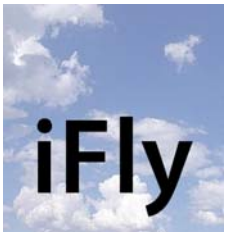


Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

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 D4.1
Report on hybrid models and critical observer synthesis for multi-agent situation awareness

Due date of deliverable: 22 February 2008
Actual submission date: 12 September 2008

Start date of project: 22 May 2007 Duration: 39 months

University of L'Aquila

Version: 1.2

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 hybrid models and critical observer synthesis for multi-agent situation awareness*
Authors of document:	*M. Colageo, M.D. Di Benedetto, A. D'Innocenzo*
Deliverable number:	*D4.1*
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 #	Issue Date	Sections affected	Relevant information
0.0	21.01.2008	All	Draft for internal review
0.1	21.02.2008	All	Second draft for internal review
1.0	20.03.2008	Chapters 2, 4, 5	Updated version for external review
1.1	15.05.08	Chapter 3, Conclusions	Updated version for external review
1.2	12.09.08	Conclusions	Final Version

Version 1.0		Organisation	Signature/Date
Authors	Marco Colageo	AQUI	
	Maria D. Di Benedetto	AQUI	
	Alessandro D'Innocenzo	AQUI	
Internal reviewers	Stefano Di Gennaro	AQUI	
	Giordano Pola	AQUI	
	Emmanuele Serra	AQUI	
	Antonio Di Francesco	AQUI	
	Henk A.P. Blom	NLR	
	Jan Kubalcik	HONEYWELL	
	Pascal Lezaud	ENAC	
	Thierry Miquel	ENAC	
External reviewers	Uwe Volckers	University of Braunschweig	

Abstract

The present report is the first deliverable of Work Package 4 of the iFLY project. In this report, we introduce the hybrid systems mathematical framework used to perform formal observability analysis of procedure errors in an Air Traffic Management multi-agent environment. Observability verification and observer construction techniques for hybrid systems are illustrated, along with their computational complexity analysis. We then develop hybrid models of the agents involved in the Airborne Traffic Situational Awareness In Trail Procedure (ATSA-ITP) and show their effectiveness by analyzing their observability properties.

Contents

Acronyms

ADS-C	Airborne Dependent Surveillance Contract
ADS-B	Airborne Dependent Surveillance Broadcast
ASAS	Airborne Separation Assistance System
ASEP	Airborne Separation
ASSTAR	Advanced Safe Separation Technologies and Algorithms
ATC	Air Traffic Controller
ATM	Air Traffic Management
ATSA	Airborne Traffic Situational Awareness
CNS	Communication Navigation Surveillance
CPDLC	Controller-Pilot Datalink Communication
DCPC	Direct Controller-Pilot Communication
FL	Flight Level
fpm	Feet per minute
HF	High Frequency
ITP	In-Trail Procedure
NM	Nautical Miles
NAT	North Atlantic Airspace
OTS	Operational Track Structure
PAC	Pacific Airspace
RVSM	Reduced Vertical Separation Minima
RFG	Requirement Focus Group
SA	Situational awareness
TCAS	Traffic Alert and Collision Avoidance System
TIS-B	Traffic Information System Broadcast
UTC	Coordinated Universal Time
VHF	Very High Frequency

Chapter 1

Introduction

In an Air Traffic Management (ATM) multi-agent distributed system, it is of paramount importance to guarantee that all agents participating in the decisions have a similar, if not identical, perception of what the situation is. Situational awareness, i.e. the perception of each agent of the surrounding environment, has been the subject of research for guaranteeing safe operation in ATM. Many operation problems (some of potential catastrophic outcome) can be traced to erroneous or inconsistent multi-agent situational awareness. The study of techniques that can detect automatically that there are problems with situational awareness, and that these problems may be leading to a catastrophic situation, is the aim of this first deliverable of Work Package 4.

The approach we propose is to develop hybrid models for the multi-agent case, and then to develop observers for these distributed hybrid systems. The hybrid observers will be targeted to critical states, i.e. behavioral modes of the hybrid model that correspond to dangerous operations, so that the complexity of the computation can be minimized. We will begin our work by analyzing hybrid models of the single agents for the verification of Situational Awareness consistency, in the presence of non deterministic disturbances. Then, we will analyze critical observability (i.e., the property related to the possibility of detecting whether the current state of the system might lead to a catastrophic state) for the proposed hybrid models. In fact, the assessment of structural properties is an important step in building techniques to cope with situational awareness issues. In the next deliverables, work will focus on compositional properties of critical observability.

In order to show effectiveness of our approach to a real ATM procedure, we consider in this report the *In-Trail Procedure (ITP)*, which is an airborne

application that provides a novel procedure for Air Traffic Service Providers to approve, and for flight crews to conduct, flight plan change operations in non-radar zones. In particular we focus on the ATSA-In-Trail procedure [24] which has been developed to support a potential improvement of air traffic operations in Oceanic areas.

ATSA-ITP aims to improve the efficiency of the flight level change manoeuvre, with respect to the current procedure. In fact, in the last years, the volume of air traffic has significantly increased. This situation has favored the aeronautical industrial sector. However, the consequence has been a dramatic increase of airspace congestion that the air traffic control infrastructure is not ready to support in an efficient way. In oceanic airspace, aircraft frequently fly in close proximity one to another along the *Same Track*, with fixed vertical separation. Currently, the separation management is executed procedurally: the flight crew that desires climbing or descending to increase safety and operational benefits (i.e. fuel saving, turbulence avoidance, capacity increase, passenger comfort) can request a flight plan change grant (e.g. altitude change) to the air traffic controller. However, a change of flight level can be refused due to the presence of other aircraft at the adjacent flight levels. Standing on flight plan and information reported by the aircraft crew at each reporting point, the air traffic controller monitors the traffic situation and can allow flight level change clearance. The aircraft must be considered as "blind".

With a new procedure and an appropriate equipment, aircraft can be allowed a change of flight levels with less stringent conditions than today's procedures. One of the current research objectives is to address this problem and propose a more efficient and effective management of the air traffic. However, when introducing new procedures in an environment that is quite safe, the improvement of efficiency must not affect current safety of the flight and comfort of passengers. **It needs to be proved, with concrete evidence, that safety is not affected.**

Formally proving properties related to safety of the **ATSA-In Trail procedure** is the objective of our work. We will apply the **Hybrid Control Systems Theory** to define mathematical models of the procedural behavior of the agents involved in the ATSA-ITP. Then, we will apply results on **critical observability** of hybrid systems to investigate whether Situational Awareness errors in the ATSA-ITP can be detected, on the basis of the procedural measurable information exchanged between the flight crew and the air traffic controller, and possibly using data obtained from the technical system.

Chapter 2

Hybrid Systems and Critical Observability

In this chapter, we introduce the mathematical background that will be used for the observability analysis of ATSA-ITP. We discuss the observability property of the discrete state of hybrid systems using their continuous and discrete outputs. We propose a definition of observability motivated by safety critical applications given with respect to a subset of *critical* discrete states, that model unsafe or unallowed behaviors. We address the problem in the setting of formal (regular) languages and propose a novel observability verification algorithm. We characterize the minimal set of extra output information to be provided by the continuous signals in order to satisfy observability conditions, and propose a milder observability notion that allows a bounded delay in state detection.

2.1 Introduction

In many safety critical applications, e.g. in air traffic management procedures [8, 9, 10], it is often required to detect if the current behavior of the system is associated to a dangerous or unallowed operation. Estimation methods and observer design techniques are essential in this regard, for the design of a control strategy for error propagation avoidance and/or error recovery. Hybrid systems are a powerful tool for the analysis and control of multi agent systems. When using hybrid systems to model safety critical applications, it is convenient to model undesired or dangerous behaviors by means of discrete states that we call *critical* states. Then, the possibility of detecting dangerous situations depend on the observability properties of the

hybrid system with respect to the critical states.

Various notions of observability have been introduced in the literature for discrete event systems [22, 21, 5, 25, 20] and hybrid systems [4, 11, 6, 7, 9, 12]. Roughly speaking, hybrid observability corresponds to the estimation of the continuous and discrete components of the hybrid state the hybrid state [4]. We focus here only on the discrete component and propose a definition of observability of a hybrid system $\mathcal{H}$ with respect to a subset of discrete *critical* states. We require that the system is observable *for every control strategy*, and discuss conditions under which it is possible to detect whether the current discrete state is *critical* using the discrete and continuous outputs.

2.2 Mathematical Models

Systems that have both discrete and continuous aspects in their dynamics are called hybrid systems. One prominent theoretical framework that is used to model hybrid systems is proposed in [19], where the discrete part consists of a labeled oriented graph, and the continuous part is described by a dynamical continuous system associated to each discrete state. The interaction between the continuous and discrete part is described by invariant, guard, and reset conditions.

Definition 1 (Hybrid system)**.** *A hybrid system is a tuple* $\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, \mathcal{E}, E, \Psi, \eta, Inv, G, R)$ *such that:*

- $Q \times X$ 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
$$\mathcal{E}_q \colon \dot{x} = f_q(x, u),$$
with output $y = g_q(x)$. Given an initial condition x_0 and a *cadlag*[1] control input $u|_{t_0}^t \colon [t_0, t] \to U$, we define the solution at time t according to f_q by
$$x(t) = x_{f_q}(t, x_0, u|_{t_0}^t).$$

[1] Piecewise–continuous from the right and with left limit.

The solution exists and is unique under the assumption that f_q is assumed to be continuous with respect to time and Lipschitz continuous with respect to the dependent variables.

- $E \subseteq Q \times Q$ is a collection of edges; each edge $e \in E$ is an ordered pair of discrete states, the first component of which is the source and is denoted by $s(e)$, while the second is the target and is denoted by $t(e)$.
- 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.
- $\{Inv_q\}_{q \in Q}$ associates to each discrete state $q \in Q$ an invariant set $Inv_q \subseteq X$.
- $\{G_e\}_{e \in E}$ associates to each edge $e \in E$ a guard set $G_e \subseteq Inv_{s(e)}$.
- $\{R_e\}_{e \in E}$ associates to each edge $e \in E$ a reset map $R_e \colon Inv_{s(e)} \to 2^{Inv_{t(e)}}$. ◁

This class of hybrid automata is in general non deterministic. The continuous state evolves following deterministic dynamics, and the discrete state execution only depends on the continuous state according to guards, possibly with non deterministic behaviors in the discrete transitions.

Referring to [19], we recall the definitions of *hybrid time basis*, *hybrid execution* and *minimum and maximum dwell time.*

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 the cardinality* $|\tau|$ *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. ◁

Definition 3 (Hybrid execution)**.** *A hybrid execution is a triple $\chi = (\tau, q, x)$, where τ is a hybrid time basis, and q, x describe the evolution of the discrete and continuous state by means of functions $q\colon \tau \to Q$ piecewise continuous, and $x\colon \tau \to X$. Functions q, x are defined on the hybrid time basis τ, take values on the hybrid state space, and satisfy the continuous and discrete dynamics and their interactions (invariant, guard and reset).* ◁

Definition 4 (Minimum and maximum dwell time)**.** *Given a hybrid system $\mathcal{H}$, we define for each state $q \in Q$ a (possibly infinite) minimum dwell time $\Delta_m(q) \geq 0$ and a (possibly infinite) maximum dwell time $\Delta_M(q) \geq 0$, namely the minimum and maximum time that can be spent in the discrete state q. This implies that given an execution χ of $\mathcal{H}$, then $\Delta_m\big(q(I_k)\big) \leq t'_k - t_k \leq \Delta_M\big(q(I_k)\big)$ for all $k = 0, \cdots, |\tau|$.* ◁

Let $\mathcal{X}$ be the set of all executions χ of $\mathcal{H}$. In this paper, we consider *non blocking* [18] hybrid automata, i.e. systems such that all hybrid executions are defined for all time instants. We say that a hybrid execution is *Zeno* [2] if it is characterized by an infinite number of jumps in a finite time. We consider hybrid systems that do not generate Zeno executions.

To each execution $\chi = (\tau, q, x) \in \mathcal{X}$ we associate a unique string $\rho(\chi)$ as a sequence $\{q(I_k)\}_{k=0}^{|\tau|}$ with cardinality $|\rho(\chi)| = |\tau|$. Namely, $\rho(\chi)$ represents an execution of the discrete state $\mathcal{H}$, with $q(I_k)$ the discrete state in the time interval I_k.

Definition 5 (Formal language of executions)**.** *The formal language of the executions of a discrete state q of $\mathcal{H}$ is given by*

$$\mathcal{L} \triangleq \{\rho(\chi)\colon \chi = (\tau, q, x) \in \mathcal{X}\}.$$ ◁

Given a subset of discrete states $Q^* \subseteq Q$, we define $\mathcal{L}_{Q^*}$ the language of strings with finite cardinality, such that the last visited discrete state belongs to Q^*:

$$\mathcal{L}_{Q^*} \triangleq \left\{\rho \in \mathcal{L}\colon |\rho| < \infty, \rho_{|\rho|} \in Q^*\right\}$$

Given $q \in Q$, we abuse of notation using $\mathcal{L}_q$ for $\mathcal{L}_{\{q\}}$. Given a string $\rho = \{q(I_k)\}_{k=0}^{|\rho|}$, we define the associated output string as $\left\{\eta\big(q(I_k), q(I_{k+1})\big)\right\}_{k=0}^{|\rho|-1}$. The associated *observation* $P(\rho)$ is obtained erasing all unobservable outputs from the output string.

Definition 6 (Formal language of observations)**.** *The formal language of the discrete observations of $\mathcal{H}$ is given by*

$$\mathcal{P} \triangleq \{P(\rho)\colon \rho \in \mathcal{L}\}.$$ ◁

Given a subset of discrete states $Q^* \subseteq Q$, we define $\mathcal{P}_{Q^*}$ the language of the observations generated by strings whose last visited state belongs to Q^*:

$$\mathcal{P}_{Q^*} \triangleq \{P(\rho)\colon \rho \in \mathcal{L}_{Q^*}\}\,.$$

Since two distinct executions can generate the same observation, the intersection set $\mathcal{P}_{Q_1^*} \cap \mathcal{P}_{Q_2^*}$ is not necessarily empty for $Q_1^* \neq Q_2^*$. This is a crucial issue for observability of the discrete state, as we will show in the following sections.

We now focus on a particular subclass of non-deterministic hybrid systems, the so-called *hybrid automata*. We define three classes of hybrid automata which are of fundamental importance for the study of hybrid systems in general and in particular for the application discussed here.

Definition 7 (Hybrid automaton)**.** *A hybrid automaton is a hybrid system* $\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, \mathcal{E}, E, \Psi, \eta, \mathrm{Inv}, G, R)$ *such that* $U = \emptyset$*. So, we will denote it as a collection of objects* $\mathcal{H} = (Q \times X, Q_0 \times X_0, Y, \mathcal{E}, E, \Psi, \eta, \mathrm{Inv}, G, R)$

A hybrid automaton is non-deterministic, as is the general model; the difference is that this kind of systems is not equipped with the notion of continuous input. Hybrid automata are very important because the most advanced results in formal analysis of hybrid systems have been obtained for this class of systems; in fact, the loss of descriptive power is counterbalanced by a simpler analysis of their behavior.

We will use *rectangular sets* to define many objects of the systems. We remind that, given n bounded or unbounded intervals of the real line $B_i, i = 1, \ldots, n$, a rectangular set $B \subseteq \mathbb{R}^n$ is of the form $B = B_1 \times B_2 \times \ldots B_n$.

We first consider the class of *rectangular automata*.

Definition 8 (Rectangular automaton)**.** *A rectangular automaton is a hybrid automaton* $\mathcal{H} = (Q \times X, Q_0 \times X_0, Y, \mathcal{E}, E, \Psi, \eta, \mathrm{Inv}, G, R)$ *such that*

- *For every* $q \in Q$*, the set Inv is a rectangular set;*
- *For every* $q \in Q$*, the set of initial conditions associated to the discrete state is a rectangular set;*
- *For every* $q \in Q$*, there is a rectangular set* B^q *such that*

$$\mathcal{E}_q : \dot{x} \in B^q;$$

- *For every edge* $e \in E$*, the set Guard(e) is a rectangular set;*

- *For every edge $e \in E$, there is a rectangular set B^e and a subset $J^e \subseteq \{1, \ldots, n\}$ such that for all $x \in \mathbb{R}^n$*

$$Reset(e, q) = \{(x_1^{'}, \ldots, x_n^{'}) \in \mathbb{R}^n | \text{ for all } 1 \leq i \leq n, \text{ if } i \in J^e \text{ then } x_i^{'} \in B_i^e \text{ else } x_i^{'} = x_i\}.$$

This means that in a rectangular automaton the derivative of each variable stays between two fixed bounds, which may differ in the different locations. Furthermore, we have that the values of the domain and of the initial hybrid state in each discrete location are rectangular sets and that the guards are also rectangular sets. Finally, in each discrete transition e the value of a variable x_i is either reset nondeterministically to a new value within the interval B_i^e (if $i \in J^e$), or is left unchanged.

We decide to use rectangular automata to describe the dynamics of our case of study, the ATSA-ITP. They are simple, but the descriptive power of their dynamics is rich enough for the purposes of our investigation, as we will see in the next chapter.

The *multi-rate automata* can be seen as a particular case of rectangular automata:

Definition 9 (Multi-Rate automaton)**.** *A multi-rate automaton is a rectangular automaton that satisfies the following constraints:*

- *For every $q \in Q$, the set of initial conditions associated to the discrete state is either empty or a singleton set;*
- *For every $q \in Q$, the set B^q is a singleton state;*
- *For every edge $e \in E$, the set B^e is a singleton set.*

Therefore, in a multi-rate automaton, each variable follows constant, rational slope, which may be different in different locations.

The simplest hybrid automaton is the *timed automaton*:

Definition 10 (Timed automaton)**.** *A timed automaton is a multi-rate automaton such that for every $q \in Q, B^q = \{(1, 1, \ldots, 1)\}$.*

Timed automata are very good for encoding timing constraints and their variables can be seen as clocks associated to the time the state is in a discrete state. Automatic verification of temporal properties of timed automata is decidable, i.e. it can be done in finite time [1].

Using the same notation as above, and according to the classical definitions in [15], we define:

Definition 11 (Non deterministic finite automaton)**.** *A non deterministic finite automaton (NFA) is a tuple* $\mathcal{N} = (Q, Q_0, Q_f, \Psi, E, \eta)$*, such that the set of initial states* $Q_0 = \{q_0\}$ *is a singleton and* $Q_f \subseteq Q$ *is the set of final states. The language accepted by a NFA* $\mathcal{N}$ *is the language of the observations* $\mathcal{P}_{Q_f}$ *on the alphabet* Ψ*.* ◁

Definition 12 (Deterministic finite automaton)**.** *A deterministic finite automaton (DFA) is a NFA* $\mathcal{D} = (Q, q_0, Q_f, \Psi, E, \eta)$*, such that* $\eta \colon E \to 2^{\Psi}$ *and for each* $q \in Q$ *the set* $\{\eta(e)\}_{e \in E \colon s(e)=q}$ *is a partition of* Ψ*. The language accepted by a DFA* $\mathcal{D}$ *is the language of the observations* $\mathcal{P}_{Q_f}$ *on the alphabet* Ψ*.* ◁

Definition 13 (Regular language)**.** *A language* $\mathcal{L}$ *is called a* regular language *if there exists a NFA that accepts* $\mathcal{L}$*.* ◁

Proposition 1. *Given a regular language* $\mathcal{L}$ *accepted by a NFA* $\mathcal{N}$*, it is possible to construct a DFA* $\mathcal{D}$ *that accepts* $\mathcal{L}$*. The cardinality of the state space of* $\mathcal{D}$ *is exponential with respect to the cardinality of the state space of* $\mathcal{N}$*.* ◁

Proposition 2. *Regular languages are closed with respect to the operations of union, intersection and complement.* ◁

2.3 Observability definition

Let $Q_c \subset Q$ 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 Q_c is observable for $\mathcal{H}$ if it is possible to construct a system that, on the basis of the observation, is able to detect whether the current discrete state of $\mathcal{H}$ belongs to Q_c or not. Formally:

Definition 14 (Discrete state observer)**.** *Given a hybrid system* $\mathcal{H}$*, an observer of the critical set* Q_c *is a system* $\mathcal{O}_{Q_c}$ *whose input is the output of* $\mathcal{H}$*, and whose output* $\hat{y}(t)$ *is such that:*

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

A set Q_c *is said to be observable for* $\mathcal{H}$ *if an observer* $\mathcal{O}_{Q_c}$ *exists.* ◁

A necessary and sufficient condition for critical discrete state observability can be given in terms of observations as:

Proposition 3. *Given a hybrid system $\mathcal{H}$, the set Q_c is observable if and only if*

$$\mathcal{P}_{Q_c} \cap \mathcal{P}_{Q \setminus Q_c} = \varnothing. \tag{2.1}$$

$\triangleleft$

Intuitively, each observation can be generated either only by strings whose last visited state belongs to Q_c, or only by strings whose last visited state does not belong to Q_c.

2.4 Observability verification

We now address the observability verification problem in the setting of *regular languages* [15]. Given a hybrid system $\mathcal{H}$, one of the algorithms proposed in [4, 9, 21, 22] can be used to construct the discrete state observer $\mathcal{O}_{Q_c}$. Let $cl_\varepsilon(Q^*)$ be the ε–closure [15] of a set of states $Q^* \subseteq Q$, namely the set of states that can be reached from Q^* via a path of edges whose outputs are unobservable.

Algorithm 1 (Discrete state observer construction)**.** *Given a hybrid system $\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, \mathcal{E}, E, \Psi, \eta, Inv, G, R)$, and a critical set Q_c, construct a DFA $\mathcal{O}_{Q_c} = (\hat{Q}, \hat{q}_0, \hat{Q}_c, \hat{\Psi}, \hat{E}, \hat{\eta})$ as follows:*

1. $\hat{Q} \triangleq cl_\varepsilon(Q_0) \subseteq 2^Q$;
2. $\hat{q}_0 \triangleq \{Q_0\} \subseteq 2^Q$;
3. $\hat{Q}_c \triangleq \{\hat{q} \in \hat{Q} \colon \hat{q} \cap Q_c \neq \varnothing \wedge \hat{q} \cap Q \setminus Q_c \neq \varnothing\} \subseteq 2^Q$;
4. $\hat{\Psi} \triangleq \Psi \setminus \{\varepsilon\}$;
5. In order to define $\hat{E}$ and $\hat{\eta}$, for each unvisited discrete state $\hat{q} \in \hat{Q}$ do:
   - 5.1 For each $\psi \in \hat{\Psi}$, define $\hat{q}' = \{q' \in Q \colon \exists e \in E, \exists q \in \hat{q}, q = s(e), q' = t(e), \eta(e) = \psi\}$: if $\hat{q}' \neq \varnothing$ then assign $\hat{Q} = \hat{Q} \cup cl_\varepsilon(\hat{q}')$, $\hat{E} = \hat{E} \cup \tilde{e} = \{\hat{q}, \hat{q}'\}$, and $\tilde{\eta}(\tilde{e}) = \psi$;
   - 5.2 Mark $\hat{q}$ as visited;

$\mathcal{O}_{Q_c}$ is a deterministic finite automaton, where each discrete state $\hat{q} \in \hat{Q}$ is a subset of Q, and the final set $\hat{Q}_c$ is induced by the critical set Q_c as follows:

$$\hat{Q}_c \triangleq \{\hat{q} \in \hat{Q} \colon \hat{q} \cap Q_c \neq \varnothing \wedge \hat{q} \cap Q \setminus Q_c \neq \varnothing\}.$$

The DFA $\mathcal{O}_{Q_c}$ accepts the language $\mathcal{P}_{Q_c} \cap \mathcal{P}_{Q \setminus Q_c}$ and it is therefore possible to verify observability conditions directly on $\mathcal{O}_{Q_c}$ checking if the accepted language is empty, i.e. if $\hat{Q}_c = \varnothing$. Hence, the observability verification can be done in time exponential in $N = |Q|$ by constructing the observer. However, there exists a NFA having a discrete state space cardinality polynomial in N, which accepts the same language as $\mathcal{O}_{Q_c}$. This implies that it is possible to construct an observer that consists of a set of concurrent DFAs, and whose output is given by a logical operation on the outputs of the DFAs. We exploit this property of regular languages to define an observability verification procedure that can be executed in time polynomial in N, on a hybrid system $\mathcal{H}$ whose output is only the discrete one. The main idea of the algorithm is to use operations on regular languages to check condition (2.1), without performing the observer construction.

Algorithm 2. *Given a hybrid system $\mathcal{H}$ and a critical set Q_c:*

1. Construct the NFA $\mathcal{N}_{Q_c}$ that accepts $\mathcal{P}_{Q_c}$;
2. Construct the NFA $\mathcal{N}_{Q \setminus Q_c}$ that accepts $\mathcal{P}_{Q \setminus Q_c}$;
3. Construct the NFA $\mathcal{N}_{\cap}$ that accepts $\mathcal{P}_{Q_c} \cap \mathcal{P}_{Q \setminus Q_c}$;
4. Q_c is observable for $\mathcal{H}$ if and only if $\mathcal{N}_{\cap}$ accepts the empty language.

Theorem 1. *Algorithm 2 can be executed in $O(N^4)$.*

Proof. The first and second steps require N^2 iterations each, since $\mathcal{P}_{Q_c}, \mathcal{P}_{Q \setminus Q_c}$ are finite unions of the regular languages $|Q_c|, |Q \setminus Q_c|$, respectively. The third step requires N^4 iterations, since the intersection of the two regular languages $\mathcal{P}_{Q_c}, \mathcal{P}_{Q \setminus Q_c}$ is accepted by a NFA with state space cardinality $N^2 \times N^2$. The last step can be executed in constant time. Hence, the overall complexity is given by $2\,N^2 + N^4 \sim O(N^4)$. □

The previous result can be extended to the case of state observability after a transient of K transitions.

Proposition 4. *Given a hybrid system $\mathcal{H}$, the set Q_c is observable in K–steps if and only if*

$$\forall\, \rho\colon P(\rho) \in \mathcal{P}_{Q_c} \cap \mathcal{P}_{Q\setminus Q_c}, \quad |\rho| < K. \tag{2.2}$$

$\triangleleft$

In order to verify condition (2.2), Algorithm 2 can be adapted replacing line 4 with:

4'. Q_c is observable in K–steps for $\mathcal{H}$ if and only if the final states of $\mathcal{N}_\cap$ can only be reached by finite paths that contain less than K transitions.

The minimum value K_{min} such that Q_c is observable in K_{min}–steps can be computed in polynomial time by searching for the maximum length of all paths that reach a final state of the system $\mathcal{N}_\cap$.

2.5 Extra output design

Given a hybrid system $\mathcal{H}$ that does not satisfy the observability condition (2.1), it was proposed in [4] to exploit the knowledge coming from the continuous dynamics to generate additional discrete signals that provide extra information to discriminate the discrete states. We define a partial function $h\colon Q \to \Psi_e$ that associates to some states $q \in Q$ an additional discrete output symbol $h(q) \in \Psi_e$. Our goal is to find (Ψ_e, h) such that the observability condition (2.1) is satisfied for a set Q_c. An optimal solution (Ψ_e^*, h^*), which is not necessarily unique, is the one minimizing the number $|\Psi_e^*|$ of extra discrete outputs, and can be computed in exponential time using the following algorithm.

Algorithm 3. *Given a system $\mathcal{H}$ and a critical set Q_c:*

1. Compute $\mathcal{N}_\cap$ applying Algorithm 2 to system $\mathcal{H}$;

2. For each set $\bar{Q} \in 2^Q$, delete from $\mathcal{N}_\cap$ the discrete states (q_1, q_2) such that $q_1, q_2 \in \bar{Q}$. If the language accepted by $\mathcal{N}_\cap$ is empty, then define $\Psi_e^* \triangleq \{\psi_q\colon q \in \bar{Q}\}, h^*(q) \triangleq \psi_q$ and exit.

If (Ψ_e^*, h^*) is still undefined when the algorithm terminates, then a solution does not exist. A non optimal solution $(\Psi_e^\sharp, h^\sharp)$ can be computed in polynomial time as follows.

Algorithm 4. *Given a system $\mathcal{H}$ and a critical set Q_c:*

1. For all $q_c \in Q_c$, initialize $Q_{q_c} \triangleq \varnothing$;

2. Compute $\mathcal{N}_\cap = (Q^\cap, q_0^\cap, Q_f^\cap, \Psi^\cap, E^\cap)$ applying Algorithm 2 to system $\mathcal{H}$;

3. Given $(q_1, q_2) \in Q_f^\cap$, by definition, either $q_1 \in Q_c, q_2 \notin Q_c$, or $q_2 \in Q_c, q_1 \notin Q_c$. In the former case, add q_2 to Q_{q_1}, and in the latter case, add q_1 to Q_{q_2};

4. For any $q_c \in Q_c$ and $q \in Q_{q_c}$, define $\Psi_e^\sharp = \{\psi_q \colon q \in Q_c \text{ or } q \in \bigcup_{q_c \in Q_c} Q_{q_c}\}, h^\sharp(q) \triangleq \psi_q$.

Even if Algorithm 4 fails to find a solution, a solution may exist. Since the number $|Q|$ of discrete states is finite, Algorithms 3 and 4 are guaranteed to converge.

A solution (Ψ_e, h) obtained using the algorithms above is not necessarily achievable, since it may happen that the extra signals cannot be generated for all discrete states, or that different discrete states have "similar" continuous dynamics (namely $h(q_i) = h(q_j), q_i \neq q_j$). If our solution is achievable, we also have to consider that each signal $h(q)$ is generated using the continuous dynamics associated with q within a time $\delta_{h(q)}$. For example in [4], where a bank of Luenberger observers is used for the generation of extra outputs, $\delta_{h(q)}$ depends on the gain matrices of the observers. If the generation times $\delta_{h(q)}$ are non zero for all q (which is almost always the case), then Q_c might be not observable in the sense of Definition 14, since the extra output signals might be generated some time after the system has entered a critical discrete state. Hence, we introduce a milder definition of observability that requires a bounded delay in the detection of a critical state.

Definition 15 (Observer with bounded delay)**.** *Given a hybrid system $\mathcal{H}$, an observer with delay δ of the critical set Q_c is a system $\mathcal{O}_{Q_c}^\delta$ whose input is the output of $\mathcal{H}$, and whose output $\hat{y}(t)$ is such that:*

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

A set Q_c is said to be observable with delay δ for $\mathcal{H}$ if and only if an observer $\mathcal{O}_{Q_c}^\delta$ exists. ◁

In order to verify if the additional information obtained by (Ψ_e, h) are sufficient to satisfy the observability condition with delay, we propose a procedure to construct a system $\tilde{\mathcal{H}}$ that formalizes the generation of extra information as additional discrete output symbols. We use here the notion of minimum $\Delta_m(q)$ and maximum $\Delta_M(q)$ dwell time associated to a discrete state q (see the Appendix).

Algorithm 5. *Given a hybrid system $\mathcal{H}$:*

Construct a hybrid system $\tilde{\mathcal{H}}$ as follows. First assign $\Psi \triangleq \Psi \cup \Psi_e$, and $Y \triangleq \varnothing$. Then, for each discrete state $q \in Q$ do:

1.1. Replace each q by the discrete states q^1 and q^2, and assign $Inv_{q^2} \triangleq Inv_{q^1} \triangleq Inv_q$;

1.2. For all $e \in E$ such that $t(e) = q$ assign $t(e) \triangleq q^1$, and for all $e \in E$ such that $s(e) = q$ assign $s(e) \triangleq q^2$;

1.3. Add $e_q \triangleq (q^1, q^2)$ to E: assign $G_{e_q} \triangleq Inv_q$, $R_{e_q}(x) \triangleq x, \forall\, x \in Inv_q$, and $\eta(e_q) \triangleq h(q)$;

1.4. Assign $\Delta_m(q^1) \triangleq \Delta_M(q^1) \triangleq \delta_{h(q)}$, $\Delta_m(q^2) \triangleq \Delta_m(q) - \delta_{h(q)}$ and $\Delta_M(q^2) \triangleq \Delta_M(q) - \delta_{h(q)}$;

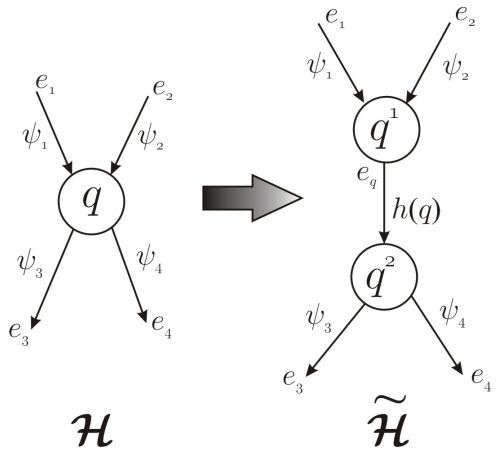


Figure 2.1: Discrete states of $\mathcal{H}$ are split by Algorithm 5, to consider the generation time of $h(q)$.

The intuition of Algorithm 5 is illustrated in Figure 2.1. We assume that the generation time $\delta_{h(q)}$ is less then the minimum dwell time $\Delta_m(q)$, namely $h(q)$ is generated before the discrete state q is left. This assumption implies that the executions of $\tilde{\mathcal{H}}$ are the same as those of $\mathcal{H}$, splitting the time bases intervals.

Proposition 5. *For each execution $\chi = (\tau, q, x)$ of $\mathcal{H}$, there exists an execution $\tilde{\chi} = (\tilde{\tau}, \tilde{q}, \tilde{x})$ of $\tilde{\mathcal{H}}$ such that:*

1. Let $\tau = \{I_k\}_{k=0}^{|\tau|}, I_k = [t_k, t'_k]$, then $\tilde{\tau} = \{I_k^1\}_{k=0}^{|\tau|} \cup \{I_k^2\}_{k=0}^{|\tau|}$, where $I_k^1 = [t_k, t_k + \delta_{h(q(I_k))}]$ and $I_k^2 = [t_k + \delta_{h(q(I_k))}, t'_k]$;

2. Let $q(I_k) = q$, then $\tilde{q}(I_k^1) = q^1, \tilde{q}(I_k^2) = q^2$;

3. $x(t) = \tilde{x}(t), \forall\, t \in \tau$.

and viceversa. ◁

It is possible to verify observability with delay for $\mathcal{H}$ by checking observability conditions (2.1) for $\tilde{\mathcal{H}}$. Let Q and $\tilde{Q}$ be the discrete state spaces of $\mathcal{H}$ and $\tilde{\mathcal{H}}$ respectively. Let $suc(q) \triangleq \{\bar{q} \in Q \colon \exists e \in E, s(e) = q, t(e) = \bar{q}\}$ be the set of successors of q.

Theorem 2. *Given $\mathcal{H}$ and $\tilde{\mathcal{H}}$, Q_c is observable with delay δ for $\mathcal{H}$ if:*

1. The set $\tilde{Q}_c \triangleq \bigcup_{q \in Q_c} \left(q^2 \cup suc(q^2)\right)$ is observable for $\tilde{\mathcal{H}}$.

2. $\delta_{h(q)} \leq \delta, \forall\, q \in Q_c \cup suc(Q_c)$.

Proof. Define $\delta^* = \max_{q \in Q_c \cup suc(Q_c)} \delta_{h(q)}$, where $\delta^* \leq \delta$ by Condition 2. Condition 1 implies that there exists an observer $\tilde{\mathcal{O}}_{\tilde{Q}_c}$ for $\tilde{\mathcal{H}}$ such that if $\tilde{q}(\tilde{I}_k) \in \tilde{Q}_c$, then the observer's output $\tilde{y}(t) = 1$ for all $t \in \tilde{I}_k$. By construction of $\tilde{\mathcal{H}}$ and by Proposition 5, there exists an observer for $\mathcal{O}_{Q_c}$ such that if $q(I_k) \in Q_c, I_k = [t_k, t'_k]$, then the observer's output $y(t) = 1$ for all $t \in \tilde{I}_k = [t_k + \delta_{h(q(I_k))}, t'_k] \supseteq [t_k + \delta^*, t'_k] \supseteq [t_k + \delta, t'_k]$. Condition 1 also implies that there exists an observer $\tilde{\mathcal{O}}_{\tilde{Q}_c}$ for $\tilde{\mathcal{H}}$ such that if $\tilde{q}(\tilde{I}_k) \notin \tilde{Q}_c$, then the observer's output $\tilde{y}(t) = 0$ for all $t \in \tilde{I}_k$. By construction of $\tilde{\mathcal{H}}$ and by Proposition 5, there exists an observer for $\mathcal{O}_{Q_c}$ such that if $q(I_k) \notin Q_c, I_k = [t_k, t'_k]$, then the observer's output $y(t) = 0$ for all $t \in \tilde{I}_k = [t_k + \delta_{h(q(I_k))}, t'_k] \supseteq [t_k + \delta^*, t'_k] \supseteq [t_k + \delta, t'_k]$. □

If Q_c is observable with delay $\delta^* \geq 0$, then it is observable with delay δ for any $\delta > \delta^*$. Let δ_{min} be the minimum value such that Q_c is observable with delay δ_{min}. Given a solution (Ψ_e, h) obtained using Algorithms 3, 4, and if the first condition of Theorem 2 holds, then $\delta_{min} = \delta^*$ as defined in the proof. The condition is only sufficient since $\tilde{\mathcal{H}}$ embeds continuous inputs and outputs of $\mathcal{H}$ by means of extra output discrete signals, and becomes necessary and sufficient if these extra output signals represent all the available information.

2.6 Illustrative example

Consider a hybrid system $\mathcal{H}$ with the discrete layer described in Figure 2.2. We show on this simple example how the theoretical results discussed above can be used to analyze discrete state observability. Let $Q_c = \{q_7\}$, and assume that $h(q_4) = h(q_7)$, i.e. the continuous dynamics of q_4 and q_7 do not allow the distinction between q_4 and q_7. It is possible to define the languages of observations for each discrete state by means of regular expressions [15]:

$$\mathcal{P}_{q_1} = \{\varepsilon\}, \quad \mathcal{P}_{q_2} = a(aa+bb)^*, \quad \mathcal{P}_{q_3} = a(bb)^*, \quad \mathcal{P}_{q_4} = a(aa+bb)^*b,$$
$$\mathcal{P}_{q_5} = a(aa+bb)^*b, \quad \mathcal{P}_{q_6} = a(bb)^*b, \quad \mathcal{P}_{q_7} = a(bb)^*b.$$

Following Algorithm 2, it is possible to compute the language

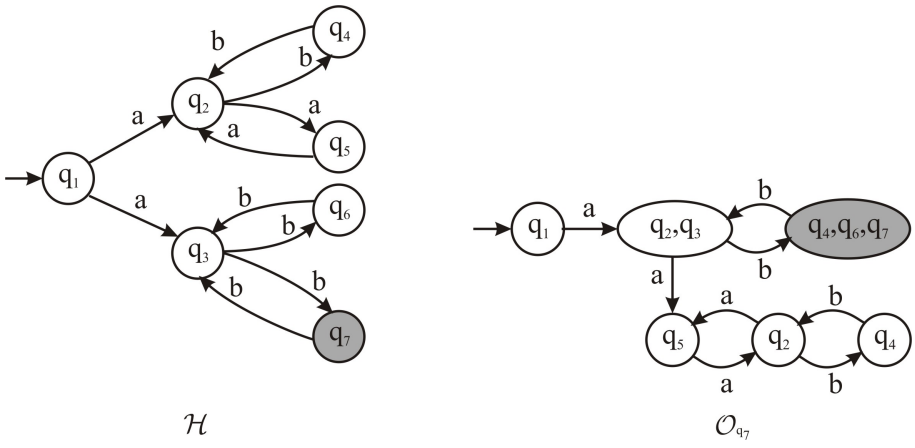


Figure 2.2: Discrete layers of $\mathcal{H}$ and $\mathcal{O}_{q_7}$

$$\mathcal{P}_{Q_c} \cap \mathcal{P}_{Q \setminus Q_c} = \mathcal{P}_{q_7} \cap \bigcup_{i=1}^{6} \mathcal{P}_{q_i} = a(bb)^* b \neq \varnothing.$$

The discrete state observer $\mathcal{O}_{q_7}$ associated to $\mathcal{H}$ is illustrated in Figure 2.2. It is clear that the system is not observable. As discussed before, we can use the information given by the continuous output, and we therefore apply Algorithms 3 and 4 to find the set of extra information we need to achieve observability. The sub–optimal approach yields to a set of extra outputs $\{h(q_4), h(q_6), h(q_7)\}$, that is not a solution to obtain observability of $\{q_7\}$ since $h(q_4) = h(q_7)$. The optimal algorithm provides the set of extra information $\{h(q_2), h(q_3)\}$. In this case, by detecting if the system visited q_2 or q_3, we anticipate the uncertainty between q_4, q_6, q_7 and we use only 2 extra outputs. Even if the generation times $\delta_{q_2}, \delta_{q_3}$ are greater than zero, Theorem 2 implies that the system augmented with the extra output $\{h(q_2), h(q_3)\}$ is observable with delay 0.

Chapter 3

Airborne Traffic Situational Awareness In Trail Procedure

In this chapter, the Airborne Traffic Situational Awareness In Trail Procedure (ATSA-ITP) is described. We first introduce some basic terms and notations. Then we define the ATSA-ITP in some detail. Finally, we propose examples of application of the procedure.

3.1 Basic definitions

The correct understanding of an airborne application requires some technical definitions. Figure 3.1 can be considered as a typical scenario for an ITP manoeuvre, and can be used to help defining terms and notations used throughout this report.

Suppose that the aircraft at flight level FL340 is fully qualified to conduct an ITP manoeuvre, and that its flight crew is considering a change of flight level towards FL370; this aircraft is called *ITP Aircraft*. FL340 is called *Initial Flight Level* whereas the FL370 is called *Requested Flight Level*, and must be a same-direction flight level above or belove the initial flight level. According to the operational region requirements, a requested flight level can be at least 2000 ft and no more than 4000 ft from the initial flight level.

Any same-direction flight level above or below the initial flight level is called *Intervening Flight Level*. Any aircraft at the intervening flight level whose *ADS-B report* is available to the ITP aircraft is called *Potentially Blocking Aircraft*. One or two of these aircraft can be identified as *Reference*

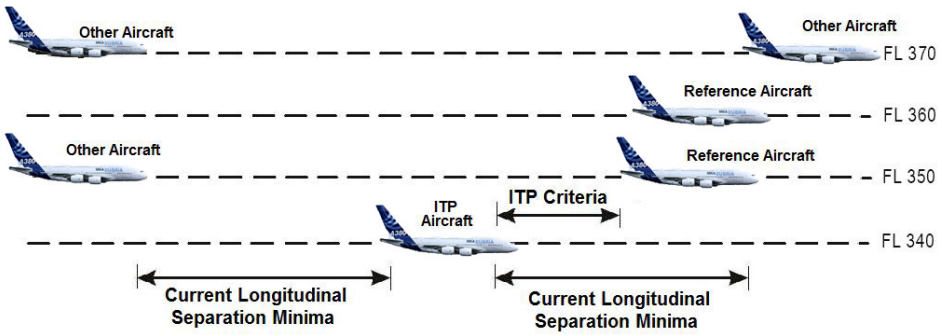


Figure 3.1: Typically ITP Scenario (Side View)

Aircraft if they meet the *ITP speed/distance criteria*, i.e. a set of values required to initiate an ITP manoeuvre.

The term *All Aircraft* is used to identify any aircraft above or below the initial flight level up to, and including, the requested flight level. The term *Other Aircraft* is used to identify all aircraft that are neither ITP aircraft nor reference aircraft.

The term *Same Track*, as defined in [3], identifies the same-direction tracks and intersecting tracks or portion of, the angular difference of which is less than 45 degrees or more than 315 degrees and whose protection area overlap (i.e. without lateral separation).

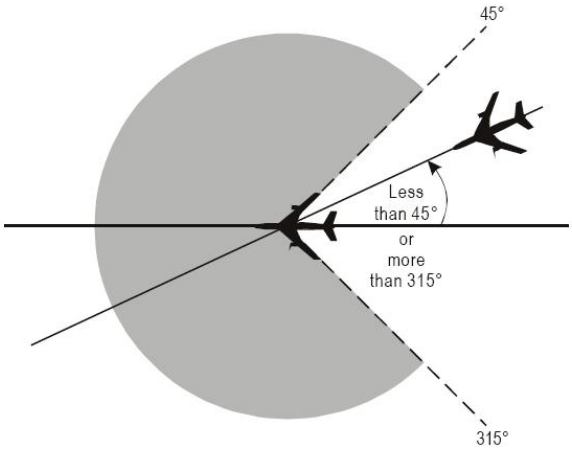


Figure 3.2: Aircraft on same track

As we will show in the next section, the airspace where ITP can be

applied is characterized by a particular structure with five or six parallel tracks. For this reason, it can be assumed that the aircraft are Same Track inside a common published track; a top view of the example scenario used in this section is depicted in Figure 3.3.

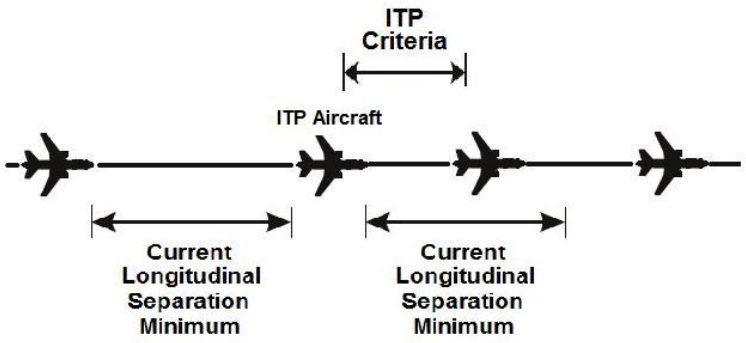


Figure 3.3: Typically ITP scenario (top view)

3.1.1 Oceanic Airspace Characteristics

The airborne procedure explained in this report is developed for the Oceanic Airspace, which lies in the international airspace where radar surveillance is unavailable and where *procedural control* is applied. These procedures provide *separation minima* between the aircraft on the basis of different methods, and require the pilot to periodically report information on the flight status (e.g. direction, speed, altitude, and arrival at predetermined way-points). The oceanic airspace controllers have to estimate the position of an airplane from pilot reports and computer models. These communications are performed using the *High Frequency (HF) Radio system*: the pilot contacts the *Oceanic Area Control Center (OAC)* via radio stations staffed by communicators. The HF is affected by weather conditions, thus audibility can be limited and sometimes impossible.

The airspaces considered are *North Atlantic (NAT)* and *Pacific (PAC)* airspaces: because of the distance to be covered, the lack of navigational aids, and the weather conditions, a system of daily tracks exists, for aircraft to be able to plan their flights using the best flight levels and winds. These operational specifications together with time zone differences and passenger demand give as an effect that most of the traffic is concentrated only on a

same direction and during a specific time interval: between 1130 UTC, and 1800 UTC for westbound flights and between 0100 UTC and 0800 UTC for eastbound flights.

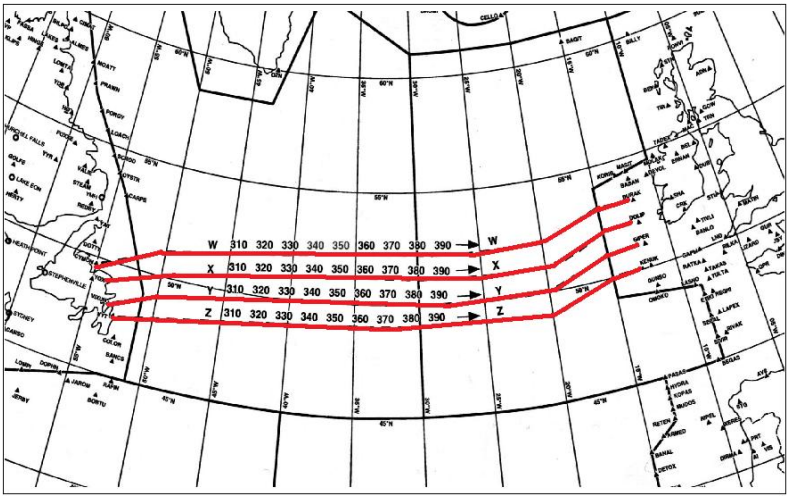


Figure 3.4: Example of night-time eastbound NAT-OTS

The definition of a specific organized tracks system is therefore necessary. *Separate Organized Track Structures (OTS)* are daily published for eastbound and westbound flows (i.e. a detailed description of the NAT-OTS is presented in [13]). This airspace usually consists of five parallel tracks, marked with alphabetic designators and separated laterally by 60 nautical miles.

Special procedures can be followed if the aircraft is unable to continue the flight inside the oceanic airspace in accordance with its *Air Traffic Controller (ATC) clearance*. All possible contingencies cannot be covered, thus the pilot's judgement shall ultimately determine the sequence of actions taken and ATC shall provide all possible assistance. The *Special Procedures for In-Flight Contingencies in Oceanic Airspace* provide a general guide to air traffic services personnel for the more frequent cases which such as:

1. Inability to maintain assigned flight level due to meteorological conditions, aircraft performance or pressurization failure;

2. En route diversion across the prevailing traffic flow;

3. Loss of, or significant reduction in, the required navigation capability when operating in an airspace where the navigation performance

accuracy is a prerequisite to the safe conduct of flight operations.

In this context an aircraft that knew or believed to be in a state of emergency, shall have the priority over the other aircraft: it can use an unlawful interference in order to inform immediately the ATC. Air Traffic Services personnel shall be prepared to recognize any indication of the occurrence of unlawful interference with an aircraft.

3.1.2 Separation management in non-radar zone

The current *separation minima* prescribed by *International Civil Aviation Organization (ICAO)* for a track system in Oceanic Airspace can be maintained with respect to three dimensions:

- *Vertical* : the separation minima are 1000 feet in *Reduced Vertical Separation Minima (RVSM)* airspace and 2000 feet in non-RVSM airspace. ATC assigns aircraft to flight levels and flight crew keep altitude.
- *Lateral* : the distance between tracks depends on the airspace. In the North Atlantic (NAT) region, the typical spacing between closest tracks is 60 Nms (or 1 degree of latitude or change latitude by no more than 2 degrees over a longitude of 10 degrees). In the composite route structure of the Pacific ICAO Region, the applicable lateral separation minimum is 50 NM. ATC assigns aircraft to tracks and flight crew maintain track.
- *Longitudinal Separation* between subsequent aircraft following the same track is provided using the *Mach Number Technique*. Typically separation minima are 10 minutes in the NAT region (i.e. at Mach 0.8, about 80 NM) and 15 minutes in the Pacific ICAO region.

Current flight level change procedures are used with these separation minima, then throughout a flight level change the aircraft have to meet these values. Today's procedures guarantee safety, but are not very efficient for fuel consumption. An increase of the number of flight level changes during the en-route flight can provide a considerable reduction of fuel burning. In these terms, the ITP introduces a new longitudinal separation criteria that enable more flight level changes with less stringent applicability conditions than today's operations. This new procedure can be applied when the aircraft are able to manipulate the *Automatic Dependent Surveillance - Broadcast Data* [16].

3.1.3 Automatic Dependent Surveillance Broadcast

The *Automatic Dependent Surveillance - Broadcast (ADS-B)* is a device that automatically and periodically, broadcasts (without pilot command) information about aircraft state vector (3D position and 3D velocity) and various information to an other ADS-equipped vehicles (aircraft or ground station) using an air-to-air datalink or air-to-ground datalink. Agents who receive these information have to decide between rejecting or processing them. This kind of ADS device represents the latest technology inside the *Communication Navigation Surveillance - Air Traffic Management (CNS-ATM)* research. The first ADS concept was based on a contract between an aircraft and ATC in order to share information and perform a particular application. This ADS system is named ADS-Contract, and it is currently used by the pilot to periodically report on the aircraft's position to the ATC throughout the oceanic flight. This kind of communication is very expensive. The ADS-Broadcast is much closer to a real-time surveillance system, and aims at providing a cheaper way of increasing efficiency without affecting safety towards the *Free Flight Concept*.

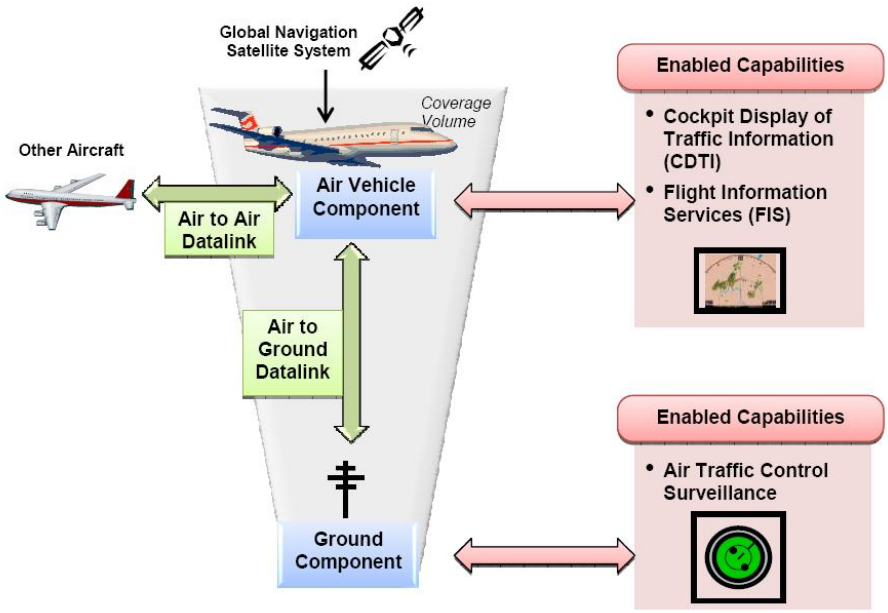


Figure 3.5: ADS-B components and links

ADS-B could be integrated into current surveillance systems where the radar coverage is available, in order to complete the available data and to improve surveillance on the airborne area. On the other hand, it could be used in remote or oceanic areas where radar surveillance is unavailable, providing the aircraft with a situational awareness of the traffic environment. The ADS-B equipment provides the aircraft with capability of receiving, processing, displaying and broadcasting the ADS-B data. Up to now, it is not planned by any State to require the ADS-B equipment on-board all aircraft. Some aircraft could be capable only of broadcasting ADS-B data (*ADS-B In aircraft*), and some aircraft could be capable only of receiving, processing and displaying ADS-B data (*ADS-B Out aircraft*). An interim solution could be implemented using the *Traffic Information Service - Broadcast (TIS-B)*, that consists of broadcasting the radar information used by ATC, via data-link, towards all aircraft (i.e. in oceanic airspace this type of data exchanges are expensive).

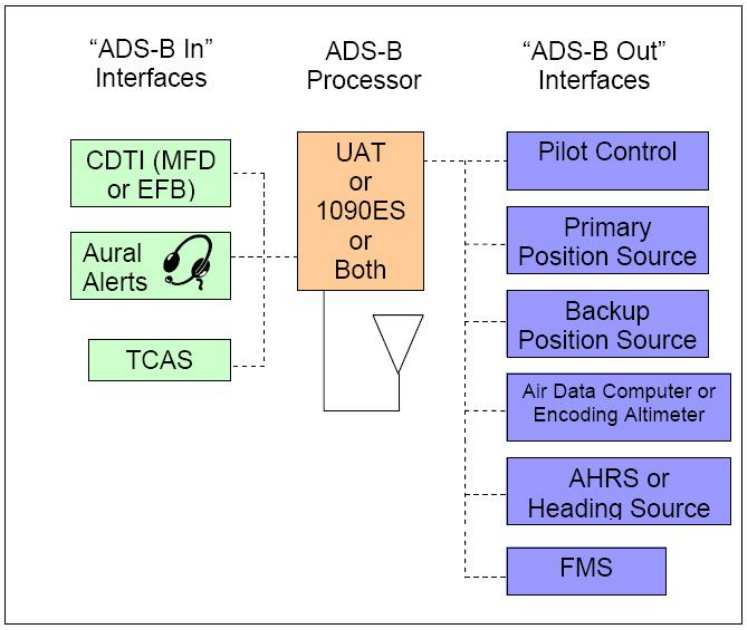


Figure 3.6: ADS-B components and links

An ADS report can be composed of data blocks selected from the following:

a) *Basic ADS* : latitude, longitude, altitude, time

b) *ground Vector* : track, ground speed, rate of climb or descent

c) *Air Vector* : heading, mach

d) *Projected profile* : next way-point, estimated altitude and estimated time at next way-point

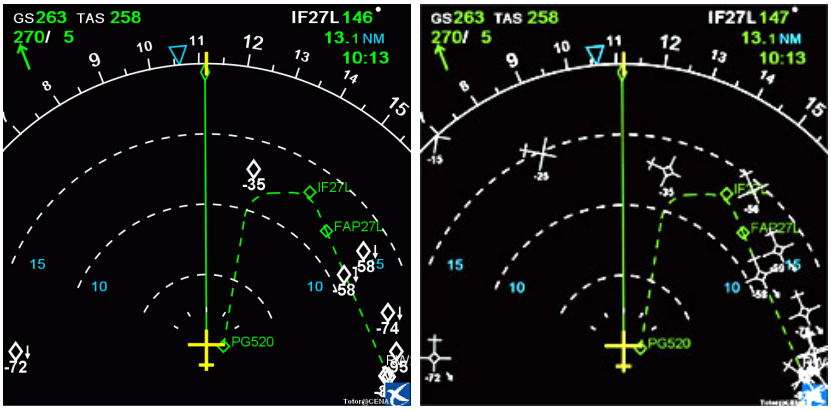
e) *Meteorological Information* : wind speed, wind direction, temperature, turbulence, humidity

However, the ADS-B transmission might produce several disadvantages when any misleading information sent by an aircraft are processed by the ATC (e.g. a wrong position). Furthermore, the image of the traffic environment that ADS-B provide to the flight crew might be incomplete because not all aircraft are equipped with ADS-B device, and thus they are not visible to the flight crew. A more detailed description of the ADS-B technology is proposed in [16].

3.1.4 Cockpit Display of Traffic Information

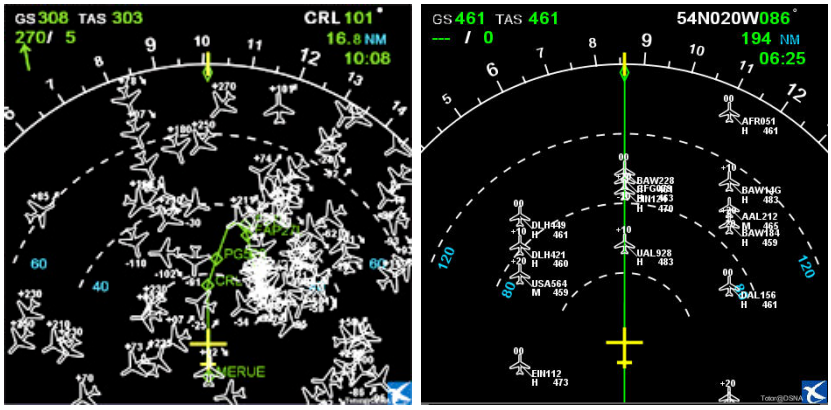
In order to provide flight crew with technical means to safely navigate their aircraft trough airspace in which airborne separation assurance is applied, additional information have to be available to the flight crew. Without ATC instructions, the flight crew can maintain separation from all aircraft even in low visibility conditions, using an *ADS-B Cockpit Display of Traffic Information (CDTI)*. This device provides permanently updated traffic information received automatically from the ADS-B equipped aircraft.

The simplest CDTI (i.e. without ADS-B data) shows nearby traffic inside a variable range less than 40NM, displaying a traffic symbol for the eight nearest aircraft with vertical tendency, relative altitude and trend information. These information are provided by the *Traffic Alert and Collision Avoidance System (TCAS)*, which is an onboard application designed in order to reduce the danger of mid-air collisions between aircraft. Through an exchange of information between all the aircraft, and using an appropriate *TCAS-Transponder*, the TCAS system is able to build a three dimensional map of the environment (i.e. maximum number of aircraft managed by TCAS is about 40), determining the relative vertical tendency, the relative altitude and the relative range for each aircraft.



(a) Simple TCAS view: each of the nearest eight aircraft within a range less of 40 NM are displayed using a rhombus with just information about the relative altitude (belove the rhombus) and the vertical tendency. The TCAS display is not suitable for clear, unambiguous awareness of the air traffic situation due the lack of heading or identification information.

(b) With ADS-B data, the image can be improved introducing the direction and identification for ranges up to 100 NM. In this way the flight crew have a useful mean to understand the environment. The traffic symbol used here can be merged with the TCAS symbol of the eight nearest aircraft without loss of clearness.



(c) Just ADS-B data: sometimes with a CDTI range up to 40 NM can require displaying of more than 100 traffic symbols. In this context the flight crew cannot use easily the CDTI views to understand the environment: using of software filters is absolutely necessary.

(d) An oceanic tracks view: the flight crew can display on the CDTI the same view that the oceanic airspace controller use, just selecting an high value of the CDTI range.

Figure 3.7: Example of CDTI views [17]

More advanced CDTI devices can use ADS-B data, together with software filters and graphical effects which allow the flight crew to select only desired traffic information (i.e. specified sub-group of traffic or more details about a single aircraft) in order to simplify the understanding of the environment when the number of aircraft is high. Furthermore, the CDTI can display useful additional information automatically generated from ADS-B data, such as closure rate, ground speed differential or Mach differential. Same examples are depicted in Figure 3.7.

3.2 ATSA-ITP description

In this section, we describe the *Airborne Traffic Situational Awareness In Trail Procedure (ATSA-ITP) [24].* This ITP application is developed by the *Requirements Focus Group (RFG)*, an international group consisting of members from the Federal Aviation Administration (FAA), the Radio Technical Commission for Aeronautics (RTCA), the European Organization for the Safety of Air Navigation (Eurocontrol), the European Organization for Civil Aviation Equipment (EUROCAE), and other interested parties. The primary object of the RFG is to internationally harmonize operational concepts and minimum safety.

The procedure has been developed within the *Airborne Traffic Situational Awareness (ATSA)* project the target of which is enhancing the flight crew's situational awareness during the flight and on the surface at airports and thus improving the flight crew's decision process for safe and efficient management of the flights. The ATSA applications provide an enhancement of currents operations for surface, airborne and visual separation procedure, without introducing radical changes in separation tasks or responsibility. The ATSA applications represent the first category of *Airborne Separation Assistance System (ASAS) [17]* applications, and a first step towards an innovative transfer of responsibility for the separation from the ATC to the flight crew.

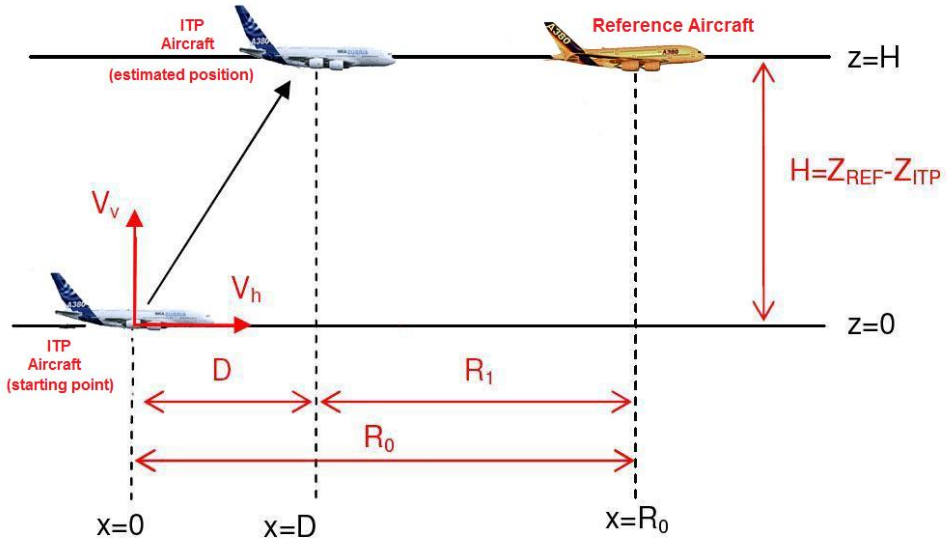
3.2.1 Overview

The purpose of *ATSA-ITP* is to enable an aircraft to perform a climb or a descent towards a requested flight level, with less stringent applicability conditions than today's operations. This procedure is based on the assumption that ADS-B data and CDTI can be used.

In the *Initiation Phase* the flight crew uses information derived on aircraft (i.e. displayed on CDTI with TCAS and ADS-B data information)

to determine if a specified set of maximum positive ground speed differential and minimum ITP distance values between the ITP aircraft and the Potentially Blocking Aircraft are met. These values represent the *ITP Speed/Distance Criteria* and have to be met prior to requesting or initiating an ITP manoeuvre. These constraints guarantee that the estimated positions between the reference aircraft and the ITP aircraft will be greater than a specified *ITP separation minimum* during the brief portion of the flight level change where the vertical separation does not exist. The proposed ITP separation minimum is 10 NM. If these criteria are met, the flight crew can request or initiate an ITP.

Figure 3.8 shows a schematic side view of an ITP manoeuvre, when the ITP aircraft is performing a climb manoeuvre and it is following a potentially blocking aircraft.



(a) In this coordinate system the potentially blocking aircraft shown in the right side on the flight level above is blocked; the ITP aircraft is in the left side on the flight level below and is moving with a ground speed V_h equal to the ground speed differential between the two aircraft. According to the ITP speed/distance criteria, the climb rate V_v has to be greater than 300 fpm and the ITP initial distance R_0 has to be greater than a specific set of values. The value R_1 represents the distance between the potentially blocking aircraft and the estimated position of the ITP aircraft during the climbing: according to the ITP speed/distance criteria, if the initiation criteria is met, this values can be no less than 10 NM.

Figure 3.8: Geometry for an ITP climb manoeuvre

In this scenario, the aircraft that wishes to perform a climb is in the flight level below (i.e. *ITP aircraft*), whereas the *potentially blocking aircraft* is in the flight level above (i.e. intervening flight level). Figure 3.8 does not include the requested flight level that the aircraft will reach at the end of ITP manoeuvre, and H represents just the altitude difference between the initial flight level and the intervening flight level.

The model is expressed in a coordinate system moving with the potentially blocking aircraft (i.e. in which the potentially blocking aircraft is still). In this way, it is possible to identify the initial horizontal range R_0 between the ITP aircraft and the potentially blocking aircraft. This range is the *ITP distance* used in the ITP speed/distance criteria, then R_0 has to be closer than a specified initiation distance value. If so, the potentially blocking aircraft can be considered as reference aircraft.

Supposing the reference aircraft is still, the ITP aircraft moves with a virtual ground speed V_h that is equal to the differential between the ITP and the reference aircraft ground speeds. Then, V_h represents the *ground speed differential* used in the ITP speed/distance criteria and has to be less than a specified maximum positive ground speed differential. The term R_1 represents the range between the position of reference aircraft and the estimated position which ITP aircraft reaches on the intervening flight level when vertical separation does not exist. The ITP aircraft moves towards the requested flight level, and then towards the intervening flight level, with a climb rate V_v specified by the ITP speed/distance criteria. Using this frame the ratio between the altitude H and the rate of climb V_v determines the time at which the ITP aircraft reaches the intervening flight level.

The ITP is limited to a total flight level change of 4000 ft: the potentially blocking aircraft can be 1000, 2000 or 3000 ft above or below the ITP aircraft. The remaining flight levels can be occupied by other aircraft flying in the same direction of or in the opposite direction to the ITP aircraft.

Air traffic controller has to check that the ITP aircraft and the reference aircraft are *Same Track* and that the maximum *positive Mach differential* was not exceeded. The separation minima between the ITP aircraft and the Reference Aircraft is not verified by the controller who has to check only the separation minima with all other aircraft.

3.2.2 Rules and Responsibility

The ATSA-ITP proposes a longitudinal separation of 10 Nm applied during the brief portion of the flight level change where the vertical separation does not exist. In the current procedure, if the estimated distance

between the ITP aircraft and another aircraft in all intervening flight levels is no greater than 10 minutes, then the ATC denies the clearance. The ITP provides a great reduction of this safety distance in order to enable more frequent flight level changes.

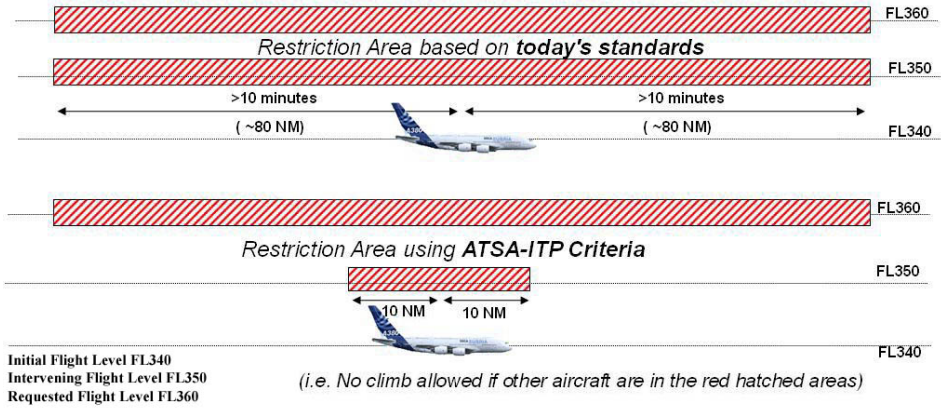


Figure 3.9: Difference between current and ITP Restriction Area

The *ITP speed/distance criteria* establish that an ITP manoeuvre might be initiated when the ITP distance is no closer than a specified initiation ITP distance, and ground speed differential is less than a specified maximum positive ground speed differential. The *Initiation Criteria* that satisfy the proposed ITP separation minimum of 10 NM are explained below:

- Initiation ITP distance of no less than 15 NM and a zero or negative ground speed differential (i.e. it provides an increasing distance between the aircraft), *or*
- Initiation ITP distance of no less than 15 NM and a positive ground speed differential of no more than 20 kts, *or*
- Initiation ITP distance of no less than 20 NM and a positive ground speed differential of no more than 30 kts.

These values of the ITP distance were selected assuming a 4000 ft flight level change at 300 fpm climb or descent rate with a 20 or 30 kts ground speed differential. The proposed initiation criteria do not contemplate a ground speed differential of more than 30 kts: in this situation, the ITP procedure cannot be requested using these initiation criteria. The ground speed differential is the only variable in the ITP distance and speed criteria

and determines the minimum ITP distance. The ITP distance criteria are the same for climbs and descents, and for both leading or following situations.

The ITP aircraft has to maintain a minimum 300 fpm rate of climb or descent and a constant Mach number throughout the ITP manoeuvre. The reference aircraft must not begin any manoeuvre during the ITP. In this context, a change of course to remain on the Same Identical Track would not be considered as a manoeuvre. On the contrary, a change of speed, flight level or direction would be considered as a manoeuvre.

The flight crew cannot request a flight level change over 4000 ft: an additional flight level change would be requested separately before or after the ITP is completed.

The controller has to check the positive Mach differential between the ITP aircraft and the reference aircraft, in order to provide potentially unsafe closure rates due to abnormal adverse wind gradient conditions, so the controller will not issue an ITP clearance if the positive Mach differential is greater than 0.04 Mach. Anyway, the controller can issue the request for an ITP manoeuvre towards the requested flight level or can offer another flight level if the standard longitudinal separation would be met at that flight level. The controller assesses all other aircraft at all intervening flight levels using standard procedure-based separation minima and procedures.

The ITP manoeuvre terminates when the flight crew reports to the controller that the ITP aircraft has reached the Requested flight level. If the ITP aircraft cannot complete the flight level change once the manoeuvre has been initiated, the flight crew has to request immediately a new ATC clearance or, in lieu of this clearance, it has to follow *Special Procedures for In-Flight Contingencies in Oceanic Airspace*. Anyway, the controller has to deny all manoeuvre requests made by the reference aircraft throughout the ITP manoeuvre.

3.2.3 ITP flight level change geometries

The ITP provides a set of six different flight level change geometries, which depend on the relationship between the ITP aircraft and the reference aircraft and on the kind of manoeuvre that the ITP aircraft has requested. The ITP criteria are the same for all six geometries. These geometries are explained below.

1) ***Following Climb*** **:** The ITP aircraft is following two reference aircraft which are at higher Intervening flight level (see Figure 3.10). The

other aircraft at FL370 and FL350 are not specifically part of the ITP manoeuvre: the ATC provides the separation between the ITP aircraft and the other aircraft using the standard procedure.

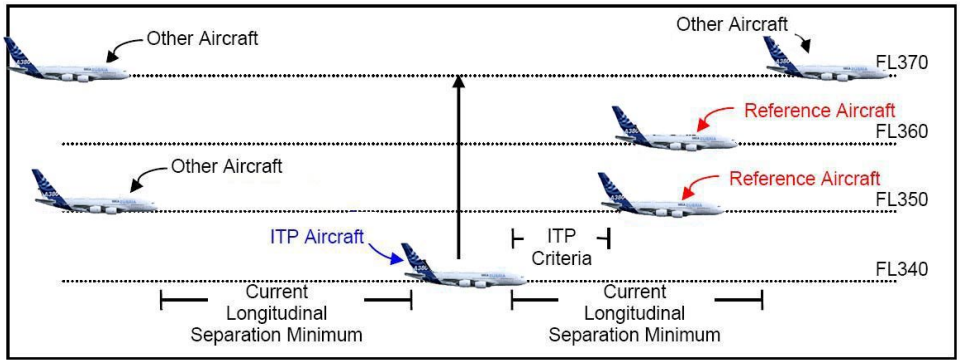


Figure 3.10: ITP following-climb with two reference aircraft

Similar to this Following Climb geometry, the next geometries can also admit two reference aircraft at two different intervening flight levels.

2) ***Following Descent*** **:** The ITP aircraft is following a reference aircraft that is at a lower Intervening flight level (see Figure 3.11).

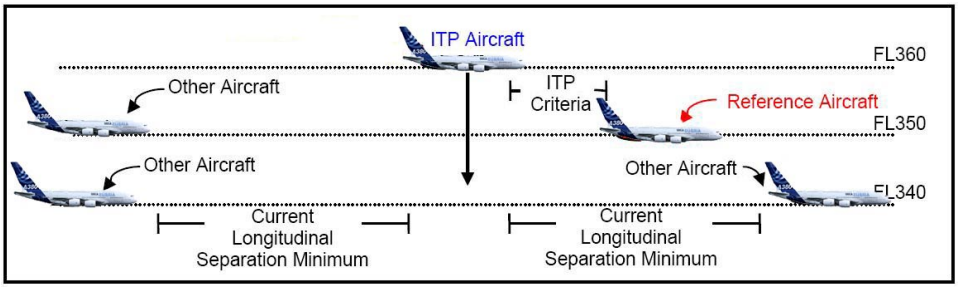


Figure 3.11: ITP following-descent

3) ***Leading Climb*** **:** The ITP aircraft is leading a reference aircraft that is at a higher Intervening flight level (see Figure 3.12).

4) ***Leading Descent*** **:** The ITP aircraft is leading a reference aircraft that is at a lower intervening Flight Level (see Figure 3.13).

5) ***Combined Leading-Following Climb*** **:** The ITP aircraft is leading one reference aircraft and following another reference aircraft. At the

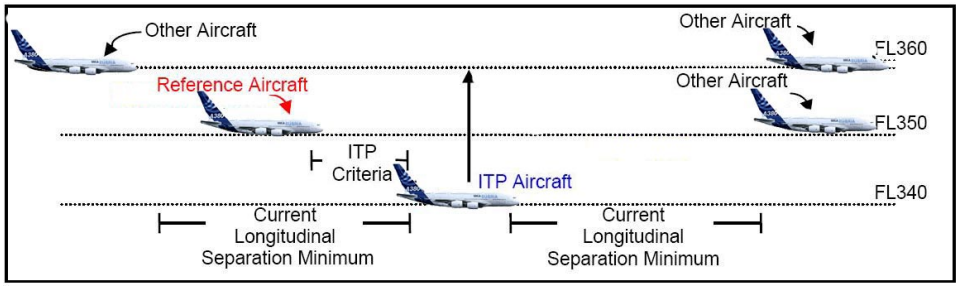


Figure 3.12: ITP leading-climb

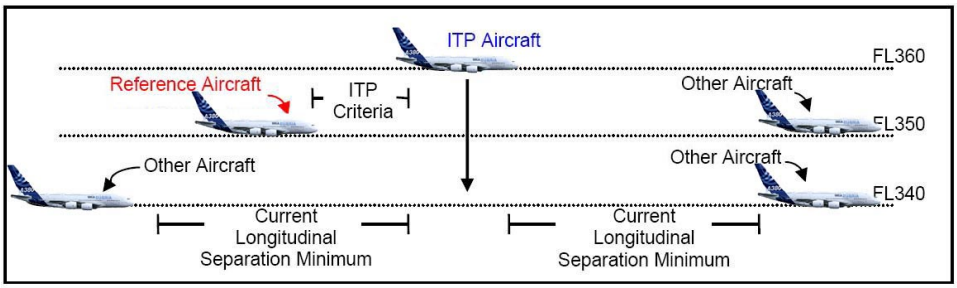


Figure 3.13: ITP leading-descent

same time, both reference aircraft can be at the same higher Intervening flight level or in two different higher intervening flight levels (see Figure 3.14).

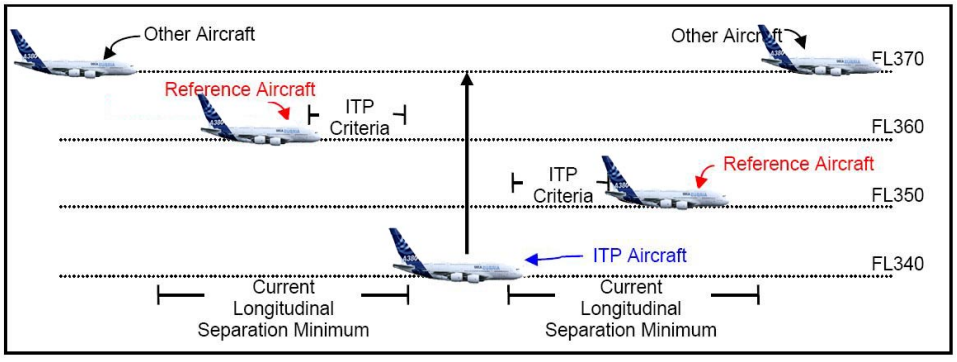


Figure 3.14: ITP combined leading-following climb

6) ***Combined Leading-following Descent*** **:** The ITP aircraft is leading

one reference aircraft and following another reference aircraft. At the same time, both reference aircraft can be at the same lower Intervening flight level or in two different lower intervening flight levels (see Figure 3.15).

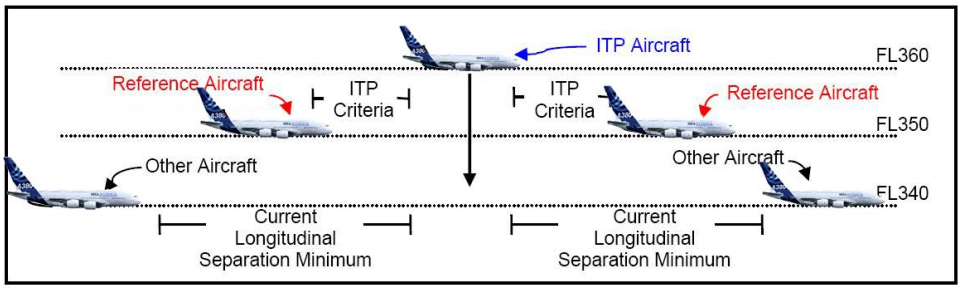


Figure 3.15: ITP combined leading-following descent

3.2.4 ITP Pre-Conditions

Prior to considering an ITP, the flight crew must verify the following *ATSA-ITP Pre-Conditions*:

- The ITP aircraft crew determines if there is a desire to change flight level based on any number of operational factors including fuel burn, wind and turbulence avoidance.

- The aircraft desiring to perform an ITP has approved ITP equipment which provides the flight crew with the ability to determine Flight ID, flight level, same direction status, ITP distance and ground speed differential for Potentially Blocking Aircraft with qualified ADS-B data.

- The air carrier Operation Specifications (OpSpecs), Operational Manual, or other appropriate material, as required by the regulator permit the use of the ITP on the aircraft.

- The flight crew of the ITP aircraft is properly qualified for the ITP.

If these ITP Pre-Conditions are met, the flight crew can request an ITP. The ITP can be divided into four phases:

P_0) ITP initiation phase

P_1) ITP instruction phase

P_2) ITP execution phase

P_3) ITP termination phase

These ITP phases are explained in the following sections.

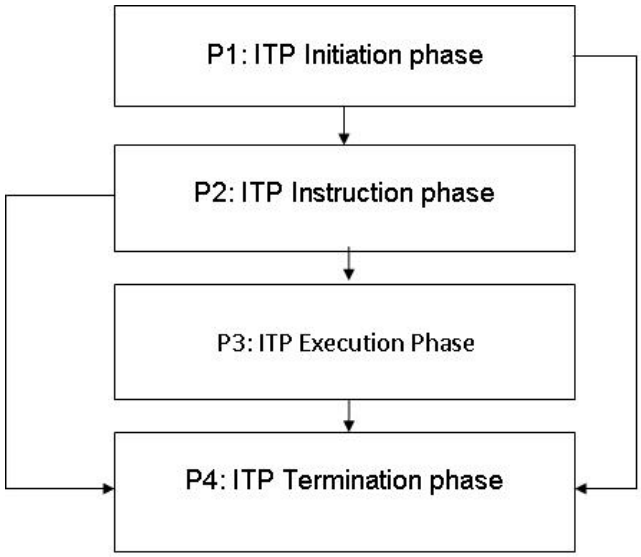


Figure 3.16: ITP phase diagram

3.2.5 ITP initiation

The decision to request an ITP rather than a standard flight level change can be due to different factors, such as crew preference and judgement, company policy, and any other information available to the crew about the flight's progress and proximate traffic situation.

Once he has decided to request an ITP, the flight crew has to follow the steps explained below, in order to formulate and initiate the request to the ATC:

- **Identification of ITP flight levels** → the flight crew identifies the *requested flight level* and identifies the *intervening flight levels* using the ITP equipment.

- **Verification of ITP flight levels** → the flight crew verifies that

1. The ITP aircraft's position data meet the accuracy requirement for ITP.
2. The ITP aircraft can perform a rate climb or a descent of at least 300 fpm at the assigned Mach number to the Request Flight Level.
3. The ITP aircraft is not expected to manoeuvre except for keeping their clearance.

- Identification of reference aircraft → the flight crew verifies that

1. The ITP aircraft is *same-direction* with *Potentially Blocking Aircraft.*
2. Qualified ADS-B Data are available from Potentially Blocking Aircraft.
3. The *ITP speed/distance Criteria* is met with Potentially Blocking Aircraft.

Then, the crew selects as *reference aircraft* up to two Potentially Blocking Aircraft that meet the above criteria.

- ITP Request → If the criteria are met, the ITP aircraft crew makes a request using the *ITP Phraseology*, which provides the controller with the following information:

- The requested ITP flight level change geometry
- ITP distance
- Flight ID of reference aircraft.

3.2.6 ITP Instruction

- Controller ITP clearance issuance → The air traffic controller, on reception of the ITP request, has to :

1. determine if the *standard separation* will be met with all aircraft at the initial flight level, at the requested flight level, and at all the intermediate flight levels. *If so,* a standard flight level change clearance can be issued (i.e. non-ITP clearance is necessary). *If not*:
2. determine if the ITP request message format is correct and that the flight crew has correctly identified the reference aircraft at the intervening flight levels.

3. determine if standard separation will be met with all *other aircraft* (i.e. excepted the Reference Aircraft) at the initial flight level, at requested flight level, and at all the Intermediate Flight Levels.
4. determine that the ITP aircraft is not a reference aircraft in another ITP clearance.
5. determine that the ITP aircraft and the reference aircraft are *Same-Track*.
6. determine that the reference aircraft is non-manoeuvring and not expected to manoeuvre during the ITP. *If not*, the controller will not issue an ITP clearance.
7. determine that the positive mach differential is not greater than 0.04.

The controller can grant the ITP flight level change request, based on the ITP aircraft's request and the determination of the previous seven conditions.

- ITP Crew Performance during the ITP manoeuvre → After the ITP clearance is issued and before initiating the climb or the descent, the flight crew has to determine again that the ITP criteria are still met with respect to the reference aircraft. This re-assessment should not cause an undue delay in the initiation of the ITP manoeuvre. If the ITP criteria are no longer met, the crew refuses the ITP Clearance and remains at the initial flight level.

3.2.7 ITP Execution

- ITP Crew Performance during the ITP manoeuvre → As with a standard climb or descent clearance, the crew has to initiate the ITP without delay after receipt of the clearance.

1. The crew must maintain the original cruise Mach number during the climb or descent.
2. The ITP aircraft must maintain a minimum 300 fpm climb or descent rate, or the minimum rate required by regulation if greater, throughout the ITP manoeuvre.
3. The ITP aircraft crew is not required to monitor the ITP distance to the reference aircraft during the climb or descent.

4. The ITP flight crew reports to the ATC establishment at the new flight level.

- Controller Performance 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 terminated abnormally.

- ITP Termination → There are two possibilities to complete an ITP manoeuvre:

- the ITP flight crew reports establishment at the new flight level (i.e. *successfully completed manoeuvre*), *or*
- the ITP aircraft cannot successfully complete the ITP once the climb or descent has been initiated, because an abnormal terminations occurs (i.e. *abnormal completed manoeuvre*).

3.2.8 ITP Equipage

The ATSA-ITP does not require all aircraft to be able to receive, process, display and broadcast qualified ADS-B data. The procedure requires that the ITP-Aircraft are capable to receive, process and display ADS-B data (i.e the ITP aircraft must be at least ADS-B In) and the reference aircraft are capable of broadcasting qualified ADS-B data (i.e. the reference aircraft must be at least ADS-B Out). Not all aircraft in the ITP environment are expected to be ADS-B equipped. The ITP can readily be used in a mixed-equipage environment.

The flight crew can show the ADS-B data using the CDTI in order to identify all the Potentially Blocking Aircraft and the reference aircraft. In this context, the ITP application can be implemented as part of a more general application that provides other traffic information. The flight crew can use first the more general traffic awareness application, in order to decide between standard and ITP flight level change request. Subsequently, the flight crew can use a specific ITP application, in order to evaluate and make an ITP request.

The ATC can use the standard procedures and the available standard traffic information in order to grant or deny an ITP request.

3.3 Example Scenarios

The following examples provide interesting cases studies, that show the main characteristic and behavior of the ATSA-ITP. It is assumed that the ITP aircraft can perform an ITP, i.e. the flight crew, the ITP equipment and the aircraft meet the ITP requirements. It is also assumed that the ITP aircraft's flight crew has decided to request an ITP flight level change.

3.3.1 Following Climb Request with ATC approval

In this scenario, we consider two aircraft, where the ITP aircraft is identified by ID-Flights XY76 while the other aircraft by AB371. The considered airspace is included between FL330 and FL350.

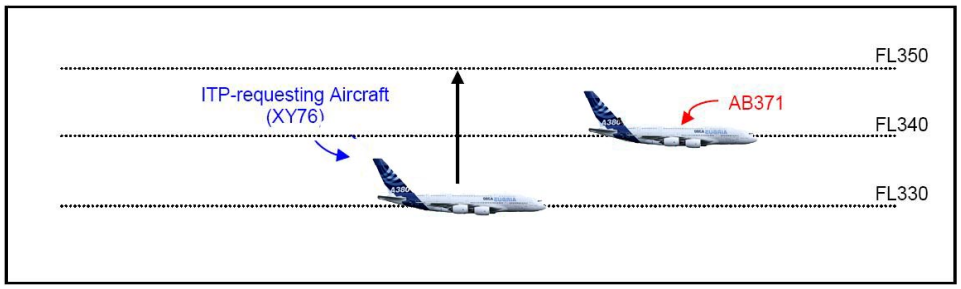


Figure 3.17: A following climb scenario

The flight crew of XY76 has the intent to climb from FL330 to FL350. This decision is taken just using the standard on board data. The flight crew also determines that the aircraft can perform a climb of at least 300 fpm at the assigned Mach number.

Using the ITP equipment, the ITP flight crew identifies aircraft that are between FL330 and FL350, that are within a 45 degree relative ground track to their own ground track (i.e. all the aircraft that are on the same common published route of the ITP aircraft). In the case illustrated in Figure 3.17, the flight crew identifies aircraft AB371, and determines that it is providing *Qualified ADS-B Data* (i.e. ADS-B data that meet the accuracy and integrity required for the ITP).

Using the ITP equipment, the flight crew also determines that the ITP distance is 19 NM (i.e. XY76 is 19 NM behind AB371), and the ground speed differential is 7 kts (i.e. the XY76 is closing to AB371 at 7 kts).

The flight crew determines that these values meet the ITP speed/distance criteria, which request that the ITP distance is not less than 15 NM and a positive ground speed differential less than 20 kts.

The flight crew can request an ITP climb using the standard phraseology:

"Gander, XY76, request I-T-P climb to flight level three five zero following AB731 at one niner miles"

Using standard procedures, ATC determines if the standard separation can be met for all aircraft at FL350 and at all flight levels between FL330 and FL350, in order to grant a standard flight level change clearance instead of an ITP clearance. However, in this scenario, the distance between the two aircraft is less than the standard separation, thus the controller evaluates the possibility of an ITP manoeuvre (i.e. a standard flight level change is not possible).

Using standard procedures, ATC determines if standard separation with XY76 will be met at the requested flight level FL350 and at all flight levels between FL330 and FL350 for all other aircraft (i.e. all aircraft except ITP aircraft and reference aircraft). In this scenario, standard separation does exist with all other aircraft.

ATC also determines if AB371 has previous clearance to change speed or change flight level, if it is close to a point at which a significant change of track will occur, or if it is expected to manoeuvre. If so, the ATC refuses the ITP request.

Using standard flight information, the controller establishes that the speed of AB371 is Mach 0.79 and the speed of XY76 is Mach 0.81. The controller determines that there is a positive mach differential of 0.02 (because the ITP aircraft is following the reference aircraft that has a higher Mach) and thus determines that this positive mach differential is less than the ITP maximum value of 0.04 Mach.

Since the separation criteria are met with all other aircraft and AB371 is maintaining spacing, flight level and track, ATC issues the ITP flight level change clearance:

"XY76, Gander, I-T-P climb and maintain flight level three five zero following AB371, report level flight level three five zero"

After the clearance has been received, the flight crew determines that AB371 is still within a 45 degree relative ground track and is providing Qualified ADS-B data. They also determine that they are 17 NM behind

AB371 and are closing on AB371 at 7 kts, and determines that these values still meet the ITP distance speed criteria.

Since the ITP criteria are still met, the ITP flight crew initiates the flight level change to FL350. Once reached FL350, the flight crew reports establishment at this flight level, using the standard phraseology:

"Gander, XY76, Level at flight level three five zero"

3.3.2 Combined Leading-Following Descent Request with ATC approval

Using standard on board data, the flight crew of the XY76 determines that they wish to descend from FL370 to a requested flight level of 330. The flight crew determines that a descent of a least 300 fpm at the assigned Mach number is possible. Using their ITP equipment, the ITP flight crew of XY76 identifies aircraft that are on the same common published route, i.e. the aircraft AB372 at FL360, and the aircraft RFG54 at FL340. Using their equipment, the flight crew determines that AB372 and RFG54 are providing Qualified ADS-B Data.

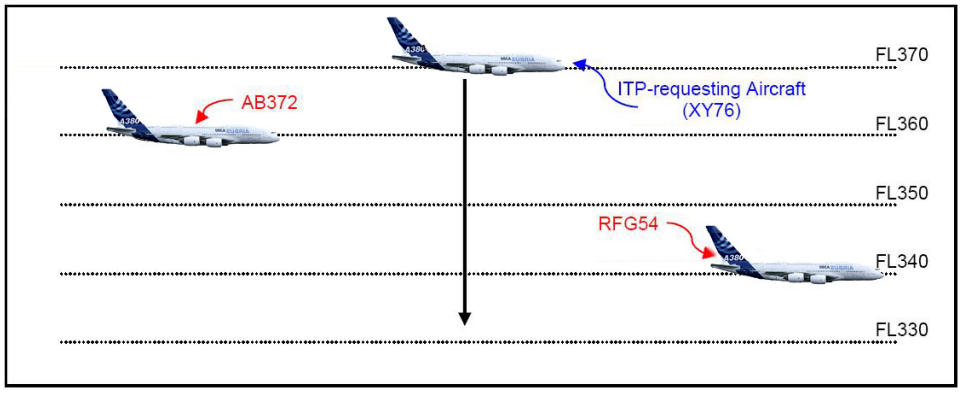


Figure 3.18: A combined leading-following descent scenario

The flight crew determines that they are 29 NM ahead of AB372 (ITP distance) with a closure rate on AB372 of 27 kts (positive ground speed differential). The flight crew also determines that they are 33 NM behind RFG54 and are not coming near to RFG54 (i.e. no positive ground speed differential). Thus, the flight crew determines that these values meet the ITP speed/distance criteria for both aircraft. The flight crew requests an ITP Descent:

"Gander, XY76, request I-T-P descent to flight level three three zero leading AB372 at two niner miles following RFG54 at three miles"

Using standard procedures, ATC determines whether standard separation can be met for all aircraft at FL330 and at all flight levels between FL330 and FL370. If so, a standard flight level change clearance can be granted instead of an ITP clearance. However, in this scenario the distances between the ITP aircraft XY76 and the aircraft AB372 and RFG54 are less than standard longitudinal separation so the controller evaluates the ITP request.

Using standard procedure, ATC determines if the standard separation with XY76 will be met at the requested flight level and at all flight levels between FL330 and FL370 for all aircraft except AB372 and RFG54. In this scenario, standard separation does exist with all other aircraft.

ATC also determines that AB372 or RFG54 have been approved to change speed or change flight level, or if they are about to reach a point in which a significant change of track will occur. If so, the ATC refuses the ITP request.

Using standard flight information, the controller notes that the speed of AB372 is Mach 0.83 and the speed of XY76 is Mach 0.81, then a positive mach differential of 0.02 Mach exists because the ITP aircraft is leading AB372 which has a lower Mach, and is not greater than 0.04 Mach. The controller also notes that the speed of RFG54 is Mach 0.83 and the speed of XY76 is Mach 0.81; then a positive mach differential does not exist because the ITP aircraft is following RFG54 which has a greater Mach, and is not greater than 0.04 Mach.

Since the separation criteria are met with all other aircraft and both AB372 and RFG54 are maintaining speed, flight level and track, ATC issues the ITP flight level change clearance:

"XY76, Gander, I-T-P descent and maintain flight level three three zero leading AB372 following RFG54, report level flight level three three zero"

After receiving the clearance, the flight crew determines that AB372 and RFG54 are still within a 45 degree relative ground track and are still providing Qualified ADS-B Data. They also determine that they are 27 NM ahead of AB372 and are closing on AB372 at 17 kts. They also determine that they are 35 NM behind of RFG54 and are not closing on RFG54. Then, the flight crew determines that these values still meet the ITP speed/distance criteria with the reference aircraft AB372 and RFG54.

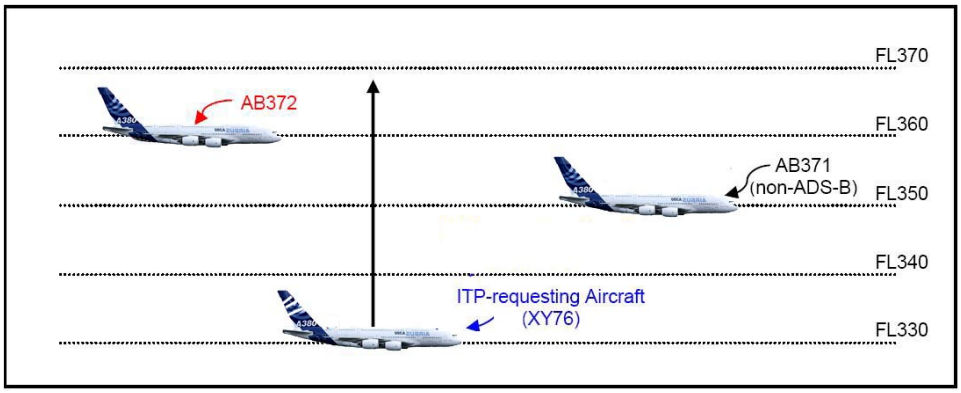


Figure 3.19: A leading climb scenario with ATC disapproval

Since the ITP criteria are still met, the flight crew initiates the flight level change to FL330. Once FL330 is reached, the flight crew reports establishment at this flight level:

"Gander, XY76, Level at flight level three three zero"

3.3.3 Leading Climb Request using CPDLC with ATC Disapproval

In this scenario, the communication between controller and pilot are supposed to be made by using the *Controller Pilot Datalink Communication (CPDLC)* instead of the *High Frequency radio*. CPDLC is a data link application that allows direct exchange of text-based messages between a controller and a pilot. This hypothesis does not influence the execution of an ITP manoeuvre. The scope of this scenario is to emphasize the role of the ATC, when there is any aircraft that is not equipped with ADS-B instrumentation (i.e. aircraft that are not ADS-B out) in the proximity of the ITP aircraft.

By using standard on board data, the flight crew of XY76 determines that they wish to climb from FL330 to a requested flight level FL370. The flight crew determines that a climb of at least 300 fpm at the assigned Mach number is possible.

Using their ITP equipment, the ITP flight crew of XY76 identifies aircraft that are between FL330 and FL370, that are also within a 45 degree

relative ground track to their own ground track (i.e. all aircraft that are on the same common published route of the ITP aircraft). In the case illustrated in Figure 3.19, the flight crew identifies the aircraft AB372 at FL360, and then determines that it is providing Qualified ADS-B Data. Aircraft AB371 is not visible to the flight crew since it is not transmitting ADS-B Data.

Using their ITP equipment, the flight crew also determines that they are 29 NM ahead of AB372 (ITP distance) with a closure rate on AB372 of 27 kts (positive ground speed differential). Then, the flight crew determines that these values meet the ITP speed/Diastance criteria. The flight crew can request an ITP climb. The CPDLC free text used would be "ITP L/AB372/29", which indicates an ITP request leading AB372 at 29 miles. For instance, a combined leading-following climb would be "ITP F/RFG54/61.L/AB372/29".

Using standard procedures, ATC determines whether standard separation can be met for All Aircraft at FL370 and at all Flight Levels between FL330 and FL370. If so, a standard flight level change clearance can be granted. In this scenario, standard separation would not exist between the ITP aircraft and either AB371 or AB372 during climb. Since AB371 is not in the ITP request, the controller denies this request, unable due to traffic.

3.3.4 Abnormal Modes

We do not formalize all possible abnormal scenarios, because of the high number of variables that affect the manoeuvre (e.g. various human errors). Assuming that all failures occur while the aircraft is executing the ITP manoeuvre, the high-level failure scenarios and responses can be summarized as follows:

1. **Failure of ITP equipment during the ITP manoeuvre:** the flight crew will continue to perform the ITP maneuver as instructed; reference to the ITP equipment during the manoeuvre is not required.

2. **ITP aircraft unable to continue climb/descent at the required performance criteria:** flight crew informs ATC. If possible, obtain alternative clearance. Otherwise regional contingency procedures apply.

3. **ITP aircraft unable to continue a climb/descent:** flight crew informs ATC. If possible, obtain alternative clearance. Otherwise regional contingency procedures apply.

4. **ITP aircraft needs to make an emergency descent:** flight crew informs ATC. If possible, obtain alternative clearance. Otherwise regional contingency procedures apply.

5. **ITP aircraft needs to change course or divert from the track:** flight crew informs ATC. If possible, obtain alternative clearance. Otherwise regional contingency procedures apply.

6. **ITP aircraft experiences a radio communication failure:** standard procedures for communication loss apply.

7. **ITP aircraft experiences TCAS RA during ITP manoeuvre:** standard procedures apply. The flight crew responds to the RA and resumes the clearance when the TCAS situation is solved.

8. **Reference aircraft needs to make an emergency descent:** if observed before the ITP manoeuvre, inform ATC and reject any ITP clearance. Although the flight crew is not required to monitor the ITP equipment during the ITP manoeuvre, if observed during the ITP manoeuvre, the flight crew will continue to perform the maneuver as instructed.

9. **Reference aircraft needs to change course or divert from the track:** if observed before the ITP maneuver, inform ATC and reject any ITP clearance. Although the flight crew is not required to monitor the ITP equipment during the ITP manoeuvre, if observed during the ITP manoeuvre, the flight crew will continue to perform the manoeuvre as instructed.

10. **Leading reference aircraft reduces speed or trailing reference aircraft increases speed:** If observed before the ITP manoeuvre, inform ATC and reject any ITP clearance. Although the flight crew is not required to monitor the ITP equipment during the ITP manoeuvre, if observed during the manoeuvre, the flight crew will continue to perform the ITP manoeuvre as instructed.

3.3.5 Different ITP applications

The ATSA-ITP application described in this chapter is currently being standardized by the Requirements Focus Group as part of *Airborne Separation Assistance System (ASAS)* Package 1 applications. Beginning from spring 2008, it will be tested in the North Atlantic Airspace above Iceland

(where radar coverage is available) with a small set of aircraft equipped with special ADS-B devices. Then ATSA-ITP represents the near-future of ITP oceanic airspace applications.

In this context, the next-future is represented by the *Airborne Separation - In Trail Procedure (ASEP-ITP)* studied inside the *Advanced Safe Separation Technologies and Algorithms (ASSTAR)* project, which can be considered as the next-step of the ATSA-ITP. This new application introduces an innovative transfer of separation management responsibilities from ATC to the flight crew throughout the ITP manoeuvre. The rationale behind this is that the flight crew, in contrast to ATC, disposes of the appropriate surveillance equipment (i.e. ADS-B and ASAS Equipment), and is therefore instantly able to monitor separation and act if necessary.

Chapter 4

ATSA-ITP hybrid model and observability analysis

In this chapter, a hybrid model of the ATSA-ITP is proposed. The ATSA-ITP application described in the previous chapter involves three agents: the *ITP aircraft*, the *Controller*, and the *reference aircraft*. The reference aircraft does not actively interfere in the procedure, because it does not have the situational awareness that it is part of an ITP manoeuvre. When an ITP manoeuvre is performing, the reference aircraft can request a new clearance to the ATC, but the ATC must deny it. On the other hand, the clearance can be granted due to an ATC wrong situational awareness. All failures due to the technical instruments can be embedded in hybrid models of the agents. A malicious failure is defined as a failure that generates erroneous information, but it is not evidently revealed by an accuracy uncertainty parameter or other mechanism. A failure that manifests itself as the absence of data is not a malicious failure, because the absence of data is a mechanism for detection. For these reasons, the hybrid model proposed here provides only two hybrid agents, the *ITP aircraft flying* and the *Controller*.

Before describing the hybrid models of the agents in Sections 4.2 and 4.3, we present in Section 4.1 a hazard analysis based on [23]. In Sections 4.4 and 4.5 we perform observability analysis on the hybrid models of the agents.

4.1 Operational hazards and main assumptions

The complexity of the safety analysis of an airborne application derives from the specific structure of the environment. In an airborne application

the operations are the result of interactions between different human agents. For this reason, it is not possible at the same time to consider all the abnormal events that might happen. Our modeling approach considers only those hazards that might be encountered during ATSA-ITP procedures. A detailed description of these operational hazards is proposed in [23]. Other hazards associated with normal flight are not considered.

The following list introduces the main *operational hazards (OH)* whose effects are considered inside the hybrid model.

OH1: Interruption of an ITP manoeuvre that prevents successful completion of ITP. Aircraft experiences a system failure, or an adverse performance/ environmental condition exists during an ITP manoeuvre, which requires the flight crew to abandon the manoeuvre and follow regional contingency procedures (i.e. A detailed description of NAT contingency procedures is available in [14] , [3]).

OH2: Execution of an ITP clearance not compliant with ITP criteria. This operational hazard is divided into 7 cases depending on which ITP criterion is not met, and whether the sub-hazard is detected or undetected. It is assumed that the initiation of an ITP manoeuvre with 2 or more incompliant criteria is extremely unlikely, and thus this case is not considered. The sub-hazards for **OH2** are the followings:

- ◇ **OH2D: Detected non-compliance with climb/descent rate (i.e. rate less than 300 ft/minute).** It is assumed that, at any given time during the manoeuvre, the flight crew detects the failure to maintain climb/descent rate. Once the flight crew detects the non-compliance condition, it is also assumed that a 300 feet/minute rate is established or that the flight crew follows regional contingency procedures ([14] , [3]).
- ◇ **OH2U-1:** Undetected non-compliance with climb/descent rate (i.e. rate less than 300 ft/minute). It is assumed that the flight crew does not detect this failure for the entire climb/descent manoeuvre.
- ◇ **OH2U-2: Undetected non-compliance with the initiation distance criterion (i.e. distance from 0 to 15 NM).** It can happen if there is an error in determining what the distance initiation criteria is, or if the ITP flight crew incorrectly calculates the distance, or if there is a malicious failure in the ITP or ADS-B equipment leading to erroneous distance information. It

is assumed that if the flight crew detects a reduction in safety margins during the manoeuvre, then the flight crew acts in order to avoid a potential near mid-air collision.

- ◇ **OH2U-3: Undetected non-compliance with the ground speed difference values (i.e difference more than 30 knots).** It can be due to a decrease of the reference aircraft speed when the reference aircraft is the lead one, or due to an increase of its speed when it is the following aircraft. An aircraft can in fact decrease its speed during cruise to reduce the effect of turbulence.
- ◇ **OH2U-4: Undetected non-compliance with the Mach difference (i.e difference greater that 0.04 Mach).**
- ◇ **OH2U-5: Undetected non-compliance with the reference aircraft not manoeuvring.** It can be due to a wrong situational awareness of the ATC who grants a flight plan change for a reference aircraft.
- ◇ **OH2U-6: Undetected non-compliance with the maximum flight level change of 4000 feet.** It can be due to a wrong situational awareness of the ATC who does not detect a wrong flight level requested by the flight crew, or it can be due to a leveling off at a wrong flight level by the flight crew.

OH3: ITP request not accepted by ATC. Flight crew requests an ITP but the request is denied by ATC. In fact, the ATC can detect that:

- An unauthorized aircraft has requested an ITP, *or*
- ITP flight crew has not identified a potentially blocking aircraft, *or*
- The blocking aircraft information are erroneous or inappropriate, *or*
- ITP request is corrupted.

OH4: Rejection by the flight crew of an ITP clearance not compliant with the ITP criteria. In fact, the flight crew can detect that:

- The ATC clearance has been misdirected, *or*
- The ATC instructs a non requested ITP manoeuvre, *or*
- One of the ITP criteria is not compliant.

OH5: Rejection by the flight crew of an ITP clearance compliant with the ITP criteria. The ITP flight crew is not able to confirm positively the ATC clearance during the reassessment.

OH6: Incorrect execution of an ITP manoeuvre. The flight crew levels off at the wrong flight level or delaying the initiation of the ITP climb/descent.

These operational hazards have been identified based on the application modeling, which describes the application at the phase, sequence and action level. Hazards are identified at the boundary of the application under assessment and they are normally distinguished in "detectable" and "undetectable". A list of abnormal events can be obtained considering three failure modes to each of the identified actions expressed in the modeling:

- *Loss:* action not available or not executed.
- *Incorrect:* action is performed incorrectly or is performed using incorrect information.
- *Others:* actions executed in non-suitable conditions or executed out of sequence.

From these abnormal events, a list of operational hazards can be determined by grouping the abnormal events leading to a same hazard. From an operational point of view, only a subset of these operational hazards affects the application. To each operational hazard of this subset can be associated a rating from 1 to 5, which represents severity class. The severity class 1 is the most severe and it includes all the hazards which cause a total loss of flight control or a total loss of separation, and thus a possible mid-air collision. The least severe class 5 includes all the hazards whose effects do not influence safety or operational capabilities. According to [23], the severity of the ATSA-ITP operational hazards OH1, OH2 and OH6 have been rated level 3 (i.e. significant reduction in safety margins or aircraft functional capabilities and significant reduction in air traffic control capability), while the remaining operational hazards have been rated level 4.

Before defining the hybrid models of the ATSA-ITP agents, we state the following assumptions, which simplify the mathematical model w.l.o.g.:

AS.1: When the ATC is waiting for the ITP starting confirmation by the flight crew, a request for a clearance from a reference aircraft cannot occur. The reference aircraft can request a new clearance only when the ITP aircraft is performing the manoeuvre.

AS.2: When the ATC receives an emergency communication by the flight crew, the ATC does not change his activity and does not have enough

time to issue a new clearance. Thus the flight crew immediately starts the regional contingency procedures ([3, 23]). The ATC will evaluate for possible unsafe situations as soon as he receives the communication of the achievement of a new flight level by flight crew.

AS.3: If a technical failure occurs during assessment, it will continue during the reassessment.

AS.4: If the flight crew makes an error during assessment, the same error will not be detected during the reassessment task.

These assumptions complete the ones presented during the operational hazards analysis.

4.2 ITP Aircraft Flying Agent

In this section, the hybrid model of the behavior of the ITP flight crew performing the ITP manoeuvre is described. The mathematical framework and notations are based on the definitions given in Chapter 2, and also embeds a set Σ of discrete input signals. Each edge $e = (q_s, \sigma, q_t) \in E \subseteq Q \times \Sigma \times Q$ is associated to a symbol $\sigma \in \Sigma$, that triggers the discrete transition between the states linked by the edge. These inputs can be considered as discrete disturbance or control inputs which model communication among the agents. When the discrete input and the guard transition simultaneously occur, then one of the two transitions in non-deterministically triggered. Before proposing the model, we introduce the following notations and variables:

- z_i the initial flight level of the ITP aircraft.
- z_r the requested flight level.
- z_f the final flight level reached after the manoeuvre (i.e. z_f can be different from z_r).
- $\dot{x}$ the ground speed of the aircraft.
- $\dot{z}$ the rate of climb/descent.
- $v_t = \sqrt{\dot{x}^2 + \dot{z}^2}$ the airspeed.
- M mach number assigned to the ITP aircraft.

- $V_i = [v_{i,min}, v_{i,max}]$ for $i \in \{t, x, z\}$, the sets of admissible speeds, respectively for airspeed, ground speed and rate of climb/descent.

- $A_i = [a_{i,min}, v_{a,max}]$ for $i \in \{x, z\}$, the sets of admissible accelerations, respectively for longitudinal acceleration and acceleration of climb/descent.

Using the International Standard Atmosphere, all the flight levels can be calculated from the altitude expressed in feet divided for hundred.

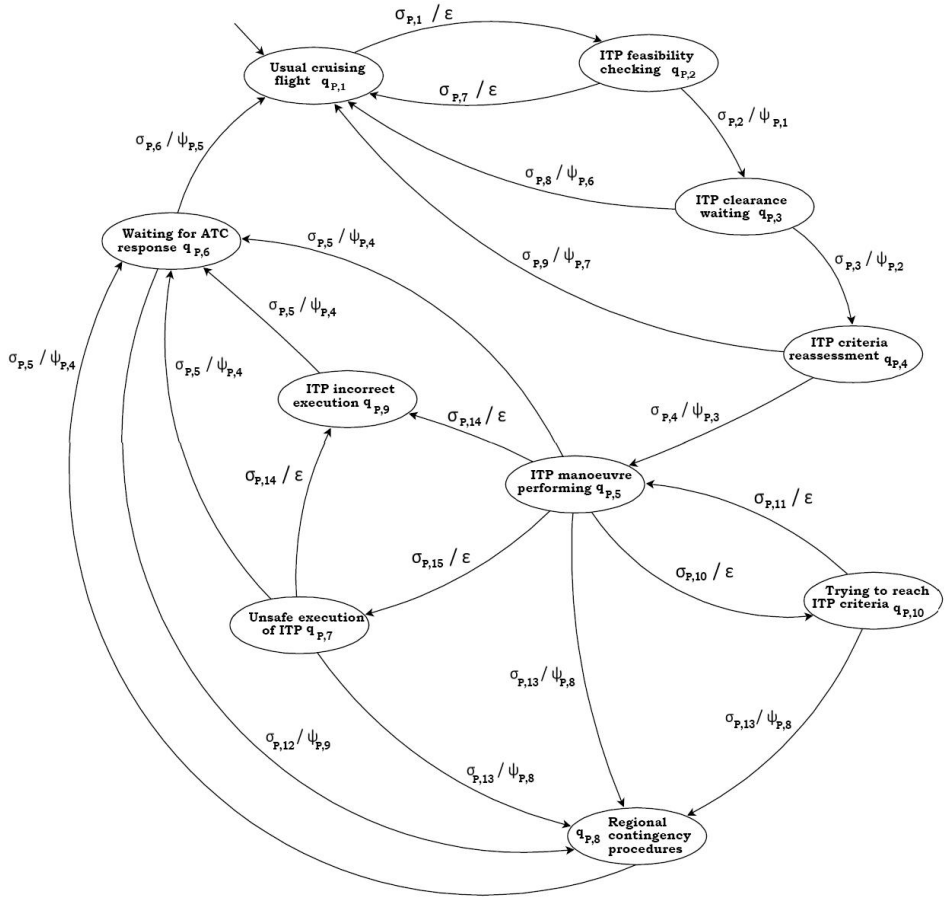


Figure 4.1: ITP Aircraft Discrete Layer

The non-deterministic hybrid system $\mathcal{H}_p$ that describes the ITP flying aircraft agent is composed by:

◇ **The discrete states set** $Q_p = \{q_{p,1}, q_{p,2}, \cdots, q_{p,10}\}$, where:

$q_{p,1}$ **:** *Usual cruising flight*, the aircraft is cruising at the assigned flight level and follows the ATC clearance (i.e. Mach constant and flight level assigned).

$q_{p,2}$ **:** *ITP feasibility checking*, the flight crew performs the ITP Precondition checks and the ITP initiation checks in order to evaluate if an ITP manoeuvre can be requested.

$q_{p,3}$ **:** *ITP clearance waiting*, the flight crew waits that the ATC grants or denies the ITP request.

$q_{p,4}$ **:** *ITP criteria reassessment*, once received the ATC granted communication, the flight crew checks if the ITP criteria are still satisfied before starting the manoeuvre.

$q_{p,5}$ **:** *ITP manoeuvre performing*, the flight crew has accepted the ATC grant and is performing the ITP climb/descent respecting the Performance Criteria.

$q_{p,6}$ **:** *Waiting for ATC response*, the flight crew has leveled off at new flight level and it has communicated this to the ATC. The flight crew is waiting for the flight level confirmation by ATC.

$q_{p,7}$ **:** *Unsafe execution of ITP manoeuvre*, the flight crew is performing the manoeuvre but an error has been made during the ITP feasibility checking and/or during the ITP reassessment. This error is due to a wrong situational awareness.

$q_{p,8}$ **:** *Regional contingency procedures performing*, the flight crew has identified un unsafe situation and is following the regional contingency procedures in order to avoid possible mid-air collisions.

$q_{p,9}$ **:** *ITP incorrect execution*, the flight crew has performed the ITP manoeuvre leveling off at the reference aircraft level (i.e. wrong flight level reached) or the ITP manoeuvre is started with a notable delay.

$q_{p,10}$ **:** *Trying to reach again the performance criteria*, the flight crew was performing the ITP manoeuvre when it has detected that the performance criteria was not satisfied. In this situation the flight crew can try to achieve again the performance criteria.

- ◇ **The continuous states set is** $X_p = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+, z \in \mathbb{R}^+, \dot{x} \in \mathbb{R}^+, \dot{z} \in \mathbb{R}\}$. The variable x represents the longitudinal position of the ITP aircraft expressed in nautical miles; z represents the altitude of the ITP aircraft expressed in hundred of feet (i.e. flight level inside the International Standard Atmosphere ISA); $\dot{x}$ is the ground speed of

the aircraft measured in knots; finally $\dot{z}$ is the rate of climb expressed in feet per minute.

- ◇ **The initial discrete states set** $Q_{p0} = \{q_{p,1}\}$.
- ◇ **The discrete inputs set** $\Sigma_p = \{\sigma_{p,1}, \sigma_{p,2}, \sigma_{p,3}, \sigma_{p,4}, \cdots, \sigma_{p,15}\}$, that essentially models decisions of the agent (internal events) or communication among the agents involved in the ITP procedure (external events):

  $\sigma_{p,1}$ **:** Wish to perform an ITP manoeuvre (internal event).

  $\sigma_{p,2}$ **:** Positive response of feasibility checking (internal event).

  $\sigma_{p,3}$ **:** ITP granted communication by ATC (external event).

  $\sigma_{p,4}$ **:** Positive response of reassessment (internal event).

  $\sigma_{p,5}$ **:** Manoeuvre completed (internal event).

  $\sigma_{p,6}$ **:** Flight level confirmation by ATC (external event).

  $\sigma_{p,7}$ **:** Negative response of feasibility checking (internal event).

  $\sigma_{p,8}$ **:** ITP communication denied by ATC (external event).

  $\sigma_{p,9}$ **:** Negative response of reassessment OR decision to refuse by flight crew (internal event).

  $\sigma_{p,10}$ **:** Performance criteria not compliant (internal event).

  $\sigma_{p,11}$ **:** Positive response of restoring performance criteria (internal event).

  $\sigma_{p,12}$ **:** Command to start regional contingencies procedures by ATC (external event).

  $\sigma_{p,13}$ **:** ITP manoeuvre interrupted by flight crew (internal event).

  $\sigma_{p,14}$ **:** Manoeuvring towards a wrong flight level (internal event).

  $\sigma_{p,15}$ **:** Wrong situational awareness OR Undetect incompliant performance criteria (internal event).

- ◇ **The set of transitions** $E_p \subseteq Q_p \times \Sigma_p \times Q_p$ given by the graph in Figure 4.1 where each edge $e = (q_s, \sigma, q_t) \in E_p$ is associated to a symbol $\sigma \in \Sigma$ that triggers the discrete transition.
- ◇ **Discrete outputs set** $\Psi_p = \{\psi_{p,1}, \psi_{p,2}, \psi_{p,3}, \psi_{p,4} \cdots, \psi_{p,9}\} \cup \{\epsilon\}$

  $\psi_{p,1}$ **:** ITP request communication to ATC.

$\psi_{p,2}$ **:** Starting of the reassessment.

$\psi_{p,3}$ **:** Starting ITP confirmation to ATC.

$\psi_{p,4}$ **:** Achievement of new flight level communicated to ATC.

$\psi_{p,5}$ **:** ITP conclusion confirmation to ATC.

$\psi_{p,6}$ **:** ITP denied confirmation by flight crew.

$\psi_{p,7}$ **:** ITP clearance refused communication to ATC.

$\psi_{p,8}$ **:** Emergency communication to ATC.

$\psi_{p,9}$ **:** Starting regional contingency procedures confirmation to ATC.

◇ **The discrete output function** $\eta_p : E_p \to \Psi_p$, defined by the graph in Figure 4.1. The outputs corresponding to transitions $\{(q_{p,1}, q_{p,2}),$ $(q_{p,2}, q_{p,1}),$ $(q_{p,5}, q_{p,9}),$ $(q_{p,5}, q_{p,7}),$ $(q_{p,7}, q_{p,9}),$ $(q_{p,5}, q_{p,10}),$ $(q_{p,10}, q_{p,5})\}$ are unobservable (i.e. empty string ε as output).

◇ **The invariant conditions** are defined as follows:

- $Inv_{qi} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+ : x \geq x_i, z \in \mathbb{R}^+ : z = z_i, \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : \dot{z} = 0\}$ for $i = 1, 2, 3, 4$
- $Inv_{qi} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+ : x \geq x_i, z \in \mathbb{R}^+ : z \in (z_i, z_r), \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : |\dot{z}| \in [300, v_{z,max}]\}$ for $i = 5, 7$
- $Inv_{q_{10}} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+ : x \geq x_i, z \in \mathbb{R}^+ : z \in (z_i, z_r), \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : \dot{z} \in [v_{z,min}, v_{z,max}]\}$
- $Inv_{q6} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+ : x > x_i, z \in \mathbb{R}^+ : z \in \{z_r, z_f\}, \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : \dot{z} = 0\}$
- $Inv_{q8} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+, z \in \mathbb{R}^+, \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : \dot{z} \in [0, v_{z,max}]\}$
- $Inv_{q9} = \{(x, z, \dot{x}, \dot{z}) : x \in \mathbb{R}^+ : x > x_i, z \in \mathbb{R}^+ : z \in (z_i, z_f), z_f \neq z_r, \dot{x} \in \mathbb{R}^+ : \dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in \mathbb{R} : \dot{z} \in [v_{z,min}, v_{z,max}]\}$

◇ **The continuous dynamics** F_{p,q_i} **for** $i = 1, 2, \cdots, 10$ are defined as follows:

- $F_{p,q_1} = \{v_T = \sqrt{\dot{x}^2 + \dot{z}^2} = (100z)M, \ddot{x} \in [a_{x,min}, a_{x,max}], \ddot{z} = 0\}$
- $F_{p,q_j} = F_{p,q_1}$ for $j = 2, 3, 4, 6$
- $F_{p,q_5} = \{v_T = \sqrt{\dot{x}^2 + \dot{z}^2} = (100z)M, \ddot{x} \in [a_{x,min}, a_{x,max}], |\ddot{z}| \in [a_{z,min}, a_{z,max}]\}$
- $F_{p,q_j} = F_{p,q_5}$ for $j = 7, 9$

- $F_{p,q_8} = \{v_T = \sqrt{\dot{x}^2 + \dot{z}^2} \in [v_{T,min}, v_{T,max}], \ddot{x} \in [a_{x,min}, a_{x,max}], |\ddot{z}| \in [a_{z,min}, a_{z,max}]\}$
- $F_{p,q_10} = F_{p,q_8}$

◇ **The guard conditions** $G_p(e)$ are defined as follows:

- $G(q_4, q_5) = \{(x, z, \dot{x}, \dot{z}) : z = z_i, \dot{z} \neq 0\}$
- $G(q_5, q_{10}) = \{(x, z, \dot{x}, \dot{z}) : \sqrt{\dot{x}^2 + \dot{z}^2} \neq (100z)M\}$
- $G(q_{10}, q_5) = \{(x, z, \dot{x}, \dot{z}) : \sqrt{\dot{x}^2 + \dot{z}^2} = (100z)M\}$
- $G(q_5, q_6) = \{(x, z, \dot{x}, \dot{z}) : z = z_r, \dot{z} = 0\}$
- $G(q_7, q_6) = G(q_5, q_6)$
- $G(q_9, q_6) = \{(x, z, \dot{x}, \dot{z}) : z = z_f, \dot{z} = 0\}$
- $G(q_8, q_6) = G(q_9, q_6)$
- $G(e) = \emptyset$ for the remaining $e \in E_p$ which are never enabled by a guard and can only occur if triggered by a discrete input $\sigma \in \Sigma$.

◇ **The reset map** $R_p(e)$ is the identity for all $e \in E_p$.

The followings subsections explain how the hybrid proposed model describes the behavior of the ITP aircraft and how the operational hazards presented in Section 4.1 have been modelled.

4.2.1 Correct execution without rejections and errors

The most simple scenario for the ITP aircraft agent considers a correct execution of the ITP manoeuvre without errors or wrong situational awareness of the agents. This scenario is represented using the paths of discrete transitions highlighted in Figure 4.2.

Starting from the location *Usual cruising flight (i.e. discrete state $q_{p,1}$)* in which the aircraft is cruising at the assigned flight level, the flight crew can wish to perform an ITP manoeuvre (i.e. discrete input $\sigma_{p,1}$). Once decided to evaluate an ITP request, the flight crew has to check the initiation criteria. In this phase there is no communication between the flight crew and the controller. Thus the transition from *Usual cruising flight ($q_{p,1}$)* to *ITP feasibility checking ($q_{p,2}$)* may be considered unobservable. Only if the initiation criteria are met ($\sigma_{p,2}$) the flight crew requests an ITP manoeuvre to the ATC (i.e. discrete output $\psi_{p,1}$) and a transition to *ITP clearance waiting ($q_{p,3}$)* occurs. In this phase the flight crew has to wait for the ATC response. As soon as the ATC grants the ITP request ($\sigma_{p,3}$) the flight crew can start the

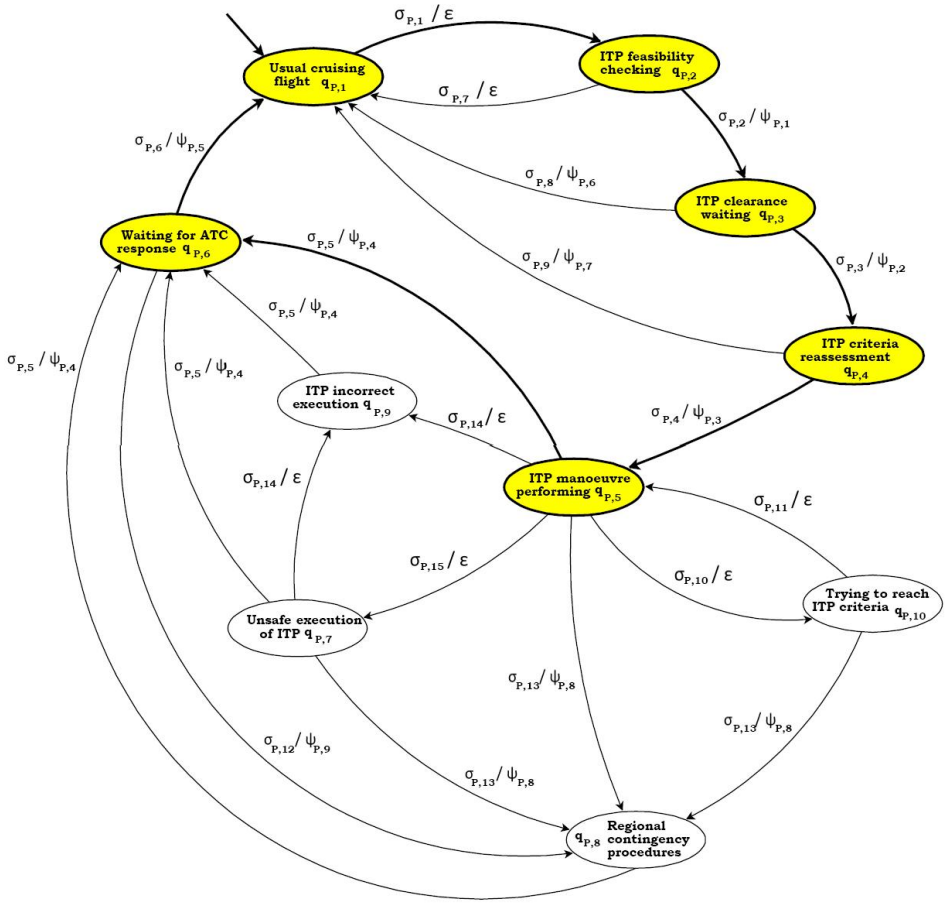


Figure 4.2: ITP Aircraft Agent - Correct execution without rejections and errors

reassessment phase ($\psi_{p,2}$), and the transition to *ITP criteria reassessment ($q_{p,4}$)* occurs. In this phase the flight crew has to verify if the ITP criteria are still met. If the response of the reassessment is positive ($\sigma_{p,4}$), the flight crew has to start immediately the ITP manoeuvre communicating it to the ATC ($\psi_{p,3}$). The transition to *ITP manoeuvre performing ($q_{p,5}$)* takes place. During this phase the flight crew has to follow the ITP execution criteria. When the manoeuvre is terminated ($\sigma_{p,5}$) the flight crew communicates the achievement of the new flight level to the ATC ($\psi_{p,4}$) and then waits for the confirmation from the ATC. A transition to *Waiting for ATC response ($q_{p,6}$)* occurs. The ITP manoeuvre can be considered correctly terminated when the ATC confirms the flight level ($\sigma_{p,6}$) and the flight crew confirms again the end of the ITP manoeuvre ($\psi_{p,5}$).

4.2.2 Correct execution with rejection by ATC or by the flight crew

The scenarios presented here are modelled using the transitions highlighted in Figure 4.3. They consider different ways to terminate correctly the ITP procedure with rejections either by the flight crew or by the ATC. During the first checking of the ITP initiation criteria, the flight crew can detect a non-compliance with one or more initiation criteria, and thus decide to abort the ITP request. This scenario is modelled by an unobservable transition triggered by the negative response of the feasibility checking ($\sigma_{p,7}$), from *ITP feasibility checking ($q_{p,2}$)* to *Usual cruising flight ($q_{p,1}$)*.

Furthermore it is possible that the ATC decides to deny the ITP request because of one or more non-compliances, as described by the operational hazard OH3 in Section 4.1. When ATC communicates that the ITP is denied ($\sigma_{p,8}$), the flight crew confirms the reception of this communication ($\psi_{p,6}$) and a transition from *ITP clearance waiting ($q_{p,3}$)* to *Usual cruising flight ($q_{p,1}$)* takes place.

Finally it is possible that after an ITP granted communication by the ATC, the flight crew detects one or more non-compliances during the reassessment phase($\sigma_{p,9}$), as described by OH4 and OH5 in Section 4.1. Thus the flight crew communicates rejection of the clearance to the ATC ($\psi_{p,7}$), and the transition from *ITP criteria reassessment ($q_{p,4}$)* to *Usual cruising flight ($q_{p,1}$)* occurs.

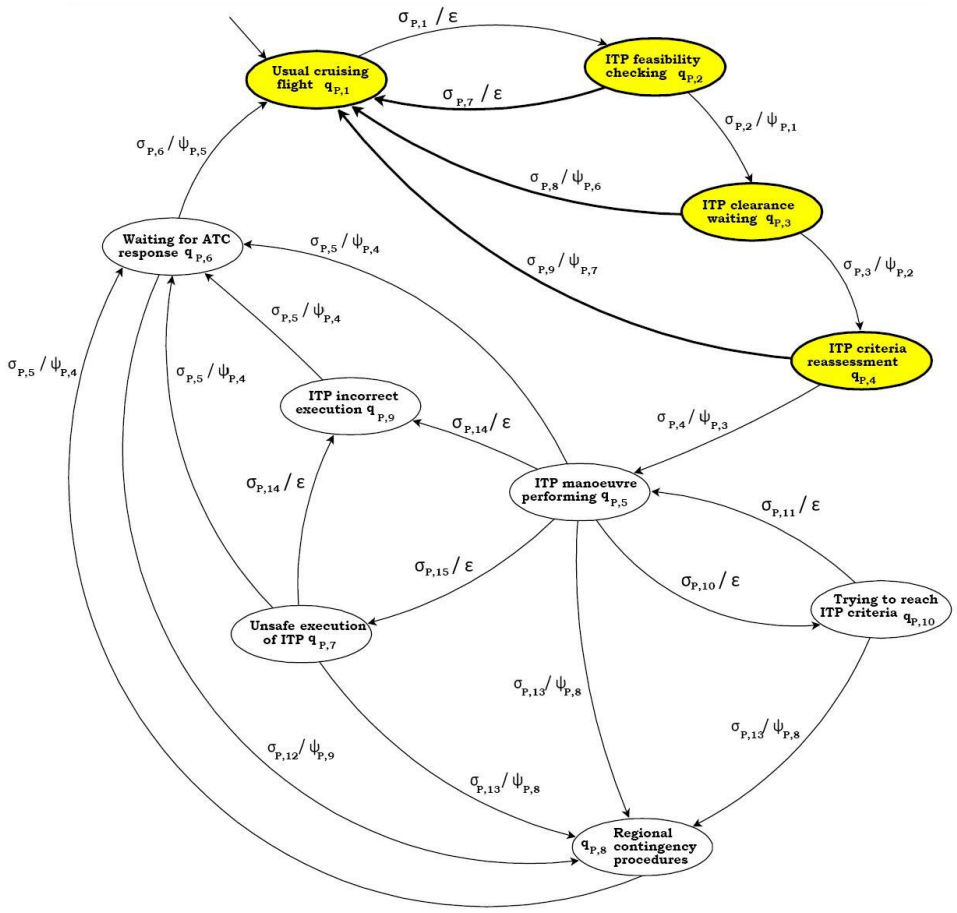


Figure 4.3: ITP Aircraft Agent - Correct execution with rejection by ATC or by the flight crew

4.2.3 Detected case of a wrong execution of ITP manoeuvre

During the ITP performing, the flight crew can detect a non-compliance with the ITP performance criteria. According to the severity of these non-compliances, the flight crew can decide to interrupt the manoeuvre, as described by OH1 in Section 4.1, or can try to restore the ITP performance criteria, as described by OH2D in Section 4.1.

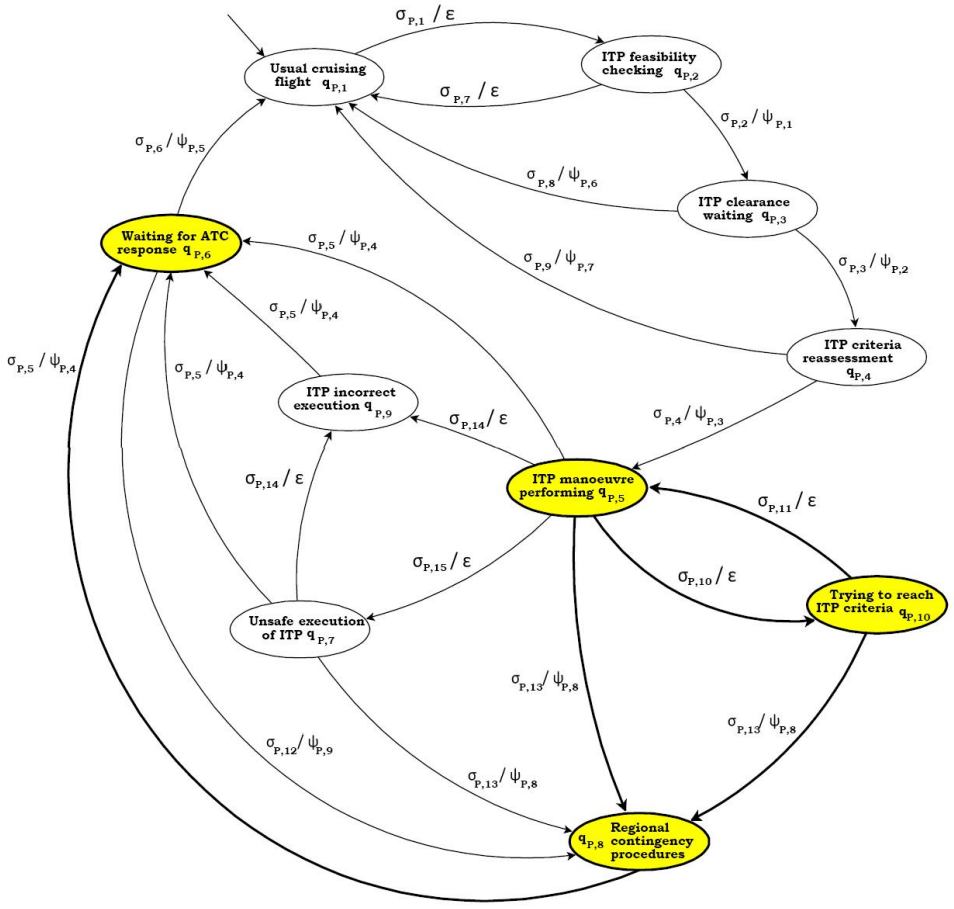


Figure 4.4: ITP Aircraft Agent - Detected case of a wrong execution of ITP manoeuvre

In the first case, if the flight crew decides to interrupt the manoeuvre

($\sigma_{p,13}$) an emergency communication to the ATC ($\psi_{p,8}$) is performed, and the flight crew immediately starts the regional contingency procedures. The transition from *ITP manoeuvre performing ($q_{p,5}$)* to *Regional contingency procedures ($q_{p,8}$)* occurs. In the second case, if the flight crew established again the ITP performance criteria the ITP manoeuvre is not ended off. This scenario is modelled using an unobservable transition triggered by the awareness of a non-compliance ($\sigma_{p,10}$) from *ITP manoeuvre performing ($q_{p,5}$)* to *Trying to reach again the performance criteria ($q_{p,10}$)*, and later by another unobservable transition which takes back to *ITP manoeuvre performing ($q_{p,5}$)*. If the flight crew does not restore the ITP performance criteria and decides to interrupt the ITP manoeuvre, then the flight crew interrupts the ITP manoeuvre ($\sigma_{p,13}$) and an emergency communication to the ATC is performed ($\psi_{p,8}$). The transition from *Trying to reach again the performance criteria ($q_{p,10}$)* to *Regional contingency procedures ($q_{p,8}$)* takes place. In any case, when the regional contingency procedures are terminated leveling off in a new flight level ($\sigma_{p,5}$), the flight crew reports the achievement of new flight level to the ATC ($\psi_{p,9}$), and the transition from *Regional contingency procedures ($q_{p,8}$)* to *Waiting for ATC response ($q_{p,6}$)* occurs.

4.2.4 Undetected case of a wrong execution of ITP manoeuvre

The scenarios described here are originated from different wrong situational awareness.

The first considered scenario represents the operational hazards OH2U-1, OH2U-2, OH2U-3 and OH2U-6 in Section 4.1. The possibility that the flight crew has made an error during the first or the second assessment and the ATC has granted the ITP manoeuvre is considered. The flight crew does not have the awareness of these errors, and the manoeuvre is performed as usual. This scenario is modeled by an unobservable transition ($\sigma_{p,15}$) from *ITP manoeuvre performing ($q_{p,5}$)* to *Unsafe execution of ITP manoeuvre ($q_{p,7}$)* triggered by a wrong situational awareness.

The second scenario considers a wrong execution of the ITP manoeuvre due to a wrong flight level awareness ($\sigma_{p,14}$), as described by OH6 in Section 4.1. As for the previous, the flight crew does not have the situational awareness of this error, and the ITP manoeuvre is performed as usual but towards a flight level that is different from the correct requested flight level. This is modeled using an unobservable transition from *ITP manoeuvre performing ($q_{p,5}$)* to *ITP incorrect execution ($q_{p,9}$)*. We also consider the scenario in which both a wrong situational awareness linked by the initiation criteria

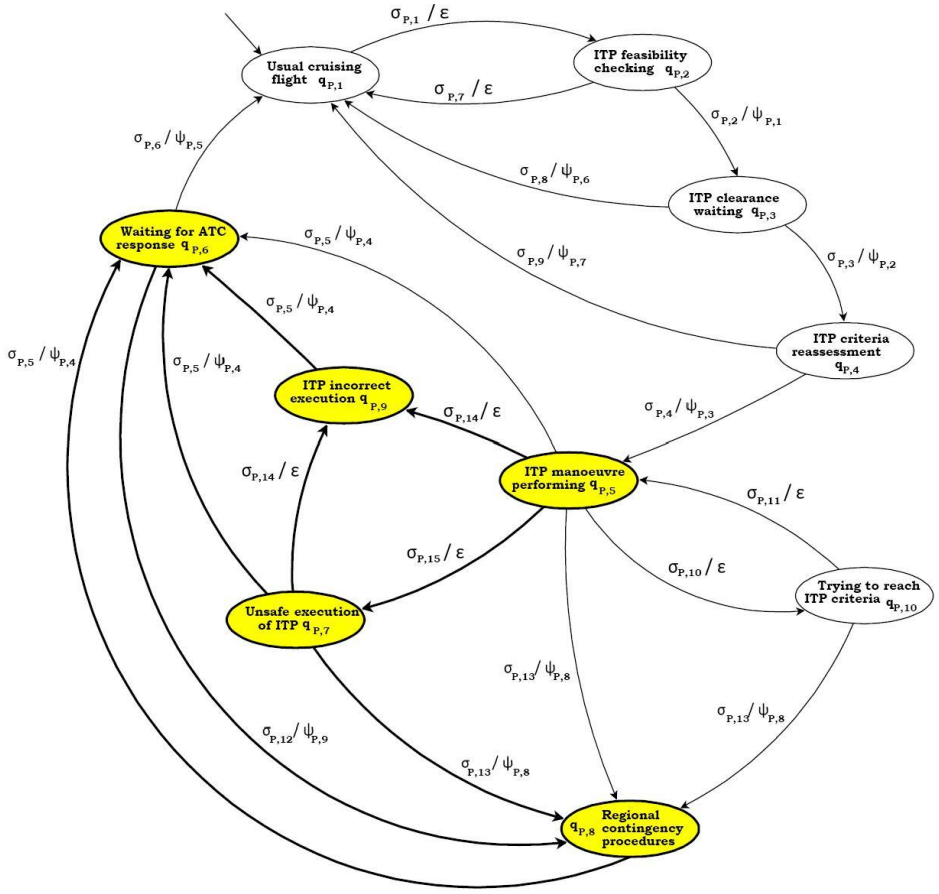


Figure 4.5: ITP Aircraft Agent - Undetected case of a wrong execution of ITP manoeuvre

and a wrong flight level awareness exist: from *ITP manoeuvre execution ($q_{p,5}$)* a first unobservable transition to *Unsafe Execution of ITP manoeuvre ($q_{p,7}$)* takes place, as described in the previous paragraph, and then a second unobservable transition to *ITP incorrect execution* $q_{p,9}$ occurs.

The third scenario considers the possibility that both from an *Unsafe execution of ITP manoeuvre ($q_{p,7}$)* and from *ITP incorrect execution ($q_{p,9}$)* the flight crew can terminate the manoeuvre leveling off at new flight level. When the manoeuvre is terminated ($\sigma_{p,5}$) and the flight crew reports the achievement of a new flight level to the ATC ($\psi_{p,4}$), the transition to *Waiting*

for ATC response ($q_{p,6}$) from *ITP incorrect execution ($q_{p,9}$)* or from *Unsafe execution of ITP manoeuvre ($q_{p,7}$)* takes place.

The last scenario considers a leveling off at an unsafe flight level. When the flight crew reports the achievement of new flight level to ATC, the ATC can detect an unsafe situation and can command the flight crew to start the regional contingency procedures ($\sigma_{p,12}$). The flight crew confirms the starting of the emergency procedures ($\psi_{p,9}$) and the transition from *Waiting for ATC response ($q_{p,6}$)* to *Regional contingency procedures ($q_{p,8}$)*. When the regional contingency procedures are terminated ($\sigma_{p,5}$), the flight crew reports the achievement of a new flight level to the ATC ($\psi_{p,4}$) and the transition to *Waiting for ATC response ($q_{p,6}$)* takes place.

4.3 Controller Agent

In this section, the hybrid model of the controller behavior during an ITP manoeuvre is defined. All discrete transitions are due to discrete inputs, and the continuous dynamics are absent. Thus, this model is a discrete event system $\mathcal{C} = (Q_c, Q_{c0}, \Sigma_c, \Psi_c, E_c, \eta_c)$ composed by:

- ◇ **The discrete states set** $Q_c = \{q_{c,1}, q_{c,2}, q_{c,3}, q_{c,4}, q_{c,5}, q_{c,6}, q_{c,7}\}$, where

  $q_{c,1}$ **:** *Usual monitoring.*

  $q_{c,2}$ **:** *Checking an ITP request.*

  $q_{c,3}$ **:** *Waiting for response of flight crew.*

  $q_{c,4}$ **:** *Monitoring after an ITP granted.*

  $q_{c,5}$ **:** *Checking for reference aircraft request.*

  $q_{c,6}$ **:** *Monitoring with a wrong situational awareness.*

  $q_{c,7}$ **:** *Monitoring after an ITP incorrect execution.*

- ◇ **The initial discrete states set** $Q_{c,0} = \{q_{c,1}\}$

- ◇ **The discrete inputs set** $\Sigma_c = \{\sigma_{c,1}, \sigma_{c,2}, \cdots, \sigma_{c,11}\}$ where:

  $\sigma_{c,1}$ **:** Request for an ITP manoeuvre received.

  $\sigma_{c,2}$ **:** Decision to grant an ITP request.

  $\sigma_{c,3}$ **:** Starting ITP confirmation by flight crew.

  $\sigma_{c,4}$ **:** Achievement of a new flight level by ITP flight crew.

  $\sigma_{c,5}$ **:** Decision to deny an ITP request.

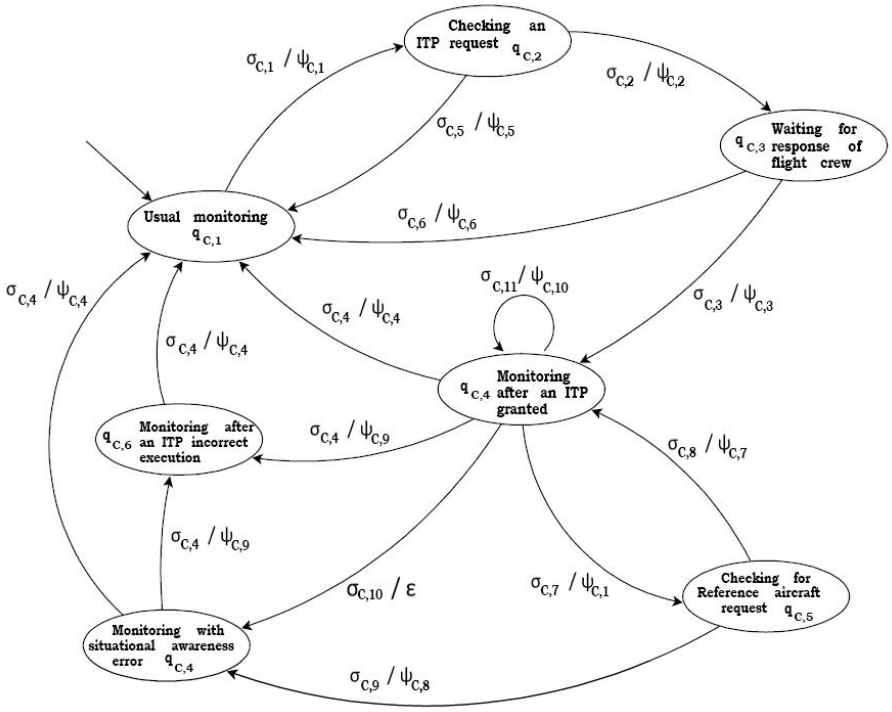


Figure 4.6: Controller Discrete Layer

$\sigma_{c,6}$ **:** ITP refused communication by flight crew.

$\sigma_{c,7}$ **:** Flight plan change request from a reference aircraft.

$\sigma_{c,8}$ **:** Decision to deny a plan change request to a reference aircraft.

$\sigma_{c,9}$ **:** Decision to grant a plan change request to a reference aircraft.

$\sigma_{c,10}$ **:** Wrong situational awareness followed by ITP grant.

$\sigma_{c,11}$ **:** Emergency communication by ITP flight crew.

◇ **Discrete Outputs Set** $\Psi_c = \{\psi_{c,1}, \psi_{c,2}, \psi_{c,3}, \cdots, \psi_{c,10}\} \cup \{\epsilon\}$, where:

$\psi_{c,1}$ **:** Command to wait for grant.

$\psi_{c,2}$ **:** ITP request granted communication to flight crew.

$\psi_{c,3}$ **:** ITP starting confirmation by ATC.

$\psi_{c,4}$ **:** ITP conclusion confirmation by ATC.

$\psi_{c,5}$ **:** ITP request denied communication to flight crew.

$\psi_{c,6}$ **:** ITP refused confirmation by ATC.

$\psi_{c,7}$ **:** Request denied communication to a reference aircraft.

$\psi_{c,8}$ **:** Request granted communication to a reference aircraft.

$\psi_{c,9}$ **:** Command to start regional contingency procedures by ATC.

$\psi_{c,10}$ **:** Emergency confirmation to ITP flight crew.

- ◇ **The set of transitions** $E_c \subseteq Q_c \times \Sigma_c \times Q_c$ is defined by the graph in Figure 4.6.
- ◇ **The discrete output function** $\eta_c : E_c \to \Psi_c$ is defined as in Figure 4.6.

The followings subsections explain how the proposed discrete event system C describes the behavior of the controller involved in the ATSA-ITP, and how the operational hazards presented in Section 4.1 can be modeled.

4.3.1 Correct execution without rejections and errors

In the simplest scenario we consider a correct execution of the ITP procedure, where the ITP aircraft requests, performs and terminates the manoeuvre without errors or wrong situational awareness, and the controller monitors the manoeuvre with a correct situational awareness. This scenario is represented in Figure 4.7.

Starting from location *Usual Monitoring (i.e. discrete state $q_{c,1}$)*, when the ATC receives the request for an ITP (i.e. discrete input $\sigma_{c,1}$) the discrete transition to *Checking an ITP request ($q_{c,2}$)* takes place. The discrete output $\psi_{c,1}$ is the communication made from the ATC to the flight crew in which the ATC confirms that has received the ITP request. Then, the ATC verifies the ITP criteria and if they are met, the ATC grants the ITP request ($\sigma_{c,2}$) and informs the flight crew by a specific communication ($\psi_{c,2}$). The transition to *Waiting for response of flight crew ($q_{c,3}$)* takes place: the flight crew has received the ITP granted communication and it is reassessing the ITP criteria. The ATC waits for the starting confirmation by the flight crew. Normally, this waiting time is short. The flight crew has to reassess and in case start the manoeuvre immediately after the ATC grant. When the Starting ITP confirmation ($\sigma_{c,3}$) has been received, the ATC confirms it to the flight crew ($\psi_{c,3}$), and the transition to *Monitoring after an ITP granted ($q_{c,4}$)* takes place. Once the flight crew terminates the manoeuvre, it communicates to the ATC the achievement of a new flight level ($\sigma_{c,4}$), and the ATC confirms the flight level ($\psi_{c,4}$). Then the transition to the first location *Usual monitoring ($q_{c,1}$)* occurs.

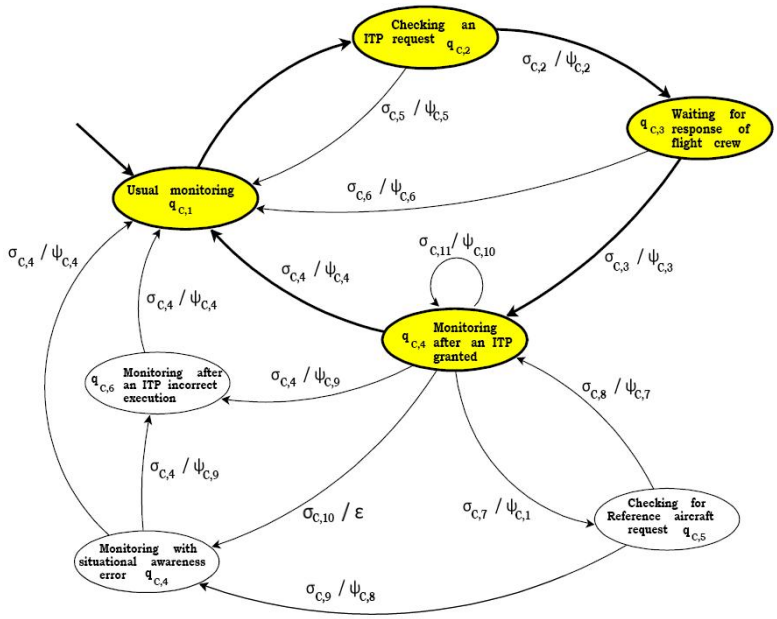


Figure 4.7: Controller Agent - Correct execution without rejections and errors

4.3.2 Correct execution with rejection or request denied

The scenarios presented here are modelled using the transitions depicted in Figure 4.8. When the flight crew requests an ITP clearance, the ATC can decide to deny the ITP request. When ATC decides to deny the ITP request ($\sigma_{c,5}$) and communicates to the flight crew this decision ($\psi_{c,5}$), the transition from location *Checking an ITP request ($q_{c,2}$)* to *Usual monitoring ($q_{c,1}$)* occurs. This models the operational hazard OH3 described in Section 4.1.

It is also possible that the flight crew rejects the ITP clearance. When the flight crew communicates the rejection of the ITP clearance ($\sigma_{c,6}$), the controller confirms the ITP rejection ($\psi_{c,6}$). The transition from *Waiting for response of flight crew ($q_{c,3}$)* to *Usual monitoring ($q_{c,1}$)* takes place. This transition models the operational hazards OH4 and OH5 described in Section 4.1.

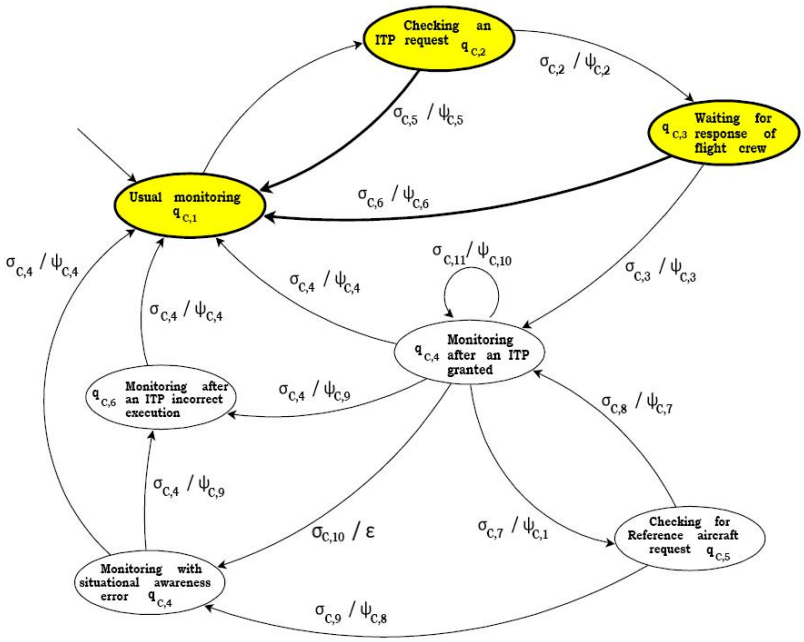


Figure 4.8: Controller Agent - Correct execution with rejection or request denied

4.3.3 Wrong situational awareness errors or ITP incorrect execution

The states and the edges which are used for modeling the following operational hazards are highlighted in Figure 4.9. The first scenario considers the possibility that ATC has granted an ITP request making some errors due to a wrong situational awareness ($\sigma_{c,10}$) during the checking phase, as described by the operational hazard OH2U-6 and OH2U-4 in Section 4.1. The ATC does not have the awareness of these errors and then grants the ITP request. The hybrid model represents this scenario using an unobservable transition from *Monitoring after an ITP granted ($q_{c,4}$)* to *Monitoring with a wrong situational awareness ($q_{c,6}$)*. From both these locations when the flight crew reports the achievement at a new flight level ($\sigma_{c,4}$), the ATC can value if the flight reached level is safe. If the flight level is unsafe, the ATC communicates the starting command for the regional contingency procedures to flight crew ($\psi_{c,9}$) and the transition to *Monitoring after an ITP incorrect execution ($q_{c,7}$)* takes place. These transitions take into account

the operational hazard OH6 described in Section 4.1.

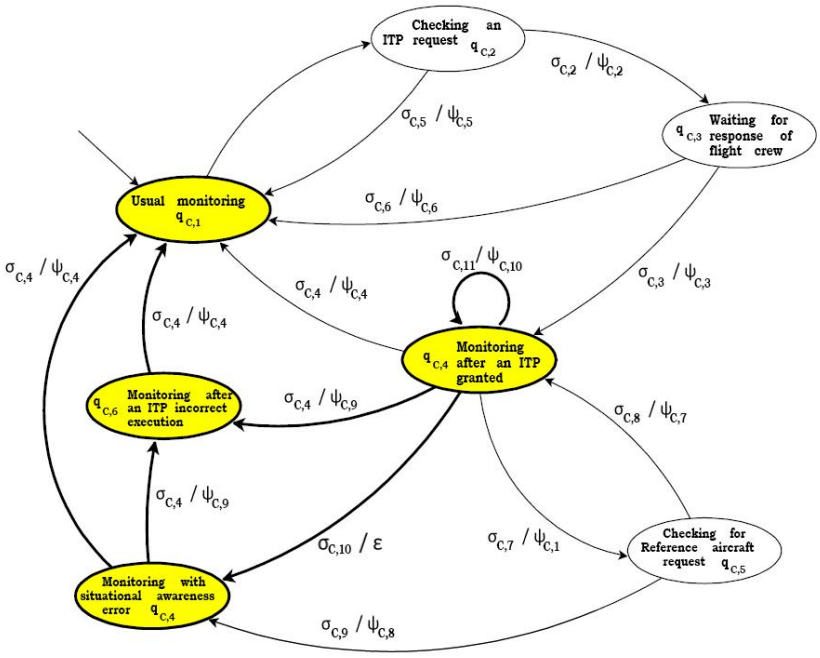


Figure 4.9: Wrong situational awareness errors or ITP incorrect execution

On the other hand, if the reached flight level is evaluated as safe by the ATC, the manoeuvre can be considered correctly finished, and the transition either from *Monitoring after an ITP incorrect execution ($q_{c,7}$)* or from *Monitoring with a wrong situational awareness ($q_{c,6}$)*, to *Usual monitoring ($q_{c,1}$)*, takes place. These last transitions take into account a possible correct termination of the manoeuvre even if errors have been made during the checking phases or during the manoeuvre itself.

Furthermore, it is possible that the flight crew detects an abnormal event and decides to interrupt the manoeuvre, as described by OH1 in Section 4.1. The ATC receives the emergency communication by the flight crew ($\sigma_{c,11}$) and confirms ($\psi_{c,10}$). Following the assumption AS.2 introduced in Section 4.1, the ATC does not have enough time to grant a new clearance. For this reason, the input ($\sigma_{c,11}$) triggers a transition to the same location.

4.3.4 Execution with a flight plan change request of a reference aircraft

The last scenario we consider consists of the operational hazards OH2U-5 described in Section 4.1. The locations and the transitions involved in the description of this scenario are shown in Figure 4.10.

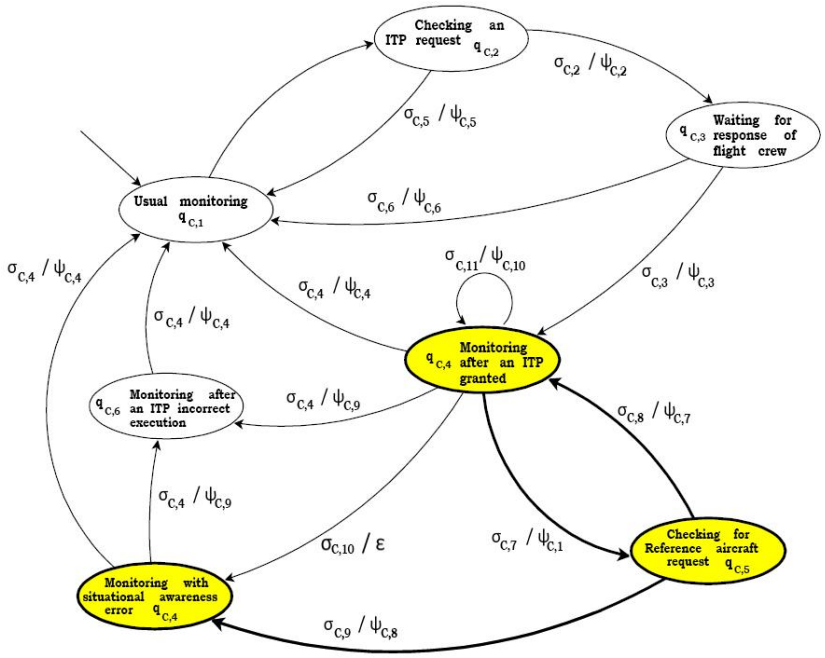


Figure 4.10: Execution with a flight plan change request of a reference aircraft

If a reference aircraft requests a flight plan change ($\sigma_{c,7}$), the ATC confirms the reception of the request ($\psi_{c,1}$). Normally the ATC must deny all requests from the reference aircraft throughout the ITP manoeuvre. If the ATC decides to deny the request ($\sigma_{c,8}$), he communicates this decision to the flight crew of the reference aircraft ($\psi_{c,7}$). This behavior is modeled using the transition from *Monitoring after an ITP granted ($q_{c,4}$)* to *Checking for reference aircraft request ($q_{c,5}$)* takes place. On the other hand, the ATC might decide to grant this request due to a wrong situational awareness. In this context, a transition from *Monitoring after an ITP granted ($q_{c,4}$)* to *Monitoring with a wrong situational awareness ($q_{c,6}$)* occurs.

4.4 Hybrid Observer for ITP Aircraft Flying Agent

The ITP Aircraft Flying Agent can be modeled using the non-deterministic hybrid system $\mathcal{H}_p$ which has been defined in the above section. Using this hybrid model it is possible to identify a set of critical states due to wrong situational awareness or errors performed during the manoeuvre performing. Let $Q_p^c = \{q_{p,9}, q_{p,7}\}$ be the set of critical states of $\mathcal{H}_p$. Algorithm 1 provides a method to design an observer $\mathcal{O}_p$ which can be used to verify the discrete states observability conditions for the hybrid model $\mathcal{H}_p$. The observer $\mathcal{O}_p = \{\hat{Q}_p, \hat{q}_{p,0}, \hat{Q}_{p,m}, \hat{\Psi}_p, \hat{E}_p, \hat{\eta}_p\}$ is shown in Figure 4.11, and is composed by the following objects:

- ◇ **The discrete states set** $\hat{Q}_p = \{\hat{q}_{p,1}, \hat{q}_{p,2}, \cdots, \hat{q}_{p,6}\}$, where: $\hat{q}_{p,1} = \{q_{p,1}, q_{p,2}\}$, $\hat{q}_{p,2} = \{q_{p,3}\}$, $\hat{q}_{p,3} = \{q_{p,4}\}$, $\hat{q}_{p,4} = \{q_{p,5}, q_{p,7}, q_{p,9}, q_{p,10}\}$, $\hat{q}_{p,5} = \{q_{p,6}\}$ and $\hat{q}_{p,6} = \{q_{p,8}\}$, with $q_{p,i} \in Q_p$ discrete states of the hybrid model $\mathcal{H}_p$.
- ◇ **The initial discrete states set** $\hat{q}_{p,0} = \{q_{p,1}, q_{p,2}\}$.
- ◇ **The marked states set** $\hat{Q}_{p,m} = \{\hat{q}_{p,4}\}$.
- ◇ **The set of discrete inputs** $\hat{\Psi}_p = \{\psi_{p,1}, \psi_{p,2}, \cdots, \psi_{p,9}\}$ where each $\psi_{p,i}$ represents a discrete output of the hybrid system $\mathcal{H}_p$.
- ◇ **The set of transitions** $\hat{E}_p \subseteq \hat{Q}_p \times \hat{Q}_p$ given by the graph in Figure 4.11. To each edge $e \in \hat{E}_p$ is associated a label $\psi_{p,i} \in \hat{\Psi}$ which corresponds to the discrete input that triggers the transition.
- ◇ **The discrete output function** $\hat{\eta}_p$ is the identity for all edges.

The observer $\mathcal{O}_p$ accepts as input the observable output of $\mathcal{H}_p$, and returns the current observer state $\hat{q} \in \hat{Q}$ (or a boolean value which indicates the achievement or not of a critical state). As discussed in Chapter 2, the observable discrete might be not sufficient to build an observer for the discrete state of a hybrid system. In fact the observer $\mathcal{O}_p$ cannot be used, in this case, to detect if the system has reached a critical state: given the output string $P(\varrho) = \psi_{p,1}\psi_{p,2}\psi_{p,3}$ the observer reaches the state $\hat{q}_{p,4}$, in which both safe states (i.e. $q_{p,5}, q_{p,10}$) and unsafe states (i.e. $q_{p,7}, q_{p,9}$) of $\mathcal{H}_p$ coexist. Thus, the observability condition is not satisfied and the set of critical states $Q_p^c = \{q_{p,9}, q_{p,7}\}$ is unobservable.

However, it is possible to design a set of extra output signals taken from the continuous inputs, outputs and dynamics in order to provide additional

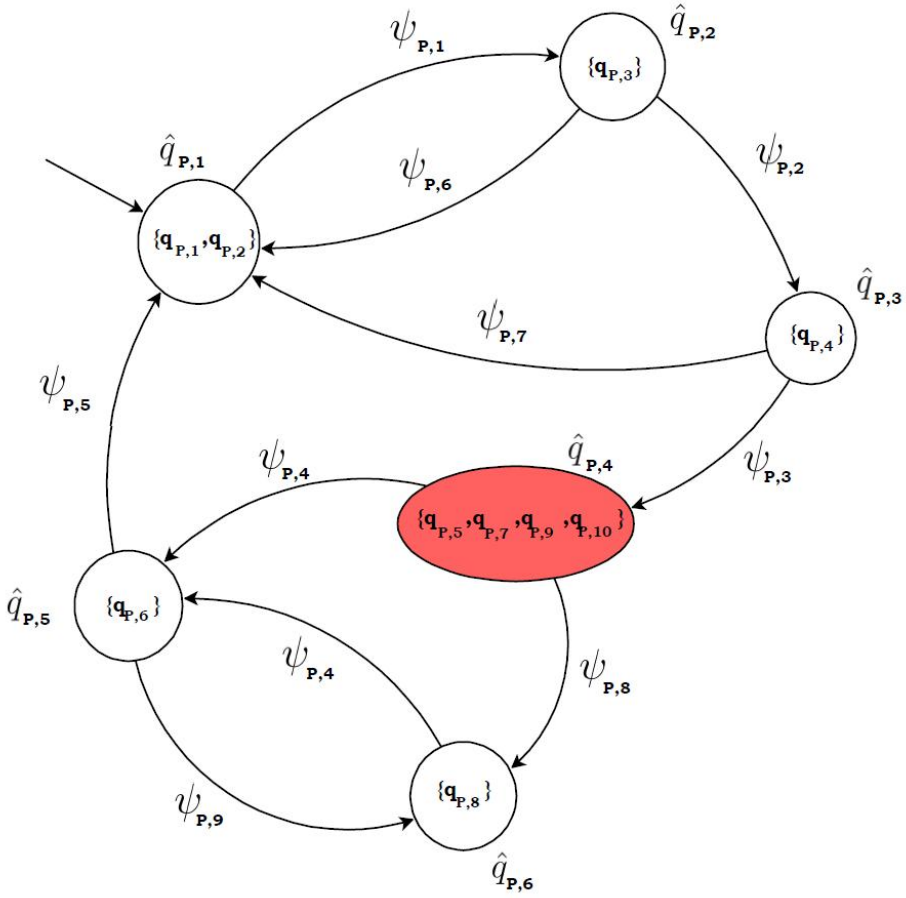


Figure 4.11: Observer $\mathcal{O}_p$ of the ITP Aircraft Flying Agent $\mathcal{H}_p$

information to discriminate the discrete states. A function $h_p : Q_p \rightarrow \Psi_e$ that associates to each state $q \in Q_p$ an additional discrete output symbol $h(q) \in \Psi_e$ can be designed as follows, in order to detect when the execution reaches one of the critical discrete states $q_{p,7}$ or $q_{p,9}$:

$$h_p(q) = \begin{cases} h(q_{p,7}) & if \quad q = q_{p,7} \\ h(q_{p,9}) & if \quad q = q_{p,9} \\ \varepsilon & otherwise \end{cases}$$

These extra output signals can be generated using the ADS-B data or other signals available from the on board equipments. Considering $h_p(\cdot)$, $\mathcal{H}_p$ can be modified in $\tilde{\mathcal{H}}_p$ by splitting each critical discrete state in two different states, linked by a new edge that represents the transition triggered by the extra output signal. The discrete layer of $\tilde{\mathcal{H}}_p$ is illustrated in Figure 4.12.

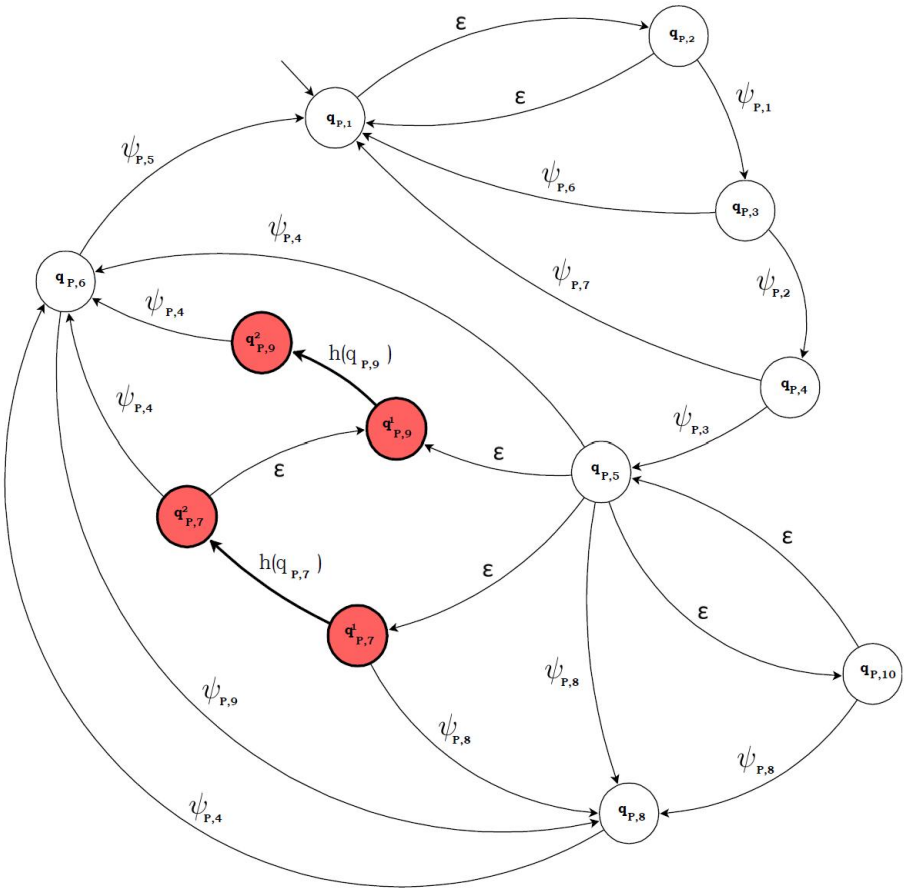


Figure 4.12: Discrete Layer of $\tilde{\mathcal{H}}_p$ using the extra output signals

Using again Algorithm 1 on $\tilde{\mathcal{H}}_p$, a new observer $\mathcal{O}_p^{\delta_p}$ can be designed, as illustrated in Figure 4.13, which satisfies the observability conditions.

The extra output signals $h(q_{p,7})$ and $h(q_{p,9})$ can be generated within a non-zero time $\delta_{h(q)}$. As explained in Chapter 2, the generation time $\delta_{h(q)}$ has to be less than the minimum dwell time associated to the corresponding

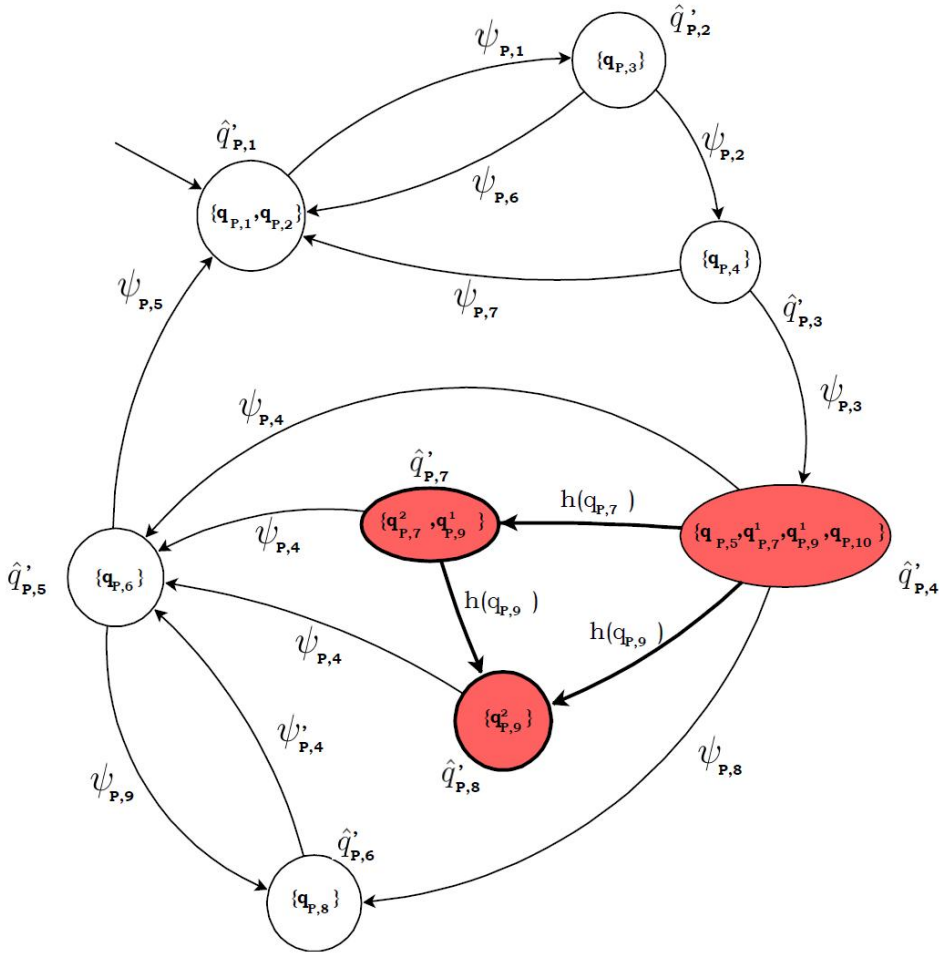


Figure 4.13: Observer $\mathcal{O}'_p$ of the ITP Aircraft Flying Agent $\tilde{\mathcal{H}}_p$

critical state. In that case, the observer $\mathcal{O}_p^{\delta_p}$ can be used to identify a critical discrete state with a delay $\delta_p = max\{\delta_{h(q)} : h(q) \in \Psi_e\}$, and the set of critical discrete states $Q_p^c = \{q_{p,9}, q_{p,7}\}$ can be considered observable with delay δ_p.

4.5 Hybrid Observer for Controller Agent

This section presents the hybrid observer of the controller agent $\mathcal{H}_c$ that has been defined in Section 4.3. As explained in the previous section, the first step consists of applying the Algorithm 1 in order to design the observer for the set of critical discrete states $Q_c^c = \{q_{c,6}, q_{c,7}\}$. $\mathcal{O}_c = \{\hat{Q}_c, \hat{q}_{c,0}, \hat{Q}_{c,m}, \hat{\Psi}_c, \hat{E}_c, \hat{\eta}_c\}$ is composed by the following objects:

- ◇ **The discrete states set** $\hat{Q}_c = \{\hat{q}_{c,1}, \hat{q}_{c,2}, \cdots, \hat{q}_{c,7}\}$, where: $\hat{q}_{c,1} = \{q_{c,1}\}$, $\hat{q}_{c,2} = \{q_{c,2}\}$, $\hat{q}_{c,3} = \{q_{c,3}\}$, $\hat{q}_{c,4} = \{q_{c,4}, q_{c,6}\}$, $\hat{q}_{c,5} = \{q_{c,7}\}$, $\hat{q}_{c,6} = \{q_{c,5}\}$ and $\hat{q}_{c,7} = \{q_{c,6}\}$, with $q_{c,i} \in Q_c$ discrete states of the hybrid model $\mathcal{H}_c$.
- ◇ **The initial discrete states set** $\hat{q}_{c,0} = \{q_{c,1}\}$.
- ◇ **The marked states set** $\hat{Q}_{c,m} = \{\hat{q}_{c,4}\}$.
- ◇ **The set of discrete inputs** $\hat{\Psi}_c = \{\psi_{c,1}, \cdots, \psi_{c,10}\}$ where each $\psi_{c,i}$ represents a discrete output of the hybrid system $\mathcal{H}_c$.
- ◇ **The set of transitions** $\hat{E}_c \subseteq \hat{Q}_c \times \hat{Q}_c$ given by the graph in Figure 4.14. To each edge $e \in \hat{E}_c$ is associated a label $\psi_{c,i} \in \hat{\Psi}$ that corresponds to the discrete input that triggers the transition.
- ◇ **The discrete output function** $\hat{\eta}_p$ is the identity for all the edges.

The observer $\mathcal{O}_c$ is depicted in Figure 4.14, and does not satisfy observability conditions. In fact, given the output string $P(\varrho)_{q_{c,4}} = \psi_{c,1}\psi_{c,2}\psi_{c,3}$ the observer reaches the states $\hat{q}_{c,4}$, in which both the safe state (i.e. $q_{c,4}$) and the unsafe state (i.e. $q_{c,6}$) of $\mathcal{H}_c$ coexist. Thus, the set $Q_c^c = \{q_{c,6}, q_{c,7}\}$ of critical discrete states is not observable.

As done in the previous section, it is possible to design a set of extra output signals in order to provide additional information to discriminate the discrete states. A function $h_c : Q_c \to \Psi_e$ which associates to each state $q \in Q_c$ an additional discrete output symbol $h(q) \in \Psi_e$ can be designed as follows, in order to detect when the execution has reached one of the critical discrete states $q_{c,6}$ or $q_{c,7}$:

$$h_c(q) = \begin{cases} h(q_{c,6}) & if \quad q = q_{c,6} \\ \varepsilon & otherwise \end{cases}$$

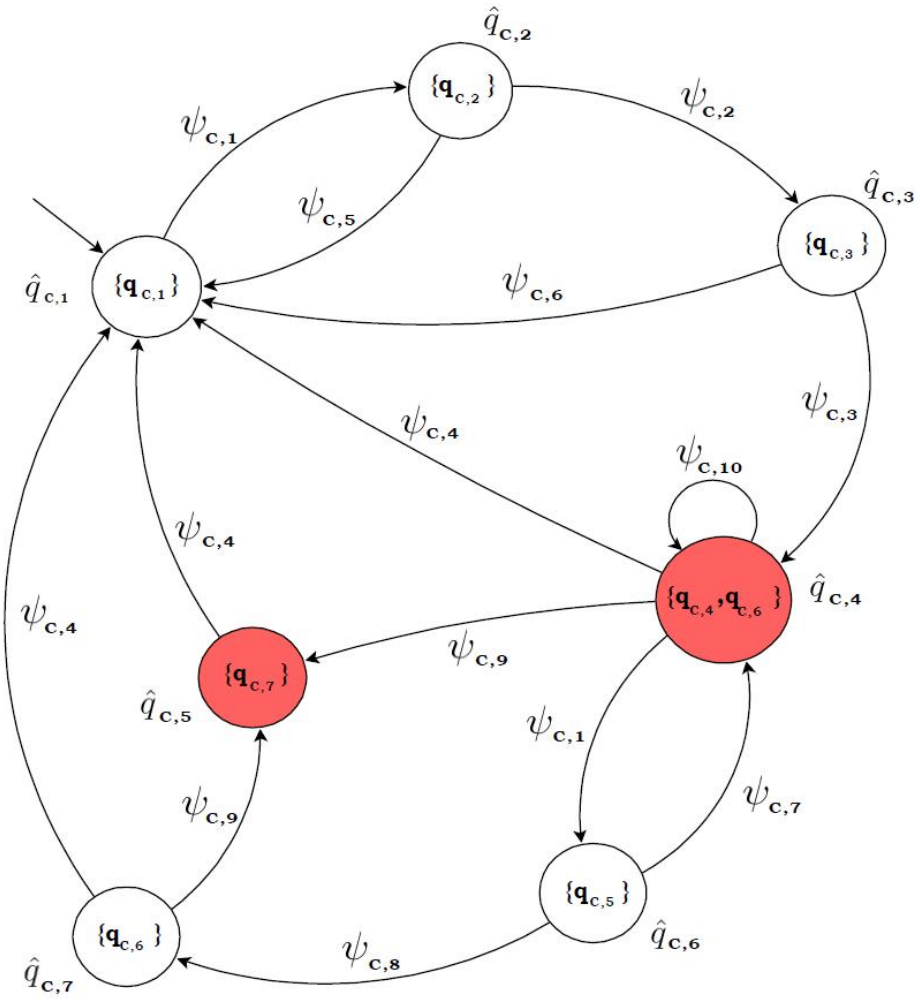


Figure 4.14: Observer $\mathcal{O}_c$ of the Controller Agent

This extra output signal can be generated automatically using the ADS-B data available by the controller. Considering the function $h_c(q)$, the discrete layer of $\mathcal{H}_c$ can be modified in $\tilde{\mathcal{H}}_c$ by splitting the states $q_{c,6}$ in two different states $q^1_{c,6}$ and $q^2_{c,6}$ linked by a new edge which represents the transition triggers by the extra output signal. The discrete layer of $\tilde{\mathcal{H}}_c$ is depicted

in Figure 4.15.

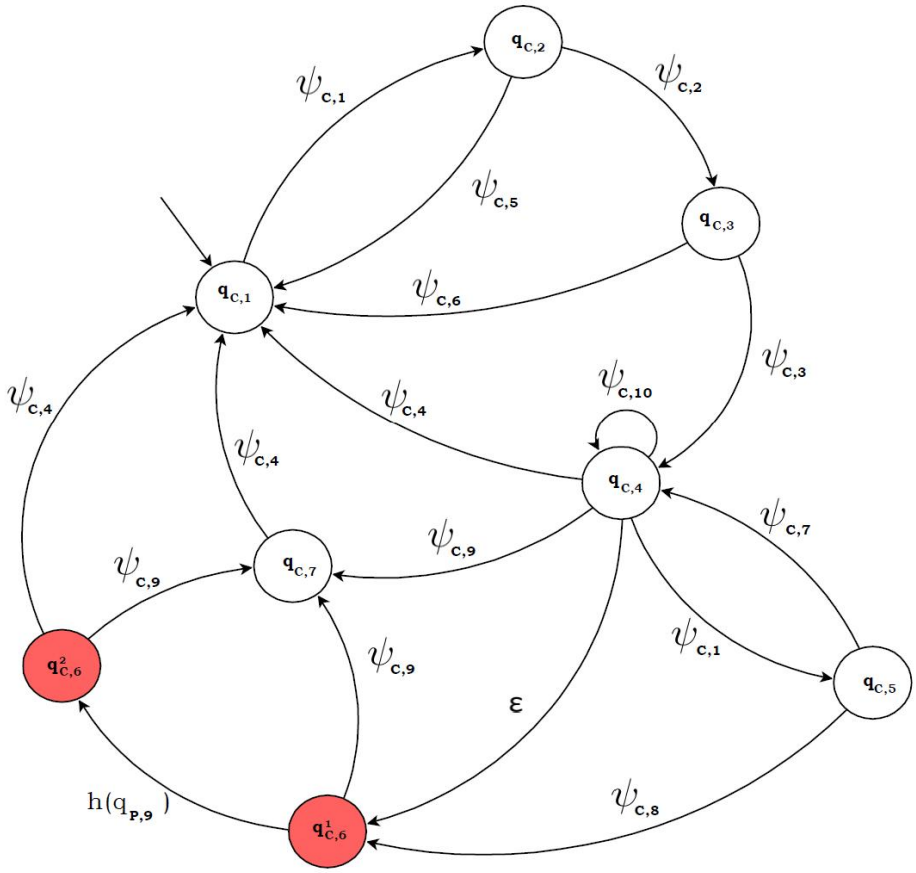


Figure 4.15: Discrete Layer of $\tilde{\mathcal{H}}_c$ using the extra output signals

Using again Algorithm 1 on $\tilde{\mathcal{H}}_c$, a new observer $\mathcal{O}_c^{\delta_c}$ which satisfies the observability conditions can be designed. The system obtained is depicted in Figure 4.16.

Notice that the extra output signals $h(q_{c,6})$ can be generated within a non-zero time. Assuming as generating delay $\delta_{h(q)}$, the observer $\mathcal{O}_c^{\delta_c}$ can be used to identify a critical discrete state with a delay $\delta_c = max\{\delta_{h(q)} : h(q) \in \Psi_e\}$ and the set of critical discrete states $Q_c^c = \{q_{c,6}, q_{c,7}\}$ can be considered observable with delay δ_c.

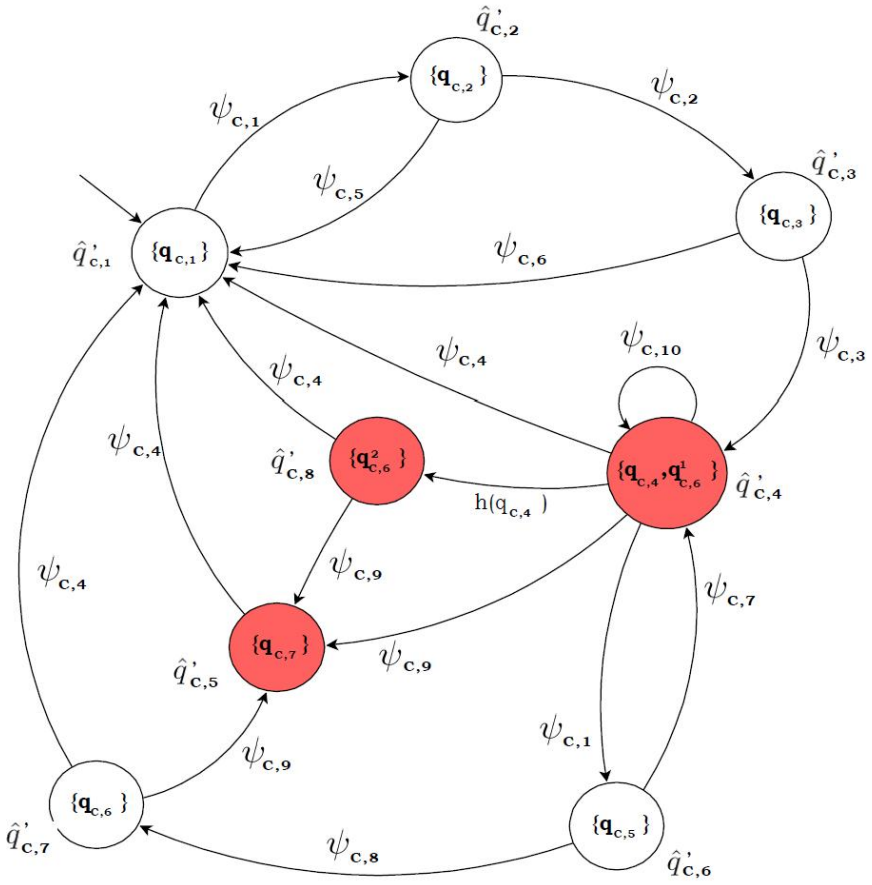


Figure 4.16: Observer $\mathcal{O}_c^{\delta_c}$ of the Controller Agent

Chapter 5

Conclusions

In this report, the hybrid system framework was used for safety modeling and automatic verification of air traffic management applications. The need to develop new sophisticated modeling and automatic verification methodologies originated from new challenges in safety and from the increasing complexity in the airborne procedures. In the aviation context, possible catastrophic events can occur due to e.g. unnoticed misunderstanding between agents involved. The hybrid system framework allows modeling and detecting these errors and their effects on the evolution of the procedures. We proposed a methodological framework to represent a complex multi-agent application in which a large set of possible abnormal situations may appear. Using hybrid modeling, we defined a set of critical states that correspond to wrong situational awareness or errors that may occur. The possibility of detecting those critical states depends on some observability properties of the system, called critical observability. We derived some algorithms for checking critical observability, which provide (i) the minimum number of steps K after which the critical states can be observed, and (ii) the minimum set of the extra signals needed to satisfy the observability conditions. In other words, 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 algorithms identify the extra information needed to obtain critical observability.

In order to validate our mathematical framework, we considered a specific procedure, the Airborne Traffic Situational Awareness In Trail Procedure (ATSA-ITP). The ATSA-ITP was developed to support a potential improvement of air traffic operations in Oceanic areas. With a new procedure and appropriate equipment, aircraft can be allowed a change of flight

levels with less stringent conditions than todays procedures. However, when introducing new procedures, the improvement of efficiency must not affect current safety of the flight and comfort of passengers. Hence, it needs to be proved, with concrete evidence, that safety is not affected. The advantage of our algorithmic framework is that, for very complex procedures whose state flow diagram contains a large number of states and transitions, automatic verification can uncover undesired and dangerous behaviors that might lead to catastrophic events.

We first applied Hybrid Control Systems Theory to define mathematical models of the procedural behavior of the agents involved in the ATSA-ITP. Using this hybrid model, we identified a set of critical states that correspond to wrong situational awareness or errors occurring during the manoeuvre. We then applied our results to investigate whether Situational Awareness errors in the ATSA-ITP design considered can be detected on the basis of the procedural measurable information exchanged between the flight crew and the air traffic controller. We found that the ATSA-ITP is not critically observable since a set of procedure errors that are not observable were identified. We finally used our algorithms to specify the set of extra output information needed to satisfy the critical observability conditions.

List of Figures

Bibliography

[1] R. Alur, T. Henzinger, G. Lafferriere, and G. Pappas. Discrete abstractions of hybrid systems. *Proccedings of the IEEE*, 88(2):971–984, July 2000.

[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] International Civil Aviation. Icao pans.atm doc 444. *Procedures for Air Navigation Services - Air Traffic Management, Fourteenth Edition*, pages 211–214, 2001.

[4] 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.

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

[6] E. De Santis, M. D. Di Benedetto, and G. Pola. On observability and detectability of continuous–time switching linear systems. In *Proceedings of the* 42^{nd} *IEEE Conference on Decision and Control, CDC 03, Maui, Hawaii, USA*, pages 5777–5782, December 2003.

[7] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Critical observability and hybrid observers for error detection in air traffic management. In *Proceedings of* 13^{th} *Mediterranean Conference on Control and Automation, Limassol, Cyprus*, 2005.

[8] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Critical observability for a class of stochastic hybrid systems and application to

air traffic management. Deliverable 7.5, Project IST-2001-32460 HYBRIDGE, http://www.nlr.nl/public/hosted-sites/hybridge, May 2005.

[9] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Error detection within a specific time horizon and application to air traffic management. In *Proceedings of the Joint* 44^{th} *IEEE Conference on Decision and Control and European Control Conference (CDC–ECC'05), Seville, Spain*, pages 7472–7477, December 2005.

[10] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Critical states detection with bounded probability of false alarm and application to air traffic management. In *Proceedings of the* 2^{nd} *IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), Alghero, Sardinia, Italy*, June 7-9 2006.

[11] S. Di Gennaro. Notes on the nested observers for hybrid systems. In *Proceedings of the European Control Conference 2003 – ECC'03, Cambridge, UK*, 2003.

[12] A. D'Innocenzo, M. D. Di Benedetto, and S. Di Gennaro. Observability of hybrid automata by abstraction. In J. Hespanha and A. Tiwari, editors, *Hybrid Systems: Computation and Control*, volume 3927 of *Lecture Notes in Computer Science*, pages 169–183. Springer Verlag, 2006.

[13] European and North Atlantic Office of ICAO. North atlantic mnps airspace operations manual (nat mnps). pages 6–13, 2005.

[14] European and North Atlantic Office of ICAO. North atlantic mnps airspace operations manual (nat mnps). pages 63–66, 2005.

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

[16] Lester and Hansman. Benefits and incentives for ads-b equipage in the national airspace system. *Report No. ICAT-2007-2*, August 2007.

[17] Jean-Marc Loscos. Asas:towards new cooperation based on airborne spacing. *Revue Technique de la DTI, ISNN 776-1239*, December 2005.

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

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

[20] M. Oishi, I. Hwang, and C. Tomlin. Immediate observability of discrete event systems with application to user–interface design. In *Proceedings of the* 42^{nd} *IEEE Conference on Decision and Control, Maui, Hawaii, USA*, pages 2665–2672, December 2003.

[21] C.M. Ozveren and A.S. Willsky. Observability of discrete event dynamic systems. *IEEE Transactions on Automatic Control*, 35(7):797–806, 1990.

[22] P.J. Ramadge. Observability of discrete event systems. In *Proceedings of the* 25^{th} *IEEE Conference on Decision and Control, Athens, Greece*, pages 1108–1112, December 1986.

[23] Requirements Focus Group (RFG). In-trail procedure in non-radar oceanic airspace (atsa-itp) - operational safety assessment (osa), v2.3. November 2007.

[24] Requirements Focus Group (RFG). In-trail procedure in procedural airspace (atsa-itp) application description, v8.0. June 2007.

[25] T. Yoo and S. Lafortune. On the computational complexity of some problems arising in partially–observed discrete event systems. In *Proceedings of the 2001 American Control Conference, Arlington , Virginia*, pages 25–27, 2001.