Preprint proceedings 8-th Innovative Research Workshop & Exhibition, EUROCONTROL, Paris, France, 1-3 December 2009

A Compositional Hybrid System Approach to the Analysis of Air Traffic Management Systems

E. De Santis, M.D. Di Benedetto, A. Petriccone, G. Pola
Department of Electrical Engineering and Computer Science, Center of Excellence DEWS
University of L'Aquila, Italy

***Abstract*—In Air Traffic Management (ATM) systems catastrophic events may be caused by error propagation in a multi-agent procedure [SBdP03]. The inherent complexity of these systems typically involving many agents makes their analysis prohibitive today. We approach the analysis of multi–agent ATM systems using compositional hybrid systems techniques. Hybrid systems formalism is shown to capture the dynamics of each agent acting in ATM systems in normal and abnormal operative conditions. The interaction of different agents is formalized by means of an appropriate notion of composition of hybrid systems that captures the information exchange among the agents involved. A formal analysis of the obtained composed hybrid system is intractable in realistic ATM scenarios. We provide results that substantially reduce the computational effort required in this analysis, and that allow us to manage ATM scenarios characterized by an arbitrary large number of agents. The *ASAS Lateral Crossing Procedure* is analyzed to illustrate the benefits of the proposed methodology in the analysis of ATM systems.**

***Index Terms*—Air Traffic Management Procedures Modeling, Hybrid Systems, Lateral Crossing Manoeuvre, Complexity Reduction, Critical Observability.**

I. Introduction

THE volume of air traffic is increasing rapidly so that a major efficiency overhaul to manage air traffic flows is necessary to maintain normal operation. New procedures needed to satisfy this requirement have to increase capacity without affecting safety. This issue is particularly relevant since the more capacity increases, the more complex the air traffic management (ATM) system becomes, thus making a formal approach to safety analysis very difficult. Relevant factors contributing to making the formal analysis of ATM systems complex are:

- (Heterogeneity) In ATM systems, agents, (e.g. aircraft, electrical devices, and humans) are characterized by different mathematical models.
- (Size of the System) The number of agents acting in an ATM scenario is generally very large. For example, an air traffic controller is responsible for hundreds of aircraft flying to their designed sky area.

In our previous work [CD08], [DDP08] we showed the benefits of the use of hybrid system formalism to model agents in ATM systems. In particular, we presented an analysis of critical issues, due to unsafe or unallowed operations of the agents in the scenario, that leveraged results on critical observability of hybrid systems developed in [DDD$^+$05], [BGD09]. The main drawback of the approach presented in [CD08], [DDP08] is that the different agents acting in ATM scenarios are considered as isolated systems. This drawback is particularly relevant because agents' interaction is responsible in the occurrence of unsafe situations that cannot be captured when considering different agents in isolation. In this paper, we introduce a formal notion of composition of hybrid systems, each modeling the behaviour of an agent in the environment, to take into consideration agent interactions. This notion has been inspired by the notion of parallel composition in automata theory [HU79]. The composition operation models exchange of information and orders that the different agents send to or infer from the others in the scenario. This formalization allows us to formally analyze and detect the occurrence of unsafe and of unallowed events arising from the interaction. This approach albeit theoretically sound, leads to a mathematical model whose analysis is difficult to deal with, due to the large number of agents involved. To cope with the complexity of this mathematical model, we present a complexity reduction approach based on the decomposition of the set of states of the system associated with situations that are critical, unsafe and/or unallowed, into smaller subsets whose detection can be performed with less computational effort. In particular, we provide a method to analyze a system with an arbitrary large number of agents. To illustrate the proposed approach and its benefits, we consider the ASAS (Airborne Separation Assistance System) *Lateral Crossing Procedure* [LMH$^+$05] as the running example for our approach.

The organization of the paper is as follows. We start by introducing the Lateral Crossing Procedure in Section 2. We present in Section 3 a technique based on compositional hybrid systems to formally analyze the interaction of different agents. We then apply in Section 4 the proposed methodology to the Lateral Crossing Procedure. Concluding remarks are presented in Section 5.

II. Description of the Lateral Crossing Procedure

In this section we report the main steps of the (ASAS) Lateral Crossing Procedure, as illustrated in detail in [LMH$^+$05]. The purpose of the Lateral Crossing Procedure is to provide a new set of air traffic control clearances, allowing an aircraft to cross or pass a target aircraft using ASAS.

A. Roles and Responsibilities

The controller delegates separation responsibility to one aircraft and transfers the corresponding separation tasks to the flight crew. The separation responsibility delegated to the flight crew is limited to a unique designated aircraft and is limited in time (duration of the lateral crossing) space (manoeuvre envelope) and scope (maintain separation with target aircraft). The transfer of responsibility starts as soon as the clearance aircraft has accepted the clearance. The transfer of responsibility back to the controller occurs when the clearance aircraft has passed the clear of traffic (COT) point and the flight crew reports this event to the ground.

B. Operating Principles

1) ATC perspective: The Lateral Crossing Procedure can only be initiated by the controller. The controller should ensure that the target will maintain its track and speed; it is not foreseen that ATC will have to specifically inform the flight crew of the target aircraft. Then a manoeuvring envelope is defined by:

- a maximum track alteration (a maximum value of 45 degrees);
- a maximum along track distance TKmax, after which the responsibility for separation reverts to the controller;
- a maximum cross track deviation, XTKmax (e.g. 8 NM).

When the clearance aircraft is clear of traffic, the flight crew reports to the controller and the Lateral Crossing Procedure is completed. The separation task reverts to the controller. The Lateral crossing procedure is illustrated in Figure 1.

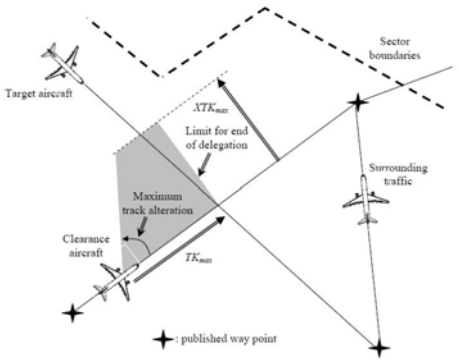

Fig. 1. ASAS Lateral Crossing Procedure. ATC perspective.

2) Airborne perspective: The flight crew performs the Lateral Crossing manoeuvre and the corresponding separation task using onboard ASAS functions. Prior to the acceptance of the Lateral Crossing Procedure, positive identification of the target aircraft is required by the clearance aircraft.

C. Phases of the Lateral Crossing Procedure

The Lateral Crossing Procedure can be divided into the following phases:

1) Set up phase: During this phase, the controller makes a decision whether to initiate the Lateral Crossing Procedure. The controller checks that some applicability conditions are satisfied. If the applicability conditions are not satisfied, the controller engages an ATC based conflict resolution. Otherwise, he may initiate the identification phase.

2) Identification phase: The controller nominates a target aircraft to the clearance aircraft using the target aircraft identification. The clearance aircraft confirms reception of the identification message to the controller. Then, the flight crew identifies the target aircraft on the on–board traffic display. Finally, the flight crew communicates the result of the target acquisition process to the controller. If the target aircraft is not positively identified, the controller engages an ATC based conflict resolution.

3) Clearance phase: The controller passes a Lateral Crossing clearance. This message includes: clearance aircraft and target aircraft identification and details the specific manoeuvre to be carried out (pass behind or pass in front), no agreement is required from the flight crew of the target aircraft. Nevertheless, it may be required that ATC instructs the target aircraft to maintain a heading or track so as to ensure that any unexpected manoeuvre of the target aircraft will not thwart the ASAS Lateral Crossing Procedure. The clearance aircraft flight crew initiates the onboard ASAS crossing function (ASAS Logic) according to the received clearance. The ASAS crossing function provides an ASAS separation advisory which consists in a suggestion for new navigation. The controller monitors the separation between surrounding traffic, but does not monitor separation between the clearance aircraft and the target aircraft.

4) Execution phase: The execution phase deals with the implementation of the ASAS separation advisory and the monitoring of the lateral crossing manoeuvre. As far as the clear of traffic point is passed, the clearance aircraft reports to the controller and the termination phase is engaged.

5) Termination phase: Once the flight crew has determined that the aircraft is clear of traffic, the flight crew reports this to the controller and then resumes its own navigation. The Lateral Crossing Procedure ends when the controller acknowledges the clear of traffic report and resumes responsibility for separation.

6) Abort phase: If the flight crew of the clearance aircraft becomes unable to maintain separation with the target aircraft, he must report to the air traffic controller, and a contingency procedure is used.

III. Compositional Hybrid Systems and Critical Observability

In this section we propose an approach based on compositional hybrid systems to the analysis of ATM multi–agent systems. In particular, Section III-A introduces the hybrid systems' mathematical framework and Section III-B is devoted to the analysis of the obtained multi–agent system.

A. Hybrid Systems and Composition

In this section we recall the notion of hybrid systems used in the model of each agent acting in ATM systems and in particu-

lar in the Passing Crossing Procedure described in the previous section. We then provide a compositional framework capturing interaction among the agents. The following definition of hybrid systems is inspired by the classical model proposed in [LTS99].

Definition 1. *A hybrid system is a tuple*

$$\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, \mathcal{E}, \Sigma, E, \Psi, \eta), \qquad (1)$$

where:

- $Q \times X$ *is the hybrid state space, where* Q *is a finite set of discrete states, and* $X \subseteq \mathbb{R}^n$ *is the continuous state space.*
- $Q_0 \times X_0 \subseteq Q \times X$ *is the set of initial discrete and continuous states.*
- $U \subseteq \mathbb{R}^m, Y \subseteq \mathbb{R}^p$ *are the sets of continuous inputs and outputs.*
- $\mathcal{E} = \{\mathcal{E}_q\}_{q \in Q}$ *associates to each discrete state* $q \in Q$ *the continuous dynamics* $\dot{x} = f_q(x, u)$*, with output* $y = g_q(x)$*.*
- $\Sigma \cup \{\varepsilon\}$ *is the set of discrete inputs, where the empty string* ε *corresponds to the null input.*
- $E \subseteq Q \times \Sigma \times Q$ *is a collection of edges.*
- $\Psi \cup \{\varepsilon\}$ *is the set of discrete outputs, where the empty string* ε *corresponds to the null output.*
- $\eta \colon E \to \Psi$ *is the output function, that associates to each edge a discrete output symbol.*

We do not give here a formal definition of the evolution in time of the above model; mathematical details can be found in [LTS99]. The above model can be used to describe the behaviour of agents acting in ATM scenarios: discrete inputs and outputs model the exchange of information among the agents involved. For example the situation in which an air traffic controller (ATC) orders an aircraft to abort a procedure can be modeled by introducing as an output of the ATC model a discrete signal saying "abort the procedure" and as one input of the aircraft a discrete signal saying "the ATC asked to abort the procedure". On the basis of these information each agent decides his own action.
A formal model of the interaction among the agents involved in a ATM scenario can be captured by the following notion of composition. Consider a scenario characterized by N agents (e.g. ATC, aircraft and etc.), each one represented by the hybrid system:

$$\mathcal{H}_i = (Q_i \times X_i, Q_{0,i} \times X_{0,i}, U_i, Y_i, \mathcal{E}_i, \Sigma_i, E_i, \Psi_i, \eta_i).$$

Suppose that hybrid systems $\mathcal{H}_i$ share information in order to accomplish their tasks. The communication scheme that models the exchange of information among agents can be described by a directed graph $\mathbb{F} = (\mathbb{V}, \mathbb{E})$ where:

- $\mathbb{V} = \{\mathcal{H}_1, \mathcal{H}_2, ..., \mathcal{H}_N\}$ is the set of vertices.
- $\mathbb{E} \subseteq \mathbb{V} \times \mathbb{V}$ is the set of edges, where $(\mathcal{H}_i, \mathcal{H}_j) \in \mathbb{E}$, if $\mathcal{H}_i$ interacts with[1] $\mathcal{H}_j$.

The evolution of each hybrid system $\mathcal{H}_i$ depends on the information that he has from all the hybrid systems $\mathcal{H}_j$ sharing information with him.

[1]Note that according to this definition $\mathcal{H}_i$ interacts with $\mathcal{H}_j$ while the converse is not true in general.

Figure 4 illustrates the graph $\mathbb{F}$ representing the communication scheme in an ATM scenario in which for example aircraft agent $P1$ communicates with agent $ATC1$ but not with agents $P2$, $P3$, $ATC2$ and $ATC3$.
We partition the sets of discrete inputs and of discrete outputs of each hybrid system $\mathcal{H}_i$, in order to capture shared and non–shared information, as follows:

- $\Sigma_i = (\bigcup_{(\mathcal{H}_j, \mathcal{H}_i) \in \mathbb{E}} \Sigma_i^j) \cup \{\varepsilon\}$, where Σ_i^i is the set of internal inputs of $\mathcal{H}_i$, Σ_i^j is the set of inputs of $\mathcal{H}_i$ coming from $\mathcal{H}_j$ and ε is the null input corresponding to no information and/or action given from any $\mathcal{H}_j$.
- $\Psi_i = (\bigcup_{(\mathcal{H}_i, \mathcal{H}_j) \in \mathbb{E}} \Psi_i^j) \cup \{\varepsilon\}$, where Ψ_i^i is the set of outputs of $\mathcal{H}_i$ representing information that $\mathcal{H}_i$ does not share with any $\mathcal{H}_j$, Ψ_i^j is the set of outputs of $\mathcal{H}_i$ representing information that $\mathcal{H}_i$ shares with $\mathcal{H}_j$ and ε is the null output corresponding to no information and/or action given to any $\mathcal{H}_j$.

Given a communication scheme $\mathbb{F}$, the composition of the hybrid systems $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_N$, denoted $\mathcal{H}_1 || \mathcal{H}_2 \ldots || \mathcal{H}_N$, is the hybrid system:

$$(Q \times X, Q_0 \times X_0, U, Y, \mathcal{E}, \Sigma, E, \Psi, \eta), \qquad (2)$$

where:

- $Q = Q_1 \times Q_2 \times \ldots \times Q_N$.
- $X = X_1 \times X_2 \times \ldots \times X_N$.
- $Q_0 = Q_{0,1} \times Q_{0,2} \times \ldots \times Q_{0,N}$.
- $X_0 = X_{0,1} \times X_{0,2} \times \ldots \times X_{0,N}$.
- $U = U_1 \times U_2 \times \ldots \times U_N$.
- $Y = Y_1 \times Y_2 \times \ldots \times Y_N$.
- $\mathcal{E}$ associates to each discrete state $(q_1, q_2, ..., q_N) \in Q$ the continuous dynamics

  $$\dot{x} = (f_{1,q_1}(x_1, u_1), f_{2,q_2}(x_2, u_2), ..., f_{N,q_N}(x_N, u_N)),$$

  with output $y = (g_{1,q_1}(x_1), g_{2,q_2}(x_2), ..., g_{N,q_N}(x_N))$.
- $\Sigma = \Sigma_1 \times \Sigma_2 \times \ldots \times \Sigma_N \cup \{\epsilon\}$.
- $\Psi = \Psi_1 \times \Psi_2 \times \ldots \times \Psi_N \cup \{\epsilon\}$.
- $\eta(e_1, e_2, \ldots, e_N) = (\eta_1(e_1), \eta_2(e_2), \ldots, \eta_N(e_N))$, for any $(e_1, e_2, \ldots, e_N) \in E$,

and the transition relation $E \subseteq Q \times \Sigma \times Q$ is defined as follows. Given $e_1 = (q_1, \sigma_1, p_1) \in E_1, e_2 = (q_2, \sigma_2, p_2) \in E_2, \ldots, e_N = (q_N, \sigma_N, p_N) \in E_N$ the transition

$$e = ((q_1, q_2, \ldots, q_N), (\sigma_1, \sigma_2, \ldots, \sigma_N), (p_1, p_2, \ldots, p_N)) \in E,$$

occurs if one of the following conditions is satisfied:

- Agent $\mathcal{H}_i$ communicates an action and/or information $\eta_i(e_i) = \sigma_j$ to $\mathcal{H}_j$ that evolves according to this information.
- Agent $\mathcal{H}_i$ evolves according to his own plan without interacting with any other $\mathcal{H}_j$.

The above notion of composition has been inspired by the classical notion of parallel composition in the theory of automata [HU79].

B. Analysis of Critical Observability

Given an ATM scenario characterized by N agents, one can model their interaction as an hybrid system

$$\mathcal{H} = \mathcal{H}_1||\mathcal{H}_2||...||\mathcal{H}_N \tag{3}$$

resulting from the composition of N hybrid systems $\mathcal{H}_i$. In this section we analyze the obtained hybrid system and study the possibility of detecting the occurrance of unsafe or unallowed operations in the evolution of the system. This analysis can be carried out by resorting to the notion of critical observability as introduced in [DDD$^+$05] (see also [BGD09]), which we briefly recall hereafter. Given a hybrid system $\mathcal{H}$ let $\mathcal{R} \subset Q$ be the set of *critical states* of $\mathcal{H}$, i.e. the set of discrete states associated to unsafe or unallowed behaviors of $\mathcal{H}$. We say that $\mathcal{H}$ is $\mathcal{R}$–critically observable if it is possible to construct a system that on the basis of the observation, is able to detect whether the current discrete state of $\mathcal{H}$ belongs to $\mathcal{R}$ or not. If such system exists it is called a $\mathcal{R}$–critical observer for $\mathcal{H}$. We do not report here algorithms for the construction of such observer (the interested reader can refer to [DDD$^+$05], [BGD09]), we only recall here its definition. A critical observer of a hybrid system $\mathcal{H}$ is a finite state machine:

$$\mathcal{O} = (\hat{Q}, \hat{Q}_0, \hat{\Sigma}, \hat{\Psi}, \hat{E}, \hat{\eta}),$$

where:

- $\hat{Q} \subseteq 2^Q$ is a set of states.
- $\hat{Q}_0 \subseteq \hat{Q}$ is the set of initial states.
- $\hat{\Sigma}$ is the set of inputs which coincides with the set of discrete outputs Ψ of $\mathcal{H}$.
- $\hat{\Psi}$ is the set of outputs which coincides with $\hat{Q}$.
- $\hat{E}$ is the transition relation.
- $\hat{\eta} : \hat{Q} \rightarrow \Psi$ is the output function which coincides with identity function.

Examples of critical observers will be shown in the next section. If a hybrid system $\mathcal{H}$ is not critically observable, information coming from the continuous dynamics can be used to generate additional discrete signals that provide extra information to discriminate the discrete states, as it was proposed in [BGD09]. In this case a delay in the generation of such extra signals is needed. If a critical observer can be constructed on the basis of these extra delayed outputs, such observer is said to be an observer with delay.

The results briefly recalled above can be used to study critical observability of the composed hybrid system $\mathcal{H}$ of (3) as follows. Define the set of critical states associated with the composed system $\mathcal{H}$ by means of the following relation

$$\mathcal{R} \subseteq Q_1 \times Q_2 \times ... \times Q_N, \tag{4}$$

so that $(q_1, q_2, ..., q_N) \in \mathcal{R}$ if the interaction of states q_i of $\mathcal{H}_i$, $i = 1, 2, ..., N$ yields a critical situation for the overall system $\mathcal{H}$. By performing the analysis of critical observability of the system $\mathcal{H}$ with respect to the set of critical states $\mathcal{R}$ one may assess whether the system is critically observable or not. However, this approach may be computationally demanding if the number of agents involved is large as it is the case in realistic ATM scenarios. We therefore propose hereafter a method that reduces the computational effort in checking critical observability of composed hybrid systems.

The key idea in the subsequent results is the decomposition of the critical relation $\mathcal{R}$ defined in (4) into critical sub–relations, as follows:

- $\mathcal{R}_{i_1} \subseteq Q_{i_1}$ is the set of critical states for hybrid system $\mathcal{H}_{i_1}$, for any $i_1 = 1, 2, ..., N$.
- $\mathcal{R}_{i_1,i_2} \subseteq Q_{i_1} \times Q_{i_2}$ is the set of critical states arising from the interaction of hybrid systems $\mathcal{H}_{i_1}$ and $\mathcal{H}_{i_2}$, for any $i_1, i_2 = 1, 2, ..., N$.

  ...
- $\mathcal{R}_{i_1,i_2,...,i_N} \subseteq Q_{i_1} \times Q_{i_2} \times \ldots \times Q_{i_N}$ is the set of critical states arising from the interaction of hybrid systems $\mathcal{H}_{i_1}$, $\mathcal{H}_{i_2}$, ..., $\mathcal{H}_{i_N}$, for any $i_1, i_2, ..., i_N = 1, 2, ..., N$.

Given one of the sub–relation $\mathcal{R}_{i_1,i_2,...,i_k} \subseteq Q_{i_1} \times Q_{i_2} \times \ldots \times Q_{i_k}$ as defined above define the following set:

$$\mathcal{R}'_{i_1,i_2,...,i_k} = \{(q_1, q_2, \ldots, q_N) \in Q \text{ s.t. } (q_{i_1}, q_{i_2}, \ldots, q_{i_k}) \in \mathcal{R}_{i_1,i_2,...,i_k}\}.$$

It is readily seen that:

$$\mathcal{R} = (\bigcup_{i_1} \mathcal{R}'_{i_1}) \cup (\bigcup_{i_1,i_2} \mathcal{R}'_{i_1,i_2}) \cup \ldots \cup (\bigcup_{i_1,i_2,...,i_N} \mathcal{R}'_{i_1,i_2,...,i_N}). \tag{5}$$

The above decomposition of the critical relation $\mathcal{R}$ in (4) allows us to state the following result which reduces the computational effort in checking critical observability of composed hybrid systems.

Theorem 1. *Consider N hybrid systems $\mathcal{H}_1$, $\mathcal{H}_2$, ..., $\mathcal{H}_N$ and the hybrid system $\mathcal{H} = \mathcal{H}_1||\mathcal{H}_2||...||\mathcal{H}_N$. Let $\mathcal{R} \subseteq Q_1 \times Q_2 \times ... \times Q_N$ be a critical relation for $\mathcal{H}$. Then $\mathcal{H}$ is $\mathcal{R}$–critically observable if and only if the following conditions are satisfied:*

- *$\mathcal{H}_{i_1}$ is $\mathcal{R}_{i_1}$–critically observable for any $i_1 = 1, 2, ..., N$.*
- *$\mathcal{H}_{i_1}||\mathcal{H}_{i_2}$ is $\mathcal{R}_{i_1,i_2}$–critically observable for any $i_1, i_2 = 1, 2, ..., N$.*

  ...
- *$\mathcal{H}_{i_1}||\mathcal{H}_{i_2}||...||\mathcal{H}_{i_N}$ is $\mathcal{R}_{i_1,i_2,...,i_N}$–critically observable for any $i_1, i_2, ..., i_N = 1, 2, ..., N$.*

The advantage of using the above result in checking critical observability of the composed system $\mathcal{H}$ is in that in many ATM scenarios interaction from different agents which may cause unsafe and unallowed situations in the overall system is due to the interaction of few agents. For example, consider an ATM scenario in which N aircraft operate and only one aircraft is allowed to proceed with a specific manoeuvre. Then, critical situations arise when two aircraft, three aircraft, ..., N aircraft decide to start the procedure at the same time. However, it is easy to see that detection of this critical issue arising from the interaction of *only two aircraft* is enough to consider also the case in which three, four, ..., N aircraft are involved. Hence with reference to the above result, one only needs to check critical observability with respect to critical relations $\mathcal{R}_{i_1}$ and $\mathcal{R}_{i_1,i_2}$. The advantages of this result will be illustrated in the next section, when applied to the Lateral Crossing Procedure.

IV. Analysis of Critical Observability of the Lateral Crossing Procedure

In this section we apply the methodology illustrated in the previous section to the Lateral Crossing Procedure. The Lateral Crossing Procedure is characterized by the following agents:

- Clearance Aircraft
- Reference Aircraft
- Air Traffic Controller

In the further developments we do not provide the model of the reference aircraft because the flight crew of the reference aircraft does not have the awareness of existence of a lateral crossing manoeuvre in which it is involved. We provide instead the hybrid model of the clearance aircraft in Section IV-A, the hybrid model of the air traffic controller in Section IV-B, the hybrid model resulting from the composition of the obtained hybrid systems in Section IV-C and the analysis of critical observability of the composed hybrid system in Section IV-D.

A. Clearance Aircraft

The hybrid model of the clearance aircraft is given by:

$$\mathcal{H}_p = (Q_p \times X_p, Q_{p,0} \times X_{p,0}, U_p \times Y_p, \mathcal{E}_p, \Sigma_p, E_p, \Psi_p, \eta_p)$$

where:

- $Q_p = \{q_i, i = 1, 2, ..., 15\}$ is the set of discrete states as detailed in Figure 2.
- $X_p \subset \mathbb{R}^6$ is the continuous state space with $x = (x_1, x_2, x_3, x_4, x_5, x_6) \in X_p$, where $x_1 = X$ and $x_2 = Y$ indicate the horizontal position, $x_3 = h$ is the altitude, $x_4 = V$ is the true airspeed, $x_5 = \psi$ is the heading angle, $x_6 = \gamma$ is the flight path angle.
- $Q_{p,0} = \{q_1\}$ and $X_{p,0} = \{(x_{1_0}, x_{2_0}, x_{3_0}, x_{4_0}, x_{5_0}, x_{6_0})\}$ is the set of initial states.
- $U_p \subset \mathbb{R}^3$ with $u = (u_1, u_2, u_3) \in U_p$, where $u_1 = T$ is the engine trust, $u_2 = \phi$ is the bank angle, $u_3 = \gamma$ is the flight path angle.
- $Y_p = X_p$.
- $\{\mathcal{E}_{p,q}\}_{q \in Q}$ associates to each discrete state $q \in Q$ the continuous dynamics $\dot{x} = f_q(x)$ and $y = x$, where $f_q(x)$ is given[2] by:

$$f_{q_i}(x) = \begin{cases} \dot{X} = V\cos(\psi)\cos(\gamma) \\ \dot{Y} = V\sin(\psi)\cos(\gamma) \\ \dot{h} = V\sin(\alpha) \\ \dot{V} = \frac{1}{m}\big[T\cos(\alpha) - D - mg\sin(\gamma)\big] \\ \dot{\psi} = \frac{1}{mV}\big[L\sin(\phi) + T\sin(\alpha)\sin(\phi)\big] \\ \dot{\gamma} = \frac{1}{mV}\big[(L + T\sin(\alpha))\cos(\phi) - mg\cos(\gamma))\big] \end{cases}$$

  for each $i = 1, 2, ..., 15$, where L is the lift force, D the drag force, α the angle of attack, g gravitational acceleration.
- $\Sigma_p = \{\sigma_i, i = 1, 2, ..., 14\} \cup \{\varepsilon\}$ is the set of discrete inputs, where σ_1 represents the communication from the controller of target selected for the procedure to execute, σ_2 the communication from the controller of target correctly identified, σ_3 the ackowledgement of feasible manoeuvre, σ_4 the ackowledgement of COT point passed, σ_5 the ackowledgement from the controller that he has received communication on the COT passed point, σ_6 the target not identified onboard (conflict detection), σ_7 the order from the controller to abort the procedure, due to uncorrect identification of the target, σ_8 the communication from the controller of target not correctly identified, σ_9 indicates that the manoeuvre cannot be executed (conflict detection), σ_{10} the order from the controller to undertake the procedure of back–up for wrong execution, σ_{11} the order from the controller to undertake the procedure of back–up for dangerous situation, σ_{12} the order from the controller to undertake the procedure of back–up for loss of onboard information, σ_{13} the order from the controller to undertake the procedure of back–up for unexpected behavior of the target, σ_{14} the order from the controller to undertake the procedure of back–up due to wrong orders sent by the controller.
- E_p is the set of transitions as shown in Figure 2.
- $\Psi_p = \{\Psi_i, i = 1, 2, ..., 11\} \cup \{\varepsilon\}$ is the set of discrete outputs, where Ψ_1 represents the communication to the controller of the possibility to execute the manoeuvre, Ψ_2 the communication to the controller that the CTO point was passed, Ψ_3 the communication to the controller to abort the procedure, Ψ_4 the communication to the controller of conflict detection (target not identified), Ψ_5 the communication to the controller of conflict detection (not feasible manoeuvre), Ψ_6 the communication to the controller to abort the procedure for not feasible manoeuvre, Ψ_7 the message of confirmation to the controller of received order to undertake the procedure of back–up for wrong execution, Ψ_8 message of confirmation to the controller of received order to undertake the procedure of back–up for dangerous situation, Ψ_9 the message of confirmation to the controller of received order to undertake the procedure of back–up for loss of onboard information, Ψ_{10} the message of confirmation to the controller of received order to undertake the procedure of back–up for unexpected behavior of the target, Ψ_{11} the message of confirmation to the controller of received order to undertake the procedure of back–up for wrong orders.
- η_p is the output function as shown in Figure 2.

B. Air Traffic Controller

We start by providing the hybrid model of an air traffic controller which interacts with only one clearance aircraft. The hybrid model of the air traffic controller is given by the hybrid system $\mathcal{H}_{atc}$ consisting in the tuple

$$(Q_{atc} \times X_{atc}, Q_{atc,0} \times X_{atc,0}, U_{atc} \times Y_{atc}, \mathcal{E}_{atc}, \Sigma_{atc}, E_{atc}, \Psi_{atc}, \eta_{atc})$$

where:

- $Q_{atc} = \{q_i, ..., i = 1, 2, ..., 9\}$ is the set of discrete state, as detailed in Figure 3 and $X_{atc} = \varnothing$.
- $Q_{atc,0} = \{q_1\}$ and $X_{atc,0} = \varnothing$.

[2]The proposed model has been taken from [GL04].

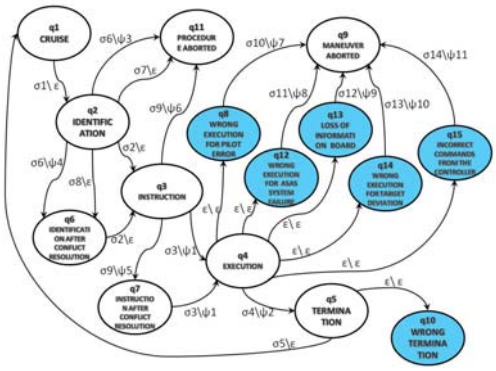

Fig. 2. Hybrid system of the clearance aircraft.

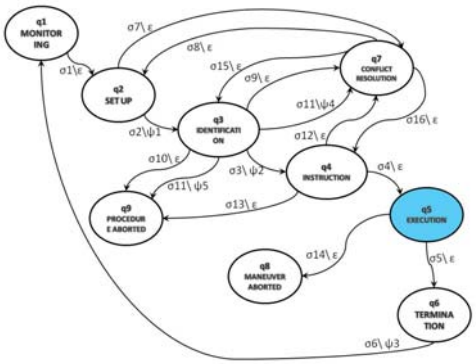

Fig. 3. Hybrid system of the air traffic controller.

- $U_{atc} = \varnothing$ and $Y_{atc} = \varnothing$.
- $\mathcal{E}_{atc} = \varnothing$.
- $\Sigma_{atc} = \{\sigma_i, i = 1, 2, ..., 16\} \cup \{\varepsilon\}$ is the set of discrete inputs, where σ_1 represents the decision to undertake the lateral crossing procedure, σ_2 the ackowledgement of satisfied conditions for the procedure to start, σ_3 the target aircraft correctly identified, σ_4 the communication from the clearance aircraft of executable manoeuvre, σ_5 the communication from the clearance aircraft of COT point passed, σ_6 the resumption of the responsibilities for the control of the separation, σ_7 the conflict detection (conditions for the applicability of the procedure are not satisfied), σ_8 the conflict resolved in phase of set up, σ_9 the communication from the clearance aircraft of unidentified target on board (conflict detection), σ_{10} the communication from the clearance aircraft of decision to undertake the procedure of back up for an unidentified target on board, σ_{11} the target aircraft not correctly identified, σ_{12} the communication from the clearance of not executable instruction (conflict detection), σ_{13} the communication from the clearance aircraft of decision to undertake the procedure of back–up for not executable manoeuvre, σ_{14} the communication from the clearance aircraft of decision to undertake the procedure of back–up for dangerous situation, σ_{15} the conflict resolved in identification phase, σ_{16} the conflict resolved instruction phase.
- E_{atc} is the set of transitions as shown in Figure 3.
- $\Psi_{atc} = \{\Psi_i, i = 1, 2, ..., 5\} \cup \{\varepsilon\}$ is the set of discrete outputs, where Ψ_1 represents the communication to the clearance aircraft of target aircraft candidate to the manoeuvre, Ψ_2 the communication to the clearance of target aircraft correctly identified, Ψ_3 the confirmation to the clearance aircraft of reception of the message of CTO passed, Ψ_4 the communication to the clearance of target not correctly identified, Ψ_5 the order for the clearance aircraft of execution of the procedure of back–up for target not correctly identified.
- $\eta_{atc} : E_{atc} \rightarrow \Psi_{atc}$ is the discrete output function as shown in Figure 3.

The above hybrid model is characterized by no continuous variables and in fact its state space X_{atc} is empty. In ATM systems one air traffic controller is responsible for more than one clearance aircraft flying in his designed sky area. A hybrid system modelling one air traffic controller, responsible for N clearance aircraft can be obtained by composing the hybrid model $\mathcal{H}_{atc}$ with $N-1$ copies of it, resulting in:

$$\underbrace{\mathcal{H}^1_{atc}||\mathcal{H}^2_{atc}||...||\mathcal{H}^N_{atc}}_{N}.$$

C. Hybrid Model of the Lateral Crossing Procedure

Consider a scenario in which N clearance aircraft $\mathcal{H}^1_p, \mathcal{H}^2_p, ..., \mathcal{H}^N_p$ and one ATC $\mathcal{H}_{atc}$ operate. As already discussed in the previous section one ATC interacting with N clearance aircraft can be modelled by the composition of N hybrid models $\mathcal{H}^1_{atc}, \mathcal{H}^2_{atc}, ..., \mathcal{H}^N_{atc}$ that are copies of $\mathcal{H}_{atc}$. The communication scheme that models exchange of information among the agents involved, can be described by the directed graph $\mathbb{F} = (\mathbb{V}, \mathbb{E})$ where:

- $\mathbb{V} = \bigcup_{i=1,...,N}\{\mathcal{H}^i_{atc}, \mathcal{H}^i_p\}$ is the set of vertices.
- $\mathbb{E} = \bigcup_{i=1,...,N}\{(\mathcal{H}^i_{atc}, \mathcal{H}^i_p)\} \cup \bigcup_{i,j=1,...,N}\{(\mathcal{H}^i_{atc}, \mathcal{H}^j_{atc})\}$ is the set of edges.

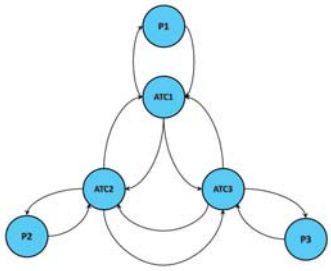

Fig. 4. Interaction of $N = 3$ agents acting in the lateral crossing manouevre.

The resulting graph for $N = 3$ is depicted in Figure 4. By applying the composition rules introduced in Section III-A the hybrid system modelling the interaction of the agents can be defined; we denote such hybrid system by $\mathcal{H}$.

D. Analysis of Critical Observability of the Lateral Crossing Procedure

We now have all the ingredients to study critical observability of the hybrid system $\mathcal{H}$ defined in the previous section. By applying the techniques shown in Section III-B a critical observer $\mathcal{O}$ can be constructed to check critical observability of $\mathcal{H}$. However, the cardinality of the state space of the obtained observer may be intractable from the computational point of view. Suppose for example that $N = 5$ clearance aircraft are involved. Then the cardinality $|Q|$ of the set Q of discrete states of $\mathcal{H}$ is given by

$$|Q| = \prod_{i=1,2,\ldots,5} |Q^i_{atc}| \cdot \prod_{i=1,2,\ldots,5} |Q^i_p| = 9^5 \cdot 15^5 = 4.484 \cdot 10^{10}.$$

It is well known that the cardinality of the set of the discrete states of the critical observer $\mathcal{O}$ for $\mathcal{H}$ grows exponentially with $|Q|$ possibly accounting at $2^{|Q|} = 2^{4.484 \cdot 10^{10}}$ in the worst case. It is clear that the construction of such an observer can be very demanding from the computational point of view. Thus we approach the analysis of critical observability by using the complexity reduction techniques illustrated in Section III-B and summarized in Theorem 1.

As a first step we need to define the critical relation among the agents involved. By analysing the hybrid models of the agents and their interaction the following critical relation is obtained:

$$\mathcal{R} = (\bigcup_{i=1,2,\ldots,N} \mathcal{R}'_{p_i}) \cup (\bigcup_{i,j=1,2,\ldots,N} \mathcal{R}'_{p_i,atc_i,atc_j,p_j}),$$

where $\mathcal{R}_{p_i} = \{q^{p,i}_8, q^{p,i}_{10}, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}\}$ is the set of critical states related to the i–th clearance aircraft and $\mathcal{R}_{p_i,atc_i,atc_j,p_j} = \{q^{p,i}_4, q^{atc,i}_5, q^{atc,j}_5, q^{p,j}_4\}$ is the set of critical states arising from the interaction of the i–th clearance aircraft, the j–th clearance aircraft, the i–th ATC and the j–th ATC.

We now have all the ingredients to study critical observability of the hybrid system $\mathcal{H}$. By applying Theorem 1 it is possible to show that the hybrid system $\mathcal{H}$ is $\mathcal{R}$–critically observable if the following conditions are satisfied:

(C1) $\mathcal{H}^i_p$ is $\mathcal{R}_{p_i}$–critically observable;
(C2) $\mathcal{H}^i_p$ is $\{q^{p,i}_4\}$–critically observable;
(C3) $\mathcal{H}^i_{atc}$ is $\{q^{atc,i}_5\}$–critically observable.

We start by checking condition (C1). By using the results recalled in Section III-B the following observer is obtained:

$$O_{p_i} = (\hat{Q}_{p_i}, \hat{Q}_{0p_i}, \hat{\Sigma}_{p_i}, \hat{\Psi}_{p_i}, \hat{E}_{p_i}, \hat{\eta}_{p_i})$$

where:

- $\hat{Q}_{p_i} = \{\{q^{p,i}_1, q^{p,i}_2, q^{p,i}_3, q^{p,i}_6, q^{p,i}_{11}\}, \{q^{p,i}_{11}\}, \{q^{p,i}_3, q^{p,i}_6\}, \{q^{p,i}_7\}, \{q^{p,i}_4, q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}\}, \{q^{p,i}_5, q^{p,i}_{10}\}, \{q^{p,i}_9\}\}$.
- $\hat{Q}_{0p_i} = \{\{q^{p,i}_1, q^{p,i}_2, q^{p,i}_3, q^{p,i}_6, q^{p,i}_{11}\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi}_{p_i} = \hat{Q}_{p_i}$.
- $\hat{E}_{p_i}$ is depicted in Figure 5 (Left panel).
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_{p_i}$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 5 (Left panel) shows that $\mathcal{H}^i_p$ is not $\mathcal{R}_{p_i}$–critically observable. Indeed when the state of $\mathcal{O}_{p_i}$ is in $\{q^{p,i}_4, q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}\}$ it is not possible to distinguish the critical states $q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}$ from the noncritical state $q^{p,i}_4$. Analogously when the state of $\mathcal{O}_{p_i}$ is in $\{q^{p,i}_5, q^{p,i}_{10}\}$, it is not possible to distinguish the critical state $q^{p,i}_{10}$ from the noncritical state $q^{p,i}_5$. In order to render the hybrid model $\mathcal{H}^i_p$, $\mathcal{R}_{p_i}$–critically observable, extra discrete–outputs are needed, and can be designed as follows. We define a partial function $h_p : Q_p \to \Psi_p$ that associates to each state $q \in Q_p$ an additional discrete output symbol $h(q) \in \Psi_p$ in order to detect when the execution reaches one of the critical discrete states $q^{p,i}_8$, $q^{p,i}_{12}$, $q^{p,i}_{13}$, $q^{p,i}_{14}$, $q^{p,i}_{15}$ or $q^{p,i}_{10}$. The extra outputs $h(q^{p,i}_8)$, $h(q^{p,i}_{14})$ and $h(q^{p,i}_{15})$ can be generated using an alarm generated from the ASSAP function alert. The extra output $h(q^{p,i}_{13})$ can be generated through an alarm from ground surveillance systems. The extra output $h(q^{p,i}_{12})$ and $h(q^{p,i}_{10})$ can be obtained by using information coming from the ground systems. The generation of these extra outputs requires a time delay which affects the rapidity of detection of the critical states. The observer with delay associated with agent $\mathcal{H}^i_p$ and critical relation $\mathcal{R}_{p_i}$ is illustrated in Figure 5 (Right panel). The obtained observer is now critical in the sense that it is possible to detect when the discrete state reaches the set of critical states after the bounded time delay needed for the generation of the extra outputs.

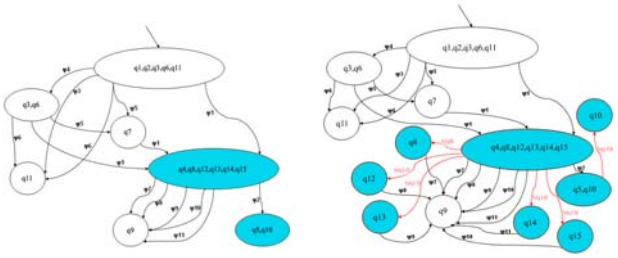

Fig. 5. Left panel: $\mathcal{R}_{p_i}$–critical observer for hybrid system $\mathcal{H}^i_p$. Right panel: $\mathcal{R}_{p_i}$–critical observer with delay for hybrid system $\mathcal{H}^i_p$.

We proceed one step further by checking condition (C2). By using the results recalled in Section III-B the following observer is obtained:

$$\mathcal{O}_{p_i} = (\hat{Q}_{p_i}, \hat{Q}_{0p_i}, \hat{\Sigma}_{p_i}, \hat{\Psi}_{p_i}, \hat{E}_{p_i}, \hat{\eta}_{p_i})$$

where:

- $\hat{Q}_{p_i} = \{\{q^{p,i}_1, q^{p,i}_2, q^{p,i}_3, q^{p,i}_6, q^{p,i}_{11}\}, \{q^{p,i}_{11}\}, \{q^{p,i}_3, q^{p,i}_6\}, \{q^{p,i}_7\}, \{q^{p,i}_4, q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}\}, \{q^{p,i}_5, q^{p,i}_{10}\}, \{q^{p,i}_9\}\}$.
- $\hat{Q}_{0p_i} = \{\{q^{p,i}_1, q^{p,i}_2, q^{p,i}_3, q^{p,i}_6, q^{p,i}_{11}\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi}_{p_i} = \hat{Q}_p$.
- $\hat{E}_{p_i}$ is depicted in Figure 6 (Left panel).
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_p$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 6 (Left panel), shows that $\mathcal{H}^i_p$ is not critically observable with respect to the set of critical states $\{q^{p,i}_4\}$. Indeed when the state of the critical observer $\mathcal{O}_{p_i}$ is in $\{q^{p,i}_4, q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}\}$ it is not possible to distinguish the critical state $q^{p,i}_4$ from the noncritical state $q^{p,i}_8, q^{p,i}_{12}, q^{p,i}_{13}, q^{p,i}_{14}, q^{p,i}_{15}$. In order to render the

hybrid model $\mathcal{H}_p^i$ critically observable the extra discrete output $h(q_4^{p,i})$ is needed to be designed; this can be done by using an alarm generated from ground surveillance systems. The obtained critical observer with delay is depicted in Figure 6 (Right panel).

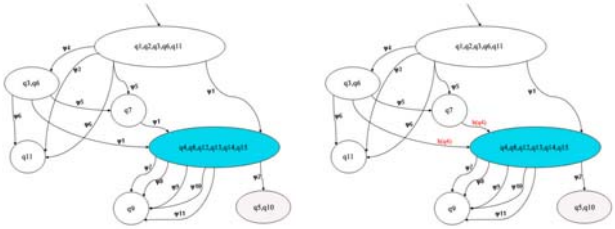

Fig. 6. Left panel: $\{q_4^{p,i}\}$–critical observer for $\mathcal{H}_p^i$. Right panel: $\{q_4^{p,i}\}$–critical observer with delay for $\mathcal{H}_p^i$.

We conclude by checking condition (C3). By using the results recalled in Section III-B the following observer is obtained:

$$\mathcal{O}_{atc} = (\hat{Q}_{atc}, \hat{Q}_{0atc}, \hat{\Sigma}_{atc}, \hat{\Psi}_{atc}, \hat{E}_{atc}, \hat{\eta}_{atc}),$$

where:

- $\hat{Q}_{atc} = \{\{q_1, q_2, q_7\}, \{q_3, q_7, q_9\}, \{q_7\}, \{q_9\}, \{q_4, q_5, q_6, q_7, q_8, q_9\}, \{q_1\}\}$.
- $\hat{Q}_{0atc} = \{\{q_1, q_2, q_7\}\}$.
- $\hat{\Sigma}_{atc} = \Psi_{atc}$.
- $\hat{\Psi}_{atc} = \hat{Q}_{atc}$.
- $\hat{E}_{atc}$ is depicted in Figure 7 (Left panel).
- $\hat{\eta}_{atc}(\hat{q}) = \hat{q}$, for any $\hat{q} \in \hat{Q}_{atc}$.

The observer $\mathcal{O}_{atc}$ illustrated in Figure 7 (Left panel), shows that $\mathcal{H}_{atc}$ is not critically observable with respect to the set of critical states $\{q_5^{atc}\}$ because it fails in distinguishing between the critical states q_5^{atc} and the noncritical states $q_4^{atc}, q_6^{atc}, q_7^{atc}, q_8^{atc}, q_9^{atc}$. By proceeding as in the previous cases it is possible to render the hybrid system $\mathcal{H}_{atc}$ critically observable with respect to $\{q_5^{atc}\}$ by introducing an extra discrete–output $h(q_5^{atc})$; such extra output can be generated by the technical instrumentations. The obtained critical observer with delay is illustrated in Figure 7 (Right panel).

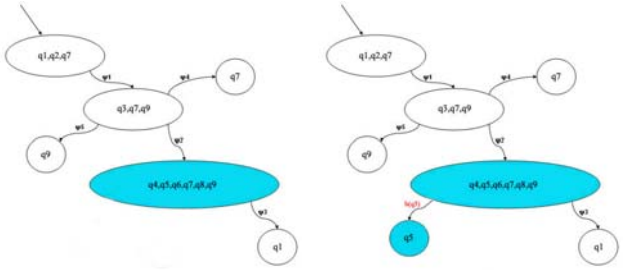

Fig. 7. Left panel: $\{q_5^{atc,i}\}$–critical observer for $\mathcal{H}_{atc}^i$. Right panel: $\{q_5^{atc,i}\}$–critical observer with delay for $\mathcal{H}_{atc}^i$.

The analysis that we performed highlights that the Lateral Crossing Procedure is not critically observable in the sense that not all unsafe and/or unallowed operations by the agents can be detected. However, provided that additional signals can be generated, as detailed in the above analysis, the procedure can be made critically observable. We stress that the above analysis has been carried out for a scenario in which an arbitrary large number of agents operate.

V. Conclusion

We presented a compositional hybrid system framework for modeling ATM systems in a multi–agent environment and addressed the analysis of critical observability of the composed hybrid system to detect critical events that may lead to catastrophic events. Since the computational effort required in the formal analysis of such systems was shown to be intractable in realistic scenarios, we derived some theoretical results that are used to substantially reduce the effort in checking such observability property. The benefits from the use of the proposed methodology were illustrated in the analysis of the Lateral Crossing Procedure.

Acknowledgments

This work was partially supported by European Commission under STREP project IFLY. The authors are grateful to Pascal Lezaud and Thierry Miguel for suggesting the lateral crossing case study and providing the reference [LMH+05], and to Alessandro D'Innocenzo and Valentina D'Alessandro for useful insights on the content of the paper.

References

[BGD09] M.D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Discrete state observability of hybrid systems. *International Journal of Robust and Nonlinear Control*, 19(14):1564–1580, 2009. Special Issue on Observability and Observer Design for Hybrid Systems.

[CD08] M. Colageo and A. Di Francesco. Hybrid system framework for the safety modelling of the in trail procedure. In *ICRAT 2008 - 3rd International Conference on Research in Air Transportation, Fairfax, Virginia, USA*, June 01-04 2008.

[DDD+05] E. De Santis, M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, and G. Pola. Critical observability of a class of hybrid systems and application to air traffic management. *Book Chapter of Lecture Notes on Control and Information Sciences, Springer Verlag*, 2005.

[DDP08] M.D. Di Benedetto, A. D'Innocenzo, and A. Petriccone. Automatic verification of temporal properties of air traffic management procedures using hybrid systems. In *EUROCONTROL Innovative ATM Research Workshop Exhibition*, December 2008.

[GL04] W. Glover and J. Lygeros. A multi-aircraft model for conflict detection and resolution algorithm evaluation. Deliverable 1.3, Project IST-2001-32460 HYBRIDGE, 18 February 2004.

[HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison–Wesley, 1979.

[LMH+05] J.M. Loscos, T. Miquel, B. Hasquenoph, B. Gayraud, S. Chabert, and B. Raynaud. D1.3 specific and detailed conditions of use for applicability to radar airspace. Technical report, 17 April 2005. ASSTAR, AST4-CT-2005-516140.

[LTS99] J. Lygeros, C. Tomlin, and S. Sastry. Controllers for reachability specications for hybrid systems. *Automatica, Special Issue on Hybrid Systems*, 35, 1999.

[SBdP03] S. Stroeve, H.A.P. Blom, and M. Van der Park. Multi–agent situation awareness error evolution in accident risk modelling. *FAA–Eurocontrol, ATM2003*, http://atm2003.eurocontrol.fr/, 2003.