A Complexity Reduction Approach to the Detection of Safety Critical Situations in Air Traffic Management Systems

Alessandro Petriccone, Giordano Pola, Maria D. Di Benedetto, Elena De Santis

***Abstract*— In Air Traffic Management (ATM) systems, catastrophic events are often caused by errors made by agents operating in the procedures. Detecting safety critical situations that may arise in the evolution of ATM systems is of primary importance in the analysis of their behavior. The inherent complexity of ATM systems, typically involving a large number of agents, makes this analysis prohibitive today. Compositionality has been an effective way of tackling this problem. We present a compositional hybrid systems framework to accurately describe the behavior of the agents operating in ATM scenarios and of their interaction. We then expose some results that reduce the computational effort required in detecting safety critical situations. Benefits from the use of this complexity reduction approach are illustrated using the analysis of the Airborne Separation–In Trail Procedure (ASEP–ITP).**

keywords: Air traffic management systems, hybrid systems, critical observability, computational complexity reduction, airborne separation in–trail procedure.

I. Introduction

The volume of air traffic is increasing so rapidly that a major efficiency overhaul to manage air traffic flows is necessary to maintain normal operation. This issue suggested to many researchers in the area of Air Traffic Management (ATM) systems new procedures with the aim of increasing capacity while preserving safety. This is particularly relevant since the more capacity increases, the more complex the air traffic management system becomes, thus making a formal approach to safety analysis very difficult. Factors which further complicate this formal analysis are heterogeneity in the mathematical models of the agents involved and the number of agents which is very large in realistic ATM scenarios. In our previous work [1], [2], [3] we showed the benefits from the use of hybrid system formalism to model agents in ATM systems and we analyzed the occurrence of unsafe or unallowed situations by making use of the notion of critical observability studied in [4], [5]. The main drawback of the approach presented in [1], [2] is that the different agents acting in ATM scenarios are considered as isolated systems. This drawback is particularly relevant because agents' interaction is responsible of the occurrence of unsafe situations that cannot be captured when considering different agents in isolation. In this paper, we overcome the limits of the previous work in [1], [2] by studying ATM scenarios in which interaction among the agents is formally analyzed. We first introduce a compositional hybrid systems framework which accurately describes the behavior of the agents operating in ATM scenarios and their interaction. In particular, we introduce a notion of composition among hybrid systems which has been inspired by the notion of parallel composition in automata theory [6] and by the one of switching systems in [7]. This mathematical framework allows us to formally analyze and detect the occurrence of unsafe and of unallowed events for each agent, and for the interaction of the agents. Although this approach is formally correct, it is applicable only with great difficulty to realistic ATM scenarios with a large number of agents. This drawback motivated us to look for ways for reducing this computational complexity. In this paper we present results in complexity reduction and the analysis of the Airborne Separation In Trail Procedure [8], [9] is used to demonstrate their applicability. We also present a detailed description of the preliminary results presented in [3].

This work has been partially supported by European Commission under STREP project IFLY and by the Center of Excellence for Research DEWS, University of L'Aquila, Italy.

The authors are with the Department of Electrical and Information Engineering, Center of Excellence DEWS, University of L'Aquila, 67100 L'Aquila, Italy, {alessandro.petriccone,giordano.pola,mariadomenica.dibenedetto,elena.desantis}@univaq.it.

II. Compositional Hybrid Systems and Critical Observability

A. Compositional Hybrid Systems

Consider a scenario characterized by $N \geq 1$ agents, each one modelled by a hybrid system [10]

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

where Q_i is a finite set of M discrete states and $X_i \subseteq \mathbb{R}^n$ is the continuous state space, $Q_{0,i} \times X_{0,i} \subseteq Q_i \times X_i$ is the set of initial discrete and continuous conditions, $U_i \subseteq \mathbb{R}^m, Y_i \subseteq \mathbb{R}^p$ are the sets of continuous control inputs and outputs, $\{\mathcal{E}_i^q\}_{q \in Q_i}$ associates to each discrete state $q \in Q_i$ the continuous dynamics $\dot{x} = f_i^q(x,u)$, with output $y = g_i^q(x)$, $\Sigma_i \cup \{\varepsilon\}$ is the set of discrete inputs, where the empty string ε corresponds to the null input, $E_i \subseteq Q_i \times \Sigma_i \times Q_i$ is a collection of edges, $\Psi_i \cup \{\varepsilon\}$ is the set of discrete outputs, where the empty string ε corresponds to the null output, $\eta_i \colon E_i \to \Psi_i$ is the output function, that associates to each edge a discrete output symbol. The evolution in time of hybrid systems is described by the classical notion of execution [10] which we briefly recall hereafter. A *hybrid time basis* $\tau = \{I_k\}_{0 \leq k \leq |\tau|}$ is a finite or infinite sequence of intervals $I_k = [t_k, t'_k]$ satisfying the following conditions: (i) $t_k \leq t'_k$ for $k > 0$, and $t'_{k-1} = t_k$ for $k > 1$; (ii) if the sequence $\{I_k\}_{0 \leq k \leq |\tau|}$ is infinite, then I_k is closed for all k; (iii) if the sequence $\{I_k\}_{0 \leq k \leq |\tau|}$ is finite, then the last

interval $I_{|\tau|}$ might be right–open. A *hybrid execution* is a triple $\chi = (\tau, q, x)$, where τ is a hybrid time basis, and q, x describe the evolution of the discrete and continuous states by means of functions $q\colon \tau \to Q$ and $x\colon \tau \to X$. Functions q, x satisfy the continuous and discrete dynamics and their interactions.

The communication scheme that models the exchange of information among agents $\mathcal{H}_i$ 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 and $\mathbb{E} \subseteq \mathbb{V} \times \mathbb{V}$ is the set of edges, so that $(\mathcal{H}_i, \mathcal{H}_j) \in \mathbb{E}$, if $\mathcal{H}_i$ interacts with[1] $\mathcal{H}_j$. The evolution of each hybrid system $\mathcal{H}_i$ depends on the information that $\mathcal{H}_i$ receives from all hybrid systems $\mathcal{H}_j$ sharing information with it, i.e. all $\mathcal{H}_j$ for which $(\mathcal{H}_j, \mathcal{H}_i) \in \mathbb{E}$. We partition the sets of discrete inputs and of discrete outputs of each hybrid system, 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 $\mathcal{H}_j$.

The interaction among hybrid systems $\mathcal{H}_i$ can be captured by the following notion of composition. Given a communication scheme $\mathbb{V}$, 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:

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

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 in $\mathcal{H}_1 || \mathcal{H}_2 || \ldots || \mathcal{H}_N$, if one of the following conditions are satisfied:

- $\eta_i(e_i) \in \Psi_i^j \wedge \eta_i(e_i) = \sigma_j \wedge \sigma_j \in \Sigma_j^j \wedge \eta_j(e_j) \neq \sigma_i \wedge \eta_k(e_k) \neq \sigma_j \ \forall k \neq i, j$; for $i, j, k \in \{1, 2, \ldots, N\}$ with $i \neq j$. This condition models the situation in which $\mathcal{H}_i$ communicates an action and/or information $\eta_i(e_i) = \sigma_j$ to $\mathcal{H}_j$ that evolves according to this information;
- $\eta_i(e_i) \in \Psi_i^i \wedge \eta_i(e_i) \neq \sigma_j$, for $i, j \in \{1, 2, \ldots, N\}$ with $i \neq j$. This condition models the situation in which $\mathcal{H}_i$ evolves according to its own plan without interacting with any other $\mathcal{H}_j$.

The above notion composition has been inspired by the notion of parallel composition in automata theory [6] and by the one for switching systems introduced in [7].

B. Critical Observability

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 $\mathcal{H}$. System $\mathcal{H}$ is said to be $\mathcal{R}$–critically observable if it is possible to determine whether the current discrete state of $\mathcal{H}$ belongs to $\mathcal{R}$ using output information. As shown in [4], [5], conditions for checking critical observability of hybrid systems rely upon construction of observers for discrete event systems, see e.g. [11]. Given a hybrid system $\mathcal{H}$, an observer for $\mathcal{H}$ is described by the following tuple:

$$\mathcal{O} = (\hat{Q}, \hat{Q}_0, \hat{\Sigma}, \hat{\Psi}, \hat{E}, \hat{\eta}), \tag{1}$$

where $\hat{Q} \subseteq 2^Q$ is a set of states, $\hat{Q}_0 \subseteq Q$ 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, and $\hat{\eta} : \hat{Q} \to \hat{\Psi}$ is the output function which coincides with the identity function. Techniques to construct observers are well–known in the literature, see e.g. [11]. We can now give the following:

Definition 1: Given a hybrid system $\mathcal{H}$ and a critical relation $\mathcal{R}$, an $\mathcal{R}$–critical observer is an observer $\mathcal{O}_\mathcal{R}$ of the form (1), whose input $\hat{\sigma} \in \hat{\Sigma}$ is the output of $\mathcal{H}$ and whose output $\hat{\psi} \in \hat{\Psi}$ is such that for any $k \geq 0$, $\hat{\psi}(k) = 1$, if $q(I_k) \in \mathcal{R}$ and $\hat{\psi}(k) = 0$, if $q(I_k) \notin \mathcal{R}$ where $q(I_k)$ is the discrete state of $\mathcal{H}$ in the time interval $I_k = [t_k, t'_k]$. System $\mathcal{H}$ is said to be $\mathcal{R}$–critically observable if an $\mathcal{R}$–critical observer $\mathcal{O}_\mathcal{R}$ exists.

For a detailed analysis of critical observability of hybrid systems we refer to [4], [5]. It is readily seen that the size of $\hat{Q}$ of $\mathcal{O}_\mathcal{R}$ grows exponentially with the size of the set Q of discrete states of $\mathcal{H}$, i.e. the computational complexity of $\mathcal{O}_\mathcal{R}$ is $O(|2^Q|)$. If a hybrid system $\mathcal{H}$ is not $\mathcal{R}$–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 [12].

Results established in [4], [5] can also be used to study critical observability of compositional hybrid systems. Consider the composed hybrid system $\mathcal{H} = \mathcal{H}_1 || \mathcal{H}_2 || ... || \mathcal{H}_N$. The set of critical states associated with the composed system $\mathcal{H}$ can be defined by means of the relation

$$\mathcal{R} \subseteq Q_1 \times Q_2 \times ... \times Q_N, \tag{2}$$

[1]Note that according to this definition, while $\mathcal{H}_i$ interacts with $\mathcal{H}_j$ the converse interaction cannot hold in general.

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 $\mathcal{H}$. Assessing $\mathcal{R}$–critical observability of $\mathcal{H}$ may be computationally demanding if the number of the agents $\mathcal{H}_i$ involved is large. We therefore propose now a method which substantially reduces the computational effort required in checking critical observability. The key idea in the subsequent results is the decomposition of the critical relation $\mathcal{R}$ defined in (2) into critical sub–relations.

Definition 2: Consider a compositional hybrid system framework in which N hybrid systems $\mathcal{H}_i$ interact and consider the following sequence of sets:

- $\mathcal{R}_{i_1} \subseteq Q_{i_1}$ is the set of critical states for $\mathcal{H}_{i_1}$;
- $\mathcal{R}_{i_1,i_2} \subseteq Q_{i_1} \times Q_{i_2}$ is the set of critical states for $\mathcal{H}_{i_1}||\mathcal{H}_{i_2}$;
  ...
- $\mathcal{R}_{i_1,i_2,...,i_N} \subseteq Q_{i_1} \times Q_{i_2} \times \ldots \times Q_{i_N}$ is the set of critical states for $\mathcal{H}_{i_1}||\mathcal{H}_{i_2}||...||\mathcal{H}_{i_N}$.

The information contained in the critical relation $\mathcal{R}$ of (2) can been decomposed into the ones contained in the sequence of sets defined above, as follows.

Lemma 1: Define the following sequence of sets:

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

Then,

$$\mathcal{R} = (\bigcup_{i_1} \mathcal{R}'_{i_1}) \cup (\bigcup_{i_1,i_2} \mathcal{R}'_{i_1,i_2}) \cup \ldots \cup (\bigcup_{i_1,i_2,...,i_N} \mathcal{R}'_{i_1,i_2,...,i_N}). \tag{3}$$

Before stating the main result of this section we need some preliminary results, which we report hereafter.

Proposition 1: Consider a hybrid system $\mathcal{H}$ and a set of critical states $\mathcal{R}$. Suppose that $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$. Then $\mathcal{H}$ is $\mathcal{R}$–critically observable if $\mathcal{H}$ is $\mathcal{R}_1$–critically observable and $\mathcal{R}_2$–critically observable.

Proposition 2: Consider a pair of hybrid systems $\mathcal{H}_1$ and $\mathcal{H}_2$ and the sets of critical states $\mathcal{R}_1 \subseteq Q_1$ and $\mathcal{R}_2 \subseteq Q_2$ for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. The composed system $\mathcal{H}_1||\mathcal{H}_2$ is $\mathcal{R}_1 \times \mathcal{R}_2$–critically observable if $\mathcal{H}_1$ is $\mathcal{R}_1$–critically observable and $\mathcal{H}_2$ is $\mathcal{R}_2$–critically observable.

We can now give the main result of this section.

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 iff 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 $i_1, i_2, ..., i_N = 1, 2, ..., N$.

III. Airborne Separation - In Trail Procedure

In this section we show the benefits and applicability of our results to the analysis of ATM systems, by applying them to the Airborne Separation–In Trail Procedure (ASEP-ITP) [8], [9]. The In Trail Procedure (ITP) is part of the *Airborne Separation Assistance Systems (ASAS)*. ASAS embraces the goal of improving flight management by introducing a stronger interaction between pilots and controllers. The In Trail Procedure is seen as an *Airborne Separation (ASEP) Application* which is one of the four ASAS application categories. ASEP–ITP applications involve the transfer of responsibilities for the separation from the controller to the flight crew during the execution of the procedure. This can happen when the flight crew have more appropriate surveillance equipments (i.e. ADS-B and ASAS equipment) and is therefore able to monitor separation and act, if necessary. The ASEP-ITP is a procedure that aims at improving flight efficiency along oceanic routes where procedural control is performed. The procedure provides a safe and practical method for air traffic controller to approve, and flight crew to perform climb and descent manoeuvers through different flight levels with less stringent applicability conditions than today's operations. The ASEP-ITP mathematical model can be decomposed in various subsystems representing the agents involved in the procedure, i.e. Air crew flying of ASEP-ITP aircraft (ITP aircraft), Reference Aircraft and Oceanic controller. In the following we do not model the reference aircraft as an agent because its flight crew does not have the awareness of existence of an ASEP-ITP manoeuvre in which it is involved. Hybrid modeling of the ASEP–ITP procedure has already been introduced in [2] and used for the automatic verification of temporal safe properties of the procedure, through the toolbox UPPAAL.

A. Pilot flying of ITP aircraft Agent

The hybrid model of the agent Pilot Flying is given by:

$$\mathcal{H}_p = (Q_p \times X_p, Q_{p,0} \times X_{p,0}, U_p, Y_p, \mathcal{E}_p, \Sigma_p, E_p, \Psi_p, \eta_p) \tag{4}$$

where:

- $Q_p = \{q_{p,i}, i = 1, 2, ..., 13\}$ where $q_{p,1}$ is the normal cruise, $q_{p,2}$ the ITP aborted, $q_{p,3}$ the ITP initiation, $q_{p,4}$ the ITP instruction, $q_{p,5}$ the ITP rejected, $q_{p,6}$ the ITP denied, $q_{p,7}$ the ITP standard execution, $q_{p,8}$ the non ITP criteria compliant execution, $q_{p,9}$ the wrong execution, $q_{p,10}$ the wrong termination, $q_{p,11}$ is the abnormal termination, $q_{p,12}$ the ITP termination, $q_{p,13}$ the execution after ASAS conflict detection.
- $X_p \subset \mathbb{R}^6$ where $x = (x_1, x_2, x_3, x_4, x_5, x_6) \in X_p$, where x_1 and x_2 indicate the horizontal position, x_3 is the altitude, x_4 is the true airspeed, x_5 is the heading angle and x_6 is the flight path angle.
- $Q_{p,0} = \{q_1\}$ and $X_{p,0} = \{(x_0, z_i, v_{x0}, 0)\}$.
- $U_p \subset \mathbb{R}^3$ where $u = (u_1, u_2, u_3) \in U_p$, where u_1 is the engine thrust, u_2 is the bank angle and u_3 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 $f_{q_i}(x)$ is given [13] for any $i = 1, 2, ..., 13$ by:

$$\begin{cases} \dot{x_1} = x_4 \cos(x_5)\cos(x_6) \\ \dot{x_2} = x_4 \sin(x_5)\cos(x_6) \\ \dot{x_3} = x_4 \sin(\alpha) \\ \dot{x_4} = \frac{1}{m}(u_1 \cos(\alpha) - D - mg\sin(x_6)) \\ \dot{x_5} = \frac{1}{mx_4}(L\sin(u_2) + u_1 \sin(\alpha)\sin(u_2)) \\ \dot{x_6} = \frac{1}{mx_4}(L + u_1 \sin(\alpha))\cos(u_2) - mg\cos(u_3)) \end{cases}$$

  where L is the lift force, D the drag force, α the angle of attack, g gravitational acceleration.
- $\Sigma_p = \{\sigma_{p,i}, i = 1, 2, ..., 9\} \bigcup \{\varepsilon\}$, where $\sigma_{p,1}$ represents the verification of ITP pre-conditions, $\sigma_{p,2}$ the reassessment failed after a clearance reception, $\sigma_{p,3}$ the ITP criteria not verified, $\sigma_{p,4}$ the ITP criteria verified, $\sigma_{p,5}$ the clearance denied, $\sigma_{p,6}$ the clearance issued, $\sigma_{p,7}$ the detection of an abnormal event, $\sigma_{p,8}$ a situational awareness inconsistency, $\sigma_{p,9}$ an ASAS conflict detection communication, ε an internal event.
- E_p is the set of transitions given by the graph depicted in Figure 1 - Left panel.
- $\Psi_p = \{\psi_{p,i}, i = 1, 2, ..., 7\} \cup \{\varepsilon\}$, where $\psi_{p,1}$ represents the clearance rejected by the crew, $\psi_{p,2}$ the clearance request, $\psi_{p,3}$ the setting of flight parameters for the climb, $\psi_{p,4}$ the abnormal termination communication by the crew to the controller, $\psi_{p,5}$ the report established at the new flight level, $\psi_{p,6}$ the reversion to cruise operation, $\psi_{p,7}$ the setting of flight parameters to solve an ASAS conflict detection, ε an unobservable transition.
- η_p is the output function defined in the graph depicted in Figure 1 - Left panel.

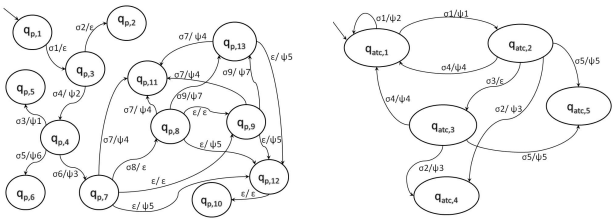

Fig. 1. Left panel: Directed graph of pilot flying of ITP aircraft agent. Right panel: Directed graph of the Air Traffic Controller.

B. Air Traffic Controller

The hybrid model of the air traffic controller is given by the hybrid system $\mathcal{H}_{atc}$ consisting in the tuple:

$$(Q_{atc} \times X_{atc}, Q_{atc,0} \times X_{atc,0}, U_{atc} \times Y_{atc}, \mathcal{E}_{atc}, \Sigma_{atc}, E_{atc}, \Psi_{atc}, \eta_{atc}) \quad (5)$$

where:

- $Q_{atc} = \{q_{atc,i}, i = 1, 2, ..., 5\}$, where $q_{atc,1}$ is the monitoring of the airspace, $q_{atc,2}$ the clearance issued, $q_{atc,3}$ the wrong clearance issued, $q_{atc,4}$ the abnormal termination, $q_{atc,5}$ the clearance refused; $X_{atc} = \varnothing$.
- $Q_{atc,0} = \{q_{atc,1}\}$ and $X_{atc,0} = \varnothing$.
- $U_{atc} = \varnothing$ and $Y_{atc} = \varnothing$.
- $\mathcal{E}_{atc} = \varnothing$.
- $\Sigma_{atc} = \{\sigma_{atc,i}, i = 1, 2, ..., 5\}$, where $\sigma_{atc,1}$ represents the request of an ITP, $\sigma_{atc,2}$ the abnormal termination communication, $\sigma_{atc,3}$ a situational awareness inconsistency, $\sigma_{atc,4}$ the communication by the crew of the establishment at the new flight level, $\sigma_{atc,5}$ is the message of rejection of the clearance by the aircrew.
- E_{atc} is the set of transitions given by the graph depicted in Figure 1 - Right panel.
- $\Psi_{atc} = \{\psi_{atc,1}, i = 1, 2, ..., 5\} \cup \{\varepsilon\}$, where $\psi_{atc,1}$ represents the clearance issued, $\psi_{atc,2}$ the ITP request denied, $\psi_{atc,3}$ the communication to the aircrew of the abnormal termination message reception, $\psi_{atc,4}$ the confirmation of the reception of a standard ITP termination message, $\psi_{atc,5}$ the confirmation of the reception of the rejection of the clearance by the aircrew, ε is associated with an unobservable transition.
- $\eta_{atc} : E_{atc} \to \Psi_{atc}$, is the discrete output function defined in the graph depicted in Figure 1 - Right panel.

In ATM systems one air traffic controller is responsible for more than one clearance aircraft flying in his designed sky area. A hybrid system modeling 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 $\mathcal{H}^1_{atc}||\mathcal{H}^2_{atc}||...||\mathcal{H}^N_{atc}$.

IV. Analysis of Critical Observability of the ASEP-ITP

Consider a scenario in which 4 ITP aircraft $\mathcal{H}^1_p, \mathcal{H}^2_p, \mathcal{H}^3_p, \mathcal{H}^4_p$ and one ATC $\mathcal{H}_{atc}$ operate. As stressed in the previous section, one ATC interacting with 4 ITP aircraft can be modeled by means of the composition of 4 hybrid systems $\mathcal{H}^1_{atc}, \mathcal{H}^2_{atc}, \mathcal{H}^3_{atc}, \mathcal{H}^4_{atc}$. Hybrid models of $\mathcal{H}^i_p$ and $\mathcal{H}^i_{atc}$ coincide with the ones in (4) and (5), respectively. In the further developments we refer to state $q_{p,j}$ of $\mathcal{H}^i_p$ by $q^i_{p,j}$ and to state $q_{atc,j}$ of $\mathcal{H}^i_{atc}$ by $q^i_{atc,j}$. 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 $\mathbb{V} = \bigcup_{i=1,...,4}\{\mathcal{H}^i_{atc}, \mathcal{H}^i_p\}$ and $\mathbb{E} = \bigcup_{i=1,...,4}\{(\mathcal{H}^i_{atc}, \mathcal{H}^i_p)\} \cup \bigcup_{i,j=1,...,4}\{(\mathcal{H}^i_{atc}, \mathcal{H}^j_{atc})\}$. The hybrid system resulting from the composition of agents $\mathcal{H}^i_p$ and $\mathcal{H}^i_{atc}$ is given by:

$$\mathcal{H} = \mathcal{H}^1_p||\mathcal{H}^2_p||\mathcal{H}^3_p||\mathcal{H}^4_p||\mathcal{H}^1_{atc}||\mathcal{H}^2_{atc}||\mathcal{H}^3_{atc}||\mathcal{H}^4_{atc}. \quad (6)$$

The next step in the analysis of the ASEP–ITP is the definition of the critical relation $\mathcal{R}$, resulting in:

$$\begin{aligned} \mathcal{R} \;=\; & (\bigcup_{p_i} \mathcal{R}'_{p_i}) \cup \\ & (\bigcup_{p_i,p_j,atc_i,atc_j} \mathcal{R}'_{p_i,p_j,atc_i,atc_j}) \cup \\ & (\bigcup_{p_i,p_j,p_k,atc_i,atc_j,atc_k} \mathcal{R}'_{p_i,p_j,p_k,atc_i,atc_j,atc_k}) \cup \\ & \mathcal{R}'_{p_1,p_2,p_3,p_4,atc_1,atc_2,atc_3,atc_4}, \end{aligned}$$

where:

- $\mathcal{R}_{p_i} = \{q^i_{p,8}, q^i_{p,9}, q^i_{p,10}\}$;
- $\mathcal{R}_{p_i,p_j,atc_i,atc_j} = \{q^i_{p,7}, q^j_{p,7}, q^i_{atc,3}, q^j_{atc,3}\}$;

- $\mathcal{R}_{p_i,p_j,p_k,atc_i,atc_j,atc_k} = \{q^i_{p,7}, q^j_{p,7}, q^k_{p,7}, q^i_{atc,3}, q^j_{atc,3}, q^k_{atc,3}\}$;
- $\mathcal{R}_{p_1,p_2,p_3,p_4,atc_1,atc_2,atc_3,atc_4} = \{q^1_{p,7}, q^2_{p,7}, q^3_{p,7}, q^4_{p,7}, q^1_{atc,3}, q^2_{atc,3}, q^3_{atc,3}, q^4_{atc,3}\}$.

Second, third and fourth critical relations model the situation in which the ATC asks at the same time to more than one aircraft to execute the ASEP–ITP and this can result in being safety critical.

Step 0. A critical observer $\mathcal{O}$ can be constructed to check critical observability of $\mathcal{H}$ in (6). However, the cardinality of the state space of the obtained observer may be intractable from the computational point of view. In fact, the cardinality $|Q|$ of the set Q of discrete states of $\mathcal{H}$ is given by, $|Q| \simeq 1.78 \cdot 10^7$, which may imply a cardinality of the state space 2^Q of $\mathcal{O}$, possibly amounting to $2^{|Q|} \simeq 1.03 \cdot 10^{5358034}$ 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 II-B, as follows:

Step 1. Since $\mathcal{R}'_{p_i,p_j,p_k,atc_i,atc_j,atc_k} \subset \mathcal{R}'_{p_i,p_j,atc_i,atc_j}$ and $\mathcal{R}'_{p_1,p_2,p_3,p_4,atc_1,atc_2,atc_3,atc_4} \subset \mathcal{R}'_{p_i,p_j,atc_i,atc_j}$, by applying Proposition 1, the hybrid system $\mathcal{H}$ in (6) is $\mathcal{R}$–critically observable iff it is critically observable w.r.t. the critical relation:

$$\mathcal{R} = (\bigcup_{p_i} \mathcal{R}'_{p_i}) \cup (\bigcup_{p_i,p_j,atc_i,atc_j} \mathcal{R}'_{p_i,p_j,atc_i,atc_j}).$$

By applying Theorem 1 the hybrid system $\mathcal{H}$ is $\mathcal{R}$–critically observable iff:

(C1) $\mathcal{H}^i_p$ is $\mathcal{R}_{p_i}$–critically observable.

(C2) $\mathcal{H}^i_p||\mathcal{H}^j_p||\mathcal{H}^i_{atc}||\mathcal{H}^j_{atc}$ is $\mathcal{R}_{p_i,p_j,atc_i,atc_j}$–critically observable.

Since $|Q_p| = 13$ and the number of aircraft involved is 4, the computational complexity in checking condition (C1) is $O(32768)$; regarding condition $(C2)$ the cardinality of $|Q^i_p \times Q^j_p \times Q^i_{atc} \times Q^j_{atc}| = 4225$ and the computational complexity in the construction of the critical observer is therefore given by $O(|2^{Q^i_p \times Q^j_p \times Q^i_{atc} \times Q^j_{atc}}|) \simeq O(6.4210^{1271})$. Since we have to consider all possible combinations of the agents involved, the overall computational complexity in checking condition (C2) yields $O(3.85 \cdot 10^{1272})$, which added to the computational complexity of condition (C1) finally amounts to $O(3.85 \cdot 10^{1272})$.

Step 2. Condition $(C1)$ involves the study of critical observability for each of the 4 agents $\mathcal{H}^i_p$ with respect to their critical relations $\mathcal{R}_{p_i}$. Since the hybrid models $\mathcal{H}^i_p$ coincide one each other and the critical relations $\mathcal{R}_{p_i}$ coincide one each other, it is sufficient to analyze critical observability of only one aircraft. Hence, the computational complexity in checking condition $(C1)$ becomes $O(8192)$. By using similar arguments, the computational complexity in checking condition $(C2)$ becomes $O(6.42 \cdot 10^{1271})$. The overall computational complexity in checking conditions (C1) and (C2) amounts to $O(6.42 \cdot 10^{1271})$.

Step 3. We now proceed with a further step by considering condition $(C2)$. By applying Proposition 2, $\mathcal{H}^i_p||\mathcal{H}^j_p||\mathcal{H}^i_{atc}||\mathcal{H}^j_{atc}$ is $\mathcal{R}_{p_i,p_j,atc_i,atc_j}$–critically observable iff $\mathcal{H}^i_p||\mathcal{H}^i_{atc}$ is $\mathcal{R}_{p_i,atc_i}$–critically observable and $\mathcal{H}^j_p||\mathcal{H}^j_{atc}$ is $\mathcal{R}_{p_j,atc_j}$–critically observable. The overall computational complexity in checking this condition is $O(2^{13 \cdot 5} \cdot 4)$ which, added to the computational complexity in checking condition $(C1)$, yields an overall complexity of $O(1.47 \cdot 10^{20})$.

	Computational Complexity		
Step 0	$O(1.03 \cdot 10^{5358034})$	Step 4	$O(3.68 \cdot 10^{19})$
Step 1	$O(3.85 \cdot 10^{1272})$	Step 5	$O(16416)$
Step 2	$O(6.42 \cdot 10^{1271})$	Step 6	$O(8224)$
Step 3	$O(1.47 \cdot 10^{20})$		

TABLE I

COMPUTATIONAL COMPLEXITY REDUCTION ANALYSIS.

Step 4. Since hybrid models of $\mathcal{H}^i_p||\mathcal{H}^i_{atc}$ and $\mathcal{H}^j_p||\mathcal{H}^j_{atc}$ are the same and critical relations $\mathcal{R}_{p_i,atc_i}$ and $\mathcal{R}_{p_j,atc_j}$ are the same we need to only analyze critical observability of $\mathcal{H}^i_p||\mathcal{H}^i_{atc}$ with respect to $\mathcal{R}_{p_i,atc_i}$. The overall computational complexity in checking this condition is $O(2^{13 \cdot 5})$ which, added to the computational complexity in checking condition $(C1)$, yields an overall computational complexity of $O(3.68 \cdot 10^{19})$.

Step 5. By applying Proposition 2 the system $\mathcal{H}^i_p||\mathcal{H}^i_{atc}$ is $\mathcal{R}_{p_i,atc_i}$–critically observable iff $\mathcal{H}_p$ is $\{q_{p,7}\}$–critically observable and $\mathcal{H}_{atc}$ is $\{q_{atc,3}\}$–critically observable. The overall computational complexity in checking this condition is $O(8224)$ which, added to the computational complexity in checking condition $(C1)$, yields an overall computational complexity of $O(16416)$.

Step 6. Finally the conditions outlined in Step 5 reduce to the following ones:

(C3) $\mathcal{H}_p$ is $\mathcal{R}_p$–critically observable and $\{q_{p,7}\}$–critically observable.

(C4) $\mathcal{H}_{atc}$ is $\{q_{atc,3}\}$–critically observable.

The improvement obtained in Step 6 w.r.t. Step 5 is due to the fact that while checking conditions in Step 5 requires the construction of 3 observers, 2 for the agent pilot and 1 for the agent air traffic controller, checking conditions in Step 6 require the construction of only 2 observers, one for the agent pilot and one for the agent air traffic controller. The overall computational complexity required in checking conditions (C3) and (C4) is $O(8224)$. The computational complexity reduction achieved by the procedure shown above is summarized in Table I. The above procedure reduces the analysis of critical observability of the ASEP–ITP to the analysis of critical observability in conditions (C3) and (C4). We start by considering condition $(C3)$. For doing so we need to construct an observer for $\mathcal{H}_p$. By using the results recalled in Section II-B we obtain the observer

$$O_p = (\hat{Q}_p, \hat{Q}_{0p}, \hat{\Sigma}_p, \hat{\Psi}_p, \hat{E}_p, \hat{\eta}_p)$$

where $\hat{Q}_p = \{\{q_{p,1}, q_{p,2}, q_{p,3}\}, \{q_{p,4}\}, \{q_{p,5}\}, \{q_{p,6}\}, \{q_{p,7}, q_{p,8}, q_{p,9}\}, \{q_{p,11}\}, \{q_{p,10}, q_{p,12}\}\}$; $\hat{Q}_{0p} = \{\{q_{p,1}, q_{p,2}, q_{p,3}\}\}$; $\hat{\Sigma}_p = \Psi_{p_i}$; $\hat{\Psi}_p = \hat{Q}_{p_i}$, $\hat{E}_p$ is depicted in Figure 3 and

$\hat{\eta}_p(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_{p_i}$. We start by checking the first part of condition (C3): the obtained observer $\mathcal{O}_p$ illustrated in Figure 2, shows that $\mathcal{H}_p$ is not $\mathcal{R}_p$–critically observable. Indeed, when the state of $\mathcal{O}_p$ is in $\{q_{p,7}, q_{p,8}, q_{p,9}\}$ it is not possible to distinguish the critical states $q_{p,8}, q_{p,9}$ from the noncritical state $q_{p,7}$. Analogously when the state of $\mathcal{O}_p$ is in $\{q_{p,10}, q_{p,12}\}$, it is not possible to distinguish the critical state $q_{p,10}$ from the noncritical state $q_{p,12}$. In order to render the hybrid model $\mathcal{H}_p$, $\mathcal{R}_p$–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 $q_{p,8}$, $q_{p,9}$ or $q_{p,10}$. The extra output $h(q_{p,8})$ might be generated using an alarm that detects a failure in the surveillance system. The extra output $h(q_{p,9})$ might be generated using measurements of position and velocity of the aircraft. The extra output $h(q_{p,10})$ might be obtained by adding to the procedure a communication from the oceanic controller to the pilot, after the Aircraft Status Report at the next waypoint. The generation of these extra outputs requires a time delay. Construction of critical observers with time delay has been studied in [5]. We do not report here these results for lack of space. The observer with delay associated with agent $\mathcal{H}_p$ is illustrated in Figure 3. 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. By proceeding as in the previous case it is possible to check condition (C4); the same analysis can be applied to the construction of the observer for the ATC. We do not report hereafter such analysis for lack of space. The analysis that we performed highlights that the ASEP-ITP is not critically observable. However, provided that additional signals can be generated, the procedure can be made critically observable. It is readily seen that the analysis that we performed can be easily extended to a scenario in which an arbitrary large number of agents operate.

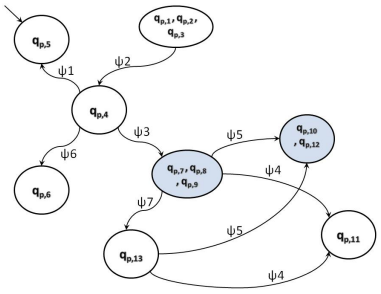

Fig. 2. $\mathcal{R}_p$–critical observer for hybrid system $\mathcal{H}_p$.

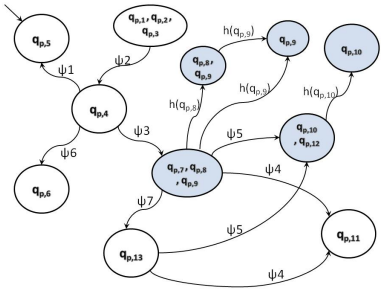

Fig. 3. $\mathcal{R}_p$–critical observer with delay for hybrid system $\mathcal{H}_p$.

V. Conclusions

In this paper we addressed the problem of critical observability analysis in ATM multi–agent systems. We first provided a compositional hybrid systems framework, capturing the behaviour of each agent and the relative interaction acting in ATM systems. We further presented results for the reduction of the computational complexity of checking critical observability of ATM multi–agent systems. The benefits of our approach were illustrated using the analysis of the ASEP In Trail procedure.

References

[1] 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.

[2] M. 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 And Exhibition*, December 2008.

[3] M. D. Benedetto, A. Petriccone, and G. Pola, "Compositional hybrid system approach to the analysis of air traffic management systems," in *8-th Innovative Research Workshop Exhibition, EUROCONTROL*, December 2009.

[4] 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.

[5] M. D. Benedetto, S. D. Gennaro, and A. D'Innocenzo, "Discrete state observability of hybrid systems," *International Journal of Robust and Nonlinear Control*, vol. 19, pp. 1564–1580, 2009, special Issue on "Observability and Observer Design for Hybrid Systems".

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

[7] E. De Santis, M. D. Di Benedetto, and G. Pola, "Observability of internal variables in interconnected switching systems," in *Proceedings of the 45^{th} IEEE Conference on Decision and Control, CDC 06, San Diego, CA, USA*, December 2006, pp. 4121–4126.

[8] C. Montijn, G. Graniero, and B. K. Obbink, "Qualitative Risk Assessment for ASEP-ITP, D6.1b ASSTAR Projects," 01 February 2007, v.1.0.

[9] "In-Trail Procedure in Procedural Airspace (ATSA-ITP) Application descriptionASSTAR Projects," 21 June 2007, v.8.0.

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

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

[12] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A. Sangiovanni-Vincentelli, "Design of observers for hybrid systems," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, C. Tomlin and M. Greensreet, Eds. Springer Verlag, 2002, vol. 2289, pp. 76–89.

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