Hybrid System Framework for the Safety Modelling of the In Trail Procedure

Marco Colageo, Antonio Di Francesco
MSc Final-year students
College of Engineering, Center of Excellence DEWS
University of L'Aquila (Italy)

***Abstract*—The purpose of this paper is to provide a framework based on hybrid systems theory for safety modelling in air traffic management applications. This framework can be used to represent complex multi-agent applications in which a wide set of possible abnormal scenarios has been considered. In the aviation context possible catastrophic events can take place due to an error of a single agent involved in the procedure. It will be shown how the hybrid system framework allows a description and detection of these errors and their effects on the evolution of the procedure. At first it is proposed a description of the *ASEP-In Trail Procedure* which has been chosen to illustrate the methodology. Then, a general view about hybrid systems is proposed in order to explain the mathematical environment. Once basic concepts have been introduced, the hybrid model of the ASEP-ITP is explained and the concept of critical observability is introduced. Finally, an hybrid observer is proposed in order to detect unsafe situations associated with the hybrid system evolution.**

***Index Terms*—Safety Modelling, Hybrid Systems, Critical Observability, Air Traffic Management, In Trail Procedure.**

I. Introduction

THE volume of air traffic in the oceanic airspace is quickly increasing inducing the necessity of an improved efficiency in the management of the air traffic flows along these routes. The new procedures that are developed to satisfy this necessity have to increase capacity without affecting safety. This has to be proved using advanced methods. The complexity of the safety analysis of new procedures comes from the specific structure of the environment on which they are applied. The main aspect to be considered is that operations are the result of interactions between many entities of various types and at multiple locations. Furthermore the air traffic management systems are characterized by a mixed environment with human-controlled and computer-controlled subsystems the behaviors of which evolve following completely different logics that cannot be represented using the same class of mathematical models. This complexity can easily be modelled by means of agents in the context of hybrid system theory. Each decision taken by a single agent, either human operator or computer aid, influences the actions of all other agents involved. An hazardous decision induced by a wrong situational awareness can then be reflected into a catastrophic event. When modelling this kind of multi-agent systems all the decision making processes of each agent and their interactions have to be taken into account in order to identify non-nominal situations and act accordingly to prevent them to evolve into accidents.

Up to now the methodologies used for safety analysis can be classified in three main categories which reflect the temporal evolution of the complexity of airborne scenarios. As proposed in [5], [6] these categories are Sequential Modelling, Epidemiological Modelling and Systemic Accident Modelling: the *Sequential modelling* represents the accident as the outcome of a series of individual steps that occur in a given and (in principle) predictable order, using hierarchies such as the event tree or networks (Critical Path models or Petri networks); the *Epidemiological modelling* describes accidents as the outcome of a combination of manifest and latent factors that happen to exist together in space and time; the *Systemic accident modelling* considers accidents as something that must be expected. Systemic models have their roots in control theory and emphasize the need to base accident analysis on an understanding of the functional characteristics of the system rather than on assumptions or hypotheses about internal mechanisms or cause-effect chains. Systemic models deliberately try to avoid a description of an accident as a sequential or ordered relation among individual events or even as a concatenation of latent conditions.

In this paper we propose to apply a new methodology for safety modelling that has been developed in [3], [7], [9], [10]. This methodology is based on hybrid systems theory that provides a powerful framework to develop multi-agents models. Using this methodology it is possible to link the changes of the physical systems behaviour with the actions made by each agent. These actions can be right decisions taken by human operators, like pilots and controllers, but also decisions due to situational awareness errors. In this context each decision can represent an instantaneous change inside the continuous dynamics of an agent. Using hybrid model it is possible to describe the behaviour of single agent by means of discrete states. Different continuous dynamics that are associated with each discrete state and represent different aspects of the behaviour of the agent; the decisions taken by the agent and by the other agents involved generate the switches between the different discrete states. In this way, a complex behaviour of an agent can be suitably represented with simplified dynamics whose descriptive power is enhanced using the event-driven discrete systems, without making use of a more complex mathematical model. Once all the agents have been modelled, the behaviour of the whole system can

be analyzed by following the evolution of each agent and, at the same time, their interactions. In this way non-nominal and abnormal situations can be identified and subsequently inserted in the model as an additional state.

The paper is organized as follows. In Section 2 a description of the *In Trail Procedure (ITP)* application which has been chosen to illustrate the hybrid system framework is proposed. In Section 3, the hybrid model of the airborne procedure is presented explaining how it describes the procedure's steps. In Section 4, the hybrid observability problem is introduced and a hybrid observer is proposed. Section 5 provides some concluding remarks.

II. Description of the In Trail Procedure

The In Trail Procedure (ITP) is part of the *Airborne Separation Assistance Systems (ASAS)* area. ASAS embraces the goal of improving flight management by introducing a stronger interaction between pilots and controllers. The In Trail Procedure (ITP) here considered is envisioned as an *Airborne Separation (ASEP) Application* which is one of the four ASAS application categories. ASEP applications involve the transfer of responsibilities for the separation from the controller to the flight crew during the execution of the procedure. This can happen when the flight crew does have the most appropriate surveillance equipments (i.e. ADS-B and ASAS equipment) and is therefore able to monitor separation and act if necessary.

The ASEP-ITP [1], [2] described hereafter is a procedure that aims at improving flight efficiency along oceanic routes where procedural control is performed. The procedure provides a safe and practical method for air traffic controller to approve, and flight crew to conduct, climb and descent through different flight levels with less stringent applicability conditions than today's operations.

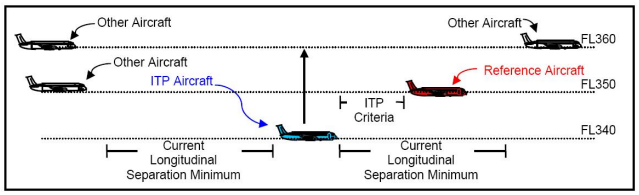

Fig. 1. Example of ITP geometry

A. ITP Criteria

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

- initiation ITP distance of no less than 10 NM and positive ground speed differential of no more that 20 kts, or
- ITP distance of no less than 15 NM and positive ground speed differential of no more that 30 kts.

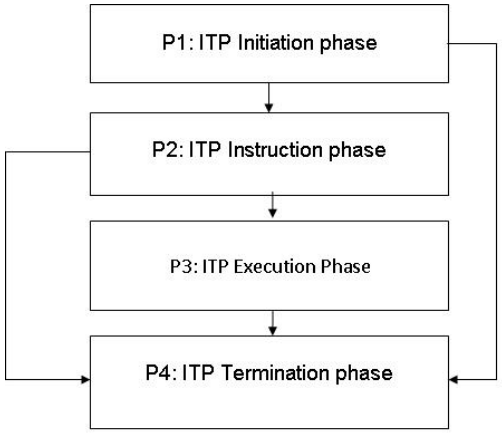

Fig. 2. ASEP-ITP phases diagram

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

The initiation criteria *(ITP speed/distance criteria)* that are necessary to start an ITP procedure are designed so that the estimated distance between the airliner which performs the climb or descent *(ITP aircraft)* and one or two ADS-B equipped aircraft *(reference aircraft)* in the surrounding area should get no closer than the *ITP separation minimum* of 5 NM until vertical separation is again achieved. These ITP speed/distance criteria are based on combinations of relative speed and relative distance values between the ITP aircraft and the reference aircraft are necessary conditions which have to be verified by the flight crew before requesting an ITP manoeuvre to the air traffic controller (ATC).

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

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

B. ITP Initiation phase

The decision to request an ITP rather than a standard flight level change will typically be based on a number of

factors outside the scope of the ITP application, such as crew preference and judgment, the magnitude of the desired flight level change, and any other information available to the crew about the flight's progress and proximate traffic situation.

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

1) Identification of ITP flight levels
   - The crew identifies a requested flight level, which is a flight level above (for a climb) or below (for a descent) one flight level and that is no more than 4000 ft from the initial flight level.
2) Checking ITP aircraft Performance by the crew:
   - The ITP aircraft is capable of performing a rate of climb or descent of at least 300 fpm at the assigned Mach number to the requested flight level.
   - The ITP aircraft is not expected to manoeuvre except for a climb or descent or a change of course to remain on their clearance.
3) Identification of reference aircraft The crew selects as reference aircraft up to two potentially blocking aircraft which meet the following criteria:
   - The ITP aircraft has the same direction with potentially blocking aircraft.
   - Qualified ADS-B data are available from potentially blocking aircraft.
   - The ITP speed/distance criteria are met with potentially blocking aircraft.
4) ITP Request
   - If the ITP criteria are met, the ITP aircraft crew requests the ITP, using the required ITP phraseology which provides the controller with the requested ITP flight level change geometry (i.e., leading or following), the ITP distance and the flight ID of reference aircraft.

C. ITP Instruction Phase

1) Issue of ITP Clearance by controller ATC determines if standard separation will be met with all aircraft at the requested flight level and at all flight levels between the ITP aircraft's initial flight level and requested flight level. If so, a standard (non-ITP) flight level change clearance can be issued. *If not,*
   - Determine that the ITP request message format is correct and that the flight crew has correctly identified the reference aircraft at the intervening flight level.
   - Determine that standard separation will be met with other aircraft (i.e., all but the reference aircraft) at the requested flight level and at all flight levels between the ITP aircraft's initial Flight Level and requested flight level.
   - Determine that the ITP aircraft is not a reference aircraft in another ITP clearance;
   - Determine that the ITP aircraft and the reference aircraft are on the same track.
   - Determine that the reference aircraft are non-manoeuvring and not expected to manoeuvre during the ITP. A change of course (only) to remain on the same identical Track as the ITP aircraft would not be considered a manoeuvre. The controller will not issue an ITP clearance if a reference aircraft is in the process of a manoeuvre or expected to manoeuvre.
   - Determine that the positive mach differential is no greater than 0.03 Mach.

   Based on the ITP aircraft's request and the controller's determination of the previous six conditions, the controller would issue the ITP clearance.
2) ITP Crew Re-Assessment
   - After the ITP clearance is issued, the flight crew of the ITP aircraft must again determine that the ITP criteria continue to be met with respect to the reference aircraft immediately before initiating the climb or descent. If the ITP criteria are no longer met, the crew refuses the clearance and remains at the initial flight level.

D. ITP Execution Phase

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

E. ITP Termination Phase

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

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

III. HYBRID MODEL OF THE ITP PROCEDURE

In this section the hybrid model of the ASEP-ITP is proposed.

A. Preliminaries on Hybrid System Theory

The following description provides a general view of the hybrid systems (i.e [3], [4]). Thus, only the basic definitions are presented in order to facilitate the understanding of the ITP hybrid model proposed.

Definition 1. ***(Non Deterministic Hybrid System [3])*** *A hybrid system is a tuple* $H = (Q \times X, Q_0 \times X_0, U, Y, \varepsilon, E, \Psi, \eta, Inv, G, R)$ *such that:*

- $Q = \{q_1, q_2, ..., q_N\}$ *is a set of* ***discrete states****.*
- $X \in \mathbb{R}^n$ *is a set of* ***continuous states****.*
- $Q_0 \subseteq Q$ *is a set of* ***initial discrete states****.*
- $X_0 \subseteq X$ *is a set of* ***initial continuous states****.*
- $U \subseteq \mathbb{R}^m$ *is a set of* ***continuous control input.***
- $Y \subseteq \mathbb{R}^p$ *is the set of* ***continuous observable output****.*
- $\{\varepsilon_q\}_{q \in Q}$ *associates to each discrete state* $q \in Q$ *the continuous time-invariant dynamics* $\varepsilon_q : \dot{x} = F_q(x)$ *with output* $y = g_q(x)$*.*
- $E \subseteq Q \times Q$ *is a* ***collection of edges****, where each edge* $e \in E$ *is a ordered pair of discrete states, the first component of which is known as 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* $\varepsilon, \psi_1, \psi_2, ..., \psi_r$ *where* ε *is the empty string that corresponds to unobservable output.*
- $\eta : E \rightarrow \Psi$ *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* $R_e : Inv_{s(e)} \rightarrow 2^{Inv_{t(e)}}$*, from* $Inv_{s(e)} \subset X$ *to the power set (i.e. the set of all the subsets) of* $Inv_{t(e)}$*.*

The system so defined can be compactly described using the graph depicted in the Figure 3. It should be noticed that this representation contains all the mathematical attributes introduced in the definition 1. The evolution of an Hybrid System can be synthesized in this way: supposed $(q_1, x_0) \in Init$ the initial hybrid system state, the continuous state x evolves according to the continuous dynamic $\dot{x}$ with $x(0) = x_{1,0}$, as long as $x \in Inv_{q_1}$, whereas the discrete state q remains constant $q(t) = q_1$. If at some point, state reaches guard G_{e1} then the discrete transition from q_1 to q_2 is enable. In this situation, when the continuous state leaves the Inv_{q_1} the discrete transition is forced, and the state x changes value according to the reset map R_{e1}. Next the process is repeated starting from $(q_2, x_{2,0})$.

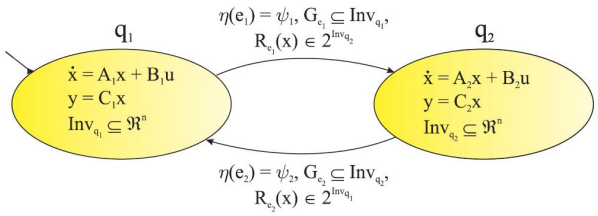

Fig. 3. Non-deterministic Hybrid System

A particular class of non-deterministic hybrid systems is represented by the *rectangular automata*. This subclass is introduced here and is the one that will be used in the hybrid model of ASEP-ITP. Considered the space $\mathbb{R}^n$ with variables $x_1, \cdots, x_n$, a rectangular set B of dimension n is the product of n intervals $B_i \subseteq \mathbb{R}$ of the real line, where each B_i is a bounded or unbounded interval.

Definition 2. ***(Rectangular Automaton [4])****: A rectangular automaton is a hybrid system, as defined in Definition 1, that also satisfies the following constraints:*

- *For every discrete state* $q \in Q$*, the set of initial continuous states* $X_0 \subseteq X$ *and the invariant set* $Inv_q \subseteq X$ *are rectangular sets.*
- *For every discrete state* $q \in Q$*, there is a rectangular set* B^q *such that the continuous time invariant dynamics* $\varepsilon_q : \dot{x} = F_q(x) \in B^q$ *for all* $x \in \mathbb{R}^n$*.*
- *For every edge* $e \in E$*, the set* $Guard_e$ *is a rectangular set, and there is a rectangular set* B^e *and a subset* $J^e \subseteq \{1, \cdots, n\}$ *such that for all* $x \in \mathbb{R}^n$ *the reset map is* $R_e = \{(x_1^{'}, \cdots, x_n^{'}) \in \mathbb{R}^n |$ *for all* $1 \leq i \leq n$*, if* $i \in J^e$ *then* $x_i^{'} \in B_i^e$ *else* $x_i^{'} = x_i\}$*.*

Therefore, in a rectangular automaton, the derivative of each variable stays between two fixed bounds, which can be different in different discrete states. Then in each discrete state $q \in Q$ the continuous dynamics can be defined as $\dot{x}_i \in B_i^q \subseteq B^q$ for all $1 \leq i \leq n$. With each discrete jump across an edge e, the value of the variable x_i either does not change if $i \notin J^e$, or resets non-deterministically to a new value within some fixed constant interval $B_i^e \subseteq B^e$ if $i \in J^e$.

The hybrid model proposed below is slightly different from the one of the Definition 2. This model also embeds a set Σ of discrete input signals, and each edge $e \in E$ is associated to a symbol $\sigma \in \Sigma$ that triggers the discrete transition between the states linked by e. These inputs can be considered as discrete disturbance or control inputs which model the communication among the agents.

B. Assumptions

The ASEP-ITP can be decomposed in various subsystems representing the agents involved in the procedure, each with hybrid dynamics modelling its specific operations. It should be remarked that to exploit the descriptive power of hybrid system each agent must be considered by itself and subsequently the effects of their actions on the dynamics of other agents can be considered merging the models so obtained.

The agents considered are:

- Air crew flying of ITP aircraft
- Oceanic controller

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

The model proposed considers the simplest case of ASEP-ITP execution where the ITP aircraft requests a climb through one flight level, with only one leading reference aircraft involved and without other blocking aircraft. Furthermore, no wind is assumed. The continuous dynamics used in this approach are intentionally simplified. In fact due to the configuration of the traffic flows in the oceanic airspace (i.e organized parallel tracks system) it is possible to focus on longitudinal and vertical dynamics without considering the lateral dynamics. Moreover, for safety analysis of this ITP, using a more complicated model that considers a complete dynamic of the aircraft would not be relevant.

C. Pilot flying of ITP aircraft Agent

Before explaining the model, the following variables are introduced:

1) z_i initial flight level of the aircraft
2) z_f requested flight level of the ITP aircraft
3) $v_{x,min}$ minimal ground speed of the ITP aircraft
4) $v_{x,max}$ maximal ground speed of the ITP aircraft
5) $v_{z,max}$ maximal vertical speed of the ITP aircraft
6) x_r longitudinal position of the reference aircraft
7) v_{rx} the ground speed of the reference aircraft
8) M_i assigned Mach number for the ITP aircraft
9) a speed of sound, assumed as a constant value

Furthermore the following interesting areas of the airspace can be identified:

1) A safe region in which the ITP aircraft performing the ITP manoeuvre respects the ITP minimum distance separation. The safe zone is defined as $\Omega_S = \{(x,z) : x \in [-\infty, x_r - 5], z \in (z_i, z_f)\}$.
2) Thus, an unsafe zone can be defined as follows: $\Omega_U = \{(x,z) : x \in [x_r - 5, +\infty], z \in (z_i, z_f)\}$.

The agent $\mathcal{H}_p$ *Pilot Flying of ITP Aircraft* can be described using a model based on Definition 2. The following are the objects of the system:

- $Q = \{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}, q_{11}, q_{12}\}$ is the set of discrete states each associated with a node inside the graph depicted in Figure 4;
- $X = \{(x,z) : x \in \mathbb{R}_0^+, z \in \mathbb{R}^+\}$, with $\mathbb{R}_0^+ = \mathbb{R}^+ \cup \{0\}$ is the set of the continuous state values where x represents the longitudinal position of the aircraft expressed in nautical miles, z the altitude of the aircraft expressed in hundred of feet (i.e. flight level inside the International Standard Atmosphere).
- The initial discrete state is q_1;
- The continuous dynamics are the followings:
  - $F_{q_1}(x,z) = \{\dot{x} = M_i a, \dot{z} = 0\}$
  - $F_{q_7}(x,z) = \{\dot{x} \in [v_{x,min}, v_{rx} + 30], \dot{z} \in [300, v_{z,max}]\}$
  - $F_{q_8}(x,z) = \{\dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in [300, v_{z,max}]\}$
  - $F_{q_9}(x,z) = \{\dot{x} \in [v_{x,min}, v_{x,max}], \dot{z} \in [0, 300]\}$
  - $F_{q_{10}}(x,z) = \{\dot{x} = Ma, \dot{z} = 0, M \neq M_i\}$
  - $F_{q_i}(x,z) = F_{q_1}(x,z)$ for $i = 2,3,4,5,6,11,12$
- $\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9\}$ is the set of discrete inputs, where σ_1 means decision to make an ITP, σ_2 represents the reassessment failed, σ_3 represents the ITP criteria are not verified, σ_4 means the ITP criteria verified, σ_5 represents the clearance denied, σ_6 means the clearance issued, σ_7 means detection of an abnormal event, $\sigma_8 = \varepsilon$, σ_9 represents a situational awareness error;
- $\Psi = \{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6\} \cup \{\varepsilon\}$ is the set of discrete outputs, where ψ_1 means the clearance rejected by the crew, ψ_2 represents the clearance request , ψ_3 represents the clearance accepted by the crew, ψ_4 means the abnormal termination communication by the crew to the controller, ψ_5 means the report established at the new flight level, ψ_6 represents the confirmation by the crew of the reception of the denied clearance;
- $E \subseteq Q \times Q$ is the set of transitions given by the graph depicted in Figure 4. A label $\sigma \in \Sigma$ is associated to each edge as shown in Figure 4;
- $\eta : E \rightarrow \Psi$ the discrete output function defined by the graph depicted in Figure 4;
- The domains of the discrete states are the following:
  - $Inv_{q_1} = \{(x,z) : x \in \mathbb{R}_0^+, z = z_i\}$
  - $Inv_{q_7} = \{(x,z) \in \Omega_S\}$
  - $Inv_{q_8} = \{(x,z) \in \Omega_S \cup \Omega_U\}$
  - $Inv_{q_9} = Inv_{q_8}$
  - $Inv_{q_{10}} = \{(x,z) : x \in \mathbb{R}_0^+, z = z_f\}$
  - $Inv_{q_{12}} = Inv_{q_{10}}$
  - $Inv_{q_i} = Inv_{q_1}$ for $i = 2,3,4,5,6,11$
- The guards are the empty set for all the discrete transitions excepted for:
  - $G(q_7, q_{12}) = \{x \in \Omega_S, z = z_f\}$
  - $G(q_8, q_{12}) = G(q_9, q_{12}) = \{(x,y) : x \in \mathbb{R}^+\}$
- The reset function is always the identity function excepted for:
  - $R(q_7, q_{11}) = \{x_{q_{11}} = x_{q_7}, z_{q_{11}} = z_i\}$
  - $R(q_8, q_{11}) = R(q_9, q_{11}) = R(q_7, q_{11})$

The direct graph of this hybrid model is shown in the Figure 4. The evolution of an ITP could be followed on the graph in this way. Initially the aircraft is in the *cruise (i.e. discrete*

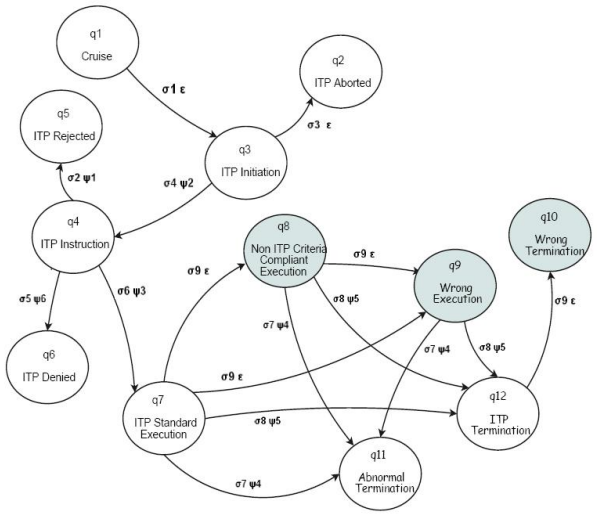

Fig. 4. Direct graph of pilot flying of ITP aircraft agent. The shadowed locations are the critical states

state q_1) phase. When the flight crew performs an ASEP-ITP manoeuvre, the discrete transition to the *ITP Initiation (q_3)* takes place. Then, the flight crew has to verify if the ITP speed/distance criteria are met. If the criteria are not satisfied, the flight crew aborts the ITP initiation phase and there exists the discrete transition to the *ITP Aborted* (q_2) state. If the criteria are verified, the flight crew requests the clearance to the ATC and the discrete transition to *ITP instruction* (q_4) takes place. In this phase, if the clearance is denied by the ATC the ITP is not executed and the discrete switch to *ITP denied* (q_6) takes place. When the clearance is issued, the flight crew has to recheck the ITP speed/distance criteria in order to evaluate if the criteria are still met. If the criteria are not met, the flight crew rejects the clearance and this is represented by the discrete switch to the *ITP rejected* (q_5) state. If the ITP criteria are still met, the flight crew accepts the clearance, communicates it to the ATC and the discrete state *ITP Instruction* (q_4) changes to *Standard ITP execution* (q_7) state. It can happen that during the first or the second verification of ITP speed/distance criteria the flight crew makes an error due to a wrong situational awareness. This scenario is modelled using an unobservable transition from the *Standard ITP execution* (q_7) to *Non ITP criteria compliant execution* (q_8); this transition is not detectable because the flight crew does not know that an error occurred. From both these discrete states, it is possible to jump to the *Wrong execution* (q_9) state, which models the situation where, again due to a situational awareness error, the flight crew is performing the manoeuvre without compliance with the performance criteria (i.e. vertical speed more than 300 ft/min and Mach number constant). Starting from the discrete states *Standard ITP execution* (q_7), *Non ITP criteria compliant execution* (q_8) and *Wrong execution* (q_9), the manoeuvre is terminated in two different ways. In the first case the flight crew detects an abnormal event and the manoeuvre is terminated in an abnormal mode. The flight crew communicates to the ATC the abnormal termination and the discrete transition takes place to *Abnormal Termination* (q_{11}). In the second case, the ITP terminates in the correct way; the flight crew communicates to the ATC established in the requested flight level and the discrete state changes to *ITP termination* (q_{12}) state. From this discrete state a situational awareness error can bring to an unsafe situation. In fact, if the flight crew has changed the Mach number during the manoeuvre for safety reasons and it does not revert to the assigned Mach number when the requested flight level is reached, an unobservable transition to *Wrong termination* (q_{10}) takes place.

D. Oceanic controller Agent

The hybrid model of the oceanic controller agent does not include continuous dynamics and all the discrete transitions take place because of the occurrence of a discrete input. Thus, this hybrid model can be considered as a *discrete event system*. The objects of the model are the followings:

- $Q = \{q_1, q_2, q_3, q_4\}$ is the set of discrete states which are associated with the corresponding vertices of the graph shown in Figure 5.
- The initial discrete state is q_1.
- $\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ is the set of discrete inputs, where σ_1 represents the request of an ITP, σ_2 means the abnormal termination communication, σ_3 means a situational awareness error and σ_4 represents the communication of ITP terminated.
- $\Psi = \{\psi_1, \psi_2, \psi_3, \psi_3, \psi_4\} \cup \{\varepsilon\}$ is the set of discrete outputs where ψ_1 means the clearance issued, ψ_2 represents the ITP request denied, ψ_3 represents the abnormal termination confirmation, ψ_4 means the confirmation of a standard ITP termination.
- $E \subseteq Q \times Q$ is the set of transitions given by the graph depicted in Figure 5. A label $\sigma \in \Sigma$ is associated to each edge as shown in Figure 5.
- $\eta : E \rightarrow \Psi$ the discrete output function defined by the graph depicted in Figure 5.

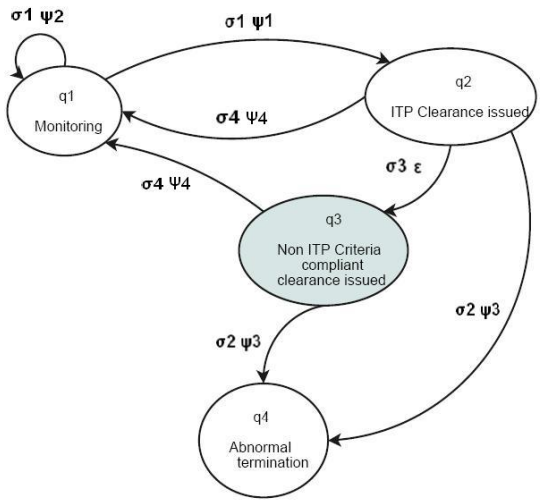

Fig. 5. Discrete graph of the Oceanic Controller agent

At the beginning of the ITP application, the discrete state is *Monitoring (i.e. discrete state q_1)*, which models the usual monitoring of the controller. When the ITP request from the flight crew is received, the controller can decide to issue or deny the clearance on the basis of the verification of some criteria. If the request is not accepted, the controller communicates the deny to the flight crew and the discrete state does not change; if the clearance is issued, the discrete transition to the *ITP clearance issued* (q_2) takes place. During the verification of the criteria, the controller can make an error due to a wrong situational awareness. In this case, an unobservable transition from *ITP clearance issued* (q_2) to *Non ITP criteria compliant clearance issued* (q_3) takes place. From both *ITP clearance issued* (q_2) to *Non ITP criteria compliant clearance issued* (q_3) it is possible to jump to *Abnormal Termination* (q_4), when the flight crew communicates the occurrence of an abnormal event; otherwise, if the controller receives the confirmation of a standard ITP termination by the flight crew, the discrete state is reverted to the initial *Monitoring* (q_1) state.

IV. Hybrid Observer of the ITP Agents

The hybrid model presented in the previous section describes in detail the procedure and identifies safe and unsafe scenarios. For safety analysis it is important to detect, instantaneously or with an acceptable delay, the discrete states of the hybrid model associated with hazardous situations. This issue represents a typical discrete observability problem of hybrid systems. The idea is to design a finite state machine, known as an "observer", which is able to discriminate the current discrete state using only the observable output generated by the transitions.

In the literature, several definitions of observability for hybrid systems have been proposed. As defined in [7], [11], an hybrid system is K-current-state observable if any discrete location of the hybrid system can be identified by the use of the discrete outputs, after a finite number $K > 0$ of discrete transitions. It should be noticed that this notion cannot allow for the immediate detection of critical states (i.e. $K = 0$). An alternative definition is presented in [8] and requires that all the states of the system, both safe and unsafe, have to be immediately observable. For safety analysis it is sufficient to consider the observability only of the set of the critical states instead of the whole discrete state space. This approach is considered in [9] where *critical observability* is proposed.

The next section presents the hybrid observer designed for the Pilot Flying of ITP Aircraft Agent. This observer checks for the critical observability of the agent, assuming $Q_c = \{q_8, q_9, q_{10}\}$ as set of critical states. The same approach can be used to design the observer of the other agents involved in the ITP procedure.

A. Hybrid Observer of Pilot flying of ITP aircraft Agent

The algorithm presented in [9] provides a method to design the observer $\mathcal{O}_p$ of the hybrid system $\mathcal{H}_p$ starting from the direct graph associated to the system. In this way, the observer obtained is a finite state machine $\mathcal{O}_p = (\hat{\mathcal{Q}}, \hat{q}_0, \hat{\mathcal{Q}}_m, \hat{\Psi}, \hat{E}, \hat{\eta})$ defined as follows:

- $\hat{\mathcal{Q}} = \{\{q_1, q_2, q_3\}, \{q_4\}, \{q_5\}, \{q_6\}, \{q_7, q_8, q_9\}, \{q_{11}\}, \{q_{10}, q_{12}\}\}$, where q_i are the discrete states of $\mathcal{H}_p$.
- The initial state is $\hat{q}_0 = \{q_1, q_2, q_3\}$.
- The set of final or accepting states is $\hat{\mathcal{Q}}_m = \{\{q_7, q_8, q_9\}, \{q_{12}, q_{10}\}\}$
- The set of discrete inputs $\hat{\Psi} = \{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6\}$, where each ψ_i represents a discrete output of the hybrid system $\mathcal{H}_p$.
- The set of transitions $\hat{E} \subseteq \hat{\mathcal{Q}} \times \hat{\mathcal{Q}}$ given by the graph in Figure 6.
- The discrete output function $\hat{\eta}$ defined as the identity for all the edges.

Roughly speaking, assuming ψ_i a discrete output of $\mathcal{H}_p$ and $\hat{q}_i$ the current state of $\mathcal{O}_p$, each state of the observer is designed by grouping together the discrete states q_i which can be reached from all the states $q_i \in \hat{q}_i$ by a transition labeled with ψ_i, and all the discrete states q_i which can be reached from the first ones by an unobservable transition. The discrete outputs of the hybrid model now are used to trigger the transitions of the observer (i.e. they are considered discrete inputs of $\mathcal{O}_p$). For this reasons, the discrete states of the observer are defined as sets of q_i. The graph of the observer $\mathcal{O}_p$ is depicted in Figure 6: the initial state groups the initial states of $\tilde{\mathcal{H}}_p$ (i.e. q_1), and the states that can be reached from q_1 through transitions with unobservable output (i.e. q_2, q_3). As the first observable output (i.e. ψ_2) is available, the associated transition of $\mathcal{O}_p$ (i.e. from $\{q_1, q_2, q_3\}$ to $\{q_4\}$) takes place. Then, each time that a new observable output is generated, a new transition of the observer is triggered according to the graph.

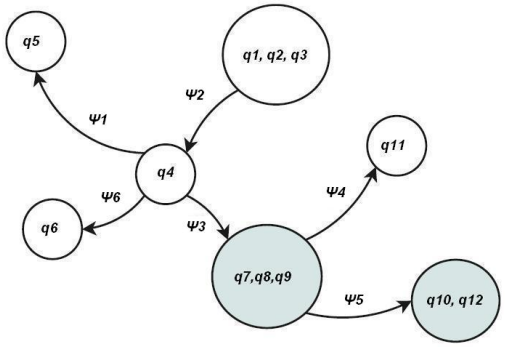

Fig. 6. The observer $\mathcal{O}_p$

It should be noticed that the observer $\mathcal{O}_p$ cannot be used to identify immediately the critical discrete states. In fact, there exists two discrete states of the observer where both safe and unsafe states q_i coexist. However, critical observability can be recovered by generating a set of extra output signals which can be used to distinguish when the system reaches a critical state. These signals can be generated with a non-zero time δ from the

continuous inputs, outputs and dynamics. The generating time of the extra outputs creates a delayed detection of the critical states. This kind of observability is known as $\delta-observability$ (i.e. [3]). The observer $\tilde{\mathcal{O}}_p$ defined after the generation of the extra-output is able to discriminate the critical states with a delay δ which has to be acceptable. $\tilde{\mathcal{O}}_p$ is shown in Figure 7: within this graph, the new transitions triggered by the extra output signal (i.e. from $\{q_7, q_8, q_9\}$ to $\{q_8, q_9\}$ and $\{q_{10}, q_{12}\}$ to $\{q_{10}\}$) allows to discriminate the unsafe states.

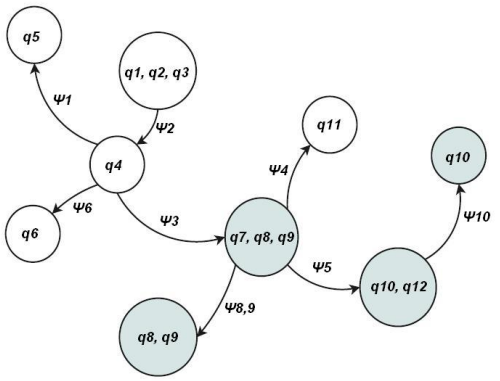

Fig. 7. The observer $\tilde{\mathcal{O}}_p$ with delay δ. New outputs are $\psi_{8,9}$ and ψ_{10}

V. Conclusion

In this paper the hybrid system framework for safety modelling in air traffic management applications has been discussed. The need to develop new sophisticated modelling methodologies originates from new challenges in safety and from the increasing of inherent complexity in the airborne procedures. A specific procedure, the ASEP-ITP, has been investigated to show how this framework can be used to represent a complex multi-agent application in which a wide set of possible abnormal scenarios may happen. In the aviation context, possible catastrophic events can take place due to an error of a single agent involved in the procedure. It has been shown how the hybrid system framework allows the description and the detection of these errors and the understanding of their effects on the evolution of the procedure. The observers which have been proposed here will allow to perform a formal safety analysis, which investigates unforeseen circumstances originated by the interaction of the hybrid agents.

Acknowledgments

This work was partially supported by European Commission under STREP project n.TREN/07/FP6AE/S07.71574/037180 IFLY. It was carried out within the Erasmus Student Placement program, involving the College of Engineering, Center of Excellence DEWS, of University of L'Aquila (Italy) and DSNA-DTI-R&D of Toulouse (France). The authors are grateful to Pascal Lezaud, Thierry Miquel (DSNA-DTI-R&D), Maria Domenica Di Benedetto and Alessandro D'Innocenzo (Center of Excellence DEWS) for their support and suggestions.

References

[1] "D6.1b Qualitative Risk Assessment for ASEP-ITP", ASSTAR Projects, 01 February 2007 v.1.0
[2] "In-Trail Procedure in Procedural Airspace (ATSA-ITP) Application Description", Package I Requirements Focus Group, 21 June 2007 v8.0
[3] A. D'Innocenzo, PhD november 2006, "Observability and Temporal Properties of Hybrid Systems: Analysis and Verification"
[4] R. Alur, T.A. Henzinger, G. Laferriere and G.J. Pappas, "Discrete Abstractions of Hybrid Systems", Proceedings of the IEEE, vol. 88, NO. 7, July 2000
[5] A. Dijkstra, "Resilience Engineering and Safety Management Systems in Aviation", KLM Royal Dutch Airlines / TU Delft
[6] E. Hollnagel, O. Goteman, "The Functional Resonance Accident Model"
[7] E. De Santis, M.D. Di Benedetto, S. Di Gennaro, G. Pola, "Hybrid observer design methodology", Public deliverable D7.2, project IST-2001-32460 HYBRIDGE, August 19,2003, http://www.nlr.nl/public/hosted-sites/hybridge
[8] M. Oishi,I. Hwang,C. Tomlin, "Immediate Observability of Discrete Event Systems with Application to User-Interface Design", Proceedings of the 42nd IEEE conference on decision and control, Maui, Hawaii, USA, pag. 2665-2672, 2003.
[9] M.D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, "Error Detection Within a Specific Time Horizon", public delivarable D7.4, project IST-2001-32460 HYBRIDGE, January 26,2005, http://www.nlr.nl/public/hosted-sites/hybridge
[10] M. D. Di Benedetto, S. Di Gennaro, A. DInnocenzo, "Situation Awareness Error Detection" , Public Deliverable D7.3, Project IST200132460 HYBRIDGE, August 18, 2004, http://www.nlr.nl/public/hostedsites/hybridge.
[11] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, A. L. SangiovanniVincentelli, "Design of Observers for Hybrid Systems", In Claire J. Tomlin and Mark R. Greenstreet, Editors, Hybrid Systems: Computation and Control, Vol. 2289 of Lecture Notes in Computer Science, pp. 7689, Springer-Verlag, Berlin Heidelberg New York, 2002.