# Systematic Validation of a Mathematical Model of ACAS Operations for Safety Assessment Purposes

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

Henk Blom
National Airspace Laboratory NLR,
Air Transport Safety Institute, Amsterdam, and
TU Delft, Faculty of Aerospace Engineering, Delft,
The Netherlands
blom@nlr.nl

*Abstract*— **Current international regulations and policies do not consider the effect of airborne safety nets 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 standing regulations. In order to close this gap, there is a need for systematic development of safety risk analyses of airborne safety nets within an Air Traffic Management context. The aim of the research described in this paper is to address the systematic validation of an unambiguous mathematical model of Airborne Collision Avoidance System (ACAS) operations, together with its interactions with own and other pilots and with air traffic controllers. The specific modelling formalism used for this is Stochastically and Dynamically Coloured Petri Nets (SDCPN); which supports both mathematical analysis as well as Monte Carlo simulation. In order to build confidence, the focus of this paper is on the performance of a systematic validation of the developed model. This validation includes both comparisons against "real data" and comparison with the results of Eurocontrol's ACAS simulation model. Initial application of this validation process to the novel model shows that it is at least as good as the existing ACAS simulation model. However, the added value is that the novel model defines both an unambiguous mathematical model as well as an unambiguous simulation model.**

***Keywords- ACAS, Petri Nets, Safety Risk Assessment, Safety Critical Systems, Model Validation***

## 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 Traffic Alert and Collision Avoidance System (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 Air Traffic Management (ATM). Although recent accidents [3, 4] 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 [5, 6]. Unfortunately, this may imply that ACAS improvements by SESAR/NextGen are not properly valued, as a result of which regulaton may pose overly conservative safety requirements upon the non-ACAS part of ATM.

In view of the SESAR and NextGEN objectives of increasing both capacity and safety there simply is a need to conduct safety risk analysis of new operations, including ACAS behaviour. 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 [7, 8, 9, 10, 11]. 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 [12], State Charts [13; 14] and Hybrid Automata [15]. In order to understand human behaviour related to TCAS, Causal analysis [16], and Timed Knowledge-based modelling and analysis [17], are applied. The necessity to examine ACAS safety is followed by development of encounter models based on Fault Tree Analysis coupled with the Monte Carlo Simulation [18, 19, 20], by Markov processes coupled with Bayesian networks [21, 22] and Bayesian belief networks alone [23]. Finally, a range of encounter models is developed and applied with aim to study TCAS performances and evaluate a new TCAS logics or proposed changes of TCAS logic in use [24, 25, 26, 27, 28, 29, 30]. Complementary to these mathematical models, an interactive simulator InCAS was also developed [31, 32] 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 [31].

Recently [33, 34] have developed another model of ACAS using a Petri net formalism that is named Stochastically and Dynamically Coloured Petri Nets (SDCPN). This SDCPN-based ACAS model covers TCAS II version 7 as well as the pilots, the air traffic controllers, some other relevant equipment and the interactions between these model entities. The main reason for using the SDCPN is the possibility of modelling complex relations existing between different system elements (humans, procedures, equipment) in a systematic and compositional way [35]. This also allows for new ACAS models, for some previously or future developed SDCPN modules related to current or advanced operational concepts, to be added. This is confirmed by previous experiences using Petri Nets for safety analysis [36], as well as Dynamically Coloured Petri Net (DCPN) for aviation purposes [37, 38, 39]. Moreover, the SDCPN formalism brings both Monte Carlo simulation approach as well as powerful analysis frameworks within reach [40], and it is fully embedded in the advanced safety risk assessment methodology TOPAZ [41, 42, 43].

Hence, the SDCPN-based ACAS model from [33] has a significant advantage over other ACAS models when it comes to mathematical analysis and flexibility to integrate the model with other elements of an ATM operation. But what happens to the validity of the SDCPN-based ACAS model? A well-known fear is that a model with mathematical and flexibility advantages easily leads to a model that cannot be validated. The aim of the current paper is to investigate this validation aspect of the SDCPN-based ACAS model.

In order to accomplish this, we developed a systematic validation process based on the model validation principles that have been developed by [44, 45]. Their validation principles are based on viewing model validation as a "*substantiation that a model within its domain of applicability possesses a satisfactory range of accuracy consistent with the intended application of the model*". In [34] these principles have been used for the development of a systematic validation approach of the SDCPN-based ACAS model. Subsequently [34] has applied the developed validation approach to the model in [33]. The findings of [34] were twofold: the developed validation approach worked well, and at the same time the outcomes revealed that there were some issues that could be improved in the conceptual ACAS model of [33] only.

The aim of the current paper is threefold:

- To outline the improved conceptual ACAS model, including an explanation of the changes relative to [33];
- To develop a systematic validation process according to the principles of [44, 45], using both real life encounter data and Eurocontrol's ACAS simulation model;
- To initially apply this validation process to the newly-developed ACAS model.

This paper is organized as follows. Section II provides a detailed description of the ACAS conceptual model, including an explanation of the improvements made over the conceptual model in [33]. Sections III develop the systematic validation approach. Section IV presents the initial validation results obtained for the novel ACAS model. Section V draws conclusions.

## II. ACAS CONCEPTUAL MODEL

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, 13, 46].

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 [46]. 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 [46]: 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, 13, 46]: Normal flight, Appearance of Traffic Alert (TA), Appearance of Resolution Advisory (RA) and Return to normal flight. Details about each phase are given in [33, 34].

The ACAS conceptual model is based on [1] and [46] documents, and specifies mathematical models of all algorithms used for threat detection and threat resolution.

### 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).

SL depends of the aircraft altitude range and contains values for horizontal and vertical $\tau$ thresholds in case of TA or RA issuance, 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 and vertical threshold value (ZTHR) at Closest Point of Approach (CPA). During an encounter, if the horizontal or vertical $\tau$ 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 $\tau$ values are lower than the RA threshold or if the miss distances are lower than the RA DMOD and RA ALIM respectively, or predicted vertical miss distance at CPA is lower then ZTHR, then an RA is annunciated [1, 46].

For the purpose of range and altitude tests, aircraft are identified in a Cartesian coordinate system. Let $x^i_t = (x^i_{x,t}, x^i_{y,t}, x^i_{z,t})^T$ and $v^i_t = (v^i_{x,t}, v^i_{y,t}, v^i_{z,t})^T$ be the 3D position and 3D velocity of aircraft *i*; the superscripts *x* and *y* refer to the horizontal axis system, and *z* stands for the altitude. Let $\theta^i_t$ 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 $\psi^i_t$ represent the orientation of velocity vector vit in the vertical plane (measured from the horizontal plane up as positive and down as negative, where $-\pi/2 \le \psi^i_t \le \pi/2$).

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 aircraft at time *t*.

*a) 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 $\tau$). The encounter geometry observed in the range test is shown in Figure 1.

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 distance and the relative velocity in horizontal plane (respectively) between aircraft *i* and *k* at time *t*. In reality these distances and relative velocities are not known to the TCAS system; instead a filtered version of these distances $\hat{x}^{ik}_{h,t}$ and relative velocities $\hat{v}^{ik}_{h,t}$ are known, where the filter used by TCAS is the [1] specified $\alpha$ - $\beta$ tracker.

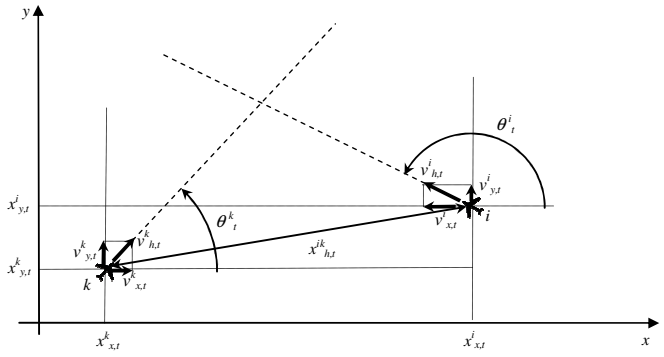


Figure 1. Encounter geometry in the horizontal plane at time *t*

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*, i.e.:

$$\tau^{ik}_{h,t} = \frac{-\left|\hat{x}^{ik}_{h,t}\right|}{\left|\hat{v}^{ik}_{h,t}\right| \cdot \cos(\delta^{ik}_t - \varphi^{ik}_t)} \tag{1}$$

with $\delta^{ik}_t$ the bearing of the velocity difference vector:

$$\delta^{ik}_t = \arctan\left(\frac{v^{ik}_{x,t}}{v^{ik}_{y,t}}\right) \tag{2}$$

and $\varphi^{ik}_t$ the bearing of the position difference vector:

$$\varphi^{ik}_t = \arctan\left(\frac{x^{ik}_{x,t}}{x^{ik}_{y,t}}\right) \tag{3}$$

Equation (3) is defined under the explicit condition that the denominator does not equal zero, i.e.:

$$\left(\delta^{ik}_t - \varphi^{ik}_t \neq \pi/2\right) \wedge \left(\delta^{ik}_t - \varphi^{ik}_t \neq -\pi/2\right) \wedge \left(\left|\hat{v}^{ik}_{h,t}\right| \neq 0\right) \tag{4}$$

*b) Altitude test:*

At each moment *t*, both the vertical distance separation and the 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 $\tau$).

Let $\hat{x}^{ik}_{z,t} = \hat{x}^i_{z,t} - \hat{x}^k_{z,t}$ and $\hat{v}^{ik}_{z,t} = \hat{v}^i_{z,t} - \hat{v}^k_{z,t}$ be the estimated distance and the estimated relative velocity in the vertical plane between aircraft *i* and *k,* at time *t*, using the $\alpha - \beta$ tracker [1].

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 equation for $\hat{v}^{ik}_{z,t} \neq 0$:

$$\tau^{ik}_{z,t} = -\left(\hat{x}^{ik}_{z,t} / \hat{v}^{ik}_{z,t}\right) \tag{5}$$

*c) TA or RA issuance*

The Range and Altitude tests compare given criteria and calculated values for $\tau^{ik}_{h,t}$, $\tau^{ik}_{z,t}$, $\hat{x}^{ik}_{h,t}$, $\hat{x}^{ik}_{z,t}$, $\bar{x}^{ik}_{h,t+\tau^{i,k}_{h,t}}$ and $\bar{x}^{ik}_{z,t+\tau^{ik}_{h,t}}$. If the $\left|\bar{x}^{ik}_{h,t+\tau^{i,k}_{h,t}}\right| < DMOD_{TA}$ (horizontal miss distance filter), then an intruder aircraft is declared to be a threat to the own aircraft and then the TA and RA issuance process follows. So, according to [1], TA alert shall be issued whenever one of the following sets of conditions is satisfied:

$$\begin{aligned}
&\left(0 < \tau^{ik}_{h,t} < \tau_{TA}\right) \wedge \left(0 < \tau^{ik}_{z,t} < \tau_{TA}\right) \ \vee \\
&\left(0 < \tau^{ik}_{h,t} < \tau_{TA}\right) \wedge \left(\left|\hat{x}^{ik}_{z,t}\right| < ALIM_{TA}\right) \ \vee \\
&\left(\left|\hat{x}^{ik}_{h,t}\right| < DMOD_{TA}\right) \wedge \left(0 < \tau^{ik}_{z,t} < \tau_{TA}\right) \ \vee \\
&\left(\left|\hat{x}^{ik}_{h,t}\right| < DMOD_{TA}\right) \wedge \left(\left|\hat{x}^{ik}_{z,t}\right| < ALIM_{TA}\right) \ \vee \\
&\left(\left|\hat{x}^{ik}_{z,t}\right| < ALIM_{TA}\right) \wedge \left(\left|\bar{x}^{ik}_{h,t+\tau^{i,k}_{h,t}}\right| < DMOD_{TA}\right) \ \vee \\
&\left(0 < \tau^{ik}_{z,t} < \tau_{TA}\right) \wedge \left(\left|\bar{x}^{ik}_{h,t+\tau^{i,k}_{h,t}}\right| < DMOD_{TA}\right)
\end{aligned} \tag{6}$$

And RA will be issued when one of the following set of conditions is satisfied:

$$\begin{aligned}
&\left(0 < \tau^{ik}_{h,t} < \tau_{RA}\right) \wedge \left(\left|x^{ik}_{z,t}\right| < ALIM_{RA}\right) \wedge \left(\left|\bar{x}^{ik}_{z,t+\tau^{i,k}_{h,t}}\right| < ZTHR\right) \ \vee \\
&\left(0 < \tau^{ik}_{h,t} < \tau_{RA}\right) \wedge \left(0 < \tau^{ik}_{z,t} < \tau_{RA}\right) \wedge \left(\left|\bar{x}^{ik}_{z,t+\tau^{i,k}_{h,t}}\right| < ZTHR\right) \ \vee \\
&\left(0 < \tau^{ik}_{h,t} < \tau_{RA}\right) \wedge \left(0 < \tau^{ik}_{z,t} < \tau_{RA}\right) \wedge \left(\tau^{ik}_{z,t} < \tau^{ik}_{h,t}\right) \ \vee \\
&\left(0 < \tau^{ik}_{h,t} < \tau_{RA}\right) \wedge \left(\left|x^{ik}_{z,t}\right| < ALIM_{RA}\right)
\end{aligned} \tag{7}$$

OR the same set of conditions where the equation $\left(0 < \tau_{h,t}^{ik} < \tau_{RA}\right)$ is replaced with the equation $\left(\left|\hat{x}_{h,t}^{ik}\right| < DMOD_{RA}\right)$, producing the set of conditions (8), or with the equation $\left(\left|\bar{x}_{h,t+\tau_{h,t}^{i,k}}^{ik}\right| < DMOD_{RA}\right)$ producing the set of conditions (9).

In the above, $\bar{x}_{z,t+\tau_{h,t}^{i,k}}^{ik}$ is defined as follows: if $\tau_{h,t}^{ik} < \tau_{RA}$ at moment $t$ then predicted vertical positions of aircraft $i$ and $k$ at CPA are given by the following equations:

$$\bar{x}_{z,t+\tau_{h,t}^{ik}}^{i} = \hat{x}_{z,t}^{i} - \hat{v}_{z,t}^{i} \cdot \tau_{h,t}^{ik} \tag{10}$$

$$\bar{x}_{z,t+\tau_{h,t}^{ik}}^{k} = \hat{x}_{z,t}^{k} - \hat{v}_{z,t}^{k} \cdot \tau_{h,t}^{ik} \tag{11}$$

Predicted vertical miss distance between aircraft $i$ and $k$ at CPA is given by the following equation:

$$\bar{x}_{z,t+\tau_{h,t}^{ik}}^{ik} = \bar{x}_{z,t+\tau_{h,t}^{ik}}^{i} - \bar{x}_{z,t+\tau_{h,t}^{ik}}^{k} \tag{12}$$

Similarly, $\bar{x}_{h,t+\tau_{h,t}^{i,k}}^{ik}$ is defined as follows: if $\tau_{h,t}^{ik} < \tau_{TA}$ at moment $t$ then predicted horizontal positions of aircraft $i$ and $k$ at CPA are given by the following equations:

$$\bar{x}_{h,t+\tau_{h,t}^{ik}}^{i} = x_{h,t}^{i} + v_{h,t}^{i} \cdot \tau_{h,t}^{ik} \tag{13}$$

$$\bar{x}_{h,t+\tau_{h,t}^{ik}}^{k} = x_{h,t}^{k} + v_{h,t}^{k} \cdot \tau_{h,t}^{ik} \tag{14}$$

Predicted horizontal miss distance between aircraft $i$ and $k$ at CPA is given by the following equation:

$$\bar{x}_{h,t+\tau_{h,t}^{ik}}^{ik} = \bar{x}_{h,t+\tau_{h,t}^{ik}}^{i} - \bar{x}_{h,t+\tau_{h,t}^{ik}}^{k} \tag{15}$$

### *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.

#### *a) Sense selection*

Let $t$ be the moment at which an RA for own aircraft $i$ is issued, i.e. $\tau_{RA}$ 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.

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

$$\bar{x}_{z,t+\tau_{RA}}^{i}(up) = \hat{x}_{z,t}^{i} + (\hat{v}_{z,t}^{i} + \Delta_{z,t}^{i}) \cdot \tau_{RA} \tag{16}$$

- if the current rate is maintained

$$\bar{x}_{z,t+\tau_{RA}}^{i}(current) = \hat{x}_{z,t}^{i} + \hat{v}_{z,t}^{i} \cdot \tau_{RA} \tag{17}$$

- if the downward sense is selected

$$\bar{x}_{z,t+\tau_{RA}}^{i}(down) = \hat{x}_{z,t}^{i} + (\hat{v}_{z,t}^{i} - \Delta_{z,t}^{i}) \cdot \tau_{RA} \tag{18}$$

where $\Delta_{z,t}^{i}$ has a fixed value of 1500 feet/min [2, 13].

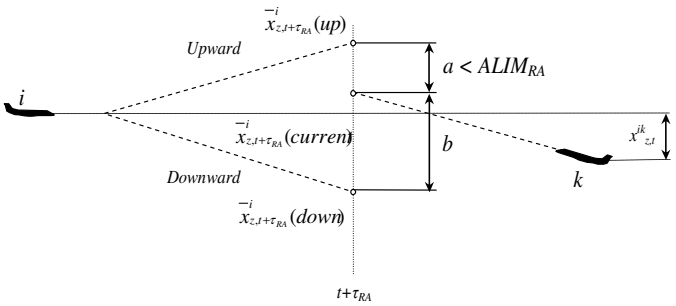


Figure 2. RA sense selection (illustrative example)

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 equations (see Figure 2):

$$a \equiv \left|\bar{x}_{z,t+\tau_{RA}}^{i}(up) - \bar{x}_{z,t+\tau_{RA}}^{k}(current)\right| \tag{19}$$

$$b \equiv \left|\bar{x}_{z,t+\tau_{RA}}^{i}(down) - \bar{x}_{z,t+\tau_{RA}}^{k}(current)\right| \tag{20}$$

The sense is represented by the variable $c_t^i$ which assumes the value: $c_t^i = 1$ in case of the upward sense selected, $c_t^i = -1$ in case of downward sense, and $c_t^i = 0$ otherwise.

In case aircraft $i$ already receives a sense from aircraft $k$ before it has finished its own sense calculations then:

$$c_t^i = -\,c_t^k \tag{21}$$

otherwise:

$$c_t^i = \begin{cases} -1, & if \begin{cases} (b > a) \wedge (a < ALIM_{RA}) \vee \\ (b \le a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}]\ such that\ \bar{x}_{z,t+\varepsilon}^{ik} = 0\right) \wedge (b \ge ALIM_{RA}) \end{cases} \\ 1, & if \begin{cases} (b \le a) \wedge (b < ALIM_{RA}) \vee \\ (b > a) \wedge \left(\exists \varepsilon \in (0, \tau_{RA}]\ such that\ \bar{x}_{z,t+\varepsilon}^{ik} = 0\right) \wedge (a \ge ALIM_{RA}) \end{cases} \\ 0, & otherwise \end{cases} \tag{22}$$

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.

Hence, the RA sense sent to the intruder aircraft satisfies:

$$c_t^k = \begin{cases} 0, & if\ v_{z,t}^k = 0\ or\ c_t^i = 0 \\ -c_t^i, & otherwise \end{cases} \tag{23}$$

Equation (23) covers the possibility that $c^k_t = 0$ if $v^k_{z,t} = 0$. This means that when the intruder aircraft is in horizontal (level) flight, then its flight profile will not be changed, i.e. it will not receive an RA.

*b) Strength selection*

Once the sense has been selected, TCAS logic will determine 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 $t+\tau_{RA}$), under the assumption that intruder aircraft doesn't change the flight profile.

This means that the change of vertical speed $\Delta^{i*}_{z,t}$ should be minimal. The determination of the appropriate strength (vertical speed) is carried out as follows:

if $\left|\bar{x}^{ik}_{z,t+\tau_{RA}}(current)\right| \geq ALIM_{RA}$ then no RA is issued, otherwise the strength is calculated using:

$$v^{i*}_{z,t} = \begin{cases} \hat{v}^i_{z,t} + \Delta^{i*}_{z,t}; & c^i_t = 1 \\ \hat{v}^i_{z,t} - \Delta^{i*}_{z,t}; & c^i_t = -1 \end{cases} \tag{24}$$

where:

$$\Delta^{i*}_{z,t} = \left[ ALIM_{RA} + \left| \left( \hat{x}^k_{z,t} + \hat{v}^k_{z,t} \cdot \tau_{RA} \right) - \left( \hat{x}^i_{z,t} + \hat{v}^i_{z,t} \cdot \tau_{RA} \right) \right| \right] / \tau_{RA} \tag{25}$$

*c) RA modification*

Nine seconds [46] after an RA has been issued, i.e. at moment $t$+9, logic is checking the evolution of the encounter. At that moment $\tau_{RA}$-9 second remains until CPA.

In the case that at moment $t+9$ the predicted vertical separation between aircraft $i$ and $k$ at CPA is $\left|\bar{x}^{ik}_{z,t+\tau_{RA}}\right| \geq ALIM_{RA}$, then RA should be modified. The new RA could contain a sense modification and/or strength modification. Modified sense values are then given by the following equations:

$$c^i_{t+9} = \begin{cases} -c^i_t, & \left|\bar{x}^{ik}_{z,t+\tau_{RA}}\right| \geq ALIM_{RA} \\ c^i_t, & otherwise \end{cases} \tag{26}$$

$$c^k_{t+9} = \begin{cases} 0, & if\ \hat{v}^k_{z,t+9} = 0\ or\ c^i_{t+9} = 0 \\ -c^i_{t+9}, & otherwise \end{cases} \tag{27}$$

and modified strength value by the following equation:

$$v^{i*}_{z,t+9} = \begin{cases} \hat{v}^i_{z,t+9} + \Delta^{i*}_{z,t+9}; & if\ c^i_{t+9} = 1 \\ \hat{v}^i_{z,t+9} - \Delta^{i*}_{z,t+9}; & if\ c^i_{t+9} = -1 \end{cases} \tag{28}$$

where:

$$\Delta^{i*}_{z,t+9} = \left[ ALIM_{RA} + \left| \begin{matrix} \left( \hat{x}^k_{z,t+9} + \hat{v}^k_{z,t+9} \cdot (\tau_{RA} - 9) \right) - \\ - \left( \hat{x}^i_{z,t+9} + \hat{v}^i_{z,t+9} \cdot (\tau_{RA} - 9) \right) \end{matrix} \right| \right] / (\tau_{RA} - 9) \tag{29}$$

*d) 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, 13]; b) a CoC occurs after an encounter has been resolved [13]).

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:

$$\left|\hat{x}^{ik}_{h,t'}\right| > \left|\hat{x}^{ik}_{h,t_{CPA}}\right| \tag{30}$$

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

### C. *Enhancements over the conceptual model in* [33]

In [34] initial SDCPN-based ACAS model from [33] has been partially evaluated using the validation approach described in the sequel of this paper. Based on these outcomes some issues have been identified for which this initial model should be improved. This has resulted in the ACAS model as described in the above equations (1) to (30). These equations differ from those in [33] as follows:

- $\alpha$ - $\beta$ tracking has been included, as a consequence in all conceptual model equations, (1) through (30), true aircraft states have been replaced by estimated aircraft states;
- an improved set of conditions for triggering TA and RA have been introduced in equations (6) to (15) including also horizontal miss distance filter;
- modified conditions for own aircraft sense selection in equation (22);
- an additional condition for determining intruder sense has been introduced in equation (23); and
- an RA modification has been introduced in equations (26) through (29).

## III. Systematic Validation Process

Proper validation of the developed SDCPN-based model of ACAS operations is a prerequisite in order to establish confidence in it for safety risk analysis purposes. In [44] and [45] model validation is 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*". Following [45] the main principles of validation are:

- Validation must be conducted throughout the entire life cycle of a simulation study;
- The outcome of simulation model should not be considered as a binary variable where the model is absolutely correct or incorrect.
- A simulation model is built with respect to 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) [45]. Sargent in [44] 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.

### A. Validation Process of ACAS Operations Model

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

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, were each level is represented with a certain question, while successive levels become more detailed. The following questions are asked (Figure 3) [34, 47]:

- 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 close enough to the same separation in Control case?

At each validation level a modelled case (encounter) is compared with Control case (which could be from real life or from other model). 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.

### B. Collection of ACAS encounter data

The approach taken in this research is to make validation by comparing the outputs from the developed SDCPN model with Real Life Encounters or outputs from other models with similar purpose. Inputs for the comparison are data for seven real life encounters, chosen in a way to represent different conflict situations, provided by Technical University Braunschweig [48]. A Eurocontrol model InCAS was available and was used for validation of SDCPN model [31, 32, 49]. This model was well-proven across Europe in TCAS encounters analysis (see Table I for comparison with SDCPN model). Real Life data served as a basis for the preparation (reconstruction and approximation) of input data for both the SDCPN-based model of ACAS operations as well as the InCAS model (Figure 4).

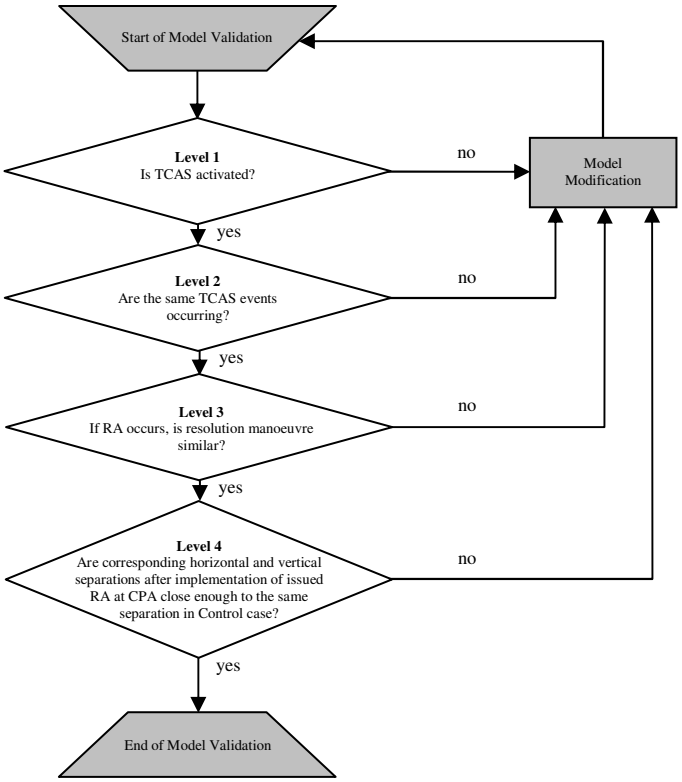


Figure 3. The proposed Validation Process [34, 47]

TABLE I. MODELS CHARACTERISTICS [34]

| | ACAS SDCPN model | InCAS |
|---|---|---|
| Model Nature | Stochastic (encounter type model) | Deterministic (encounter type model) |
| Purpose | Risk and Safety Assessment of TCAS operation | Analysis of ACAS encounters taken from real radar data |
| TCAS II Logic | Model of TCAS II Logic | Real TCAS II logic, provided by MITRE Co. |
| Altitude change | Continuous | Step change (quantization of 25ft and 100 ft) |
| Vertical speed, Ground speed, Magnetic heading | Constant during encounter | In case of recorded radar data they are variable during encounter, otherwise they are constant |
| Pilot reaction | 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 | Included, with delayed reaction and idealised pilot response (with return to original trajectory or original vertical speed after Clear of Conflict) |
| ATCo role | Included as active (responsible for separation) or passive (when pilot is reacting according to RA). Reaction is randomly delayed. | Not included |
| Reliability of technical system | Included (failure rates) | Not included |

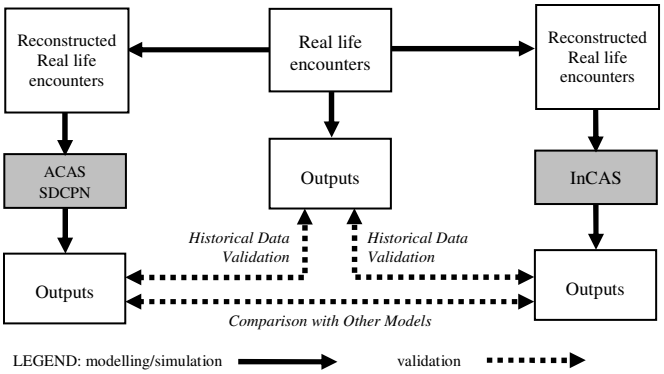


Figure 4. Validation Approach

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. The following outputs were chosen for validation:

- selected sense and strength for the issued RA;
- minimum horizontal distance at CPA as well as corresponding vertical distance and time;

The facts that TCAS is activated and RA is issued are considered at validation Level 1 and 2 respectively. Further details from the data are used at validation Levels 3 and 4.

Real life encounters data serve to create inputs for the SDCPN-based model of ACAS operations and InCAS model. Namely, the horizontal situation and horizontal distance versus time plots are used for aircraft initial positions and magnetic headings. 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 and InCAS models.

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.

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.

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 as well as InCAS model produces outputs which are used for validation, together with the real life data.

### C. *Comparison against Real Life*

Taking into account the abovementioned, it is likely that certain differences between model outputs and real life cases will appear.

Possible causes of such differences are the following [34]:

- Inputs for both ACAS SDCPN and InCAS models are obtained by reconstructing the real event. Such a procedure may generate certain errors in input values because it uses the average ground speed, rate of descent/climb and magnetic heading values. Additionally, a geographic coordinate system from reality was transformed into the Cartesian coordinate system used in both models. This transformation could form an additional source of errors in the aircraft position input;
- RA strength in the SDCPN-based model is assumed to have the maximal value, from the suggested range of strength values (maximal from the flight profile change point of view). It is applicable both for initial RA issuance and for RA modification. Applied values in reality belong to the range suggested to pilots during specific encounter; InCAS applied values are not fully known however.
- 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 and InCAS model all aircraft are equipped with the same model of TCAS II Version 7. All manufacturers should satisfy minimum requirements for TCAS II, but it could be expected that some differences in logic might exist due to the fact that manufacturers respond to the required minimum providing even more rigorous logic. For example, the SDCPN and InCAS models are based on documents dating from 2007 and earlier [1, 13, 46]. However, in 2008 a new set of documents was issued containing a new logic called Version 7.1 [50, 51]. According to authors best knowledge these changes still haven't came into force [52]. However, in the near future there may be certified aircraft that carry an enhanced ACAS, while this is not yet covered by all models of ACAS.

## IV. ACAS Model Validation Results

### A. *Validation – Level 1 results*

At Level 1 a simple matrix (Table II) is 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.

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 conservative 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.

The results of Level 1 validation between SDCPN-based model of ACAS operations and Real Life data are presented in Table II. In 7 out of 7 available cases (encounters) ACAS was activated both in reality and in the SDCPN-based model.

The results are in green fields, meaning that satisfactory validation results were obtained. The same results are obtained in the case of validation between InCAS model and Real Life and SDCPN-based model and InCAS (that's why they are not presented in separate tables).

TABLE II. LEVEL 1 VALIDATION RESULTS (ACAS SDCPN MODEL VS. REAL LIFE ENCOUNTERS DATA)

| | | Real Life Encounter Data | |
|---|---|---|---|
| | | No | Yes |
| SDCPN | No | *0* | *0* |
| | Yes | *0* | ***7*** |

*B. Validation – Level 2 results*

If the answer to the Level 1 question is positive, then at Level 2 the question is more detailed. A matrix is constructed (Table III), 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. Situations that are covered in Table III 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);
- $RA_{MAC}$ - case in which an RA is issued but MAC occur.

Like before, green fields in the matrix present a matching 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.

Level 2 validation results for comparison between ACAS SDCPN model and Real Life data are presented in Table IIIa. It was shown that in 6 out of 7 available 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).

However, in 1 out of 7 encounters 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 that trajectories of aircraft in the given case in reality were not converging or crossing, and the aircraft were laterally and vertically well separated when the RA was issued. Therefore there is a possibility that in reality this encounter was a false alarm.

Similar behaviour is observed in the case of comparison between InCAS model and Real Life data (Table IIIb). Here it is also shown that in 1 out of 7 encounters a TA only was issued in the InCAS model instead of RA which was activated in reality, placing it in a red field.

It happened that is the same encounter as it is in case of ACAS SDCPN model. That's why this result was taken as the necessary proof for the decision to pass on to the level 3 validation.

At validation level 2, the responses of InCAS and SDCPN model are the same. The comparison of the ACAS SDCPN model and InCAS model (Table IIIc) shows that perfect match exist, i.e. that all encounters fall on the green diagonal.

TABLE III. LEVEL 2 VALIDATION RESULTS (A DIFFERENCE HAS BEEN IDENTIFIED ONLY FOR ENCOUNTER 5)

| | | No evennt | TA | RA | RA | $RA_{MAC}$ |
|---|---|---|---|---|---|---|
| a) | | Real Life Encounter Data | | | | |
| SDCPN | No event | *0* | *0* | *0* | *0* | *0* |
| | TA | *0* | *0* | ***1*** | *0* | *0* |
| | RA | *0* | *0* | ***6*** | *0* | *0* |
| | RA* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | *0* | *0* | *0* | *0* | *0* |
| b) | | Real Life Encounter Data | | | | |
| InCAS | No event | *0* | *0* | *0* | *0* | *0* |
| | TA | *0* | *0* | ***1*** | *0* | *0* |
| | RA | *0* | *0* | ***6*** | *0* | *0* |
| | RA* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | *0* | *0* | *0* | *0* | *0* |
| c) | | InCAS | | | | |
| SDCPN | No event | *0* | *0* | *0* | *0* | *0* |
| | TA | *0* | ***1*** | *0* | *0* | *0* |
| | RA | *0* | *0* | ***6*** | *0* | *0* |
| | RA* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | *0* | *0* | *0* | *0* | *0* |

### C. Validation – Level 3 results

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 IV), 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.

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 IV 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 sense 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.

Table IVa presents the results of the Level 3 validation in case of comparison between ACAS SDCPN model and Real Life data. It was shown that in 5 out of 6 available encounters (which were placed in green field at level 2) resolution manoeuvre, i.e. issued sense, was similar both in reality and in the SDCPN-based model.

In one out of 6 encounters the manoeuvre was different (see red number in Table IVa, it was actually encounter 2). However, 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.

To verify this, complementary Monte Carlo simulations for encounter 2 have been carried out. The input value for vertical speed of own aircraft is randomly changed in the range of ±10% of nominal value -1275 fpm, i.e. in the range [-1148, 1403 fpm] using the uniform probability distribution. The experiment is repeated 1000 times. In 129 encounters manoeuvre (sense) was the same like in reality with the resulting vertical separation at CPA being between 949 and 1543 ft.

Additionally, it was found that for vertical speed in the range of [-1148, -1185 fpm] the manoeuvre was the same as in reality, and in the range [-1186, -1403 fpm] the manoeuvre was opposite. This experiment demonstrated that the selected sense could easily switch to the opposite when small changes in vertical speed are introduced.

Also, the 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. In the case of InCAS vs. Real Life, all encounters fall on the green diagonal (Table IVb), meaning that the selected senses were similar.

Table IVc shows that in the case of ACAS SDCPN vs. InCAS there is still one (same) encounter as in Table IVa, were SDCPN model selected a different sense. This result also proves that there are some differences in the sense selection algorithms used in the SDCPN model relative to real life ACAS, or ACAS used in the InCAS model.

TABLE IV. LEVEL 3 VALIDATION RESULTS (A DIFFERENCE HAS BEEN IDENTIFIED ONLY FOR ENCOUNTER 2)

| | | | RA | | RA* | | $RA_{MAC}$ | |
|---|---|---|---|---|---|---|---|---|
| | | | u/d | d/u | u/d | d/u | u/d | d/u |
| a) | | | Real Life Encounters Data | | | | | |
| SDCPN | RA | u/d | ***1*** | *0* | *0* | *0* | *0* | *0* |
| | | d/u | ***1*** | ***4*** | *0* | *0* | *0* | *0* |
| | RA* | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |
| b) | | | Real Life Encounters Data | | | | | |
| InCAS | RA | u/d | ***2*** | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | ***4*** | *0* | *0* | *0* | *0* |
| | RA* | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |
| c) | | | InCAS | | | | | |
| SDCPN | RA | u/d | ***1*** | *0* | *0* | *0* | *0* | *0* |
| | | d/u | ***1*** | ***4*** | *0* | *0* | *0* | *0* |
| | RA* | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |
| | $RA_{MAC}$ | u/d | *0* | *0* | *0* | *0* | *0* | *0* |
| | | d/u | *0* | *0* | *0* | *0* | *0* | *0* |

### D. Validation – Level 4 results

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.

Under Level 4 validation, the correspondence between ACAS SDCPN-based model data and Real encounter data are presented in Figure 5a (horizontal and vertical separations at CPA are presented in separate graphs). The numbers attached to small boxes represent the corresponding encounters. Dashed lines present the range of ±0.5 Nm in the horizontal plane and ±500 ft in the vertical plane. They are introduced only for easy visual comparison. Horizontal distances obtained using the model are within the range of -0.24 Nm to +0.39 Nm relative to the real one, i.e. to the diagonal. The range of vertical distances is broader and relative to real life cases it goes from –773 ft, for encounter 5 where only TA is recorded in SDCPN model, up to +345 ft, for encounter 4 (Figure 5a). In encounter 2 which is at previous Level 3 recognized as the encounter with difference in sense, vertical separation at CPA is greater then in reality (1064 ft vs. 1000 ft). The corresponding range of values without encounter 5 is from -533 to +345 ft. Generally, vertical separation in two encounters (2 and 4) is greater then in reality, while for the rest it is lower. In the SDCPN model case, in all encounters with RA issued, except in encounter 1, the vertical separation at CPA is greater than 1000ft (vertical separation minima).

The comparison between InCAS model and Real Life data is represented on Figure 5b. Also in this case differences exist between the InCAS model and reality. The differences in horizontal separations range between -0.21 Nm and +0.44 Nm. Differences in vertical separations at CPA range between -719ft in encounter 5 were TA is issued up, and 585 ft in encounter 2. Generally, vertical separation in three cases (2, 4 and 7) is equal or greater then in reality, while in four cases (1, 3, 6 and 5 (case with TA issued)) it is lower. Having in mind that the InCAS model behaves similar as pilots in reality (meaning that strength value chosen for RA was determined from the recommended strength range), the possible reason for differences is related to differences in TCAS logic. In the case of the InCAS model, in all encounters with RA issued, except in encounter 1 and 3, the vertical separation at CPA is greater then 1000ft (vertical separation minima). Finally, mutual comparison between the ACAS SDCPN-based model and the InCAS model was performed.

The results are shown on Figure 5c. In the case of horizontal spacing the match is almost perfect, while differences in vertical spacing exist. They are in the range of -521ft (encounter 2) up to +204 ft (encounter 4). In encounters 1, 3 and 4 the corresponding vertical separations at CPA are greater for SDCPN then for the InCAS case. In the remaining encounters the vertical separation is smaller

Additional analysis shows that in encounters 1, 3 and 5, the initial RA was not modified during the encounter while in encounter 2 and 6 it was modified in all cases (Reality, InCAS and SDCPN model). In reality in encounters 4 and 7, RA was not modified, while in the case of the InCAS and SDCPN models, RA was modified.

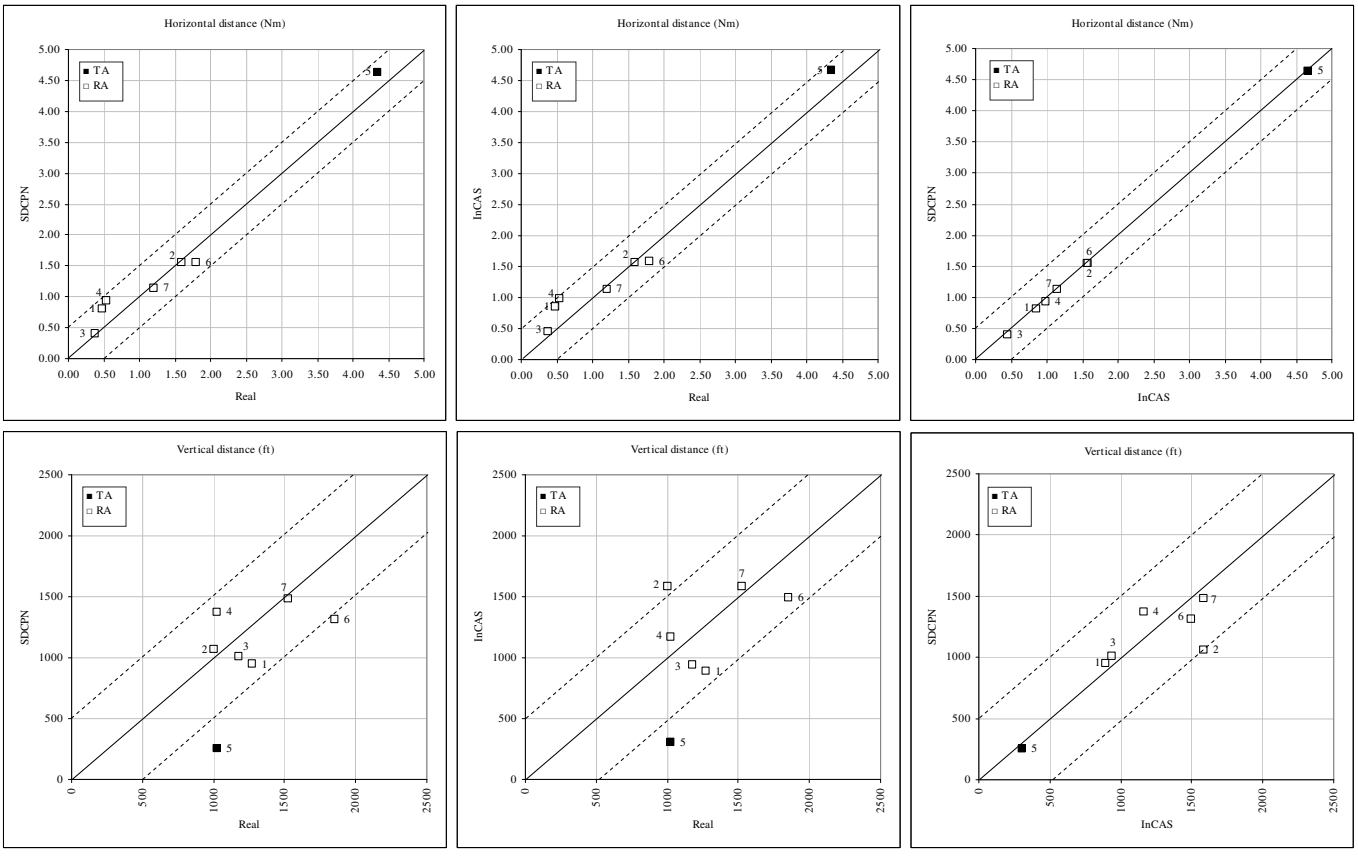


Figure 5. Level 4 Validation Results

## V. CONCLUSION

This research addressed systematic validation of a newly-developed mathematical model of Airborne Collision Avoidance System (ACAS). This newly-developed ACAS model has a significant advantage over models of similar kind when it comes to mathematical analysis and flexibility to integrate the model with other elements of an ATM operation. The key question then is whether these advantages come at the cost of model validity. The investigation of this validation question has been addressed in this paper.

First in section II the conceptual ACAS model has been specified, including an explanation of the improvements made relative to the ACAS conceptual model in [33]. Next, in Section III the model validation principles of [44] and [45] have been used to develop a systematic validation process using both real life data and an existing, well-tested ACAS simulation model. Subsequently this systematic validation process has initially been applied to the novel SDCPN-based ACAS model. The results obtained show that the systematic validation process works well, and that the novel ACAS mathematical model is working as well as the well-tested ACAS simulation model does.

Some follow-up research activities are foreseen. At this moment the number of real life ACAS encounter data is rather limited. Hence much more real life data will be collected in order to complete the systematic validation. The advantage of working with a larger set of real life encounter data is that at each validation level we can make use of a statistical hypothesis testing formalism. Another research activity is to enhance the SDCPN-based model with the TCAS version 7.1 modifications.

The novel ACAS model can easily be integrated with other TOPAZ simulation models for various existing or future operational concepts. This way it can for example be assessed how well ASAS based approaches work together with ACAS, and what the total risk reduction is of a combined use of airborne safety nets.

## ACKNOWLEDGEMENT

This research was conducted with support from the "RESET - Reduced Separation Minima" project, commissioned by the European Commission Directorate General for Transport and Energy (DG TREN), under the FP6 Program (2006-2010), and project "Methods for evaluation of development scenarios of the air transport system in Serbia (airlines, airports, ATC) - safety, efficiency, economic and environmental aspects", 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.

For the validation of the developed model, authors are very grateful to Prof. Peter Form and Dr Jens Gottstein from the Institut für Eisenbahnwesen und Verkehrssicherung, TU Braunschweig, Germany, for providing real life TCAS encounters data, and to Mr. Garfield Dean from the EUROCONTROL Experimental Centre, Bretigny-sur-Orge, France, for providing InCAS Version 2.6, together with insightful explanations.

## REFERENCES

[1] ICAO, 2007, *Annex 10 – Volume 4*, International Civil Aviation Organization, Canada.

[2] Kuchar J. and Drumm A., 2007. The Traffic Alert and Collision Avoidance System. *Lincoln Laboratory Journal*, 16 (2), 277-296.

[3] Brooker P., 2008. The Uberlingen accident: Macro-level safety lessons. *Safety Science*, 46, 1483–1508.

[4] de Carvalho P., Gomes J., Huber G., Vidal M., 2009. Normal people working in normal organizations with normal equipment: System safety and cognition in mid-air collision. *Applied Ergonomics*, 40 (3), 325-340.

[5] Brooker P., 2004. Why the Eurocontrol Safety Regulation Commission Policy on Safety Nets and Risk Assessment is Wrong. *The Journal of Navigation*, 57 (2), 231-243.

[6] Brooker P., 2005. Airborne Collision Avoidance Systems and Air Traffic Management Safety. *The Journal of Navigation*, 58 (1), 1-16.

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

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

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

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

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

[12] Leveson N., Heimdahl M., Hildreth H., Reese J., 1994. Requirements Specification for Process-Control Systems. *IEEE Transactions on Software Engineering*, 20 (9), 684-707.

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

[14] Chan W., Anderson R., Beame P., Jones D., Notkin D., Warner W., 2001. Optimizing Symbolic Model Checking for Statecharts. *IEEE Transactions on Software Engineering*, 27 (2), 170-190.

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

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

[17] Küster-Filipe J., Felici M., Anderson S., 2003. *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.

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

[19] Zeitlin A. and McLaughlin M., 2006. *Modeling for UAS Collision Avoidance*. Proceedings of AUVSI Unmanned Systems North America, USA.

[20] Zeitlin A., Lacher A., Kuchar J., Drumm A., 2006. *Collision Avoidance for Unmanned Aircraft: Proving the Safety Case*. The MITRE Corporation and MIT Lincoln Laboratory, USA.

[21] Kochenderfer M., Espindle L., Kuchar J., Griffith J., 2008. A Comprehensive Aircraft Encounter Model of the National Airspace System. *Lincoln Laboratory Journal*, 17 (2), 41-53.

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

[23] Neil M., Malcolm B., Shaw R., 2003. *Modelling an Air Traffic Control Environment Using Bayesian Belief Networks*. Proceedings of 21st International System Safety Conference, Canada.

[24] Drumm A., 1996. *Lincoln Laboatory Evaluation of TCAS II Logic Version 6.04a, Volume I (Project Report ATC-240).* MIT Lincoln Laboratory, USA.

[25] Chludzinski B., 1999. *Lincoln Laboratory Evaluation of TCAS II Logic Version 7 – Volume I (Project Report ATC-268 I).* MIT Lincoln Laboratory, USA.

[26] Billingsley T., Espindle L., Griffith J., 2009. *TCAS Multiple Threat Encounter Analysis (Project Report ATC-359)*. MIT Lincoln Laboratory, USA.

[27] Chludzinski B., 2009. *Evaluation of TCAS II Version 7.1 Using the FAA Fast-Time Encounter Generator Model (Project Report ATC-346 I).* MIT Lincoln Laboratory, USA.

[28] Espindle L., Griffith J., Kuchar J., 2009. *Safety Analysis of Upgrading to TCAS Version 7.1 Using the 2008 U.S. Correlated Encounter Model (Project Report ATC-349).* MIT Lincoln Laboratory, USA.

[29] Temizer S., Kochenderfer M., Kaelbling L., Lozano-Perez T., Kuchar J., 2009. *Unmanned Aircraft Collision Avoidance Using Partially Observable Markov Decision Processes (Project Report ATC-356).* MIT Lincoln Laboratory, USA.

[30] Kochenderfer M., Chryssanthacopoulos J., Kaelbling L., Lozano-Perez T., 2010. *Model-Based Optimization of Airborne Collision Avoidance Logic (Project Report ATC-360).* MIT Lincoln Laboratory, USA.

[31] GAIN, 2003. *Guide to Methods and Tools for Safety Analysis in Air Traffic Management*. Global Aviation Information Network, USA.

[32] EEC, 2005. *InCAS 2.6 – User Guide.* EUROCONTROL Experimental Centre, France.

[33] Netjasov F., Vidosavljevic A., Tosic V., Everdij M., Blom H., 2010. *Stochastically and Dynamically Coloured Petri Net Model of ACAS Operations*. Proceedings of 4th International Conference on Research in Air Transportation, Hungary.

[34] Netjasov F., 2010. *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*, PhD Thesis, Faculty of Transport and Traffic Engineering, University of Belgrade, Serbia

[35] Everdij M., Klompstra M., Blom H., Klein Obbink B., 2006. *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: Blom H., Lygeros J.), Springer.

[36] Leveson N. and Stolzy J., 1987. Safety Analysis Using Petri Nets. *IEEE Transactions on Software Engineering*, SE-13 (3), 386-397.

[37] Shortle J., Xie Y., Chen C., Donohue G., 2004. Simulating Collision Probabilities of Landing Airplanes at Non-towered Airports. *Simulation*, 80 (1), 21-31.

[38] Everdij M., Blom H., Bakker B., 2007. Modelling Lateral Spacing and Separation for Airborne Separation Assurance Using Petri Nets. *Simulation*, 83 (5), 401-414.

[39] Netjasov F. and M. Janic, 2008. A Review of Research on Risk and Safety Modelling in Civil Aviation. *Journal of Air Transport Management*, 14 (4), 213-220.

[40] Everdij M., Blom, H., 2008. *Enhancing Hybrid State Petri Nets with the Analysis Power of Stochastic Hybrid Processes*. Proceedings of the 9th International Workshop on Discrete Event Systems, Sweden.

[41] Everdij M., Blom, H., 2003. *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.

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

[43] Everdij M., Blom, H., 2005b. Piecewise deterministic Markov processes represented by dynamically coloured Petri nets. *Stochastics: An International Journal of Probability and Stochastic Processes*, 77 (1), 1-29.

[44] Sargent R., 2009. *Verification and Validation of Simulation Models*. Proceedings of the 2009 Winter Simulation Conference, USA.

[45] Balci O., 1998. *Verification, Validation and Testing, in Handbook of Simulation* (edited by Jerry Banks), John Wiley & Sons, pp. 335-393.

[46] DoT, 2000. *Introduction to TCAS II Version 7*. Department of Transportation, Federal Aviation Administration, USA.

[47] Netjasov F., Vidosavljevic A., Tosic V., *Validation of SDCPN Model for TCAS II Version 7 Operation in ATM*, (Technical report, RESET WP7), 2010.

[48] Gottstein J., Form P., 2009. *Five Million Flight Hours Continuous Reception of ACAS - Communications and Reporting of ACAS/TCAS - Interventions in the German Airspace*, Proceedings of EUROCONTROL Safety R&D Seminar, Germany.

[49] Dean G., 2007. *TCAS Analysis of Safety events using InCAS*, Eurocontrol Experimenat Centre (presentation)

[50] RTCA, 2008. *Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment – Volume I*. Radio Technical Commission for Aeronautics, (RTCA/DO-185B), USA.

[51] EUROCAE, 2008. *Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) - Volume I.* The European Organisation for Civil Aviation Equipment, (ED-143), France.

[52] Hindsight, 2009. *TCAS II and Level Bust*. EUROCONTROL, (Winter 2010), pp. 38-41, Belgium

## AUTHOR BIOGRAPHY

**Fedja Netjasov** (BS'99–MS'03–PhD2010) is Assistant Professor 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. His PhD thesis was 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.

**Henk Blom** (MS'78–PhD'90) is Principal Scientist at the National Aerospace Laboratory NLR, Air Transport Safety Institute, Amsterdam, and part time Professor, chair of ATM Safety, at the TU Delft, Faculty of Aerospace Engineering , Delft, the Netherlands. He received the MS degree in Electrical Engineering from Twente University, and PhD from Delft University of Technology in the field of Bayesian Estimation. He is an IEEE Fellow.