Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

iFly

Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management

Specific Targeted Research Projects (STREP)

Thematic Priority 1.3.1.4.g Aeronautics and Space

iFly Deliverable D4.2
Report on Observability Properties of Hybrid-System Composition

Version 1.1 (Final)

Authors: M.D. Di Benedetto, A. Petriccone, G. Pola,
University of L'Aquila

Due date of deliverable: 22 January 2010
Actual submission date: 27 January 2011

Start date of project: 22 May 2007 Duration: 51 months

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

DOCUMENT CONTROL SHEET

Title of document:	*Report on Observability Properties of Hybrid-System Composition*
Authors of document:	*M.D. Di Benedetto, A. Petriccone, G. Pola*
Deliverable number:	*D4.2*
Project acronym:	*iFly*
Project title:	*Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management*
Project no.:	*TREN/07/FP6AE/S07.71574/037180 IFLY*
Instrument:	*Specific Targeted Research Projects (STREP)*
Thematic Priority:	*1.3.1.4.g Aeronautics and Space*

DOCUMENT CHANGE LOG

Version x.x	Issue Date	Sections affected	Relevant information
0.1	22.01.2010	All	First Draft
0.2	12.02.2010	All	Second Draft
0.3	31.03.2010	All	Third Draft
0.4	30.05.2010	All	Comments from WP4 Partners
1.0	17.11.2010	All	Comments from WP4 Partner NLR
1.1	27.01.2011	All	Comments from External Reviewer

Version 1.0		Organisation	Signature/Date
Authors	Maria D. Di Benedetto	AQUI	
	Alessandro Petriccone	AQUI	
	Giordano Pola	AQUI	
Internal reviewers	Elena De Santis	AQUI	
	Stefano Di Gennaro	AQUI	
	Alessandro D'Innocenzo	AQUI	
	Henk Blom	NLR	
	Maria Prandini	PoliMi	
	Vicente Bordon, Leticia Biescas	Isdefe	
External reviewers	Uwe Voelckers		

Contents

Abstract

This report is Deliverable D4.2 of Work Package 4 of the iFLY project. The main contribution of D4.2 is to use tools from Hybrid Systems and Automata Theory formalism to study situational awareness inconsistencies arising in multi–agent air traffic management systems and in particular in Autonomous Aircraft Advanced (A^3) ConOps. The multi–agent case is particularly challenging since even though situation awareness inconsistencies may not cause any significant problem in isolation, they may yield a catastrophic outcome when taken in a multi–agent environment. We first review the formal observability analysis of procedural errors in Air Traffic Management systems. We then introduce a compositional framework for hybrid systems which allows us to capture interaction among the agents operating in ATM scenarios. The notion of composition proposed here is based on the exchange of discrete data between the systems involved. Critical observability of the composition of hybrid systems is addressed, and a result is presented that allows computational complexity reduction when checking the critical observability of the composed system. The effectiveness of our theoretical results is shown by applying them to the following case studies: the Airborne Separation In Trail Procedure (ASEP-ITP), the ASAS Lateral Crossing Procedure, and a scenario in the context of A^3 ConOps.

Acronyms

ADS-B	Airborne Dependant Surveillance Broadcast
ASAS	Airborne Separation Assistance System
ASEP	Airborne Separation
ASSAP	Airborne Surveillance and Separation Assurance Processing
ASSTAR	Advanced Safe Separation Technologies and Algorithms
ATCo	Air Traffic Controller
ATSA	Airborne Traffic Situational Awareness
CD	Conflict Detection
CDTI	Cockpit Display of Traffic Information
CR	Conflict Resolution
fpm	Feet per minute
ITP	In-Trail Procedure
NM	Nautical Miles
MT	Medium Term
ST	Short Term
RBT	Reference Business Trajectory
RVSM	Reduced Vertical Separation Minima
SA	Situational awareness
SWIM	System Wide Information Management

1 Introduction

The iFly project is concerned with the development of a highly automated Air Traffic Management (ATM) design for en-route traffic, which takes advantage of autonomous aircraft operation capabilities. Meeting this ambitious goal requires a complete re-thinking not only of air traffic management concepts, but also of the design practices used to develop such concepts. Within iFly, two design cycles and one intermediate assessment cycle are addressed. The first cycle aims at designing state-of-the-art Autonomous Aircraft Advanced (A^3) [8] en-route operation. By taking advantage of progress already made in previous projects and research, and of a human responsibility study carried out in WP2, the A^3 ConOps was developed in iFly Deliverable D1.3 [8] of WP1. The second design cycle aims at refining the A^3 en-route operation, by also using the mathematical developments of Work Packages WP3 ("Prediction of complexity under uncertainty"), WP4 ("Multi-Agent Situation Awareness consistency protection") and WP5 ("Conflict resolution with performance assurance"). In particular, the goal of increasing efficiency of air traffic control is solved by a distribution of tasks among autonomous agents. It is therefore necessary to guarantee that all the agents who participate in the decisions have a similar, if not identical, perception of what the situation is. Many operation problems, some of potential catastrophic outcome, can be traced to erroneous or inconsistent multi–agent situation awareness (each agent perception of the surrounding environment). The study of techniques that can detect automatically whether there are problems with situation awareness, and that these problems may lead to a catastrophic situation, is the main topic of Work Package WP4.

We start from the results of D4.1 [7], where we applied a methodology for formal reasoning based on hybrid systems theory, which provides a powerful framework to develop multi–agents models. Using this methodology, it is possible to link the changes of the physical systems behavior to the actions made by each agent, including actions caused by situational awareness inconsistencies. Building on the preliminary results of the intermediate deliverable D4.2i [4], we investigate in this report the observability properties of multi–agent systems where the agents interact. We consider the system as a composition of the mathematical models of the agents acting in the ATM scenario. The notion of composition we propose is based on the exchange of discrete data between the systems involved. Critical observability of the composition of hybrid systems is addressed, and a method is proposed for separately analyzing the single agents instead of analyzing

directly their composition. This allows a computational effort reduction in checking critical observability of the composed system. The effectiveness of our theoretical results is shown by considering some case studies. We start with their application to the Airborne Separation In Trail Procedure (ASEP-ITP) [1, 17] and the ASAS Lateral Crossing procedure [13]. We then consider a scenario in the Autonomous Aircraft Advanced (A^3) ConOps [8] and analyze the possibility of detecting unallowed and/or unsafe operations. The analysis of this third case study can provide a useful input to the further ConOps development within WP8. In particular, we are collaborating for proposing strategies that allow the agents to reach correct situation awareness.

The report is organized as follows. In Section 2 we define the mathematical framework of hybrid systems, the compositional operator we use to compose agents modeled by hybrid systems, the basic definition of critical observability, and state the main theoretical result of this deliverable. In Section 3, the hybrid model of the ASEP-ITP procedure is derived and critical observability in a multi–agent environment is analyzed. In Section 4, the ASAS Lateral Crossing procedure is considered and the possibility of detecting unallowed and/or unsafe operations by means of the theoretical framework illustrated in the previous sections is analyzed. In Section 5, critical observability of a scenario in the A^3 ConOps is considered in a multi–agent environment. Section 6 provides concluding remarks.

2 Hybrid systems, Composition and Critical Observability

In this section, we introduce the mathematical framework that will be used for the analysis of the observability properties of compositions of hybrid systems. We first review the notion of hybrid systems. We then introduce a notion of composition of hybrid systems, which can capture well the interaction of different agents acting in an ATM scenario. We then review the notion of critical observability, which corresponds to the possibility of instantly detecting critical situations that may lead to dangerous or even catastrophic events. Finally, we propose a technique for reducing the computational effort required in the test of critical observability of the composed hybrid system. The theoretical results presented in this section generalize the ones achieved in the intermediate deliverable D4.2i [4].

2.1 Hybrid Systems

The following definition of hybrid systems is inspired by the classical model proposed in [15].

Definition 1 (Hybrid system)**.** *A hybrid system is a tuple*

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

where:

- $Q \times X$ *is the hybrid state space, where* Q *is a finite set of* N *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 conditions.*
- $U \subseteq \mathbb{R}^m, Y \subseteq \mathbb{R}^p$ *are the sets of continuous control input and observable output.*
- $\{\mathcal{E}(q)\}_{q \in Q}$ *associates to each discrete state* $q \in Q$ *the continuous time–invariant dynamics*

  $$\mathcal{E}(q) \colon \dot{x} = f_q(x, u),$$

  and the output map $y = g_q(x)$*. Given an initial condition* x_0 *at time* t_0 *and a control input* $u|_{t_0}^t \colon [t_0, t] \to U$*, we denote the solution at time* t *according to* f_q *by*

  $$x(t) = x_q(t, x_0, u|_{t_0}^t).$$

The solution of the above differential equation exists and it is unique, provided that f_q is Lipschitz[1] *continuous with respect to its arguments.*

- Σ *is the set of discrete input symbols. It includes the empty string* ε*, that corresponds to the null input.*
- $E \subseteq Q \times \Sigma \times Q$ *is a collection of edges.*
- Ψ *is the finite set of discrete output symbols. It includes the empty string* ε*, that corresponds to unobservable output.*
- $\eta \colon E \to \Psi$ *is the output function, that associates to each edge a discrete output symbol.*

Referring to [15], we recall the definition of *hybrid time basis*.

Definition 2 (Hybrid time basis)**.** *A hybrid time basis* $\tau \triangleq \{I_k\}_{0 \le k \le |\tau|}$ *is a finite or infinite sequence of intervals* $I_k = [t_k, t'_k]$*. The length* $t'_k - t_k$ *of every interval* I_k *denotes the dwelling time in a discrete state, while the extremes* t_k, t'_k *specify the switching instants of the hybrid flow. The number of such intervals is* $|\tau| + 1$*, where* $|\tau|$ *is the cardinality of the time basis. Furthermore, the following hold:*

1. $t_k \le t'_k$ for $k > 0$, and $t'_{k-1} = t_k$ for $k > 1$;
2. If the sequence is infinite, i.e. $|\tau| = \infty$, then I_k is closed for all k;
3. If the sequence is finite, i.e. $|\tau| < \infty$, then the last interval $I_{|\tau|}$ might be right–open.

A hybrid execution is a tuple

$$\chi = (\tau, \sigma, u, q, x, y),$$

where τ is a hybrid time basis, $\sigma : \tau \to \Sigma$ is the discrete input, u is the continuous input, y is the continuous output, and q, x describe the evolution of the discrete and continuous state by means of functions $q \colon \tau \to Q$ and $x \colon \tau \to X$. The interested reader can refer to [15] for a precise definition of execution. In this deliverable, we consider *non blocking* [14] and *non Zeno* [2] hybrid systems, i.e. systems such that all hybrid executions are defined for all time instants.

[1] A function $f : \mathbb{R}^n \to \mathbb{R}^m$ is said to be Lipschitz continuous if there exists a constant $L > 0$ so that $\|f(x_1) - f(x_2)\| \le L\|x_1 - x_2\|$ for any $x_1, x_2 \in \mathbb{R}^n$.

2.2 Composition

Interaction among different hybrid systems can be captured by an appropriate notion of composition which we now introduce. Consider a scenario characterized by $N \geq 1$ hybrid systems:

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

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[2] $\mathcal{H}_j$.

The evolution of each hybrid system $\mathcal{H}_i$ depends on the information that $\mathcal{H}_i$ has from all hybrid systems $\mathcal{H}_j$ sharing information with it, i.e. all $\mathcal{H}_j$ for which $(\mathcal{H}_j, \mathcal{H}_i) \in \mathbb{E}$ in the communication scheme $\mathbb{V}$. More precisely, if $(\mathcal{H}_j, \mathcal{H}_i) \in \mathbb{E}$ then the evolution of $\mathcal{H}_i$ depends on some discrete outputs of $\mathcal{H}_j$, which become a part of the discrete inputs of $\mathcal{H}_i$.

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 $\mathcal{H}_j$;
  - 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 $\mathcal{H}_j$;

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

– ε is the null output corresponding to no information and/or action given to any $\mathcal{H}_j$.

The interaction among the hybrid systems $\mathcal{H}_i$ can be captured by the following notion of composition. 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[3]:

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

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:

[3]The composed hybrid system depends on the communication scheme $\mathbb{F}$ which therefore should appear explicitly in the notation $\|$. However, for the sake of notational simplicity we will omit $\mathbb{F}$ in the further developments.

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

The above notion of composition is inspired by the classical notion of parallel composition in the theory of automata [12] and by the notion of composition of switching systems introduced in [10]. In the above notion of composition, we are considering event driven transitions and we are implicitly assuming that events cannot occur at the same time. Hence algebraic loops cannot occur. This assumption can appear restrictive in general. However, in the case of ATM systems this is quite reasonable. We stress that the above definition captures interactions between discrete variables and not between continuous variables. This choice is motivated by the application domain we are interested in, where interaction among agents can be naturally represented by an exchange of discrete signals (and not of continuous signals) in the hybrid systems that model the agents.
The above notion of composition also captures the special instance in which agents do not communicate. In fact, consider a scenario with two hybrid systems $\mathcal{H}_1$ and $\mathcal{H}_2$ and suppose that $\Sigma_1^2 = \Sigma_2^1 = \varnothing$ and $\Psi_1^2 = \Psi_2^1 = \varnothing$. Then the resulting hybrid system $\mathcal{H}$ is given by the composition of $\mathcal{H}_1$ and $\mathcal{H}_2$ which behave independently from each other. This special case models situations where agents acting in an ATM scenario cannot interact directly, for example in case of lack of communication and/or when a specific ATM procedure does not suppose such a communication. From a theoretical point of view, the composition in this special case is known in the literature of discrete event systems as **shuffle product** and is usually denoted by the operator $\times$ instead of $||$. In the following, we maintain this classical notation and denote by $\mathcal{H}_1 \times \mathcal{H}_2$ the composition of agents $\mathcal{H}_1$ and $\mathcal{H}_2$ which do not interact.

2.3 Critical Observability

In this section, we first review the notion of critical observability of [9]. We then propose some theoretical results to achieve computational effort reduction in checking critical observability in multi–agent scenarios.
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 is able to detect whether the current discrete state of $\mathcal{H}$ belongs to $\mathcal{R}$ or not on the basis of the observations. Formally:

Definition 3. *Given a hybrid system $\mathcal{H}$, an observer of the critical set $\mathcal{R}$ is a system $\mathcal{O}_{\mathcal{R}}$ whose input is the discrete output of $\mathcal{H}$ and whose output $\hat{y}(t)$ is such that*[4]*:*

$$\forall\, k \geq 0, \forall\, t \in [t_k, t'_k), \qquad \hat{y}(t) = \begin{cases} 1 & \text{if } \; q(I_k) \in \mathcal{R} \\ 0 & \text{if } \; q(I_k) \in Q \setminus \mathcal{R}. \end{cases}$$

System $\mathcal{H}$ is said to be $\mathcal{R}$–critically observable if an observer $\mathcal{O}_{\mathcal{R}}$ exists. Moreover, if $\mathcal{O}_{\mathcal{R}}$ exists it is said to be a $\mathcal{R}$–critical observer for $\mathcal{H}$.

Given a hybrid system $\mathcal{H}$, we refer to a critical observer of $\mathcal{H}$ as a tuple:

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

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.
- $\hat{\eta} : \hat{Q} \rightarrow \hat{\Psi}$ is the output function which coincides with identity function.

The construction of such observers is rather standard within the community of discrete event systems. We refer to Deliverables 4.1 [7] and 4.2i [4] for references on this topic and for a detailed description on how such observers can be constructed.

From the above definition it is readily seen that the space complexity of $\mathcal{O}$ is $O(|2^Q|)$, i.e. the size of the set of states $\hat{Q}$ of $\mathcal{O}$ grows exponentially with the size of the set of discrete states Q of the hybrid system $\mathcal{H}$.

[4]The entities t_k, t'_k, I_k and $q(.)$ have been introduced in Section 2.1.

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 proposed in [3]. When using information coming from the continuous dynamics, some time is required in the generation of additional discrete signals. This implies a non–instantaneous detection of critical states. However in many cases a bounded delay in the detection of such critical states is acceptable[5] and this motivates the definition of [16] reported hereafter:

Definition 4. *Given a hybrid system $\mathcal{H}$, an observer with delay $\delta > 0$ of the critical set $\mathcal{R}$ is a system $\mathcal{O}^{\delta}_{\mathcal{R}}$ whose input is the discrete output of $\mathcal{H}$ and whose output $\hat{y}(t)$ is such that:*

$$\forall\, k \geq 0, \forall\, t \in [t_k + \delta, t'_k), \qquad \hat{y}(t) = \begin{cases} 1 & \text{if } \; q(I_k) \in \mathcal{R} \\ 0 & \text{if } \; q(I_k) \notin \mathcal{R}. \end{cases}$$

System $\mathcal{H}$ is said to be $\mathcal{R}$–critically observable with delay δ if an observer $\mathcal{O}^{\delta}_{\mathcal{R}}$ exists. Moreover if $\mathcal{O}^{\delta}_{\mathcal{R}}$ exists it is said to be a $\mathcal{R}$–critical observer with delay δ for $\mathcal{H}$.

An algorithm to check critical observability with delay can be found in [16]. The results in the work of [9, 16] can be used to analyze critical observability of an ATM scenario in which different agents take part. Suppose that the ATM scenario involves N agents that are represented by N hybrid systems $\mathcal{H}_1, \mathcal{H}_2, ..., \mathcal{H}_N$. Interactions among these agents can be modeled by 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

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

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 $\mathcal{H}$. Critical observability of the system $\mathcal{H}$ may be assessed with respect to the set of critical states $\mathcal{R}$. However, this may be computationally demanding if the number of agents involved is large, as it is the case in realistic ATM scenarios. The key idea for reducing the computational effort required in checking critical observability is based on the following construction of $\mathcal{R}$, using critical sub-relations.

Definition 5. *Consider the following sequence of sets:*

[5] Bounded delay in the detection of critical states is acceptable for example for hybrid systems with positive dwell time, i.e. hybrid systems in which the dwelling time in each discrete state is greater than a positive real, called dwell time.

- $\mathcal{R}_{i_1} \subseteq Q_{i_1}$ *is the set of critical states for hybrid system* $\mathcal{H}_{i_1}$*;*
- $\mathcal{R}_{i_1,i_2} \subseteq Q_{i_1} \times Q_{i_2}$ *is the set of critical states arising from the interaction of hybrid systems* $\mathcal{H}_{i_1}$ *and* $\mathcal{H}_{i_2}$*;*

  $\vdots$
- $\mathcal{R}_{i_1,i_2,\ldots,i_N} \subseteq Q_{i_1} \times Q_{i_2} \times \ldots \times Q_{i_N}$ *is the set of critical states arising from the interaction of hybrid systems* $\mathcal{H}_{i_1}$*,* $\mathcal{H}_{i_2}$*, ...,* $\mathcal{H}_{i_N}$*.*

Definition 6. *Consider the sequence of sets in Definition 5 and define the following sequence of sets:*

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

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

The above decomposition of the critical relation $\mathcal{R}$ is important for two reasons. First, it reduces the analysis of critical observability w.r.t $\mathcal{R}$ to the analysis of critical observability w.r.t. the sequence of sets in Definition 5 and this may yield a remarkable reduction in the computational effort required.

Secondly, suppose that during the evolution of the system, a new hybrid system $\mathcal{H}_{N+1}$ enters the scenario. In this case the new critical relation $\bar{\mathcal{R}}$ can be computed on the basis of $\mathcal{R}$ with no need of recalculating the critical relation from the beginning. In fact, in this case the critical relation $\bar{\mathcal{R}}$ would result in:

$$\bar{\mathcal{R}} = \mathcal{R} \cup \mathcal{R}'_{N+1} \cup (\bigcup_{i_1} \mathcal{R}'_{i_1,i_{N+1}}) \cup \ldots \cup (\bigcup_{i_1,\ldots,i_N} \mathcal{R}'_{i_1,\ldots,i_N,i_{N+1}}).$$

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.*

If $\mathcal{H}$ is $\mathcal{R}^1$–critically observable and $\mathcal{R}^2$–critically observable there exist a pair of observers $\mathcal{O}_1$ and $\mathcal{O}_2$ which are able to detect whether the discrete state of $\mathcal{H}$ is in $\mathcal{R}^1$ and $\mathcal{R}^2$ or not. Define the hybrid observer $\mathcal{O}$ as the

shuffle product $\mathcal{O}_1 \times \mathcal{O}_2$ of the observers $\mathcal{O}_1$ and $\mathcal{O}_2$ and with output $\hat{y}$ defined by $\hat{y}(t) = [\hat{y}_1(t) \ \vee \ \hat{y}_2(t)]$. Suppose that $q(I_k) \in \mathcal{R}$ at time t. Then either $q(I_k) \in \mathcal{R}^1$ or $q(I_k) \in \mathcal{R}^2$, which corresponds to $\hat{y}_1(t) = 1$ or $\hat{y}_2(t) = 1$, from which $\hat{y}(t) = 1$. Suppose now that $q(I_k) \in Q \backslash \mathcal{R}$ at time t. Then $q(I_k) \in Q \backslash \mathcal{R}^1$ and $q(I_k) \in Q \backslash \mathcal{R}^2$, which corresponds to $\hat{y}_1(t) = 0$ and $\hat{y}_2(t) = 0$, from which $\hat{y}(t) = 0$. Thus $\mathcal{O}$ is a $\mathcal{R}$–critical observer for $\mathcal{H}$ and hence $\mathcal{H}$ is $\mathcal{R}$–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.*

For $i = 1, 2$ let $\mathcal{O}_i$ be a $\mathcal{R}_i$–critical observer for $\mathcal{H}_i$ and denote by $\hat{y}_i$ the output of $\mathcal{O}_i$. Define the hybrid observer $\mathcal{O}$ as the shuffle product $\mathcal{O}_1 \times \mathcal{O}_2$ of the observers $\mathcal{O}_1$ and $\mathcal{O}_2$ and with output $\hat{y}$ defined by $\hat{y}(t) = [\hat{y}_1(t) \ \wedge \ \hat{y}_2(t)]$. We now show that $\mathcal{O}$ is a $\mathcal{R}^1 \times \mathcal{R}^2$–critical observer for $\mathcal{H}_1 || \mathcal{H}_2$. Suppose that $q(I_k) = (q_1(I_k), q_2(I_k)) \in \mathcal{R}^1 \times \mathcal{R}^2$ at time t. Then $q_i(I_k) \in \mathcal{R}^i$ which implies $\hat{y}_i(t) = 1$; thus $\hat{y}(t) = 1$. Suppose now that $q(I_k) \notin \mathcal{R}^1 \times \mathcal{R}^2$ at time t. By using similar arguments it is easy to show that $\hat{y}(t) = 0$. Thus $\mathcal{O}$ is a $\mathcal{R}^1 \times \mathcal{R}^2$–critical observer for $\mathcal{H}$ and hence $\mathcal{H}$ is $\mathcal{R}^1 \times \mathcal{R}^2$–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 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 $i_1, i_2 = 1, 2, ..., N$;*
  $\vdots$
- *$\mathcal{H}_{i_1} || \mathcal{H}_{i_2} || ... || \mathcal{H}_{i_N}$ is $\mathcal{R}_{i_1, i_2, ..., i_N}$–critically observable for any $i_1, i_2, ..., i_N = 1, 2, ..., N$.*

(Necessity) Obvious. (Sufficiency) By Proposition 1, $\mathcal{H}$ is $\mathcal{R}$–critically observable if $\mathcal{H}$ is critical observable w.r.t. the critical relations in Definition 6. Now consider the set $\mathcal{R}'_{i_1}$. It is readily seen that such set can be rewritten as

$$\mathcal{R}'_{i_1} = Q_1 \times Q_2 \times ... \times Q_{i_1 - 1} \times \mathcal{R}_{i_1} \times Q_{i_1 + 1} \times ... \times Q_N.$$

By Proposition 2 hybrid system $\mathcal{H}$ is $\mathcal{R}'_{i_1}$–critically observable if:

- $\mathcal{H}_1||\mathcal{H}_2||...||\mathcal{H}_{i_1-1}$ is $Q_1 \times Q_2 \times ... \times Q_{i_1-1}$–critically observable;
- $\mathcal{H}_{i_1}$ is $\mathcal{R}_{i_1}$–critically observable;
- $\mathcal{H}_{i_1+1}||\mathcal{H}_{i_1+2}||...||\mathcal{H}_N$ is $Q_{i_1+1} \times Q_{i_1+2} \times ... \times Q_N$–critically observable.

From the definition of critical observability it is clear that the first and third conditions are always satisfied. Indeed, the discrete state of hybrid system $\mathcal{H}_1||\mathcal{H}_2||...||\mathcal{H}_{i_1-1}$ always evolves in its state space $Q_1 \times Q_2 \times ... \times Q_{i_1-1}$: hence the first condition is satisfied. The same ratio applies to the third condition. From this discussion we get that $\mathcal{H}$ is $\mathcal{R}'_{i_1}$–critically observable if $\mathcal{H}_{i_1}$ is $\mathcal{R}_{i_1}$–critically observable. By applying the same reasoning to other critical relations appearing in Definition 6, the result follows.

Benefits from the use of the above result in the analysis of critical observability of ATM multi–agent systems are illustrated in the next sections.

3 Evaluation of Airborne Separation In Trail Procedure

In this section we model and analyze critical observability of the Airborne Separation–In Trail Procedure (ASEP-ITP).

3.1 Description of the In Trail Procedure

The Airborne Separation In Trail Procedure (ASEP-ITP) [17, 1] described hereafter is a procedure that aims at improving flight efficiency along oceanic routes where procedural control is performed, and is an extension of the Airborne Traffic Situational Awareness In Trail Procedure (ATSA-ITP) [1] considered in D4.1.

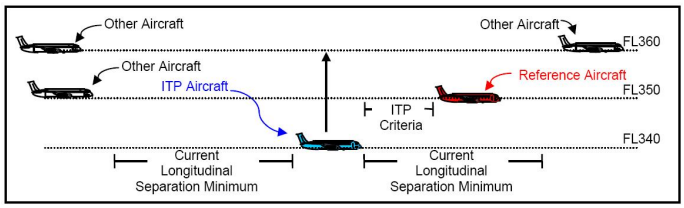

Figure 1: Example of ITP geometry

3.1.1 ASEP ITP Criteria

The ASEP-ITP allows climb or descend through only one flight level for a maximum of 2000 feet in RVSM airspace (and 4000 feet in non-RVSM) and the ITP speed/distance criteria are designed so that under nominal conditions the proposed 5NM separation minimum is preserved throughout the ITP manoeuvre. The proposed ITP speed/distance criteria are the following:

- initiation ITP distance of no less than 10 NM and positive ground speed differential of no more than 20 kts, or

- ITP distance of no less than 15 NM and positive ground speed differential of no more than 30 kts.

The ITP encompasses a set of six vertical geometries: leading climb (as shown in Figure 1), leading descend, following climb, following descend, combined leading-following climb and combined leading-following descend. These geometries are designed on the basis of the relative position of the ITP aircraft and one or two reference aircraft.

The ITP aircraft must maintain a minimum 300 ft/min of climb or descend and constant cruise Mach number throughout the ITP manoeuvre. The reference aircraft must be non-manoeuvring and it is not expected to manoeuvre during the ITP. Given these conditions, it can be shown that a 4000 ft flight level change would result in a reduction in the initial distance of 4.5 NM assuming a positive ground speed differential of 20 kts. To ensure that the ITP separation minimum of 5NM will be guaranteed during the flight level change under these conditions, the initial distance between the aircraft must exceed 9.5 NM. So using 10 NM of initial distance the separation minimum is guaranteed. In the same way it could be proved that with positive ground speed differential of more than 20 but less than 30 kts, an initial distance of 15 NM ensures that ITP separation minimum is respected.

A compact view of the ASEP-ITP phases is illustrated in Figure 2, and is now described.

3.1.2 ASEP-ITP phases

ITP Initiation phase

The decision to request an ITP rather than a standard flight level change will typically be based on a number of factors outside the scope of the ITP application, such as crew preference and judgment, the magnitude of the

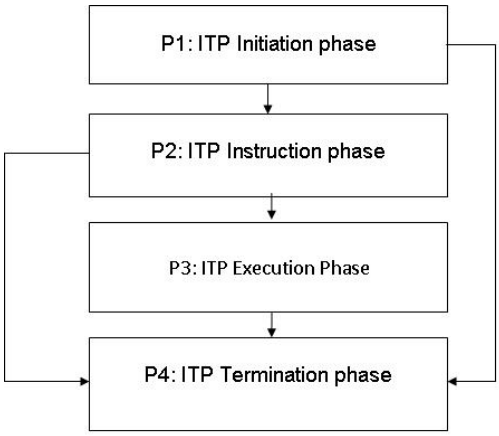

Figure 2: ASEP-ITP phases diagram

desired flight level change, and any other information available to the crew about the flight's progress and proximate traffic situation.

Once the flight crew has decided to consider requesting an ITP, the flight crew proceeds through the following steps to formulate and initiate the request:

1. Identification of ITP flight levels

   - The crew identifies a requested flight level, which is a flight level above (for a climb) or below (for a descend) one flight level and that is no more than 4000 ft from the initial flight level.

2. Checking ITP aircraft Performance by the crew:

   - The ITP aircraft is capable of performing a rate of climb or descend of at least 300 fpm at the assigned Mach number to the requested flight level.
   - The ITP aircraft is not expected to manoeuvre except for a climb or descend or a change of course to remain on their clearance.

3. Identification of reference aircraft. The crew selects as reference aircraft up to two potentially blocking aircraft which meet the following criteria:

   - The ITP aircraft has the same direction with potentially blocking aircraft.
   - Qualified ADS-B data are available from potentially blocking aircraft.
   - The ITP speed/distance criteria are met with potentially blocking aircraft.

4. ITP Request

    - If the ITP criteria are met, the ITP aircraft crew requests the ITP, using the required ITP phraseology which provides the controller with the requested ITP flight level change geometry (i.e., leading or following), the ITP distance and the flight ID of reference aircraft.

ITP Instruction Phase

1. Issue of ITP Clearance by ATCo controller depends if standard separation will be met with all aircraft at the requested flight level and at all flight levels between the ITP aircraft's initial flight level and requested flight level. If so, a standard (non-ITP) flight level change clearance can be issued. *If not,*

    - Determine whether the ITP request message format is correct and that the flight crew has correctly identified the reference aircraft at the intervening flight level.
    - Determine whether standard separation will be met with other aircraft (i.e., all but the reference aircraft) at the requested flight level and at all flight levels between the ITP aircraft's initial Flight Level and requested flight level.
    - Determine whether the ITP aircraft is not a reference aircraft in another ITP clearance.
    - Determine whether the ITP aircraft and the reference aircraft are on the same track.
    - Determine whether the reference aircraft are non-manoeuvring and not expected to manoeuvre during the ITP. The controller will not issue an ITP clearance if a reference aircraft is starting a manoeuvre or expected to manoeuvre.
    - Determine whether the positive Mach differential is no greater than 0.03 Mach.

    Based on the ITP aircraft's request and the controller's determination of the previous six conditions, the controller would issue the ITP clearance.

2. ITP Crew Re-Assessment

- After the ITP clearance is issued, the flight crew of the ITP aircraft must again determine whether the ITP criteria continue to be met with respect to the reference aircraft immediately before initiating the climb or descend. If the ITP criteria are no longer met, the crew refuses the clearance and remains at the initial flight level.

ITP Execution Phase

1. ITP Aircraft Crew Tasks during the ITP Manoeuvre

   - As after a standard climb or descend clearance, the crew must initiate the ITP without delay after receipt of the clearance. Note that the crew re-assessment should not cause an undue delay in the initiation of this manoeuvre.
   - The crew must maintain the original cruise Mach number during the climb or descend.
   - The ITP aircraft must maintain a minimum 300 fpm climb or descend rate, or the minimum rate required by regulation, whichever greater, throughout the ITP manoeuvre.
   - The ITP aircraft crew shall monitor the ITP distance to the reference aircraft during the climb or descend. The crew monitors the ASAS equipment indicating the range of the blocking aircraft. If the separation minimum is predicted to be violated a temporary speed change is allowed.
   - The ITP flight crew reports the establishment at the new flight level.
   - If the ITP cannot be successfully completed as cleared once the climb or descend has been initiated, an abnormal termination occurs. ATCo must be notified immediately when this condition occurs.

2. Controller Tasks during the ITP Manoeuvre

   - The controller will not issue any manoeuvre clearance to the reference aircraft until the ITP Aircraft reports establishment at the new flight level or the ITP is abnormally terminated.

ITP Termination Phase

1. The ITP is completed when the ITP flight crew reports established at the new flight level.

2. If the ITP aircraft cannot successfully complete the ITP once the climb or descend has been initiated, an abnormal termination occurs.

3.2 Modeling of the ASEP-ITP

The ASEP-ITP can be decomposed in various subsystems representing the agents involved in the procedure, each with hybrid dynamics modeling its specific operations. It should be remarked that to exploit the descriptive power of hybrid systems, each agent must be considered by itself and subsequently the effects of their actions on the dynamics of other agents can be considered by composing such models. The agents considered here are:

- Air crew flying of ASEP-ITP aircraft;
- Oceanic controller.

The approach used for selecting the agents does not provide the modeling of the reference aircraft as an agent. The main reason is that the flight crew of the reference aircraft does not have the awareness of existence of an ASEP-ITP manoeuvre in which it is involved. In fact, there is no communication between the controller or the flight crew of the ASEP-ITP aircraft and the flight crew of the reference aircraft. Furthermore any hazardous actions of the reference aircraft can be considered inside the hybrid dynamics of other agents.

The proposed model considers the case of ASEP-ITP execution where there are N ASEP-ITP aircraft that require a climb through one flight level, in which everyone of the N aircraft can be the reference of the other and without taking into account other surrounding aircraft. Furthermore, no wind is assumed.

3.2.1 Pilot flying of ITP aircraft Agent

The behavior of the agent Pilot Flying of ITP Aircraft can be formalized by means of the hybrid system:

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

where:

- $Q_p = \{q_i, i = 1, 2, ..., 13\}$ is the set of discrete states, each one associated with a node inside the graph depicted in Figure 3, where:
  - q_1 represents the normal cruise of the aircraft;
  - q_2 represents a situation in which the procedure is aborted;
  - q_3 represents verification of the ITP criteria;
  - q_4 represents the phase of instruction of the procedure;
  - q_5 represents a situation in which the pilot refuses the authorization to proceed;
  - q_6 represents a situation in which the controller does not grant the authorization to proceed;
  - q_7 represents a standard execution of the procedure;
  - q_8 represents non ITP criteria compliant execution of the procedure.
  - q_9 represents a wrong execution of the procedure. This state models situations in which procedure parameters are not fulfilled.
  - q_{10} represents wrong termination of the procedure. This state models situations in which safe termination of the procedure is guaranteed, after having resolved a conflict arising during the evolution of the manoeuvre.
  - q_{11} represents abnormal termination of the procedure. For example: if the pilot detects the occurrence of an abnormal event, i.e. failure in the ADS-B system or impossibility to keep the flight performances, he interrupts immediately the manoeuvre, he returns to the initial flight level and communicates the verification of an abnormal termination to the ATCo.
  - q_{12} represents termination of the procedure;
  - q_{13} represents execution of the procedure after ASAS conflict detection;
- $X_p \subset \mathbb{R}^6$ 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[6] 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 $i = 1, 2, ..., 13$, where L is the lift force, D the drag force, α the angle of attack, g gravitational acceleration;

- $\Sigma_p = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9\} \bigcup \{\varepsilon\}$ is the set of discrete inputs, where:

  - σ_1 represents the verification of ITP pre-conditions.
  - σ_2 represents the reassessment failed after a clearance reception.
  - σ_3 represents the ITP criteria are not verified.
  - σ_4 represents the ITP criteria verified.
  - σ_5 represents the clearance denied.
  - σ_6 represents the clearance issued.
  - σ_7 represents detection of an abnormal event.

[6]The proposed model has been taken from [11].

- σ_8 represents a situational awareness inconsistency.
- σ_9 represents an ASAS conflict detection communication.
- ε is an internal event.

- E_p is the set of transitions given by the graph depicted in Figure 3;
- $\Psi_p = \{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6, \psi_7\} \cup \{\varepsilon\}$ is the set of discrete outputs, where:
  - ψ_1 represents the clearance rejected by the crew.
  - ψ_2 represents the clearance request.
  - ψ_3 represents the setting of flight parameters for the climb.
  - ψ_4 represents the abnormal termination communication by the crew to the controller.
  - ψ_5 represents the report established at the new flight level.
  - ψ_6 represents the reversion to cruise operation.
  - ψ_7 represents the setting of flight parameters to solve an ASAS conflict detection.
  - ε represents an unobservable transition.
- η_p is the output function defined by the graph depicted in Figure 3.

3.2.2 Oceanic controller Agent

The hybrid model of the oceanic controller agent is characterized by no continuous dynamics. Hence, it reduces to a discrete event system:

$$\mathcal{H}_{atc} = (Q_{atc} \times X_{atc}, Q_{atc,0} \times X_{atc,0}, U_{atc}, Y_{atc}, \mathcal{E}_{atc}, \Sigma_{atc}, E_{atc}, \Psi_{atc}, \eta_{atc}), \quad (3)$$

where:

- $Q_{atc} = \{q_1, q_2, q_3, q_4, q_5\}$ is the set of discrete states, where:
  - q_1 represents the monitoring of the airspace.
  - q_2 represents situation in which the controller authorizes to proceed.
  - q_3 represents the wrong clearance issued.
  - q_4 represents the abnormal termination of the procedure.

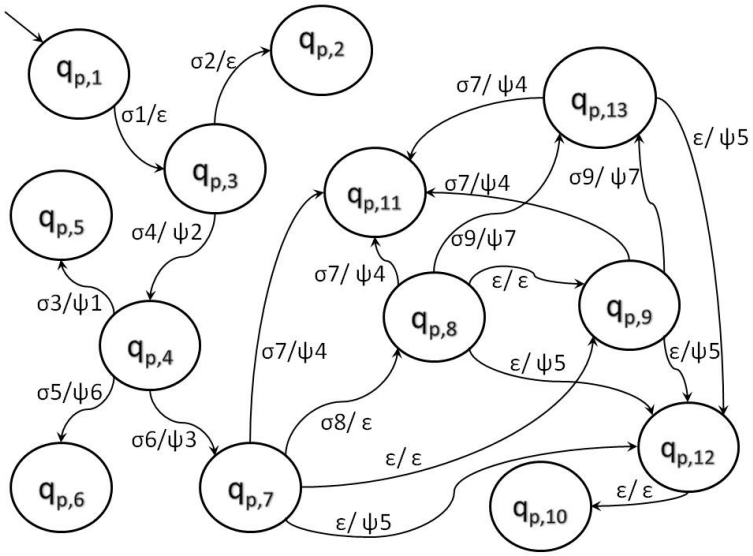

Figure 3: Directed graph of pilot flying of ITP aircraft agent.

- q_5 represents the clearance refused from the pilot.

- $Q_{atc,0} = \{q_1\}$ and $X_{atc,0} = \varnothing$.
- $U_{atc} = \varnothing$.
- $Y_{atc} = \varnothing$.
- $\mathcal{E}_{atc} = \varnothing$.
- $\Sigma_{atc} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ is the set of discrete inputs, where:
  - σ_1 represents the request of an ITP.
  - σ_2 represents the abnormal termination communication.
  - σ_3 represents a situational awareness inconsistency.
  - σ_4 represents the communication by the crew of the establishment at the new flight level.
  - σ_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 4.
- $\Psi_{atc} = \{\psi_1, \psi_2, \psi_3, \psi_3, \psi_4, \psi_5\} \cup \{\varepsilon\}$ is the set of discrete outputs where:

- ψ_1 represents the clearance issued.
- ψ_2 represents the ITP request denied.
- ψ_3 represents the communication to the aircrew of the abnormal termination message reception.
- ψ_4 represents the confirmation of the reception of a standard ITP termination message.
- ψ_5 represents the confirmation of the reception of the rejection of the clearance by the aircrew.
- ε is associated with an unobservable transition.

- $\eta_{atc} : E_{atc} \rightarrow \Psi_{atc}$ is the discrete output function defined by the graph depicted in Figure 4.

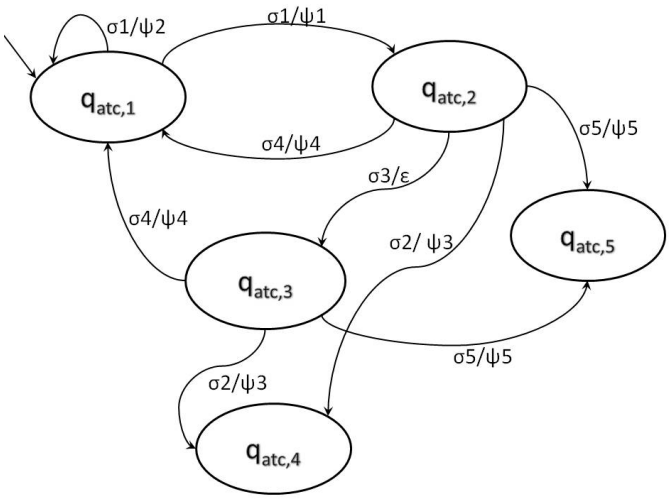

Figure 4: Discrete graph of the Oceanic Controller agent

In ATM systems one air traffic controller is responsible for more than one clearance aircraft flying in his assigned airspace. 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:

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

3.3 Analysis of critical observability in ASEP-ITP model

Consider a scenario in which N clearance aircraft $\mathcal{H}_p^1, \mathcal{H}_p^2, ..., \mathcal{H}_p^N$ and one ATCo $\mathcal{H}_{atc}$ operate. As already discussed in the previous section one ATCo interacting with N clearance aircraft can be modeled by the composition of N hybrid models $\mathcal{H}_{atc}^1, \mathcal{H}_{atc}^2, ..., \mathcal{H}_{atc}^N$ 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:

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

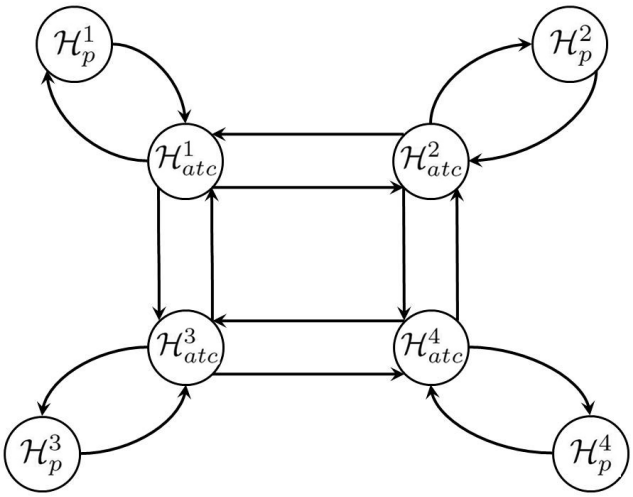

Figure 5: Interaction of $N = 5$ agents acting in the ASEP-ITP.

We consider a scenario with $N = 5$ agents, i.e. four aircraft and one ATCo. This framework results in four hybrid models for the aircraft and four hybrid models for the ATCo, as shown in Figure 5. By applying the composition rules introduced in Section 2.2, a hybrid system modeling the interaction of the agents can be defined; we denote such hybrid system by $\mathcal{H}$. In the further developments we denote state q_j of aircraft i by means of $q_{p,j}^i$ and state q_j of air traffic controller i by means of $q_{atc,j}^i$.

By applying the compositional rules introduced in Section 2.2 the hybrid system modeling the interaction of the agents $\mathcal{H}_p^i$ and $\mathcal{H}_{atc}^i$ can be defined, and resulting in:

$$\mathcal{H} = \mathcal{H}_p^1||\mathcal{H}_p^2||\mathcal{H}_p^3||\mathcal{H}_p^4||\mathcal{H}_{atc}^1||\mathcal{H}_{atc}^2||\mathcal{H}_{atc}^3||\mathcal{H}_{atc}^4. \tag{4}$$

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

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

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 ATCo 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. By applying the techniques shown in Section 2.3 a critical observer $\mathcal{O}$ can be constructed to check critical observability of $\mathcal{H}$ in (4). 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:

$$|Q| = \prod_{i=1,2,\ldots,4} |Q^i_{atc}| \cdot \prod_{i=1,2,\ldots,4} |Q^i_p| = 5^4 \cdot 13^4 \simeq 1.78 \cdot 10^7.$$

Remember from previous sections that the cardinality of the set of discrete states of the critical observer $\mathcal{O}$ for $\mathcal{H}$ grows exponentially with $|Q|$ possibly amounting to

$$2^{|Q|} \simeq 2^{1.78 \cdot 10^7} \simeq 1.03 \cdot 10^{5358034},$$

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 2.3, as follows:

Step 1. Since

$$\begin{array}{l}\mathcal{R}'_{p_i,p_j,p_k,atc_i,atc_j,atc_k} \subset \mathcal{R}'_{p_i,p_j,atc_i,atc_j}, \\ \mathcal{R}'_{p_1,p_2,p_3,p_4,atc_1,atc_2,atc_3,atc_4} \subset \mathcal{R}'_{p_i,p_j,atc_i,atc_j},\end{array} \tag{5}$$

by applying Proposition 1, the hybrid system $\mathcal{H}$ in (4) is $\mathcal{R}$–critically observable if and only if 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 if and only if:

(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 $O(4{\cdot}2^{13}) = O(32768)$; regarding condition $(C2)$ the cardinality of $|Q^i_p \times Q^j_p \times Q^i_{atc} \times Q^j_{atc}| = 13^2 \cdot 5^2 = 4225$ and the computational complexity in the construction of the critical observer is therefore given by $O(|2^{Q^i_p \times Q^j_p \times Q^i_{atc} \times Q^j_{atc}}|) \simeq O(2^{4225}) \simeq O(6.4210^{1271})$. Since we have to consider all possible combinations of the agents involved, resulting in 6 combinations, the overall computational complexity in checking condition (C2) yields $O(6.4210^{1271} \cdot 6) \simeq O(3.85 \cdot 10^{1272})$, which added to the computational complexity of condition (C1) finally amounts to

$$O(4225 + 6.4210^{1271} \cdot 6) \simeq O(3.85 \cdot 10^{1272}).$$

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 with each other and the critical relations $\mathcal{R}_{p_i}$ coincide with each other, it is sufficient to analyze critical observability of only one aircraft. Hence, the computational complexity in checking condition $(C1)$ becomes $O(2^{13}) \simeq O(8192)$. 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

$$O(8192 + 6.42 \cdot 10^{1271}) \simeq O(6.42 \cdot 10^{1271}).$$

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 if and only if $\mathcal{H}^i_p||\mathcal{H}^i_{atc}$ 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 $O(2^{13{\cdot}5} \cdot 4) \simeq O(1.47 \cdot 10^{20})$, which

added to the computational complexity in checking condition $(C1)$ yields an overall complexity equal to

$$O(2^{13} + (2^{13 \cdot 5} \cdot 4)) \simeq O(1.47 \cdot 10^{20}).$$

Step 4. Since hybrid models of $\mathcal{H}_p^i || \mathcal{H}_{atc}^i$ and $\mathcal{H}_p^j || \mathcal{H}_{atc}^j$ 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 $\mathcal{H}_p^i || \mathcal{H}_{atc}^i$ with respect to $\mathcal{R}_{p_i,atc_i}$. The overall computational complexity in checking this condition is $O(2^{13 \cdot 5}) \simeq O(3.68 \cdot 10^{19})$, which added to the computational complexity in checking condition $(C1)$ yields an overall computational complexity equal to

$$O(3.68 \cdot 10^{19}).$$

Step 5. By applying Proposition 2 the system $\mathcal{H}_p^i || \mathcal{H}_{atc}^i$ is $\mathcal{R}_{p_i,atc_i}$–critically observable if and only if $\mathcal{H}_p$ 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 $O(2^{13} + 2^5) \simeq O(8224)$, which added to the computational complexity in checking condition $(C1)$ yields an overall computational complexity equal to

$$O(8192 + 8224) \simeq O(16416).$$

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 2 observers, 1 for the agent pilot and 1 for the agent air traffic controller. The overall computational complexity required in checking conditions (C3) and (C4) is

$$O(2^{13} + 2^5) \simeq O(8224).$$

The computational complexity reduction achieved by the procedure shown above is summarized in Table 1.

The above procedure reduces the analysis of critical observability of the ASEP–ITP to the analysis of critical observability in conditions (C3) and

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

Table 1: Computational complexity reduction analysis.

(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 2.3 the following observer is obtained:

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

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 6 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), i.e.

(C3.1) $\mathcal{H}_p$ is $\mathcal{R}_p$–critically observable.

The obtained observer $\mathcal{O}_p$ illustrated in Figure 6 left panel, 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 $q_{p,12}$.

We proceed with a further step by checking the second part of condition (C3), i.e.

(C3.2) $\mathcal{H}_p$ is $\{q_{p,7}\}$–critically observable.

The obtained observer $\mathcal{O}_p$ illustrated in Figure 7 left panel, shows that $\mathcal{H}_p$ is not critically observable with respect to the set of critical states $\{q_7\}$. Indeed when the state of the critical observer $\mathcal{O}_p$ is in $\{q_7, q_8, q_9\}$ it is not

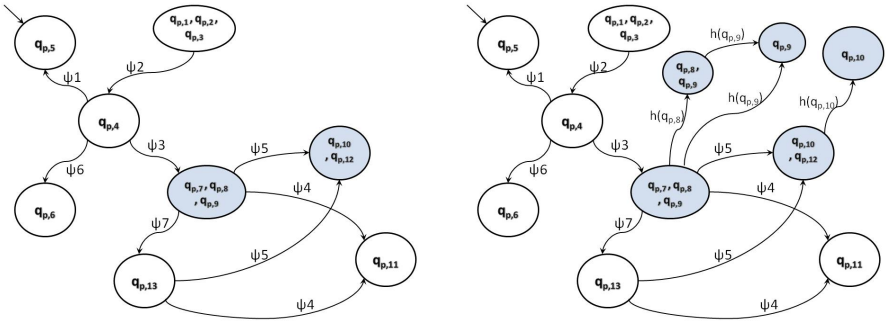

Figure 6: Left panel: $\mathcal{R}_p$–critical observer for hybrid system $\mathcal{H}_p$. Right panel: $\mathcal{R}_p$–critical observer with delay for hybrid system $\mathcal{H}_p$.

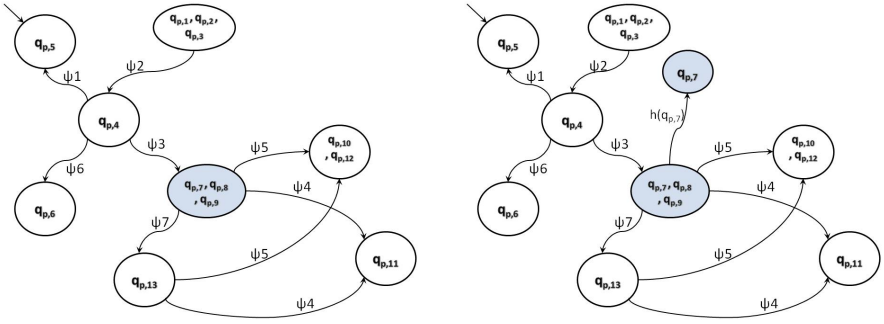

Figure 7: Left panel: $\{q_7\}$–critical observer for $\mathcal{H}_p$. Right panel: $\{q_7\}$–critical observer with delay for $\mathcal{H}_p$.

possible to distinguish the critical state q_7 from the noncritical state q_8, q_9. We conclude by checking condition (C4). 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 $\hat{Q}_{atc} = \{\{q_{atc,1}\}, \{q_{atc,2}, q_{atc,3}\}, \{q_{atc,4}\}, \{q_{atc,5}\}\}$, $\hat{Q}_{0atc} = \{\{q_{atc,1}\}\}$, $\hat{\Sigma}_{atc} = \Psi_{atc}$, $\hat{\Psi}_{atc} = \hat{Q}_{atc}$, $\hat{E}_{atc}$ is depicted in Figure 8 and $\hat{\eta}_{atc}(\hat{q}) = \hat{q}$, for any $\hat{q} \in \hat{Q}_{atc}$. The observer $\mathcal{O}_{atc}$ illustrated in Figure 8 left panel, shows that $\mathcal{H}_{atc}$ is not critically observable with respect to the set of critical states $\{q_3^{atc}\}$ because it fails in distinguishing between the critical state $q_{atc,3}$ and the noncritical state $q_{atc,2}$.

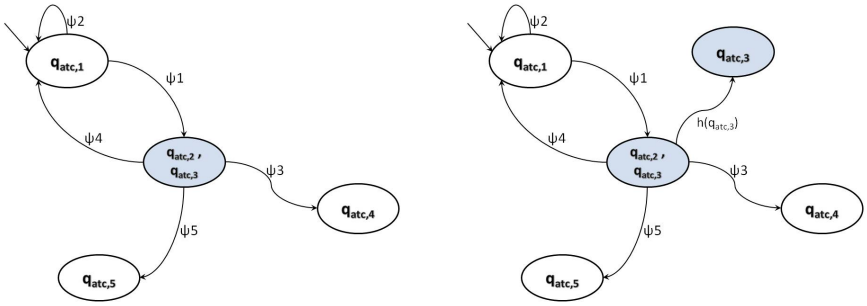

Figure 8: Left panel: $\{q_{atc,3}\}$–critical observer for $\mathcal{H}_{atc}$. Right panel: $\{q_{atc,3}\}$–critical observer with delay for $\mathcal{H}_{atc}$

3.4 Discussion of evaluation results for ASEP-ITP

From the analysis detailed above, the ASEP-ITP is not critically observable and therefore not all unsafe and/or unallowed operations can be detected.
The detection of unobservable critical states identified in the previous section can be approached, as follows.
Regarding the critical states of the hybrid model $\mathcal{H}_p$ in the critical relation $\mathcal{R}_p$ of each pilot, we define a partial function $h_p : Q_p \to \Psi_p$ that associates to each state $q \in \{q_{p,8}, q_{p,9}, q_{p,10}\}$ an additional discrete output symbol $h(q) \in \Psi_p$ as follows:

- 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 causes a time delay. The observer with delay associated with agent $\mathcal{H}_p$ and critical relation $\mathcal{R}_p$ is illustrated in Figure 6 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.

Regarding the critical state q_7 of the hybrid model $\mathcal{H}_p$, the extra discrete output $h(q_7)$ can be designed by using an alarm generated from ground surveillance systems. The obtained critical observer with delay is depicted in Figure 7 right panel.
Finally, regarding the critical state $q_{atc,3}$ in the mathematical model $\mathcal{H}_{atc}$ of the air traffic controller, the extra discrete output $h(q_{atc,3})$ can be generated by the technical instrumentations. The obtained critical observer with delay is illustrated in Figure 8 right panel.
We finally stress that even though we considered a scenario with 4 aircraft and 1 air traffic controller, the analysis here presented can be easily extended to the case where an arbitrary large number of agents operate.

4 Evaluation of ASAS Lateral Crossing Procedure

In this section we model and analyze critical observability of the ASAS Lateral Crossing Procedure [13].

4.1 Description of the ASAS Lateral Crossing Procedure

The purpose of the ASAS Lateral Crossing procedure is to provide a new set of air traffic control clearances, allowing one aircraft to cross or pass a target aircraft through the use of ASAS. The controller gives the responsibility for the separation to the flight crew of the clearance aircraft with respect to a specific single other aircraft. Except in these limited specific circumstances where the flight crew takes responsibility for separation, ATCo retains all other separation responsibility.

The separation task is delegated to the flight crew in order to support an increase in controller availability, leading to gains in efficiency, and potential capacity within the considered sectors, whilst maintaining or raising current safety levels. The ASAS Lateral Crossing procedure is a procedure in which the qualified flight crew of suitably equipped aircraft maintain safe separation when crossing one aircraft designated by ATCo, in compliance with the separation minima to be applied during the ASAS Lateral Crossing procedure, i.e. Airborne separation minima.

4.1.1 Roles and responsibilities

The separation assurance related tasks are delegated to flight crews, upon controller initiative who decides to delegate if appropriate and helpful.

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. During the execution of the ASAS Lateral Crossing procedure the flight crew of the clearance aircraft is in charge of maintaining separation from the target aircraft. Throughout the procedure, the air traffic controller remains responsible for maintaining separation between the clearance aircraft and all other aircraft in the sector.

4.1.2 Operating principles

ATCo perspective. The ASAS Lateral Crossing procedure can only be initiated by the controller. There is no obligation for the controller to use the ASAS Lateral Crossing procedure. The controller should ensure that the target will maintain its track and speed. This could be done by checking the flight plan or by giving an explicit instruction. It is not foreseen that ATCo will have to specifically inform the flight crew of the target aircraft. Then a manoeuvring envelope is defined by:

- a maximum track alteration; within the ASSTAR project, a maximum value of 45 degrees for track alteration is envisaged;
- a maximum along track distance TKmax, after which the delegation should end and the responsibility for separation would revert to the controller. By default, this distance corresponds to the along track distance between the current position of the clearance aircraft and the crossing point between the target aircraft track and the own aircraft track;
- a maximum cross track deviation, XTKmax (e.g. 8 NM).

When the clearance aircraft is clear of traffic (COT), the flight crew reports to the controller and the ASAS Lateral Crossing procedure is completed: the separation task reverts to the controller.

Airborne perspective. The flight crew performs the ASAS Lateral Crossing manoeuvre and the corresponding separation task using onboard

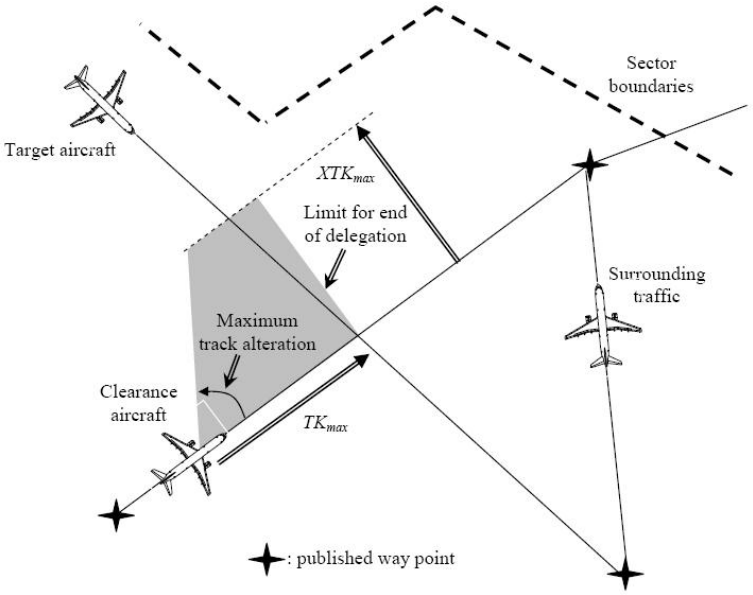

Figure 9: ASAS Lateral crossing: ATCo perspective.

ASAS functions. Prior to the acceptance of the ASAS Lateral Crossing procedure, positive identification of the target aircraft is required by the clearance aircraft. It is neither envisaged that the ASAS Lateral Crossing separation advisories are directly coupled to the aircraft flight control system without any check by the flight crew.

Indeed, the operational implementation of the ASAS separation advisories is envisioned through a pilot in the loop process. The foreseen implementation sequence is:

- the ASAS algorithms provide ASAS separation advisories on a specific display; this should enable the flight crew to anticipate the duration and the shape of the deviation.
- the flight crew analyses the ASAS separation advisories; ASAS separation advisories such as an offset route or a turning point route will be examined.
- If the flight crew is satisfied with the ASAS separation advisories, then the appropriate manual action will be undertaken by the flight crew to modify the aircraft navigation.

The flight crew will be responsible for reporting information about their navigation change back to the controller. 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 COT report and resumes

responsibility for separation. The COT point is computed such that the resuming navigation does not put the clearance aircraft and the target aircraft on converging tracks.

The Clear of Traffic (COT) point with respect to the target aircraft is generated when:

- Target and clearance aircraft are diverging laterally and the current distance between aircraft is equal or greater than the value of the applicable lateral separation.
- The resume manoeuvre anticipated onboard the clearance aircraft will not generate a conflict with the target aircraft.

It is anticipated that in some cases, no deviation from the current navigation may be required. This would result in a better flight efficiency.

4.1.3 Phases of the ASAS Lateral Crossing Procedure

The ASAS Lateral Crossing procedure can be divided into the following phases:

- **Phase 1**: set up phase
- **Phase 2**: identification phase
- **Phase 3**: clearance phase
- **Phase 4**: execution phase
- **Phase 5**: termination phase
- **Phase 6**: abort phase

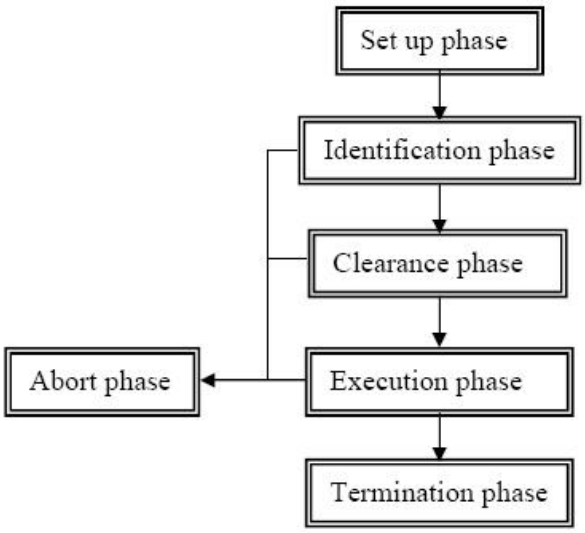

Figure 10: Phase diagram for ASAS Lateral Crossing procedure.

Set up phase. During this phase, the controller makes a decision whether to initiate the ASAS Lateral Crossing procedure. The controller checks that the following applicability conditions are satisfied:

- A conflict between the clearance aircraft and the target aircraft is anticipated by the air traffic controller;
- The angle of convergence between initial tracks is between 45 degrees and 135 degrees (that is the ICAO definition of crossing tracks).
- Appropriate ADS-B capabilities for the target aircraft.
- The target aircraft is in steady flight conditions: the controller shall ensure that the target will maintain its track and speed. This could be by checking the flight plan or by giving an explicit instruction.
- Appropriate ASAS lateral crossing capabilities for clearance aircraft.
- ASAS lateral crossing capabilities can only be used when there is sufficient time for the various stages to be performed.
- Confirmation of absence of other conflicting aircraft by checking that the distance from surrounding traffic (other than the target aircraft) to the clearance aircraft is compatible with the lateral crossing envelope manoeuvre (i.e. maximum track alteration, maximum along track distance TKmax, maximum cross track deviation, XTKmax).

If the applicability conditions are not satisfied the controller engages an ATCo based conflict resolution. Otherwise, he may initiate the identification

phase. There is no requirement for the ATCo to inform the target aircraft about the set up phase of ASAS Lateral Crossing procedure.

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 ATCo based conflict resolution.

Clearance phase. The controller passes an ASAS 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 ATCo 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 suggested new navigation enables the flight crew to anticipate the duration and the shape of the whole lateral crossing manoeuvre. Then the flight crew assesses the feasibility of the ASAS separation advisory.

If the flight crew reports that the ASAS Lateral Crossing manoeuvre is not achievable, the controller engages an ATCo based conflict resolution. Indeed, as far as air traffic controller must maintain separation between the surrounding traffic and both aircraft involved in the procedure, the lateral crossing envelope manoeuvre is a way to give some visibility of the airborne solution to the controller.

If the flight crew feels that the ASAS Lateral Crossing manoeuvre is achievable, he reports to the controller that the execution phase of the ASAS lateral crossing manoeuvre is engaged. Then, the controller monitors the separation between surrounding traffic, but does not monitor separation between the clearance aircraft and the target aircraft.

Execution phase. The execution phase deals with the implementation of the ASAS separation advisory and the monitoring of the lateral crossing manoeuvre. It is anticipated that in some cases, the trajectory suggested by the ASAS separation advisory is the same as the current navigation, so that no deviation from the current navigation will occur.

As far as the clear of traffic (COT) point is passed, the clearance aircraft reports to the controller and the termination phase is engaged. In case of inconsistent ASAS lateral crossing advisory, the clearance aircraft flight crew reports to the controller, who engages the abort phase. The manoeuvre induced by the ASAS lateral crossing advisory should not trigger short term conflict alerts (STCA). Nevertheless if such event occurs (e.g. the flight crew does not precisely follow the ASAS lateral crossing advisory), the procedure is immediately aborted by the air traffic controller.

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 COT report and resumes responsibility for separation.

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. The contingency procedure will in particular address the conditions under which the separation management task could be reverted to the controller. The controller may also initiate the termination of the ASAS Lateral Crossing procedure at any of the stages. In that case, the separation management task reverts immediately to the controller.

4.2 Modeling of the ASAS Lateral Crossing Procedure

The ASAS 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.

4.2.1 Clearance Aircraft

The hybrid model of the clearance aircraft and the pilot is given by:

$$\mathcal{H}_p = (Q_p \times X_p, Q_{p,0} \times X_{p,0}, U_p, Y_p, \mathcal{E}_p, \Sigma_p, E_p, \Psi_p, \eta_p), \tag{6}$$

where:

- $Q_p = \{q_i, i = 1, 2, ..., 15\}$ is the set of discrete states as detailed in Figure 11.
- $X_p \subset \mathbb{R}^6$ 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 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 represents the communication from the controller of target correctly identified.
- σ_3 represents the acknowledgment of feasible manoeuvre.
- σ_4 represents the acknowledgment of COT point passed.
- σ_5 represents the acknowledgment from the controller that he has received communication on the COT passed point.
- σ_6 represents the target not identified onboard (conflict detection).
- σ_7 represents the order from the controller to abort the procedure, due to uncorrect identification of the target.
- σ_8 represents the communication from the controller of target not correctly identified.
- σ_9 indicates that the manoeuvre cannot be executed (conflict detection).
- σ_{10} represents the order from the controller to undertake the procedure of back–up for wrong execution.
- σ_{11} represents the order from the controller to undertake the procedure of back–up for dangerous situation.
- σ_{12} represents the order from the controller to undertake the procedure of back–up for loss of onboard information.
- σ_{13} represents the order from the controller to undertake the procedure of back–up for unexpected behavior of the target.
- σ_{14} represents 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 11.
- $\Psi_p = \{\Psi_i, i = 1, 2, ..., 11\} \cup \{\varepsilon\}$ is the set of discrete outputs, where:
  - Ψ_1 represents the communication to the controller of the possibility to execute the manoeuvre.
  - Ψ_2 represents the communication to the controller that the CTO point was passed.
  - Ψ_3 represents the communication to the controller to abort the procedure.

- Ψ_4 represents the communication to the controller of conflict detection (target not identified).
- Ψ_5 represents the communication to the controller of conflict detection (not feasible manoeuvre).
- Ψ_6 represents the communication to the controller to abort the procedure for not feasible manoeuvre.
- Ψ_7 represents the message of confirmation to the controller of received order to undertake the procedure of back–up for wrong execution.
- Ψ_8 represents message of confirmation to the controller of received order to undertake the procedure of back–up for dangerous situation.
- Ψ_9 represents the message of confirmation to the controller of received order to undertake the procedure of back–up for loss of onboard information.
- Ψ_{10} represents 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} represents 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 11.

4.2.2 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

$$(Q_{atc} \times X_{atc}, Q_{atc,0} \times X_{atc,0}, U_{atc}, Y_{atc}, \mathcal{E}_{atc}, \Sigma_{atc}, E_{atc}, \Psi_{atc}, \eta_{atc}), \qquad (7)$$

where:

- $Q_{atc} = \{q_i, ..., i = 1, 2, ..., 9\}$ is the set of discrete state, as detailed in Figure 12 and $X_{atc} = \varnothing$.
- $Q_{atc,0} = \{q_1\}$ and $X_{atc,0} = \varnothing$.

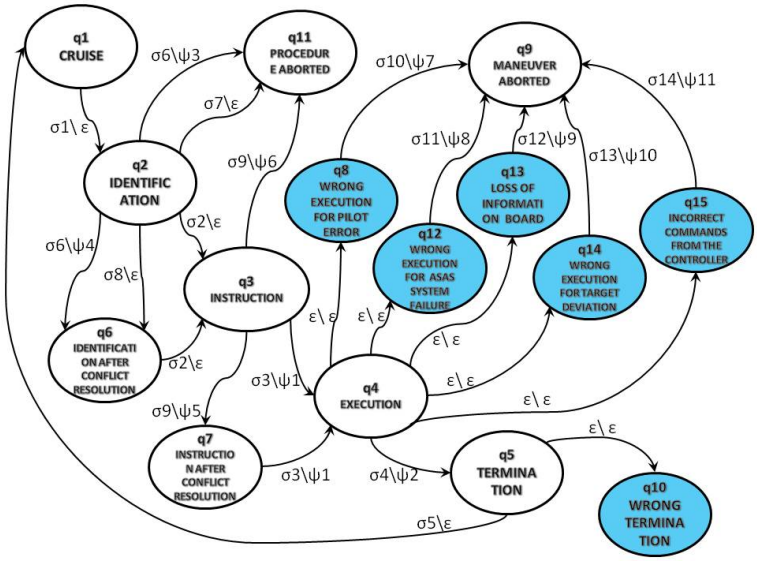

Figure 11: Hybrid system of the clearance aircraft.

- $U_{atc} = \varnothing$ 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 ASAS Lateral Crossing procedure.
  - σ_2 the acknowledgment 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 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 set–up phase.

- 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 in the instruction phase.

- E_{atc} is the set of transitions as shown in Figure 12.
- $\Psi_{atc} = \{\Psi_i, i = 1, 2, ..., 5\} \cup \{\varepsilon\}$ 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 12.

The above hybrid model is characterized by no continuous variables, so that its continuous state space X_{atc} is empty. As before, we model one air traffic controller, responsible for N clearance aircraft, by the composition of N copies of $\mathcal{H}_{atc}$:

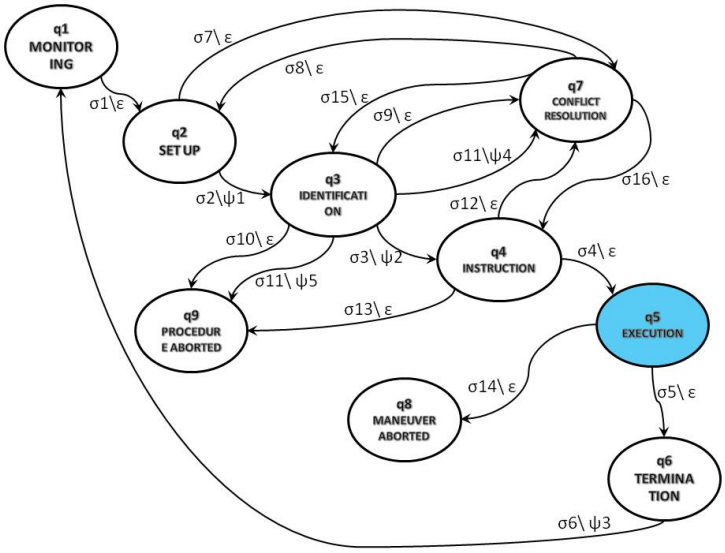

Figure 12: Hybrid system of the air traffic controller.

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

4.3 Analysis of critical observability in the ASAS Lateral Crossing Procedure

As we did in Section 3.3, we consider a scenario in which N clearance aircraft $\mathcal{H}^1_p, \mathcal{H}^2_p, ..., \mathcal{H}^N_p$ and one ATCo $\mathcal{H}_{atc}$ operate. We suppose that $N = 4$. 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.

If we had to construct a critical observer $\mathcal{O}$ to check critical observability of the hybrid model $\mathcal{H}$ representing the ASAS lateral crossing procedure, the cardinality of the state space of the obtained observer could be intractable from the computational point of view. In fact, suppose for example that $N = 4$ clearance aircraft are involved. Then the cardinality $|Q|$ of the set Q of discrete states of $\mathcal{H}$ is

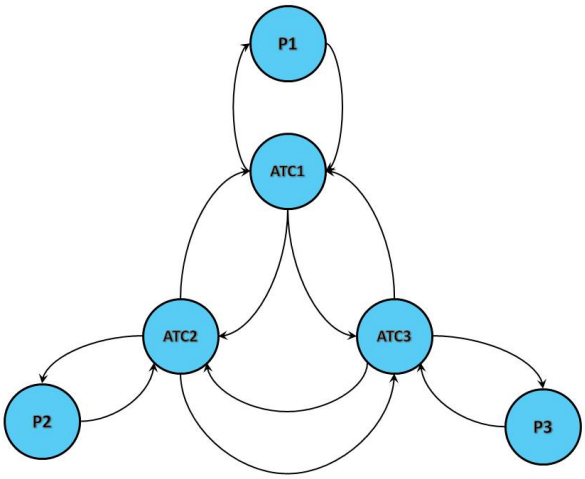

Figure 13: Interaction of $N = 4$ agents acting in the lateral crossing manouevre.

$$|Q| = \prod_{i=1,2,\ldots,4} |Q^i_{atc}| \cdot \prod_{i=1,2,\ldots,4} |Q^i_p| = 9^4 \cdot 15^4 = 3.321 \cdot 10^8.$$

The cardinality of the set of the discrete states of the critical observer $\mathcal{O}$ for $\mathcal{H}$ grows exponentially with $|Q|$ possibly amounting to $2^{|Q|} = 2^{3.321 \cdot 10^8}$ 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 2.3 and summarized in Theorem 1.
As a first step we need to define the critical relation among the agents involved. By analyzing 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 $\mathcal{R}_{p_i} = \{q^i_8, q^i_{10}, q^i_{12}, q^i_{13}, q^i_{14}, q^i_{15}\}$ is the set of critical states related to the i–th clearance aircraft and $\mathcal{R}_{p_i,atc_i,atc_j,p_j} = \{q^i_4, q^{atc,i}_5, q^{atc,j}_5, q^j_4\}$ is the set of critical states arising from the interaction of the i–th clearance aircraft, the j–th clearance aircraft, the i–th ATCo and the j–th ATCo.
By following the same reasoning as in the analysis of the ASEP–ITP detailed in the previous section, it is possible to show that the hybrid system $\mathcal{H}$ is $\mathcal{R}$–critically observable if the following conditions are satisfied:

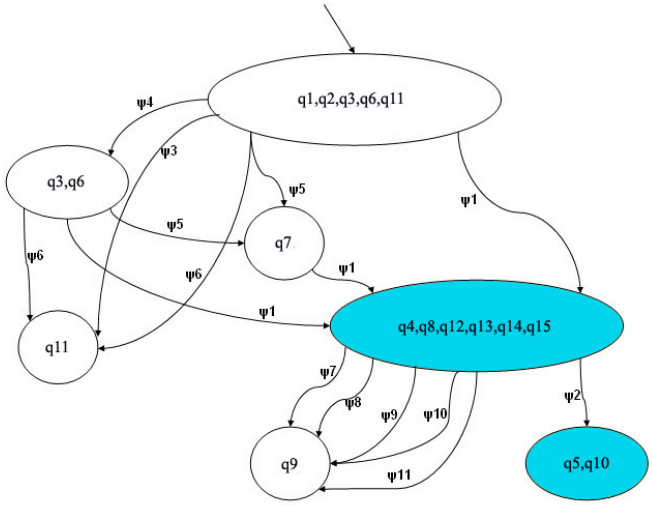

Figure 14: $\mathcal{R}_{p_i}$–critical observer for hybrid system $\mathcal{H}_p^i$.

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

(C2) $\mathcal{H}_p^i$ is $\{q_4^i\}$–critically observable.

(C3) $\mathcal{H}_{atc}^i$ is $\{q_5^{atc,i}\}$–critically observable.

We start by checking condition (C1). By using the results recalled in Section 2.3 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:

- $\hat{Q}_{p_i} = \{\{q_1^i, q_2^i, q_3^i, q_6^i, q_{11}^i\}, \{q_{11}^i\}, \{q_3^i, q_6^i\}, \{q_7^i\}, \{q_4^i, q_8^i, q_{12}^i, q_{13}^i, q_{14}^i, q_{15}^i\}, \{q_5^i, q_{10}^i\}, \{q_9^i\}\}$.
- $\hat{Q}_{0p_i} = \{\{q_1^i, q_2^i, q_3^i, q_6^i, q_{11}^i\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi}_{p_i} = \hat{Q}_{p_i}$.
- $\hat{E}_{p_i}$ is depicted in Figure 14.
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_{p_i}$.

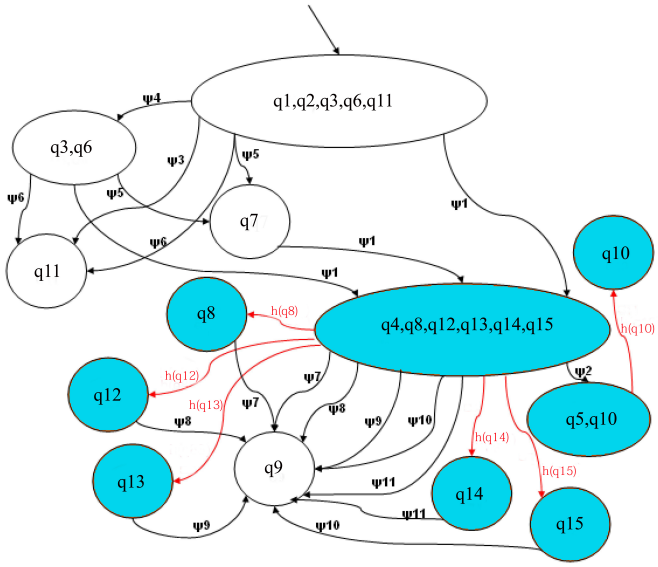

Figure 15: $\mathcal{R}_{p_i}$–critical observer with delay for hybrid system $\mathcal{H}_p^i$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 14 shows that $\mathcal{H}_p^i$ is not $\mathcal{R}_{p_i}$–critically observable. Indeed, when the state of $\mathcal{O}_{p_i}$ is in $\{q_4^i, q_8^i, q_{12}^i, q_{13}^i, q_{14}^i, q_{15}^i\}$ it is not possible to distinguish the critical states $q_8^i, q_{12}^i, q_{13}^i, q_{14}^i, q_{15}^i$ from the noncritical state q_4^i.

Analogously when the state of $\mathcal{O}_{p_i}$ is in $\{q_5^i, q_{10}^i\}$, it is not possible to distinguish the critical state q_{10}^i from the noncritical state q_5^i.

We proceed one step further by checking condition (C2). By using the results recalled in Section 2.3 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:

- $\hat{Q}_{p_i} = \{\{q_1^i, q_2^i, q_3^i, q_6^i, q_{11}^i\}, \{q_{11}^i\}, \{q_3^i, q_6^i\}, \{q_7^i\}, \{q_4^i, q_8^i, q_{12}^i, q_{13}^i, q_{14}^i, q_{15}^i\}, \{q_5^i, q_{10}^i\}, \{q_9^i\}\}$.
- $\hat{Q}_{0p_i} = \{\{q_1^{p,i}, q_2^{p,i}, q_3^{p,i}, q_6^{p,i}, q_{11}^{p,i}\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi_{p_i}} = \hat{Q}_{p_i}$.
- $\hat{E}_{p_i}$ is depicted in Figure 16.
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_p$.

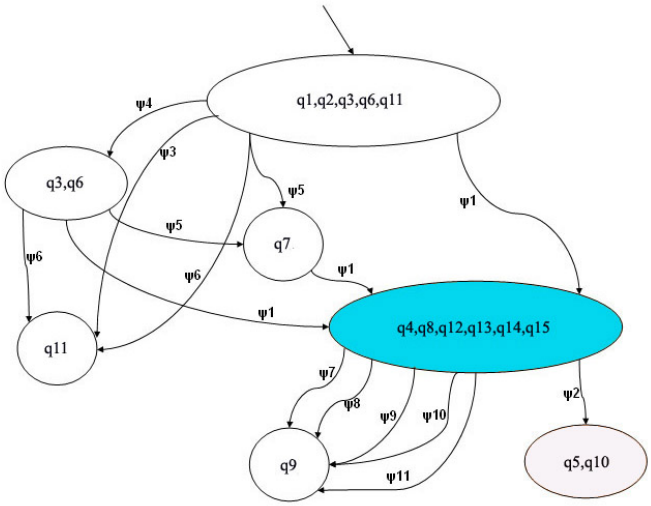

Figure 16: $\{q_4^{p,i}\}$–critical observer for $\mathcal{H}_p^i$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 16, shows that $\mathcal{H}_p^i$ is not critically observable with respect to the set of critical states $\{q_4^{p,i}\}$. Indeed when the state of the critical observer $\mathcal{O}_{p_i}$ is in $\{q_4^{p,i}, q_8^{p,i}, q_{12}^{p,i}, q_{13}^{p,i}, q_{14}^{p,i}, q_{15}^{p,i}\}$ it is not possible to distinguish the critical state $q_4^{p,i}$ from the noncritical state $q_8^{p,i}, q_{12}^{p,i}, q_{13}^{p,i}, q_{14}^{p,i}, q_{15}^{p,i}$.

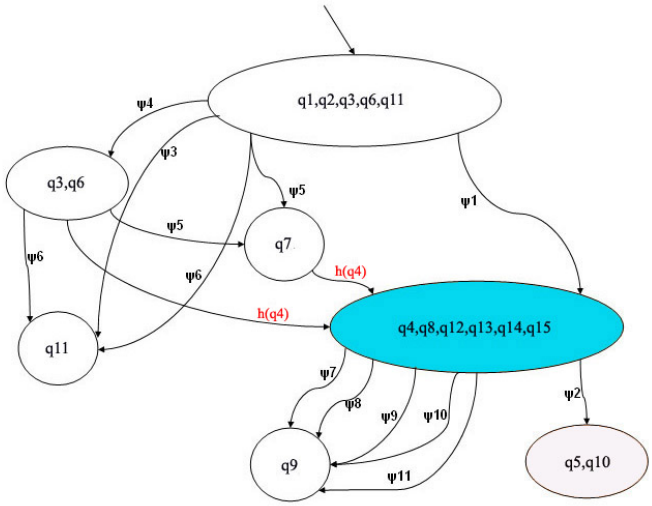

Figure 17: $\{q_4^{p,i}\}$–critical observer with delay for $\mathcal{H}_p^i$.

We conclude by checking condition (C3). By using the results recalled in Section 2.3 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:

- $\hat{Q}_{atc} = \{\{q_1, q_2, q_7\}, \{q_3, q_7, q_9\}, \{q_7\}, \{q_9\}, \{q_4, q_5, q_6, q_7, q_8, q_9\}, \{q_1\}\}$.
- $\hat{Q}_{0atc} = \{\{q_1, q_2, q_3, q_6, q_{11}\}\}$.
- $\hat{\Sigma}_{atc} = \Psi_{atc}$.
- $\hat{\Psi}_{atc} = \hat{Q}_{atc}$.
- $\hat{E}_{atc}$ is depicted in Figure 18.
- $\hat{\eta}_{atc}(\hat{q}) = \hat{q}$, for any $\hat{q} \in \hat{Q}_{atc}$.

The observer $\mathcal{O}_{atc}$ illustrated in Figure 18, shows that $\mathcal{H}_{atc}$ is not critically observable with respect to the set of critical states $\{q_5^{atc}\}$ because $\mathcal{O}_{atc}$ fails in distinguishing the critical states q_5^{atc} from the noncritical states $q_4^{atc}, q_6^{atc}, q_7^{atc}, q_8^{atc}, q_9^{atc}$.

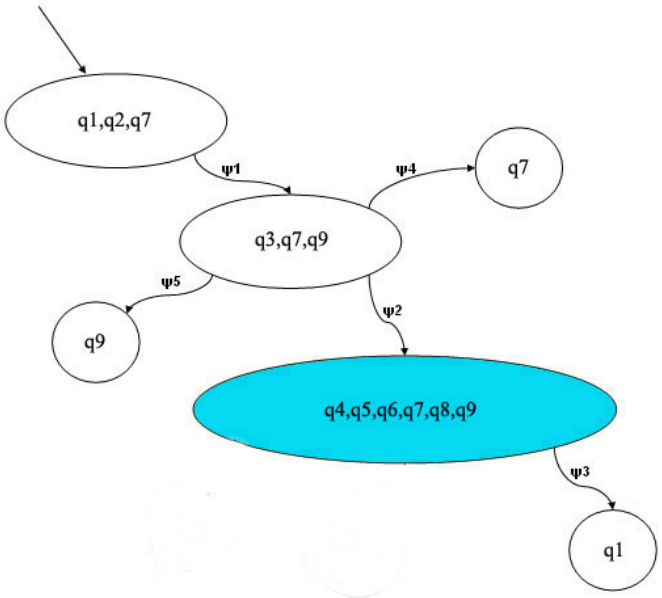

Figure 18: $\{q_5^{atc,i}\}$–critical observer for $\mathcal{H}_{atc}^i$.

4.4 Discussion of evaluation results for ASAS Lateral Crossing

From the analysis detailed above, the ASAS Lateral Crossing is not critically observable and therefore not all unsafe and/or unallowed operations by the agents can be detected.

The detection of unobservable critical states identified in the previous section can be approached, as follows.
Regarding the critical states of the hybrid model $\mathcal{H}_p^i$ in the critical relation $\mathcal{R}_{p_i}$ of each pilot, we define a partial function $h : Q_{p_i} \to \Psi_{p_i}$ that associates to each state $q \in \{q_8^i, q_{12}^i, q_{13}^i, q_{14}^i, q_{15}^i, q_{10}^i\}$ an additional discrete output symbol $h(q) \in \Psi_p$ as follows:

- The extra output $h(q_8^i)$, $h(q_{14}^{p,i})$ and $h(q_{15}^{p,i})$ could correspond to an alarm generated by the ASSAP function alert.
- The extra output $h(q_{13}^{p,i})$ can be generated by an alarm from ground surveillance systems.
- The extra output $h(q_{12}^{p,i})$ and $h(q_{10}^{p,i})$ can be obtained by using information coming from the ground systems.

The observer with delay associated with agent $\mathcal{H}_p^i$ and critical relation $\mathcal{R}_{p_i}$ is illustrated in Figure 15. The obtained observer is now critical in the

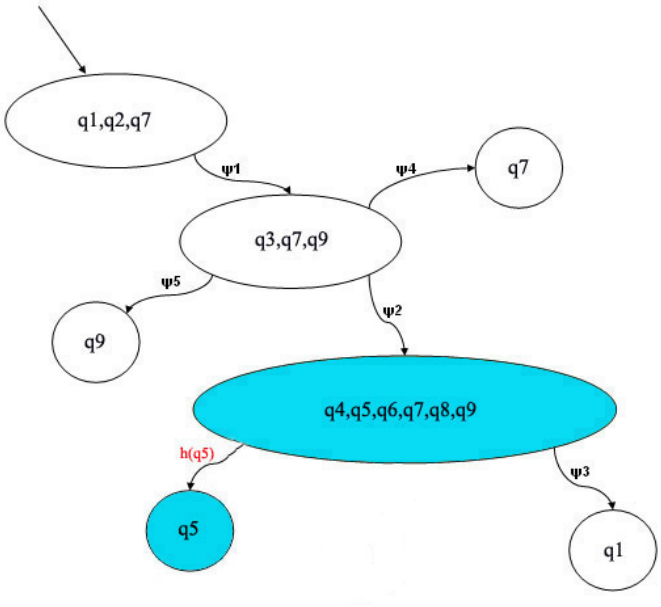

Figure 19: $\{q_5^{atc,i}\}$–critical observer with delay for $\mathcal{H}_{atc}^i$.

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.
Regarding the critical state $q_4^{p,i}$ of the hybrid model $\mathcal{H}_p^i$ the extra discrete output $h(q_4^{p,i})$ can be generated by the ground surveillance systems. The obtained critical observer with delay is illustrated in Figure 17.
Regarding the critical state q_5^{atc} of the mathematical model $\mathcal{H}_{atc}$, the extra discrete output $h(q_5^{atc})$ could be generated by the technical instrumentation. The obtained critical observer with delay is illustrated in Figure 19.
We stress that our analysis was carried out for an arbitrary large number of agents operating in the scenario.

5 Autonomous Aircraft Advanced (A^3) ConOps

In this section we analyze critical observability of a scenario in the Autonomous Aircraft Advanced (A^3) ConOps framework.

5.1 Description of the A^3 ConOps scenario

In this section, we review the main features of Scenario 1 presented in Deliverable 9.1 [6] (Section 8, page 33). Intent related non–nominal conditions identified in D7.1b [5] (some of which caused by situation awareness inconsistencies) are considered in the modeling of the scenario.
In this scenario two aircraft operate and their RBTs may intersect; in this case a conflict occurs and procedures for conflict resolution have to be designed. In particular, we focus on a mid–term conflict. Then a conflict resolution procedure is engaged and based on priority rules associated with the aircraft. Priorities are assigned to each aircraft so that when a conflict takes place, the aircraft with lower priority has to solve the conflict by generating a closed manoeuvre, i.e. a conflict solution provided in the form of a consistent RBT update; we recall also that closed manoeuvres contrast open manouevres which solve a detected conflict situation but a consistent continuation of the flight after the maneuver is not considered. In the following we describe the scenario from a single aircraft perspective. This scenario covers the situation when own aircraft is flying its RBT and a mid-term conflict is detected, i.e., the RTTL (Remaining Time To Loss of separation) for closed solution is more than STT (Short Term time Threshold). The conflict is assumed to be solved through a closed manoeuvre. Actions taken by own aircraft depend on the priorities of the aircraft involved. If own aircraft has higher priority than the other aircraft then own aircraft continues flying its RBT. The only action required on own aircraft is an enhanced monitoring of the conflicting aircraft. The other aircraft is requested instead, to solve the conflict. If the other aircraft starts to broadcast and fly a new trajectory, which does not cause other conflicts, no further actions are required on own aircraft. If TTL<STT and the other aircraft still has not broadcasted information on the resolution of the conflict, own aircraft is requested to solve the conflict through an open manoeuvre. An open manoeuvre solves the conflict situation but does not guarantee a consistent continuation of the flight. The system of the other aircraft which is requested to solve the conflict situation should suggest several possible solutions. The flight crew may select one solution and approve it or may require modifications or even suggest its own solution. As soon as the flight crew accepts one of the solu-

N.	Description
1	Own a/c intent is not conflict free and nobody is aware
2	Another a/c intent is not conflict free and nobody is aware
3	Another a/c intent intentionally not conflict free; others are not aware
4	Own a/c intent intentionally is not conflict free; others are not aware
5	Intent of ownship aircraft not broadcasted
6	Intent of one other aircraft not received
7	New intents of multiple a/c not received and crew does not know
8	Own crew has SA difference for another a/c
9	Ownship state/intent is not properly perceived by encountering crew
10	Intent exchange does not work well and nobody is aware

Table 2: Intent related non–nominal conditions identified in D7.1b.

tions and executes the manoeuvre, the new intent is broadcasted.
The correct working of this procedure relies upon many factors, one of which is a correct situation awareness of the agents involved. In particular, each agent needs to have a correct awareness of its situation and of the surrounding agents situations, as well. However, in many cases agents lack in having such correct situation awareness. Deliverable 7.1b [5] identified ten intent related (non-nominal) conditions, eight of which are caused by situation awareness inconsistencies of the agents involved. Table 2, taken from Deliverable 7.1b summarizes such conditions.
In the next section we provide a mathematical model of this scenario, where we also consider the occurrence of unsafe and/or unallowed actions taken by the agents and due to situation awareness inconsistencies.

5.2 Hybrid modeling of the A^3 ConOps scenario

The hybrid model of the aircraft and the pilot can be represented as follows:

$$\mathcal{H}_p = (Q_p \times X_p, Q_{p,0} \times X_{p,0}, U_p, Y_p, \mathcal{E}_p, \Sigma_p, E_p, \Psi_p, \eta_p), \tag{8}$$

where:

- $Q_p = \{q_i, i = 1, 2, ..., 21\}$ is the set of discrete states as detailed in Figure 20.
- $X_p \subset \mathbb{R}^6$ 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 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 $i = 1, 2, ..., 21$, where L is the lift force, D the drag force, α the angle of attack, g gravitational acceleration.

- $\Sigma_p = \{\sigma_i, i = 1, 2, ..., 27\} \cup \{\varepsilon\}$ is the set of discrete inputs, where:
  - σ_1 represents the monitoring phase.
  - σ_2 represents the detection of a MT conflict with another aircraft.
  - σ_3 represents the monitoring phase.
  - σ_4 represents an open manoeuvre initiation for the resolution of a ST conflict.
  - σ_5 represents the execution of an open manoeuvre for the resolution of a ST conflict.

- σ_6 represents the RBT update.
- σ_7 represents the normal cruise.
- σ_8 represents the generation of a closed manoeuvre with lower priority.
- σ_9 represents the initiation of analysis and the refusal of the CR solution.
- σ_{10} represents the generation of a new CR solution.
- σ_{11} represents the initiation of an open manoeuvre for the resolution of a ST conflict.
- σ_{12} represents the generation of a new CR solution.
- σ_{13} represents the analysis and the acceptance of the CR solution.
- σ_{14} represents the change in the CR solution.
- σ_{15} represents the acceptance of the CR solution.
- σ_{16} represents the execution of a closed manoeuvre.
- σ_{17} represents the conflict not solved by the other aircraft.
- σ_{18} represents the detection of a MT conflict from the other aircraft.
- σ_{19} represents the conflict solved by the other aircraft.
- σ_{20} represents the conflict not solved by the other aircraft.
- σ_{21} represents the execution of an open manoeuvre from the other aircraft.
- σ_{22} represents a non-existent MT conflict.
- σ_{23} represents not received data.
- σ_{24} represents the continuation of monitoring.
- σ_{25} represents the non-reception of data by the other aircraft.
- σ_{26} represents a problem on on-board system.
- σ_{27} represents intent not received.

- E_p is the set of transitions as shown in Figure 20.
- $\Psi_p = \{\Psi_i, i = 1, 2, ..., 12\} \cup \{\varepsilon\}$ is the set of discrete outputs, where:
  - Ψ_1 represents information on surrounding traffic.
  - Ψ_2 represents the presence of a MT conflict with the other aircraft.

- Ψ_3 represents the highest priority in the CR.
- Ψ_4 represents the continuation of monitoring.
- Ψ_5 represents the start of an open manoeuvre.
- Ψ_6 represents the execution of an open manoeuvre to solve a MT conflict.
- Ψ_7 represents the update of RBT.
- Ψ_8 represents the resolution of the conflict.
- Ψ_9 represents the broadcast of information to the other aircraft regarding the existence of a conflict.
- Ψ_{10} represents the broadcast of a new RBT and the return to regular flight.
- Ψ_{11} represents the conflict resolution.
- Ψ_{12} represents the order to the other aircraft to quit the CR through a closed manoeuvre.

- η_p is the output function as shown in Figure 20.

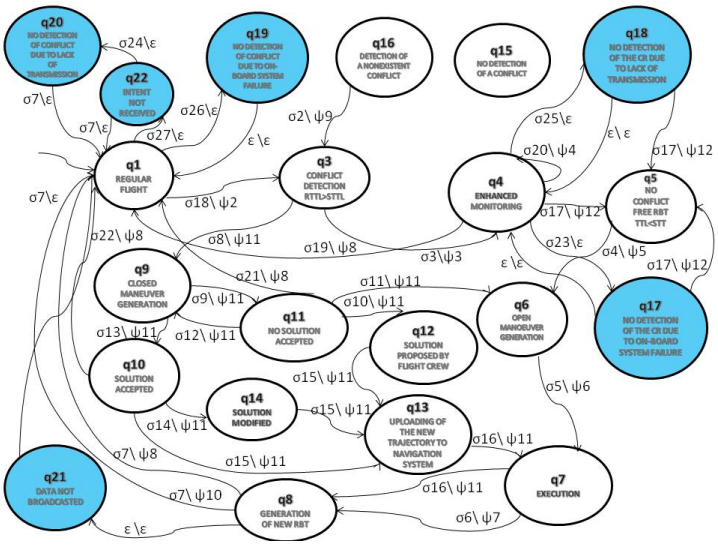

Figure 20: Hybrid system of the aircraft.

The above hybrid system models also all the situation awareness inconsistencies in the execution of ATM manoeuvres, which have been identified in Deliverable 7.1b and summarized in Table 2.

(1) **Own a/c intent is not conflict free and nobody is aware.** This situation is modeled by means of two or more hybrid systems $\mathcal{H}_p^i$ in which one hybrid system, say $\mathcal{H}_p^1$, is in state q_{15} and the remaining ones are either in state q_{19} or in state q_{20}.

(2) **Another a/c intent is not conflict free and nobody is aware.** This situation can be modeled by following the same reasoning as in the previous situation.

(3) **Another a/c intent intentionally not conflict free; others are not aware.** This situation is modeled by means of two or more hybrid systems $\mathcal{H}_p^i$ in which one hybrid system, say $\mathcal{H}_p^1$, is in state q_3 and the remaining ones are either in state q_{19} or in state q_{20}.

(4) **Own a/c intent intentionally is not conflict free; others are not aware.** This situation can be modeled by following the same reasoning as in the previous situation.

(5) **Intent of ownship aircraft not broadcasted.** This situation is modeled by means of state q_{21} in the hybrid system $\mathcal{H}_p$.

(6) **Intent of one other aircraft not received.** This situation can be modeled by following the same reasoning as in the previous situation.

(7) **New intents of multiple a/c not received and crew does not know.** This situation is modeled by means of state q_{22} in the hybrid system $\mathcal{H}_p$.

(8) **Own crew has SA difference for another a/c.** The specialization of this situation to non proper detection of conflict situations has been modeled as in case (3).

(9) **Ownship state/intent is not properly perceived by encountering crew.** This situation is modeled by means of states $q_{17}, q_{18}, q_{19}, q_{20}$ and q_{22} in the hybrid system $\mathcal{H}_p$.

(10) **Intent exchange does not work well and nobody is aware.** This situation is modeled by means of state q_{22} in the hybrid system $\mathcal{H}_p$.

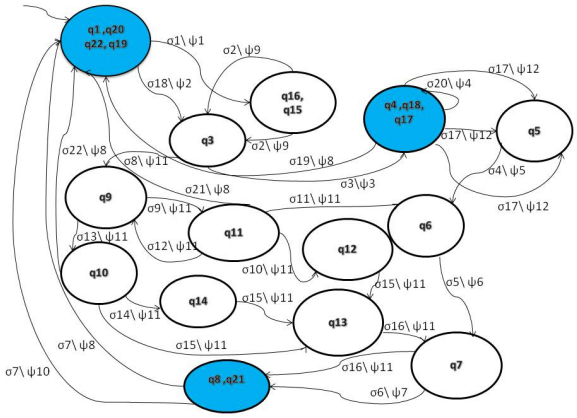

Figure 21: $\mathcal{R}_{p_i}$–critical observer for hybrid system $\mathcal{H}_p^i$.

5.3 Analysis of critical observability of the A^3 ConOps scenario

Consider a scenario in which N aircraft $\mathcal{H}_p^1, \mathcal{H}_p^2, ..., \mathcal{H}_p^N$ operate. 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:

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

The hybrid system modeling the interaction of the agents can be defined by applying the composition rules introduced in Section 2.2; we denote such hybrid system by $\mathcal{H}$ and use the results presented in Section 2.3 and summarized in Theorem 1 to check critical observability of $\mathcal{H}$.
As a first step we need to define the critical relation among the agents involved. By analyzing the hybrid models of the agents and their interaction, the following critical relation is obtained:

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

where $\mathcal{R}_{p_i} = \{q_{17}^{p,i}, q_{18}^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, q_{21}^{p,i}\}$ is the set of critical states related to the i–th clearance aircraft and $\mathcal{R}_{p_i,p_j} = \{(q_7^{p,i}, q_7^{p,j}), (q_{15}^{p,i}, q_{15}^{p,j}), (q_{16}^{p,i}, q_{16}^{p,j})\}$ is the set of critical states arising from the interaction of the i–th aircraft and the j–th aircraft.

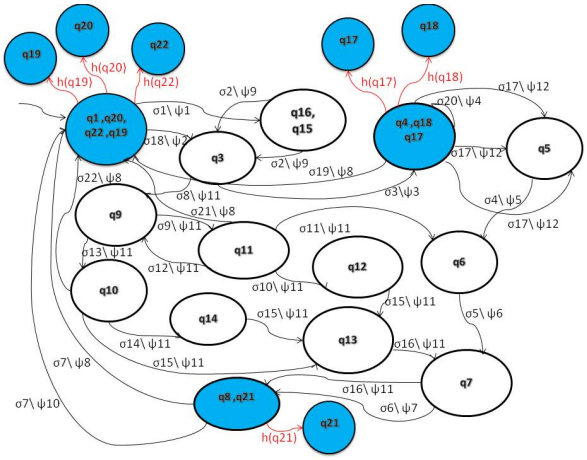

Figure 22: $\mathcal{R}_{p_i}$–critical observer with delay for hybrid system $\mathcal{H}_p^i$.

By following the same reasoning as in the analysis of the ASEP–ITP detailed in Section 3, it is possible to show that the hybrid system $\mathcal{H}$ is $\mathcal{R}$–critically observable if the following conditions are satisfied:

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

(C2) $\mathcal{H}_p^i$ is $\{q_7^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}$–critically observable.

We start by checking condition (C1). By using the results recalled in Section 2.3 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:

- $\hat{Q}_{p_i} = \{\{q_1^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, q_{22}^{p,i}\}, \{q_2^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}, \{q_4^{p,i}, q_{17}^{p,i}, q_{18}^{p,i}\}, \{q_3^{p,i}\}, \{q_5^{p,i}\}, \{q_6^{p,i}\}, \{q_7^{p,i}\}, \{q_8^{p,i}, q_{21}^{p,i}\}, \{q_9^{p,i}\}, \{q_{10}^{p,i}\}, \{q_{11}^{p,i}\}, \{q_{12}^{p,i}\}, \{q_{13}^{p,i}\}, \{q_{14}^{p,i}\}\}$.
- $\hat{Q}_{0p_i} = \{\{q_1^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, q_{22}^{p,i}\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi}_{p_i} = \hat{Q}_{p_i}$.
- $\hat{E}_{p_i}$ is depicted in Figure 21.
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_{p_i}$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 21 shows that $\mathcal{H}_p^i$ is not $\mathcal{R}_{p_i}$–critically observable. Indeed when the state of $\mathcal{O}_{p_i}$ is in $\{q_1^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, q_{22}^{p,i}\}$ it is not possible to distinguish the critical states $q_{19}^{p,i}, q_{20}^{p,i}$ from the noncritical state $q_1^{p,i}$. Analogously when the state of $\mathcal{O}_{p_i}$ is in $\{q_4^{p,i}, q_{17}^{p,i}, q_{18}^{p,i}\}$, it is not possible to distinguish the critical states $q_{17}^{p,i}, q_{18}^{p,i}$ from the noncritical state $q_4^{p,i}$. When the state of $\mathcal{O}_{p_i}$ is in $\{q_8^{p,i}, q_{21}^{p,i}\}$, it is not possible to distinguish the critical state $q_{21}^{p,i}$ from the noncritical state $q_8^{p,i}$.

We proceed one step further by checking condition (C2). By using the results recalled in Section 2.3, 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:

- $\hat{Q}_{p_i} = \{\{q_1^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, , q_{22}^{p,i}\}, \{q_2^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}, \{q_{15}^{p,i}, q_{16}^{p,i}\}, \{q_3^{p,i}\}, \{q_5^{p,i}\}, \{q_6^{p,i}\}$ $, \{q_7^{p,i}\}, \{q_8^{p,i}, q_{21}^{p,i}\}, \{q_9^{p,i}\}, \{q_{10}^{p,i}\}, \{q_{11}^{p,i}\}, \{q_{12}^{p,i}\}, \{q_{13}^{p,i}t\}, \{q_{14}^{p,i}\}\}$.
- $\hat{Q}_{0p_i} = \{\{q_1^{p,i}, q_{19}^{p,i}, q_{20}^{p,i}, q_{22}^{p,i}\}\}$.
- $\hat{\Sigma}_{p_i} = \Psi_{p_i}$.
- $\hat{\Psi_{p_i}} = \hat{Q}_{p_i}$.
- $\hat{E}_{p_i}$ is depicted in Figure 23.
- $\hat{\eta}_{p_i}(\hat{q}) = \hat{q}$ for any $\hat{q} \in \hat{Q}_p$.

The obtained observer $\mathcal{O}_{p_i}$ illustrated in Figure 23 left panel, shows that $\mathcal{H}_p^i$ is not critically observable with respect to the set of critical states $\{q_7^{p,i}\}, \{q_{15}^{p,i}\}, \{q_{16}^{p,i}\}$. Indeed when the state of the critical observer $\mathcal{O}_{p_i}$ is in $\{q_2^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}$ it is not possible to distinguish the critical states $q_{15}^{p,i}$,$q_{16}^{p,i}$ from the noncritical state $q_2^{p,i}$.

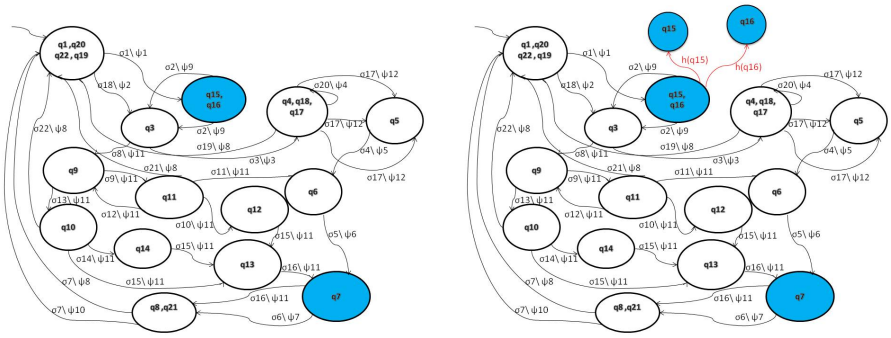

Figure 23: Left panel: $\{q_2^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}$–critical observer for $\mathcal{H}_p^i$. Right panel: $\{q_2^{p,i}, q_{15}^{p,i}, q_{16}^{p,i}\}$–critical observer with delay for $\mathcal{H}_p^i$.

5.4 Discussion of evaluation results for A^3 ConOps

The formal analysis of the A^3 ConOps scenario reported in the above section demonstrated that this scenario is not critically observable. In particular, according to the previous analysis, this happens because:

- It is not possible to distinguish critical states q_{19} and q_{20} from the non-critical state q_1.
- It is not possible to distinguish critical states q_{17} and q_{18} from the noncritical state q_4.
- It is not possible to distinguish critical state q_{21} from the noncritical state q_8.
- It is not possible to distinguish critical states q_{19}, q_{20}, q_{22} from the noncritical state q_1.
- It is not possible to distinguish critical states q_{15} and q_{16} from the noncritical state q_2.

An analysis of the mitigation means of potential unsafe events due to not detection of the aforementioned critical states has been performed in collaboration with Honeywell. Such analysis is reported hereafter:

1. Critical states q_{20}, q_{18}, q_{22} related to the absence of transmission. This type of failure is detectable for onboard system. According to D9.3 the update rates are required both for state and intent ADS-B messages.

If information is not refreshed within the specified time period, information is marked as degraded and alternative information sources (e.g. SWIM, point-to-point data links) are used to get recent data. Furthermore, for the degraded intent information the trajectory prediction used in CD is reduced to shorter look-ahead time. Also there is onboard conformance monitoring function, continuously comparing the received state data with the available intent information and again reducing the look-ahead time when a deviation is detected. Furthermore, an independent CD functions working only with state data is required within ASAS equipment.

2. Critical states q_{17} and q_{19} related to the failure of onboard (ASAS) equipment. The main mitigation mean for this type of failure are built–in test functions which inform flight crew about a failure of the system. Another backup is the situation awareness of the flight crew maintained through CDTI. However, this type of CD may be feasible only for short term time horizon (e.g., ATCo today considers about 5 minutes look ahead time only). The potential needs for further mitigation means (e.g., some form of explicit coordination or ground support) should be identified within the concept validation.

3. Critical states q_{15} and q_{16} related to the general failure of CD function. The main mitigation of the impact (effect) for this type of problems is the short-term CR with implicit coordination ensuring that the other conflicting aircraft will solve potential conflict even without the manoeuvering of own aircraft. Considering the prevention of this hazard, the flight crew situation awareness and training remain the main mitigation means. However, the same statement about the validation as in item 2 applies here.

4. Critical state q_{21} not affecting own onboard functions. This failure is difficult to detect onboard own aircraft. In addition to built-in test function in transponder, it is assumed that within the SWIM there will be a conformance monitoring function (ASSUMP-OPA.4) detecting if there is no deviation between the known RBT and actual state information and will potentially inform surrounding aircraft. However these aspects are not yet quite developed in A^3 ConOps and shall be refined based on the validation results.

6 Conclusions

In WP4 we used Hybrid Systems and Automata Theory formalism to model and analyze complex ATM scenarios in which a large set of possible abnormal situations may appear. Situation awareness inconsistencies have been modeled by a set of critical states. We defined a set of critical states that correspond to situation awareness inconsistencies. The possibility of detecting those critical states depends on the so–called critical observability property of the system: if the hybrid model is critically observable, our algorithms allow the detection of errors, on the basis of the information available. If the hybrid model is not critically observable, then our proposed approach is able to identify potential extra information that could be of use in obtaining critical observability.

In this deliverable we develop a compositional framework to model and analyze a complex multi–agent ATM scenario. We addressed critical observability of a composition of hybrid systems. We first proposed a definition of composition based on the exchange of discrete data between the systems involved. Then, we investigated compositional properties for critically observable subsystems. We proposed a method for separately analyzing the single agents instead of analyzing directly their composition, which usually generates an explosion of the computational complexity of the system. We proved that a safety critical observer for the total system can be derived from the critical observers designed for each of the subsystems. We considered three different procedures involving an arbitrary number of agents, the ASEP-ITP [1], the ASAS Lateral Crossing procedure [13] and an Autonomous Aircraft Advanced (A^3) ConOps [8] scenario from Deliverable D9.1 [6]. The analysis of observability of critical states arising in the composition of the agents involved in those procedures presents a particular interest from the situation awareness inconsistencies point of view. Often the mathematical model of each agent i is not enough to define critical states that reflect an inconsistent situation awareness of agent i with respect to the other agents. Using our compositional framework, situation awareness inconsistencies among agents can be easily modeled by defining a relation among agents, which correspond to inconsistencies of inter-agent situation awareness.

The analysis that we performed showed that the aforementioned three case studies are not critically observable and therefore not all unsafe and/or unallowed operations can be detected. Possible solutions to render those procedures critically observable have been discussed and based on the generation of extra (alarm) signals, which detect the occurrence of such events. In particular, the critical observability analysis of the A^3 ConOps scenario has

been complemented with a detailed analysis of the current A^3 ConOps architecture employed in the scenario considered. This analysis, reported in Section 5.4 and performed in collaboration with Honeywell, finds out the potential weak points of the current concepts of operations. It therefore serves as an input to WP8 to further improve robustness of the current A^3 ConOps architecture towards the detection of safety critical operations.

Bibliography

[1] In-Trail Procedure in Procedural Airspace (ATSA-ITP) Application description. ASSTAR Projects, 21 June 2007. v.8.0.

[2] A. Ames, A. Abate, and S. Sastry. Sufficient Conditions for the Existence of Zeno Behavior in Hybrid Systems. In *Proceedings of the 44th IEEE Conference on Decision and Control, Seville, Spain*, December 2005.

[3] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A.L. Sangiovanni-Vincentelli. Design of observers for hybrid systems. In C.J. Tomlin and M.R. Greensreet, editors, *Hybrid Systems: Computation and Control*, volume 2289 of *Lecture Notes in Computer Science*, pages 76–89. Springer Verlag, 2002.

[4] M.D. Di Benedetto, A. D' Innocenzo, A. Petriccone, and G. Pola. Intermediate report on compositionality properties of critical observability. Technical report, 12 November 2010. Deliverable 4.2i, iFly.

[5] H.A.P. Blom, G.J. Bakker, M.B. Klompstra, and F.J.L. Bussink. Hazard Identification and Initial Hazard Analysis of A^3 ConOps based operation. Technical report, August 2009. Deliverable 7.1b, iFly.

[6] Petr Casek and Eva Gelnarova. Operational Services and Environment Description (OSED) of Airborne Self-Separation Procedure (SSEP). Technical report, 2009. Deliverable 9.1, iFly.

[7] M. Colageo, M. D. Di Benedetto, and A. D'Innocenzo. Report on hybrid models and critical observer synthesis for multi-agent situation awareness. Technical report, 22 May 2007. Deliverable 4.1, iFly.

[8] G. Cuevas, I. Echegoyen, J. Garcia, P. Casek, C. Keinrath, R. Weber, P. Gotthard, F. Bussink, and A. Luuk. Autonomous Aircraft Advanced (A^3) ConOps. Technical report, 22 August 2009. Deliverable 1.3, iFly.

[9] 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.

[10] E. De Santis, M. D. Di Benedetto, and G. Pola. Observability of internal variables in interconnected switching systems. In *Proceedings of the 45th IEEE Conference on Decision and Control, San Diego, CA, USA*, pages 4121–4126, December 13-15 2006.

[11] 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.

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

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

[14] J. Lygeros. Lecture notes on hybrid systems. *ENSIETA, 2-6/2*, 2004.

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

[16] M. D. Di Benedetto and S. Di Gennaro and A. D'Innocenzo. Discrete state observability of hybrid systems. *International Journal of Robust and Nonlinear Control, Special Issue on Observability and Observer Design for Hybrid Systems.*, 19(14):1564–1580, 2008.

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