

The fifth chapter presents an illustration of developed model application. A real life accident is used for illustration. Namely, the collision between Inex Adria DC9 and British Airways Trident 3, which occurred on September 10, 1976 over VOR Zagreb (former Yugoslavia) at FL330. TCAS was not in use at the time of the collision. It was shown that if TCAS II would have existed at the time of the accident, it could have prevented a collision.

The sixth chapter draws some final conclusions and defines some further research steps.
2 AIR TRAFFIC CONTROL AND SAFETY

Air Traffic Management System (ATM), as defined by ICAO, is intended for “dynamic, integrated management of air traffic and airspace in a safe, economic and efficient way” (SESAR, 2006).

ATM consists of the Air Traffic Control system (ATC), the Air Space Management System (ASM) and the Air Traffic Flow Management System (ATFM). The core of the ATM system consists of Communication, Navigation and Surveillance Systems (CNS). Existing ATM systems are based on ground-based systems usage, although much information and functionality also exists in airborne systems which could be used for the improvement of performance of existing and future ATM systems (SESAR, 2006).

The ATM systems contain technologies and procedures enabling maximization of capacity and safety of system resources (airports and airspace) while simultaneously minimizing delay and operational costs (Whelan, 2001). The tendency to increase capacity could jeopardize safety. Therefore, without new technologies, operational procedures and corresponding regulations, it is not possible to increase capacity without decreasing system safety.

Further growth of demand required new changes in ATM system. These changes led to further system evolution, i.e. to synchronized change of procedures, pilot and ATCo working methods, airborne and ground systems, legislative and regulatory frameworks and aeronautical data sources.

Presently, two ongoing programmes define the future of ATC/ATM systems. One is a Europe’s SESAR - Single European Sky Air Traffic Management Research, and other one is USA’s NextGEN – Next Generation Air Transport System. The main goal of both programmes is to increase system capacity cost-effectively, while ensuring safety (Brooker, 2008). The common vision is to integrate and implement new technologies to improve ATM performance. Both they combine increased automation with new procedures to achieve safety, economics, capacity, environmental and security benefits (Brooker, 2008).

2.1 Air Traffic Control and Safety Assessment

System evolution could be realized through maintenance, modernization (renewal of large system elements) or complete system replacement. However, whenever changes are made, no matter what was the driving force, it should be demonstrated that they satisfy existing safety criteria, usually expressed as target level of safety (Blom et al, 1998). This is especially important in situations when new, previously nonexistent technologies, procedures or operational concepts are introduced. Satisfaction of safety criteria is demonstrated through the safety assessment process which usually provides a safety feed-back to system or concept designers. If the proposed change does not satisfy the given safety criteria, it should then be re-designed or even withdrawn.

2.2 Target Level of Safety

The fundamental quantitative concept of ATC/ATM systems is target level of safety - TLS (Target Level of Safety), i.e. the “acceptable” accident rate. TLS presents a design limitation, i.e. predefined level of risk that the system should satisfy (achieve).
It is usually expressed as number of fatal accidents per flight hour, although other indicators could be used (number of fatal accidents or number of casualties per year, flown mile, number of passengers, passenger hour, etc. (Brooker, 2004a, 2005)).

This concept is very important because it considers all the changes that could appear in the ATC/ATM system. Namely, if a new system is being designed or an existing system is being modified, it is necessary to assess (estimate) the level of risk in such a new system and make a comparison with given TLS. The actual, i.e. achieved level of safety (ALS) in a new system should be less then or equal to the given TLS in order to allow application of a new system in an operational environment.

2.3 Safety Nets

Apart from the evolution of ATC/ATM systems towards an increase in system safety and capacity, which was mainly related to technological innovations in the communication, navigation and surveillance part of the ATC/ATM system, special attention is given to the development and application of airborne and ground systems, representing the last-resort means of reducing the risk of mid-air collision (MAC) between aircraft, aimed at warning pilots and air traffic controllers of potentially dangerous (hazard) situations and at helping them resolve these situations. These types of systems are known as “safety nets” and they are basically intended to increase pilot and air traffic controller situational awareness, and significantly enhance air traffic safety.

Eurocontrol’s Safety Regulation Commission (SRC) defines “safety nets” as airborne or ground-based systems designed exclusively for collision avoidance between aircraft, aircraft and other objects or ground (terrain) (SRC, 2000) which alert controllers or pilots to potentially hazardous situations in an effective manner and with sufficient warning time for the situation to be resolved.

Airborne Collision Avoidance Systems (ACAS) constitute a world-wide accepted last-resort means of reducing the risk of mid-air collision (MAC) between aircraft (ICAO Annex 10, Brooker, 2005). Currently, the only commercially available implementation of ICAO standard for ACAS II is TCAS II version 7.0 (Traffic alert and Collision Avoidance System).

TCAS is intended to provide last-minute collision avoidance guidance directly to the flight crew (Kuchar and Drumm, 2007) instructing them to climb or descent the aircraft (resolution advisory - RA) in order to resolve the conflict situation. Hence, TCAS constitutes the last layer in the multi-layered defence against MAC, with all other layers typically belonging to ground based ATM. Apart from TCAS II, also in existence is TCAS I whose role is to warn pilots of the presence of other aircraft in the vicinity of their aircraft (traffic advisory - TA).

Although recent accidents (Überlingen, Germany, 2002; Amazon jungle, Brazil 2006) show that the current ACAS is not perfect, there are many more known examples where ACAS made a positive difference (e.g. for Europe, ACAS is estimated to reduce the risk of mid-air collision by a factor of about 5, i.e. a risk ratio of 22%\(^1\). In reality, an average of 3 ACAS-interventions per day, or one per 5000 flight hours of ACAS-equipped aircraft, is recorded in Germany (Gottstein, Form, 2009)).

TCAS as a safety net has existed as a mandatory element since 2000 (in certain regions of the world, see Table 1).

Table 1. World regions where TCAS II is mandatory (compiled from (Whelan, 2001))

<table>
<thead>
<tr>
<th>Jurisdiction (Agency)</th>
<th>Classification of aircraft</th>
<th>TCAS mode</th>
<th>Date of mandate</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (FAA)</td>
<td>All commercial turbine-powered transport aircraft with more than 30 passenger seats (or MTOW above 15000kg)</td>
<td>TCAS II</td>
<td>1 January, 1993</td>
</tr>
<tr>
<td>Europe (EASA)</td>
<td>All commercial turbine-powered transport aircraft with more than 30 passenger seats (or MTOW above 15000kg)</td>
<td>TCAS II</td>
<td>1 January, 2000</td>
</tr>
<tr>
<td>Europe (EASA)</td>
<td>All commercial turbine powered transport aircraft with more than 19 passenger seats (or MTOW above 5700kg)</td>
<td>ACAS II (Effectively TCAS II Version 7.0)</td>
<td>1 January, 2005</td>
</tr>
<tr>
<td>Australia (CASA)</td>
<td>All commercial turbine powered transport aircraft with more than 30 passenger seats (or MTOW above 15000kg)</td>
<td>TCAS II</td>
<td>1 January, 2000</td>
</tr>
<tr>
<td>Hong Kong, China (Civil Aviation Department)</td>
<td>All aircraft in Hong Kong with more than 19 passenger seats (or MTOW greater than 5700kg)</td>
<td>TCAS II Version 7.0</td>
<td>1 January, 2000</td>
</tr>
<tr>
<td>Brazil (National Civil Aviation Agency)</td>
<td>All aircraft with more than 19 passenger seats (or MTOW greater than 5700kg)</td>
<td>TCAS II</td>
<td>28 January, 2005</td>
</tr>
</tbody>
</table>

An important issue related to safety nets is their consideration during the process of determining TLS for a given system in existing international regulations. Namely, TLS is determined relative to all risks which the aircraft could be exposed to, so it depends on the entire system, i.e. all failure types, mechanical, procedural or human that generate collision risk should be considered (Brooker, 2004a). However, current ICAO TLS philosophy does not consider safety nets as a part of the entire system (Brooker, 2005).

Similarly, the Safety Regulatory Commission (SRC) of Eurocontrol in its regulation requires that for a certain system, where a certain change is carried out or some new technology is applied, the given TLS should be satisfied without the use of safety nets (SRC, 2000; Brooker, 2004a), since every safety benefit resulting from the application of safety nets is an additional safety benefit resulting from the ATC/ATM system. Brooker in his paper (Brooker, 2004a) criticizes such an approach by the SRC as being non-rational and inconsistent with the definition of the TLS and the entire ATM system, i.e. that safety nets represent an integral part of ATM systems. According to Brooker (2004a), a revision of current regulations regarding the definition of TLS values is necessary in order for it to be applicable to all system changes that could have an influence on safety.
2.4 Aircraft Separation and Safety

The paramount goal of ATC/ATM systems is to provide safe air traffic. In order to fulfil this goal ATC services separate aircraft during flight. Separation is very important because it influences airspace capacity, i.e. it is recognized as a fundamental capacity constraint (Reynolds and Hansman, 2001). In existing (centralized) ATC systems, ATCos are responsible for maintaining separation between aircraft. However, there is a tendency to delegate the separation responsibility to pilots, i.e. to share the separation responsibility between ATCos and pilots. The foundation for that is the development of future ATC/ATM systems as well as new “safety nets”.

The basic mechanism used in ATC in order to maintain safety is application of separation minima. It is assumed that factors influencing separation minima also have influence safety. Namely, greater accuracy of aircraft position and greater aircraft position update rate allow for the application of smaller separation minima as well as greater safety of the system, i.e. reduction of collision risk.
3 OBJECTIVE OF THE RESEARCH

3.1 Literature Survey

A Review of the Research on Risk and Safety Modelling in Civil Aviation has been performed (Netjasov, Janic 2008a, 2008b, see Appendix 1). Four categories of models are identified: causal methods/models for risk and safety assessment of aircraft and ATC/ATM operations, collision risk methods/models, human factor error methods/models, and third-party risk methods/models.

These are aimed at increasing system capacity, on the one hand, and reducing acceptable risk and safety thresholds on the other. In many cases, the need for developing “specialized” or “dedicated” methods/models for particular parts of the system have been ascertained. Furthermore, difficulties such as the lack of real-life data have been overcome by including expert judgment despite awareness of its uncertainty and biases.

The main findings have provided insight into the efforts already carried out in developing these methods/models, their inherent complexity and lack of sufficient flexibility, lack of the available data for calibration and testing, and lack of the sufficient prediction capabilities enabling easier application to the assessment of risk and safety of new technological, procedural and operational concepts.

Also, it was found that among the numerous risk and safety assessment methods/models ACAS operations were not specifically considered, especially not as part of existing and future ATC/ATM operational concepts.

Modelling of ACAS operations has been the subject of research since the introduction of TCAS. Many different modelling approaches with different needs have since been identified:

a) Several approaches have emerged for verification i.e. formal analysis of complex safety-critical systems such as TCAS: Finite State Machine approach (Leveson et al, 1994), State Charts (RTCA, 1997), and Hybrid Automata (Livadas et al, 1999).

b) In order to understand human behaviour related to TCAS, causal analysis (Ladkin, 2004), and timed knowledge-based modelling and analysis (Küster-Filipe et al, 2003), are applied.

c) Finally, the necessity to examine ACAS safety is followed by development of encounter models based on Fault Tree Analysis coupled with the Monte Carlo Simulation (Kuchar, 2005), and by Markov processes coupled with Bayesian networks (Kochenderfer 2008, 2009).

Apart from the mentioned models, an Interactive Collision Avoidance System (InCAS) simulator was developed (GAIN, 2003; EEC, 2005) in order to replay and analyse ACAS related incidents and to learn from encounters; and a tool called Replay Interface for TCAS Alerts (RITA) was developed for ACAS training of air traffic controllers and pilots (GAIN, 2003).
3.2 Research Objective

In view of the SESAR and NEXTGEN objectives of increasing both capacity and safety (advances in ATM may have significant impact on the effective performance of ACAS) there simply is a need to conduct safety risk analyses of new operations, including safety nets. This need also exists, even when the inclusion of safety nets in safety regulation would not be taken up. Taking into account that safety nets are represent integral part of ATM systems (Brooker, 2004a) then the only way to include it in the safety assessment process is through the modelling of their operation. Also, it was found that among numerous risk and safety assessment methods/models safety net operations were not specifically considered, especially not as part of existing and future ATC/ATM operational concepts.

Considering the abovementioned mentioned facts, the aim of the research described in this dissertation is to develop a model for risk/safety assessment of ACAS operations that would allow for the assessment of the possible benefit of ACAS as airborne safety net in risk reduction for current and advanced ATM operation. Also, the aim was to model ACAS in a way that would be easy to insert into broader models concerning safety assessment of current and advanced ATM operations, or to be used as a standalone model.

In view of this objective, the specific modelling framework used in this research is the Stochastically and Dynamically Coloured Petri Net (SDCPN) modelling formalism. Once a proper ACAS model in terms of SDCPN formalism is developed, this can easily be incorporated into the modelling of current and advanced ATM operations that also uses the SDCPN formalism.

The main reason for using SDCPN is the possibility of modelling complex relations existing between different system elements (humans, procedures, equipment) in a dynamic and stochastic way, as well as the possibility of easily determining the causes or contributing factors of non-nominal system behaviour or accidents.

The SDCPN formalism makes it possible to model a complex distributed operation in a systematic and compositional way (Everdij et al, 2006), while at the same time bringing powerful analysis frameworks within reach (Everdij and Blom, 2008) and full embedding in advanced safety risk assessment methodology TOPAZ - Traffic Organization and Perturbation Analyzer (Everdij and Blom, 2003, 2005a, 2005b).

Previous experience using Petri Nets for safety analysis (Leveson and Stolzy, 1987) as well as Dynamically Coloured Petri Net (DCPN) for aviation purposes (Shortle et al, 2004; Everdij et al, 2007; Netjasov and Janic, 2008b) also supports this choice.

3.3 TOPAZ Methodology

TOPAZ Methodology consists of several stages (Figure 1). Each stage contains several other sub-stages internally inter-related. Inter-relation also exists between different stages (de Oliveira et al, 2006).

Stage 1 - Identification of operation and hazards

This stage contains three interrelated sub-stages (Figure 1). This stage should describe the time horizon and the operational and physical boundaries of the Air Traffic Management

8
TOPAZ Methodology

(ATA) scenario under consideration. Also, traffic flow characteristics, available statistical data, human responsibilities, operational procedures and the functioning of the technical systems (that are part of the ATM scenario) should be identified, assuming normal working condition within the mentioned boundaries. Based on that, a high level description of the ATM environment is developed, depicting it through sub-systems and sub-processes, represented by modules and the information flows between them. Also, Stage 1 includes the identification of encounter type(s) (for which TOPAZ evaluations are executed and the separation criteria is evaluated) and identification of lists of hazards that might compromise safety.

Figure 1. TOPAZ Methodology stages (de Oliveira et al, 2006)
Stage 2 - Development of mathematical model

This stage contains five interrelated sub-stages (Figure 1) explaining the instantiation² of Stochastically and Dynamically Coloured Petri Nets (SDCPN) and decomposition of the collision risk. In Figure 1, it can be seen that some sub-stages in Stage 2 are dependant on sub-stages from Stage 1. The SDCPN model, instantiated in this stage for a given scenario, consists of Local Petri Nets (LPN) between which certain connections exist. Hazards identified in the Stage 1, in Stage 2 should be covered by instantiation of the SDCPN model. Also, some assumptions are adopted during model development. In addition to model development description, Stage 2 should also provide an overview of LPN connections and adopted assumptions, as well as show how previously identified hazards have been covered.

Additionally, Stage 2 explains how the collision risk decomposition necessary for efficiently evaluating the accident risk for instantiated SDCPN is performed. In order to perform the decomposition it is necessary to determine an appropriate set of events or event sequences collected in classes, and to identify an appropriate event sequence classification sampling time. This set of event sequence classes is then used to develop equations for the decomposition of the collision risk. Finally, the SDCPN model developed in mentioned way is implemented into the simulator part of the TOPAZ toolset.

Stage 3 - Accident risk assessment

This stage contains four interrelated sub-stages (Figure 1) where some of them are dependant on certain sub-stages from Stage 2. Simulations of the SDCPN are performed in Stage 3, providing results that present estimates for probability distribution of the event sequence classification process. Conditional collision risk is also determined. Knowing the previously determined probability distribution and conditional collision risk, determination of collision (accident) risk is possible. Finally, a bias and uncertainty assessment should be carried out in order to present how, due to all model assumptions and parameter values, the bias and uncertainty influence collision (accident) risk estimates. This effect is determined through the examination of statistical data, expert judgment and model evaluations.

Stage 4 - ATM safety criticality assessment

This stage contains three sub-stages (Figure 1) influenced by sub-stages from Stage 3 as well as from Stage 1. In Stage 4, firstly the consequences of a collision for passengers and aircrew are determined. Then assessment of the economic and societal safety harm (as a compound measure of collision risk and consequences) and comparison of the harms against accident target levels. This stage also provides the possibility to investigate the bottlenecks with respect to ATM safety as well as identification of values of the event sequence classification process as main contributors to collision risk. Finally, the main sources of collision risk are traced back to the level of ATM modules.

---
² Term instantiation is used in order to emphasize that each application of TOPAZ methodology on a specific test case requires the construction of a new model.
4 DESCRIPTION OF THE TRAFFIC ALERT AND COLLISION AVOIDANCE SYSTEM

Traffic Alert and Collision Avoidance System (TCAS) presents a solution for reduction of the risk of mid-air collision between aircraft, i.e. a solution for the system defined by ICAO as the Airborne Collision Avoidance System (ACAS, (ICAO, 2002)).

TCAS is designed to work autonomously, independently of the aircraft navigation equipment and independently of the ground systems used to provide ATC Services. Generally, TCAS monitors the airspace around the own* aircraft and warns pilots of the presence of the other aircraft, so called intruders*, which may present a threat^ of mid-air collision.

TCAS is certified to operate only as an advisory and alerting system, i.e. it is a decision aid intended for use in emergency situations involving extreme time pressure. As an alerting system, TCAS operates quietly in the background most of the time. It assists pilots in the visual acquisition of potential threats (by issuing Traffic Alerts - TA) and if necessary provides last-minute collision avoidance guidance directly to the flight crew (through Resolution Advisories - RA) (Kuchar and Drumm, 2007).

TCAS II Version 7, as the latest version of TCAS which is commercially used, offers vertical manoeuvres as an RA. Basically, TCAS interrogates transponders of all the aircraft in own aircraft vicinity (of some determined range), and based on replies received it tracks the slant range, bearing and altitude (if it is included in the reply message) of surrounding traffic (Figure 2), i.e. builds a 3D map of aircraft in that airspace. Based on successive replies, TCAS calculates the time to the Closest Point of Approach (CPA) with the intruder. Time to CPA is the main parameter for determination if a potential collision threat exists and for issuing alerts (DoT, 2000).

TCAS can simultaneously track up to 30 aircraft in a range of up to 14 Nm. It operates on a relatively short time scales: 48 seconds before CPA for issuing TA and 35 seconds for issuing RA (time scales are shorter at lower altitudes) (Drozdowski, 2007). Depending on intruder’s equipment, own aircraft TCAS II can provide either the TA (in case intruder is equipped with Mode A transponder), TA/vertical RA when intruder is equipped with Mode C/S or with TCAS I, or TA/coordinated vertical RA when intruder is equipped with TCAS II.

The main functions of TCAS are to identify a potential collision threat, to communicate the detected threat to the pilot and to assist in the resolution of the threat by recommending an avoidance manoeuvre.

---

3 “Own aircraft” - the aircraft fitted with the ACAS that is the subject of the discourse, which ACAS is to protect against possible collisions, and which may enter a maneuver in response to an ACAS indication (ICAO, 2002).
4 “Intruder” - an SSR transponder-equipped aircraft within the surveillance range of ACAS for which ACAS has an established track (ICAO, 2002), a target that has satisfied the traffic detection criteria (DoT, 2000).
5 “Threat” - An intruder that has satisfied the threat detection criteria and thus requires an RA to be issued (DoT, 2000).
4.1 Components of TCAS

Major components of the TCAS system are (DoT, 2000; Kuchar and Drumm, 2007; Love, 1997; RTCA, 1997):

a) TCAS processor (computer unit);
b) Mode S transponder;
c) Mode S/TCAS control panel;
d) Antennas;
e) Traffic display and Resolution Advisory display;
f) Performance monitor.

a) the TCAS processor performs:
   - airspace surveillance;
   - tracking of aircraft in vicinity;
   - own aircraft altitude tracking;
   - threat detection;
   - RA manoeuvre determination and selection; and
   - generation of advisories.

The processor uses pressure and radar altitude as inputs as well as discrete aircraft status inputs from its own aircraft to control the collision avoidance logic parameters that determine the protection volume around its own aircraft.

If an intruder is a collision threat, the processor will select an avoidance manoeuvre that will provide adequate vertical miss distance between the intruder and the own aircraft. If the intruder is also equipped with TCAS II, the avoidance manoeuvre will be coordinated between own aircraft and the intruder.
b) In order for TCAS II to be operational it is necessary that a Mode S transponder is installed and operational in own aircraft. If the Mode S transponder fails, the TCAS Performance Monitor will detect this failure and automatically put TCAS on standby.

c) Mode S/TCAS control panel is provided to allow the flight crew to select and control all TCAS components (processor, transponder and displays). A typical panel provides four basic control positions (RTCA, 1997):

- **Standby**: (TCAS does not issue any interrogation). When the TCAS function is turned off, the TCAS unit is essentially in a standby state. The term *standby* may be used to designate this selection. This does not place the transponder(s) on board the TCAS aircraft in a standby state;
- **Transponder**: (Mode S will reply, TCAS is in standby). When the operation of the Mode S transponder only is selected, the control panel provides a unique signal which indicates the transponder is operative, but that TCAS must be placed in Standby;
- **TA Only**: (Mode S fully operational, TCAS only issues TA) When the TA Only mode is selected, the control panel provides a unique signal which indicates the transponder is operative and the pilot has selected a TCAS operating mode which inhibits RAs; and
- **Automatic or TA/RA**: (TCAS will issue both TA and RA). When the TA/RA mode is selected, the control panel provides a unique signal which indicates the transponder is operative and that TCAS is capable of issuing RAs.

Apart from existing control positions, it is recommended that during all operations in RVSM airspace and transition areas, TCAS should be operated in TA/RA mode (TTP, 2000)

d) The antennas used by TCAS II include a directional antenna (mounted on the top of the aircraft) and either an omni-directional or a directional antenna (mounted on the bottom of the aircraft). Both antennas transmit interrogations and also receive transponder replies, as well as send these replies to the TCAS Processor. Also, two additional antennas are required for the Mode S transponder (one is mounted on the top of the aircraft while the other on the bottom). These antennas enable the Mode S transponder to receive interrogations and reply.

e) The traffic display presents the position of the surrounding traffic relative to its own aircraft. It is designed to provide information that will assist the pilot in visual acquisition of other aircraft and prepare the pilot for the potential issuing of an RA. The Resolution Advisory display provides the pilots with information on the vertical speed or pitch angle in order to a resolve conflict situation. Usually, both displays are integrated into one (Figure 3).

f) The performance monitor continuously and automatically monitors the health and performance of TCAS, whenever power is applied to TCAS.
4.2 TCAS Functions

How does TCAS work? TCAS works sequentially. State information about the intruder aircraft (position and velocity) are collected by surveillance sensors. The collected information is then analyzed by a set of algorithms in order to determine whether a collision threat exists. If a threat is identified, a set of threat resolution algorithms determines an appropriate response (Figure 4) (Kuchar and Drumm, 2007; RTCA, 1997). Figure 4 contain the principles of functioning and also the basic functions of TCAS:

1. surveillance;
2. collision avoidance consisting of
   - threat detection and display function; and
   - threat resolution function.
1. Surveillance of the air traffic environment is based on air-to-air interrogations broadcast from antennae on the own aircraft. Transponders on nearby intruder aircraft receive these interrogations and send replies. This TCAS function is performed independently of any ground input, and serves to provide information to the pilot on the position (range and bearing from own aircraft) and altitude of intruder aircraft, so that the collision detection and avoidance algorithms can perform their functions.

2. Own aircraft TCAS tracks the range and altitude of each Mode S target. These target reports are provided to the Collision Avoidance (CA) logic for use in the detection and advisory (resolution) logic and for presentation to the pilot on the traffic display. The relative bearing of the target is also provided to the CA logic so that the targets position can be properly shown on the traffic display, but is not used by the CA logic for the threat detection and advisory selection. The threat detection and display function classifies the intruders into one of four discrete levels (Figure 5):

- distant, non threatening aircraft (the display symbol is a hollow diamond);
- proximate traffic but not yet a threat (the display symbol is a solid diamond);
- TCAS issues a TA warning if collision is predicted to occur within the next 20-48 seconds (the display symbol is a solid yellow circle and a spoken message is heard); and
- TCAS issues an RA warning 15-35 seconds before collision (display symbol is a filled red square and a spoken command is heard).

![Figure 5. Standardized Symbology for use on the TCAS Displays](image_url)

Examples in Figure 5 correspond to values on TCAS display presented in Figure 3 and have the following meaning (respectively from left to right): distant traffic (in level flight, 1800ft above own aircraft), proximate traffic (descending, 1000ft below own aircraft), traffic advisory – intruder (climbing, 200ft below own aircraft) and resolution advisory – threat (level flight, 200ft below own aircraft).

The system performs a linear extrapolation of own and intruder aircraft positions in order to anticipate the future aircraft position, based on estimated current velocity. The algorithms then use several metrics to decide whether an intruder is a threat or not, including the estimated vertical and slant range separations between aircraft. If the intruder presents a threat, the TCAS threat resolution algorithms determine what manoeuvre is appropriate to avoid collision, firstly deciding the vertical sense of the manoeuvre (climbing or descending) and then deciding the strength of the RA (how rapidly altitude should be changed). Algorithms that monitor the evolution of the manoeuvre also exist. If necessary, they issue an RA modification. The given RA should be coordinated with the intruder aircraft in order to provide it with the opposite RA.
4.3 Collision Avoidance Concepts and Functions

Collision avoidance (CA) is based on a three main concepts, which are used to explain the operation of the CA logic (DoT, 2000; Love, 1997; RTCA, 1997):

a) sensitivity level;

b) time to CPA (tau - τ); and

c) protected volume.

a) A trade off is required between the necessary protection and the unnecessary advisories. It is achieved by controlling the sensitivity level (SL) which controls the time (tau thresholds) for TA/RA issuance (the higher the SL – the larger the amount of protected airspace (see Table 2 in Section 12.3.1)). TCAS uses two means of determining the operating SL (DoT, 2000):

- Pilot selected, through selection of three operations modes:
  - Standby position (no interrogation). When the Control Panel switch is placed in the Standby Position, TCAS is operating in SL1. In SL1, TCAS does not transmit any interrogations. SL1 is normally selected only when the aircraft is on the ground or if TCAS has failed. The pilot selection of Standby on the Control Panel is normally the only way that SL1 will be selected;
  - TA-ONLY (surveillance but only TA is issued). When the pilot selects TA-ONLY on the control panel, TCAS is placed into SL2. While in SL2, TCAS performs all surveillance functions and will issue TAs, as required. RAs are inhibited in SL2; and
  - TA-RA (surveillance with both TA and RA issued). When the pilot selects TA-RA or the equivalent mode on the control panel, the TCAS logic automatically selects the appropriate SL based on the altitude of the own aircraft. Table 2 provides the altitude threshold at which TCAS automatically changes SL and the associated SL for that altitude band. In these SLs, TCAS performs all surveillance functions and will issue TAs and RAs, as required.

- Ground based selection. Although the use of ground-based control of SL has not been agreed to between pilots, controllers, and the FAA and is not envisioned for use in U.S. airspace, the capability for ground-based selection of SL is included in the TCAS design. This design feature allows the operating SL to be selected from the ground by using a Mode S uplink message.

b) TCAS uses time-to-go to CPA, rather than distance, to determine when a TA or an RA should be issued. Tau is an approximation of the time to CPA (in seconds) or to the aircraft being at the same altitude (\( \tau_{\text{Hor}} \) vs. \( \tau_{\text{Ver}} \)). For either a TA or an RA to be issued, both the range and vertical criteria, in terms of tau or the fixed thresholds, must be satisfied. However, if only one of the criteria is satisfied, TCAS will not issue an advisory.

c) Protected volume presents an airspace that surrounds each TCAS equipped aircraft. The size of it depends on the speed and heading of the aircraft involved in the encounter. TCAS II is designed to provide collision avoidance protection in the case of any two aircraft that are closing horizontally at any rate up to 1200 kt and vertically up to 10,000 fpm.

---

6 "Sensitivity Level" is a value used in defining the size of the protected volume around the own aircraft (DoT, 2000)
Collision Avoidance Concepts and Functions

CA logic functions are presented in Figure 6 (grey boxes) and are described further in the text:

![Collision Avoidance Logic Functions Diagram](https://via.placeholder.com/150)

**Figure 6. Collision avoidance logic functions (DoT, 2000)**

**Tracking**
CA logic initiates and maintains a 3D track of each aircraft and uses this information to determine the time to CPA and the altitude of each aircraft at CPA. In addition to altitude, range and bearing from surrounding aircraft provided by surveillance function, the CA logic also uses data from its own aircraft pressure altitude to determine the own altitude, vertical speed and relative altitude of each aircraft.

**Traffic Advisory**
The range and altitude tests are performed using the track from nearby aircraft, for each altitude, reporting target. Exact expressions used for both tests are given in following sub-chapter describing the Conceptual model of TCAS logic. If the TA logic declares an aircraft to be an intruder, a TA will be issued against that aircraft.

**Threat Detection**
The intruder is declared a threat if during the range and altitude tests the conditions for issuing an RA associated with the current SL are met. Depending on the geometry of the encounter and the quality and age of the vertical track data, an RA may be delayed or not selected at all. Exact expressions used for issuing an RA are given in following sub-chapter describing the Conceptual model of TCAS logic.

**Resolution Advisory**
When an intruder is declared a threat, a two step process is used to select the appropriate RA for the encounter geometry. The first step is to select the RA sense (upward/downward). The second step is to choose the strength of the advisory (CAS logic continuously monitors the vertical separation that is provided at CPA and if necessary, the initial RA will be modified).

---

7 In some events, the intruder aircraft will manoeuvre vertically in a manner that thwarts the effectiveness of the issued RA. In these cases, the initial RA will be modified to either increase the strength or reverse the sense of the initial RA (DoT, 2000). This process is known as "RA modification".
**TCAS-TCAS Coordination**
In a TCAS-TCAS encounter, each aircraft transmits interrogations to the other via the Mode S link to ensure the selection of complementary RAs by the two aircraft. Coordination interrogations contain information about an aircraft’s intended RA sense to resolve the encounter with the other TCAS-equipped intruder. The information in the coordination interrogation is expressed in the form of a complement, e.g. when an aircraft selects an upward sense RA, it will transmit a coordination interrogation to the other aircraft that restricts that aircraft’s RA selection to those in the downward sense. The strength of the downward sense RA would be determined by the threat aircraft based on the encounter geometry and the RA Selection logic.

**Advisory Annunciation**
The CAS logic also performs the function of setting flags that control the displays and aural announcement. These flags are used to alert the pilot to the presence of TAs and RAs. The TCAS aural announcements are integrated with other environmental aural alerts available on the aircraft.

**Performance Monitoring**
When some anomalous performance within TCAS or an invalid input from a required on-board system is detected, the failure is announced to the pilot. If appropriate, all or a portion of the TCAS functions may be disabled or inhibited. If it disables any TCAS capability, it will continue to monitor the remaining functions, and if the detected failure is removed, full operational capability will be restored.
5 MODEL OF TCAS OPERATIONS IN AIR TRAFFIC CONTROL

5.1 Operational use of TCAS II Version 7: Brief Description and Human Roles

The operation considered in this research is usage of TCAS II version 7 during en-route or the TMA phase of flight, i.e. during flight through a given sector and/or adjacent sectors, due to the assumption that this operation may start before/after the aircraft enters/leaves in/from a given sector.

Taking into account that TCAS represents an advisory and alerting system, intended for use in emergency situations, it is assumed that TCAS is always turned-on during the flight and works in the appropriate mode (e.g. it is recommended that during all operations in RVSM airspace and transition areas, TCAS should be operated in the TA/RA mode (TTP, 2000)). Also, during the entire flight, the flight crew must be aware of the surrounding traffic through Cockpit Display of Traffic Information (CDTI), or another dedicated Traffic Display.

In order to model TCAS operation in this research, it is first described. According to Chapter 11, it is assumed that TCAS operation contains the following phases:

- normal flight;
- appearance of TA;
- appearance of RA; and
- return to normal flight.

Normal flight
In nominal situation, i.e. during normal evolution of flight, the aircraft crew receives instructions and clearances from Air Traffic Controllers (ATCos) and flying according to it (manually or using autopilot). Separation assurance is the responsibility of ATCos. TCAS is works in TA/RA mode, which means that it is continuously surveying the surrounding airspace, by broadcasting interrogations and receiving replays from near-by aircraft. It is assumed that TCAS works properly, which means that both TCAS antennas and Mode S Transponder are installed and operational on own aircraft.

Appearance of TA
When an aircraft enters into the airspace within range of the own aircraft TCAS, and a collision is predicted to occur within next 20 to 48 seconds (depending on altitude) a TA is issued, warning the flight crew by issuing the aural announcement “Traffic, Traffic”. The mentioned aircraft is designated as “intruder”. Immediately, the icon representing the intruder aircraft on the Traffic Display changes shape and colour, becoming a solid yellow circle. The crew responds to the TA by attempting to establish visual contact with the intruder aircraft as well as other aircraft in the vicinity. The crew should not deviate from the assigned clearance given by the ATCo, and should continue to maintain or attain safe separation while reporting the situation to the ATCo.
Appearance of RA

If the previous situation worsens, and collision is predicted to occur within 15 to 35 seconds (depending on altitude), an RA is issued. The previously mentioned “intruder” now becomes a “threat”. The RA includes an aural announcement in the cockpit “Climb, Climb” or “Descend, Descend” (depending on situation), the icon representing threat aircraft on the Traffic Display changes shape and colour, becoming a solid red square and Resolution Display becoming active, showing the appropriate vertical rate, which should be used in order to resolve the conflict situation. A pilot receiving an RA should disengage the autopilot and manually control the aircraft to achieve the recommended vertical rate.

When an RA occurs, the pilot flying should respond immediately by directing attention to the RA displays and manoeuvring as indicated, unless doing so will jeopardize safe operation of the flight. By not responding to an RA, the flight crew takes responsibility for achieving safe separation. In some instances, it may not be possible to respond to an RA and continue to satisfy an ATC clearance (issued before an RA) at the same time. Even if an RA manoeuvre is inconsistent with the current clearance, pilots are obligated to respond appropriately to the RA. Also, pilots are obligated to report RA occurrence, i.e. that they are responding to the RA, to the ATCos when appropriate, and to inform the ATCo about the RA deviation as soon as possible, using the defined phraseology. ATCos are advised to not issue control instructions that are contrary to the given RA. ATCo should provide safety alerts regarding terrain or obstructions and traffic advisories for the aircraft responding to an RA. When aircraft has begun a manoeuvre in response to an RA, the ATCo is not responsible for providing standard separation between that aircraft and other aircraft, airspace, terrain or obstructions.

Return to normal flight

When the RA is cleared, the flight crew receives the aural announcement “Clear of Conflict”. Next that they should advise ATCo that they are returning to their previously assigned clearance or should acknowledge any amended clearance issued, using the defined phraseology. After that, pilot could reengage the autopilot. ATCo resumes responsibility for standard separation when one of the following conditions are met: the responding aircraft has returned to its assigned altitude, the flight crew informs ATCo that the TCAS manoeuvre is completed and it is observable that standard separation has been re-established; and the responding aircraft has executed an alternate clearance and it is observable that standard separation has been re-established.

5.2 Conceptual Model of TCAS II Version 7 Logic

The main part of TCAS II version 7 is the TCAS Logic. In order to instantiate SDCPN model of TCAS operational use, it was necessary to create and verify a model of TCAS Logic. In this research a conceptual model of TCAS logic is developed containing algorithms for threat detection and threat resolution. The model is of an encounter type and is based on TCAS principles and basic functions as well as on descriptions of TCAS logic (DoT, 2000; ICAO, 2002; RTCA, 1997). A block diagram of TCAS Logic (operation) is presented in Figure 7.
Figure 7. Block diagram of TCAS logic (operation)
5.2.1 Threat Detection Algorithms

In order to determine whether a collision threat exists, i.e. to issue Traffic Alert (TA) or Resolution Advisory (RA), both the range and vertical criteria must be satisfied, i.e. if one of them is not satisfied, the TCAS will not issue an advisory. For checking whether the range and vertical criteria are satisfied, Range Test and Altitude Test are continuously performed during encounters. The criteria used for making the decision on TA and RA issuance depend on Sensitivity Level (SL) (Table 2).

Table 2. Sensitivity level and threshold values (DoT, 2000)

<table>
<thead>
<tr>
<th>Own altitude (feet)</th>
<th>SL</th>
<th>( \tau ) (seconds)</th>
<th>DMOD (Nm)</th>
<th>ALIM (feet)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TA</td>
<td>RA</td>
<td>TA</td>
<td>RA</td>
</tr>
<tr>
<td>&lt;1000</td>
<td>2</td>
<td>20</td>
<td>n.a.</td>
<td></td>
</tr>
<tr>
<td>(1000-2350]</td>
<td>3</td>
<td>15</td>
<td>0.33</td>
<td>0.20</td>
</tr>
<tr>
<td>(2350-5000]</td>
<td>4</td>
<td>30</td>
<td>0.48</td>
<td>0.35</td>
</tr>
<tr>
<td>(5000-10000]</td>
<td>5</td>
<td>25</td>
<td>0.75</td>
<td>0.55</td>
</tr>
<tr>
<td>(10000-20000]</td>
<td>6</td>
<td>30</td>
<td>1.00</td>
<td>0.80</td>
</tr>
<tr>
<td>(20000-42000]</td>
<td>7</td>
<td>35</td>
<td>1.30</td>
<td>1.10</td>
</tr>
<tr>
<td>&gt;42000</td>
<td>7</td>
<td>35</td>
<td>1.30</td>
<td>1.10</td>
</tr>
</tbody>
</table>

n.a. – not available

Sensitivity level (SL) depends on the aircraft altitude range. Obtained SL contains certain values for horizontal and vertical \( \tau \) thresholds in the case of TA or RA issuance, and dimensions for protected airspace (Distance Modification - DMOD and Altitude Limit - ALIM) which should be satisfied in case of slow closure encounters, when \( \tau \) threshold values are not appropriate. During encounters, if the horizontal or vertical \( \tau \) is lower than the TA threshold, or horizontal and vertical miss distance is lower than TA DMOD and TA ALIM respectively, then TA is issued. If the situation further deteriorates and \( \tau \) values are lower than RA threshold, or miss distances are lower than RA DMOD and RA ALIM respectively, then RA is issued (DoT, 2000).

For the purpose of range and altitude tests, aircraft are identified in a Cartesian coordinate system (Figure 8). Let \( x_i^t \) and \( v_i^t \), be the 3D position and 3D velocity of aircraft \( i \) given in expressions (1) and (2); the superscripts \( x \) and \( y \) refer to the axis system in Figure 8, and \( z \) stands for the height. Let \( \theta_i^t \) present an orientation velocity vector \( v_i^t \) in the horizontal plane (measured from \( x \) axis in counter-clockwise direction, where \( 0 \leq \theta_i^t \leq 2\pi \)) and \( \psi_i^t \), orientation of velocity vector \( v_i^t \) in the vertical plane (measured from the horizontal plane up as positive, and down as negative, where \(-\pi/2 \leq \psi_i^t \leq \pi/2\)).

\[
x_i^t = \begin{bmatrix} x_{x,i}^t \\ x_{y,i}^t \\ x_{z,i}^t \end{bmatrix}
\]

\[
v_i^t = \frac{dx_i^t}{dt} = \begin{bmatrix} v_{x,i}^t \\ v_{y,i}^t \\ v_{z,i}^t \end{bmatrix} = \begin{bmatrix} v_i^t \cos \psi_i^t \cos \theta_i^t \\ v_i^t \cos \psi_i^t \sin \theta_i^t \\ v_i^t \sin \psi_i^t \end{bmatrix}
\]

Let \( x_{ik}^t = x_i^t - x_k^t \) be the distance in 3D space between own aircraft \( i \) and intruder aircraft \( k \) at time \( t \) and let \( v_{ik}^t = v_i^t - v_k^t \) be the relative velocity between aircraft, at time \( t \).
Conceptual Model of TCAS II Version 7 Logic

**Figure 8. Velocity vector in Cartesian coordinate system**

**Range test:**

At each moment $t$, both the distance and closing speed (relative velocity) between own aircraft $i$ and intruder aircraft $k$ in the horizontal plane are calculated. Knowledge about both values is required in order to calculate “time to closest point of approach” (horizontal, i.e. range $\tau$). The encounter geometry observed in the range test (horizontal plane) is shown in Figure 9. Let $\bar{x}_{i,t}^h = (\bar{x}_{i,x,t}^h, \bar{x}_{i,y,t}^h)^T$ and $\bar{v}_{i,t}^h = (\bar{v}_{i,x,t}^h, \bar{v}_{i,y,t}^h)^T$ be the position and velocity of aircraft $i$ in the horizontal plane. Let $\bar{x}_{ik,t}^h = \bar{x}_{i,t}^h - \bar{x}_{k,t}^h$ and $\bar{v}_{ik,t}^h = \bar{v}_{i,t}^h - \bar{v}_{k,t}^h$ be the horizontal distance and relative velocity in the horizontal plane (respectively) between aircraft $i$ and $k$, at time $t$.

![Figure 9. Encounter geometry in the horizontal plane at time $t$](image_url)

Let us define $\tau_{ik,t}$ as Time to Closest Point of Approach (CPA) in the horizontal plane between aircraft $i$ and $k$, at time $t$, with the following expression:

$$
\tau_{ik,t} = \frac{|\bar{x}_{ik,t}^h|}{|\bar{v}_{ik,t}^h| \cdot \cos(\delta_{ik,t}^h - \varphi_{ik,t}^h)}
$$

(3)
Where $\delta_{ik}^t$ is the bearing of the velocity difference vector satisfying

$$\delta_{ik}^t = \arctan\left(\frac{v_{ik}^t}{v_{yk}^t}\right)$$

(4)

and $\phi_{ik}^t$ is the bearing of the position difference vector satisfying

$$\phi_{ik}^t = \arctan\left(\frac{x_{ik}^t}{x_{yk}^t}\right)$$

(5)

Expression (3) is defined under the explicit condition that nominator is not equal to zero, i.e. when the following conditions are met:

$$(\delta_{ik}^t - \phi_{ik}^t \neq \pi/2) \land (\delta_{ik}^t - \phi_{ik}^t \neq -\pi/2) \land (|v_{ik}^t| \neq 0)$$

(6)

**Altitude test:**

At each moment $t$, both the vertical distance (separation) and combined speed (vertical closing speed) between own and the intruder aircraft are calculated. Knowledge about both values is required in order to calculate “time to closest point of approach” (vertical $\tau$). The encounter geometry observed in the altitude test (vertical plane) is shown in Figure 10. Let $x_{ik}^{z,t} = x_i^z - x_k^z$, and $v_{ik}^{z,t} = v_i^z - v_k^z$ be the vertical distance and the relative velocity in the vertical plane (respectively) between aircraft $i$ and $k$, at time $t$.

![Figure 10. Encounter geometry in the vertical plane at time $t_i$.](image)

Let's define $\tau_{ik}^{z,t}$ as Time to Closest Point of Approach (CPA) in the vertical plane between aircraft $i$ and $k$, at time $t$, by the following expression:

$$\tau_{ik}^{z,t} = -(\frac{x_{ik}^{z,t}}{v_{ik}^{z,t}})$$

(7)

Expression (7) is defined as long as $v_{ik}^{z,t} \neq 0$. 

24
TA or RA issuance

Range and Altitude tests compare the given criteria (see Table 2) and calculated values for \( \tau_{ik}^{h,t}, \tau_{ik}^{z,t}, x_{ik}^{h,t}, \) and \( x_{ik}^{z,t} \). So, whenever one of the following conditions are satisfied:

\[
\left( \theta < \tau_{ik}^{h,t} < \tau \right) \land \left( \theta < \tau_{ik}^{z,t} < \tau \right)
\]

or

\[
\left( x_{ik}^{h,t} < DMOD \right) \land \left( x_{ik}^{z,t} < ALIM \right)
\]

alerts shall be issued (TA or RA depending on the \( \tau, DMOD \) and \( ALIM \) criteria given in Table 2).

5.2.2 Threat Resolution Algorithm

Once a threat is identified, a two-step process is followed to select the appropriate RA for the given encounter geometry. In the first step the appropriate sense is selected (upward or downward), i.e. whether the aircraft should to climb or to descent. In the second step the appropriate strength (vertical speed) is determined, i.e. how rapidly the aircraft needs to change its altitude.

Sense selection

Let \( t \) be the moment at which RA for own aircraft \( i \) is issued, i.e. \( \tau_{RA} \) seconds remains until CPA with intruder aircraft \( k \). The TCAS Logic performs tests (trials) with upward and downward sense for own aircraft, in order to determine which sense provides the most vertical separation at CPA (time moment \( t + \tau_{RA} \) at Figure 11), provided that the intruder aircraft does not change its flight profile. The sense that provides greater vertical separation shall be selected.

Figure 11. RA sense selection (illustrative example)
Let’s consider possible vertical position of aircraft \(i\) at moment \(t+\tau_{RA}\) during the test (see Figure 11):

\[
\begin{align*}
\bar{x}_{z,t+\tau_{RA}}^{i}(up) &= x_{z,t}^{i} + (v_{z,t}^{i} + \Delta_{z,t}^{i}) \cdot \tau_{RA}, \text{ if upward sense is selected; } \\
\bar{x}_{z,t+\tau_{RA}}^{i}(current) &= x_{z,t}^{i} + v_{z,t}^{i} \cdot \tau_{RA}, \text{ if current rate is maintained; } \\
\bar{x}_{z,t+\tau_{RA}}^{i}(down) &= x_{z,t}^{i} + (v_{z,t}^{i} - \Delta_{z,t}^{i}) \cdot \tau_{RA}, \text{ if downward sense is selected; }
\end{align*}
\]

where \(\Delta_{z,t}^{i}\) has a fixed value of 1500 feet/min (RTCA, 1997; Kuchar and Drumm, 2007).

Two vertical separations at CPA between own aircraft \(i\) and intruder \(k\), are recognized in the sense selection process and are given by following expressions (see Figure 11):

\[
\begin{align*}
a &= |\bar{x}_{z,t+\tau_{RA}}^{i}(up) - \bar{x}_{z,t+\tau_{RA}}^{k}(current)| \\
b &= |\bar{x}_{z,t+\tau_{RA}}^{i}(down) - \bar{x}_{z,t+\tau_{RA}}^{k}(current)|
\end{align*}
\]

Sense is represented by the variable \(c_{i,t}^{j}\), which takes the following values: \(c_{i,t}^{j} = 1\) in case of the upward sense selected, \(c_{i,t}^{j} = -1\) in the case of the downward sense, and \(c_{i,t}^{j} = 0\) otherwise.

In the event that aircraft \(i\) has already received sense from aircraft \(k\) before it has finished its own sense calculations then \(c_{i,t}^{j} = -c_{k,t}^{j}\), otherwise:

\[
c_{i,t}^{j} = \begin{cases} 
(b > a) \lor \\
-1, \quad \text{if } (b \leq a) \land \left( \exists e \in (0, \tau_{RA}) \text{ such that } x_{z,t+e}^{i} = 0 \right) \lor \\
(b > a) \land \left( \exists e \in (0, \tau_{RA}) \text{ such that } x_{z,t+e}^{i} = 0 \right) \land (a > ALIM_{RA}) \\
(c_{i,t}^{j} = \begin{cases} 
(b \leq a) \lor \\
1, \quad \text{if } (b > a) \land \left( \exists e \in (0, \tau_{RA}) \text{ such that } x_{z,t+e}^{i} = 0 \right) \lor \\
(b \leq a) \land \left( \exists e \in (0, \tau_{RA}) \text{ such that } x_{z,t+e}^{i} = 0 \right) \land (b > ALIM_{RA}) \\
0, \quad \text{otherwise}
\end{cases}
\end{cases}
\]

The obtained sense for the own aircraft \(i\) is coordinated through the Mode S data link with intruder aircraft \(k\), with aim of ensuring that both aircraft do not select the same vertical sense. So, the RA sense sent to the intruder aircraft is the calculated \(c_{i,t}^{j}\).
Strength selection

Once the sense has been selected, TCAS Logic determines the RA strength. RA Strength should be least disruptive to the existing flight path, while providing at least $ALIM_{RA}$ vertical separation between aircraft $i$ and $k$ at CPA (time moment $t+\tau_{RA}$), provided that the intruder aircraft does not change its flight profile. This means that the change of vertical speed $\Delta'_{z,t}$ should be minimal.

Determination of the appropriate strength (vertical speed) should satisfy a following condition:

$$\text{if } x_{z,t+\tau_{RA}}^{ik}(current) \geq ALIM_{RA} \text{ then no RA is issued, otherwise the strength is calculated as follows:}$$

$$v_{z,t}^{i} = \begin{cases} v_{z,t}^{i} + \Delta'_{z,t}^{i} ; & c_{t}^{i} = 1 \\ v_{z,t}^{i} - \Delta'_{z,t}^{i} ; & c_{t}^{i} = -1 \end{cases}$$

(16)

where:

$$\Delta'_{z,t}^{i} = \frac{[ALIM_{RA} + (x_{z,t}^{i} + v_{z,t}^{i} \cdot \tau_{RA}) - (x_{z,t}^{k} + v_{z,t}^{k} \cdot \tau_{RA})]}{\tau_{RA}}$$

(17)

5.2.3 Clear of Conflict Annunciation

The following conditions should be satisfied in order to announce Clear of Conflict:

- RAs may terminate for a number of reasons: normally, when the conflict has been resolved and the threat is diverging in range (RTCA, 1997; ICAO, 2002);
- Clear of conflict occurs after an encounter has been resolved (RTCA, 1997; ICAO, 2002).

Let $t_{CPA}$ be the first moment when both aircraft are at CPA. Let $t' > t_{CPA}$ be the first moment when both aircraft are safely passing the CPA and following condition is satisfied:

$$\left| x_{h,t}^{ik} \right| > \left| x_{h,t,CPA}^{ik} \right|$$

(18)

then “Clear of Conflict” will be announced and TCAS encounter can be terminated.
5.3 Hazards Identified

A hazard is anything that might negatively affect safety (de Jong, 2004) or an event or situation with possibly harmful effects (FAA/ Eurocontrol, 2007). A hazard is an event/state that may:

a) lead to a dangerous situation, or
b) hamper resolution of such a situation,

possibly in combination with other hazards or under certain conditions.

Analysis of information on Operational use of TCAS II version 7s, available only from literature but not from brainstorming sessions, identifies certain possible hazards. They are presented together with an explanation of the situation leading to specific hazard. The given list of hazards is exhaustive and is compiled from the following papers and documents: (Drozdowski, 2007; Kuchar and Drumm, 2007; DoT, 2000).

1. TCAS operates on a relatively short time scales. The maximum generation time for a TA is 48 sec before CPA. For an RA the time is 35 sec. Unexpected or rapid aircraft manoeuvre may cause an RA to be generated with much less lead time. It is possible that an RA will not be preceded by a TA if a threat is imminent.

   Hazard 1: occurrence of rapid aircraft manoeuvre.

2. Pilots are required to immediately comply with all RAs, even if the RAs are contrary to ATC clearances or instructions. Everyday experience shows that in some cases pilots will choose to follow the ATCo instructions rather then the RA.

   Hazard 2: pilot follows ATCo instruction instead of RA.

3. When the pilot reports an RA, controllers are not allowed to modify the aircraft flight path until the pilot reports returning to the current air traffic control clearance.

   Hazard 3: modification of aircraft flight path by ATCo.

4. Currently, the pilot report is the only source of information available to controllers to notify them that an aircraft is deviating from the ATC clearance. However, due to a high level of workload in the cockpit, pilot reports of an RA are often delayed or fragmented.

   Hazard 4: pilot report is incomplete and not understandable by ATCo;
   Hazard 5: pilot did not report to ATCo at all, so the ATCo is not aware of RA existence.

5. If ATCo are not aware of an RA and if they provide the aircraft with instructions for avoiding action, horizontal instructions are more appropriate as they will not adversely affect any vertical manoeuvre required by TCAS RAs.

   Hazard 6: ATCo issues vertical manoeuvre instruction to aircraft.

6. To minimize the likelihood of unnecessary RA, controllers are advised to provide traffic information to aircraft climbing or descending above or bellow other aircraft.

   Hazard 7: ATCo does not provide traffic information.

---

8 Given list of hazards is made based on information from available literature, not on information from brainstorming sessions.
7. Certain older transponders do not report altitude information when interrogated. TCAS cannot generate collision avoidance commands against such threats.

   **Hazard 8**: no altitude information about threat aircraft.

8. Aircraft without a functioning transponder cannot be detected or tracked by TCAS at all. Pilots therefore should take the responsibility to apply “see and avoid” concept in the case of such traffic.

   **Hazard 9**: transponder is not functioning.

9. Due to TCAS update rate (1 Hz) and filtering lags, its estimates may lag compared to the actual situation during periods of sudden acceleration. This lag may in turn lead to an inappropriate RA sense or strength. To help alleviate this problem, TCAS refrains from issuing an RA if there are large uncertainties regarding the intruder’s track.

   **Hazard 10**: issuing of inappropriate RA.

10. TCAS cannot handle all situations. In particular, it is dependent on the accuracy of the threat aircraft’s reported altitude and on the expectation that the threat aircraft will not make an abrupt manoeuvre that defeats the TCAS RA.

   **Hazard 11**: threat aircraft altitude is not reported accurately;

   **Hazard 12**: threat aircraft makes an abrupt manoeuvre.

11. The Mode S transponder is also used to provide air-to-air data exchange between TCAS equipped aircraft so that coordinated, complementary RAs can be issued when required.

   **Hazard 13**: Mode S failure, so the issuing of coordinated RA between aircraft is not possible.

12. The traffic display/aural annunciation will automatically activate whenever a TA or an RA is issued.

   **Hazard 14**: display/aural annunciation fails and does not issue a TA or an RA.

13. The RA display provides the pilot with information on the vertical speed or pitch angle, to resolve a conflict.

   **Hazard 15**: display fails and does not issue speed or angle directive.

14. Occasionally, the two aircraft declare each other as threats simultaneously, and therefore, both aircraft will select their RA sense based on the encounter geometry. In such encounters, there is a chance that both aircraft will select the same sense. When this occurs, the aircraft with the higher Mode S address will detect the selection of the same sense and will reverse its sense.

   **Hazard 16**: possibility that reverse sense is not selected due to some failure.

15. Operational experience has indicated that some problems related to TCAS continue to occur. These issues include the following:

   **Hazard 17**: pilots sometimes deviate significantly further from their original clearance than was required or desired while complying with an RA.
Hazard 18: pilots are often slow in reporting the initial deviations to the controller and this has resulted in situations where the controller was issuing clearances that were in contrary to that directed by the RA;

Hazard 19: some pilots request information, or refuse a clearance, based upon information shown on the traffic display;

Hazard 20: aircraft have also been observed making horizontal manoeuvres based solely on the information shown on the traffic display, without visual acquisition by the aircrew;

Hazard 21: event reports also indicate that some pilots have not reacted to RAs, when they have traffic information from the controller, but did not visually acquired the intruder.

16. Operational experience has shown that the unexpected interactions between TCAS and the ATC systems can occur under the following conditions:

Hazard 22: aircraft levelling off at 1000ft above or below conflicting traffic that is level, may result in RAs being issued to the level aircraft;

Hazard 23: altitude crossing clearances issued by a controller based on maintaining visual separation may result in RAs being issued, particularly if one of the aircraft is level.

5.4 Agents and Local Petri Nets for Operational use of TCAS II version 7

In this research, the SDCPN formalism is used to specify a simulation model of TCAS operational use. The SDCPN model for TCAS operational use is developed and presented in two hierarchical levels:

a) The first level distinguishes the agents and the operation, where an agent is an entity that has situational awareness components (Blom and Stroeve, 2004).

b) At the second level, the Local Petri Nets (LPNs) of each agent are described, where each LPN is a Petri net describing an agent-specific process. There may be connections between LPNs within the same agent or between different agents. Connections are realised using the Compositional Specification principles presented in (Everdij et al, 2006).

In order to distinguish between two hierarchical levels a high level representation of TCAS agents and their mutual relations is given in Figure 12. Arcs represent information flows between agents. Own/intruder aircraft are designated as Aircraft $i$ and $k$ respectively. Agent $State_i$ provides information on position, velocity and acceleration of the aircraft at moment $t$ to agents $TCAS_i$ and $Mode\ S\ Link_i$. Agent $Mode\ S\ Link_i$ contains the interrogator, transponder and coordination link between aircraft $i$ and $k$. Through this link the own aircraft sends the state information as well as resolution adviser information to other surrounding aircraft, i.e. to their $Mode\ S\ Link_k$. Also, through $Mode\ S\ Link_i$ it receives the same information from surrounding aircraft and passes it to agent $TCAS_i$. $TCAS_i$ performs the necessary tests in order to detect and resolve conflicts. When conflict resolution is determined then this information is announced through agents $CDTI_i$ and $Aural_i$ to the agent $Crew_i$. The crew should follow those instructions providing control inputs to agent $State_i$ and informs agent $ATCo$ about RA appearance through the air/ground communication link, i.e. through agent $COM$. 
Here it is assumed that the SDCPN Model of TCAS operation could present a module that could be added to some, previously developed SDCPN Model. However, in order to be efficient during the validation process, the SDCPN model is developed as a standalone model.

Based on high level representations of TCAS agents, five agents are recognized for the SDCPN model of TCAS operation. They and their corresponding LPNs are given in Table 3.

Table 3. Agents vs. LPNs for TCAS II Version 7 operation

<table>
<thead>
<tr>
<th>Agent</th>
<th>LPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Own Aircraft</strong></td>
<td></td>
</tr>
<tr>
<td>Own aircraft state</td>
<td></td>
</tr>
<tr>
<td>Own aircraft Mode S Link</td>
<td></td>
</tr>
<tr>
<td>TCAS Processor</td>
<td></td>
</tr>
<tr>
<td>TCAS Processor Working Mode</td>
<td></td>
</tr>
<tr>
<td>CDTI Display</td>
<td></td>
</tr>
<tr>
<td>CDTI Display Working Mode</td>
<td></td>
</tr>
<tr>
<td>Aural Annunciation</td>
<td></td>
</tr>
<tr>
<td>Aural Annunciation Working Mode</td>
<td></td>
</tr>
<tr>
<td><strong>Own Aircraft Crew</strong></td>
<td></td>
</tr>
<tr>
<td>Crew</td>
<td></td>
</tr>
<tr>
<td><strong>Intruder Aircraft</strong></td>
<td></td>
</tr>
<tr>
<td>Intruder aircraft state</td>
<td></td>
</tr>
<tr>
<td>Intruder aircraft Mode S Link</td>
<td></td>
</tr>
<tr>
<td><strong>Air/Ground Communication Link</strong></td>
<td></td>
</tr>
<tr>
<td>Air/Ground Communication Link</td>
<td></td>
</tr>
<tr>
<td><strong>Tactical Air Traffic Controller (ATCo)</strong></td>
<td></td>
</tr>
<tr>
<td>ATCo</td>
<td></td>
</tr>
</tbody>
</table>
5.5 Specification of Local Petri Nets

A Stochastically and Dynamically Coloured Petri Net is, according to (Everdij and Blom, 2003, 2005a, 2005b; Everdij et al., 2006) given by the following tuple:


where:

- \( P \) - is a set of places (generally representing possible pre or post conditions for transitions);
- \( T \) - is a set of transitions (generally representing possible actions), consisting of a set of guard transitions (\( T_G \), enabled transition fires when a given predefined condition is satisfied, e.g. when colours of input tokens have reached certain values), a set of delay transitions (\( T_D \), enabled transition fires with a predefined time delay) and a set of immediate transitions (\( T_I \), enabled transition fires without time delay, i.e. immediately when it is enabled);
- \( A \) - is a set of arcs, consisting of a set of ordinary arcs (\( A_O \), that connect places with transitions and vice versa, and allow for the removal of tokens from input places to output places after transition fires), a set of enabling arcs (\( A_E \), they connect places with transitions but do not allow removal of the token from its input place after transition fires) and a set of inhibitor arcs (\( A_I \), that connect places with transitions and disable the transition when its input place contains a token);
- \( N \) - is a node function, which maps each arc to an ordered pair of one transition and one place (multiple arcs between the same place and transition are permitted);
- \( S \) - is a set of colour types for the tokens occurring in the net;
- \( C \) - is a colour function, which maps each place to a colour type in \( S \);
- \( V \) and \( W \) - are sets of place-specific colour functions, which describe what happens to the colour of a token while it resides in the given place;
- \( G \) - is a set of Boolean-valued transition guards associating each transition in \( T_G \) with a guard function which is evaluated when the transition has a token in each of its input places. The guard function must evaluate to True before the transition is permitted to fire (i.e. remove and produce tokens). Its evaluation depends on the colours of the input tokens of the transition;
- \( D \) - is a set of transition delays associating each transition in \( T_D \) with a delay function, which is evaluated when the transition has a token in each of its input places. The delay function determines for how long the transition must wait before it is allowed to fire (i.e. remove and produce tokens). The firing rate depends on the colours of the input tokens of the transition;
- \( F \) - is a set of (probabilistic) firing functions describing the quantity and colours of the tokens produced by the transitions at their firing. Its evaluation depends on the colours of the input tokens of the transition;
- \( I \) - is an initial marking, which defines the set of tokens initially present, i.e. it specifies in which places they reside initially, and the colours they initially have.

Specification of the LPNs represents the definition of each element of the tuple for each LPN. Specification of LPNs for the SDCPN model of TCAS operational use, as well as determination of interconnections between LPNs are presented in the following chapters.

---

9 all terms in following text are part of standard TOPAZ terminology used for SDCPN description and specification.
5.6 Local Petri Nets vs. Agents

This chapter contains a description of each agent with LPN identified in it, as well as depicts the identified connections between LPNs and/or agents. The principles followed in the specification are those presented in (Everdij and Blom, 2003, 2005a, 2005b; Everdij et al., 2006).

The SDCPN model of Operational use of TCAS II version 7 consists on the Agents and LPNs given in Table 3 and presented in Figure 13.

![Diagram of interaction between agents and their corresponding LPNs for TCAS operations](image)

Figure 13. Interaction between agents and their corresponding LPNs for the TCAS operations

In order to avoid repetition of modelling specification, a detailed specification containing the description of each LPN, together with the list of modelling assumptions as well as explanation of how and where the hazards are covered in the SDCPN model, is given in Appendices 2, 3 and 4.
5.6.1 Own Aircraft as Agent

This agent contains eight LPNs and represents a technical part of the Own aircraft TCAS system. LPN $\text{Own aircraft state}_i$ provides state information to LPN $\text{Own aircraft Mode S Link}_i$, which could be placed either in Work or Fail state. Through LPNs $\text{Own aircraft state}_i$ and $\text{Own aircraft Mode S Link}_i$, the own aircraft and intruder aircraft positions are provided to the LPN $\text{TCAS Processor}_i$, which contains threat detection and threat resolution algorithms. The LPN $\text{TCAS Processor}_i$ can have one of the following three states (places): no conflict, conflict detection and conflict resolution. Whenever the LPN $\text{TCAS Processor}_i$ is in conflict resolution state, it enables LPNs $\text{CDTI}_i$ and $\text{Aural Annunciation}_i$ to move into Active state, meaning that they audio/visually represent the selected RA. LPNs $\text{TCAS Processor Working Mode}_i$, $\text{CDTI Working Mode}_i$ and $\text{Aural Annunciation Working Mode}_i$ represent working modes of the corresponding LPNs. TCAS Own aircraft agent is represented in Figure 14. Detailed LPNs specification is provided in Appendix 4.

Figure 14. LPNs contained in Agent Own Aircraft and their mutual relationship
5.6.2 Intruder Aircraft as Agent

This agent (Figure 15) contains two LPNs and represents a technical part of the Intruder aircraft TCAS system. LPN *Intruder aircraft state* \(_k\) provides state information to LPN *Intruder aircraft Mode S* \(_k\) which could be placed either in Work or Fail state. Detailed LPNs specification is provided in Appendix 4.

![Figure 15. LPNs contained in Agent Intruder Aircraft and their mutual relationship](image)

5.6.3 Own Aircraft Crew as Agent

This agent (Figure 16) contains one LPN and represents a key human entity in the ACAS operation. LPN *Crew* \(_i\) contains three places in which the crew can be:

a) Nominal - in which the crew is performing their usual tasks during the flight;

b) Active – in which an RA is issued and the crew is following the RA, i.e. is taking proper action in time or with some delay in case they are too preoccupied to act immediately; and

c) Passive – in which the crew is refusing to act according to the issued RA.

Detailed LPNs specification is provided in Appendix 4.

![Figure 16. Agent Own Aircraft Crew](image)

5.6.4 Air/Ground Communication Link as Agent

This agent (Figure 17) contains one LPN which represents a technical part of the system. This LPN presents working modes of the air/ground communication system. Detailed LPNs specification is provided in Appendix 4.
5.6.5 Tactical Air Traffic Controller (ATCo) as Agent

This agent (Figure 18) is represented by only one LPN representing a human part of the system: LPN \( \text{ATCo} \) could be in one of two places:

a) Crew is responsible – in which an RA is issued and the ATCo is informed about it by the Crew and the ATCo is no longer responsible for separation assurance between the aircraft in conflict;

b) ATCo is responsible – in which the ATCo is responsible for separation assurance between the aircraft, or the aircraft are not in the conflict or a TA is issued.

Detailed LPNs specification is provided in Appendix 4.

Part of the TCAS II system related to procedures is represented by enabling arcs between Agent Crew and Agent ATCo (Figure 13). Therefore, whenever LPN \( \text{Crew}_i \) is in “Active” state, LPN \( \text{ATCo} \) switches to state “Crew is responsible”; LPN \( \text{ATCo} \) returns to state “ATCo is responsible” when an LPN \( \text{Crew}_i \) is in “Passive” or “Nominal” state (of course under condition that LPN Air/Ground Communication Link is in “Work” state).
6  VALIDATION OF MODEL OF TCAS OPERATIONS

6.1 Definition and Principles of Validation

Model validation is usually defined as “substantiation that a model within its domain of applicability possesses a satisfactory range of accuracy consistent with the intended application of the model” (Sargent, 2009; Balci, 1998). Model validation deals with building the right (appropriate) model (Balci, 1998).

The main principles of validation are (Balci, 1998):

1. Validation must be conducted throughout the entire life cycle of a simulation study;
2. The outcome of simulation model should not be considered as a binary variable where the model is absolutely correct or incorrect.
3. A simulation model is built with respect to the study objectives and its credibility is judged with respect to those objectives.

Since a model is an abstraction of a system, perfect representation is never expected. The outcome of the model validation should be considered as a degree of credibility on a scale from 0 (absolutely incorrect) to 100 (absolutely correct) (Balci, 1998).

As depicted in Figure 19, as the degree of model credibility increases, so will the model development cost. At the same time, the model utility will also increase, but most likely at a decreasing rate. The point of intersection of two curves changes from one model to another (Balci, 1998).

Sargent in his paper (Sargent, 2009) presents “validation techniques and tests”. Among the numerous techniques, those accepted in this research, i.e. recognized as best suitable for the available data, are the following:

- **Historical data validation**: if historical data exists it is used to determine (test) whether the model behaves as the system does.
- **Comparison to other models**: various outputs of the simulation model being validated are compared to outputs of other simulation models that have been validated.
- **Event Validity**: the “events” of occurrences of the simulation model are compared to those of the real system to determine if they are similar.

The third, event validity, in this research is used both in historical data validation and comparison to other model.
6.2 Validation Process

The aim of validation in this research is to provide evidence how well the model represents real world TCAS operation, taking into account that the model is developed for the purpose of safety assessment.

“Is the model an adequate representation of the phenomena under study? The procedure by which an answer to this question is sought constitutes the validation (testing) of the model. This aspect of the research is not separated in time from other phases of research but continually interacts with them, particularly with the construction of the model” (Ackoff et al, 1962).

In order to validate the developed model, an iterative validation process is proposed in this research based on abovementioned thinking, were in each iteration the developed model is improved if necessary, and if not it passes to the next iteration. It consists of four successive validation levels, i.e. iterations (Figure 20), were each level is represented with a certain question, while successive levels become more detailed.

At each validation level a modelled case (encounter) is compared with Control Case from real life. If at one level the validation results are not satisfactory, then a modification of model might be proposed. If the validation results are satisfactory then it is possible to pass on the next validation level. The process is repeating until the end of validation is reached.

The following questions are asked (Figure 20):

- At Level 1 - Is TCAS activated?
- At Level 2 - Are the same TCAS events occurring?
- At Level 3 - If RA occurs, is the resolution manoeuvre similar?
- At Level 4 - Are corresponding horizontal and vertical separations at CPA great enough?

According to Ackoff et al. (1962) it is suggested that the model should be subjected to continuous testing while it is under construction. It is followed in this research through logical testing, comparison with the given TCAS rules during conceptual model development, verification of developed conceptual model during writing of the computer code, etc. However, the presented validation process in this research came up after the model development and was applied in order to obtain feedback about the model quality.
6.2.1 Level 1 - Is TCAS activated?

At Level 1 a simple matrix (Table 4) should be constructed, where for each pair of Control and SDCPN-based cases, a frequency of occurrence, i.e. number of situations in which both cases are the answer to the given question, is presented.

Table 4. Level 1 validation: SDCPN-based model vs. Controls

<table>
<thead>
<tr>
<th>Level 1 Validation</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDCPN</td>
<td></td>
</tr>
<tr>
<td>1 (no)</td>
<td>1 (no)</td>
</tr>
<tr>
<td>2 (yes)</td>
<td>2 (yes)</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model

It would be ideal that pairs of cases are located in the green fields, meaning that a perfect match exists between SDCPN-based model and Control for the given case. If the pair of cases are located in the red corner it means that something was disabling the TCAS to activate in the SDCPN-based model, while in the Control in the same case TCAS was activated. Such a situation is considered as unwanted from the safety assessment point of view as the model does not “recognize” appropriate severity of the case. If cases are located in the yellow corner it means that the SDCPN-based model was enabling TCAS to activate in situations when in the Control TCAS was not activated for the same case. Such a situation is considered a false alarm, but it is not negative although it is not wanted from the safety assessment point of view, i.e. the model is liberal compared to the Control. While some of the cases are different or cases in red or yellow corner exist, it might be decided to improve the model as much as possible.

Start of Model Validation

Level 1
Is TCAS activated?

yes

Level 2
Are the same TCAS events occurring?

yes

Level 3
If RA occurs, is resolution manoeuvre similar?

yes

Level 4
Are corresponding horizontal and vertical separations after implementation of issued RA at CPA great enough?

yes

End of Model Validation

Model Modification

Figure 20. The proposed Validation Process
6.2.2 Level 2 - Are the same TCAS events occurring?

If the answer to the Level 1 question is positive, then at Level 2 the question is more detailed. A matrix should be constructed (Table 5), where for each pair of Control cases and SDCPN-based cases, a frequency of occurrence, i.e. number of situations in which both cases are answer on the given question is presented.

Table 5. Level 2 validation: SDCPN-based model vs. Controls

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 (No event)</td>
</tr>
<tr>
<td>1 (No event)</td>
<td>green</td>
</tr>
<tr>
<td>2 (TA)</td>
<td>green</td>
</tr>
<tr>
<td>3 (RA)</td>
<td>green</td>
</tr>
<tr>
<td>4 (RA*)</td>
<td>green</td>
</tr>
<tr>
<td>5 (RAMAC)</td>
<td>green</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model

RA* - RA activated but vertical separation at CPA violated; RAMAC – RA activated but Mid-Air Collision occurred

Situations that are covered in Table 5 are the following:
- No event – case in which there is no need for either TA or RA to be issued;
- TA – case in which a TA is issued;
- RA – case in which an RA is issued and satisfactory resolved (vertical separation at CPA appropriate);
- RA* – case in which an RA is issued but not satisfactory resolved (vertical separation at CPA violated);
- RAMAC - case in which an RA is issued but MAC occur;

Like at previous validation levels, a matrix containing green fields which presents a perfect situation, i.e. situations in which answers to the given question are the same both in the SDCPN-based model and in the Control, for the same case. If the situation falls in the red fields (above and right from the green diagonal) this means that TCAS is not properly activated or not activated at all, and this behaviour of the SDCPN-based model is designated as unwanted from a safety assessment point of view, since the model does not “recognize” the appropriate severity of cases.

Finally, if the situations fall in the yellow filed (below and left from the green diagonal) this means that TCAS was activated in situation when in the Control for the same case TCAS was not activated or it is but it was less severe. Such a situation is considered a false alarm, but it is not negative although it is not wanted from the safety assessment point of view. As in the case of the previous validation level, it might be suggested to improve the model as much as possible if some of the results are different or cases in red or yellow corner exist.

6.2.3 Level 3 - If RA occurs, is resolution manoeuvre similar?

If the answer to the Level 2 question is positive, then at Level 3 for events in which RA is activated the question takes into account the type of resolution manoeuvre (chosen resolution sense). A matrix should be constructed (Table 6), where for each pair of Control and SDCPN-based cases a frequency of occurrence, i.e. number of situations in which certain pair of senses, occurs.
Table 6. Level 3 validation: SDCPN-based model vs. Controls

<table>
<thead>
<tr>
<th>Level 3 Validation</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 (RA)</td>
</tr>
<tr>
<td></td>
<td>u/d</td>
</tr>
<tr>
<td>SDCPN</td>
<td></td>
</tr>
<tr>
<td>1 (RA)</td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
<tr>
<td>2 (RA*)</td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
<tr>
<td>3 (RA_MAC)</td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
</tbody>
</table>

**LEGEND:**
green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model

RA* - RA activated but vertical separation at CPA violated;
RA_MAC – RA activated but Mid-Air Collision occurred
u/d – (up or up-level or no-change)/(down or down-level or no-change) manoeuvre,
d/u – (down or down-level or no-change)/(up or up-level or no-change) manoeuvre

Due to the possibility that a large number of different sense combinations can appear, it was decided to aggregate them into two groups of similar pairs of senses. Aggregation is always a difficult issue and the possibility always exists that some important information and differences between the model and control could remain hidden.

For each cell in the matrix in Table 6 further division is made into pairs of senses, which can be “u/d” or “d/u”, were first letter is related to own aircraft while the second to intruder. “u/d” presents situations in which the own aircraft obtains an up or up-level or no-change sense while intruder aircraft obtains a down or down-level or no-change sense. The similar applies for the “d/u” combination, were own aircraft receives down or down-level or no-change instructions, while the intruder receives the up or up-level or no-change sense. Here, ideally all situations should fall on the upper-left – lower-right diagonal, meaning that manoeuvres (senses) provided both by the Control and the SDCPN-based model are similar. If the situation does not fall onto it, this means that the corresponding manoeuvres (senses) differ.

6.2.4 Level 4 - Are corresponding horizontal and vertical separations at CPA great enough following implementation of the issued RA?

The idea of the validation process in this research is to go into greater detail when we approach deeper levels of validation (from rough to fine information). That is why at Level 4 a graphical comparison between horizontal and vertical separations at CPA following implementation of the issued RA was chosen instead of table, i.e. continuous rather than discrete variables. Usage of a table is avoided due to necessity to perform certain aggregations, which will hide some of the results that are visible in graphical form.

The perfect case would be in situation where both SDCPN and Control data lay on the line, presented with equation $x = y$, meaning that both the Control and the SDCPN-based model have the same horizontal and vertical separation at CPA.

6.2.5 Criteria for passing to the next validation level

In order to pass on the next validation level the following criteria were applied: no events should appear in red cells or bellow $x = y$ line. If the test outcome is not satisfactory, then it is necessary to understand what was causing that. Subsequently the model should be improved and the validation test has to done again.
6.3 Historical Data Validation

Before application in risk/safety assessment, a validation of developed SDCPN model is performed in order to develop trust in it. Only a validated model could be used for risk/safety assessment because its outputs could be considered as credible. A historical data validation is presented here, although a comparison with other models is performed as well, as an alternative before real life data was obtained. The results of the Comparison with other model are presented in Appendix 6, 7, 8, 9 and 10.

6.3.1 Real Life Encounter Data

Sponsored by the German Department of Economy and Technology and supported by the European Agency for Aviation Safety EASA and the German Department of Transportation, the “Institut fur Eisenbahnwesen und Verkehrssicherung” (IfEV) of the Technische Universität Braunschweig developed an experimental 1030/1090MHz-receiver station listening to the SSR-Mode S- and ACAS-communication of aircraft in the airspace over north Germany. During August 2008 this experimental system considerable enhanced with the addition of 5 1030/1090MHz-receiver stations industrially produced by Thales (Gottstein, Form, 2009).

Those stations observe collision alerts and vertical Resolution Advisories (RA) issued by the Airborne Collision Avoidance System (ACAS). The observations are complemented by detailed descriptions of the traffic situation before the ACAS intervention and the actual reaction of the aircraft. Communication of 600 to 800 airliners simultaneously has been received (Gottstein, Form, 2009).

Every ACAS-Event-Report describes, in plain text and in Diagram form, the communicated messages such as the resolution messages, the corresponding coordination replies and the resolution advisory broadcast versus time of arrival at the station. The software also checks the standard conformity of every received message and its logical sense for validation (Gottstein, Form, 2009).

The frequent altitude reports of the aircraft involved were taken from the database for the period starting 3 minutes before and ending 3 minutes after an observed ACAS-Event, to describe precisely their altitude tracks versus the same time interval. The Mode S-addresses of the aircraft are used to also include their tail number, aircraft type and airline in each report. If ADS-B is available, the horizontal situation and horizontal distance versus time is plotted (Gottstein, Form, 2009).

6.3.2 Validation of TCAS SDCPN model vs. Real Life Encounters data

The approach taken in this research is to make validation by comparing the outputs from the developed SDCPN model with Real Life Encounters (Figure 21). Inputs for the comparison are data for seven real life encounters, chosen in a way to represent different conflict situations, provided by TU Braunschweig. This data served as a basis for the preparation (reconstruction and approximation) of inputs data for the TCAS SDCPN-based model (Figure 21).

Although the number of real life encounters was not large, this kind of validation was very valuable due to the fact that it is rarely performed for such models.

---

10 Data were kindly provided by Prof. dr Peter Form and Dipl.-Inf Jens Gottstein from Institut fur Eisenbahnwesen und Verkehrssicherung, TU Braunschweig, Braunschweig, Germany.
The following outputs were chosen:

a) selected sense and strength for the issued RA;

b) minimum horizontal distance at CPA as well as corresponding vertical distance and time;

c) moments when Traffic alert (TA), Resolution Advisory (RA) and Clear of Conflict (CoC) were issued; and

d) vertical and horizontal distance at TA, RA and CoC moments.

The facts that TCAS is activated and RA is issued are considered at Level 1 and Level 2 respectively. From listed outputs only those under a) and b) are used in validation process at Level 3 and Level 4, while c) and d) are used only for illustration (see Appendix 5).

Real life encounter data was used to create inputs for the SDCPN-based model. Namely, the horizontal situation and horizontal distance versus time plots are used for aircraft initial positions and magnetic headings, (Figure 22). Positions are given in the geographical coordinate system. They are read directly from the plots and translated into the Cartesian coordinate system used in SDCPN-based model. Similarly, magnetic headings were calculated taking the coordinates for initial positions and positions in which the Clear of Conflict message was issued, and using basic equations from theory of navigation. Additionally, the time interval between the initial point and point were CoC was issued, allowed for the calculation of ground speed (Figure 22).

Aircraft initial altitudes are calculated using the vertical situation versus time plot. As was the case with headings, the rates of descend/climb is calculated using the vertical differences between altitudes at the aircraft initial position and position at which the RA message was issued, and time between those two positions (Figure 23). All the variables determined by the previous method are used in the model having constant values, while in real life encounters they aren’t constant.

Using this input data SDCPN-based model produces outputs which are used for validation, together with the real life data. The results of the comparison are provided separately for each scenario and for the given test variable, in tabular as well as in graphical form, in Appendix 5. The validation results are presented in the following text.
Figure 22. Example of reconstruction (approximation) of initial positions, ground speeds and magnetic headings.

Figure 23. Example reconstruction (approximation) of rate of climb.
Records on seven real life encounters were available. They were used to run TCAS SDCPN model providing the replication of these seven encounters.

The results of Level 1 validation are presented in Table 7. It was shown that in 7 out of 7 available cases (encounters) TCAS was activated both in reality and in the SDCPN-based model. The results are in green field, meaning that satisfactory validation results were obtained.

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>Real Encounter Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 (no)</td>
</tr>
<tr>
<td>1 (no)</td>
<td>0</td>
</tr>
<tr>
<td>2 (yes)</td>
<td>0</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model

Table 8 presents the results of Level 2 validation. It was shown that in 6 out of 7 available cases (encounters) TCAS generated a RA both in reality and in the SDCPN-based model (results are in the green fields, meaning that satisfactory validation results were obtained). But, in 1 out of 7 a TA only is issued in the SDCPN-based model instead of RA which was activated in reality, placing it in a red field. Additional analysis showed (see Encounter 5 in Appendix 5) that trajectories of aircraft in given case were not converging or crossing and aircraft were laterally and vertically well separated when the RA was issued, therefore there is a possibility that in reality this case was false alarm. Because proof for this does not exist, although this situation is unwanted; it was decided to pass on Level 3 validation.

<table>
<thead>
<tr>
<th>Real Life Encounter Data</th>
<th>1 (no event)</th>
<th>2 (TA)</th>
<th>3 (RA)</th>
<th>4 (RA*)</th>
<th>5 (RA_{MAC})</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDCPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (no event)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 (TA)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 (RA)</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4 (RA*)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 (RA_{MAC})</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model
RA* - RA activated but vertical separation at CPA violated; RA_{MAC} – RA activated but Mid-Air Collision occurred

Table 9 presents the results of the Level 3 validation. It was shown that in 4 out of 6 available cases (encounters) resolution manoeuvre, i.e. issued sense, was similar both in reality and in the SDCPN-based model. In two out of 6 cases manoeuvre was different (see red numbers in Table 9) but still cases were resolved and satisfactory separation at CPA was achieved (see Level 4 results), implying that different senses does not mean they are wrong. But, it seems it should be considered that there might be more than one solution for certain encounters. This could be the explanation for the differences that appear at this level.

Also, aggregation of similar senses into two groups could be the potential reason for differences. Although certain differences exist, it seems that in encounters involving two aircraft such aggregation would be suitable, while in encounters with three or more aircraft involved, the chosen senses are very sensitive to encounter geometry. So, disaggregation of similar senses could be additionally considered for such encounters.
### Table 9. Level 3 validation: TCAS SDCPN model vs. Real Life Encounters Data

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>Real Life Encounter Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 (RA)</td>
</tr>
<tr>
<td></td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
<tr>
<td></td>
<td>2 (RA*)</td>
</tr>
<tr>
<td></td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
<tr>
<td></td>
<td>3 (RA_MAC)</td>
</tr>
<tr>
<td></td>
<td>u/d</td>
</tr>
<tr>
<td></td>
<td>d/u</td>
</tr>
</tbody>
</table>

**LEGEND:** green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model.

RA* - RA activated but vertical separation at CPA violated; RA_MAC - RA activated but Mid-Air Collision occurred.

Under Level 4 validation, in Figure 24, correspondence between TCAS SDCPN-based model data and Real encounter data are presented. It can be seen that the SDCPN-based model provides vertical distances which are systematically overoptimistic (in the order of thousand feet) compared to reality (points presenting an RA are placed above x = y line (Figure 24)). Explanations for that are the following:

a) Inputs for the SDCPN-based model are obtained by reconstructing the real event. Such a procedure probably generated certain errors in input values because it uses the average ground speed, rate of descent/climb and magnetic heading values (see Figures 22 and 23). Additionally, a geographic coordinate system from reality was transformed into the Cartesian coordinate system in the SDCPN model used. This transformation could be additional source of errors in the aircraft position input;

b) RA strength in the SDCPN-based model was assumed to have the maximal value, from the suggested range of strength values, while the applied values in reality are from the range given to pilots. That is why vertical separations are greater in the SDCPN-based model (all of them are at or above the x = y line);

c) The SDCPN-based model assumes that intruder tracking performed perfectly. In reality this occurs with a systematic delay according to an alpha-beta filtering approach;

d) Certain differences in TCAS logic could also be a reason for differences, especially due to the possibility that aircraft in the real encounters were equipped with TCAS II equipment by different manufacturers, while in the SDCPN-based model all aircraft were equipped with the same TCAS II. All manufacturers should satisfy minimum requirements for TCAS II, but it could be expected that some additional differences in logic might exist. Also, the SDCPN logic is based on documents dating from 2000, while TCAS in reality may contain logic that is newer and probably enhanced, relative to the document from 2000.

Because of the systematic overoptimistic outcome for level four it is recommended that the SDCPN model be improved for the issues identify above (see a)-d)) and then that the validation for the improved SDCPN model be repeated.

It could be concluded that the first two validation levels were passed satisfactorily but in the third and fourth some differences appeared which did not pass the validation test. The validation tests also provided feedback about the necessary model requirements to be met in further research.
Figure 24. Level 4 validation: TCAS SDCPN model vs. Real Life Encounters Data
7 ILLUSTRATION OF THE MODEL APPLICATION

A real life accident is taken for illustration of the developed SDCPN model of ACAS operations. Namely, a collision between Inex Adria DC9 and British Airways Trident 3 which occurred on September 10, 1976 over VOR Zagreb (former Yugoslavia) at FL330 (DoT, 1977, 1982). TCAS was not in use at the time of collision.

7.1 Event Validity

“Event validity” is a validation technique (Sargent, 2009) in which occurrences of the simulation model are compared to those of the real system to determine if they are similar. For that purpose a real life accident data without TCAS involvement is used.

A Collision between Inex Adria DC9 and British Airways Trident Three, which occurred on September 10, 1976 over VOR Zagreb (former Yugoslavia) at FL330, was chosen for validation (DoT, 1977, 1982). TCAS was not in use at the time of collision, therefore geometry of the collision is used for checking event validity.

Figure 25 shows a schematic representation of the collision location as well as the flight paths of both aircraft several minutes before collision (DoT, 1977, 1982). Figure 26 contain a detailed horizontal situation and Figure 27 presents a detailed vertical situation (both 32 seconds before collision) (DoT, 1982). Figure 26 and 27 are used to reconstruct the encounter and to prepare inputs for the TCAS SDCPN simulation (Table 10).

Due to the SDCPN assumption that vertical speed is constant an average vertical speed (rate of climb) is calculated according to aircraft altitudes in the last 32 seconds before collision and also with the aim to place both aircraft in the same point at moment t = 0 sec. The obtained value for rate of climb was 1670fpm. Also, magnetic heading for British Airways aircraft was decided to be 115.5° (the heading actually varied between 115° and 116° (Figure 25)). After the reconstruction, the event is placed in a Cartesian coordinate system with horizontal distances given in Nm.

Table 10. Encounter geometry (input)

<table>
<thead>
<tr>
<th></th>
<th>Own aircraft</th>
<th>Intruder aircraft</th>
</tr>
</thead>
<tbody>
<tr>
<td>X coordinate</td>
<td>19.69 Nm</td>
<td>3.56 Nm</td>
</tr>
<tr>
<td>Y coordinate</td>
<td>4.54 Nm</td>
<td>26.78 Nm</td>
</tr>
<tr>
<td>Height</td>
<td>29620 ft</td>
<td>32960 ft</td>
</tr>
<tr>
<td>Magnetic Heading</td>
<td>353°</td>
<td>115.5°</td>
</tr>
<tr>
<td>Ground Speed</td>
<td>465 kt</td>
<td>476 kt</td>
</tr>
<tr>
<td>Vertical Speed</td>
<td>1670 fpm</td>
<td>0 fpm</td>
</tr>
</tbody>
</table>

The SDCPN simulation was performed using data from Table 10 without active TCAS. The obtained results are presented in Table 11. Real values for horizontal and vertical separation are taken from Figures 26 (horizontal distances were transformed into Nm) and 27, respectively.
Figure 25. Schematic representation of the collision location and flight paths before collision (taken from (DoT, 1977))
Figure 26. Detailed horizontal situation 32 second before collision (taken from (DoT, 1982))
Figure 27. Detailed vertical situation 32 seconds before collision (taken from (DoT, 1982))
Pairs of real vs. simulated data which are very similar are represented in grey cells in Table 11. Simulated values are lower than real one for 0.02Nm (37m) in periods 32, 25, 16 and 6 seconds before collision. At the moment of collision, the simulated value is greater than 0.08Nm (148m). The remaining cells provide pairs of data with significant differences. It can be noted from Table 11 that the horizontal distances obtained with the SDCPN simulation are almost the same as those given in the accident investigation reports. Naturally vertical values are different. A reason for the difference is the SDCPN assumption that vertical speed was constant during the encounter. Only the vertical separation at the time of collision is the same. The geometry of simulated encounter is shown in Figure 28.

A new encounter is set up in order to decrease the differences in the vertical separation; namely a new value of 1688 fpm is used for the average rate of climb. This value represents the rate between 32 and 16 seconds before collision, during which period aircraft DC9 was stable in the vertical plane. Inputs for this encounter are provided in Table 12 and the comparison results are presented in Table 13. More similarities are present in the vertical separation values (see grey cells) which are now lower by only 1 ft in moments 32 and 16 seconds before collision, and 2 ft higher in moment 25 seconds before collision, while horizontal separations remain the same as in Table 11.

### Table 12. Modified encounter geometry (input)

<table>
<thead>
<tr>
<th></th>
<th>Own aircraft</th>
<th>Intruder aircraft</th>
</tr>
</thead>
<tbody>
<tr>
<td>X coordinate</td>
<td>19.69 Nm</td>
<td>3.56 Nm</td>
</tr>
<tr>
<td>Y coordinate</td>
<td>4.54 Nm</td>
<td>26.78 Nm</td>
</tr>
<tr>
<td>Height</td>
<td>*30025 ft</td>
<td>32960 ft</td>
</tr>
<tr>
<td>Magnetic Heading</td>
<td>353°</td>
<td>115.5°</td>
</tr>
<tr>
<td>Ground Speed</td>
<td>465 kt</td>
<td>476 kt</td>
</tr>
<tr>
<td>Vertical Speed</td>
<td>*1688 fpm</td>
<td>0 fpm</td>
</tr>
</tbody>
</table>

* new values relative to Table 14.

### Table 13. TCAS SDCPN vs. Real Life Encounter Data without TCAS (modified)

<table>
<thead>
<tr>
<th>Time before collision [sec]</th>
<th>Horizontal separation [Nm]</th>
<th>Vertical separation [ft]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Real</td>
<td>TCAS SDCPN</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0.08</td>
</tr>
<tr>
<td>-6</td>
<td>1.38</td>
<td>1.36</td>
</tr>
<tr>
<td>-16</td>
<td>3.67</td>
<td>3.65</td>
</tr>
<tr>
<td>-25</td>
<td>5.74</td>
<td>5.71</td>
</tr>
<tr>
<td>-32</td>
<td>7.34</td>
<td>7.32</td>
</tr>
</tbody>
</table>
Comparison of outputs from the TCAS SDCPN simulation model with occurrences of the real collision shows significant similarity. This analysis helped to decide that the developed SDCPN model is credible for illustration purposes.

Figure 28. Geometry of the simulated encounter (without TCAS activity) (Note: headings and rate of climb are not in scale)
7.2 Illustration

According to the detailed vertical and horizontal situation in the last 32 seconds before collision an encounter is reconstructed and input data for the simulation of TCAS operation is prepared (Table 14). The main assumption is that the DC-9 is the Own aircraft.

<table>
<thead>
<tr>
<th>Own aircraft</th>
<th>Intruder aircraft</th>
</tr>
</thead>
<tbody>
<tr>
<td>X coordinate</td>
<td>19.69 Nm</td>
</tr>
<tr>
<td>Y coordinate</td>
<td>4.54 Nm</td>
</tr>
<tr>
<td>Height</td>
<td>29620 ft</td>
</tr>
<tr>
<td>Magnetic Heading</td>
<td>353°</td>
</tr>
<tr>
<td>Ground Speed</td>
<td>465 kt</td>
</tr>
<tr>
<td>Vertical Speed</td>
<td>1670 fpm</td>
</tr>
</tbody>
</table>

Results of the TCAS SDCPN simulation are provided in Table 15, Figures 29 and 30. If TCAS II would have existed at the time of the accidents, it could have prevented a collision by issuing a TA 73 sec, RA 86 sec and CoC 122 sec, from the beginning of the encounter.

The estimated minimum horizontal and vertical separations at CPA are 0.08Nm and 1933ft, respectively. Own aircraft would have received a Downward sense RA while the Intruder aircraft would have received an Upward sense RA.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA [sec]</td>
<td>73</td>
</tr>
<tr>
<td>RA [sec]</td>
<td>86</td>
</tr>
<tr>
<td>CoC [sec]</td>
<td>122</td>
</tr>
<tr>
<td>TA Vertical Distance [ft]</td>
<td>1308.00</td>
</tr>
<tr>
<td>Horizontal Distance [Nm]</td>
<td>10.75</td>
</tr>
<tr>
<td>RA Vertical Distance [ft]</td>
<td>946.00</td>
</tr>
<tr>
<td>Horizontal Distance [Nm]</td>
<td>7.77</td>
</tr>
<tr>
<td>CoC Vertical Distance [ft]</td>
<td>2011.00</td>
</tr>
<tr>
<td>Horizontal Distance [Nm]</td>
<td>0.48</td>
</tr>
<tr>
<td>Sense Own/Intruder Aircraft</td>
<td>Down/Up</td>
</tr>
<tr>
<td>Strenght [fpm]</td>
<td>(170,-330)/ (1500, 2000)</td>
</tr>
<tr>
<td>Minimum Separation</td>
<td></td>
</tr>
<tr>
<td>Vertical [ft]</td>
<td>1933.00</td>
</tr>
<tr>
<td>Horizontal [Nm]</td>
<td>0.08</td>
</tr>
<tr>
<td>Time from beginning of the encounter [sec]</td>
<td>120</td>
</tr>
</tbody>
</table>
ILLUSTRATION OF THE MODEL APPLICATION

Figure 29. Horizontal situation of the simulated encounter (Note: headings are not to scale)

Figure 30. Vertical situation of the simulated encounter (Note: rates of climb/descent are not to scale)
8 CONCLUSION

The aim of the research described in this dissertation was to make a contribution through the systematic development of an unambiguous model of ACAS operation, i.e. TCAS II version 7, including its interactions with pilots and air traffic controllers.

The research resulted in a model that is intended for risk/safety assessment of ACAS operations and which would allow for the assessment of the possible benefit of ACAS in risk reduction in current and advanced ATC/ATM.

The specific modelling formalism used was Stochastically and Dynamically Coloured Petri Nets (SDCPN). It was shown that the SDCPN representation is very powerful and allows the modeller to represent all elements of such a complex (technical elements, pilots, air traffic controllers, procedures in force), dynamic and stochastic system, as well as interactions between them in a flexible and modular way. It was also concluded that it is quite simple to develop computer code following the SDCPN formalism. Such a way of ACAS operations modelling has not been used previously and was chosen to be complementary and easy added to certain previously developed SDCPN models of existing or future operational concepts, providing assessment of the benefits of the safety net in it. Modularity and flexibility of the SDCPN model was an important feature for the mentioned purpose. The model could also be used as standalone.

The fact that the model is stochastic and dynamic allows for its use in the Monte Carlo simulation of rare events, such as aircraft collisions, repeating the experiments many times (order of magnitude $10^{10}$) and tracing back in order to determine the chain of events leading to collision. However, in this research this kind of application, i.e. risk assessment itself, was not performed.

Apart from model development, attention was given to validation in order to develop trust in the model and to use it as a credible tool for safety assessment purposes of current and future ATM operational concepts.

A validation process consisting of four successive validation levels is proposed in this research and applied to historical data, in which a set of seven different real life encounters was compared to simulation outputs of the developed SDCPN-based model. Although the number of real life encounters was not large, this kind of validation was very valuable due to the fact that it is rarely performed for such kind of models. Apart from this, an additional validation was performed comparing the developed model with a similar model (InCAS).

It could be concluded that the first two validation levels were passed satisfactorily but in the third and fourth some differences appeared which did not pass the validation test. The validation tests also provided feedback about the necessary model requirements to be met in further research.

After validation, model application is illustrated on a real life accident. Namely, the collision between Inex Adria DC9 and British Airways Trident 3, which occurred on September 10, 1976 over VOR Zagreb (former Yugoslavia) at FL330. ACAS was not in use at the time of collision. The SDCPN model was proven to work well - if TCAS II had existed at the time of the accidents, it could have prevented a collision.
Further research steps are proposed. The developed SDCPN-based model could be applied as standalone in certain characteristic cases (encounters) for risk/safety assessment with the aim of estimating possible benefits of risk reduction of airborne safety nets. Additionally, further improvement of TCAS SDCPN-based model and Conceptual model of TCAS Logic is needed in order to make the model suitable for application in advanced ATC/ATM operational concept validation. Finally, the developed model should be integrated in broader model for risk and safety assessment of existing or future operational concepts, which will show the full benefit of airborne safety nets.
REFERENCES


REFERENCES


Dean G., TCAS Analysis of safety events using InCAS, Eurocontrol Experimental Centre (presentation), 2007.


Department of Trade (DoT), Accident Investigation Branch, Aircraft accident report 9/82, British Airways Trident G-AWZT and Inex Adria DC9 YU-AJR, Report on the collision in the Zagreb Area, Yugoslavia, on 10 September 1976”, 1982.

Department of Transportation (DoT), Federal Aviation Administration, Introduction to TCAS II Version 7, USA, 2000.


REFERENCES


References


REFERENCES


INTRODUCTION

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

Physically and operationally, the air transport system is a rather complex system with the main components - airlines, airports and air traffic control services - interacting with each other on different hierarchical levels constituting a very complicated, highly distributed network of human operators, procedures and technical/technological systems. In particular, risk of accidents and related safety in such a complex system is crucially influenced by interactions between the various components and elements. This implies that providing a satisfactory level of safety (i.e., low risk of accident) is more than making sure that each of the components and elements functions safely (Blom et al, 1998). Due to such inherent complexity and severe consequences of accidents, risk and safety have always been considered as issues of the greatest importance for the contemporary air transport system (Janic, 2000).

Consequently, they have been a matter of continuous research from different aspects and perspectives ranging from the purely technical/technological to the strictly institutional. In general, the former have dealt with design of safe aircraft and other system facilities and equipment. The later have implied setting up adequate regulations for system design and operations.

The objective of this paper is to present a review of part of the research dealing with risk and safety in the contemporary civil aviation system. The paper particularly focuses on the methods/models for assessment of the risk and safety of individual aircraft and Air Traffic Control/Management (ATC/ATM) operations, aircraft collisions, human factor errors, and the effect on airport third parties.

11 The material in this Part is published as:

Netjasov F., Janic M., A Review of the Research on Risk and Safety Modelling in Civil Aviation, Proceedings of “3rd International Conference on Research in Air Transportation ICRAT 2008”, Fairfax (VA), USA, June 1-4, 2008, pp. 169-176 (in English)

CONCEPTS AND DEFINITIONS OF RISK AND SAFETY

For a long time, risk and safety have been differently and ambiguously interpreted depending on the system and purpose (Kumamoto and Henley, 1996). For technical systems, risk is related to the chance of failure of components or of the entire system causing exposure to hazard and related consequences.

In economic business systems, risk is a chance of being exposed to the hazard of losing business opportunities and/or money due to making decisions under uncertain circumstances. In social systems, risk is the chance of being exposed to the hazard of injuries and/or losing of life. Consequently, risk could be considered as combination of the probability (or frequency of occurrence) and the magnitude of consequences (or severity) of a hazardous event (Bahr, 1997).

In the air transport system, risk and safety have always been related to air traffic accidents which resulted in the significant loss of life and property (aircraft and the property on the ground). Assuming that making an air trip is an individual choice and that the system deploys some resources to satisfy such choice, four types of risks can be identified in the air transport system (Janic, 2000):

i) **Real risk to an individual** (determined on the basis of future circumstances after their full development, frequently incorporated in decisions on introduction of new aerospace technologies in any system component);

ii) **Statistical risk of occurrence of an accident** (important for companies providing insurance, determined by the available statistical data on the incidents and accidents);

iii) **Predicted risk** (important for air transport authorities while introducing changes in technologies and air traffic patterns, determined from methodologies using some relevant historical research); and

iv) **Perceived risk** (important for users of the air transport system and determined by the individual’s intuition, feeling and perception).

In addition, air traffic accidents may have some features distinguishing them from accidents in other transport modes as follows (Janic, 2000):

i) They may occur at any point in time and space mainly because flights may take place over large areas;

ii) The primal target groups exposed to the risk exposure are passengers and crew; in addition, individuals on the ground may be exposed but generally have a lower probability of losing life or property;

iii) They are relatively rare events but usually with severe consequences;

iv) Conditionally, each of them can be classified as an inherently risky although highly unlikely (but still possible) event; and v) risk of an accident is inherently present during the time of a flight.

In the above-mentioned context, assessing the risk of occurrence of an air traffic accident with the associated consequences can be used as a measure of the system safety for people, systems and environment.
OVERVIEW OF THE METHODS/MODELS FOR ASSESSMENT OF THE RISK AND SAFETY

Risk implies exposure of an individual to the hazard of an air traffic accidental event such as the aircraft crash, collision between aircraft, and/or collision between the aircraft and terrain. This could result in losing life or getting severe injuries both onboard the aircraft and/or on the ground, damaging and/or destroying property (the aircraft and eventually buildings on the ground), and contamination of the environment (water and soil) by burning and/or leaking fuel and oil, and hazardous cargo. Analyzing air traffic accidents and their consequences classification of the methods/models of the risk and safety assessment is determined as follows:

i) **Causal methods/models for risk and safety assessment of aircraft and ATC/ATM operations.** This category deals with assessment of risk and safety of aircraft operations supported by ATC/ATM. In particular, it deals with failures of particular technical systems and components resulting in the aircraft crash. The failures can be due to many interrelated causes and happen either in the aircraft or at ATC/ATM;

ii) **Collision risk methods/models** are dealing with assessment of the risk of aircraft collision while airborne and/or on the ground due to deterioration of ATC/ATM separation rules;

iii) **Human factor error methods/models.** This category deals with risk and safety assessment of air traffic incidents and accidents due to human error, and

iv) **Third-party risk methods/models.** This category of methods/models considers the risk assessment for people on the ground, who might be affected by the aircraft crash.

The main criterion for selection of particular methods/models has been the authors’ judgment about their both theoretical importance and practical contribution. Also, authors’ are focusing on proactive modeling approach, i.e. on methods/models which are attempting to anticipate problems before accidents occur.

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

Causal methods/models of assessment of risk and safety of aircraft and ATM/ATC operations establish the theoretical framework of causes that might lead to aircraft accidents. These methods/models can be qualitative or quantitative. The former provide a diagrammatic or hierarchical description of the factors that might cause accidents. They are useful for improving understanding of causes of accidents and proposing preventive interventions. The later estimate the probability of occurrence of each cause and hence estimate the risk of accident. They might be restricted to pure statistical analysis based on the available data or combine these data with expert judgment on the accident causes. In addition, they can estimate the relative benefits of different interventions aiming at preventing accidents in the future (FAA/EUROCONTROL, 2005; Spouge, 2004). Some of the methods/models are as follows:
**Fault Tree Analysis (FTA)** is a method developed by Bell Telephone Laboratories, US in 1961 (Kumamoto and Henley, 1996) and has been used for analyzing events or combinations of events that might lead to a hazard or an event with serious consequences. Usually, the analysis has been carried out using a fault tree with several paths representing different combinations of instant-direct and intermediate causes described with logical operators (“and” and “or”). At the top of the tree there is a hazard event or a serious consequence. Then, for a given tree the minimum cut set has been determined, i.e., the minimal set of failures of which if all happen causes the top event to happen too. One fault tree might have several minimal cut sets, and if only one happens, the top event also happens. The probability of occurrence of given minimum cut sets is equivalent to the product of probabilities of occurrence of each event within the set. Consequently, the probability of the occurrence of the top event is equal to the sum of probabilities of particular minimum cut sets. The method has been frequently applied (as the best recommended) to assessment of risk and safety as well as reliability of the aircraft and ATC/ATM computer (hardware) components;

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

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

**TOPAZ accident risk assessment methodology** is a complex method that uses scenario analysis and a Monte Carlo simulation technique for assessment of the risk and safety of ATC/ATM operations modeled as a Petri Nets. It has been developed by NLR (The Netherlands National Aerospace Laboratory) during the 1990’s. The method addresses all types of system safety issues such as technical/technological, organizational, environmental, and human-related and other hazards and their combinations. Risk and safety assessment is performed through few steps enabling identification of safety bottlenecks. The method has been widely applied to risk assessment of ATC/ATM operations (FAA/EUROCONTROL, 2005);

**Bayesian Belief Networks (BBN)** is a method based on probability theory, which has been developed to improve understanding of the impacts of different causes on the risk of aircraft accidents (originating from mid of 1980’s, applied in aviation filed at beginning of
2000’s). The method is supposed to capture the wide range of failures of aircraft systems both qualitatively and quantitatively and thus provide rather objective and unambiguous information on the state of system safety relevant for the managerial decisions (Luxhoj and Coit, 2006; Roelen et al, 2003a, 2003b). The method has been applied as a decision-support tool to calculate effects of specific changes to the aviation system on the overall risk as well as support in developing a proactive policy by providing an insight into the effects of anticipated system changes on risk.

Purpose

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

i) Better understanding of effects of different influencing factors on level of risk;

ii) Evaluation of overall risk, risk communication, and cost-benefit analysis of new technologies;

iii) Training of aviation staff and identification of system components that could be improved; and

iv) Identifying “critical” causes of the aircraft accident as well as measures for reducing risk. For example, in order to decide which measures for risk reduction should be adopted; regulators and safety managers need an understanding of causes of accidents and an ability to evaluate benefits of various interventions. These methods/models can support these decisions (Spouge, 2004).

All mentioned methods/models are quantitative except the CCA. Related to risk types given in Section 6, it could be mentioned that FTA, ETA and CCA are generally used to determine “statistical risk” of occurrence of an accident or failures, while Bow-Ties, TOPAZ and BBN - “predicted risk” of system changes such as introduction of new technologies, procedures, operations, etc.

Problems

The causal methods/models are data driven and highly dependant in their quality on the one hand and the expert judgment about combinations of particular causal factors of the air traffic accidents on the other. Quantification of these methods/models has appeared extremely difficult and time consuming mainly due to the complexity of combinations of causal factors leading to possible accidents. In addition, calculation of probabilities and conditional probabilities in situations where dependencies between particular causal factors have not completely been known further complicates quantification of the methods/models. As well, one important problem has been the cumulative nature of these methods/models, which could make assessment of particular probabilities difficult due to the large number of causal factors and their combinations (Roelen et al, 2003a). Consequently, in some cases it has been rather difficult to express results from these methods/models in a transparent and comprehensible way (Spouge, 2004).
Collision risk methods/models

One of the principal matters of concern in the daily operation of civil aviation is preventing conflicts between aircraft either while airborne or on the ground, which might escalate to collision. Although aircraft collisions have actually been very rare events contributing to a very small proportion of the total fatalities, they have always caused relatively strong impact mainly due to relatively large number of fatalities per single event and complete destruction of the aircraft involved. In general, separating aircraft using space and time separation standards (minima) has prevented conflicts and collisions.

However, due to reduction of this separation in order to increase airspace capacity and thus cope with growing air transport demand, assessment of the risk of conflicts and collisions under such conditions has been investigated using several important methods/models as follows (Machol, 1995, Shortle et al, 2004):

• **The Reich-Marks model** is developed in early 1960’s by Royal Aircraft Establishment, UK (Reich, 1966). It is based on the assumption that there are random deviations of both aircraft positions and speeds from the expected. The model was developed to estimate the collision risk for flights over the North Atlantic and consequently to specify appropriate separation rules for the flight trajectories (Shortle et al, 2004). The model computed the probability of aircraft proximity and the conditional probability of collision given the proximity. Aircraft were represented as three-dimensional boxes, i.e., rectangular parallelepipeds, of given length, width and height reflecting the ATC/ATM minimum separation rules. The collision might occur whenever any two boxes intersected. As well, when one aircraft was represented as the dimensionless point, conflict occurred when the point entered the box. In such a context the collision risk with the vertical, lateral and longitudinal neighbor could be determined independently of each other bearing in mind that the position errors of boxes and points representing the aircraft along their tracks were random variables with zero mean and given standard deviations. Consequently, the prescribed lateral distance between aircraft could be specified with given probability of violation reflecting the acceptable collision risk (Machol, 1995; FAA/EUROCONTROL, 1998);

• **The Machol-Reich model** was developed after the ICAO had established the NAT SPG (North Atlantic System Planning Group) in 1966 with the idea of creating the Reich-Marks model as the workable tool as well as increase of airspace capacity. The modified model using actual data for the position error (collected for about 14000 flights) enabled prediction with moderate confidence of each of the vertical, horizontal and longitudinal collision risks. Consequently, the ICAO NAT SPG has adopted the threshold for risk of collision of two aircraft due to the loss of planned separation (Machol, 1975, 1995);

• **The intersection models** belong to the simplest collision risk models. They are based on assumptions that aircraft follow pre-determined crossing trajectories at constant speeds. The probability of a collision at the crossing point is computed using the intensities of traffic flows on each trajectory, aircraft speeds, and the airplane geometry (Siddiqee, 1973; Geisinger, 1985; Barnett, 2000);

• **The geometric conflict models** are similar to the intersection models. In these models (developed in 1990’s) the speed of any two aircraft is constant, but their initial three-dimensional positions are random. Based on extrapolating their positions in time, it is possible to geometrically describe the set of initial locations that eventually lead to a conflict. The conflict occurs when two aircraft are closer than the prescribed separation rules.
After integrating the probability density of the initial aircraft positions over the conflicting region, the conflict probability can be estimated (Paielli and Erzberger, 1997, 1999); (Irvine, 2002);

- **Generalized Reich model** was developed by removing restrictive assumptions of Reich model based on the fact that Reich model does not adequately cover some real air traffic situations. The model was based on the hybrid-state Markov processes, aiming to cover a larger variety of air traffic situations. The resulting collision risk equals the probability of collision between two aircraft. Such a generalized collision model was developed during 1990’s and has been used as part of the TOPAZ methodology (mentioned in previous Section) (Blom et al, 1998, 2003; Shortle et al, 2004; Bakker and Blom, 1993; Blom and Bakker, 2002; Bakker et al, 2000).

**Purpose**

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

**Problems**

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

a) Complexity and cost of collecting the enormous amount of data on aircraft three-dimensional positions necessary to define the related statistical distributions (Machol, 1975; Stachtchenko, 1965);

b) Inherent complexity of the generic collision risk method/model as the result of the modeling approach (closer to the reality). New versions of these methods/models such as those used in TOPAZ are even more complex because they embrace more details when calculating risks, such as possible failure of some technical systems (engine, avionics, etc.) or flight crew awareness or fatigue; and cover complex relationships between elements of the system (flight crew, aircraft, ATC/ATM system, other aircraft, etc. (Rouvroye and van den Bliek, 2002));

c) Inherent danger of misunderstanding or no understanding from the average user’s point of view mainly due to complexity. This requires of the specialists a long and costly familiarization time (GAIN, 2003);
d) The lack of risk-predicting capability with high degree of confidence and bias and uncertainty of the obtained results. Additional time and expertise for calculation of the credible risk intervals are needed (Everdij et al, 2006);

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

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

Human factor error methods/models

Investigation of causes of particular air traffic accidents has identified “human error” as one of the most frequent causes (Boeing, 2006). Human error is considered as an incorrect execution of a particular task, which as an event, triggers a series of consecutive errors in execution of other tasks, finally resulting in serious consequences – an aircraft accident – crash. Therefore, monitoring and modeling of human errors in the aircraft and ATC/ATM operations aiming at discovering and preventing them have always been high on the research agenda of both academics and practitioners dealing with civil aviation. Consequently, many methods for detection and prevention of “human errors” have been developed; some of them are (FAA/ EUROCONTROL, 2005):

• **HAZOP (Hazard and Operability) method** (developed in early 1970’s) aims at discovering potential hazards, operability problems, and possible deviations of the actual from the system intended operational conditions (states) including estimating the probability of escalation into a serious event. The method was intended to deal with human errors in complex technical systems such as chemical and nuclear plants having human operator in their control loop. Later on, the UK NATS (National Air Traffic Service) applied the method to different aspects of planning and assessing hazard in operation of the national ATC/ATM, particularly for identification of hazards due to human failures that might develop into risk of air traffic accidents (HAZOP can provide input to FTA and ETA, mentioned in Section 7.1);

• **HEART (Human Error Assessment and Reduction Techniques)** was developed in 1985 for identifying and quantifying errors in an operator’s task. It simultaneously considers particular ergonomic and other environmental factors, which might compromise the required operator’s performance. The impact of a particular (each) factor on the operator’s error while performing particular tasks can be quantified. Then the probability of error in executing a given task (or a series of tasks) can be estimated. The method has been applied by the UK NATS in combination with other methods for identification of the human errors in ATC/ATM;

• **TRACER-Lite (Technique for the Retrospective Analysis of Cognitive Errors)** was developed in 1999 by NATS, for predicting human errors and deriving error prevention measures in ATC/ATM. The method is retrospective, i.e., it is used for classifying types of errors contributing to the air traffic incidents, which have already happened. The method has a modular structure with three modules: the context; the error discovery; and the error recovery.
Hierarchical Task Analysis enabling identification of the “set of critical” tasks, critically influencing safety, usually classifies the human errors;

- **HERA (Human Error in ATM)** is the retrospective method providing insight into ATC/ATM controllers’ cognitive processes while dealing with air traffic incidents (developed at EUROCONTROL at beginning of 2000’s). The method consists of two parts: a retrospective part for the incident analysis; and a prospective part using the information collected on the assessment of probability of human error in cases of compromised safety. Consequently, the method enables better understanding of the constraints and conditions under which ATC/ATM controllers operate. These conditions are important for understanding ATC/ATM controllers’ incompliance with existing procedures and skill-related errors;

- **HFACS (Human Factor Analysis and Classification System)** is method developed at beginning of 2000’s in USA, as a system to categorize latent and immediate causal factors that have been identified in aviation accidents. It is based on analysis of hundreds of aviation accident reports and main purpose is to provide a framework for accident investigations and to serve as a tool for accident trends assessment. HFACS uses four levels of failure: i) unsafe acts; ii) preconditions for unsafe acts; iii) unsafe supervision and iv) organizational or cultural influences. The method is very promising for analysis of air traffic controller errors and failures in ATC/ATM and is effective for understanding the antecedents of operational errors for air traffic safety analysis.

**Purpose**

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

**Problems**

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

a) Most activities in ATC/ATM and in particular, factors influencing human operator performance and possible errors have usually been considered in isolation, i.e., independently on each other; in many cases the quantitative information has exclusively relied on expert judgment;
b) Only specialists in “human factors” have been able to use these methods/models efficiently and effectively; i.e., it has been time consuming and almost impossible to apply these methods/models in an operational environment without specialists; 

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

**Third-party risk methods/models**

Third-party risk implies risk if an individual on the ground to be killed by crashing aircraft. In such a case, the accident is called a “groundling accident” or “groundling crash” and the fatality a “groundling fatality”. Since most air traffic accidents (about 70% according to (Boeing, 2006)) happen around airports, the concept and assessment of third-party risk has been mainly focused on areas around airports. In a given context, the basic assumption has been that risk always exists, cannot be reduced to zero and should be predictable, transparent, and controllable, as well as quantifiable and measurable. Modelling of third-party risk has shown promise in resolving these problems including setting up thresholds for acceptable risk around airports (Ale, 2002; Ale et al, 2000; Rabouw et al, 2001). Three cases of assessment of the third-party risk are illustrated as follows:

- **USA case** - generally implies assessment of the risk an individual is exposed to when at some distance from a given airport during the period of a year. For such a purpose, relevant statistics on fatalities from official sources have been collected and the prospective number of ground fatalities estimated. The estimation has been carried out by multiplying two independent variables – the number of crashes around airports and the number of fatalities per individual crash. The model has shown that the probability of being killed by crashing aircraft has decreased more than proportionally with increasing distance from the airport and increased with increase in the volume of the airport traffic at distances up to about two miles. The model has not considered spatial variability of the risk due to changing residence locations and the aircraft flight paths around the airports, which might be considered as its main disadvantage (Rabouw et al, 2001);

- **The Netherlands case** - this method was developed by the NLR, inspired by the crash of cargo aircraft in the Bijlmer district of Amsterdam in 1992. Method contain the following elements (Ale et al, 2000; Hale, 2002): i) the accident probability model, which calculates the probability of an aircraft accident in the vicinity of an airport depending on the probability of an accident per aircraft movement and the annual volume of airport traffic; ii) the accident location probability model, which calculates the probability of a given location becoming an accident scene depending on its position relative to airport runways and the incoming and outgoing aircraft trajectories; and iii) the accident effect model, which combines output from both previous models to calculate the probability of an accident at each location within the area surrounding a given airport. Individual and societal risks have been used as measures of third-party risk. After calculating the individual risks for the entire area around given airport, the risk contours can be plotted on the horizontal plane (Ale et al, 2000). Societal risk applies to the entire area around a given airport and actually exists only when people are actually present in the area (Ale et al, 2000; Hale, 2002);

- **UK case** - has become important after Public Safety Zones (PSZs) were introduced in 1958. The PSZ was defined as an area adjacent to the end of a runway in which development of land had to be restricted if it would likely significantly increase the number of “residing, working or congregating people there” (Ale et al, 2000).
In the 1997 the method for third-party risk assessments around airports and the proposal of the appropriate risk assessment criteria was developed in a NATS. The method was based on distinguishing aircraft regarding their manufacturer, country of origin, type (large, small, jets, turbo-props), and category (passenger, cargo), modelling of the aircraft crash location and the crash consequences both based on a limited sample, and simplified approach, to draw the risk contours around a given airport. In addition, cost-benefit analysis was applied to set up criteria for acceptable (tolerable) risk (Ale et al, 2000).

**Purpose**

The third-party methods/models have been mainly used for decision-making and policy purposes related to airport development and operations as follows:

a) Forecasting risk for an individual to be killed by a crashing airplane in the vicinity of given airports. The information has been used for comparing the risk around airports and that around chemical or nuclear plants;

b) Zoning around airports using individual risk contours and societal risk values, i.e. determining areas, which should be considered dangerous for building houses or other vulnerable infrastructure;

c) Indicating changes in risk contours arising from airport development or changes in using existing infrastructure (changes of runways in use, arrival or departure trajectories, etc).

Relative to the classification of risk given in Section 6, it could be mentioned that third-party methods/models are used for assessment of “predicted” and “real risk to an individual”.

**Problems**

The third-party methods/models have been permanently improved and updated. The main problems identified during that process have been as follows (Hale, 2002):

a) Lack of generality, i.e., the specific method/model has been developed for the specific airport;

b) Proactive assessment of the risk could not be carried out due to the risk control measures being already in place;

c) Scarcity of data on real accidents and risk exposure around the airports in the official statistical sources;

d) Difficulties in setting up threshold values for individual and societal risk; if too high it might compromise the airport operations and development; if too low, it might put individuals at an unacceptable jeopardy.
RECOMMENDATIONS AND RELATION TO NEW TECHNOLOGIES

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

Recommendations

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

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

Collision risk methods/models

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

Human factor error methods/models

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

Certainly, development of more general methods/models for assessment of third-party risk could be recommended. They should have flexible structure in order to appropriately handle differences and specificities of traffic, layout and surrounding environment at particular airports. In addition, these methods/models should be able to handle proactive managerial, organizational, technical and/or other changes, and to represent their effects on the overall risk and safety around given airport. As well, they should have some predictive capabilities. Last but not least, there is an increasing need for common frameworks for managing third party risk by developing methodologies and tolerability criteria for comparable risk assessment in order to ensure fair competition between airports (in Europe) (EC, 1999).

Relation to new technologies

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

The causal methods/models could contribute to the proactive development of policies on implementing changes by providing insight into the effects of changes in existing systems on risk and safety (Roelen et al, 2003a). In particular, under conditions when the system changes due to implementation of new technologies, these methods/models could provide feedback about their contribution to lowering risk and consequently increasing the overall system safety.

Collision risk methods/models

Used for reduction of aircraft separation for more than 40 years, the collision risk methods/models have proved their viability. However, further reductions in aircraft separation by the use of new technologies will be needed as an option for increasing airspace capacity. Therefore, existing modified and new methods/models will have to be able to assess collision risk under such circumstances (Machol, 1995). Some models such as TOPAZ are already in place. Use of this method/model is in line with methodology proposed by the ICAO, which points out the necessity for evaluation of risk of new technologies against threshold values and its comparison with the reference system (Vismari and Camargo, 2005). In cases where there is lack of reference systems or large scale changes in existing systems, expert judgment is recommended. In addition, setting up threshold values for risk while implementing new technologies, which are expected to be of lower risk, is also a matter for further elaboration of existing systems and the development of new collision risk methods/models.

Human factor error methods/models

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

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

Prospective research agenda

Many developments in aviation are initiated as a direct result from aircraft accidents. One of them is development of risk and safety methods/models at beginning of 1960’s. As a reaction on accidents, first causal methods/models are developed with aim to find out their main causes in order to prevent further accidents. In the same time, collision risk methods/models appeared with proactive role in redesigning the air traffic system in order to safely accommodate increasing traffic demand. Since 1970’s, aviation community become more concerned in a human roles in accidents, resulting in development of Human factor errors methods/models. Latter on, during 1990’s, airports appear to be a bottleneck of an air traffic system, so the general public become aware of severity of accidents in airports vicinity and their influence on surrounding inhabitants and environment. Increased awareness was resulting in development of Third-party risk methods/models. The overview and review of the mentioned methods/models for assessment of risk and safety in civil aviation have uncovered some commonalities between them, which could be, after being summarized, used for generating prospective research agenda. These are as follows:

- Regarding the *purpose* all models have been developed to support decision-making processes during system planning, development and management, through evaluation of the risk and safety of proposed technological, organizational and managerial changes;

- Regarding *problems* that all methods/models have been confronted with: i) Necessity to have a good, statistically significant data bases on air traffic accidents and their causes (the lack of such data has been compensated by the expert judgment inherently containing unreliability and uncertainty); and ii) Complexity in quantification of risk and safety due to dependability of particular air traffic accidents on many interrelated dynamic and stochastic causes;

- Regarding the *recommendations*, all methods/models should have some predictive capabilities, flexibility, and modularity as well as should be generic;

- Regarding *application to new technologies*, all methods/models should be able to investigate their risk and safety under given circumstances. However there might be some limitations in such application due to the inherent limitations of existing models to appropriately handle the risk and safety of new technologies (Vismari and Camargo, 2005).

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

This Part has provided a review of the methods/models for assessment of risk and safety in civil aviation.

The main findings have provided insight into the efforts already carried out in developing these methods/models, their inherent complexity and lack of sufficient flexibility, lack of the available data for calibration and testing, and lack of the sufficient predicting capabilities enabling easier application to the assessment of risk and safety of new technological, procedural and operational concepts.

These have aimed at increasing system capacity on the one hand and reducing acceptable risk and safety thresholds on the other. In many cases, the need for developing “specialized” or “dedicated” methods/models for particular parts of the system have been discovered. In addition, difficulties such as the lack of real-life data have been overcome by including expert judgment despite awareness of its uncertainty and biases.

The structured need for balance and compromise between methods/models complexity, time and cost of development, and transparency of results have also been pointed out.

Prospective research has been considered to further improve existing models in line with recommendations, which have generally implied capability of risk and safety assessment during development and after implementation of new technologies, generality on the one hand and dedication on the other, predictive capabilities, flexibility and easier understood and handled modular system structures.
### APPENDIX 2: List of Modelling Assumptions for TCAS SDCPN Model

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS1</td>
<td>Own aircraft is TCAS II Version 7-equipped and this equipment is functional</td>
</tr>
<tr>
<td>AS2</td>
<td>All intruder aircraft are TCAS II Version 7-equipped</td>
</tr>
<tr>
<td>AS3</td>
<td>Own aircraft detects and resolves conflict before intruder aircraft</td>
</tr>
<tr>
<td>AS4</td>
<td>Own aircraft starts coordination, i.e. it transmits the selected sense to the intruder aircraft</td>
</tr>
<tr>
<td>AS5</td>
<td>Only encounter between a pair of aircraft is considered (own and intruder aircraft)</td>
</tr>
<tr>
<td>AS6</td>
<td>Pilots are obligated to follow instructions provided by TCAS RA</td>
</tr>
<tr>
<td>AS7</td>
<td>During an RA, ATCo does not issue control instructions that are contrary to the given RA, and is only subsequently informed of conflict</td>
</tr>
<tr>
<td>AS8</td>
<td>Failure of LPNs: TCAS Processor in working mode, CDTI in working mode, Aural annunciation in working mode, Air/ground Communication link, Own aircraft Mode S Link and Intruder aircraft Mode S Link could jeopardize safety of the TCAS operation</td>
</tr>
<tr>
<td>AS9</td>
<td>RA modification is not modelled</td>
</tr>
<tr>
<td>AS10</td>
<td>Aircraft dynamics is not explicitly modelled</td>
</tr>
<tr>
<td>AS11</td>
<td>Turning manoeuvre is not modelled</td>
</tr>
<tr>
<td>AS12</td>
<td>Encounter time interval is ((0, \text{time of CPA} + 25 \text{ sec}))</td>
</tr>
<tr>
<td>AS13</td>
<td>Change of altitude is linear without errors</td>
</tr>
<tr>
<td>AS14</td>
<td>Both own/ intruder aircraft are flying with the constant ground speeds (GS)</td>
</tr>
<tr>
<td>AS15</td>
<td>Vertical speeds (VS) of own/ intruder aircraft is changed only in case when RA is issued</td>
</tr>
<tr>
<td>AS16</td>
<td>Both own/ intruder aircraft are flying with a constant magnetic headings (MH)</td>
</tr>
<tr>
<td>AS17</td>
<td>Own aircraft state is presented by position in space, horizontal/vertical speed, and heading</td>
</tr>
<tr>
<td>AS18</td>
<td>Own aircraft state changes in time</td>
</tr>
<tr>
<td>AS19</td>
<td>Movement of the Own aircraft is assumed to be perfect, i.e. without errors in position, speed and heading estimation</td>
</tr>
<tr>
<td>AS20</td>
<td>Acceleration of Own aircraft in the horizontal plane is 0 during encounter</td>
</tr>
<tr>
<td>AS21</td>
<td>Magnetic heading of Own aircraft is constant during encounter</td>
</tr>
<tr>
<td>AS22</td>
<td>Two possible states of Mode S Link exist – work and fail</td>
</tr>
<tr>
<td>AS23</td>
<td>Switches from one state to another in Mode S Link occur at exponentially distributed times</td>
</tr>
<tr>
<td>AS24</td>
<td>Mode S Link serves to transmit Own aircraft state information to Intruder aircraft, to receive the Intruder aircraft state information and to transmit the selected sense in case of RA, i.e. for coordination purposes</td>
</tr>
<tr>
<td>AS25</td>
<td>TCAS Processor performs all the necessary calculations in order to determine whether intruder aircraft presents the threat to own aircraft</td>
</tr>
<tr>
<td>AS26</td>
<td>Two possible states of TCAS Processor Working Mode exist – functional and failure</td>
</tr>
<tr>
<td>AS27</td>
<td>Switches from one state to another in TCAS Processor Working Mode occur at exponentially distributed times</td>
</tr>
<tr>
<td>AS28</td>
<td>CDTI could be in one of the two states – passive working mode, i.e. mode presenting traffic alerts (TA) and/or surrounding traffic; and active working mode, i.e. presenting resolution advisories (RA)</td>
</tr>
<tr>
<td>AS29</td>
<td>Two possible states of CDTI Working Mode exist – work and fail</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>AS30</td>
<td>Switches from one state to another in CDTI Working Mode occur at exponentially distributed times</td>
</tr>
<tr>
<td>AS31</td>
<td>Aural Annunciation could be in one of the two states – passive working mode, i.e. mode presenting traffic alerts (TA) and/or surrounding traffic; and active working mode, i.e. presenting resolution advisories (RA), both as spoken information to the crew</td>
</tr>
<tr>
<td>AS32</td>
<td>Two possible states of Aural Annunciation Working Mode exist – work and fail</td>
</tr>
<tr>
<td>AS33</td>
<td>Switches from one state to another in Aural Annunciation Working Mode occur at exponentially distributed times</td>
</tr>
<tr>
<td>AS34</td>
<td>Intruder aircraft state is presented by position in space, horizontal/vertical speed, and heading</td>
</tr>
<tr>
<td>AS35</td>
<td>Intruder aircraft state changes in time</td>
</tr>
<tr>
<td>AS36</td>
<td>Movement of the Intruder aircraft is assumed to be perfect, i.e. without errors in position, speed and heading estimation</td>
</tr>
<tr>
<td>AS37</td>
<td>Acceleration of Intruder aircraft in the horizontal plane is 0 during encounter</td>
</tr>
<tr>
<td>AS38</td>
<td>Magnetic heading of Intruder aircraft is constant during encounter</td>
</tr>
<tr>
<td>AS39</td>
<td>Two possible states of Mode S Link exist – work and fail</td>
</tr>
<tr>
<td>AS40</td>
<td>Switches from one state to another in Mode S Link occur at exponentially distributed times</td>
</tr>
<tr>
<td>AS41</td>
<td>Mode S Link serves to transmit Own aircraft state information to intruder aircraft, to receive the Intruder aircraft state information and to transmit the selected sense in case of RA, i.e. for coordination purposes</td>
</tr>
<tr>
<td>AS42</td>
<td>Intruder aircraft follows coordination, i.e. it receives the selected sense from the own aircraft</td>
</tr>
<tr>
<td>AS43</td>
<td>Apart from the cognitive and other human factor issues, from the aspect of TCAS, the Crew (PF) can be in following states: nominal, active and passive</td>
</tr>
<tr>
<td>AS44</td>
<td>Air/Ground Communication Link could be in one of the following states – work (when no failures of adjacent systems occur) or fail (indicating that one or more failures of adjacent systems occur)</td>
</tr>
<tr>
<td>AS45</td>
<td>Apart from the cognitive and other human factor issues, from the aspect of TCAS, ATCo can be in following states: ATCo is responsible and Crew is responsible</td>
</tr>
<tr>
<td>AS46</td>
<td>When RA is issued a crew becomes responsible for aircraft separation and informs the ATCo about that, since then the ATCo switches to Crew is responsible state</td>
</tr>
<tr>
<td>AS47</td>
<td>After conflict resolution the crew returns to nominal state and informs the ATCo about this, since then the ATCo becomes again responsible for aircraft separation</td>
</tr>
</tbody>
</table>
## APPENDIX 3: List of Hazards with explanation how they are covered

<table>
<thead>
<tr>
<th>Hazard Id</th>
<th>Hazard description</th>
<th>Covered</th>
<th>Description how it is covered</th>
<th>Reason if it is not covered or if it is covered partially</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Appearance of rapid aircraft manoeuvre.</td>
<td>no</td>
<td>-</td>
<td>Existence of the following assumptions: AS14, AS15 and AS16.</td>
</tr>
<tr>
<td>2.</td>
<td>Pilot follows ATCo instruction instead of RA.</td>
<td>yes</td>
<td>If Crew doesn’t have information that an RA have been issued, as in the following situations: a) If $LPN \text{ CDTI}_i$ and $LPN \text{ Aural Annunciation}_i$ are in “passive” mode; b) if $LPN \text{ Crew}_i$ is in “passive” or “nominal” mode.</td>
<td>-</td>
</tr>
<tr>
<td>3.</td>
<td>Modification of aircraft flight path by ATCo.</td>
<td>yes (partially)</td>
<td>If ATCo is in “ATCo is responsible” mode, as in the following situations: a) if $LPN \text{ Crew}_i$ is in “passive” or “nominal” mode; b) LPN Air/Ground communication link is in “fail” mode.</td>
<td>Partially because when ATCo resides in “ATCo responsible” mode it is obligated to safely separate traffic. In TCAS SDCPN model the ATCo’s instructions are not explicitly modelled.</td>
</tr>
<tr>
<td>4.</td>
<td>Pilot report is incomplete and/or not understandable to ATCo;</td>
<td>no</td>
<td>-</td>
<td>Whenever Crew is in “active” mode and Air/Ground communication link is in “work” mode then ATCo is in “Crew is responsible” mode. This is related to the following assumptions: AS43, AS45, AS46 and AS47</td>
</tr>
<tr>
<td>5.</td>
<td>Pilot didn’t report to ATCo at all; ATCo is not aware of RA existence.</td>
<td>yes</td>
<td>If the Crew doesn’t have information that an RA has been issued, or Crew have information but Air/Ground communication link is failed. As in the</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|   |   | **following situations:**  
|   |   | a) If \(LPN\) \(CDTI\), and \(LPN\) \(Aural Annunciation\), are in “passive” mode;  
|   |   | b) if \(LPN\) \(Crew\), is in “passive” or “nominal” mode;  
|   |   | c) \(LPN\) \(Air/Ground communication link\) is in “fail” mode.  
|   |   | Partially because when \(ATCo\) resides in “\(ATCo\) is responsible” mode it is obligated to safely separate traffic. In the TCAS SDCPN model ATCos instructions are not explicitly modelled  
| 6. | ATCo is provides the vertical manoeuvre to aircraft. | yes (partially) | If \(ATCo\) is in “\(ATCo\) is responsible” mode. It is in situation when \(LPN\) \(Crew\), is in “passive” or “nominal” mode.  
|   |   | When \(ATCo\) is residing in “\(ATCo\) is responsible” mode it is obligated to safely separate traffic. In the TCAS SDCPN model ATCos instructions are not explicitly modelled  
| 7. | ATCo does not provide traffic information. | no | -  
| 8. | No altitude information about threat aircraft. | yes | If Own aircraft doesn’t receive state information about intruder aircraft. It is in following situations:  
|   |   | a) \(LPN\) \(Intruder aircraft Mode S Link\) is in “fail” mode; and/or  
|   |   | b) \(LPN\) \(Own aircraft Mode S Link\) is in “fail” mode.  
| 9. | Transponder is not functioning. | yes | If Own aircraft is not able to send state information to intruder aircraft. It is in following situation: \(LPN\) \(Own aircraft Mode S Link\) is in -  

**APPENDIX 3**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>“fail” mode.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Issuing of inappropriate RA.</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>11.</td>
<td>Threat aircraft altitude is not reported accurately;</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>12.</td>
<td>Threat aircraft makes an abrupt manoeuvre.</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>13.</td>
<td>Mode S failed, so the issuing of coordinated RA between aircraft is not possible.</td>
<td>yes</td>
<td>It is in following situations: a) LPN Own aircraft Mode S Link(i) is in “fail” mode; and/or b) LPN Intruder aircraft Mode S Link(j) is in “fail” mode.</td>
</tr>
<tr>
<td>14.</td>
<td>Display/aural annunciation fails and does not issue a TA or an RA.</td>
<td>yes</td>
<td>It is in following situations: a) LPN TCAS Processor(i) is in “fail” mode; and/or b) LPN CDTI Working Mode(i) is in “fail” mode; and/or c) LPN Aural Annunciation Working Mode(i) is in “fail” mode.</td>
</tr>
<tr>
<td>15.</td>
<td>Display fails and does not issue speed or angle for flying.</td>
<td>yes</td>
<td>It is in following situations: a) LPN TCAS Processor(i) is in “fail” mode; and/or b) LPN CDTI Working Mode(i) is in “fail” mode.</td>
</tr>
<tr>
<td>16.</td>
<td>Possibility that reverse sense is not selected due to failure.</td>
<td>yes</td>
<td>It is in following situations: a) LPN Own aircraft Mode S Link(i) is in “fail” mode; and/or b) LPN Intruder aircraft Mode S Link(j) is in “fail” mode; and/or c) LPN TCAS Processor(i) is in “fail” mode.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td>Notes</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
<td>---</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Pilots sometimes deviate significantly further from their original clearance than was required or desired while complying with an RA;</td>
<td>no</td>
<td>It is assumed that Crew will act according to an RA provided while they are in “active” mode. This is related to assumption AS43 and AS46.</td>
</tr>
<tr>
<td>18</td>
<td>Pilots are often slow in reporting the initial deviations to the controller and this resulted in a situation where the controller issued a clearance that was in the opposite sense than that directed by the RA;</td>
<td>Yes (partially)</td>
<td>It is in following situation: (LPN \text{ Crew}, i) is in “active” mode – where transition to this mode could be with some delay.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Partially because this is related to the situation when Crew residing in “active” mode and is informing ATCo about existence of an RA, only.</td>
</tr>
<tr>
<td>19</td>
<td>Some pilots request information, or refuse a clearance, based on information shown on the traffic display;</td>
<td>Yes (partially)</td>
<td>It is in following situation: (LPN \text{ Crew}, i) is in “passive” mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>It is assumed that Crew will sometimes (with small probability) refuse an RA provided while they are in “passive” mode. This is related to assumption AS43. Partially because existence of the “visual acquisition” mode is not assumed.</td>
</tr>
<tr>
<td>20</td>
<td>Aircraft have also been observed making horizontal manoeuvres based solely on the information shown on the traffic display, without visual acquisition by the aircrew;</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>21</td>
<td>Event reports also indicate that some pilots did react to RAs, when they</td>
<td>Yes (partially)</td>
<td>It is in following situation: (LPN \text{ Crew}, i) is in “passive” mode.  It is assumed that the Crew will sometimes (with small probability) refuse an</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>have traffic information from the controller, but have not visually acquired the intruder.</td>
<td>RA provided while they are in “passive” mode. This is related to assumption AS43. Partially because existence of the “visual acquisition” mode is not assumed.</td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td>Aircraft levelling off at 1000ft above or below conflicting traffic that is level, may result in RAs being issued to the level aircraft; no</td>
<td>-</td>
<td>This is related to assumption AS13.</td>
</tr>
<tr>
<td>23.</td>
<td>Altitude crossing clearances issued by a controller based on maintaining visual separation may result in RAs being issued, particularly if one of the aircraft is level. no</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
APPENDIX 4: Local Petri Net’s specification

A1. TCAS Own Aircraft as Agent

TCAS Own Aircraft is an agent which contains a following LPNs (Figure A1):
- LPN Own aircraft state
- LPN Own aircraft Mode S Link
- LPN TCAS Processor
- LPN TCAS Processor Working Mode
- LPN CDTI
- LPN CDTI Working Mode
- LPN Aural Annunciation
- LPN Aural Annunciation Working Mode

Figure A1. LPN contained in Agent TCAS Own Aircraft and their mutual relationship
A1.1 LPN Own aircraft state

Assumptions

AS17: Own aircraft state is presented by position in space, horizontal/vertical speed, and heading;
AS18: Own aircraft state changes in time;
AS19: Movement of the Own aircraft is assumed to be perfect, i.e. without errors in position, speed and heading estimation;
AS20: Acceleration of Own aircraft in the horizontal plane is 0 during encounter;
AS21: Magnetic heading of Own aircraft is constant during encounter.

a) Places P, transitions T, arcs A, node function N

The Own aircraft state is represented by the LPN in Figure A2. The place represents the following mode:
- *State* – position and speed of the aircraft in 3D;

LPN also contains a delay transition (D) which is connected to the place by an ordinary bi-directional arc.

![Figure A2. LPN Own aircraft state](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Own AC state</td>
<td>(x_i^t)</td>
<td>(\mathbb{R}^3)</td>
<td>Own aircraft position coordinates (x_{x_i}; x_{y_i}; x_{z_i})</td>
</tr>
<tr>
<td></td>
<td>(v_i^t)</td>
<td>(\mathbb{R}^3)</td>
<td>Own aircraft velocity components (v_{x_i}; v_{y_i}; v_{z_i})</td>
</tr>
<tr>
<td></td>
<td>(\psi_i^t)</td>
<td>(\mathbb{R})</td>
<td>Velocity vector orientation in the vertical plane (angle of attack)</td>
</tr>
<tr>
<td></td>
<td>(\theta_i^t)</td>
<td>(\mathbb{R})</td>
<td>Velocity vector orientation in the horizontal plane (magnetic heading)</td>
</tr>
<tr>
<td></td>
<td>(c_i^t)</td>
<td>(\mathbb{R})</td>
<td>Own aircraft selected RA sense</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Own AC state</td>
</tr>
</tbody>
</table>

d) Token colour function V and W

none
### Appendix 4

#### e) Guards G

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Λ <em>P</em>[Crew₁{Own aircraft crew}] → State</td>
<td>(dt)</td>
</tr>
</tbody>
</table>

#### f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Λ <em>P</em>[Crew₁{Own aircraft crew}] → State</td>
<td>(dt)</td>
</tr>
</tbody>
</table>

#### g) Firing function F

- **State Λ \(P\) [Crew₁{Own aircraft crew}] → State**
  
  \[
  \begin{align*}
  x'_{i,t} &= x'_{i}\{\text{State}\} + v'_{i}\{\text{State}\} \cdot dt \\
  y'_{i,t} &= y'_{i}\{\text{State}\} + d\psi'_{i,t} \\
  \theta'_{i,t} &= \theta'_{i}\{\text{State}\} + d\theta'_{i,t} \\
  v'_{x,i,t} &= v'_{i}\{\text{State}\} \cdot \cos \psi'_{i}\{\text{State}\} \cdot \cos \theta'_{i}\{\text{State}\} + a'_{x} \cdot dt \\
  v'_{y,i,t} &= v'_{i}\{\text{State}\} \cdot \cos \psi'_{i}\{\text{State}\} \cdot \sin \theta'_{i}\{\text{State}\} + a'_{y} \cdot dt \\
  \end{align*}
  
  if *Nominal*[Crew₁{Own aircraft crew}] or *Passive*[Crew₁{Own aircraft crew}] is current then
  
  \[
  v'_{z,i,t} = v'_{i}\{\text{State}\} \cdot \sin \psi'_{i}\{\text{State}\} \\
  c'_{i,t} = 0 \\
  \]
  
  else if *Active*[Crew₁{Own aircraft crew}] is current then
  
  \[
  v'_{z,i,t} = v'_{i}\{\text{State}\} \cdot \sin \psi'_{i}\{\text{State}\} + v'_{z,i}\{\text{Active}[\text{Crew}_1{\text{Own aircraft crew}}]\} \\
  c'_{i,t} = c'_{i}\{\text{Active}[\text{Crew}_1{\text{Own aircraft crew}}]\} \\
  \]

#### h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>1</td>
<td>(x'<em>{i,0}, y'</em>{i,0}, \psi'<em>{i,0}, \theta'</em>{i,0} - \text{user defined input values (scenario specific)})</td>
</tr>
</tbody>
</table>

#### i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>(dt)</td>
<td>Time increment</td>
<td>default 1 sec (DoT, 2000)</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>(a'_{x})</td>
<td>Acceleration in the horizontal plane (x axis)</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(a'_{y})</td>
<td>Acceleration in the horizontal plane (y axis)</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(d\theta)</td>
<td>Change of magnetic heading</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(d\psi)</td>
<td>Change of attack angle</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

#### j) Incoming arcs and IPNs within the same agent

none

#### k) Additional firing functions for outgoing arcs within the same agent

none
1) Interaction with other agents or LPNs

This LPN has an incoming arc from the following LPN (Figure A3):
- LPN Crew\(_i\) – through enabling arc (interconnection mapping type II (Everdij et al., 2006));

This LPN has outgoing arcs to the following LPNs (Figure A3):
- LPN Own aircraft Mode S Link\(_i\) – through enabling arcs;
- LPN TCAS Processor\(_i\) – through enabling arcs (interconnection mapping type III (Everdij et al., 2006)).

Figure A3. Interaction of LPN Own aircraft state\(_i\) with LPNs: Own aircraft Mode S Link\(_i\), TCAS Processor\(_i\), and Crew\(_i\).
A1.2 LPN Own aircraft Mode S Link

Assumptions
AS22: Two possible states of Mode S Link exist – work and fail;
AS23: Switches from one state to another in Mode S Link occur at exponentially distributed times;
AS24: Mode S Link serves to transmit Own aircraft state information to Intruder aircraft, to receive the Intruder aircraft state information and to transmit the selected sense in case of RA, i.e. for coordination purposes.

a) Places P, transitions T, arcs A, node function N
The Own aircraft Mode S Link is represented by the LPN presented in Figure A4. The places represent the following modes:
- Work – Mode S Link is working properly;
- Fail – failure of the Mode S Link.
LPN also contains two delay transitions (D) and one guard transition (G). All transitions are connected to the places by ordinary arcs (uni- or bi-directional).

![Figure A4. LPN Own aircraft Mode S Link](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Own Mode S state</td>
<td>$\dot{x}^i_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Own aircraft position coordinates $x^i_{x,t}; x^i_{y,t}; x^i_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$\dot{v}^i_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Own aircraft velocity components $v^i_{x,t}; v^i_{y,t}; v^i_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$\dot{x}^k_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft position coordinates $x^k_{x,t}; x^k_{y,t}; x^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$\dot{v}^k_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft velocity components $v^k_{x,t}; v^k_{y,t}; v^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$c^i_t$</td>
<td>$\mathbb{R}$</td>
<td>Own aircraft selected RA sense</td>
</tr>
<tr>
<td>$T$</td>
<td>$\mathbb{R}$</td>
<td>Time delay Work $\rightarrow$ Fail and Fail $\rightarrow$ Work</td>
<td></td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>All places</td>
<td>Own Mode S state</td>
</tr>
</tbody>
</table>

d) Token colour function V and W

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour token function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>$dT/dt = -1$</td>
</tr>
</tbody>
</table>
### APPENDIX 4

e) Guards $G$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Condition for transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Work \rightarrow Fail$</td>
<td>$T = 0$</td>
</tr>
</tbody>
</table>

f) Delays $D$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Fail \land P[intruder\ aircraft\ Mode\ S\ Link_k{intruder\ aircraft}]\land State[own\ aircraft\ state_i] \rightarrow Work$</td>
<td>$\tau \leftarrow f_E(\cdot; \mu_{modeS failure})$</td>
</tr>
<tr>
<td>$Work \land State[own\ aircraft\ state_i] \land P[intruder\ aircraft\ Mode\ S\ Link_k{intruder\ aircraft}] \rightarrow Work$</td>
<td>$dt$</td>
</tr>
</tbody>
</table>

g) Firing function $F$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
</table>
| $Work \land State[own\ aircraft\ state_i] \land P[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}] \rightarrow Work$ | $x_i' = x_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | $v_i' = v_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | if $Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]$ is current then  
|                                                 | $x_i' = x_i' \{Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]\}$  
|                                                 | $v_i' = v_i' \{Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]\}$  
|                                                 | else if $Fail[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]$ is current then  
|                                                 | $x_i' = 0$  
|                                                 | $v_i' = 0$  
|                                                 | end if  
|                                                 | $c_i' = c_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | $T = T \{Work\}$                          |
| $Work \rightarrow Fail$                        | $x_i' = 0$  
|                                                 | $v_i' = 0$  
|                                                 | $x_k' = 0$  
|                                                 | $v_k' = 0$  
|                                                 | $c_i' = 0$  
|                                                 | $T = 0$                                      |
| $Fail \land State[own\ aircraft\ state_i] \land P[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}] \rightarrow Work$ | $x_i' = x_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | $v_i' = v_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | if $Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]$ is current then  
|                                                 | $x_i' = x_i' \{Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]\}$  
|                                                 | $v_i' = v_i' \{Work[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]\}$  
|                                                 | else if $Fail[intruder\ aircraft\ Mode\ S\ Link_k\{intruder\ aircraft\}]$ is current then  
|                                                 | $x_i' = 0$  
|                                                 | $v_i' = 0$  
|                                                 | end if  
|                                                 | $c_i' = c_i' \{State[own\ aircraft\ state_i]\}$  
|                                                 | $T = T$                                      |
h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>1</td>
<td>$x'_t = x'_t { State[Own aircraft state,] }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$v'_t = v'_t { State[Own aircraft state,] }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x^k_t = x^k_t { Work[Intruder aircraft Mode S Link_k{ Intruder aircraft }] }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$v^k_t = v^k_t { Work[Intruder aircraft Mode S Link_k{ Intruder aircraft }] }$</td>
</tr>
<tr>
<td>Fail</td>
<td>0</td>
<td>$c'_t = 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$T \leftarrow f_E(:; \mu_{modeS}^{failure}, \left(1-p_{modeS}^{failure}\right)/p_{modeS}^{failure})$</td>
</tr>
</tbody>
</table>

i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu_{modeS}^{failure}$</td>
<td>Mean duration of $Fail \rightarrow Work$</td>
<td>$\frac{1}{2}$ hour</td>
<td>(Oliveira et al., 2006)</td>
<td>-</td>
</tr>
<tr>
<td>$p_{modeS}^{failure}$</td>
<td>Probability of $Fail$</td>
<td>$1/20000$</td>
<td>(Oliveira et al., 2006)</td>
<td>-</td>
</tr>
<tr>
<td>$dt$</td>
<td>Update rate of Mode S</td>
<td>$1$ sec</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess

j) Incoming arcs and IPNs within the same agent

none

k) Additional firing functions for outgoing arcs within the same agent

none

l) Interaction with other agents or LPNs

This LPN has incoming arcs from the following LPNs (Figure A5):
- LPN Own aircraft state, – through enabling arcs;
- LPN Intruder aircraft Mode S Link_k – through enabling arcs (interconnection mapping type II (Everdij et al., 2006));

This LPN has outgoing arcs to the following LPNs (Figure A5):
- LPN TCAS Processor_i – through enabling arcs (interconnection mapping type II and III combined (Everdij et al., 2006));
- LPN Intruder aircraft Mode S link_k – through enabling arcs (interconnection mapping type II (Everdij et al., 2006)).
Figure A5. Interaction of LPN Own aircraft Mode S Link with LPNs: Own aircraft state, Intruder aircraft Mode S Link, and TCAS Processor.
A1.3 TCAS Processor

Assumptions

**AS25**: TCAS Processor performs all the necessary calculations in order to determine whether intruder aircraft presents the threat to own aircraft;

- **Places P, transitions T, arcs A, node function N**
  The own aircraft TCAS Processor is represented by the LPN presented in Figure A6. The places represent the following modes:
  - *No conflict* – no intruders in own aircraft vicinity or conflict is resolved;
  - *Conflict detection* – intruders appear, TA is issued;
  - *Conflict resolution* – threat is worsened, RA is issued.

LPN also contains four guard transitions (G) which are connected to places with ordinary arcs and 3 delay transitions (D) connected to places with bi-directional ordinary arcs.

![Figure A6. LPN for TCAS Processor](image)

**b) Colour type S**

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCAS-1</td>
<td>$X_{ik}^{h,t}$</td>
<td>R</td>
<td>distance between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$X_{ik}^{z,t}$</td>
<td>R</td>
<td>distance between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td></td>
<td>$V_{ik}^{h,t}$</td>
<td>R</td>
<td>relative velocity between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$V_{ik}^{z,t}$</td>
<td>R</td>
<td>relative velocity between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td></td>
<td>$\phi_{ik}$</td>
<td>R</td>
<td>bearing of the position difference vector</td>
</tr>
<tr>
<td></td>
<td>$\delta_{ik}$</td>
<td>R</td>
<td>bearing of the velocity difference vector</td>
</tr>
<tr>
<td></td>
<td>$t_{ik}^{h,t}$</td>
<td>R</td>
<td>time to CPA between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$t_{ik}^{z,t}$</td>
<td>R</td>
<td>time to CPA between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td>Colour type</td>
<td>Component</td>
<td>State space</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TCAS-2</td>
<td>$x^i_{h,t}$</td>
<td>R</td>
<td>distance between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$x^i_{z,t}$</td>
<td>R</td>
<td>distance between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td></td>
<td>$v^i_{h,t}$</td>
<td>R</td>
<td>relative velocity between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$v^i_{z,t}$</td>
<td>R</td>
<td>relative velocity between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td></td>
<td>$\phi^i_{h,t}$</td>
<td>R</td>
<td>bearing of the position difference vector</td>
</tr>
<tr>
<td></td>
<td>$\delta^i_{h,t}$</td>
<td>R</td>
<td>bearing of the velocity difference vector</td>
</tr>
<tr>
<td></td>
<td>$\tau^i_{h,t}$</td>
<td>R</td>
<td>time to CPA between aircraft $i$ and $k$ at time $t$ in the horizontal plane.</td>
</tr>
<tr>
<td></td>
<td>$\tau^i_{z,t}$</td>
<td>R</td>
<td>time to CPA between aircraft $i$ and $k$ at time $t$ in the vertical plane.</td>
</tr>
<tr>
<td></td>
<td>$w^i_t$</td>
<td>N</td>
<td>Clear of Conflict indication</td>
</tr>
<tr>
<td></td>
<td>$c^i_t$</td>
<td>N</td>
<td>own aircraft selected RA sense.</td>
</tr>
<tr>
<td></td>
<td>$v^i_{**,t}$</td>
<td>R</td>
<td>own aircraft selected RA strength.</td>
</tr>
</tbody>
</table>

**c) Colour function $C$**

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>No conflict</td>
<td>TCAS-1</td>
</tr>
<tr>
<td>Conflict detection</td>
<td>TCAS-1</td>
</tr>
<tr>
<td>Conflict resolution</td>
<td>TCAS-2</td>
</tr>
</tbody>
</table>

**d) Token colour function $V$ and $W$**

none

d) **Guards $G$**

<table>
<thead>
<tr>
<th>Transition</th>
<th>Condition for transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>No conflict $\Lambda$ P[Own aircraft Mode S Link] $\Lambda$ State[Own aircraft state] $\Lambda$ Work[TCAS Processor working mode] $\rightarrow$ Conflict detection</td>
<td>$\tau^i_{h,t} {\text{No conflict}} &lt; \tau_{TA} \land \tau^i_{z,t} {\text{No conflict}} &lt; \tau_{TA}$ $\lor$ $\tau^i_{h,t} {\text{No conflict}} &lt; \text{DMOD}<em>{TA} \land \tau^i</em>{z,t} {\text{No conflict}} &lt; \text{ALIM}_{TA}$</td>
</tr>
<tr>
<td>Conflict detection $\Lambda$ P[Own aircraft Mode S Link] $\Lambda$ State[Own aircraft state] $\Lambda$ Work[TCAS Processor working mode] $\rightarrow$ No conflict</td>
<td>$\tau^i_{h,t} {\text{Conflict detection}} \geq \tau_{TA} \lor \tau^i_{z,t} {\text{Conflict detection}} \geq \tau_{TA}$ $\lor$ $\tau^i_{h,t} {\text{Conflict detection}} \geq \text{DMOD}<em>{TA} \lor \tau^i</em>{z,t} {\text{Conflict detection}} \geq \text{ALIM}_{TA}$</td>
</tr>
<tr>
<td>Conflict detection $\Lambda$ P[Own aircraft Mode S Link] $\Lambda$ State[Own aircraft state] $\Lambda$</td>
<td>$\tau^i_{h,t} {\text{Conflict detection}} &lt; \tau_{RA} \land \tau^i_{z,t} {\text{Conflict detection}} &lt; \tau_{RA}$ $\lor$ $\tau^i_{h,t} {\text{Conflict detection}} &lt; \text{DMOD}<em>{RA} \lor \tau^i</em>{z,t} {\text{Conflict detection}} &lt; \text{ALIM}_{RA}$</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>f) Delays D</strong></td>
<td></td>
</tr>
<tr>
<td>No Conflict</td>
<td>( dt )</td>
</tr>
<tr>
<td>( \land P[\text{Own aircraft Mode S Link}_i] \land \text{State}[\text{Own aircraft state}_i] \land \text{Work}[\text{TCAS Processor working mode}_i] )</td>
<td></td>
</tr>
<tr>
<td>( \rightarrow \text{No Conflict} )</td>
<td></td>
</tr>
<tr>
<td>Conflict Detection</td>
<td>( dt )</td>
</tr>
<tr>
<td>( \land P[\text{Own aircraft Mode S Link}_i] \land \text{State}[\text{Own aircraft state}_i] \land \text{Work}[\text{TCAS Processor working mode}_i] )</td>
<td></td>
</tr>
<tr>
<td>( \rightarrow \text{Conflict Detection} )</td>
<td></td>
</tr>
<tr>
<td>Conflict Resolution</td>
<td>( dt )</td>
</tr>
<tr>
<td>( \land P[\text{Own aircraft Mode S Link}_i] \land \text{State}[\text{Own aircraft state}_i] \land \text{Work}[\text{TCAS Processor working mode}_i] )</td>
<td></td>
</tr>
<tr>
<td>( \rightarrow \text{Conflict Resolution} )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>g) Firing function F</strong></td>
<td></td>
</tr>
<tr>
<td>No conflict</td>
<td>if ( \text{Work}[\text{Own aircraft Mode S link}_i] ) is current then</td>
</tr>
<tr>
<td>( \land P[\text{Own aircraft Mode S Link}_i] \land \text{State}[\text{Own aircraft state}_i] \land \text{Work}[\text{TCAS Processor working mode}_i] )</td>
<td></td>
</tr>
<tr>
<td>( \rightarrow \text{No conflict} )</td>
<td></td>
</tr>
</tbody>
</table>

- \( x^{ik}_{h,t} = (x^{i}_{x,t}\{\text{State}[\text{Own aircraft state}_i]\}, x^{i}_{y,t}\{\text{State}[\text{Own aircraft state}_i]\})^{T} - (x^{i}_{x,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}, x^{i}_{y,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\})^{T} \)

- \( v^{ik}_{h,t} = (v^{i}_{x,t}\{\text{State}[\text{Own aircraft state}_i]\}, v^{i}_{y,t}\{\text{State}[\text{Own aircraft state}_i]\})^{T} - (v^{i}_{x,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}, v^{i}_{y,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\})^{T} \)

\( \delta^{i} = \arctan\left(\frac{v^{i}_{y,t}\{\text{State}[\text{Own aircraft state}_i]\} - v^{i}_{y,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}}{v^{i}_{x,t}\{\text{State}[\text{Own aircraft state}_i]\} - v^{i}_{x,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}}\right) \)

\( \phi^{i} = \arctan\left(\frac{x^{i}_{y,t}\{\text{State}[\text{Own aircraft state}_i]\} - x^{i}_{y,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}}{x^{i}_{x,t}\{\text{State}[\text{Own aircraft state}_i]\} - x^{i}_{x,t}\{\text{Work}[\text{Own aircraft Mode S link}_i]\}}\right) \)
And, using the above values for $x_{ik}^{h,t}$, $v_{ik}^{h,t}$, $\delta_{ik}^{t}$, and $\phi_{ik}^{t}$,

$$
\tau_{ik}^{h,t} = \begin{cases} 
\frac{x_{ik}^{h,t}}{v_{ik}^{h,t}} & \text{if } v_{ik}^{h,t} \neq 0 \\
-\infty & \text{otherwise}
\end{cases},
$$

Altitude test:

$$
x_{ik}^{z,t} = (x_{ik}^{x,t} - x_{ik}^{y,t} - \frac{\pi}{2}) - \left(\frac{\delta_{ik}^{t} \cos(\phi_{ik}^{t})}{v_{ik}^{h,t}}\right)
$$

else if Fail[Own aircraft Mode S link] is current then

Range test:

$$
x_{ik}^{h,t} = (x_{ik}^{x,t} - x_{ik}^{y,t} - \frac{\pi}{2}) - \left(\frac{\delta_{ik}^{t} \cos(\phi_{ik}^{t})}{v_{ik}^{h,t}}\right)
$$

Altitude test:

$$
x_{ik}^{z,t} = (x_{ik}^{x,t} - x_{ik}^{y,t} - \frac{\pi}{2}) - \left(\frac{\delta_{ik}^{t} \cos(\phi_{ik}^{t})}{v_{ik}^{h,t}}\right)
$$

end if.

No conflict

if Work[Own aircraft Mode S link] is current then

Range test:

$$
x_{ik}^{h,t} = (x_{ik}^{x,t} - x_{ik}^{y,t} - \frac{\pi}{2}) - \left(\frac{\delta_{ik}^{t} \cos(\phi_{ik}^{t})}{v_{ik}^{h,t}}\right)
$$

$$
\delta_{ik}^{t} = \arctan\left(\frac{v_{ik}^{h,t}}{x_{ik}^{z,t}}\right)
$$

$$
\phi_{ik}^{t} = \arctan\left(\frac{x_{ik}^{h,t}}{v_{ik}^{z,t}}\right)
$$

And, using the above values for $x_{ik}^{h,t}$, $v_{ik}^{h,t}$, $\delta_{ik}^{t}$, and $\phi_{ik}^{t}$,
Appendix 4

\[ x_{ik} = \begin{cases} \frac{-\Delta x_{ih}}{v_{ik} \cos(\delta_{it} - \phi_{it})}, & \text{if } (\delta_{it} - \phi_{it} \neq \pi/2) \land (\delta_{it} - \phi_{it} \neq -\pi/2) \land (v_{ik} \neq 0) \\ -\infty, & \text{otherwise} \end{cases} \]

Altitude test:
\[ x_{ik}^{\text{h,t}} = x_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \} - x_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \} \]
\[ v_{ik}^{\text{h,t}} = v_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \} - v_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \} \]

And, using the above values for \( x_{ik}^{\text{h,t}} \) and \( v_{ik}^{\text{h,t}} \)
\[ x_{ik}^{\text{s,t}} = \begin{cases} -\Delta x_{ih}, & \text{if } v_{ik}^{\text{h,t}} \neq 0 \\ v_{ik}^{\text{h,t}}, & \text{otherwise} \end{cases} \]

else if \( \text{Fail[Own aircraft Mode S link,]} \) is current then

Range test:
\[ x_{ik}^{\text{h,t}} = x_{ik}^{\text{h,t}} \{\text{No Conflict}\} \]
\[ v_{ik}^{\text{h,t}} = v_{ik}^{\text{h,t}} \{\text{No Conflict}\} \]
\[ \delta_{ik}^{\text{t}} = \delta_{ik}^{\text{t}} \{\text{No conflict}\} \]
\[ \phi_{ik}^{\text{t}} = \phi_{ik}^{\text{t}} \{\text{No conflict}\} \]
\[ t_{ik}^{\text{h,t}} = t_{ik}^{\text{h,t}} \{\text{No Conflict}\} \]

Altitude test:
\[ x_{ik}^{\text{s,t}} = x_{ik}^{\text{s,t}} \{\text{No Conflict}\} \]
\[ v_{ik}^{\text{s,t}} = v_{ik}^{\text{s,t}} \{\text{No Conflict}\} \]
\[ t_{ik}^{\text{s,t}} = t_{ik}^{\text{s,t}} \{\text{No Conflict}\} \]

end.

\( \text{Conflict Detection} \land P[\text{Own aircraft Mode S Link,]} \land \text{State[Own aircraft state,]} \land \text{Work[TCAS Processor working mode,]} \rightarrow \text{Conflict Detection} \)

if \( \text{Work[Own aircraft Mode S link,]} \) is current then

Range test:
\[ x_{ik}^{\text{h,t}} = (x_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \}, x_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \})^T - (x_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \}, x_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \})^T \]
\[ v_{ik}^{\text{h,t}} = (v_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \}, v_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \})^T - (v_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \}, v_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \})^T \]
\[ \delta_{ik}^{\text{t}} = \arctan(v_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \} / v_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \}) \]
\[ \phi_{ik}^{\text{t}} = \arctan(x_{ik}^{\text{h,t}} \{\text{State[Own aircraft state,]} \} / x_{ik}^{\text{h,t}} \{\text{Work[Own aircraft Mode S link,]} \}) \]

And, using the above values for \( x_{ik}^{\text{h,t}}, v_{ik}^{\text{h,t}}, \delta_{ik}^{\text{t}}, \) and \( \phi_{ik}^{\text{t}} \).
APPENDIX 4

\[ \tau_{ik}^{z,t} = \begin{cases} \frac{-x_{ik}^{z,t}}{v_{ik}^{z,t}} \cdot \cos(\delta_{ik}^{z,t} - \phi_{ik}^{z,t}), & \text{if } (\delta_{ik}^{z,t} - \phi_{ik}^{z,t} \neq \pi/2) \land (\delta_{ik}^{z,t} - \phi_{ik}^{z,t} \neq -\pi/2) \land (|v_{ik}^{z,t}| \neq 0) \\ -\infty, & \text{otherwise} \end{cases} \]

Altitude test:
\[ x_{ik}^{z,t} = x_{ik}^{z,t}\{\text{State[Own aircraft state,]}\} - x_{ik}^{z,t}\{\text{Work[Own aircraft Mode S link,]}\} \]
\[ v_{ik}^{z,t} = v_{ik}^{z,t}\{\text{State[Own aircraft state,]}\} - v_{ik}^{z,t}\{\text{Work[Own aircraft Mode S link,]}\} \]

And, using the above values for \( x_{ik}^{z,t} \) and \( v_{ik}^{z,t} \)
\[ \tau_{ik}^{z,t} = \begin{cases} \frac{-x_{ik}^{z,t}}{v_{ik}^{z,t}}, & \text{if } v_{ik}^{z,t} \neq 0 \\ -\infty, & \text{otherwise} \end{cases} \]

else if \( \text{Fail[Own aircraft Mode S link,]} \) is current then

Range test:
\[ x_{ik}^{h,t} = x_{ik}^{h,t}\{\text{Conflict Detection}\} \]
\[ v_{ik}^{h,t} = v_{ik}^{h,t}\{\text{Conflict Detection}\} \]
\[ \delta_{ik}^{h,t} = \delta_{ik}^{h,t}\{\text{Conflict Detection}\} \]
\[ \phi_{ik}^{h,t} = \phi_{ik}^{h,t}\{\text{Conflict Detection}\} \]
\[ \tau_{ik}^{h,t} = \tau_{ik}^{h,t}\{\text{Conflict Detection}\} \]

Altitude test:
\[ x_{ik}^{z,t} = x_{ik}^{z,t}\{\text{Conflict Detection}\} \]
\[ v_{ik}^{z,t} = v_{ik}^{z,t}\{\text{Conflict Detection}\} \]
\[ \tau_{ik}^{z,t} = \tau_{ik}^{z,t}\{\text{Conflict Detection}\} \]

end if.

\[ \text{Conflict detection } \Lambda P[\text{Own aircraft Mode S Link,}] \Lambda \text{ State[Own aircraft state,]} \Lambda \text{ Work[TCAS Processor working mode,]} \rightarrow \text{No conflict} \]

if \( \text{Work[Own aircraft Mode S link,]} \) is current then

Range test:
\[ x_{ik}^{h,t} = (x_{ik}^{h,t}\{\text{State[Own aircraft state,]}\}, x_{ik}^{h,t}\{\text{State[Own aircraft state,]}\})^T - (x_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}, x_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\})^T \]
\[ v_{ik}^{h,t} = (v_{ik}^{h,t}\{\text{State[Own aircraft state,]}\}, v_{ik}^{h,t}\{\text{State[Own aircraft state,]}\})^T - (v_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}, v_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\})^T \]
\[ \delta_{ik}^{h,t} = \arctan(v_{ik}^{h,t}\{\text{State[Own aircraft state,]}\} - v_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}, v_{ik}^{h,t}\{\text{State[Own aircraft state,]}\} - v_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}) \]
\[ \phi_{ik}^{h,t} = \arctan(x_{ik}^{h,t}\{\text{State[Own aircraft state,]}\} - x_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}, x_{ik}^{h,t}\{\text{State[Own aircraft state,]}\} - x_{ik}^{h,t}\{\text{Work[Own aircraft Mode S link,]}\}) \]

And, using the above values for \( x_{ik}^{h,t}, v_{ik}^{h,t}, \delta_{ik}^{h,t}, \) and \( \phi_{ik}^{h,t} \)
\[
x_{ik}^{z} = \begin{cases} 
- \frac{x_{ik}^z}{v_{ik}} \cos(\delta_{ik} - \varphi_{ik}) , & \text{if } (\delta_{ik} - \varphi_{ik} \neq \pi/2) \land (\delta_{ik} - \varphi_{ik} \neq -\pi/2) \land (|v_{ik}| \neq 0) \\
- \infty , & \text{otherwise} 
\end{cases}
\]

Altitude test:
\[
x_{ik}^{x} = x_{ik}^{x} \{ \text{State[Own aircraft state]} \} - x_{ik}^{x} \{ \text{Work[Own aircraft Mode S link]} \}
v_{ik}^{x} = v_{ik}^{x} \{ \text{State[Own aircraft state]} \} - v_{ik}^{x} \{ \text{Work[Own aircraft Mode S link]} \}
\]

And, using the above values for \( x_{ik}^{x} \) and \( v_{ik}^{x} \):
\[
x_{ik}^{z} = \frac{-x_{ik}^{z}}{v_{ik}^{z}} , \quad \text{if } v_{ik}^{z} \neq 0
\]
\[
x_{ik}^{z} = -\infty , \quad \text{otherwise}
\]

else if Fail[Own aircraft Mode S link] is current then

Range test:
\[
x_{ik}^{h} = x_{ik}^{h} \{ \text{Conflict detection} \}
v_{ik}^{h} = v_{ik}^{h} \{ \text{Conflict detection} \}
\]
\[
\delta_{ik}^{h} = \delta_{ik}^{h} \{ \text{Conflict detection} \}
\]
\[
\varphi_{ik}^{h} = \varphi_{ik}^{h} \{ \text{Conflict detection} \}
\]
\[
\tau_{ik}^{h} = \tau_{ik}^{h} \{ \text{Conflict detection} \}
\]

Altitude test:
\[
x_{ik}^{h} = x_{ik}^{h} \{ \text{Conflict detection} \}
v_{ik}^{h} = v_{ik}^{h} \{ \text{Conflict detection} \}
\]
\[
\tau_{ik}^{h} = \tau_{ik}^{h} \{ \text{Conflict detection} \}
\]

end.

Conflicts detection \&
\[ P[\text{Own aircraft Mode S Link}] \land \]
\[ \text{State[Own aircraft state]} \land \]
\[ \text{Work[TCAS Processor working mode]} \]
\[ \rightarrow \text{Conflict resolution} \]

if Work[Own aircraft Mode S link] is current then

Range test:
\[
x_{ik}^{h} = (x_{ik}^{h} \{ \text{State[Own aircraft state]} \}, v_{ik}^{h} \{ \text{State[Own aircraft state]} \})^T - (x_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}, v_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \})^T
\]
\[
v_{ik}^{h} = (v_{ik}^{h} \{ \text{State[Own aircraft state]} \}, v_{ik}^{h} \{ \text{State[Own aircraft state]} \})^T - (v_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}, v_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \})^T
\]
\[
\delta_{ik}^{h} = \arctan(\frac{v_{ik}^{h} \{ \text{State[Own aircraft state]} \} - v_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}}{v_{ik}^{h} \{ \text{State[Own aircraft state]} \} - v_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}})
\]
\[
\varphi_{ik}^{h} = \arctan(\frac{x_{ik}^{h} \{ \text{State[Own aircraft state]} \} - x_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}}{x_{ik}^{h} \{ \text{State[Own aircraft state]} \} - x_{ik}^{h} \{ \text{Work[Own aircraft Mode S link]} \}})
\]

And, using the above values for \( x_{ik}^{h} \), \( v_{ik}^{h} \), \( \delta_{ik}^{h} \) and \( \varphi_{ik}^{h} \)
\[
\tau_{ik,\ell,t}^x = \begin{cases} 
\frac{-\frac{s_{ik}^x}{s_{ik}^z}}{\sqrt{s_{ik}^z} \cos(\delta_{ik} - \phi_{ik})}, & \text{if } (\delta_{ik} - \phi_{ik} \neq \pi/2) \land (\delta_{ik} - \phi_{ik} \neq -\pi/2) \land (|v_{ik}^x| \neq 0) \\
-\infty, & \text{otherwise}
\end{cases}
\]

Altitude test:
\[
x_{ik,\ell,t}^x = x_{ik,\ell,t}^x - x_{ik,\ell,t}^v, \quad \text{if } v_{ik,\ell,t}^x \neq 0
\]
\[
v_{ik,\ell,t}^x = v_{ik,\ell,t}^x - v_{ik,\ell,t}^v, \quad \text{otherwise}
\]

And, using the above values for \(x_{ik,\ell,t}^x\) and \(v_{ik,\ell,t}^x\)
\[
\tau_{ik,\ell,t}^v = \begin{cases} 
-\frac{x_{ik,\ell,t}^x}{v_{ik,\ell,t}^x}, & \text{if } v_{ik,\ell,t}^x \neq 0 \\
-\infty, & \text{otherwise}
\end{cases}
\]

Sense selection
\[
c_i^j = \begin{cases} 
(b > a) \lor \\
-1, & \text{if } (b \leq a) \land \left( \exists \varepsilon \in (0, \tau_{RA}^x) \text{ such that } \bar{x}_{ik,\ell,t}^x = 0 \right) \lor \\
(b > a) \land \left( \exists \varepsilon \in (0, \tau_{RA}^x) \text{ such that } \bar{x}_{ik,\ell,t}^x = 0 \right) \land (a > ALIM_{RA}) \\
(b \leq a) \lor \\
1, & \text{if } (b > a) \land \left( \exists \varepsilon \in (0, \tau_{RA}^x) \text{ such that } \bar{x}_{ik,\ell,t}^x = 0 \right) \lor \\
(b \leq a) \land \left( \exists \varepsilon \in (0, \tau_{RA}^x) \text{ such that } \bar{x}_{ik,\ell,t}^x = 0 \right) \land (b > ALIM_{RA})
\end{cases}
\]

where the following auxiliary variables are used:
\[
x_{ik,\ell,t}^x (\text{up}) = x_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} + \\
+ (v_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} + \Delta_{ik,\ell,t}^x) \cdot \tau_{RA}
\]
\[
x_{ik,\ell,t}^x (\text{current}) = x_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} + \\
+ (v_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} + \Delta_{ik,\ell,t}^x) \cdot \tau_{RA}
\]
\[
x_{ik,\ell,t}^x (\text{down}) = x_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} + \\
+ (v_{ik,\ell,t}^x \{ \text{State} [\text{Own aircraft state}_i] \} - \Delta_{ik,\ell,t}^x) \cdot \tau_{RA}
\]
\[
x_{ik,\ell,t}^x (\text{current}) = x_{ik,\ell,t}^x \{ \text{Work} [\text{Own aircraft Mode S link}_k] \} + \\
+ (v_{ik,\ell,t}^x \{ \text{Work} [\text{Own aircraft Mode S link}_k] \} + \Delta_{ik,\ell,t}^x) \cdot \tau_{RA}
\]
\[ a \equiv \left| x_{z, t + \tau_{RA}} \text{ (up)} - x_{z, t + \tau_{RA}} \text{ (current)} \right| \]
\[ b \equiv \left| x_{z, t + \tau_{RA}} \text{ (down)} - x_{z, t + \tau_{RA}} \text{ (current)} \right| \]

\[ x_{z, t + \tau_{RA}} = \left( x_{z, t} \{ \text{State [Own aircraft state]} \} \right) + v_{z, t} \{ \text{State [Own aircraft state]} \} \cdot c \] 
\[ + \left( x_{z, t} \{ \text{Work [Own aircraft Mode S link]} \} \right) + v_{z, t} \{ \text{Work [Own aircraft Mode S link]} \} \cdot c \]
\[ \text{and } 0 < \varnothing - 1 < c \leq 0 + 1 \leq \tau_{RA} \]

**Strength selection**

Using the value for \( c_i \) above

\[ v_{z, t} \{ \text{State [Own aircraft state]} \} + \Delta \] if \( c_i = 1 \)
\[ v_{z, t} \{ \text{State [Own aircraft state]} \} - \Delta \] if \( c_i = -1 \)

where the following auxiliary variable is used:

\[ \Delta = [ALIM + x_{z, t} \{ \text{Work [Own aircraft Mode S link]} \} + v_{z, t} \{ \text{Work [Own aircraft Mode S link]} \} \cdot \tau_{RA} - (x_{z, t} \{ \text{State [Own aircraft state]} \} + v_{z, t} \{ \text{State [Own aircraft state]} \} \cdot \tau_{RA})] / \tau_{RA} \]

**Clear of conflict test**

\[ w_{z, t} = \begin{cases} 1, & \text{if } v_{z, t} \{ \text{State [Own aircraft state]} \} > x_{z, t} \{ \text{State [Own aircraft state]} \} \\ 0, & \text{otherwise} \end{cases} \]

where the following auxiliary variables are used:

using the above values for \( x_{h, t} \)

\[ x_{h, CPA} = \begin{cases} x_{h, t}, & \text{if } t = t_{\text{CPA}} \\ \infty, & \text{otherwise} \end{cases} \]

\[ x_{h, t} = \begin{cases} x_{h, t}, & \text{if } t = t' \\ \infty, & \text{otherwise} \end{cases} \]

where:

- \( t_{\text{CPA}} \) is moment when both aircraft \( i \) and \( k \) are at CPA. Using the above values for \( \tau_{h, t} \) and \( \tau_{z, t} \):

\[ t_{\text{CPA}} = \begin{cases} t, & \text{if } \tau_{h, t} = 0 \lor \tau_{z, t} = 0 \\ \infty, & \text{otherwise} \end{cases} \]

- \( t' \) is the moment when both aircraft \( i \) and \( k \) are safely passing the CPA. Using the above value for \( t_{\text{CPA}} \):

\[ t' = t_{\text{CPA}} + dt. \]

else if \( \text{Fail [Own aircraft Mode S link]} \) is current then

**Range test**:

\[ x_{h, t} = x_{h, t} \{ \text{Conflict detection} \} \]
\[ v_{h, t} = v_{h, t} \{ \text{Conflict detection} \} \]
\[ \delta_{h, t} = \delta_{h, t} \{ \text{Conflict detection} \} \]
\[ \phi^k_{ik} = \phi^k_{ik} \text{ [Conflict detection]} \]
\[ \tau^k_{ik} = \tau^k_{ik} \text{ [Conflict detection]} \]

**Altitude test:**
\[ x^k_{ik} = x^k_{ik} \text{ [Conflict detection]} \]
\[ v^k_{ik} = v^k_{ik} \text{ [Conflict detection]} \]
\[ \tau^k_{ik} = \tau^k_{ik} \text{ [Conflict detection]} \]

**Sense selection:**
\[ c^k_{ik} = 0 \]

**Strength selection:**
\[ v^k_{ik} = 0 \]

**Clear of conflict test**
\[ w^k_{ik} = 0 \end{end} \]

**Conflict Resolution**

\[ \Lambda^k_{P[Own aircraft Mode S Link]} \Lambda^k_{State[Own aircraft state]} \Lambda^k_{Work[TCAS Processor working mode]} \rightarrow \text{Conflict Resolution} \]

if Work[Own aircraft Mode S link] is current then

**Range test:**
\[ x^k_{ik} = (x^k_{ik} \text{ [State[Own aircraft state]]}) - (x^k_{ik} \text{ [Work[Own aircraft Mode S link]]}) \]
\[ v^k_{ik} = (v^k_{ik} \text{ [State[Own aircraft state]]}) - (v^k_{ik} \text{ [Work[Own aircraft Mode S link]]}) \]

\[ \delta^k_{ik} = \arctan \left( \frac{v^k_{ik} \text{ [State[Own aircraft state]]} - v^k_{ik} \text{ [Work[Own aircraft Mode S link]]}}{x^k_{ik} \text{ [State[Own aircraft state]]} - x^k_{ik} \text{ [Work[Own aircraft Mode S link]]}} \right) \]

\[ \phi^k_{ik} = \arctan \left( \frac{x^k_{ik} \text{ [State[Own aircraft state]]} - x^k_{ik} \text{ [Work[Own aircraft Mode S link]]}}{v^k_{ik} \text{ [State[Own aircraft state]]} - v^k_{ik} \text{ [Work[Own aircraft Mode S link]]}} \right) \]

And, using the above values for \( x^k_{ik}, v^k_{ik}, \delta^k_{ik} \) and \( \phi^k_{ik} \)

\[ \tau^k_{ik} = \begin{cases} - \left| x^k_{ik} \right|, & \text{if } \left( \delta^k_{ik} \neq 0 \right) \land \left( \phi^k_{ik} \neq \pi/2 \right) \land \left( \phi^k_{ik} \neq -\pi/2 \right) \land \left( v^k_{ik} \neq 0 \right) \\ -\infty, & \text{otherwise} \end{cases} \]

**Altitude test:**
\[ x^k_{ik} = x^k_{ik} \text{ [State[Own aircraft state]]} - x^k_{ik} \text{ [Work[Own aircraft Mode S Link]]} \]
\[ v^k_{ik} = v^k_{ik} \text{ [State[Own aircraft state]]} - v^k_{ik} \text{ [Work[Own aircraft Mode S Link]]} \]

And, using the above values for \( x^k_{ik} \) and \( v^k_{ik} \)

\[ \tau^k_{ik} = \begin{cases} - \left| x^k_{ik} \right| / v^k_{ik}, & \text{if } v^k_{ik} \neq 0 \\ -\infty, & \text{otherwise} \end{cases} \]
Appendix 4

Sense selection

\[ c_i' = \begin{cases} 
(b > a) \lor \\ -1, \quad \text{if } (b \leq a) \land \left( \exists \varepsilon \in (0, \tau_{RA}) \text{ such that } x_{z,t+\varepsilon} = 0 \right) \lor \\
(b > a) \land \left( \exists \varepsilon \in (0, \tau_{RA}) \text{ such that } x_{z,t+\varepsilon} = 0 \right) \land (a > ALIM_{RA}) \\
(b \leq a) \lor \\ 1, \quad \text{if } (b > a) \land \left( \exists \varepsilon \in (0, \tau_{RA}) \text{ such that } x_{z,t+\varepsilon} = 0 \right) \lor \\
(b \leq a) \land \left( \exists \varepsilon \in (0, \tau_{RA}) \text{ such that } x_{z,t+\varepsilon} = 0 \right) \land (b > ALIM_{RA}) 
\end{cases} \]

where the following auxiliary variables are used:

\[ \left\{ x_{z,t+\tau_{RA}} (up) = x_{z,t} \{ State[Own aircraft state, i] \} + \\ + (v_{z,t} \{ State[Own aircraft state, i] \} + \Delta_{z,t}) \cdot \tau_{RA} \right\} \]

\[ \left\{ x_{z,t+\tau_{RA}} (current) = x_{z,t} \{ State[Own aircraft state, i] \} + \\ + v_{z,t} \{ State[Own aircraft state, i] \} \cdot \tau_{RA} \right\} \]

\[ \left\{ x_{z,t+\tau_{RA}} (down) = x_{z,t} \{ State[Own aircraft state, i] \} + \\ + (v_{z,t} \{ State[Own aircraft state, i] \} - \Delta_{z,t}) \cdot \tau_{RA} \right\} \]

\[ \left\{ x_{z,t+\tau_{RA}} (current) = x_{z,t} \{ Work[Own aircraft Mode S link, i] \} + \\ + v_{z,t} \{ Work[Own aircraft Mode S link, i] \} \cdot \tau_{RA} \right\} \]

\[ a = \left| x_{z,t+\tau_{RA}} (up) - x_{z,t+\tau_{RA}} (current) \right| \]

\[ b = \left| x_{z,t+\tau_{RA}} (down) - x_{z,t+\tau_{RA}} (current) \right| \]

\[ \left\{ x_{z,t} \{ State[Own aircraft state, i] \} + v_{z,t} \{ State[Own aircraft state, i] \} \cdot \varepsilon \right\} - \\
\left\{ x_{z,t} \{ Work[Own aircraft Mode S link, i] \} + v_{z,t} \{ Work[Own aircraft Mode S link, i] \} \cdot \varepsilon \right\} \]

and \( 0 < \varepsilon - 1 < \varepsilon < \varepsilon + 1 \leq \tau_{RA} \)

Strength selection

Using the value for \( c_i' \) above

\[ v_{z,t}^{s,v} = \begin{cases} 
 v_{z,t} \{ State[Own aircraft state, i] \} + \Delta_{z,t}^{s,v}, \quad \text{if } c_i' = 1 \\
 v_{z,t} \{ State[Own aircraft state, i] \} - \Delta_{z,t}^{s,v}, \quad \text{if } c_i' = -1 
\end{cases} \]
where the following auxiliary variable is used:

\[\Delta^{*}_{i,z,t} = [ALIM_{RA} + (x^{k}_{z,t}(Work[Own aircraft Mode S link,]) +
+ v^{k}_{z,t}(Work[Own aircraft Mode S link,]) \cdot \tau_{RA}) -
\]
\[-(x^{i}_{z,t}(State[Own aircraft state,]) + v^{i}_{z,t}(State[Own aircraft state,]) \cdot \tau_{RA})] / \tau_{RA}\]

Clear of conflict test

\[w'_{i} = \begin{cases} 1, & \text{if } |x^{i}_{h,i}| > |x^{i}_{h,CPA}| \\ 0, & \text{otherwise} \end{cases}\]

where the following auxiliary variables are used:
using the above values for \(x^{i}_{h,i}\)

\[x^{i}_{h,CPA} = \begin{cases} x^{i}_{h,i}, & \text{if } t = t_{CPA} \\ \infty, & \text{otherwise} \end{cases}\]

\[x^{i}_{h,t} = \begin{cases} x^{i}_{h,i}, & \text{if } t = t' \\ \infty, & \text{otherwise} \end{cases}\]

where:

- \(t_{CPA}\) is the moment when both aircraft \(i\) and \(k\) are at CPA. Using the above values for \(\tau^{i}_{h,i}\) and \(\tau^{i}_{z,t}\):

\[t_{CPA} = \begin{cases} t, & \text{if } \tau^{i}_{h,i} = 0 \lor \tau^{i}_{z,t} = 0 \\ \infty, & \text{otherwise} \end{cases}\]

- \(t'\) is the moment when both aircraft \(i\) and \(k\) safely pass the CPA. Using the above value for \(t_{CPA}\):

\[t' = t_{CPA} + dt.\]

else if \(Fail[Own aircraft Mode S link,]\) is current then

Range test:

\(x^{i}_{h,t} = x^{i}_{h,t}\{\text{Conflict resolution}\}\)

\(v^{i}_{h,t} = v^{i}_{h,t}\{\text{Conflict resolution}\}\)

\(\delta^{i}_{t} = \delta^{i}_{t}\{\text{Conflict resolution}\}\)

\(\phi^{i}_{t} = \phi^{i}_{t}\{\text{Conflict resolution}\}\)

\(\tau^{i}_{h,t} = \tau^{i}_{h,t}\{\text{Conflict resolution}\}\)

Altitude test:

\(x^{i}_{z,t} = x^{i}_{z,t}\{\text{Conflict resolution}\}\)

\(v^{i}_{z,t} = v^{i}_{z,t}\{\text{Conflict resolution}\}\)

\(\tau^{i}_{z,t} = \tau^{i}_{z,t}\{\text{Conflict resolution}\}\)

Sense selection:

\(c'_{i} = 0\)

Strength selection:

\(v'_{z,t} = 0\)

Clear of conflict test

\[w'_{i} = 0\]

end.
if Work[Own aircraft Mode S link] is current then

\[
\text{Range test:} \quad x_{hk}^i = (x_{x,t}^i \{\text{State}[\text{Own aircraft state}]\}, x_{y,t}^i \{\text{State}[\text{Own aircraft state}]\})^T - (x_{x,t}^k \{\text{Work}[\text{Own aircraft Mode S link}]\}, x_{y,t}^k \{\text{Work}[\text{Own aircraft Mode S link}]\})^T
\]

\[
v_{hk}^i = (v_{x,t}^i \{\text{State}[\text{Own aircraft state}]\}, v_{y,t}^i \{\text{State}[\text{Own aircraft state}]\})^T - (v_{x,t}^k \{\text{Work}[\text{Own aircraft Mode S link}]\}, v_{y,t}^k \{\text{Work}[\text{Own aircraft Mode S link}]\})^T
\]

\[
\delta_i^k = \arctan(v_{y,t}^i / \text{State}[\text{Own aircraft state}] - v_{y,t}^k / \text{Work}[\text{Own aircraft Mode S link}])
\]

\[
\phi_i^k = \arctan(x_{x,t}^i / \text{State}[\text{Own aircraft state}] - x_{x,t}^k / \text{Work}[\text{Own aircraft Mode S link}])
\]

And, using the above values for \(x_{hk}^i, v_{hk}^i, \delta_i^k\) and \(\phi_i^k\),

\[
x_{hk}^i = \begin{cases} 
\frac{-x_{hk}^i}{\cos(\delta_i^k - \phi_i^k)} & \text{if } \delta_i^k - \phi_i^k \neq \pi/2 \land (\delta_i^k - \phi_i^k \neq -\pi/2) \land (v_{hk}^i \neq 0) \\
-\infty & \text{otherwise}
\end{cases}
\]

Altitude test:

\[
x_{zk}^i = x_{zk}^i \{\text{State}[\text{Own aircraft state}]\} - x_{zk}^k \{\text{Work}[\text{Own aircraft Mode S link}]\}
\]

\[
v_{zk}^i = v_{zk}^i \{\text{State}[\text{Own aircraft state}]\} - v_{zk}^k \{\text{Work}[\text{Own aircraft Mode S link}]\}
\]

And, using the above values for \(x_{zk}^i\) and \(v_{zk}^i\),

\[
x_{zk}^i = \begin{cases} 
\frac{-x_{zk}^i}{v_{zk}^i} & \text{if } v_{zk}^i \neq 0 \\
-\infty & \text{otherwise}
\end{cases}
\]

else if Fail[Own aircraft Mode S link] is current then

\[
\text{Range test:} \quad x_{hk}^k = x_{hk}^k \{\text{Conflict resolution}\}
\]

\[
v_{hk}^k = v_{hk}^k \{\text{Conflict resolution}\}
\]

\[
\delta_i^k = \delta_i^k \{\text{Conflict resolution}\}
\]

\[
\phi_i^k = \phi_i^k \{\text{Conflict resolution}\}
\]

\[
\tau_{hk}^i = \tau_{hk}^i \{\text{Conflict resolution}\}
\]

Altitude test:

\[
x_{zk}^k = x_{zk}^k \{\text{Conflict resolution}\}
\]

\[
v_{zk}^k = v_{zk}^k \{\text{Conflict resolution}\}
\]

\[
\tau_{zk}^i = \tau_{zk}^i \{\text{Conflict resolution}\}
\]

end if.
### h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>No conflict</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

\[
x^{i,k}_{h,t} = (x^{i,k}_{z,t} \{State[Own aircraft state,\]}, x^{i,k}_{y,t} \{State[Own aircraft state,\}])^T - \left( x^{i,k}_{z,t} \{Work[Own aircraft Mode S link,\]}, x^{i,k}_{y,t} \{Work[Own aircraft Mode S link,\} \right)^T
\]

\[
v^{i,k}_{h,t} = (v^{i,k}_{x,t} \{State[Own aircraft state,\]}, v^{i,k}_{y,t} \{State[Own aircraft state,\}])^T - \left( v^{i,k}_{x,t} \{Work[Own aircraft Mode S link,\]}, v^{i,k}_{y,t} \{Work[Own aircraft Mode S link,\} \right)^T
\]

\[
\delta^{i,k}_t = \arctan \left( \frac{v^{i,k}_{x,t} \{State[Own aircraft state,\]} - v^{i,k}_{x,t} \{Work[Own aircraft Mode S link,\]} \right) \frac{x^{i,k}_{z,t} \{State[Own aircraft state,\]} - x^{i,k}_{z,t} \{Work[Own aircraft Mode S link,\]} \right)
\]

\[
\phi^{i,k}_t = \arctan \left( \frac{x^{i,k}_{x,t} \{State[Own aircraft state,\]} - x^{i,k}_{x,t} \{Work[Own aircraft Mode S link,\]} \right) \frac{v^{i,k}_{z,t} \{State[Own aircraft state,\]} - v^{i,k}_{z,t} \{Work[Own aircraft Mode S link,\]} \right)
\]

and using the above values for \(x^{i,k}_{h,t}, v^{i,k}_{h,t}, \delta^{i,k}_t, \) and \(\phi^{i,k}_t\)

\[
\tau^{i,k}_{h,t} = \begin{cases} 
\frac{-x^{i,k}_{z,t}}{\cos(\delta^{i,k}_t - \phi^{i,k}_t)} & \text{if } (\delta^{i,k}_t - \phi^{i,k}_t \neq \pi/2) \land (\delta^{i,k}_t - \phi^{i,k}_t \neq -\pi/2) \land (v^{i,k}_{x,t} \neq 0) \\
-\infty & \text{otherwise}
\end{cases}
\]

\[
x^{i,k}_{z,t} = x^{i,k}_{z,t} \{State[Own aircraft state,\]} - x^{i,k}_{z,t} \{Work[Own aircraft Mode S link,\}]
\]

\[
v^{i,k}_{z,t} = v^{i,k}_{z,t} \{State[Own aircraft state,\]} - v^{i,k}_{z,t} \{Work[Own aircraft Mode S link,\}]
\]

and, using the above values for \(x^{i,k}_{z,t}\) and \(v^{i,k}_{z,t}\)

\[
\tau^{i,k}_{z,t} = \begin{cases} 
\frac{-x^{i,k}_{z,t}}{v^{i,k}_{z,t}} & \text{if } v^{i,k}_{z,t} \neq 0 \\
-\infty & \text{otherwise}
\end{cases}
\]

<table>
<thead>
<tr>
<th>Conflict detection</th>
<th>0</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflict resolution</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>
i) **Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta z_i$</td>
<td>Incremental change of vertical velocity $v_{zi}$ chosen for trial during sense selection.</td>
<td>1500 feet/min</td>
<td>(RTCA, 1997; Kuchar and Drumm, 2007)</td>
<td>-</td>
</tr>
<tr>
<td>$dt$</td>
<td>Time increment</td>
<td>default 1 sec</td>
<td>(DoT, 2000)</td>
<td>-</td>
</tr>
<tr>
<td>$\tau_{TA}, \tau_{RA}$</td>
<td>Time to closest point of approach (CPA) - threshold values for TA and RA issuance</td>
<td>See Table 1</td>
<td>(DoT, 2000)</td>
<td>-</td>
</tr>
<tr>
<td>$DMOD_{TA}, DMOD_{RA}$</td>
<td>Distance Modification values for TA and RA issuance in case of slow closure encounters when $\tau$ threshold values are not appropriate</td>
<td>See Table 1</td>
<td>(DoT, 2000)</td>
<td>-</td>
</tr>
<tr>
<td>$ALIM_{TA}, ALIM_{RA}$</td>
<td>Altitude Limit values for TA and RA issuance in case of slow closure encounters when $\tau$ threshold values are not appropriate</td>
<td>See Table 1</td>
<td>(DoT, 2000)</td>
<td>-</td>
</tr>
</tbody>
</table>

j) **Incoming arcs and IPNs within the same agent**

none

k) **Additional firing functions for outgoing arcs within the same agent**

none

l) **Interaction with other LPNs**

This LPN has incoming arcs from the following LPNs (Figure A7):
- LPN Own aircraft state, $i$ – through enabling arcs (interconnection mapping type III (Everdij et al., 2006));
- LPN Own aircraft Mode S link, $i$ – through enabling arcs (interconnection mapping type II and III combined (Everdij et al., 2006));
- LPN TCAS Processor working mode, $i$ – through enabling arcs (interconnection mapping type III (Everdij et al., 2006));

Also, this LPN has outgoing arcs to the following LPNs (Figure A7):
- LPN Aural Annunciation, $i$ – through enabling and inhibitor arcs;
- LPN CDTI, $i$ – through enabling and inhibitor arcs.
Figure A7. Interaction of LPN TCAS Processor with LPNs: Own aircraft state, Own aircraft Mode S link, TCAS Processor working mode, CDTI, and Aural Annunciation.
A1.4 LPN TCAS Processor Working Mode

Assumptions

AS26: Two possible states of TCAS Processor Working Mode exist – work and failure;
AS27: Switches from one state to another in TCAS Processor Working Mode occur at exponentially distributed times.

a) Places P, transitions T, arcs A, node function N
The TCAS Processor Working Mode of aircraft is represented by the LPN presented in Figure A8. The places represent the following modes:
- Work – TCAS processor is working properly;
- Fail – TCAS processor is not working, i.e. some failure happened.
LPN also contains two delay transitions (D) which are connected to places with ordinary arcs.

![Figure A8. LPN for TCAS Processor Working Mode](image)

b) Colour type S
none

c) Colour function C
none

d) Token colour function V and W
none

e) Guards G
none

f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work → Fail</td>
<td>( \tau \leftarrow f_E(\cdot; \mu_{\text{proc failure}}(1-p_{\text{proc failure}})/p_{\text{proc failure}}) )</td>
</tr>
<tr>
<td>Fail → Work</td>
<td>( \tau \leftarrow f_E(\cdot; \mu_{\text{proc failure}}) )</td>
</tr>
</tbody>
</table>

g) Firing function F
One token without colour to each output place for all transitions.

h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>( 1-p_{\text{proc failure}} )</td>
<td>-</td>
</tr>
<tr>
<td>Fail</td>
<td>( p_{\text{proc failure}} )</td>
<td>-</td>
</tr>
</tbody>
</table>
i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu_{proc_\text{failure}}$</td>
<td>Mean duration of $\text{Fail} \rightarrow \text{Work}$</td>
<td>60 sec</td>
<td>*</td>
<td>-</td>
</tr>
<tr>
<td>$p_{proc_\text{failure}}$</td>
<td>Probability of $\text{Fail}$</td>
<td>$1/10^5$</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess according to values for similar LPNs in (Oliveira et al., 2006) and importance of TCAS system

j) Incoming arcs and IPNs within the same agent
none

k) Additional firing functions for outgoing arcs within the same agent
none

l) Interaction with other LPNs

This LPN has outgoing arcs to the following LPN (Figure A9):
- LPN TCAS Processor, – through enabling arcs (interconnection mapping type III (Everdij et al., 2006)).

This LPN has not incoming arcs from other LPNs (Figure A9):

![Figure A9. Interaction of LPN TCAS Processor working mode, with LPN TCAS Processor](image_url)
A1.5 LPN CDTI

Assumptions

AS28: CDTI could be in one of the two states – passive working mode, i.e. mode presenting traffic alerts (TA) and/or surrounding traffic; and active working mode, i.e. presenting resolution advisories (RA).

a) Places P, transitions T, arcs A, node function N

The CDTI of aircraft is represented by the LPN presented in Figure A10. The places represent the following modes:

- Passive – CDTI is presenting TA and/or surrounding traffic;
- Active – CDTI is presenting also an RA’s;

LPN also contains two immediate transitions (I) which are connected to places with ordinary arcs.

![Figure A10. LPN for CDTI](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDTI state</td>
<td>$c'_i$</td>
<td>R</td>
<td>own aircraft selected RA sense</td>
</tr>
<tr>
<td></td>
<td>$v^{j,s}_{i,t}$</td>
<td>R</td>
<td>own aircraft selected RA strength.</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>All places</td>
<td>CDTI state</td>
</tr>
</tbody>
</table>

d) Token colour function V and W

none

e) Guards G

none

f) Delays D

none
APPENDIX 4

g) Firing function $F$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive &amp; Conflict resolution[TCAS Processor i] &amp; Work[CDTI working mode] → Active</td>
<td>$c_i^f = c_i$[Conflict resolution[TCAS Processor i]] $v_i^z = v_i^z$[Conflict resolution[TCAS Processor i]]</td>
</tr>
<tr>
<td>Active (No conflict or Conflict detection) [TCAS Processor i] &amp; Work[CDTI working mode] → Passive</td>
<td>$c_i^f = 0$ $v_i^z = 0$</td>
</tr>
</tbody>
</table>

h) Initial marking $I$

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>1</td>
<td>$c_i^f = 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$v_i^z = 0$</td>
</tr>
<tr>
<td>Active</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

i) Parameters

none

j) Incoming arcs and IPNs within the same agent

none

k) Additional firing functions for outgoing arcs within the same agent

none

l) Interaction with other agents or LPNs

Also, this LPN has incoming arcs from the following LPNs (Figure A11):
- LPN TCAS Processor i – through enabling and inhibitor arcs;
- LPN CDTI working mode i – through enabling arcs (interconnection mapping type III (Everdij et al, 2006));

Also, this LPN has outgoing arcs to the following LPN (Figure A11):
- LPN Crew i – through enabling arcs.
Figure A11. Interaction of LPN CDTI with LPNs: TCAS Processor, CDTI working mode, and Crew.
A1.6 CDTI Working Mode

Assumptions
AS29: Two possible states of CDTI Working Mode exist – work and fail;
AS30: Switches from one state to another in CDTI Working Mode occur at exponentially distributed times.

a) Places P, transitions T, arcs A, node function N
The CDTI Working Mode of aircraft is presented in Figure A12. The places represent the following modes:
- Work – CDTI is working properly;
- Fail – CDTI is not working, i.e. some failure happened.
LPN also contains two delay transitions (D) which are connected to places with ordinary arcs.

![Figure A12. LPN for CDTI Working Mode](image)

b) Colour type S
none

c) Colour function C
none

d) Token colour function V and W
none

e) Guards G
none

f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work → Fail</td>
<td>( \tau \leftarrow f_E(\cdot; \mu_{CDTI\text{\ fails}}(1-\mu_{CDTI\text{\ failures}})/\mu_{CDTI\text{\ failures}}) )</td>
</tr>
<tr>
<td>Fail → Work</td>
<td>( \tau \leftarrow f_E(\cdot; \mu_{CDTI\text{\ fails}}) )</td>
</tr>
</tbody>
</table>

g) Firing function F
One token without colour to each output place for all transitions.

h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>( 1-\mu_{CDTI\text{\ fails}} )</td>
<td>-</td>
</tr>
<tr>
<td>Fail</td>
<td>( \mu_{CDTI\text{\ fails}} )</td>
<td>-</td>
</tr>
</tbody>
</table>
i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu_{\text{CDTI, failure}}$</td>
<td>Mean duration of $\text{Fail} \rightarrow \text{Work}$</td>
<td>60 sec</td>
<td>*</td>
<td>-</td>
</tr>
<tr>
<td>$p_{\text{CDTI, failure}}$</td>
<td>Probability of $\text{Fail}$</td>
<td>$10^{-5}$</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess according to values for similar LPNs in (Oliveira et al, 2006) and importance of TCAS system.

j) Incoming arcs and IPNs within the same agent
none

k) Additional firing functions for outgoing arcs within the same agent
none

l) Interaction with other LPNs

This LPN has incoming arcs from the following LPNs:
- none.

This LPN has outgoing arcs to the following LPNs (Figure A13):
- LPN CDTI, – through enabling arcs (interconnection mapping type III (Everdij et al., 2006)).

Figure A13. Interaction of LPN CDTI Working Mode, with LPN CDTI,
Aural Annunciation

Assumptions

AS31: Aural Annunciation could be in one of the two states – passive working mode, i.e. mode presenting traffic alerts (TA) and/or surrounding traffic; and active working mode, i.e. presenting resolution advisories (RA), both as spoken information to the crew.

a) Places P, transitions T, arcs A, node function N

The Aural Annunciation of the aircraft is presented in Figure A14. The places represent the following modes:

- **Passive** – Aural Annunciation presents TA and/or surrounding traffic;
- **Active** – Aural Annunciation presents also RAs;

LPN contains two immediate transitions (I) which are connected to places with ordinary arcs.

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA state</td>
<td>$c'_t$</td>
<td>R</td>
<td>own aircraft selected RA sense</td>
</tr>
<tr>
<td></td>
<td>$v^{z,t}$</td>
<td>R</td>
<td>own aircraft selected RA strength.</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
<th>AA state</th>
</tr>
</thead>
</table>

d) Token colour function V and W

none

e) Guards G

none

f) Delays D

none
g) Firing function $F$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
</table>
| Passive $\Lambda$ Conflict resolution[TCAS Processor,$i$] $\Lambda$ Work[Aural annunciation working mode,$i$] $\rightarrow$ Active | $c'_t = c'_t \{\text{Conflict resolution}[\text{TCAS Processor,$i$}]\}$
| | $v'_{s,t} = v'_{s,t} \{\text{Conflict resolution}[\text{TCAS Processor,$i$}]\}$ |
| Active $\Lambda$ (No conflict or Conflict detection) [TCAS Processor,$i$] $\Lambda$ Work[Aural annunciation working mode,$i$] $\rightarrow$ Passive | $c'_t = 0$
| | $v'_{s,t} = 0$ |

h) Initial marking $I$

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
</table>
| Passive | 1 | $c'_{s,t} = 0$
| | | $v'_{s,t} = 0$
| Active | 0 | - |

i) Parameters
none

j) Incoming arcs and IPNs within the same agent
none

k) Additional firing functions for outgoing arcs within the same agent
none

l) Interaction with other agents or LPNs

This LPN has incoming arcs from the following LPNs (Figure A15):
- LPN TCAS Processor,$i$ – through enabling and inhibitor arcs;
- LPN Aural annunciation working mode,$i$ – through enabling arcs (interconnection mapping type III (Everdij et al., 2006));

This LPN has outgoing arcs to the following LPN (Figure A15):
- LPN Crew,$i$ – through enabling arcs.
Figure A15. Interaction of LPN Aural Annunciation, with LPNs: TCAS Processor, Aural Annunciation working mode, and Crew.
A1.8  LPN Aural Annunciation Working Mode

Assumptions

AS32: Two possible states of Aural Annunciation Working Mode exist – work and fail;
AS33: Switches from one state to another in Aural Annunciation Working Mode occur at exponentially distributed times.

a) Places $P$, transitions $T$, arcs $A$, node function $N$
The Aural Annunciation Working Mode of aircraft is represented by the LPN Aural Annunciation Working Mode. The sets $P$, $T$, $A$ and $N$ are presented in Figure A16. The places represent the following modes:
- **Work** – Aural Annunciation is working properly;
- **Fail** – Aural Annunciation is not working, i.e. some failure happened.
LPN also contains two delay transitions (D) which are connected to places with ordinary arcs.

![Figure A16. LPN for Aural Annunciation Working Mode](image-url)

b) Colour type $S$
none

c) Colour function $C$
none

d) Token colour function $V$ and $W$
none

e) Guards $G$
none

f) Delays $D$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work $\rightarrow$ Fail</td>
<td>$\tau \leftarrow f_E(\cdot; \mu_{AA}^{\text{failure}}(1-p_{AA}^{\text{failure}})/p_{AA}^{\text{failure}})$</td>
</tr>
<tr>
<td>Fail $\rightarrow$ Work</td>
<td>$\tau \leftarrow f_E(\cdot; \mu_{AA}^{\text{failure}})$</td>
</tr>
</tbody>
</table>

g) Firing function $F$
One token without colour to each output place for all transitions.
APPENDIX 4

h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>1 - ( p_{AA}^{\text{failure}} )</td>
<td>-</td>
</tr>
<tr>
<td>Fail</td>
<td>( p_{AA}^{\text{failure}} )</td>
<td>-</td>
</tr>
</tbody>
</table>

i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mu_{AA}^{\text{failure}} )</td>
<td>Mean duration of ( \text{Fail} \rightarrow \text{Work} )</td>
<td>60 sec</td>
<td>*</td>
<td>-</td>
</tr>
<tr>
<td>( p_{AA}^{\text{failure}} )</td>
<td>Probability of ( \text{Fail} )</td>
<td>( 10^{-5} )</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess according to values for similar LPNs in (Oliveira et al, 2006) and importance of TCAS system

j) Incoming arcs and IPNs within the same agent

none

k) Additional firing functions for outgoing arcs within the same agent

none

l) Interaction with other LPNs

This LPN has incoming arcs from the following LPNs:

- none.

This LPN has outgoing arcs to the following LPNs (Figure A17):

- LPN Aural annunciation, – through enabling arcs (interconnection mapping type III (Everdij et al., 2006)).

![Figure A17. Interaction of LPN Aural annunciation Working Mode, with LPN Aural annunciation,](image-url)

Figure A17. Interaction of LPN Aural annunciation Working Mode, with LPN Aural annunciation,
A2. TCAS Intruder Aircraft as Agent

TCAS Intruder Aircraft is an agent which contains the following LPNs (Figure A18):

- LPN Intruder aircraft state$_k$;
- LPN Intruder aircraft Mode S Link$_k$.

![Diagram](image-url)

Figure A18. Interaction of LPN Intruder aircraft state$_k$ with LPN Intruder aircraft Mode S Link$_k$. 
A2.1 LPN Intruder aircraft state

Assumptions

AS34: Intruder aircraft state is presented by position in space, horizontal/vertical speed, and heading;
AS35: Intruder aircraft state changes in time;
AS36: Movement of the Intruder aircraft is assumed to be perfect, i.e. without errors in position,
speed and heading estimation;
AS37: Acceleration of Intruder aircraft in the horizontal plane is 0 during encounter;
AS38: Magnetic heading of Intruder aircraft is constant during encounter.

a) Places P, transitions T, arcs A, node function N

The Own aircraft state is represented by the LPN in Figure A19. The place represents the following mode:
- **State** – position and speed of the aircraft in 3D;

LPN contain a one delay transition (D) connected to the place with an ordinary bidirectional arc.

![Figure A19. LPN Intruder aircraft state](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intruder AC state</td>
<td>$x^k_k$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft position coordinates $x^k_{x,t}$, $x^k_{y,t}$, $x^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$v^k_k$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft velocity components $v^k_{x,t}$, $v^k_{y,t}$, $v^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$\psi^k_k$</td>
<td>$\mathbb{R}$</td>
<td>Velocity vector orientation in the vertical plane (angle of attack)</td>
</tr>
<tr>
<td></td>
<td>$\theta^k_k$</td>
<td>$\mathbb{R}$</td>
<td>Velocity vector orientation in the horizontal plane (magnetic heading)</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Intruder AC state</td>
</tr>
</tbody>
</table>

d) Token colour function V and W

none

e) Guards G

none
f) Delays $D$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>State → State</td>
<td>$dt$</td>
</tr>
</tbody>
</table>

$\text{g) Firing function } F$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
<tbody>
<tr>
<td>State → State</td>
<td>$x_i^k = x_i^k{\text{State}} + \dot{x}_i^k{\text{State}} \cdot dt$</td>
</tr>
<tr>
<td></td>
<td>$\theta_i^k = \theta_i^k{\text{State}} + d\theta_i^k$</td>
</tr>
<tr>
<td></td>
<td>$\psi_i^k = \psi_i^k{\text{State}} + d\psi_i^k$</td>
</tr>
<tr>
<td></td>
<td>$v_x^k, t = v_x^k{\text{State}} \cdot \cos \psi_i^k{\text{State}} \cdot \cos \theta_i^k{\text{State}} + a_x^k \cdot dt$</td>
</tr>
<tr>
<td></td>
<td>$v_y^k, t = v_y^k{\text{State}} \cdot \cos \psi_i^k{\text{State}} \cdot \sin \theta_i^k{\text{State}} + a_y^k \cdot dt$</td>
</tr>
<tr>
<td></td>
<td>$v_z^k, t = v_z^k{\text{State}} \cdot \sin \psi_i^k{\text{State}}$</td>
</tr>
</tbody>
</table>

h) Initial marking $I$

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>1</td>
<td>$x_b^i, v_b^i, \theta_i^k, \psi_i^k$ – user defined input values (scenario specific)</td>
</tr>
</tbody>
</table>

i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$dt$</td>
<td>Time increment</td>
<td>default 1 sec$^*$</td>
<td>(DoT, 2000)</td>
<td>-</td>
</tr>
<tr>
<td>$a_x^k$</td>
<td>Acceleration in the horizontal plane (x axis)</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$a_y^k$</td>
<td>Acceleration in the horizontal plane (y axis)</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$d\theta^k$</td>
<td>Change of magnetic heading</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$d\psi^k$</td>
<td>Change of attack angle</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

j) Incoming arcs and IPNs within the same agent

none

k) Additional firing functions for outgoing arcs within the same agent

none

l) Interaction with other LPNs

This LPN has an incoming arc from the following LPN (Figure A20):
  - none.

This LPN has outgoing arcs to the following LPN (Figure A20):
  - LPN Intruder aircraft Mode S Link$_k$ – through enabling arcs.
Figure A20. Interaction of LPN Intruder aircraft state with LPN Intruder aircraft Mode S Link.
A2.2 LPN Intruder aircraft Mode S Link

Assumptions
AS39: Two possible states of Mode S Link exist – work and fail;
AS40: Switches from one state to another in Mode S Link occur at exponentially distributed times;
AS41: Mode S Link serves to transmit Own aircraft state information to intruder aircraft, to receive the Intruder aircraft state information and to transmit the selected sense in case of RA, i.e. for RA coordination purposes;
AS42: Intruder aircraft follows coordination, i.e. it receives the selected sense from the own aircraft.

a) Places P, transitions T, arcs A, node function N

The Intruder aircraft Mode S Link is represented by the LPN presented in Figure A21. The places represent the following modes:
- Work – Mode S Link is working properly;
- Fail – failure of the Mode S Link.
LPN also contains two delay transitions (D) and one guard transition (G). All transitions are connected to places by ordinary arcs (uni- and bi-directional).

![Figure A21. LPN Intruder aircraft Mode S Link](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int Mode S state</td>
<td>$x^i_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Own aircraft position coordinates $x^i_{x,t}; x^i_{y,t}; x^i_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$v^i_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Own aircraft velocity components $v^i_{x,t}; v^i_{y,t}; v^i_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$x^k_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft position coordinates $x^k_{x,t}; x^k_{y,t}; x^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$v^k_t$</td>
<td>$\mathbb{R}^3$</td>
<td>Intruder aircraft velocity components $v^k_{x,t}; v^k_{y,t}; v^k_{z,t}$</td>
</tr>
<tr>
<td></td>
<td>$c^k_t$</td>
<td>$\mathbb{R}$</td>
<td>Intruder aircraft determined RA sense</td>
</tr>
<tr>
<td></td>
<td>$T$</td>
<td>$\mathbb{R}$</td>
<td>Time delay Work $\rightarrow$ Fail and Fail $\rightarrow$ Work</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>All places</td>
<td>Int Mode S state</td>
</tr>
</tbody>
</table>
d) Token colour function V and W

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour token function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>( \frac{dT}{dt} = -1 )</td>
</tr>
</tbody>
</table>

e) Guards G

<table>
<thead>
<tr>
<th>Transition</th>
<th>Condition for transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work ( \rightarrow ) Fail</td>
<td>( T = 0 )</td>
</tr>
</tbody>
</table>

f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail ( \land P[\text{Own aircraft Mode S Link}_i {\text{Own aircraft}}] \land \text{State}[\text{Intruder aircraft State}_k] \rightarrow \text{Work}</td>
<td>( \tau \leftarrow f_E(\cdot; \mu_{\text{modeS failure}}) )</td>
</tr>
<tr>
<td>Work ( \land \text{State}[\text{Intruder aircraft state}_i] \land P[\text{Own aircraft Mode S Link}_k {\text{Own aircraft}}] \rightarrow \text{Work}</td>
<td>( dt )</td>
</tr>
</tbody>
</table>

g) Firing function F

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
</table>
| Work \( \land \) State[Intruder aircraft State] \( \land \) P[Own aircraft Mode S Link\( i \{\text{Own aircraft}\}] \rightarrow \text{Work} | \( x'_i = x_i \{\text{State}[\text{Intruder aircraft State}]\} \)
| | \( v'_i = v_i \{\text{State}[\text{Intruder aircraft State}]\} \) |
| | if \( \text{Work}[\text{Own aircraft Mode S Link}_i \{\text{Own aircraft}\}] \) is current then
| | \( x'_i = x'_i \{\text{Work}[\text{Own aircraft Mode S Link}_i \{\text{Own aircraft}\}]\} \)
| | \( v'_i = v'_i \{\text{Work}[\text{Own aircraft Mode S Link}_i \{\text{Own aircraft}\}]\} \)
| | \( c'_i = -c'_i \{\text{Work}[\text{Own aircraft Mode S Link}_i \{\text{Own aircraft}\}]\} \) |
| | else if \( \text{Fail}[\text{Own aircraft Mode S link}_k \{\text{Own aircraft}\}] \) is current then
| | \( x'_i = 0 \)
| | \( v'_i = 0 \)
| | \( c'_i = 0 \)
| | end if
| | \( T = T[\text{Work}] \)
| Work \( \rightarrow \) Fail | \( x'_i = 0 \)
| | \( v'_i = 0 \)
| | \( x'_k = 0 \)
| | \( v'_k = 0 \)
| | \( c'_k = 0 \)
| | \( T = 0 \) |
| Fail \( \land P[\text{Own aircraft Mode S Link}_i \{\text{Own aircraft}\}] \land \text{State}[\text{Intruder aircraft State}_k] \rightarrow \text{Work} | \( x'_i = x'_i \{\text{State}[\text{Intruder aircraft State}_k]\} \)
| | \( v'_i = v'_i \{\text{State}[\text{Intruder aircraft State}_k]\} \) |
| | if \( \text{Work}[\text{Own aircraft Mode S link}_i \{\text{Own aircraft}\}] \) is current then
| | \( x'_i = x'_i \{\text{Work}[\text{Own aircraft Mode S link}_i \{\text{Own aircraft}\}]\} \)
| | \( v'_i = v'_i \{\text{Work}[\text{Own aircraft Mode S link}_i \{\text{Own aircraft}\}]\} \)
| | \( c'_i = -c'_i \{\text{Work}[\text{Own aircraft Mode S link}_i \{\text{Own aircraft}\}]\} \) |
| | else if \( \text{Fail}[\text{Own aircraft Mode S link}_k \{\text{Own aircraft}\}] \) is current then
| | \( x'_i = 0 \)
| | \( v'_i = 0 \)
| | \( c'_i = 0 \)
| | end if
| | \( T \leftarrow f_E(\cdot; \mu_{\text{modeS failure}}) \frac{(1-p_{\text{modeS failure}})}{p_{\text{modeS failure}}} \) |
### h) Initial marking $I$

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>$1$</td>
<td>$x'_t = x'_t { \text{Work[Own aircraft Mode S Link]} }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$v'_t = v'_t { \text{Work[Own aircraft Mode S Link]} }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$k_t = k_t { \text{State} }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$v'_t = v'_t { \text{State} }$</td>
</tr>
<tr>
<td>Fail</td>
<td>$0$</td>
<td>$T \leftarrow t_E { \frac{\mu_{\text{modeS failure}}}{p_{\text{modeS failure}}} (1-p_{\text{modeS failure}}/p_{\text{modeS failure}}) }$</td>
</tr>
</tbody>
</table>

### i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu_{\text{modeS failure}}$</td>
<td>Mean duration of $\text{Fail} \rightarrow \text{Work}$</td>
<td>$\frac{1}{2}$ hour</td>
<td>(Oliveira et al., 2006)</td>
<td>-</td>
</tr>
<tr>
<td>$p_{\text{modeS failure}}$</td>
<td>Probability of $\text{Fail}$</td>
<td>$1/20000$</td>
<td>(Oliveira et al., 2006)</td>
<td>-</td>
</tr>
<tr>
<td>$dt$</td>
<td>Update rate of Mode S</td>
<td>$1$ sec</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess

### j) Incoming arcs and IPNs within the same agent
none

### k) Additional firing functions for outgoing arcs within the same agent
none

### l) Interaction with other agents or LPNs

This LPN has incoming arcs from the following LPNs (Figure A22):
- LPN Intruder aircraft state$_k$ – through enabling arcs;
- LPN Own aircraft Mode S Link$_l$ – through enabling arcs (interconnection mapping type II (Everdij et al., 2006)).

This LPN has an outgoing arc to the following LPN (Figure A22):
- LPN Own aircraft Mode S Link$_l$ – through enabling arcs (interconnection mapping type II (Everdij et al., 2006)).

![Figure A22. Interaction of LPN Intruder aircraft Mode S Link$_k$ with LPNs: Intruder aircraft state$_k$ and Own aircraft Mode S Link$_l$.](image-url)
A3. TCAS Own Aircraft Crew as Agent

TCAS Own Aircraft crew as agent contains only one LPN: LPN Crew (Pilot Flying – PF, Pilot Not Flying - PNF)

A3.1 LPN Crew

Assumptions

AS43: Apart from the cognitive and other human factor issues, from the aspect of TCAS Crew (PF) can be in following states: nominal, active and passive;

a) Places P, transitions T, arcs A, node function N

The Crew is represented by the LPN presented in Figure A23. The places represent the following modes:

- **Nominal** – the crew is performing usual task during the flight;
- **Active** – an RA is issued, crew is following an RA immediately, i.e. is taking proper action on time or with some delay in case that is too preoccupied to act immediately;
- **Passive** – the crew is rejecting to act according to issued RA;

LPN also contains two immediate transitions (I) and one delay transition (D) which are connected to places with ordinary arcs.

![Figure A23. LPN Crew](image)

b) Colour type S

<table>
<thead>
<tr>
<th>Colour type</th>
<th>Component</th>
<th>State space</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crew state</td>
<td>$c_{i,t}$</td>
<td>R</td>
<td>own aircraft selected RA sense</td>
</tr>
<tr>
<td></td>
<td>$v_{i,t}$</td>
<td>R</td>
<td>own aircraft selected RA strength.</td>
</tr>
</tbody>
</table>

c) Colour function C

<table>
<thead>
<tr>
<th>Place</th>
<th>Colour type</th>
</tr>
</thead>
<tbody>
<tr>
<td>All places</td>
<td>Crew state</td>
</tr>
</tbody>
</table>

d) Token colour function V and W

none

e) Guards G

none

f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal → Active OR Passive</td>
<td>$\tau \leftarrow f_{[0, 10]}$</td>
</tr>
</tbody>
</table>

132
## g) Firing function F

<table>
<thead>
<tr>
<th>Transition</th>
<th>Colour of token after firing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal (\Lambda) (Active[Aural annunciation,{Own aircraft}] OR Active[CDTI,{Own aircraft}]) (\rightarrow) Active OR Passive</td>
<td>One token is produced. With probability (p_{\text{crew active}}), this token is produced in Active. With probability (1-p_{\text{crew active}}), this token is produced in Passive. The colour of this token is determined as follows:</td>
</tr>
<tr>
<td>If Active[Aural annunciation,{Own aircraft}] is current then</td>
<td></td>
</tr>
<tr>
<td>if Active receives the output token then</td>
<td></td>
</tr>
<tr>
<td>(c_i^t = c_i^t{\text{Active[Aural annunciation,{Own aircraft}]}})</td>
<td></td>
</tr>
<tr>
<td>(v_i^{*z,t} = v_i^{*z,t}{\text{Active[Aural annunciation,{Own aircraft}]}})</td>
<td></td>
</tr>
<tr>
<td>else if Passive receives the output token then</td>
<td></td>
</tr>
<tr>
<td>(c_i^t = 0)</td>
<td></td>
</tr>
<tr>
<td>(v_i^{*z,t} = 0)</td>
<td></td>
</tr>
<tr>
<td>end if</td>
<td></td>
</tr>
<tr>
<td>end if</td>
<td></td>
</tr>
<tr>
<td>If Active[CDTI,{Own aircraft}] is current then</td>
<td></td>
</tr>
<tr>
<td>if Active receives the output token then</td>
<td></td>
</tr>
<tr>
<td>(c_i^t = c_i^t{\text{Active[CDTI,{Own aircraft}]}})</td>
<td></td>
</tr>
<tr>
<td>(v_i^{*z,t} = v_i^{*z,t}{\text{Active[CDTI,{Own aircraft}]}})</td>
<td></td>
</tr>
<tr>
<td>else if Passive receives the output token then</td>
<td></td>
</tr>
<tr>
<td>(c_i^t = 0)</td>
<td></td>
</tr>
<tr>
<td>(v_i^{*z,t} = 0)</td>
<td></td>
</tr>
<tr>
<td>end if</td>
<td></td>
</tr>
<tr>
<td>end if</td>
<td></td>
</tr>
</tbody>
</table>

| Active \(\Lambda\) Passive[Aural annunciation,\{Own aircraft\}] \(\Lambda\) Passive[CDTI,\{Own aircraft\}] \(\rightarrow\) Nominal | \(c_i^t = 0\) |
| \(v_i^{*z,t} = 0\) |

| Passive \(\Lambda\) Passive[Aural annunciation,\{Own aircraft\}] \(\Lambda\) Passive[CDTI,\{Own aircraft\}] \(\rightarrow\) Nominal | \(c_i^t = 0\) |
| \(v_i^{*z,t} = 0\) |

## h) Initial marking I

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal</td>
<td>1</td>
<td>(c_i^t = 0)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(v_i^{*z,t} = 0)</td>
</tr>
<tr>
<td>Active</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Passive</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

## i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p_{\text{crew active}})</td>
<td>Probability of Active</td>
<td>0.95</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess
j) Incoming arcs and IPNs within the same agent
none

k) Additional firing functions for outgoing arcs within the same agent
none

l) Interaction with other agents or LPNs

This LPN has incoming arcs from the following LPNs (Figure A24):
- LPN Aural annunciation, – through enabling and merging arcs (interconnection mapping type I (Everdij et al., 2006));
- LPN CDTI, – through enabling and merging arcs (interconnection mapping type I (Everdij et al., 2006)).

This LPN has outgoing arcs to the following LPNs (Figure A24):
- LPN Own aircraft state, - through enabling arcs (interconnection mapping type II (Everdij et al., 2006)).
- LPN ATCo - through enabling and merging arcs (interconnection mapping type I (Everdij et al., 2006)).

Figure A24. Interaction of LPN Crew, with LPNs: CDTI, Aural annunciation, Own aircraft state, and ATCo
A4. TCAS Air/Ground Communication Link as Agent

TCAS Air/Ground Communication Link as agent contains only one LPN: LPN Air/Ground Communication Link.

A4.1 LPN Air/Ground Communication Link

Assumptions

**AS44**: Air/Ground Communication Link could be in one of the following states – work (when no failures of adjacent systems occur) or fail (indicating that one or more failures of adjacent systems occur);

a) Places $P$, transitions $T$, arcs $A$, node function $N$

The Air/Ground Communication Link of the aircraft is represented by the LPN presented in Figure A25. The places represent the following modes:
- **Work** – Air/Ground Communication Link works properly;
- **Fail** – Air/Ground Communication Link has some failure.

LPN contains two delay transitions (D), which are connected to places with ordinary arcs.

![Figure A25. Air/Ground Communication Link](image)

b) Colour type $S$
none

c) Colour function $C$
none

d) Token colour function $V$ and $W$
none

e) Guards $G$
none

f) Delays $D$

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work $\rightarrow$ Fail</td>
<td>$\tau \leftarrow f_E(\cdot; \mu_{R/T})^{\text{failures}}/\mu_{R/T}$</td>
</tr>
<tr>
<td>Fail $\rightarrow$ Work</td>
<td>$\tau \leftarrow f_E(\cdot; \mu_{R/T})^{\text{failure}}$</td>
</tr>
</tbody>
</table>
**APPENDIX 4**

**g) Firing function $F$**
One token without colour to each output place for all transitions.

**h) Initial marking $I$**

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>$1 - p_{\text{R/T failure}}$</td>
<td>-</td>
</tr>
<tr>
<td>Fail</td>
<td>$p_{\text{R/T failure}}$</td>
<td>-</td>
</tr>
</tbody>
</table>

**i) Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu_{\text{R/T failure}}$</td>
<td>Mean duration of $\text{Fail} \rightarrow \text{Work}$</td>
<td>60 sec</td>
<td>(Oliveira et al, 2006)</td>
<td>-</td>
</tr>
<tr>
<td>$p_{\text{R/T failure}}$</td>
<td>Probability of $\text{Fail}$</td>
<td>$3 \cdot 10^{-5}$</td>
<td>(Oliveira et al, 2006)</td>
<td>-</td>
</tr>
</tbody>
</table>

**j) Incoming arcs and IPNs within the same agent**
none

**k) Additional firing functions for outgoing arcs within the same agent**
none

**l) Interaction with other agents or LPNs**
This LPN has no incoming arcs from any LPNs.

This LPN has an outgoing arc to the following LPN (Figure A26):
- LPN ATCo – through enabling arcs.

![Figure A26. Interaction of LPN Air/ground communication link with LPN ATCo](image-url)
A5. TCAS Tactical Air Traffic Controller (ATCo) as Agent

TCAS Tactical Air Traffic Controller as agent contains only one LPN: LPN ATCo.

A5.1 LPN ATCo

Assumptions

**AS45:** Apart from the cognitive and other human factor issues, from the aspect of TCAS ATCo can be in following states: ATCo is responsible and Crew is responsible;

**AS46:** When RA is issued a crew becomes responsible for aircraft separation and informs the ATCo about that, since then the ATCo switches to Crew is responsible state.

**AS47:** After conflict resolution a crew returns to nominal state and informs the ATCo about this, since then the ATCo becomes again responsible for aircraft separation.

a) Places $P$, transitions $T$, arcs $A$, node function $N$

The ATCo is represented by the LPN presented in Figure A27. The places represent the following modes:
- **Crew is responsible** – RA is issued and ATCo is informed about this by the Crew, ATCo is not responsible for separation assurance between the aircraft in conflict;
- **ATCo is responsible** – ATCo is responsible for separation assurance between the aircraft, the aircraft are not in the conflict or a TA is issued.

LPN contains two delay transitions (D) which are connected to places with ordinary arcs.

![Figure A27. LPN for ATCo](image)

b) Colour type $S$
none

c) Colour function $C$
none

d) Token colour function $V$ and $W$
none

e) Guards $G$
none
f) Delays D

<table>
<thead>
<tr>
<th>Transition</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATCo is responsible → Crew is responsible</td>
<td>$\tau \leftarrow f_U(:, [0, 10] \text{ sec})$</td>
</tr>
<tr>
<td>Crew is responsible → ATCo is responsible</td>
<td>$\tau \leftarrow f_U(:, [0, 10] \text{ sec})$</td>
</tr>
</tbody>
</table>

g) Firing function $F$

One token without colour to each output place for all transitions.

h) Initial marking $I$

<table>
<thead>
<tr>
<th>Place</th>
<th>Probability of initial token</th>
<th>Initial colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crew is responsible</td>
<td>$1 - p_{\text{ATCo}}$</td>
<td>-</td>
</tr>
<tr>
<td>ATCo is responsible</td>
<td>$p_{\text{ATCo}}$</td>
<td>-</td>
</tr>
</tbody>
</table>

i) Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
<th>Value</th>
<th>Source</th>
<th>First in</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_{\text{ATCo}}$</td>
<td>Probability of ATCo is responsible</td>
<td>0.95</td>
<td>*</td>
<td>-</td>
</tr>
</tbody>
</table>

* Educated guess

j) Incoming arcs and IPNs within the same agent

See interaction with other agents

k) Additional firing functions for outgoing arcs within the same agent

None

l) Interaction with other agents or LPNs

This LPN has incoming arcs from the following LPNs (Figure A28):
- LPN Crew$_i$ – through enabling and merging arcs (interconnection mapping type I (Everdij et al., 2006));
- LPN Air/Ground Communication Link – through enabling arcs.

This LPN has no outgoing arcs to any LPNs.
### APPENDIX 5: Comparison of cases (encounters, SDCPN vs. Real Life)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>SDCPN</td>
<td>167</td>
<td>180</td>
<td>214</td>
<td>1338.00</td>
<td>11.48</td>
<td>975.00</td>
<td>8.20</td>
<td>2159.00</td>
<td>0.97</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>180</td>
<td>218</td>
<td>n.a.</td>
<td>1659.00</td>
<td>8.45</td>
<td>1175.00</td>
<td>1.27</td>
<td>0</td>
<td>Down-Level/ No change</td>
</tr>
<tr>
<td>Case 2</td>
<td>SDCPN</td>
<td>164</td>
<td>178</td>
<td>211</td>
<td>2083.00</td>
<td>7.16</td>
<td>1354.00</td>
<td>5.08</td>
<td>1398.00</td>
<td>1.58</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>180</td>
<td>211</td>
<td>n.a.</td>
<td>1235.00</td>
<td>4.97</td>
<td>1000.00</td>
<td>1.59</td>
<td>0</td>
<td>Up-Level/ Down-Level</td>
</tr>
<tr>
<td>Case 3</td>
<td>SDCPN</td>
<td>172</td>
<td>185</td>
<td>216</td>
<td>1850.00</td>
<td>9.38</td>
<td>1342.00</td>
<td>6.46</td>
<td>1896.00</td>
<td>0.69</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>179</td>
<td>220</td>
<td>n.a.</td>
<td>1551.00</td>
<td>7.81</td>
<td>1125.00</td>
<td>1.37</td>
<td>0</td>
<td>Up-Level/ No change</td>
</tr>
<tr>
<td>Case 4</td>
<td>SDCPN</td>
<td>170</td>
<td>183</td>
<td>219</td>
<td>1553.00</td>
<td>11.22</td>
<td>968.00</td>
<td>8.14</td>
<td>1193.00</td>
<td>1.09</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>180</td>
<td>221</td>
<td>n.a.</td>
<td>1121.00</td>
<td>8.86</td>
<td>1025.00</td>
<td>0.91</td>
<td>0</td>
<td>Down-Level/ Up-Level</td>
</tr>
<tr>
<td>Case 5</td>
<td>SDCPN</td>
<td>143</td>
<td>-</td>
<td>-</td>
<td>1709.00</td>
<td>10.84</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>158</td>
<td>184</td>
<td>n.a.</td>
<td>1134.00</td>
<td>7.44</td>
<td>1025.00</td>
<td>4.37</td>
<td>0</td>
<td>Down-Level/ No change</td>
</tr>
<tr>
<td>Case 6</td>
<td>SDCPN</td>
<td>169</td>
<td>182</td>
<td>211</td>
<td>1956.00</td>
<td>7.59</td>
<td>1418.00</td>
<td>5.27</td>
<td>1985.00</td>
<td>1.60</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>180</td>
<td>209</td>
<td>n.a.</td>
<td>1507.00</td>
<td>6.22</td>
<td>1800.00</td>
<td>1.81</td>
<td>0</td>
<td>Down-Level/ No change</td>
</tr>
<tr>
<td>Case 7</td>
<td>SDCPN</td>
<td>169</td>
<td>182</td>
<td>204</td>
<td>2343.00</td>
<td>2.98</td>
<td>1702.00</td>
<td>2.01</td>
<td>1918.00</td>
<td>1.16</td>
</tr>
<tr>
<td>Real</td>
<td>n.a.</td>
<td>181</td>
<td>205</td>
<td>n.a.</td>
<td>1774.00</td>
<td>2.27</td>
<td>1520.00</td>
<td>1.22</td>
<td>0</td>
<td>Down-Level/ Up-Level</td>
</tr>
</tbody>
</table>

n.a. – not available
APPENDIX 5

Case 1

Input data

<table>
<thead>
<tr>
<th>Encounter 1</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>-8.26</td>
<td>36.97</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>-9.60</td>
<td>19.46</td>
</tr>
<tr>
<td>H [ft]</td>
<td>24000</td>
<td>30000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>49</td>
<td>246</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>522</td>
<td>400</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>1675</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

Real
Appendix 5

Case 2

Input data

<table>
<thead>
<tr>
<th>Encounter 2</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>35.31</td>
<td>3.08</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>2.79</td>
<td>0.35</td>
</tr>
<tr>
<td>H [ft]</td>
<td>26000</td>
<td>15375</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>307</td>
<td>56</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>315</td>
<td>366</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-1275</td>
<td>1850</td>
</tr>
</tbody>
</table>

Results

SDCPN

![Vertical Projection Graph](vertical_projection.png)

![Horizontal Projection Graph](horizontal_projection.png)

Real

![Real Data Graph](real_data.png)
APPENDIX 5

Case 3

Input data

<table>
<thead>
<tr>
<th>Encounter 3</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>1.22</td>
<td>36.63</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>6.20</td>
<td>38.64</td>
</tr>
<tr>
<td>H [ft]</td>
<td>32575</td>
<td>24000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>61</td>
<td>214</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>400</td>
<td>432</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-2346</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN0

![Vertical Projection](image1)

![Horizontal Projection](image2)

Real

![Graph 1](image3)

![Graph 2](image4)
Case 4

Input data

<table>
<thead>
<tr>
<th></th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>12.91</td>
<td>15.11</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>4.67</td>
<td>56.22</td>
</tr>
<tr>
<td>H [ft]</td>
<td>28000</td>
<td>37200</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>349</td>
<td>200</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>471</td>
<td>417</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>1307</td>
<td>-1392</td>
</tr>
</tbody>
</table>

Results

SDCPN

Vertical Projection

Horizontal Projection

Real
Case 5

Input data

<table>
<thead>
<tr>
<th>Encounter 5</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>40.11</td>
<td>4.51</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>33.88</td>
<td>4.32</td>
</tr>
<tr>
<td>H [ft]</td>
<td>29590</td>
<td>33000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>231</td>
<td>61</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>451</td>
<td>465</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>2241</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

![Graphs showing SDCPN results for own and intruder aircraft.]
Appendix 5

Case 6

Input data

<table>
<thead>
<tr>
<th>Encounter 6</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>41.86</td>
<td>3.32</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>-0.18</td>
<td>-0.35</td>
</tr>
<tr>
<td>H [ft]</td>
<td>28950</td>
<td>20000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>306</td>
<td>45</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>491</td>
<td>374</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-1533</td>
<td>950</td>
</tr>
</tbody>
</table>

Results

SDCPN

![Graph of Vertical Projection](image1)

![Graph of Horizontal Projection](image2)

Real
APPENDIX 5

Case 7

Input data

<table>
<thead>
<tr>
<th>Encounter 7</th>
<th>AC1</th>
<th>AC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>29.29</td>
<td>42.82</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>1.56</td>
<td>12.00</td>
</tr>
<tr>
<td>H [ft]</td>
<td>21325</td>
<td>32000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>338</td>
<td>295</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>382</td>
<td>437</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>2022</td>
<td>-936</td>
</tr>
</tbody>
</table>

Results

SDCPN

Vertical Projection

Horizontal Projection

Real
APPENDIX 6: Comparison to Other Models

Validation of the developed SDCPN model of ACAS operations is performed using historical data. Here presented is a Comparison with another model which performed well, as an alternative before real life data was obtained. The results of the Comparison with the other model are presented in Appendix 6, 7, 8, 9 and 10. For the purpose of validation an InCAS model was chosen as most similar to the developed SDCPN-based model, although information about its validation was not available.

InCAS Model

Interactive Collision Avoidance Simulator (InCAS\textsuperscript{12}) is an interactive system for evaluation, studies, demonstration and training on Airborne Collision Avoidance Systems (ACAS). InCAS is a set of interactive tools providing facilities to prepare, simulate and analyse ACAS encounters. InCAS was developed and is maintained by EUROCONTROL Experimental Centre (EEC). Version 2.6 was used in this research (EEC, 2005).

InCAS is a flexible and fully-integrated ACAS simulator, including all features required to prepare, run, and analyse ACAS simulations of aircraft encounters taken from real radar data. One can prepare encounters from a number of standard radar track data formats, configure ACAS scenarios, run or playback ACAS simulations, view an ACAS encounter through simulated pilot and controller displays and analyse and diagnose ACAS behaviour (EEC, 2005).

InCAS also allows for the creation of artificial scenarios, which was used in this research with the aim of obtaining outputs for validation. Input data necessary to run InCAS are: initial 3D position, ground speed, vertical speed and headings. Using the data for a pair of aircraft, an encounter is created and then the simulation is performed. The results of the simulation are moments when TA, RA and CoC are issued, together with the sense and strength of the resolution advisory, both for the own and the intruder aircraft.

TCAS SDCPN vs. InCAS

SDCPN and InCAS models are both intended to simulate TCAS II operations, but with different intended purposes. TCAS SDCPN is intended for risk/safety assessment, i.e. to assess the benefit TCAS can bring into the ATM system in the sense of collision risk reduction. Its role is prospective, providing system designers with safety feedback. According to Dean (2007) InCAS is intended for incident/accident analysis including ACAS analysis, i.e. for analysing aircraft encounters taken from real radar data. Its role is retrospective providing analyst with insight into pilot and controller behaviour during airprox and other close encounters.

The core of the both models is the TCAS II Logic. InCAS contain logic provided by MITRE for which it is assumed that it was developed according to “Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment” (RTCA, 1997). The SDCPN-based ACAS model contains a model of TCAS II logic which is mainly developed according to “Introduction to TCAS II Version 7” (DoT, 2000).

\textsuperscript{12} InCAS model was kindly provided by Mr Garfield Dean from EUROCONTROL Experimental Centre (EEC)
In order to understand the differences between the two models for the purpose of validation, the mentioned two documents are compared, as well as an explanation provided as to what is covered in the SDCPN-based ACAS model. The comparison of both documents is provided in Appendix 7. In order to better understand behaviour of the models as well as potential differences in output results, a comparison of their main characteristics is given (Table T1).

<table>
<thead>
<tr>
<th>Model Nature</th>
<th>SDCPN-based ACAS model</th>
<th>InCAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Risk and Safety Assessment of TCAS operation</td>
<td>ACAS encounters analysis of encounters taken from real radar data</td>
</tr>
<tr>
<td>TCAS II Logic</td>
<td>Model of TCAS II Logic (without RA modification)</td>
<td>Real TCAS II logic, provided by MITRE Co.</td>
</tr>
<tr>
<td>Altitude change</td>
<td>Continuous</td>
<td>Step change (quantization of 25ft and 100 ft)</td>
</tr>
<tr>
<td>Vertical speed, Ground speed, Magnetic heading</td>
<td>Constant during encounter</td>
<td>In case of recorded radar data they are variable during the encounter, otherwise they are constant</td>
</tr>
<tr>
<td>Pilot reaction</td>
<td>Included, with randomly delayed reaction (without return to original trajectory or original vertical speed after Clear of Conflict) and with possibility to refuse to act according to issued RA</td>
<td>Included, With delayed reaction and idealised pilot response (with return to original trajectory or original vertical speed after Clear of Conflict)</td>
</tr>
<tr>
<td>ATCo role</td>
<td>Included as active (responsible for separation) or passive (when pilot is reacting according to RA). Reaction is randomly delayed.</td>
<td>Not included</td>
</tr>
<tr>
<td>Reliability of technical system</td>
<td>Included (failure rates)</td>
<td>Not included</td>
</tr>
</tbody>
</table>

Validation of the TCAS SDCPN model vs. InCAS model

The approach taken in this research was to perform validation by comparing the outputs from the developed SDCPN model with outputs from InCAS, for the same inputs (Figure B1). Inputs for the comparison experiments are chosen to be a set of nine representative cases (Raynaud, 2007), presented in I-AM-SAFE\textsuperscript{13} project (I-AM-SAFE, 2007). Descriptions of those cases are given in Appendix 8.

Following outputs are chosen:

a) selected sense and strength for issued RA; and
b) minimum horizontal distance at CPA as well as corresponding vertical distance and time.

c) moments when Traffic alert (TA), Resolution Advisory (RA) and Clear of Conflict (CoC) are issued;

d) vertical and horizontal distance at TA, RA and CoC moments.

\textsuperscript{13} I-AM-SAFE stands for IAPA – ASARP Methodology for Safety net Assessment – Feasibility Evaluation. The objective of the I-AM-SAFE project is to assess the applicability and usefulness of the encounter model approach (used in the ACAS field) in the prospect of establishing safety and performance requirements for STCA.
From listed outputs just those under a) and b) are used in the validation process (Level 3 and Level 4) while c) and d) are used for illustration. The facts that TCAS is activated (Level 1) and an RA is issued (Level 2), are considered implicitly.

Results of comparison are shown separately for each case and per given test variables in tabular as well as in graphical form in Appendix 9. Existing similarities and differences between results are explained in Appendix 10. The validation results are presented in following text.

Nine representative cases were available. They were used to run both the TCAS SDCPN model and the InCAS model, providing replications of these nine cases.

Table T2 presents results of Level 1 validation. It was shown both in InCAS and in SDCPN-based model that in 8 out of 9 simulated cases TCAS was activated. Results are in green field, meaning that satisfactory validation results are obtained. However, 1 out of 9 cases falls in the yellow field. In that case TCAS activity was not triggered in InCAS while in the SDCPN-based model it was. Consequently, it means that this scenario could present a “false alert”.

Table T2. Level 1 validation: TCAS SDCPN model vs. InCAS model

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>InCAS model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 (no)</td>
</tr>
<tr>
<td>1 (no)</td>
<td>0</td>
</tr>
<tr>
<td>2 (yes)</td>
<td>1</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model

Table T3 presents results of Level 2 validation. It was shown that TCAS was generating RAs in 5 out of 8 simulated cases, and TAs in 3 out of 8 cases, both in the InCAS and in the SDCPN-based model. Results are in green fields, meaning that satisfactory validation results were obtained. One of 9 cases SDCPN-based model generated a TA in case when no TCAS activity was recorded in the InCAS model. This situation fell in a yellow field. Actually, it is the same case appearing in the yellow field in the Level 1 validation.
Table T3. Level 2 validation: TCAS SDCPN model vs. InCAS model

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>InCAS model</th>
<th>1 (no event)</th>
<th>2 (TA)</th>
<th>3 (RA)</th>
<th>4 (RA*)</th>
<th>5 (RA_MAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (no event)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2 (TA)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3 (RA)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4 (RA*)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>5 (RA_MAC)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model
RA* - RA activated but vertical separation at CPA violated; RA_MAC – RA activated but Mid-Air Collision occurred

Table T4 presents the results of Level 3 validation. It was shown that in 5 out of 5 simulated cases the resolution manoeuvre was similar in both the InCAS and the SDCPN-based model. All results fell in a green field, meaning that satisfactory validation results were obtained.

Table T4. Level 3 validation: TCAS SDCPN model vs. InCAS model

<table>
<thead>
<tr>
<th>SDCPN</th>
<th>InCAS model</th>
<th>1 (RA)</th>
<th>2 (RA*)</th>
<th>3 (RA_MAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (RA)</td>
<td>u/d</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>d/u</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 (RA*)</td>
<td>u/d</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>d/u</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 (RA_MAC)</td>
<td>u/d</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>d/u</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

LEGEND: green – appropriate; red – failure of the model to activate TCAS; yellow – false alarm by the model
RA* - RA activated but vertical separation at CPA violated; RA_MAC – RA activated but Mid-Air Collision occurred
u/d – up/down or up/down-level or up/no-change manoeuvre, d/u – down/up or down/up-level or down/no-change manoeuvre

Under Level 4 validation, in Figure B2, matching between InCAS model and SDCPN-based model data is presented. The differences between horizontal distance values at CPA are smaller than differences at CPA in vertical distance. SDCPN-based model provides vertical distances that are higher than in the case of the InCAS model (RA points are placed above x = y line (Figure B2)), which could be explained by the following reasons:

a) RA strength in SDCPN-based model was assumed to have maximal value, from suggested range of strength values, while in InCAS applied values are from the recommended range;

b) Certain differences in TCAS logic (see Appendix 10 for details).

It could be concluded that the first three validation levels were passed satisfactorily, but in the fourth some differences appear, which were not used for further model modifications, but they were presented in order to obtain feedback about the “quality” of the model.
Figure B2. Level 4 validation: TCAS SDCPN model vs. InCAS model
### APPENDIX 7: Comparison of RTCA MOPS Do185A and DOT/FAA document

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Parameter Values</td>
<td>DMOD&lt;sub&gt;TA&lt;/sub&gt; doesn’t exist (Table 2-13, pp 123), ZTHR exist (see additional Table A)</td>
<td>ZTHR doesn’t exist (Table 2, pp. 22) and is not mentioned throughout the text. (see additional Table B)</td>
<td>Both tables are very similar, but the table in the DOT/FAA document is newer, so it is possible that the FAA (as an authority) had made some changes related to the RTCA</td>
<td>DOT/FAA Table 2, pp. 22 is applied.</td>
</tr>
<tr>
<td>Sensitivity Level (SL) selection</td>
<td>- Manual (from the cockpit switch), - Command (from ground-based Mode S sensors), - Automatic (from on-board barometric and radio altimeters) (pp 122, paragraph 2)</td>
<td>- Pilot selection (standby, TA-Only and TA-RA which automatically selects SL based on own aircraft altitude) - Ground-based selection (from the ground based Mode S sensors) (pp. 21, paragraph 4)</td>
<td>The manners of SL selection are the same. In DOT/FAA documents the type of selection are categorized differently.</td>
<td>It is assumed that TA-RA, i.e. automatic SL selection (from own on-board altimeter) is applied.</td>
</tr>
<tr>
<td>TAU (description and computation)</td>
<td>Not specifically defined.</td>
<td>- TCAS uses time-to-go to CPA, rather than distance, to determine when a TA or an RA should be issued. - TCAS uses time to CPA to determine the range tau and the time to co-altitude to determine the vertical tau. - Tau is an approximation of the time, in seconds, to CPA or to the aircraft being at the same altitude. - The range tau is equal to the slant range (nmi) divided by the closing speed (knots) multiplied by 3600. The vertical tau is equal to the altitude separation (feet) divided by the combined vertical speed of the two</td>
<td>The difference is evident (self-explanatory)</td>
<td>DOT/FAA description is applied.</td>
</tr>
<tr>
<td>DMOD/Altitude separation threshold (description and computation)</td>
<td>Not specifically defined.</td>
<td>- In events where the rate of closure is very low, an intruder aircraft can come very close in range without crossing the range tau boundaries and thus, without causing a TA or an RA to be issued. To provide protection in these types of advisories, the range tau boundaries are modified. This modification is referred to as DMOD and allows TCAS to use a fixed-range threshold to issue TAs and RAs in these slow closure encounters. The value of DMOD varies with different sensitivity levels. (pp. 22, paragraph 3)</td>
<td>The difference is evident (self-explanatory)</td>
<td>DOT/FAA description is applied.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Threat Detection</td>
<td>- An aircraft will be declared a collision threat to the TCAS aircraft if its current or projected relative position within a specific prediction time simultaneously violates slant range and relative altitude boundaries. (pp. 125, paragraph 2) - A threat aircraft will produce a collision warning in advance of closest approach by</td>
<td>- For either a TA or an RA to be issued, both the range and vertical criteria, in terms of tau or the fixed thresholds (DMOD, altitude threshold), must be satisfied. If only one of the criteria is satisfied, TCAS will not issue an advisory. (pp. 22, last paragraph) - The range test is based on tau, and the TA tau must be less than the threshold (see</td>
<td>- Both documents provide only descriptions (no figures, no equations) which are not completely clear and enough to be appropriately applied. - Also, it is noticeable that some explanations are not mutually consistent, e.g. in DOT/FAA descriptions given at page 27, paragraphs 3 and 7 with description on page 22, last paragraph. - Similarly, in RTCA Following description from DOT/FAA document is applied: “For either a TA or an RA to be issued, both the range and vertical criteria, in terms of tau or the fixed thresholds (DMOD, altitude threshold), must be satisfied. If only one of the criteria is satisfied, TCAS will not issue an</td>
<td></td>
</tr>
</tbody>
</table>
the amount of the prediction time (15 to 35 seconds). Additional time is provided for accelerating encounters by means of an incremental protected volume (DMOD) about own aircraft. (pp. 125, paragraph 3)

- To be declared a threat, an aircraft’s expected altitude separation at the point of closest approach must be less than an altitude threshold (ZTHR). (pp. 125, paragraph 4)

- A Miss Distance Filter ….. Turn and speed change detection algorithms are used to shut the filter off and allow a resolution advisory to be issued. (pp. 125, first paragraph)

Not specifically defined

<table>
<thead>
<tr>
<th>Table B</th>
<th>In addition, the current or projected vertical separation at CPA must be within the TA altitude threshold (see Table B) for a target to be declared an intruder. (pp. 27, paragraph 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>document, some facts are introduced without previous explicit explanation (e.g. DMOD and ZTHR usage. at page 125, paragraphs 3 and 5).</td>
<td></td>
</tr>
<tr>
<td>- Finally, it seems that the descriptions provided in both DOT/FAA and RTCA documents are similar in parts on page 22, last paragraph of DOT/FAA and page 125, paragraph 2 of the RTCA document, while in other parts it seems they are not so similar.</td>
<td></td>
</tr>
</tbody>
</table>

The difference is evident (self-explanatory)

<table>
<thead>
<tr>
<th>Not specifically defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reducing alert thresholds to account for the reduction in vertical separation to 1000 feet above FL290 in RVSM airspace. (pp. 27, paragraph 8, bullet 4)</td>
</tr>
<tr>
<td>The difference is evident (self-explanatory)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT/FAA description is applied. Additionally, the linear escape rate used in intruder’s flight path model of 1500 fpm is accepted from RTCA document.</td>
</tr>
</tbody>
</table>

Threat Resolution – Sense Selection

- TCAS computes the predicted vertical separation for each of the two sense selection options. The directional sense that gives the greater predicted vertical separation from the threat aircraft at the time of closest approach is normally selected as the preferred sense of the resolution advisory caused by this threat. (pp. 127, paragraph 4)

- The path model in all cases consists of a linear segment, followed by a

<table>
<thead>
<tr>
<th>Table B</th>
<th>The first step in the process is to select the RA sense, i.e., upward or downward. Based on the range and altitude tracks of the intruder, the CAS logic models the intruder’s flight path from its present position to CPA. The CAS logic then models upward and downward sense RAs for own aircraft, to determine which sense provides more vertical separation at CPA. (pp. 28, paragraph above Figure 15)</th>
</tr>
</thead>
<tbody>
<tr>
<td>document, some facts are introduced without previous explicit explanation (e.g. DMOD and ZTHR usage. at page 125, paragraphs 3 and 5).</td>
<td></td>
</tr>
<tr>
<td>- It seems that the explanations provided by both documents are the same.</td>
<td></td>
</tr>
<tr>
<td>- The DOT/FAA document also contains a figure which visually helps to better understand the description provided.</td>
<td></td>
</tr>
</tbody>
</table>

DOT/FAA description is applied. Additionally, the linear escape rate used in intruder’s flight path model of 1500 fpm is accepted from RTCA document.
constant-acceleration altitude rate change, followed by a linear segment. The linear escape rate modelled is nominally 1500 fpm. (pp. 127, first paragraph)

In the following cases, due to additional considerations, the preferred sense may not be the direction that gives the greatest modelled separation (pp. 127, paragraph 5):
- If the resultant sense is non-crossing, the higher address threat will be forced to reverse the sense of its RA to non-crossing. (pp. 127, paragraph 6)
- When the non-crossing sense is chosen because that sense will result in adequate separation at closest approach. (pp. 127, paragraph 8)

- TCAS is designed to select the non-altitude crossing sense if the non-crossing sense provides the desired vertical separation, known as ALIM, at CPA. (pp. 28, paragraph 3)
- If the non-altitude crossing sense provides at least ALIM feet of separation at CPA, this sense will be selected even if the altitude-crossing sense provides greater separation. If ALIM cannot be obtained in the non-altitude crossing sense, an altitude crossing RA will be issued. (pp. 28, paragraph 4)

- It seems that the explanations provided by both documents are the same.
- The DOT/FAA document also contains the figure which visually helps to better understand the description provided.

DOT/FAA description is applied.

<p>| TCAS may determine that the TCAS aircraft cannot execute the nominal climb escape manoeuvre. This determination may be made according to the unique characteristics of the aircraft on which TCAS is installed and the regime of flight and may use on-board inputs not otherwise required by TCAS. Path modelling will substitute level flight for the climb manoeuvre in such instances. (pp.127, paragraph 2) |
| Similarly, radio altimeter data is used to recognize when TCAS is too near to the ground to issue a |
| Not specifically defined |
| The difference is evident (self-explanatory) |
| Not applied. |</p>
<table>
<thead>
<tr>
<th>Threat Resolution – Sense reversals</th>
<th>The logic permits sense reversals of either crossing or non-crossing resolution advisories based on changes in encounter geometry, which indicate that the original advisory is being thwarted. Such geometry-based reversals can occur both in TCAS-unequipped and TCAS-TCAS encounters. (pp. 128, paragraph 3)</th>
<th>In some events, the intruder aircraft will manoeuvre vertically in a manner that thwarts the effectiveness of the issued RA. In these cases, the initial RA will be modified to either increase the strength or reverse the sense of the initial RA. (pp. 29, paragraph 2)</th>
<th>It seems that the explanations provided by both documents are the same.</th>
<th>Not applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Resolution – Strength Selection</td>
<td>- The second phase of resolution processing is the computation of the least disruptive vertical flight profile that TCAS can fly to achieve safe separation. (pp. 129, paragraph 1) - TCAS will generate a positive advisory either if the threat is</td>
<td>- TCAS is designed to select the RA strength that is the least disruptive to the existing flight path, while still providing ALIM feet of separation. (pp. 28, paragraph 5)</td>
<td>- It seems that the explanations provided by both documents are the same. - RTCA document provides a more description.</td>
<td>A combination of DOT/FAA and RTCA description is applied.</td>
</tr>
</tbody>
</table>
When two TCAS-equipped aircraft are converging vertically with opposite rates and are currently well-separated in altitude, TCAS will first issue a vertical speed limit (Negative) RA to reinforce the pilot’s likely intention to level off at adjacent flight levels. If no response to this initial RA is detected, or if either aircraft accelerates toward the other, the initial negative (VSL 0 fpm) RA is allowed to strengthen as necessary. (pp. 129, paragraph 3)

When two TCAS-equipped aircraft are converging vertically with opposite rates and are currently well-separated in altitude, TCAS will first issue a vertical speed limit (Negative) RA to reinforce the pilot’s likely intention to level off at adjacent flight levels. If no response to this initial RA is detected, or if either aircraft accelerates toward the other, the initial RA will strengthen as required. (pp. 28, last)

It seems that the explanations provided by both documents are the same.

No categorisation of RA types is made, then calculation of vertical speed ranges which will provide a safe separation at CPA.

Table:

<table>
<thead>
<tr>
<th>Threat Resolution – Strength Modification</th>
<th>Positive RA types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solved</td>
<td>- <strong>CLIMB</strong>, <strong>DESCENT</strong> (vertical speed 1500 – 2000 fpm);</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAINTAIN</strong> <strong>CLIMB</strong> or <strong>DESCENT</strong> (vertical speed &gt;1500 fpm);</td>
</tr>
<tr>
<td></td>
<td>- <strong>INCREASE</strong> <strong>CLIMB</strong> or <strong>DESCENT</strong> (vertical speed 2500 fpm);</td>
</tr>
<tr>
<td></td>
<td>(pp. 129, paragraph 1)</td>
</tr>
</tbody>
</table>

| Difference in vertical speed values is evident (DOT/FAA provides more explicit ranges). Also, instead of **INCREASE** RA type in RTCA document, in DOT/FAA document a **CROSSING** RA type exist. So it is possible that the FAA (as an authority ) was making some changes relative to the RTCA |

| No categorisation of RA types is made, then calculation of vertical speed ranges which will provide a safe separation at CPA |

| It seems that the explanations provided by both documents are the same. |

| Not applied. |
| Appendix 7 |
|-----------------|---------------------------------|---------------------------------|-----------------------------|
| **Clear of Conflict** | - The advisory will be retained until the aircraft ... diverge in range. (pp. 124, first paragraph). - It will remain classified as a threat until both aircraft ... begin to diverge in range (pp. 125, paragraph 5) | After CPA is passed and the range between the TCAS aircraft and threat aircraft begins to increase, all RAs are cancelled. (pp. 30, paragraph 4) | It seems that the explanations provided by both documents are the same. DOT/FAA description is applied. |
| **TCAS-TCAS Coordination** | When a TCAS-equipped aircraft is in an encounter with a threat that is also equipped with TCAS having on-board resolution capability, TCAS communicates to the threat the sense of its advisory with respect to that threat. The communication is in the form of a negative command (e.g., Don’t Climb or Don’t Descend) and is referred to as the aircraft’s resolution advisory complement (RAC) or, less formally, its “intent.” That is, if one aircraft has selected a climb sense advisory against a TCAS-equipped threat, it will send a Don’t Climb RAC to that threat. (pp. 131, last paragraph and pp. 132, first paragraph) | Coordination interrogations contain information about an aircraft’s intended RA sense to resolve the encounter with the other TCAS-equipped intruder. The information in the coordination interrogation is expressed in the form of a complement. For example, when an aircraft selects an upward sense RA, it will transmit a coordination interrogation to the other aircraft that restricts that aircraft’s RA selection to those in the downward sense. (pp. 30, last paragraph) | It seems that the explanations provided by both documents are the same. DOT/FAA description is applied. |
| | The basic rule for sense selection in an encounter with a TCAS-equipped threat is that before selecting a sense, each TCAS must first check if it has received an intent message from the threat. If no intent has been received, TCAS will select a sense based on the encounter geometry. If an intent has been received, in most cases TCAS will | The basic rule for sense selection in a TCAS-TCAS encounter is that each TCAS must check whether it has received an intent message from the other aircraft before selecting an RA sense. If an intent message has been received, TCAS selects the opposite sense from that selected by the other aircraft and communicated via the | It seems that the explanations provided by both documents are the same. Not applied, due to the assumption that Own aircraft has ultimate priority over intruder aircraft, i.e. it is assumed that its Mode S address is lower. |
| Multi-aircraft encounters | immediately select the complementary RA sense. (pp. 132, paragraph 2) | coordination interrogation. If TCAS has not received an intent message, the sense is selected based on the encounter geometry in the same manner as would be done if the intruder were not TCAS equipped. (pp. 31, first paragraph) | | 
| TCAS will attempt to resolve these types of encounters by selecting a single RA that will provide adequate separation from each of the intruders. (pp. 29, last paragraph) | It seems that the explanations provided by both documents are the same. | Not applied. |
### APPENDIX 8: Description of Cases Used for Model Comparison

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
<th>Layout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• This scenario illustrates a non-serious encounter in en-route airspace which eventually results in a minor separation infringement (4.9NM; 800 feet) between the aircraft at closest approach.</td>
<td>![Image 1]</td>
</tr>
</tbody>
</table>
| 2    | • This scenario illustrates an encounter in en-route airspace which eventually results in a serious separation infringement (0.6NM; 50 feet) at closest approach.  
• The encounter also triggers a TCAS Resolution Advisory (RA) on board the aircraft (as no recovery action is taken on time). | ![Image 2] |
| 3    | • This scenario illustrates an encounter in en-route airspace which eventually results in a serious separation infringement (2.3NM; 300 feet) at closest approach.  
• The encounter triggers a Traffic Advisory (TA) on board the aircraft. | ![Image 3] |
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
<th>Layout</th>
</tr>
</thead>
</table>
| 4        | - This scenario illustrates a 1,000 feet level-off encounter in en-route airspace.  
- The encounter triggers a TCAS Resolution Advisory (RA) on board the aircraft due to the high vertical convergence rate before level-off. | ![Diagram](image1.png) |
| 5        | - This scenario illustrates an altitude bust encounter in en-route airspace which eventually results in a serious separation infringement (0.4NM; 500 feet) at closest approach.  
- The encounter also triggers a TCAS Resolution Advisory (RA) on board the aircraft (as no recovery action is taken on time). | ![Diagram](image2.png) |
| 6        | - This scenario illustrates an encounter in en-route airspace which eventually results in a serious separation infringement (1.2NM; 50 feet) at closest approach.  
- The encounter triggers a TCAS Resolution Advisory (RA) on board the aircraft. | ![Diagram](image3.png) |
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
<th>Layout</th>
</tr>
</thead>
</table>
| 7        | • This scenario illustrates a slow vertical convergence encounter in TMA airspace which eventually results in a major separation infringement (1.0NM; 600 feet) at closest approach.  
• The encounter triggers a TCAS Traffic Advisory (TA) on board the aircraft. | ![Diagram 1](image1.png) |
| 8        | • This scenario illustrates an encounter in en-route airspace which eventually results in a major separation infringement (2.6NM; 740 feet) at closest approach.  
• The encounter triggers a TCAS Resolution Advisory (RA) on board the aircraft (as no recovery action is taken on time). | ![Diagram 2](image2.png) |
| 9        | • This scenario illustrates an encounter in en-route airspace which does not eventually result in a separation infringement (5.2NM; 950 feet) at closest approach, although very close to the separation minima.  
• The encounter triggers a TCAS Traffic Advisory (TA) on board the aircraft. | ![Diagram 3](image3.png) |
## APPENDIX 9: Comparison of cases (SDCPN vs. InCAS)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>SDCPN</td>
<td>165</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2050.00</td>
<td>1.72</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2397.00</td>
<td>1.28</td>
<td>157</td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2444.00</td>
<td>1.27</td>
<td>157</td>
</tr>
<tr>
<td>Case 2</td>
<td>SDCPN</td>
<td>144.00</td>
<td>157.00</td>
<td>172.00</td>
<td>2860.00</td>
<td>1.09</td>
<td>2080.00</td>
<td>0.57</td>
<td>2046.67</td>
<td>0.24</td>
<td>Up/Down (-1600,-2100)/(-1500,2000)</td>
<td>2033.00</td>
<td>0.22</td>
<td>170</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>144.00</td>
<td>168.00</td>
<td>176.00</td>
<td>2820.00</td>
<td>1.10</td>
<td>1380.00</td>
<td>0.23</td>
<td>1055.00</td>
<td>0.30</td>
<td>Up/Down (-1500,-2000)/(-1500,2000)</td>
<td>1200.00</td>
<td>0.23</td>
<td>171</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 3</td>
<td>SDCPN</td>
<td>166.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>1273.33</td>
<td>0.96</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>1007.00</td>
<td>0.04</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>164.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>1282.00</td>
<td>1.20</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>961.00</td>
<td>0.04</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td>Case 4</td>
<td>SDCPN</td>
<td>46.00</td>
<td>59.00</td>
<td>91.00</td>
<td>1983.33</td>
<td>10.21</td>
<td>1441.67</td>
<td>7.15</td>
<td>2075.00</td>
<td>0.54</td>
<td>Up/Down (-500,-1000)/(-1500,2000)</td>
<td>2025.00</td>
<td>0.37</td>
<td>89</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>46.00</td>
<td>60.00</td>
<td>94.00</td>
<td>1938.00</td>
<td>10.20</td>
<td>1355.00</td>
<td>6.90</td>
<td>730.00</td>
<td>1.20</td>
<td>Up/No change (-500,-1000)</td>
<td>800.00</td>
<td>0.36</td>
<td>89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 5</td>
<td>SDCPN</td>
<td>136.00</td>
<td>151.00</td>
<td>176.00</td>
<td>733.33</td>
<td>4.95</td>
<td>483.33</td>
<td>2.99</td>
<td>1241.67</td>
<td>0.27</td>
<td>Up/Down (500,1000)/(-500,1000)</td>
<td>1175.00</td>
<td>0.07</td>
<td>174</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>130.00</td>
<td>144.00</td>
<td>179.00</td>
<td>840.00</td>
<td>5.70</td>
<td>600.00</td>
<td>3.90</td>
<td>1031.00</td>
<td>0.70</td>
<td>Up/Down (1500,2000)/(-1500,2000)</td>
<td>1006.00</td>
<td>0.07</td>
<td>174</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 6</td>
<td>SDCPN</td>
<td>165.00</td>
<td>169.00</td>
<td>226.00</td>
<td>800.00</td>
<td>0.75</td>
<td>400.00</td>
<td>0.70</td>
<td>4358.33</td>
<td>0.06</td>
<td>Up/Down (-2800,-2300)/(-3200,2700)</td>
<td>4192.00</td>
<td>0.05</td>
<td>224</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>126.00</td>
<td>139.00</td>
<td>n.a.</td>
<td>4696.00</td>
<td>1.20</td>
<td>3394.00</td>
<td>1.10</td>
<td>n.a.</td>
<td>n.a.</td>
<td>Up/Down 0/(300, 500)</td>
<td>2423.00</td>
<td>0.05</td>
<td>226</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 7</td>
<td>SDCPN</td>
<td>160.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>766.67</td>
<td>0.33</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>710.00</td>
<td>0.20</td>
<td>177</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>133.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>847.00</td>
<td>0.70</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>701.00</td>
<td>0.20</td>
<td>177</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 8</td>
<td>SDCPN</td>
<td>131.00</td>
<td>144.00</td>
<td>172.00</td>
<td>3003.33</td>
<td>6.72</td>
<td>2180.00</td>
<td>4.54</td>
<td>2273.33</td>
<td>0.73</td>
<td>Up/Down (-800,-300)/(-500,500)</td>
<td>2287.00</td>
<td>0.68</td>
<td>170</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>131.00</td>
<td>144.00</td>
<td>175.00</td>
<td>2994.00</td>
<td>6.70</td>
<td>2169.00</td>
<td>4.50</td>
<td>1353.00</td>
<td>1.00</td>
<td>Up/Down (-500,-1000)/(-500,500)</td>
<td>1433.00</td>
<td>0.68</td>
<td>171</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 9</td>
<td>SDCPN</td>
<td>193.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>498.33</td>
<td>11.45</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2032.00</td>
<td>4.63</td>
<td>233</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InCAS</td>
<td>192.00</td>
<td>n.a.</td>
<td>n.a.</td>
<td>506.00</td>
<td>11.70</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2082.00</td>
<td>4.63</td>
<td>233</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

n.a. – not available
APPENDIX 9

Case 1

Input data

<table>
<thead>
<tr>
<th>SCENARIO 1</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$ [Nm]</td>
<td>0</td>
<td>-10.6</td>
</tr>
<tr>
<td>$y$ [Nm]</td>
<td>5</td>
<td>23.5</td>
</tr>
<tr>
<td>$H$ [ft]</td>
<td>26000</td>
<td>16800</td>
</tr>
<tr>
<td>$MH$ [degree]</td>
<td>360</td>
<td>65</td>
</tr>
<tr>
<td>$GS$ [kt]</td>
<td>540</td>
<td>240</td>
</tr>
<tr>
<td>$VS$ [fpm]</td>
<td>0</td>
<td>2600</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Appendix 9

Case 2

Input data

<table>
<thead>
<tr>
<th>SCENARIO 2</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>-6.5</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>4.3</td>
<td>7</td>
</tr>
<tr>
<td>H [ft]</td>
<td>40500</td>
<td>29000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>360</td>
<td>18</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>480</td>
<td>440</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-3600</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 3

Input data

<table>
<thead>
<tr>
<th>SCENARIO 3</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>15.7</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>4</td>
<td>11.8</td>
</tr>
<tr>
<td>H [ft]</td>
<td>36700</td>
<td>31000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>360</td>
<td>310</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>430</td>
<td>420</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-1600</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Appendix 9

Case 4

Input data

<table>
<thead>
<tr>
<th>SCENARIO 4</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>1.5</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>13.8</td>
<td>34.8</td>
</tr>
<tr>
<td>H [ft]</td>
<td>360</td>
<td>186</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>39900</td>
<td>36000</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>410</td>
<td>440</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-2500</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 5

Input data

<table>
<thead>
<tr>
<th>SCENARIO 5</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>-18</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>4.2</td>
<td>18</td>
</tr>
<tr>
<td>H [ft]</td>
<td>360</td>
<td>65</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>18200</td>
<td>15200</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>460</td>
<td>410</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-500</td>
<td>500</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 6

Input data

<table>
<thead>
<tr>
<th>SCENARIO 6</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>2.8</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>3.3</td>
<td>2.8</td>
</tr>
<tr>
<td>H [ft]</td>
<td>360</td>
<td>353</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>26100</td>
<td>8800</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>360</td>
<td>370</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-2800</td>
<td>3200</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 7

Input data

<table>
<thead>
<tr>
<th>SCENARIO 7</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>-2.3</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>1.3</td>
<td>2.5</td>
</tr>
<tr>
<td>H [ft]</td>
<td>4200</td>
<td>5500</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>360</td>
<td>20</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>150</td>
<td>130</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-750</td>
<td>-950</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 8

Input data

<table>
<thead>
<tr>
<th>SCENARIO 8</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>21.6</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>4.3</td>
<td>23.5</td>
</tr>
<tr>
<td>H [ft]</td>
<td>360</td>
<td>278</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>29000</td>
<td>17700</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>460</td>
<td>470</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-2300</td>
<td>1500</td>
</tr>
</tbody>
</table>

Results

SDCPN

InCAS
Case 9

Input data

<table>
<thead>
<tr>
<th>SCENARIO 9</th>
<th>SAFE 01</th>
<th>SAFE 02</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [Nm]</td>
<td>0</td>
<td>-11.8</td>
</tr>
<tr>
<td>y [Nm]</td>
<td>-33.2</td>
<td>26.8</td>
</tr>
<tr>
<td>H [ft]</td>
<td>38900</td>
<td>32000</td>
</tr>
<tr>
<td>MH [degree]</td>
<td>360</td>
<td>165</td>
</tr>
<tr>
<td>GS [kt]</td>
<td>520</td>
<td>430</td>
</tr>
<tr>
<td>VS [fpm]</td>
<td>-2300</td>
<td>0</td>
</tr>
</tbody>
</table>

Results

SDCPN

Horizontal Projection

Vertical Projection

InCAS
APPENDIX 10: Similarities and differences between SDCPN and InCAS results

- **Scenario 1** SDCPN generates a TA while InCAS does not. The similarity between horizontal and vertical separations at CPA is notable (1.28Nm vs. 1.27Nm and 2397ft vs. 2444ft respectively for SDCPN and InCAS (Table in Appendix 9)). This is actually the only data used for comparison in this scenario;

- **Scenario 2** a TA appears in the same moment (144 seconds), and vertical and horizontal separations in that moment are similar (40ft higher vertical distance and 0.01Nm shorter horizontal distances in SDCPN (Table in Appendix 9)).

In SDCPN an RA is issued 11 seconds earlier than in InCAS, also producing different separation values at this moment. Due to large difference in RA moment, an additional diagnosis is performed. It was determined that in SDCPN an RA is issued when both $\tau_H$ and $\tau_V$ were lower than the threshold of 35 seconds. It happened 157 seconds from the beginning of encounter. After 11 seconds an RA was issued in InCAS, when both DMOD and ALIM conditions were satisfied (see following part of the InCAS diagnosis report). It could be seen that 1 sec before the RA was issued, the predicted vertical miss distance was 702ft and is decreasing, meaning that at the next moment it was lower then 700ft (which is not completely clear from the report, given in grey).

It seems that in InCAS a combination of criteria is used for RA issuance. Further clarification on threat detection applied in InCAS is necessary.

Nonetheless, the difference in RA moments causes the difference in the horizontal and vertical separations at the RA moment, and respective separations at CoC. The RA sense is the same in both models, while the strength is very similar.

The difference in CoC time for SDCPN is due to the assumption that 1 sec after CPA a CoC is issued, while in InCAS CoC is issued 4 sec after CPA. Selected sense and strength are almost the same as well as horizontal separation at CPA (0.22Nm in SDCPN vs.
0.23Nm in InCAS (Table in Appendix 9)) and time of CPA (170 sec since the beginning of the encounter in SDCPN vs. 171 sec in InCAS).

Searching for the possible reasons for differences the following causes were found:

1. In the SDCPN model the threat detection algorithm is simpler than in InCAS (see previous comparison between SDCPN and InCAS model) meaning that either temporal (τH and τV) or spatial criteria (DMOD and ALIM) were used for TA and RA issuance while in InCAS it seems that a combination of temporal and spatial criteria was used. Nonetheless, it seems that in this respect SDCPN is on the conservative side.

2. Differences in vertical distance in TA are due to different altitude change applied (in SDCPN change is continual while in InCAS is quantization of 100ft). In the SDCPN model, extrapolating the flight path of the aircraft until the moment when in InCAS the RA is issued (168 sec), vertical separation of 40 ft can be obtained which is consistent to the vertical separation at moment when the TA is issued.

3. In both models a pilot delay of 5 sec is applied after RA issuance. However, combining this fact with the fact that the RA is issued with 11 sec difference, it is obvious that vertical separation at RA and CoC moments are different.

- Scenario 3 is also very similar although in SDCPN a TA is issued 2 sec later. Checking the possible reason for difference it was determined that in both cases the same conditions for issuing TA were satisfied (τH and τV were lower than threshold of 48 seconds). This difference also produces the differences in vertical and horizontal separation at TA (9ft lower and 0.24Nm shorter in SDCPN (Table in Appendix 9)). Horizontal separation at CPA is the same (0.04Nm) and corresponding vertical separation is 46 ft higher in the case of SDCPN (Table in Appendix 9);

- In Scenario 4 TA, RA and CoC moments are almost the same which is the case also with separations at TA (45ft higher and 0.01Nm longer in the case of SDCPN (Table in Appendix 9)). It was found that temporal criteria for threat detection were used in both models in the case of TA issuance.

Separations at RA are slightly different (87ft higher and 0.25Nm longer in the case of SDCPN (Table in Appendix 9)) and could be explained by the RA issued 1 second earlier which is possibly caused by different criteria used for RA issuance (in InCAS a combination of temporal and spatial criteria was used) and altitude change. Extrapolating the flight paths 1 sec in advance (at the moment when InCAS was issuing the RA), the achieved vertical separation will be 45 ft greater and horizontal 0.01Nm greater in the case of InCAS, which is consistent with TA case. After an RA is issued both models apply a delay of 5 sec before the aircraft begin to respond to the RA.

Different separations appear in the case of CoC which is mainly caused by the different sense selected for the intruder aircraft, but also by the way of calculating the CoC moment in SDCPN (1 second after CPA).

Sense and strength for own aircraft are the same in both models, but in the case of the intruder aircraft in the InCAS model an RA is not issued (due to complement message of type DON’T CLIMB received during coordination from own aircraft), while in SDCPN it
is. That fact produces the significant differences in vertical separations at CoC and CPA. The possible reason for differences is the coordination process used in SDCPN during which own aircraft sends the complement message which represents the opposite sense for the intruder aircraft. This means that if RA appears then it is immediately coordinated with the other aircraft, so that both aircraft will always receive an RA.

Horizontal separation at CPA is almost the same in both models (0.37Nm in SDCPN vs. 0.36Nm in InCAS (Table in Appendix 9)) while the CPN moments are the same (89 sec after the beginning of the encounter in both models);

- In Scenario 5 SDCPN produces TA and RA moments with 6 and 7 sec delay (Table in Appendix 9) which also causes differences in corresponding vertical and horizontal separations. Searching for reasons of differences it was determined that in this case SDCPN issues the TA according to the criteria that $\tau_H$ and $\tau_V$ are lower than the threshold of 45 seconds in this case.

In the case of InCAS it is not clear which criteria is applied. It seems that a combined $\tau_H < 45$ seconds and $x_{Zik} < 850$ ft (ALIM in this case) is used for issuing the TA (see part of InCAS diagnosis report, given in grey):

00:02:10: Own SAFE 01: Intruder SAFE 02
RANGE_TEST: FAILS
Modified tau (43.1 s) outside alarm limit (30.0 s)
TRAFFIC_RANGE_TEST: RANGE TEST PASSES
Tau (42.6 s) is less than threshold (45.0 s),
TRAFFIC_ALTITUDE_TEST: ALTITUDE TEST PASSES
Absolute value of relative altitude (834 ft) is small (less than 850 ft)

A similar situation occurs with RA issuance. In the case of SDCPN once again the criteria that $\tau_H$ and $\tau_V$ are lower than the threshold of 30 seconds in this case is applied. In InCAS once again it seems that a combination of temporal and spatial criteria is used for RA issuance (see following part of InCAS diagnosis report, given in grey).

00:02:24: Own SAFE 02: Intruder SAFE 01
RANGE_TEST: PASSES
Modified tau (28.7 s) within alarm limit (30.0 s) and tracked range (3.904 NM)
within threat detection limit (12.000 NM) and [range tracker (8) above minimum firmness (3) or detection hit counter (0) is not null]
DETECTION: TRACK_FIRMNESS_TEST CALL
Altitude test passes and RA not yet issued

ALTITUDE_TEST: PASSES
Current vertical separation (600 ft) and predicted vertical miss distance (46 ft)
within alarm threshold $ZTHR$ (600 ft)
ALT_SEPARATOR_TEST: PROCESSING
Processing the altitude separation test

The sense is the same in both modes but the selected strength is lower in the case of SDCPN which could possibly be explained by the different complement message exchanged during coordination. After an RA is issued both models apply a delay of 5 sec before aircraft begins to respond to the RA.

Horizontal separation at CPA is the same in both models (0.07Nm (Table in Appendix 9)), as well as CPA moment (174 sec from the beginning of the encounter) but corresponding vertical separation is significantly different (169ft higher in SDCPN case (Table in Appendix 9)). The reason for the significant difference in vertical separation at CoC and
CPA is the fact that in InCAS a RA modification is created while in SDCPN it is not (which is one of the basic assumptions).

- **Scenario 6**, the differences between models are significant. This scenario is characterised as slow closure encounter in the horizontal plane where usually spatial criteria was used for issuing the TA and the RA. Detailed analysis shows that this was the case with SDCPN both for TA and RA issuance, but not the case with InCAS model where the temporal criteria were applied (see following part of the InCAS diagnosis report related to TA issuance ($\tau_H$ and $\tau_V$), given in grey).

```
00:02:06: Own SAFE 01: Intruder SAFE 02
  RANGE_TEST: PASSES
    Modified tau (32.0 s) within alarm limit (35.0 s) and tracked range (1.460 NM)
    within threat detection limit (12.000 NM) and [range tracker (8) above
    minimum firmness (3) or detection hit counter (0) is not null]
  DETECTION: TRACK_FIRMNESS_TEST CALL
    Altitude test passes and RA not yet issued
  ALTITUDE_TEST: FAILS
    Vertical tau (47.1 s) greater than threshold TVTHR (35.0 s), or predicted
    vertical miss distance (0 ft) greater than alarm threshold ZTHR (700 ft) and
    aircraft will not cross altitudes before closest approach: tauv (74.0 s) > true tau
    (0.0 s)
  TRAFFIC_RANGE_TEST: RANGE TEST PASSES
    Tau (15.3 s) is less than threshold (48.0 s).
  TRAFFIC_ALTITUDE_TEST: ALTITUDE TEST PASSES
    Altitude tau (47.1 s) is less than altitude tau threshold (48.0 s).
```

Differences in threat detection criteria for TA and RA issuance cause differences in horizontal and vertical separation as well as in, corresponding time moments (Table in Appendix 9). Finally, CoC was not issued after conflict resolution in InCAS (due to unknown reason) but in SDCPN it was.

Apart from the mentioned differences, given strengths are not the same. The sense for own aircraft is the same in both models but the strength is much greater in case of InCAS (see inputs for Scenario 6 in Appendix 3 and 4). In the case of SDCPN the least disruptive strength was chosen. In the end, horizontal separation at CPA is the same (0.05Nm), CPA moment is very similar (224 sec from the beginning of the encounter in SDCPN vs. 226 sec in InCAS) but the vertical separation is significantly different (Table in Appendix 9).

- **Scenario 7** presents a slow convergence encounter both in the horizontal and the vertical plane, with TA issued. SDCPN issues the TA 27 seconds later (Table in Appendix 9) and uses DMOD and ALIM as criteria for TA issuance. By analysing the InCAS diagnosis report it was determined that the combination of time and distance criteria was used for TA issuance (see following part of InCAS diagnosis report, given in grey).

```
00:02:13: Own SAFE 02: Intruder SAFE 01
  RANGE_TEST: FAILS
    Modified tau (37.5 s) outside alarm limit (20.0 s)
  TRAFFIC_RANGE_TEST: RANGE TEST PASSES
    Tau (26.0 s) is less than threshold (30.0 s).
  TRAFFIC_ALTITUDE_TEST: ALTITUDE TEST PASSES
    Absolute value of relative altitude (847 ft) is small (less than 850 ft)
```

Horizontal separation at CPA is the same (0.20Nm (Table in Appendix 9)) while corresponding vertical separation is 9ft higher in the case of SDCPN (710ft in SDCPN vs. 701ft in InCAS (Table in Appendix 9)).
• **Scenario 8** is a case of almost a perfect match. TA and RA moments are the same and corresponding separations are slightly greater in the SDCPN case (9ft greater and 0.02Nm greater at TA and 11ft greater and 0.04Nm greater at RA (Table in Appendix 9)). A greater difference exists in the case of CoC moment (due to the fact that in SDCPN is issued 1 second after the CPA and in InCAS is 4 seconds) and corresponding CoC separation values, caused by different strengths selected, while the senses are the same.

A possible reason for the difference in strength values are complement message sent by the own aircraft which in the case of SDCPN are of opposite strength, while in InCAS the complement message says which strength is forbidden and then logic attempts to find the least disruptive strength (see part of InCAS diagnosis file as example).

Apart from this value the altitude values used in SDCPN are slightly different from those in InCAS (see altitude change differences in Table in Appendix 9). Therefore, these are possible causes of the differences in strength. Horizontal separation at CPA is the same in both models (0.68Nm (Table in Appendix 9)), CPA moment is similar (170 sec in SDCPN vs. 171 sec in InCAS) while vertical separation is significantly greater in the case of the SDCPN model (Table in Appendix 9) which is caused mainly by the different RA strengths.

• In **Scenario 9** both models produce very similar results. This is a scenario where only a TA issued. SDCPN issues the TA 1 second later then InCAS, so the corresponding separations are slightly lower than in case of InCAS (18ft smaller and 0.25Nm smaller (Table in Appendix 9)). Horizontal separation at CPA is the same (4.63Nm) and corresponding vertical separation is 50ft lower in the case of SDCPN model (Table in Appendix 9).

Without entering into statistical hypothesis testing, it is noticeable from Table in Appendix 9 that the results of both models are very similar. The differences in some cases are mainly caused by the differences in model characteristics and by the modelling assumptions applied in The SDCPN-based model.

Although SDCPN contains a model of TCAS II Logic, the general impression is that the SDCPN model produces comparable results for the given input, relative to InCAS which contains real TCAS II logic.