CRITICAL STATES DETECTION WITH BOUNDED PROBABILITY OF FALSE ALARM AND APPLICATION TO AIR TRAFFIC MANAGEMENT [1]

M.D. Di Benedetto [*] , S. Di Gennaro [*]
and A. D'Innocenzo [*]

[*] *Department of Electrical and Information Engineering*
and Center of Excellence DEWS, University of L'Aquila.
E.mail: {dibenede, digennar, adinnoce}@ing.univaq.it

Abstract: The analysis of error propagation in an Air Traffic Management (*ATM*) environment is addressed. The theory of Hybrid Systems is used to model the error evolution, an observability problem for a Markov Chain with discrete output symbols associated to the transitions is stated, and a runtime observer is proposed for estimating the probability of a given discrete state to be active. Sufficient conditions are given for characterizing the decidability of the addressed observability problem. The results are related to previous works on location observability of deterministic hybrid systems, and are used to analyze an *ATM* case study, the "*clearance to change the flight plan*".

Keywords: Failure Detection, Markov Chains, Air Traffic Management

1. INTRODUCTION

Hybrid systems are a powerful tool for the analysis and control of Air Traffic Management (*ATM*) systems, as shown in the IST European Project HYBRIDGE (see http://www.nlr.nl/public/hosted–sites/hybridge). Each agent, in an *ATM* environment, executes a sequence of operations that may be characterized by different dynamics (Di Benedetto *et al.*, 2005): this is a typical hybrid context. Moreover, since we are dealing with human agents, the behavior is non–deterministic. The non–determinism of human agents is mainly due to *Situation Awareness*, which is defined in (Endsley, 1995), (Stroeve *et al.*, 2003) as "*the perception of elements in the environment, the comprehension of their meaning, and the projection of their status in the near future*". *Situation Awareness* may be wrong for wrong perception of relevant information, wrong interpretation of perceived information, or wrong prediction of a future state and propagation of error due to agents communication. Moreover, statistic data retrieved by the analysis of real cases of *ATM* procedures may be used to define specific error probability in *ATM* operations, thus it is reasonable to introduce a stochastic framework to analyze error propagations. In the context of error detection analysis, partially observable discrete event systems have been extensively studied in fault detection and supervisory control problems. (Yoo and Lafortune, 2001) analyze the diagnosability of partially observable discrete event systems, and propose a polynomial verification method. (Hadjicostis, 2002) discusses a probabilistic methodology for detecting functional changes in the state transition mechanism of a deterministic finite-state machine (FSM). Results are achieved by computing the deviation between the expected observations and the actual measurements, assuming to know an appropriate statistical characterization of the FSM input. In (Kennedy *et al.*, 1987) a decision feedback equalizer (DFE) operating on a noisy channel is considered, and it is shown how the results concerning a noiseless channel can be extended to yield tight bounds on the stationary error probability performance for the noisy case. Similar approaches were developed in (Aghasaryan *et al.*, 1997; Boubour *et al.*, 1997) for Petri nets. Observability of hybrid systems has been also analyzed in (Balluchi *et al.*, 2002), where a definition of observability of the current state (*current location observability*) has been provided and a procedure for the construction of an observer of the discrete and continuous states is proposed, and in (D'Innocenzo *et al.*, 2006), where *current location observability* of hybrid automata has been studied.

[1] This work was partially supported by European Commission under Project IST NoE HyCON contract n. 511368.

The above definitions of diagnosability and observability do not require a real time state estimation, while in safety-critical applications such as *ATM*, we need to determine the actual state of the system immediately, as a delay can lead to unsafe or even catastrophic behavior of the system. For this reason, we focus here on the concept of observability in prescribed time horizon, and we introduce a stochastic framework to model and test *Situation Awareness* error evolution in *ATM* operations. In Section 2, we define a class of stochastic Hybrid Systems. In Section 3, we propose a definition of observability with bounded probability of false alarm for this class of systems. We propose a design method for a runtime estimator of the discrete state of $\mathcal{S}$ on the basis of the measured outputs, and we give conditions for the system to be observable. In Section 4, we state sufficient conditions such that observability is decidable. In Section 5, we relate our results to previous works on location observability of deterministic hybrid systems (De Santis *et al.*, 2005). In Section 6 we present a case study, the *Clearance to change the flight plan*, where the developed methodologies are used to yield a conditioned probability distribution of the *SA* error evolution. Section 6 offers conclusions and tips for further work.

2. DEFINITIONS AND SETTING

We define a Markov Hybrid System as a tuple $\mathcal{S} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta, \Pi, \Pi_0)$ where:

- $Q = q_1, \cdots, q_N$ is the discrete state set;
- X is the continuous state space;
- Q_0 is the set of initial discrete states;
- X_0 is the set of initial continuous states;
- U is the continuous input space;
- Y is the continuous output space;
- S_q associates linear continuous dynamics A_q, B_q, C_q to each discrete state $q \in Q$;
- Σ is the finite set of input symbols;
- $E \subseteq Q \times \Sigma \times Q$ is a collection of edges;
- Ψ is the finite set of output symbols;
- η: $E \rightarrow \Psi$ is the output function;
- Π is a transition probability matrix with $\Pi_{ij} = \mathcal{P}[q(k+1) = q_j \mid q(k) = q_i]$ for each k;
- Π_0 is an initial probability distribution $(\mathcal{P}[q(0) = q_1] \cdots \mathcal{P}[q(0) = q_N])$, where $\Pi_{0i} = 0$ if $q_i \notin Q_0$.

A Markov Hybrid System is similar to a Hybrid Markov chain as proposed in (Shi *et al.*, 2004). However, in our model no guard functions are considered, and we do not assume that the embedded Markov Chain is irreducible and positive recurrent.

To define the executions of $\mathcal{S}$, we introduce a hybrid time basis $\tau = \{I_k\}_{k\geq 0} \in \mathcal{T}$ as a finite or infinite sequence of intervals $I_k = [t_k, t'_k]$ such that (Lygeros *et al.*, 1999)

(1) I_k is closed if τ is infinite; I_k might be right–open if it is the last interval of a finite sequence τ;
(2) $t_k \leq t'_k$ for all k and $t'_{k-1} \leq t_k$ for $k > 0$.

The cardinality $|\tau|$ of the hybrid time basis is the number of intervals I_k in τ.

An execution of $\mathcal{S}$ is a collection $\chi = (\tau, x, q)$, with x, q satisfying the continuous and discrete dynamics of $\mathcal{S}$. A string $\rho = q_0, \cdots, q_s$ is an execution of the discrete state q of $\mathcal{S}$ with a finite number of transitions $|\rho| - 1 = s$ if $q_0 \in Q_0$ and $\forall I_k \in \{I_1, \cdots, I_s\}, (q_{k-1}, q_k) \in E$. The discrete state execution is ruled by a discrete time Markov chain.

Let $\Upsilon(Q_0)$ be the set of all executions ρ of the discrete state of $\mathcal{S}$ with a finite number of transitions. Given $q \in Q$, let $\Upsilon_q(Q_0)$ be the set of all executions $\rho \in \Upsilon(Q_0)$ such that the last visited state is $q_s = q$. We associate to each execution ρ the observed output as the string $p = P(\rho) = \psi_1 \cdots \psi_s$ where $\psi_k = \eta(q(I_{k-1}), q(I_k))$ for $k = 1, \cdots, s$. We define $\mathcal{L}(\mathcal{S}) = \{P(\rho) \mid \rho \in \Upsilon(Q_0)\}$ the set of output strings that can be generated by all executions of the system $\mathcal{S}$. Given an output string $p = \psi_1 \cdots \psi_s$, we define

$$Reach_{\mathcal{S}}(Q_0, p) := \{q \in Q \mid \exists \rho \in \Upsilon_q(Q_0), P(\rho) = p\}$$

the set of all states that can be reached from an initial state in Q_0 and such that the observed output string is p.

Let $\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta)$ be a Hybrid System defined by the same tuple of $\mathcal{S}$, except for the stochastic matrices Π and Π_0. The space of all executions of $\mathcal{S}$ and that of $\mathcal{H}$ coincide. However, the discrete execution is non deterministic on $\mathcal{H}$, while on $\mathcal{S}$ it is subtended by a probability space, denoted $(\Omega, \mathcal{F}, \mathcal{P})$, on which the stationary Markov chain $q(I_0), q(I_1), q(I_2), \cdots$ is defined. Ω is the space Υ of all executions ρ of the discrete space, and $\mathcal{F}$ the associated sigma–algebra. $\mathcal{P}$ is uniquely defined by the transition probability matrix Π and the initial probability distribution Π_0. Let $\pi_i(I_k) \colon = \mathcal{P}[q(I_k) = q_i]$ and $\pi(I_{k+1}) = \Pi^T \pi(I_k)$ the corresponding dynamics. We now introduce a well known formalism that will be necessary in the following sections:

Let a Markov Hybrid System $\mathcal{S} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta, \Pi, \Pi_0)$ and the subsets $Q' \subset Q$, $E' \subset E \cap (Q' \times Q')$ be given; $\mathcal{S}' = (Q' \times X, Q'_0 \times X_0, U, Y, S_q, \Sigma', E', \Psi', \eta', \Pi', \Pi'_0)$ is the subsystem induced by (Q', E') on S, where (Π', Π'_0) are normalized stochastic matrices.

3. P–OBSERVABILITY OF A DISCRETE STATE

In this section, we propose a definition of observability for a Markov Hybrid System, with respect to a given discrete state. We then propose a constructive procedure for an estimator of the discrete state and a verification procedure for observability. Finally, give conditions such that P–Observability is decidable.

Given a Markov Hybrid System $\mathcal{S}$, our goal is to use the discrete output string to compute the probability distribution of the current discrete state conditioned to a subset of trajectories, namely all the trajectories whose output is the measured output. Consider the probability space $(\Omega, \mathcal{F}, \mathcal{P})$. When an output string $p = \psi_1 \cdots \psi_s$ is generated up to time t_s, it is possible to define the set $\mathcal{G}(p) \subseteq \Omega$ of executions $\rho \in \Upsilon(Q_0)$ such that $P(\rho) = p$. $\mathcal{G}(p)$ is given by $\mathcal{G}_k(p)$ for $k = s$, where

$$\mathcal{G}_0(p) = \Omega$$

$$\mathcal{G}_k(p) = \mathcal{G}_{k-1}(p) \cap \left(\bigcup_{q \in Reach_{\mathcal{S}}(Q_0, p|_k)} \Upsilon_q(Q_0) \right)$$

where $p\,|_k = \psi_1 \cdots \psi_k$ is the truncation of p up to time k. Note that $\mathcal{G}(\epsilon) = \varOmega$ and $\mathcal{G}(p\,|_k) = \mathcal{G}_k(p)$. Let us define

$$\begin{aligned}\mathcal{P}[q(I_{|p|}) = q_i \mid p\,] \colon &= \mathcal{P}[\rho \in \varUpsilon_{q_i}(Q_0) \mid P(\rho) = p\,] = \\ &= \mathcal{P}[q(I_{|p|}) = q_i \mid \mathcal{G}(p)]\end{aligned}$$

and let $q_c \in Q$ be a given critical state of $\mathcal{S}$, namely a discrete state associated to a behavior of the system which may lead to unsafe situations. We want to construct an observer of a critical state with the property that it always detects if the current state of $\mathcal{S}$ is q_c, and such that the probability that detection of q_c is a false alarm is bounded. Let $P \in [0, 1]$ be the maximal probability of false alarm we accept to tolerate. We can formalize the property that such an observer exists by the following definition:

Definition 1. Given a Markov Hybrid System $\mathcal{S}$, a discrete state $q_c \in Q$ is P–Observable (observable with probability of false alarm P) if $\forall p \in \mathcal{L}(\mathcal{S})$

$$\mathcal{P}[q(I_{|p|}) = q_c \mid \mathcal{G}(p)] \in \{0\} \cup [1 - P, 1].$$

This condition implies that, given the measured output of $\mathcal{S}$, either we are sure that we are not in a critical state (thus we don't have to worry) or the probability that the current state is critical is very high, and it is reasonable to give an alarm signal. Namely, if a discrete state q_c of $\mathcal{O}$ is P–Observable, we guarantee that it is always possible to detect if the current state is q_c, with a probability of generating a false alarm less than P. We obtain the limit case (0–Observability) when the information given by the output of the system is rich enough that $\mathcal{P}[q(I_{|p|}) = q_c \mid \mathcal{G}(p)]$ assumes only the values 1 or 0 for all $p \in \mathcal{L}(\mathcal{S})$, that is we know at each time instant with probability 1 if the current state is q_c or not.

We propose now a method for constructing a system whose input is the discrete output string $p \in \mathcal{L}(\mathcal{S})$, and whose output is the probability $\mathcal{P}[q(I_{|p|}) = q_i \mid p\,], \forall i = 1 \cdots N$. Note that such system uses the only discrete output of $\mathcal{S}$ to estimate the current discrete state. Consider a hybrid system $\mathcal{O} = (\hat{Q} \times \hat{X}, \hat{q}_0 \times \hat{x}_0, \hat{U}, \hat{Y}, \hat{S}_{\hat{q}}, \hat{\Sigma}, \hat{E}, \hat{R})$ such that:

- $\hat{Q} \subseteq 2^Q$ is the set of discrete states;
- $\hat{X} = [0, 1]^N$ is the continuous state space, and $\hat{\pi} = [\hat{\pi}_1, \hat{\pi}_2, \cdots, \hat{\pi}_N]$ is the continuous state;
- $\hat{q}_0 = Q_0 \subseteq 2^Q$ is the initial discrete state of $\mathcal{O}$;
- $\hat{x}_0 = \varPi_0$ is the initial continuous state of $\mathcal{O}$, namely the initial probability distribution of each discrete state of $\mathcal{S}$;
- $\hat{U} = \varnothing$ is the continuous input space;
- $\hat{Y} = \hat{X}$ is the continuous output space;
- $\hat{S}_{\hat{q}}$ is such that $A_{\hat{q}} = B_{\hat{q}} = \mathbf{0}, C_{\hat{q}} = \mathbf{I}\ \forall \hat{q} \in \hat{Q}$;
- $\hat{\Sigma} = \varPsi$ is the set of input symbols, namely the set of output symbols of $\mathcal{S}$;
- $\hat{E} = \hat{Q} \times \hat{\Sigma} \times \hat{Q}$ is the set of edges associated to an input symbol;
- $\hat{R} : \hat{E} \times \hat{X} \to \hat{X}$ is a deterministic non-linear reset function of the continuous state $\hat{\pi}$.

The discrete layer of $\mathcal{O}$ may be constructed as in (Di Benedetto *et al.*, 2005). Given an output string $p \in \mathcal{L}(\mathcal{S})$, the associated hybrid execution of $\mathcal{O}$ is unique ($\mathcal{O}$ is deterministic), and by construction of $\mathcal{O}$ $\hat{q}(I_{|p|}) = \mathit{Reach}_{\mathcal{S}}(Q_0, p) \subseteq 2^Q$ is the set of states of Q that may be active in the time interval $I_{|p|}$ accordingly to the observed output p. Note that given any execution of $\mathcal{S}$ and the associated execution of $\mathcal{O}$, the associated hybrid time bases $\tau_{\mathcal{H}}$ and $\tau_{\mathcal{O}}$ coincide.

Let us define the dynamics of the continuous state $\hat{\pi}_i(t)$ of $\mathcal{O}$. Note that, since $\hat{\pi}(t)$ is piecewise constant for each interval $I_k = [t_k, t_{k+1})$ and is only modified by reset functions, we refer to $\hat{\pi}(I_k)$ as the value on such intervals. The reset function $\hat{R}(\hat{e}, \hat{\pi})$ for each $(\hat{e}, \hat{\pi}) \in \hat{E} \times \hat{X}$ is defined in (Di Benedetto *et al.*, 2005), and the following is proved:

Proposition 1. (Di Benedetto *et al.*, 2005) Given a system S and the associated system O. Then, $\hat{\pi}_i(I_{|p|}) = \mathcal{P}[q(I_{|p|}) = q_i \mid \mathcal{G}(p)]$, $\forall i = 1 \cdots N, \forall p \in \mathcal{L}(\mathcal{S})$.

Remark 1. Let $\hat{Q}_c = \{\hat{q} \in \hat{Q} \mid q_c \in \hat{q} \wedge |\hat{q}| > 1\}$: a discrete state q_i of a Markov Hybrid System $\mathcal{S}$ is P–Observable if the reach set of the hybrid state $(\hat{q}, \hat{\pi})$ of $\mathcal{O}$ has empty intersection with the set $\hat{Q}_c \times \{\hat{\pi}_i \in (0, 1 - P)\}$.

For all proofs of this paper the reader is referred to (Di Benedetto *et al.*, 2006). We will now characterize decidability of the P–Observability problem for a Markov Hybrid System $\mathcal{S}$. We define the set $\mathcal{K}_{q_c}(\mathcal{S}) = \{p \in \mathcal{L}(\mathcal{S}) \mid q_c \in \mathit{Reach}_{\mathcal{S}}(Q_0, p) \wedge |\mathit{Reach}_{\mathcal{S}}(Q_0, p)| > 1\}$, namely the set of *bad output strings* that yield q_c indistinguishable from some other state in Q. Moreover, let $\mathcal{L}_{\hat{Q}_f}(\mathcal{O})$ be the language accepted by a non-deterministic finite automaton (*NFA*) with the same discrete topological structure as $\mathcal{O}$ and such that the set of final states is $\hat{Q}_f$.

Lemma 1. The following statements hold:

(i) $\mathcal{L}(\mathcal{S})$ is a regular language;

(ii) $\mathcal{K}_{q_c}(\mathcal{S}) = \mathcal{L}_{\hat{Q}_c}(\mathcal{O}) = \bigcup_{\hat{q} \in \hat{Q}_c} \mathcal{L}_{\hat{q}}(\mathcal{O})$

(iii) $\mathcal{K}_{q_c}(\mathcal{S})$ is a regular language, and $\mathcal{K}_{q_c}(\mathcal{S}) \subset \mathcal{L}(\mathcal{S})$.

Proposition 2. Given a Markov Hybrid System $\mathcal{S}$, a discrete state $q_c \in Q$ is P–Observable (observable with probability of false alarm P) if $\forall p \in \mathcal{K}_{q_c}(\mathcal{S})$, $\mathcal{P}[q(I_{|p|}) = q_c \mid p\,] \in \{0\} \cup [1 - P, 1]$.

Let $\hat{q} = \{q_1, \cdots, q_m, q_{m+1}\} \in \hat{Q}_c$, where $q_c = q_{m+1}$ and $m \geq 1$ by definition of $\hat{Q}_c$. Given the output string p, let us define:

$$\theta(Q_0, q, p) \colon = \sum_{\substack{\rho \in \varUpsilon_q(Q_0) \\ P(\rho) = p}} \mathcal{P}[q(I_0) = \rho_0] \cdot \\ \cdot \left(\prod_{k=0}^{|p|} \mathcal{P}[q(I_{k+1}) = \rho_{k+1} \mid q(I_k) = \rho_k, \psi_k] \right) \quad (1)$$

where $\rho = \rho_0 \cdots \rho_{|p|+1}$. Note that 1 implies

$$\mathcal{P}[q(I_{|p|}) = q_c \mid p\ ] = \frac{\theta(Q_0, q_c, p)}{\sum\limits_{i=1}^{m+1} \theta(Q_0, q_i, p)} \qquad (2)$$

Proposition 3. A state q_c is P–Observable for a system $\mathcal{S}$ if and only if $\forall \hat{q} \in \hat{Q}_c$ and $\forall p \in \mathcal{L}_{\hat{q}}(\mathcal{O})$ the following holds:

$$\theta_c(p) \colon = \frac{\theta(Q_0, q_c, p)}{\sum\limits_{i=1}^{m} \theta(Q_0, q_i, p)} \geq \frac{1-P}{P}. \qquad (3)$$

If the cardinality of the language $\mathcal{L}_{q_c}(\mathcal{S})$ is finite, the P–Observability problem is decidable. If not, the following theorem gives sufficient conditions on the language $\mathcal{K}_{q_c}(\mathcal{S})$ to achieve decidability of the P–Observability problem.

Theorem 1. Given a Markov Hybrid System $\mathcal{S}$, let $A_{\hat{q}}$ be the regular expression that generates $\mathcal{L}_{\hat{q}}(\mathcal{O})$ for $\hat{q} \in \hat{Q}$. If $A_{\hat{q}}$ can be expressed in the form $A_1 + \cdots + A_M$ for each $\hat{q} \in \hat{Q}_c$, where $A_i = a_{i1}a_{i2}\cdots a_{in_i}$ and $a_{ij} \in \{\sigma, \sigma^*, \sigma + \sigma'\}$, $\sigma, \sigma' \in \Sigma$, then P–Observability of $\mathcal{S}$ is decidable.

4. P–OBSERVABILITY FOR $P = 0$

In this section, we introduce an equivalence relation between P–Observability of $\mathcal{S}$ and critical observability (De Santis *et al.*, 2005),(Di Benedetto *et al.*, 2005) of $\mathcal{H}$. More precisely, we prove that, given a system $\mathcal{S}$, the P–Observability conditions for $P = 0$ on the associated observer $\mathcal{O}_{\mathcal{S}}$ are equivalent to the critical observability conditions (De Santis *et al.*, 2005) on the associated observer $\mathcal{O}_{\mathcal{H}}$. Note that $\mathcal{O}_{\mathcal{S}}$ and $\mathcal{O}_{\mathcal{H}}$ have the same discrete dynamics, and therefore the same topological structure. We first recall the definition given in (De Santis *et al.*, 2005) for a non-deterministic hybrid system $\mathcal{H}$ w.r.t. a discrete state $q_c \in Q$:

Definition 2. (De Santis *et al.*, 2005) A hybrid system $\mathcal{H}$ is critically location observable w.r.t. a discrete state $q_c \in Q$ (q_c–critically location observable) if, for any initial state $q_0 \in Q_0$, the current state $q(k)$ can be detected from the output string p whenever $q(k) = q_c$.

Proposition 4. (De Santis *et al.*, 2005) A hybrid system $\mathcal{H}$ is q_c–critically location observable if and only if, for each discrete state $\hat{q}$ of the associated observer $\mathcal{O}$ such that $q_c \in \hat{q}$, then $|\hat{q}| = 1$.

We can now state the following:

Proposition 5. Given the systems $\mathcal{H}$ and $\mathcal{S}$, and the corresponding observers $O_{\mathcal{H}}$ and $O_{\mathcal{S}}$, the following are equivalent:

(1) q_c is P–Observable with $P = 0$ for $\mathcal{S}$;
(2) $\mathcal{H}$ is q_c–critically location observable.

5. CASE STUDY: CLEARANCE TO CHANGE THE FLIGHT PLAN

A Clearance to Change the Flight Plan involves a pilot of a flying aircraft and an air traffic controller. We assume that the procedure is started by a decision of the controller because of a conflict resolution. We describe now the agents involved and the specific behavior of each of them:

The **Flight Management System** (*FMS*) is a technical system that holds the flight plan, modeled as a list of positions s_i and an arrival times t_i. The *FMS* is configured by the *PF*, and controls the aircraft direction, speed and flight mode.The **Flight Data Processing System** (*FDPS*) is a system containing the flight plan, and is reconfigured by the controller. The **Aircraft** (*AC*) is totally controlled by the *FMS*. The **Pilot flying** (*PF*) interacts via VHF communication with the Controller, and can change the actual flight plan by re-configuring the *FMS* system. The **Air Traffic Controller** (*CO*) interacts via VHF communication with the *PF* and monitors the aircraft information (position, velocity, altitude, direction, aircraft code etc) on the *FDPS*.

A Clearance to Change the Flight Plan procedure starts when the Controller, to resolve a conflict, decides to ask the pilot to reconfigure the actual flight plan. The interaction between the *CO* and the *PF* may be assumed as a request by the *CO* to the *PF* to reconfigure the *FMS* with a new position and arrival time, and a confirm by the *PF*, who inserts the new data on the *FMS*. The Controller too configures the *FDPS* with the new coordinates. This simple operation may be affected by several errors, which can bring to an erroneous flight plan configuration and therefore to a risk situation. We suppose without loss of generality that the Controller decided for a secure flight plan, and that the *FMS* configuration is executed before the *FDPS* configuration. Furthermore it is assumed that the technical systems are operative, to set the focus on human *Situation Awareness* . The following errors are considered: Communication error, *FMS* configuration error and *FDPS* configuration error. An analysis of the propagation of *Situation Awareness* errors may be done by formalizing a stochastic system whose continuous dynamics are the aircraft dynamics given by the position and the velocity, and whose discrete states are all possible combinations of *Situation Awareness* values of the agents. More precisely, we define the *SA* of each agent involved in the procedure as its awareness of the flight plan. The information flow previously described can cause errors in the propagation of the *SA* among agents. The *Situation Awareness* of each agent may assume one of the following values:

(1) Former flight plan before the decision of the controller (**Old**)
(2) New flight plan decided by the controller (**New**)
(3) Erroneous flight plan due to communication error between ATC and *PF* ($\mathbf{E}_{COM}$)
(4) Erroneous flight plan due to erroneous programming of the *FMS* ($\mathbf{E}_{FMS}$)
(5) Erroneous flight plan due to erroneous programming of the *FDPS* ($\mathbf{E}_{FDPS}$)

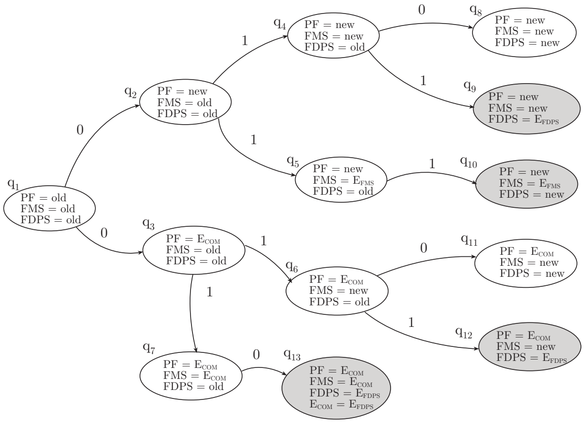

Fig. 1. System $\mathcal{S}$ modeling *Situation Awareness* error evolution

We suppose here, without loss of generality, that a communication error and a *FMS* programming error cannot happen simultaneously. This condition simplifies the number of states and transitions in the error evolution model. We consider the *SA* of the Pilot Flying (SA_{PF}), of the Flight Management System (SA_{FMS}), and of the Flight Data Processing System (SA_{FDPS}).

At the beginning of the Clearance to Change the Flight Plan, $SA_{PF} = SA_{PF} = SA_{PF} =$**Old**. This will be considered as the initial discrete state. Considering possible errors in the *SA* propagation, we can construct an automaton where each discrete state is a different value of the vector $(SA_{PF}, SA_{PF}, SA_{PF})$. The discrete states of the *SA* propagation model are all possible permutations of the considered agents' *SA*. We consider here only the most relevant states of this system, in order to avoid the generation of a too complex model. In such a system, the continuous aircraft dynamic associated with each location may be the same even in case of erroneous *FMS* configuration: e.g. if the correct altitude level given by the Air Traffic controller is 220 and the level understood by the pilot is 240, the rise dynamic of the aircraft may be identical. This means that the use of continuous dynamics to detect the current discrete state (Balluchi *et al.*, 2002) may not always solve the problem. Thus, in order to get extra discrete information from the system, we assume that it is possible to compare the flight plan configured on the *FMS* and the flight plan memorized in the *FDPS*: if they are equal, the system output is 0, otherwise it is 1.

A Clearance to Change the Flight-Plan procedure can be described by the following Markov Hybrid System $\mathcal{S}$, which models the *Situation Awareness* error evolution:

- $Q = \{q_1, \cdots, q_{13}\}$ is the set of discrete states (See Figure 1);
- $X = \mathbb{R}^3 \times \mathbb{R}^3$ is the continuous state space, where $x = (s, v)$ specifies the aircraft position s and the velocity v;
- $Q_0 \times X_0 = \{q_0\} \times \{x_0\}$, where q_1 is associated to the *Situation Awareness* vector $(SA_{PF}, SA_{PF}, SA_{PF}) = (\textbf{Old},\textbf{Old},\textbf{Old})$ and x_0 are the aircraft continuous position and velocity when the Clearance to Change the Flight Plan procedure starts;
- U is the space of the continuous input control u on the velocity of the aircraft;
- Y is the space of the continuous output (the measure of the position of the aircraft);
- S_q is given by A_q, B_q, C_q:

$$A_q = \begin{bmatrix} 0 & I_3 \\ 0 & 0 \end{bmatrix}, B_q = \begin{bmatrix} 0 \\ I_3 \end{bmatrix}, C_q = [\, I_3 \;\; 0 \,]$$

  $\forall q \in Q$ are the continuous dynamics. The velocity vector v_{q_i} depends on the flight plan configured on the *FMS* and is controlled by u.
- $\Sigma = \{\sigma\}$ is a discrete disturbance event that triggers the actions of the agents.
- $\Psi = \{0, 1, \varepsilon\}$ where ε is the unobservable output, 0 indicates that the flight plan memorized in the *FMS* is equal to the flight plan memorized on the *FDPS* ($SA_{FMS} = SA_{FDPS}$), and 1 indicates that they are not equal ($SA_{FMS} \neq SA_{FDPS}$); *SA* stays for *Situation Awareness.*
- E, η are defined according to the automaton in Figure 1;
- Π is the transition probability matrix defined according to ATM statistics, which are usually estimated by airlines companies and ATM research centers. In this analysis, we do not assign numerical values to Π_{ij} since our aim here is to illustrate how the methodology proposed in the previous section can be applied to our case study.
- $\Pi_0 = [1 \;\; 0 \; \cdots \; 0]^T$.

The construction procedure previously described leads to a system $\mathcal{O}$, that shows that the discrete output obtained comparing the FMS and the FDPS data is not sufficient to achieve 0–Observability of the discrete state q_{13} of $\mathcal{S}$, since it is indistinguishable by q_8 and q_{11}. Therefore, additional discrete outputs must be introduced. Finding the set of extra discrete outputs necessary to obtain 0–Observability is a combinatorial problem on the set of edges E of the system $\mathcal{S}$, and may be trivially solved by adding all possible combinations of additional outputs to the set E, and verifying 0–Observability conditions on the system with the new outputs. To obtain P–Observability, a similar procedure can be followed. Since P–Observability conditions are weaker than deterministic critical observability conditions, the number of necessary number of additional outputs would be lower.

In the particular example considered, suppose $\rho = q_1, q_3, q_6, q_{11}$ be the execution of $\mathcal{S}$, and $p = P(\rho) = 010$ the associated output string. The discrete state of the system $\mathcal{O}$ is steered by p to $\hat{q}(I_3) = \{q_8, q_{11}, q_{13}\}$. Since the value Π_{13} (communication error probability, transition from q_1 to q_3) is certainly very low, P–Observability does not hold for a reasonable value of P. Note that the maximal probability of false alarm that can be accepted for fault detection in an ATM procedure is a design constraint. Thus, we have to add new output $\psi_{E_{COM}}$ to the transition (q_1, q_3). To generate the output $\psi_{E_{COM}}$, since the VHF speech communication cannot be measured, it is necessary to change the Clearance to Change the Flight Plan procedure, introducing a protocol for the flight plan data transmission, such that an error in the data transfer can be detected.

By adding further output symbols as done for $\psi_{E_{COM}}$, it is easy to see that 0–Observability of q_{13} is achievable by adding the discrete outputs $\psi_{E_{COM}} = \eta((q_1, q_3))$, $\psi_{E_{FMS}} = \eta((q_2, q_5))$ and

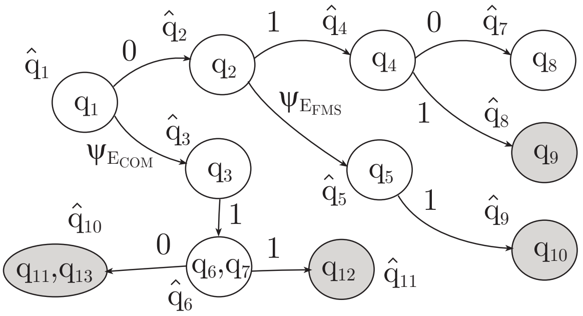

Fig. 2. System $\mathcal{O}'$ constructed from $\mathcal{H}$ with new output symbols

$\psi_{E_{FDPS}} = \eta((q_4, q_9)) = \eta((q_6, q_{12})) = \eta((q_7, q_{13}))$. However, note that the probability associated to the transition (q_3, q_6) is certainly very low, since it is very unlikely that a pilot wrongly understands a flight plan in the VHF communication and then configures the FDPS with the correct values. Hence, it is easy to see from Figure 2 that, by adding only the discrete outputs $\psi_{E_{COM}}$ and $\psi_{E_{FMS}}$, the critical discrete state q_{13} is P–Observable with a low value of P. This shows that the detection of only two errors out of three yields P–Observability with a low probability P of false alarm.

6. CONCLUSIONS

We showed that estimating and mitigating the probability of SA error in ATM can be supported by observability analysis. We proposed a definition of observability for a class of stochastic hybrid systems. For this class of systems, conditions for checking observability were given, and an algorithm to design an observer was illustrated. The equivalence between the observability notion presented here, with a zero probability of false alarm, and critical observability as defined in (De Santis *et al.*, 2005) was proven. This stochastic framework was then used to analyze error evolution in an ATM example. The framework proposed in this paper can be used for simulating ATM procedures and verifying "observability" - i.e. detectability - of dangerous operations. If the system is not observable with an acceptably low probability of generating a false alarm, the procedure must be changed with the introduction of new system outputs, and the verification procedure can be used on the resulting new system. Future research will focus on the minimization of the set of discrete outputs necessary to obtain P–Observability and on the extension of our results to continuous time Markov Chains.

7. ACKNOWLEDGEMENTS

The third author wishes to thank Rajeev Alur for interesting discussions on Regular Languages.

REFERENCES

Aghasaryan, A., E. Fabre, A. Benveniste, R. Boubour and C. Jard (1997). A petri net approach to fault detection and diagnosis in distributed systems. part ii : extending viterbi algorithm and hmm techniques to petri nets.. *Proceedings of the* 36th *Conference on Decision and Control, San Diego, California, USA* **2289**, 726–731.

Balluchi, A., L. Benvenuti, M.D. Di Benedetto and A.L. Sangiovanni-Vincentelli (2002). Design of observers for hybrid systems. *Hybrid Systems: Computation and Control 2002, Lecture Notes in Computer Science, C.J. Tomlin and M.R. Greensreet, Eds.* **2289**, 76–89.

Boubour, R., C. Jard, A. Aghasaryan, E. Fabre and A. Benveniste (1997). A petri net approach to fault detection and diagnosis in distributed systems. part i: application to telecommunication networks, motivations, and modelling.. *Proceedings of the* 36th *Conference on Decision and Control, San Diego, California, USA* pp. 720–725.

De Santis, E., M.D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo and G. Pola (2005). Critical observability of a class of hybrid systems and application to air traffic management. *To Appear as a Book Chapter to Lecture Notes on Control and Information SciencesSpringer Verlag.*

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

Di Benedetto, M.D., S. Di Gennaro and A. D'Innocenzo (2006). Critical states detection with bounded probability of false alarm and application to air traffic management. Technical Report R.06-86. www.diel.univaq.it/tr/web/web_search_tr.php.

D'Innocenzo, A., M.D. Di Benedetto and S. Di Gennaro (2006). Observability of hybrid automata by abstraction. *Hybrid Systems: Computation and Control 2006, Lecture Notes in Computer Science* **3927**, 169–183.

Endsley, M.R. (1995). Towards a theory of situation awareness in dynamic system. *Human Factors* **37,1**, 32–64.

Hadjicostis, C.N. (2002). Probabilistic fault detection in finite-state machines based on state occupancy measurements. *Proceedings of the* 41st *IEEE Conference on Decision and Control, Las Vegas, Nevada, USA* pp. 3994–3999.

Kennedy, R.A., B.D.0. Anderson and R.R. Bitmead (1987). Tight bounds on the error probabilities of decision feedback equalizers. *IEEE Transactions on communications* **COM-35(10)**, October.

Lygeros, J., C. Tomlin and S. Sastry (1999). Controllers for reachability specications for hybrid systems. *Automatica, Special Issue on Hybrid Systems.*

Shi, L., A. Abate and S. Sastry (2004). Optimal control for a class of stochastic hybrid systems. *Proceedings of the* 43rd *IEEE Conference on Decision and Control, Atlantis, Paradise Island, Bahamas* pp. 1842–1847.

Stroeve, S., H.A.P. Blom and M. Van der Park (2003). Multi-agent situation awareness error evolution in accident risk modelling. *FAA–Eurocontrol, ATM2003.*

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