Stochastically and Dynamically Coloured Petri Net Model of ACAS Operations

Fedja Netjasov, Andrija Vidosavljevic, Vojin Tosic
Division of Airports and Air Traffic Safety
Faculty of Transport and Traffic Engineering
University of Belgrade, Belgrade, Serbia
{f.netjasov; a.vidosavljevic; v.tosic}@sf.bg.ac.rs

Mariken Everdij, Henk Blom
Air Transport Safety Institute
National Airspace Laboratory NLR
Amsterdam, The Netherlands
{everdij, blom}@nlr.nl

***Abstract* - Current international regulations and policies do not consider the effect of an airborne safety net for 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 standing regulations. In order to close this gap between SESAR and NEXTGEN requirements, and standing regulation, there is need for a systematic development of safety risk analyses of airborne safety nets within the specific ATM context, which may range from current practices to advanced ATM concepts. The aim of the research described in this paper is to make a contribution through the systematic development of an unambiguous model of TCAS II version 7, together with its interactions with pilots and ATC. The specific modelling formalism used for this is Stochastically and Dynamically Coloured Petri Nets (SDCPN). The developed SDCPN model contains the technical, human and procedural elements of ACAS operations. The SDCPN model is demonstrated to work well for a historical en-route mid-air collision event.**

Keywords - ACAS, Petri Nets, Safety Risk Assessment, Safety Critical Systems

I INTRODUCTION

Airborne Collision Avoidance System (ACAS) constitutes a world-wide accepted last-resort means of reducing the risk of mid-air collision (MAC) between aircraft [1]. Key elements of the current ACAS consist of TCAS II version 7 and procedures for pilots using this system. TCAS is intended to provide last-minute collision avoidance guidance directly to the flight crew [2]. Hence, TCAS forms the last layer in the multi-layered defence against MAC, with all other layers typically belonging to ground based ATM. 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.

Current ICAO risk/safety assessment policy is restrictive relative to ACAS in the sense that maximum values for mid-air collision risk 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 [3, 4].

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 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 [5, 6, 7, 8, 9]. These examples clearly show that the only way to include ACAS in the safety assessment process is through the modelling of ACAS operations.

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. Several approaches have emerged for verification i.e. formal analysis of complex safety-critical systems such as TCAS: Finite State Machine approach [10], State Charts [11] and Hybrid Automata [12]. In order to understand human behaviour related to TCAS, Causal analysis [13], and Timed Knowledge-based modelling and analysis [14], are applied. 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 [15], and by Markov processes coupled with Bayesian networks [16, 17]. Apart from the mentioned models, an interactive simulator InCAS was developed [18, 19] 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 [19].

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 benefit of ACAS in risk reduction in current and advanced ATM. 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 [20], and at the same time brings powerful analysis frameworks within reach [21] and is fully embedded in the advanced safety risk assessment methodology TOPAZ [22, 23, 24].

This research has been conducted with support from the RESET project commissioned by European Commission DG TREN under the FP6 Program.

This paper is organized as follows. Section II describes the ACAS operation from the perspectives of the pilot and the air traffic controller (ATCo). Section III provides a description of TCAS II version 7. Next, Section IV explains the development of an ACAS model using the SDCPN formalism. This ACAS model covers TCAS II version 7 as well as the pilots, the controller, some other relevant equipment and the interactions between these model entities. Section V illustrates the behaviour of the new ACAS model in case of a historical MAC. Section VI draws conclusions.

II Description of ACAS Operation

Since January 2005, ICAO mandates the use of ACAS worldwide for all aircraft with more than 19 passenger seats or with a maximum take-off weight exceeding 5,700 kg. TCAS II Version 7 is the only TCAS version that complies with ICAO Standards and Recommended Practices (SARPs) for ACAS [1, 2, 11, 25]. TCAS is designed to work autonomously, i.e. without support of the aircraft navigation equipment, and independently of the ground systems used to provide Air Traffic Control (ATC) Services [25]. Generally, TCAS monitors the airspace around the *own* aircraft and warns pilots of the presence of other aircraft, so called *intruders*, which may present a MAC *threat*. A crucial part of TCAS is a Collision Avoidance Logic, the main functions of which are [25]: tracking, traffic advisory, threat detection, resolution advisory, TCAS/TCAS coordination, advisory annunciation and performance monitoring. In order to model an ACAS operation in this research, the operation is divided into the following phases [1, 11, 25]:

A. Normal flight

In nominal situations, i.e. during normal evolution of a flight, the aircraft crew receives instructions and clearances from the Air Traffic Controller (ATCo) and is flying according to them (manually or using the autopilot). Separation assurance is the responsibility of the ATCo. TCAS is constantly surveying the surrounding airspace, by broadcasting the interrogations and receiving replays from near-by aircraft.

B. Appearance of Traffic Alert (TA)

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

C. Appearance of Resolution Advisory (RA)

If the previous situation deteriorates, and a collision is predicted to occur within 15 to 35 seconds (depending on the altitude), an RA is issued. The previously mentioned “intruder” aircraft now becomes a “threat”. The RA includes an aural annunciation in the cockpit, being “Climb, Climb” or “Descend, Descend” (depending on the situation). An icon representing the threat aircraft on the CDTI changes its shape and colour and becomes a solid red square. In addition, the icon shows the appropriate vertical rate, which should be flown in order to resolve a conflict situation. A pilot receiving an RA should disengage the autopilot and manually control the aircraft to achieve the recommended vertical rate.

If 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 the safe operation of the flight. By not responding to an RA, the flight crew takes responsibility for achieving safe separation. Even if an RA manoeuvre is inconsistent with the current ATC clearance, pilots are obligated to respond appropriately to the RA. Pilots are also required to report an RA occurrence, i.e. that they are responding to the RA, to the ATCo when appropriate, and to inform the ATCo of 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. If an 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.

D. Return to normal flight

When the RA is cleared, the flight crew get the aural annunciation “Clear of Conflict” (CoC). After that they should advise the ATCo that they are returning to their previously assigned clearance or should acknowledge any amended clearance issued, using the defined phraseology. After that, the pilot may engage the autopilot again. The ATCo resumes responsibility for standard separation if one of the following conditions is met: a) the responding aircraft has returned to its assigned altitude, the flight crew informs the ATCo that the collision avoidance manoeuvre has been completed and that standard separation has been re-established; or b) that the responding aircraft has executed an alternate clearance and that standard separation has been re-established.

III Conceptual Model of TCAS II Version 7

As a prerequisite for developing an SDCPN model of the ACAS operation, first a conceptual model of TCAS II version 7 is developed. The development of this conceptual model is largely based on [25]. The resulting conceptual model contains models of all algorithms used for threat detection and threat resolution, and would make it possible to conduct a simulation of any encounter scenario.

A. Threat detection algorithms

In order to determine whether a collision threat exists, i.e. to issue a TA or an RA, both the range and vertical criteria must be satisfied; i.e. if one of them is not satisfied, TCAS will not issue a TA or an RA. For checking whether the range and vertical criteria are satisfied, Range tests and Altitude tests are constantly performed during an encounter. Criteria used for making a decision about TA and RA issuance depend on the Sensitivity Level (SL) (Table 1).

Table 1. Sensitivity level and threshold values [25]

Own altitude (feet)	SL	τ (seconds)		DMOD (Nm)		ALIM (feet)	
		TA	RA	TA	RA	TA	RA
<1000	2	20	N/A*	0.30	N/A	850	N/A
(1000-2350]	3	25	15	0.33	0.20	850	300
(2350-5000]	4	30	20	0.48	0.35	850	300
(5000-10000]	5	40	25	0.75	0.55	850	350
(10000-20000]	6	45	30	1.00	0.80	850	400
(20000-42000]	7	48	35	1.30	1.10	850	600
> 42000	7	48	35	1.30	1.10	1200	700

* NA – not available

The Sensitivity Level (SL) depends of the aircraft altitude range. SL contains values for horizontal and vertical τ thresholds in 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 τ threshold values are not appropriate. During an encounter, if the horizontal or vertical τ is lower than the TA threshold or if the horizontal and vertical miss distance is lower than the TA DMOD and TA ALIM respectively, then a TA is annunciated. If the situation further worsens and τ values are lower than the RA threshold or if the miss distances are lower than the RA DMOD and RA ALIM respectively, then an RA is annunciated [25].

For the purpose of range and altitude tests, aircraft are identified in a Cartesian coordinate system (Figure 1). 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 1, and z stands for the altitude. Let θ^i_t represent an orientation velocity vector v^i_t in the horizontal plane (measured from the x axis in counter-clockwise direction, where $0 \le \theta^i_t \le 2\pi$) and let ψ^i_t represent the orientation of velocity vector v^i_t in the vertical plane (measured from the horizontal plane up as positive and down as negative, where $-\pi/2 \le \psi^i_t \le \pi/2$).

$$x^i_t = \begin{bmatrix} x^i_{x,t} \\ x^i_{y,t} \\ x^i_{z,t} \end{bmatrix} \tag{1}$$

$$v^i_t = \frac{dx^i_t}{dt} = \begin{bmatrix} v^i_{x,t} \\ v^i_{y,t} \\ v^i_{z,t} \end{bmatrix} = \begin{bmatrix} v^i_t \cos\psi^i_t \cos\theta^i_t \\ v^i_t \cos\psi^i_t \sin\theta^i_t \\ v^i_t \sin\psi^i_t \end{bmatrix} \tag{2}$$

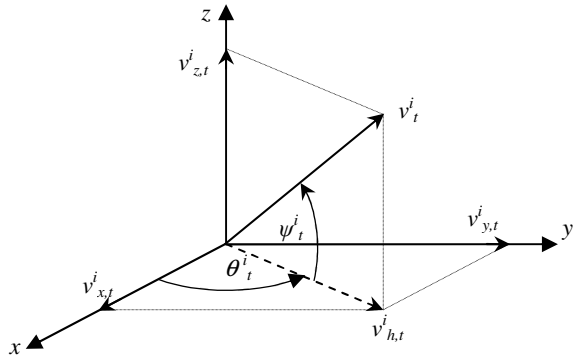

Figure 1. Velocity vector in Cartesian coordinate system

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 (closing speed) between the aircraft at time t.

1) Range test:

At each moment t, both the distance and the relative velocity between own and intruder aircraft in the horizontal plane are calculated. Knowledge about both values is required in order to calculate the "time to closest point of approach" (in horizontal direction, i.e. the range τ).

Let $x^i_{h,t} = (x^i_{x,t}, x^i_{y,t})^T$ and $v^i_{h,t} = (v^i_{x,t}, v^i_{y,t})^T$ be the position and the velocity of aircraft i in the horizontal plane (respectively), and similarly for aircraft k. Let $x^{ik}_{h,t} = x^i_{h,t} - x^k_{h,t}$ and $v^{ik}_{h,t} = v^i_{h,t} - v^k_{h,t}$ be the horizontal distance and the relative velocity in the horizontal plane (respectively) between aircraft i and k at time t.

Define $\tau^{ik}_{h,t}$ as the time to closest point of approach (CPA) in the horizontal plane between aircraft i and k at time t, which is given by the following expression:

$$\tau^{ik}_{h,t} = \frac{-\left|x^{ik}_{h,t}\right|}{\left|v^{ik}_{h,t}\right| \cdot \cos(\delta^{ik}_t - \varphi^{ik}_t)} \tag{3}$$

where δ^{ik}_t is the bearing of the velocity difference vector satisfying

$$\delta^{ik}_t = \arctan\left(\frac{v^{ik}_{x,t}}{v^{ik}_{y,t}}\right) \tag{4}$$

and φ^{ik}_t is the bearing of the position difference vector satisfying

$$\varphi^{ik}_t = \arctan\left(\frac{x^{ik}_{x,t}}{x^{ik}_{y,t}}\right) \tag{5}$$

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

$$\left(\delta^{ik}_t - \varphi^{ik}_t \neq \pi/2\right) \wedge \left(\delta^{ik}_t - \varphi^{ik}_t \neq -\pi/2\right) \wedge \left(\left|v^{ik}_{h,t}\right| \neq 0\right) \tag{6}$$

2) Altitude test:

At each moment t, both the vertical distance (separation) and the combined speed (vertical closing speed) between own and intruder aircraft are calculated. Knowledge about both values is required in order to calculate the "time to closest point of approach" (vertical τ). Let $x^{ik}_{z,t} = x^i_{z,t} - x^k_{z,t}$ and $v^{ik}_{z,t} = v^i_{z,t} - v^k_{z,t}$ be the vertical distance and the relative velocity in the vertical plane (respectively) between aircraft i and k at time t.

Define $\tau^{ik}_{z,t}$ as the time to closest point of approach (CPA) in the vertical plane between aircraft i and k at time t, which is given by the following expression:

$$\tau^{ik}_{z,t} = -\left(x^{ik}_{z,t} / v^{ik}_{z,t}\right) \tag{7}$$

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

3) TA or RA issuance

The Range and Altitude tests compare given criteria (see Table 1) 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 is satisfied:

$$\left(0 < \tau^{ik}_{h,t} < \tau\right) \wedge \left(0 < \tau^{ik}_{z,t} < \tau\right) \tag{8}$$

or

$$\left(\left|x^{ik}_{h,t}\right| < DMOD\right) \wedge \left(\left|x^{ik}_{z,t}\right| < ALIM\right) \tag{9}$$

alerts shall be issued (TA or RA depending on the τ, *DMOD* and *ALIM* criteria given in Table 1).

B. 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 an appropriate sense is selected (upward or downward); that is, whether the aircraft needs to climb or to descend. In the second step an appropriate strength (vertical speed) is determined; that is, how rapidly the aircraft needs to change its altitude.

1) Sense selection

Let t be the moment at which an RA for own aircraft i is issued, i.e. τ_{RA} seconds remain until CPA with intruder aircraft k. The TCAS Logic makes trials with upward and downward sense for own aircraft, in order to determine which sense provides the most vertical separation at CPA (time moment $t+\tau_{RA}$ in Figure 2) under the assumption that intruder aircraft doesn't change its flight profile. The sense which provides the greatest vertical separation shall be selected.

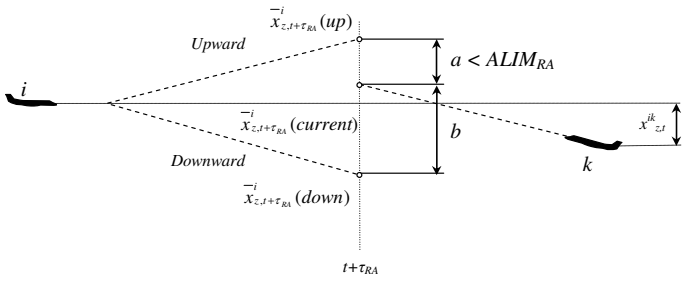

Figure 2. RA sense selection (illustrative example)

Consider a possible vertical position of aircraft i at moment $t+\tau_{RA}$ during the trial (see Figure 2):

- if the upward sense is selected

$$\bar{x}^{i}_{z,t+\tau_{RA}}(up) = x^{i}_{z,t} + (v^{i}_{z,t} + \Delta^{i}_{z,t}) \cdot \tau_{RA} \tag{10}$$

- if the current rate is maintained

$$\bar{x}^{i}_{z,t+\tau_{RA}}(current) = x^{i}_{z,t} + v^{i}_{z,t} \cdot \tau_{RA} \tag{11}$$

- if the downward sense is selected

$$\bar{x}^{i}_{z,t+\tau_{RA}}(down) = x^{i}_{z,t} + (v^{i}_{z,t} - \Delta^{i}_{z,t}) \cdot \tau_{RA} \tag{12}$$

where $\Delta^{i}_{z,t}$ has a fixed value of 1500 feet/min [2, 11].

Two vertical separations at CPA between own aircraft i and intruder k, are recognized in the sense selection process and are given by the following expressions (see Figure 2):

$$a \equiv \left|\bar{x}^{i}_{z,t+\tau_{RA}}(up) - \bar{x}^{k}_{z,t+\tau_{RA}}(current)\right| \tag{13}$$

$$b \equiv \left|\bar{x}^{i}_{z,t+\tau_{RA}}(down) - \bar{x}^{k}_{z,t+\tau_{RA}}(current)\right| \tag{14}$$

The sense is represented by the binary variable c^{i}_{t} which takes the following values: $c^{i}_{t} = 1$ in case of the upward sense selected, $c^{i}_{t} = -1$ in case of downward sense and $c^{i}_{t} = 0$ otherwise. In case aircraft i already receives a sense from aircraft k before it has finished its own sense calculations then $c^{i}_{t} = -c^{k}_{t}$, otherwise:

$$c^{i}_{t} = \begin{cases} -1, & if \begin{cases} (b > a) \vee \\ (b \le a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}] \; such\ that\ \bar{x}^{ij}_{z,t+\varepsilon} = 0\right) \vee \\ (b > a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}] \; such\ that\ \bar{x}^{ij}_{z,t+\varepsilon} = 0\right) \wedge (a > ALIM_{RA}) \end{cases} \\ 1, & if \begin{cases} (b \le a) \vee \\ (b > a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}] \; such\ that\ \bar{x}^{ij}_{z,t+\varepsilon} = 0\right) \vee \\ (b \le a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}] \; such\ that\ \bar{x}^{ij}_{z,t+\varepsilon} = 0\right) \wedge (b > ALIM_{RA}) \end{cases} \\ 0, & otherwise \end{cases} \tag{15}$$

The obtained sense for the own aircraft i is coordinated through the Mode S data link with intruder aircraft k with the aim to avoid that both aircraft select the same vertical sense. So, the RA sense sent to the intruder aircraft is represented by the calculated c^{i}_{t}.

2) Strength selection

Once the sense has been selected, TCAS Logic will determine the RA strength. The 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 $t+\tau_{RA}$), under the assumption that intruder aircraft doesn't change the flight profile. That means that the change of vertical speed $\Delta^{i*}_{z,t}$ should be minimal. The determination of the appropriate strength (vertical speed) should satisfy the following condition:

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

$$v^{i*}_{z,t} = \begin{cases} v^{i}_{z,t} + \Delta^{i*}_{z,t}; & c^{i}_{t} = 1 \\ v^{i}_{z,t} - \Delta^{i*}_{z,t}; & c^{i}_{t} = -1 \end{cases} \tag{16}$$

where:

$$\Delta^{i*}_{z,t} = \left[ALIM_{RA} + \left(x^{k}_{z,t} + v^{k}_{z,t} \cdot \tau_{RA}\right) - \left(x^{i}_{z,t} + v^{i}_{z,t} \cdot \tau_{RA}\right)\right] / \tau_{RA} \tag{17}$$

3) Clear of Conflict annunciation

The following conditions should be satisfied in order to announce CoC and terminate the encounter: a) RAs may terminate for a number of reasons: normally, when the conflict has been resolved and the threat is diverging in range [1, 11]; b) A CoC occurs after an encounter has been resolved [11].

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

$$\left|x^{ik}_{h,t'}\right| > \left|x^{ik}_{h,t_{CPA}}\right| \quad (18)$$

then "Clear of Conflict" will be annunciated and the TCAS encounter is terminated.

IV DEVELOPMENT OF THE NEW ACAS MODEL USING SDCPN FORMALISM

In this research, ACAS operations are modelled using the Stochastically and Dynamically Coloured Petri Net (SDCPN) formalism. The main reason for using SDCPN is the possibility of modelling complex relations existing between different system elements (humans, procedures, equipment) as well as the possibility to easily determining the causes or contributing factors of non-nominal system behaviour or accidents.

Previous experiences using Petri Nets for safety analysis [26] as well as Dynamically Coloured Petri Net (DCPN) for aviation purposes [27, 28, 29] also support this choice. Once a proper ACAS model in terms of SDCPN formalism is developed, this can easily be incorporated in the modelling of an advanced ATM operation that also uses the SDCPN formalism. This way, a new ACAS model contains modules that can easily be added to some previously or future developed SDCPN modules related to current or advanced operational concepts. However, in this paper a new ACAS model is developed using SDCPN modules that work together as a standalone system.

A. Hazard identification

An important step in the TOPAZ methodology is a Hazard Identification. Once the operational concept has been sufficiently described, the hazards are identified. This is done in two steps [28]:

a) Identification of entities (agents) and their functional relationships. The agents may be humans (pilots, air traffic controllers), technical systems (e.g. navigation equipment or cockpit display, etc.), or even more abstract entities (e.g. aircraft evolution); and

b) Identification of hazards, both functional and non-functional. Hazards are best identified using dedicated brainstorm sessions with a number of participants bringing complementary expertise [28].

Because hazards could be taken from literature [2, 25] in this research no brainstorm sessions have been conducted.

B. Specification of Local Petri Nets

The SDCPN modules for the new ACAS model are developed at two hierarchical levels. The first level distinguishes the agents and the operation, where an agent is an entity that has situation awareness components. 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.

A Stochastically and Dynamically Coloured Petri Net is, according to [20, 22, 23, 24] given by the following tuple:

$$SDCPN = (P, T, A, N, S, C, V, G, D, F, I)$$

where :

P - is a set of places; T - is a set of transitions; A - is a set of arcs; N - is a node function, which maps each arc to an ordered pair of one transition and one place; 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- is a set of place-specific colour functions, which describe what happens to the colour of a token while it resides in its place; G - is a set of Boolean-valued transition guards; D - is a set of transition delays; F - is a set of (probabilistic) firing functions describing the quantity and colours of the tokens produced by the transitions at their firing; I - is an initial marking, which defines the set of tokens initially present, i.e. it specifies in which places they initially reside, and the colours they initially have.

The specification of an LPN implies determination of each element of the tuple for this LPN.

C. Agents and Local Petri Nets for ACAS operation

Each agent is represented by the multiple Local Petri Nets (LPN) mutually connected forming the SDCPN. Connections between LPNs are realised using the Compositional Specification principles presented in [20]. Five agents are recognized for the ACAS operation. They and their corresponding LPNs are given in Table 2. Interactions between agents and their corresponding LPNs are represented in Figure 3.

Table 2. Agents vs. LPN's for TCAS II Version 7operation

Agent	LPN
Own Aircraft	
	Own aircraft state
	Own aircraft Mode S Link
	TCAS Processor
	TCAS Processor Working Mode
	CDTI Display
	CDTI Display Working Mode
	Aural Annunciation
	Aural Annunciation Working Mode
Own Aircraft Crew	
	Crew
Intruder Aircraft	
	Intruder aircraft state
	Intruder aircraft Mode S Link
Air/ground Communication Link	
	Air/ground Communication Link
Tactical Air Traffic Controller (ATCo)	
	ATCo

1) Own Aircraft as Agent

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

2) Intruder Aircraft as Agent

This agent (Figure 5) 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.

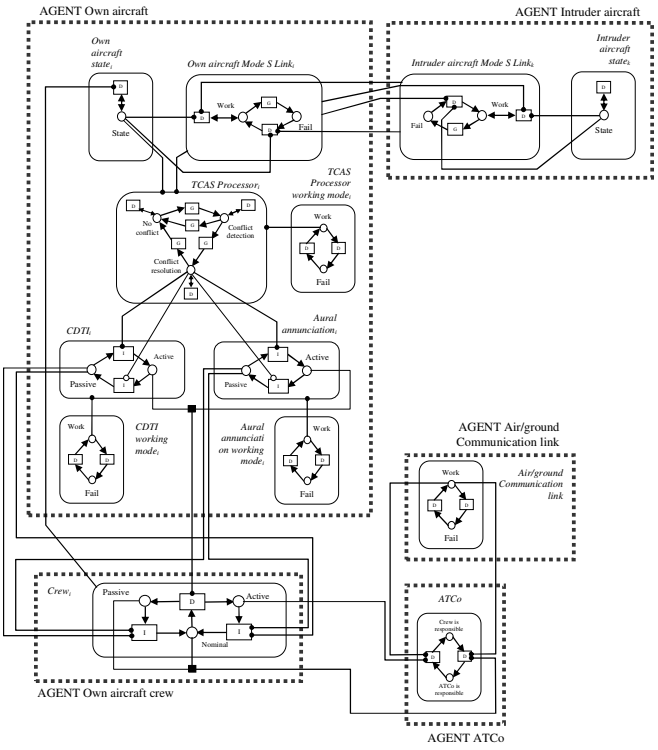

Figure 3. Interaction between agents and their corresponding LPNs for the ACAS operations

3) Own Aircraft Crew as Agent

This agent (Figure 6) 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.

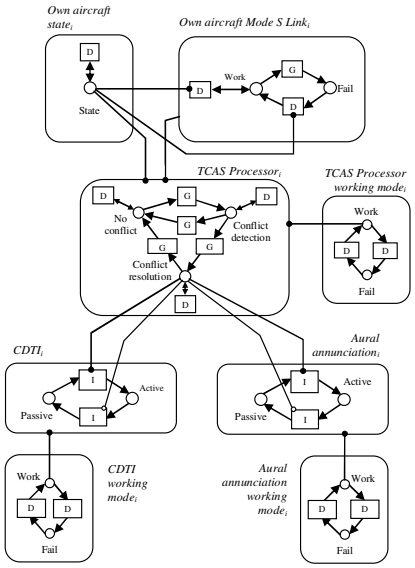

Figure 4. LPN contained in Agent Own Aircraft and their mutual relationship

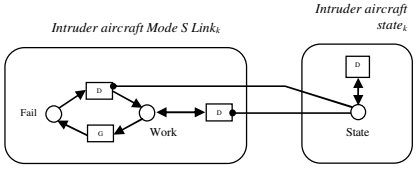

Figure 5. LPN contained in Agent Intruder Aircraft and their mutual relationship

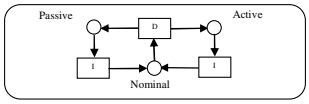

Figure 6. Agent Own Aircraft Crew

4) Air/Ground Communication Link as Agent

This agent (Figure 7) contains one LPN which represents a technical part of the system. This LPN presents working modes of the air/ground communication system.

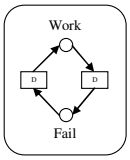

Figure 7. Agent Air/Ground Communication Link

5) Tactical Air Traffic Controller (ATCo) as Agent

This agent (Figure 8) is represented by only one LPN representing a human part of the system: LPN *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.

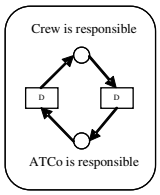

Figure 8. Agent Tactical Air Traffic Controller (ATCo)

The procedures part of the TCAS II system is represented by enabling arcs between Agent Crew and Agent ATCo (Figure 3). Therefore, whenever LPN $Crew_i$ is in "Active" state, LPN *ATCo* switches to state "Crew is responsible"; LPN *ATCo* returns to state "ATCo is responsible" when an LPN $Crew_i$ is in "Passive" or "Nominal" state (of course under condition that LPN *Air/Ground Communication Link* is in "Work" state).

V 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 [30, 31]. TCAS was not in use at the time of collision. Figure 9 provides a schematic representation of the collision location as well as flight paths of both aircraft during the few minutes before the collision [30, 31].

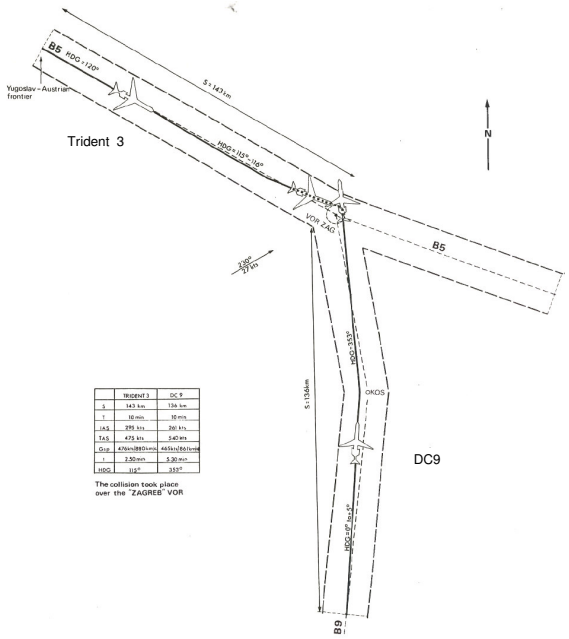

Figure 9. Schematic representation of the collision location and flight paths before collision (taken from [30])

According to the detailed vertical and horizontal situation in the last 32 seconds before collision [31] an encounter is reconstructed and input data for the simulation of the ACAS SDCPN are prepared (Table 3). Results of the ACAS SDCPN simulation are provided in Figures 10 and 11. 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.

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

Table 3. Encounter geometry (input)

	Own aircraft (DC9 - climbing)	Intruder aircraft (Trident 3 - cruising)
X coordinate	19.69 Nm	3.56 Nm
Y coordinate	4.54 Nm	26.78 Nm
Height	29620 ft	32960 ft
Magnetic Heading	353^0	115.5^0
Ground Speed	465 kt	476 kt
Vertical Speed	1670 fpm	0 fpm

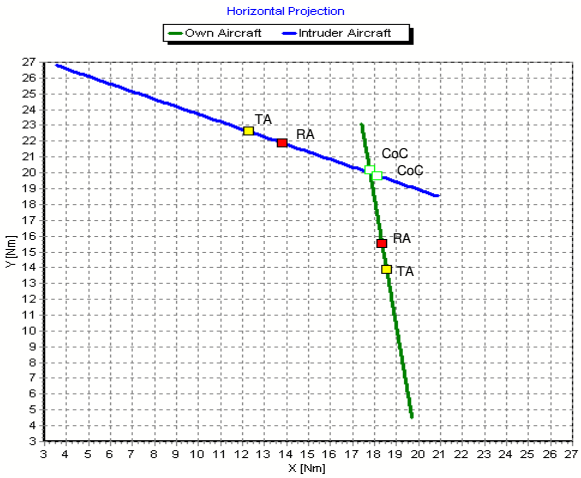

Figure 10. Horizontal situation of simulated encounter (Note: headings are not to scale)

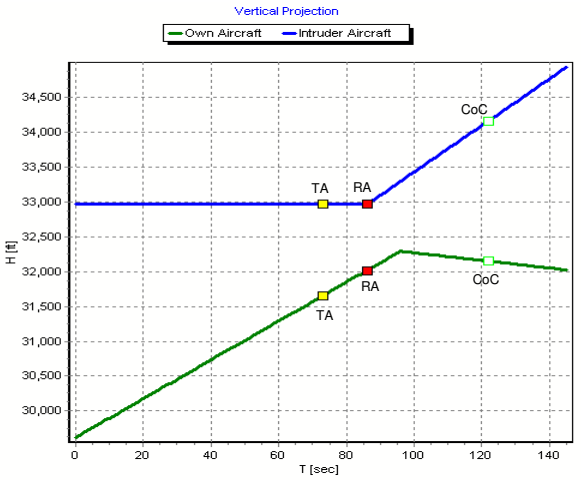

Figure 11. Vertical situation of simulated encounter (Note: rates of climb/descent are not to scale)

VI Conclusion

This paper presented the development of a mathematical model of ACAS operations using the SDCPN formalism. The motivation for the development of this ACAS SDCPN model is to use it in follow-up research for the safety analysis of current and advanced ATM concepts including ACAS. 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, ATCos, procedures in force), as

well as interactions between them in a flexible and modular way. An illustrative example was shown presenting the possibilities of the developed model. A further step before application in risk/safety assessment is validation of the developed SDCPN based ACAS model.

REFERENCES

[1] International Civil Aviation Organization, "Annex 10 – Volume 4", Canada, 2002.

[2] J. Kuchar, A. Drumm, "The Traffic Alert and Collision Avoidance System", Lincoln Laboratory Journal, Vol. 16, No. 2, 2007, pp. 277-296.

[3] P. Brooker, "Why the Eurocontrol Safety Regulation Commission Policy on Safety Nets and Risk Assessment is Wrong", The Journal of Navigation, Vol. 57, No. 2, 2004, pp. 231-243.

[4] P. Brooker, "Airborne Collision Avoidance Systems and Air Traffic Management Safety", The Journal of Navigation, Vol. 58, No. 1, 2005, pp. 1-16.

[5] A. Abeloos, M. Mulder, R. van Paassen, E. Hoffman, "Potential co-operation between the TCAS and the ASAS", Proceedings of International Conference on Human-Computer Interaction in Aeronautics, France, 2000.

[6] D. Ivanescu, D. Powell, C. Shaw, E. Hoffman, K. Zeghal, "Effect of aircraft self-merging in sequence on an airborne collision avoidance system", Proceedings of AIAA Guidance, Navigation and Control Conference and Exhibit, USA, 2004.

[7] I. de Oliveira, P. Cugnasca, H. Blom, B. Bakker, "Modelling and Estimation of Separation Criteria for Airborne Time-Based Spacing Operation", Proceedings of 7th USA/Europe Air Traffic Management R&D Seminar, Spain, 2007.

[8] H. Blom, B. Klein Obbink, B. Bakker, "Safety Risk Simulation of an airborne self separation concept of operation", Proceedings of 7th AIAA-ATIO Conference, Northern Ireland, 2007.

[9] H. Blom, B. Klein Obbink, B. Bakker, "Simulated collision risk of an uncoordinated airborne self separation concept of operation", Proceedings of 7th Eurocontrol Innovative Research Workshop, France, 2008.

[10] N. Leveson, M. Heimdahl, H. Hildreth, J. Reese, "Requirements Specification for Process-Control Systems", IEEE Transactions on Software Engineering, Vol. 20. No. 9, 1994, pp. 684-707.

[11] Radio Technical Commission for Aeronautics, "Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment – Volume I" (RTCA/DO-185A), USA, 1997.

[12] C. Livadas, J. Lygeros, N. Lynch, "High-Level modeling and analysis of TCAS", Proceedings of 20th IEEE Real-Time Systems Symposium, USA, 1999.

[13] P. Ladkin, "Causal Analysis of the ACAS/TCAS Sociotechnical System", Proceedings of the 9th Australian Workshop on Safety Related Programmable Systems (SCS'04), Australia, 2004.

[14] J. Küster-Filipe, M. Felici, S. Anderson, "Timed Knowledge-based Modelling and Analysis: On the Dependability of Socio-technical Systems", Proceedings of the 8th International Conference on Human Aspects of Advanced Manufacturing: Agility and Hybrid Automation, Italy, 2003.

[15] J. Kuchar, "Safety Analysis Methodology for Unmanned Aerial Vehicle (UAV) Collision Avoidance Systems", Proceedings of 6th USA/Europe Air Traffic Management Research and Development Seminar, USA, 2005.

[16] M. Kochenderfer, L. Espindle, J. Kuchar, J. Griffith, "A Comprehensive Aircraft Encounter Model of the National Airspace System", Lincoln Laboratory Journal, Volume 17, Number 2, 2008, pp. 41-53.

[17] M. Kochenderfer, L. Espindle, M. Edwards, J. Kuchar, J. Griffith, "Airspace Encounter Models for Conventional and Unconventional Aircraft", Proceedings of 8th USA/Europe Air Traffic Management Research and Development Seminar, USA, 2009.

[18] EUROCONTROL Experimental Centre, "InCAS 2.6 – User Guide", France, 2005.

[19] Global Aviation Information Network (GAIN), "Guide to Methods and Tools for Safety Analysis in Air Traffic Management", USA, 2003.

[20] M. Everdij, M. Klompstra, H. Blom, B. Klein Obbink, "Compositional Specification of a Multi-Agent System by Stochastically and Dynamically Coloured Petri Nets", in Lecture Notes in Control and Information Sciences, 337: "Stochastic Hybrid Systems: Theory and Safety Critical Application" (editors: H. Blom, J. Lygeros), Springer, 2006, pp. 325 – 350.

[21] M. Everdij, H. Blom, "Enhancing Hybrid State Petri Nets with the Analysis Power of Stochastic Hybrid Processes", Proceedings of the 9th International Workshop on Discrete Event Systems, Sweden, 2008, pp. 400-405.

[22] M. Everdij, H. Blom, "Petri Nets and Hybrid State Markov Processes in a Power-Hierarchy of Dependability Models", Proceedings of IFAC Conference on Analysis and Design of Hybrid System, France, 2003, pp. 355-360.

[23] M. Everdij, H. Blom, "Modelling Hybrid State Markov Processes Through Dynamically and Stochastically And Dynamically Coloured Petri Nets", Hybridge Project, deliverable D2.4, 2005, (http://www2.nlr.nl/public/hostedsites/hybridge/documents/D2.4_Hybridge-version07.pdf)

[24] M. Everdij, H. Blom, "Piecewise deterministic Markov processes represented by dynamically coloured Petri nets", Stochastics: An International Journal of Probability and Stochastic Processes, Vol. 77, No. 1, 2005, pp. 1-29.

[25] Department of Transportation, Federal Aviation Administration, "Introduction to TCAS II Version 7", USA, 2000.

[26] N. Leveson, J. Stolzy, "Safety Analysis Using Petri Nets", IEEE Transactions on Software Engineering, Vol. SE-13, No. 3, 1987, pp 386-397.

[27] J. Shortle, Y. Xie, C. Chen, G. Donohue, "Simulating Collision Probabilities of Landing Airplanes at Non-towered Airports", Simulation, Vol. 80, Issue 1, 2004, pp. 21-31.

[28] M. Everdij, H. Blom, B. Bakker, "Modelling Lateral Spacing and Separation for Airborne Separation Assurance Using Petri Nets", Simulation, Vol. 83; Issue 5, 2007, pp. 401-414.

[29] F. Netjasov, M. Janic, "A Review of Research on Risk and Safety Modelling in Civil Aviation", Journal of Air Transport Management, Vol. 14, Issue 4, 2008, pp. 213-220.

[30] Department of Trade, Accident Investigation Branch, "Aircraft accident report 5/77, Report on the collision in the Zagreb Area, Yugoslavia, on 10 September 1976", UK, 1977.

[31] Department of Trade, Accident Investigation Branch, "Aircraft accident report 9/82, Report on the collision in the Zagreb Area, Yugoslavia, on 10 September 1976", UK, 1982.

AUTHORS BIOGRAPHY

Fedja Netjasov (BS'99–MS'03) is a Teaching and Research Assistant at the Division of Airports and Air Traffic Safety, Faculty of Traffic and Transport Engineering, University of Belgrade where he received all degrees in the field of Air Transportation. He is currently finalizing his PhD thesis in the field of air traffic safety.

Andrija Vidosavljevic (BS'07) is a PhD student at the Division of Airports and Air Traffic Safety, Faculty of Traffic and Transport Engineering, University of Belgrade where he received BS degree in the field of Air Transportation.

Vojin Tosic (BS'69–MS'72–PhD'75) is a Professor and Head of the Division of Airports and Air Traffic Safety, Faculty of Traffic and Transport Engineering, University of Belgrade. He received BS degree from the same University, and MS and PhD from the University of California at Berkeley. He received BS and PhD degree in the field of Air Transportation. He is a member of the TRB Airfield and Airspace Capacity Committee and SESARJU Scientific Committee.

Mariken Everdij (MS'92–MS'94) is Senior Scientist at the Air Transport Safety Institute, National Aerospace Laboratory NLR, Amsterdam, the Netherlands. She received the first MS degree in Applied Mathematics from Twente University and the second MS degree in Industrial Mathematics from Eindhoven University of Technology. She is currently finalizing her PhD thesis on SDCPN and their associated stochastic processes.

Henk Blom (MS'78–PhD'90) is Principal Scientist at the National Aerospace Laboratory NLR, Air Transport Safety Institute, Amsterdam, the Netherlands. He received the MS degree in Electrical Engineering from Twente University, and PhD from Delft University of Technology in the field of Stochastic Control. He is an IEEE Fellow.