Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

Error Detection within a Specific Time Horizon and Application to Air Traffic Management

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

Abstract— **We propose a novel concept of observability for hybrid systems, critical observability, for estimating and mitigating the probability of errors in Air Traffic Management. Critical observability refers to states that are characterized by the existence of an evolution that may yield catastrophic situations. Detecting these states is an important element of a safety critical environment and we design a critical observer that we apply to the runway crossing problem. We also present an extension of this theory to a class of stochastic hybrid systems and apply it to a clearance changing the flight plan.**

I. Introduction

In an Air Traffic Management (ATM) closed–loop system with mixed computer–controlled and human–controlled subsystems, recovery from non–nominal situations implies the existence of an outer control loop that has to identify these situations and act accordingly to prevent them to evolve into accidents. 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.

The observer construction method proposed in [1] is based on the notion of K–current–state observability. A 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. However, in some applications, it is necessary to immediately identify those discrete locations – that we may call *critical* – which correspond to dangerous situations. Therefore, a different notion of observability has to be introduced, *critical observability*, which extends the K–current–state observability definition. Critical observability refers to a subset of states of the hybrid system, the critical ones, and we design an observer based on this definition to verify the observability of critical states and to fulfill the objective of fault and error detection in prescribed time horizon. In fact, time delay in fault or error detection and identification is critical and no results are available in the literature on this particular problem for hybrid systems.

A notion similar to critical observability was presented in [12], where a definition of *immediate observability* is introduced. Immediate observability is required for all the states of the system, while here we are looking for milder conditions regarding the observability of only the discrete states marked as "critical". In addition, more than on the analysis of a given system, we are interested in the extra information needed to make the property of critical observability hold, namely on conditions that can be used to synthesize an observer.

This new notion of observability applies well in the case of the runway crossing example because the hybrid system model ends up being critically observable. However, in general, this is not necessarily the case. To overcome this difficulty, we propose an extension of the analysis carried out in a deterministic setting to a stochastic framework. In particular, we introduce a class of stochastic hybrid systems to model and test observability of the Situation Awareness (*SA*) error evolution in ATM [8], [16]. An observer is proposed for estimating the probability of a critical state to be active. The obtained results are related to the observability of deterministic hybrid systems, and are applied to a clearance changing the flight plan.

This paper is organized as follows. In Section II, we formulate the problem and we review results on observability for hybrid systems. In Section III, we introduce the notion of critical observer and we offer conditions under which critical observers can be designed. If those conditions are not satisfied, we propose to use a stochastic analysis for the estimation of the probability of a critical state to be active. We define a class of stochastic hybrid systems, namely a Markov Chain with continuous time dynamics associated with each node. We propose a design method for an estimator of the discrete state of the stochastic hybrid system conditioned to the measured output. In Section IV, we apply these results to two case studies: the runway crossing problem and the clearance changing the flight plan. In the latter, we obtain a probability distribution of the *SA* error evolution. In Section V, we offer some concluding remarks.

II. Basic Definitions and Problem Setting

Consider a hybrid system $\mathcal{H}$ with N locations $q_1, \cdots, q_N$. The continuous dynamics are given by

$$\dot{x} = A_i x + B_i u, \qquad y = C_i x, \qquad i = 1, \cdots, N \tag{1}$$

$A_i \in \mathbb{R}^{n\times n}$, $B_i \in \mathbb{R}^{n\times m}$, $C_i \in \mathbb{R}^{p\times n}$, $x \in X \subseteq \mathbb{R}^n$ the continuous state, $y \in Y \subseteq \mathbb{R}^p$ the continuous output, and $u \in U \subseteq \mathbb{R}^m$ the continuous input. The discrete event dynamics (nondeterministic generator of formal language [15]) are

$$\begin{aligned} q(k+1) &\in \delta(q(k), \sigma(k)) \\ \psi(k+1) &= \eta(q(k), \sigma(k), q(k+1)) \\ \sigma(k) &\in \phi(q(k)) \end{aligned} \tag{2}$$

$k = 0, 1, 2, \cdots$, $q(k) \in Q = \{q_1, \cdots, q_N\}$ the discrete location, $\psi(k) \in \Psi = \{\epsilon, \psi_1, \cdots, \psi_r\}$ the output symbol, with ϵ the null event, $\sigma(k) \in \Sigma = \{\sigma_1, \cdots, \sigma_s\}$ the k^{th}

This work has been partially supported by European Commission under Project HYBRIDGE IST–2001–32460 and IST NoE HyCON contract n. 511 368.

The authors are with the Department of Electrical and Information Engineering, University of L'Aquila, 67040, – Poggio di Roio, L'Aquila, Italy. E.mail: {dibenede, digennar, adinnoce}@ing.univaq.it.

0-7803-9568-9/05/$20.00 ©2005 IEEE

input symbol, which takes place at time t_k and forces the discrete evolution. Moreover,

$$\delta\colon Q \times \Sigma \to 2^Q, \qquad \phi\colon Q \to 2^\Sigma, \qquad \eta\colon Q \times \Sigma \times Q \to \Psi$$

are the transition, the input, and the output functions. The initial state is a state $q_0 \in Q_0 \subseteq Q$. The function ϕ specifies the possible input events σ. The functions δ, η can be extended in the usual way to accept sequences $\sigma_0\sigma_1 \cdots \sigma_{k-1}\sigma_k$ as follows

$$\delta(q, \sigma_0 \cdots \sigma_{k-1}\sigma_k) = \bigcup_{q'} \delta\big(q', \sigma_k\big)$$
$$\eta(q, \sigma_0 \cdots \sigma_{k-1}\sigma_k, q'') = \eta(q, \sigma_0 \cdots \sigma_{k-1}, q')\eta(q', \sigma_k, q'')$$

for $q' \in \delta(q, \sigma_0 \cdots \sigma_{k-1})!$ and $\delta(q', \sigma_k)!$, $\eta(q', \sigma_k, q'')!$ ("!" means that the function is defined). When an input event σ occurs corresponding to a null output ϵ, it is not possible to know from η the occurrence of a transition in $\mathcal{H}$.

The interactions between continuous and discrete dynamics can be modelled by guard and reset functions (see [10] for details). To define correctly the evolution of a hybrid system $\mathcal{H}$, one introduces a hybrid time basis $\tau = \{I_k\} \in \mathcal{T}$ of $\mathcal{H}$ as a finite or infinite sequence of intervals $I_k = [t_k, t'_k]$ such that [10]

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) $t_k \le t'_k$ for all k and $t'_{k-1} \le t_k$ for $k > 0$.

The length of the hybrid time basis is $|\tau|$. An execution χ of $\mathcal{H}$ is a collection $\chi = (\tau, q, x)$, with x, q satisfying the dynamics (1), (2) and their interactions (guard and reset functions).

Given a hybrid system $\mathcal{H}$ and a time basis τ, we suppose that for each state $q \in Q$, there exists a minimum dwell time $\Delta_m(q)$ (namely the minimum time of permanence in a given state q of $\mathcal{H}$) such that $t'_k - t_k \ge \Delta_m(q) > 0$ for all $k \in \big[0, |\tau| - 1\big]$, with $q(k)$ (or $q(I_k)$) the state for $t \in I_k$, $\sigma(k)$ the input at $t = t'_k$, $\psi(k+1)$ the output at $t = t_{k+1}$.

Let a set $Q_c \subseteq Q$ of "critical" states of $\mathcal{H}$ be given, namely a set of states associated to dangerous operations. The problem considered here consists of building a system $\mathcal{O}$ (discrete observer) whose state $\hat{q}$ satisfies $\hat{q}(k) = \{q_c\}$ for all k such that $q(k) = q_c$ and $q_c \in Q_c$, for every execution χ of $\mathcal{H}$.

III. Critical Observers

Various notions of observability have been introduced in the literature for discrete event and hybrid systems (see e.g. [14], [13], [1], [7], [12], [2], [4], [6]). In general, the information given by the discrete output is not sufficient to build an observer for the discrete states of $\mathcal{H}$. The key idea in [1] is to exploit the knowledge coming from the continuous dynamics to create further discrete signals (called "signatures") which provide additional information to discriminate the discrete locations [9], [11]. Clearly, this extra information must be "rich enough" to design an observer.

Following [4], we associate to each state $q \in Q$ an additional output value $\bar{\psi} = h(q) \in \bar{\Psi}$, that is supposed to be generated within the minimum dwell–time $\Delta_m(q)$. In this way, the signature generator dynamics is "hidden" in the delay necessary to compute $\bar{\psi} = h(q)$ and can be neglected. In general, $h\colon Q \to \bar{\Psi}$ cannot be defined for all discrete states of $\mathcal{H}$.

In this section, we first propose an observer design method that exploits the signatures for the determination of critical states. Then, we solve the problem in a probabilistic setting.

A. Basic Observer Construction

We first present a simple procedure to design an observer

$$\mathcal{O} = \Big\{\hat{Q}, \hat{\Psi}, \hat{\delta}, \hat{q}_0, \hat{\phi}, \hat{\eta}\Big\} \tag{3}$$

that gives an estimate of the discrete state of $\mathcal{H}$. The state transition function $\hat{\delta}\colon \hat{Q} \times \hat{\Psi} \to \hat{Q}$, iteratively constructed, is induced by the function δ as follows

$$\hat{\delta}(\hat{q}, \psi) := \Big\{q \in Q \mid q \in \delta(q', \sigma s)! \text{ for } q' \in \hat{q},\ \sigma s \in \Sigma^* \text{ such that } \eta(q', \sigma, q'') = \psi \neq \epsilon \text{ and } \eta(q'', s, q) = \epsilon \cdots \epsilon,\ q'' \in \delta(q', \sigma)\Big\}.$$

Here Σ^* is the set of all possible sequences $\sigma_0\sigma_1 \cdots \sigma_k$, $\hat{\Psi} = \Psi \setminus \{\epsilon\}$ is the set of inputs (the outputs of $\mathcal{H}$), and $\hat{Q} \subset 2^Q$ is the observer state set obtained as the set of states $\hat{q}$ for which $\hat{\delta}(\hat{q}, \psi)!$ for some $\psi \in \hat{\Psi}$. The initial state of the observer is

$$\hat{q}_0 := Q_0 \bigcup \Big\{q \in Q \mid q \in \delta(q_0, s)! \text{ for } q_0 \in Q_0,\ s \in \Sigma^* \text{ such that } \eta(q_0, s, q) = \epsilon \cdots \epsilon\Big\}.$$

The input function $\hat{\phi}\colon \hat{Q} \to 2^{\hat{\Psi}}$ is clearly

$$\hat{\phi}(\hat{q}) := \Big\{\psi \in \hat{\Psi} \mid \hat{\delta}(\hat{q}, \psi)!\Big\}.$$

The output of $\mathcal{O}$ is the current observer state $\hat{q} \in \hat{Q}$, so that the output function $\hat{\eta}\colon \hat{Q} \to \hat{Q}$ is the identity function.

Remark 1. *The observer $\mathcal{O}$ remains in the same state $\hat{q}$ when the events σ with output ϵ occur (see the definitions of $\hat{\delta}$ and $\hat{q}_0$), namely during various subsequent time intervals I_k. Hence, the time basis for the observer has to be redefined merging these time intervals, obtaining a new time basis $\hat{\tau} = \{\hat{I}_j\}$, $j = 0, 1, 2, \cdots$. In general, $\hat{\tau}$ and τ do not coincide.* □

Remark 2. *When $\mathcal{H}$ has null output events ϵ but the time instants t_k of the corresponding transitions are known, ϵ may be viewed as an observable output event $\psi_\epsilon \neq \epsilon$. In this case the time basis $\hat{\tau}$ coincides with τ, and the state $\hat{q}$ of $\mathcal{O}$ could have cardinality greater than 1 (as subset of Q) only because of the non determinism of $\mathcal{H}$.* □

B. Critical Observers

A critical state $q_c \in Q_c$ for $\mathcal{H}$ induces the notion of *critical states $\hat{q}_c$ for the observer $\mathcal{O}$.*

Definition 1. *$\hat{q} \in \hat{Q}$ is critical for $\mathcal{O}$ if $\hat{q} \cap Q_c \neq \emptyset$.* □

Let $\hat{Q}_c$ the set of induced critical states of $\hat{\mathcal{O}}$. By taking into account the information provided by the signatures, critical states $\hat{q}_c \in \hat{Q}_c$ can be partitioned by means of "signatures" $h(\bar{q})$, $\bar{q} \in \hat{q}_c$, with the following refinement

$$\hat{q}_c|_{h(\bar{q})} := \Big\{q \in \hat{q}_c \mid h(q) = h(\bar{q})\Big\} \subseteq \hat{q}_c, \quad \bigcup_{\bar{q} \in \hat{q}} \hat{q}_c|_{h(\bar{q})} = \hat{q}_c. \tag{4}$$

Starting from the observer $\mathcal{O}$, and on the basis of the refinement of the critical states, we define a new system $\hat{\mathcal{O}}$ as follows.

Algorithm 1. *Design $\mathcal{O}$ as in (3).*

1) *Refine each critical state $\hat{q}_c \in \hat{Q}_c$ with the function h as in (4).*
2) *Enlarge $\hat{Q}_c$ to contain those refined states $\hat{q}_c|_{h(\bar{q})}$ containing critical states $q_c \in Q_c$ for $\mathcal{H}$. Redefine $\hat{Q}$.*
3) *Redefine the state transition function $\hat{\delta}$ to consider the transitions in $\mathcal{O}$ from the critical states to their refinements, and from the refinements to the other states of $\hat{Q}_c$, induced by the function δ.*
4) *Redefine $\hat{\Psi}$, $\hat{\phi}$, $\hat{\eta}$ in accordance to the new function $\hat{\delta}$.*

Let $\hat{\mathcal{O}} = \left\{\hat{Q}, \hat{\Psi}, \hat{\delta}, \hat{q}_0, \hat{\phi}, \hat{\eta}\right\}$ be the obtained system. □

When considering the events $\bar{\psi} = h(q)!$ as new input events for $\hat{\mathcal{O}}$, the hybrid time basis $\hat{\tau}$ results to be refined, since some intervals $\hat{I}_j$ may be given by $I_j = I_{1,j} \cup I_{2,j}$, with $I_{1,j} = [t_j, t_j + \rho_j]$, $I_{2,j} = [t_j + \rho_j, t'_j]$, and with $\bar{\psi}$ generated at time $t_j + \rho_j$ (of $I_{2,j}$), where $\rho_j \leq \Delta_m(q)$. If $h(q)$ is not defined, then $\rho_j \geq t'_j - t_j \geq \Delta_m(q)$, i.e. $\hat{I}_j$ is not refined.

The value of $\hat{q}$ for $t \in \hat{I}_j$ may be denoted by $\hat{q}(j)$ or $\hat{q}(\hat{I}_j)$. The system $\hat{\mathcal{O}}$ is a critical observer if it allows the detection of a critical state $q_c \in Q_c$ before $\mathcal{H}$ leaves q_c.

Definition 2. *Given a hybrid system $\mathcal{H}$ and a subset $Q_c \subseteq Q$, let $q(I_k) = q_c \in Q_c$ be a critical state. Consider the time interval $\hat{I}_j = [t_j, t'_j]$ such that $I_k \subseteq \hat{I}_j$. The system $\hat{\mathcal{O}}$ is a* critical observer *for $\mathcal{H}$ with respect to the set of states Q_c if*

$$\hat{q}(\hat{I}_j) = \{q_c\} \qquad or \qquad \hat{q}(\hat{I}_{2,j}) = \{q_c\} \tag{5}$$

with $\hat{I}_j = \hat{I}_{1,j} \cup \hat{I}_{2,j}$, $\hat{I}_{2,j} = [t_j + \rho_j, t'_j]$, $t_j + \rho_j \in I_k$, for every execution χ of $\mathcal{H}$. □

In the first case of (5), I_k and $\hat{I}_j$ have the same initial time (but possibly not the final one).

Remark 3. *In [1] the notion of K–current state observability is considered. It is clear that an observer ensuring the K–current state observability with $K = 0$, or 0–current state observer for short, is also a critical observer since the first case of (5) occurs. On the contrary, a critical observer in general is not a 0–current state observer, and in this sense it generalizes the 0–current state observer.* □

Proposition 1. *The observer (3) is a critical observer for $\mathcal{H}$ if and only if*

$$\hat{Q}_c \subseteq \hat{Q}_1 := \left\{\hat{q} = \{q\},\ \forall q \in Q\right\}.$$ □

Proof. If (3) is a critical observer, the first of (5) holds, and this implies that $\hat{Q}_c \subseteq \hat{Q}_1$. Conversely, if $\hat{Q}_c \subseteq \hat{Q}_1$ then the first of (5) holds, i.e. (3) is a critical observer. □

When the conditions of Proposition 1 do not hold, the system (3) is not a critical observer. The following statement gives a condition under which the system $\hat{\mathcal{O}}$ obtained with Algorithm 1 is a critical observer.

Theorem 1. *$\hat{\mathcal{O}}$ is a critical observer for $\mathcal{H}$ with respect to a set $Q_c \subset Q$ if and only if, for each induced critical state $\hat{q}_c \in \hat{Q}_c$ violating the first of (5),*

$$\left|\hat{q}_c|_{h(\bar{q})}\right| = \begin{cases} 1 & \text{if } \bar{q} \in \hat{q}_c \cap Q_c \\ C \geq 1 & \text{if } \bar{q} \in \hat{q}_c \backslash (\hat{q}_c \cap Q_c) \end{cases} \tag{6}$$

for refinements induced by h. □

Proof. (6) implies the second of (5), and $\hat{\mathcal{O}}$ is critical. Conversely, if $\hat{\mathcal{O}}$ is critical, (5) implies (6). □

According to Theorem 1, the function $h: Q \to \bar{\Psi}$ satisfying (6) is not unique. It is of interest to determine h such that the number of refined states for each $\hat{q}_c \in \hat{Q}_c$ is minimum.

Theorem 2. *Given an observer $\mathcal{O}$ as in (3), Algorithm 1 gives a critical observer $\hat{\mathcal{O}}$ for $\mathcal{H}$ with respect to a set $Q_c \subset Q$ with $|\hat{Q}|$ minimum, if and only if there exists a function $h: Q \to \bar{\Psi}$ such that, for each critical state $\hat{q}_c \in \hat{Q}_c$, (6) holds with*

$$C = \left|q_c \backslash (\hat{q}_c \cap Q_c)\right|.$$ □

Proof. Straightforward. □

C. Stochastic Critical Observer

In this subsection we consider the case where the system $\hat{\mathcal{O}}$ fails to be a critical observer, due to insufficient information coming from the output η of $\mathcal{H}$ and/or from h. In this case, we need to consider a generalization of the previous observer. For this purpose, we assume to know a probabilistic model of the discrete dynamics $\mathcal{H}$. This additional information will allow associating to the states of $\hat{\mathcal{O}}$ a probability distribution, which will yield an estimate of the probability of a given state of $\mathcal{H}$ to be active. This generalization will be given under the assumption that the transition times t_k are known. In this case the time basis $\hat{\tau}$ coincides with τ (Remark 2).

To characterize the stochastic behavior of $\mathcal{H}$, we define a transition probability matrix Π such that

$$\Pi_{ri} := \begin{cases} \mathcal{P}[q(k+1) = q_r \mid q(k) = q_i] & \text{if } q_r \in \delta(q_i, \sigma) \\ 0 & \text{if } q_r \notin \delta(q_i, \sigma) \end{cases}$$

where $\mathcal{P}[q(k+1) = q_r \mid q(k) = q_i]$ is constant for each k and $\sum_{r=1}^{N} \Pi_{ri} = 1$ for each $i = 1, \cdots, N$. We also define an initial probability distribution

$$\pi_0 = \pi(0) = \begin{pmatrix} \mathcal{P}_0[q(0) = q_1] & \cdots & \mathcal{P}_0[q(0) = q_N] \end{pmatrix}^T$$

where $\pi_{0i} = 0$ if $q_i \notin Q_0$ and $\sum_{i=1}^{N} \pi_{0i} = 1$. We say that $\mathcal{S} = (\mathcal{H}, \Pi, \pi_0)$ is a Markov Hybrid System.

The space of all executions of $\mathcal{H}$ and that of $\mathcal{S}$ are the same. However, the discrete execution is non deterministic on $\mathcal{H}$, while on $\mathcal{S}$ it is subtended by a probability space, denoted $(\Omega, \mathcal{F}, \mathcal{P})$ with, as usual, $(\Omega, \mathcal{F})$ a measurable space, Ω the space of all possible discrete trajectories g (defined as sequences of discrete states of $\mathcal{H}$), $\mathcal{F}$ the associated σ–algebra, and $\mathcal{P}$ a probability measure on $\mathcal{F}$, uniquely defined by Π and π_0.

Let $\pi_i(k) := \mathcal{P}[q(k) = q_i]$ and

$$\pi(k+1) = \Pi\, \pi(k).$$

the corresponding dynamics, where $\pi(k)$ is the probability distribution for $t \in I_k$.

We now associate to $\hat{O}$ a piecewise constant continuous state $\hat{\pi} = [\hat{\pi}_1, \hat{\pi}_2, \cdots, \hat{\pi}_N] \in [0,1]^N$. Consider the discrete output string $\psi_1 \cdots \psi_k$ and the associated set $\mathcal{G}_k \subset \Omega$ of discrete trajectories of $\mathcal{H}$ compatible with $\psi_1 \cdots \psi_k$ (i.e. all the discrete trajectories g_i of length $i \geq k+1$ that give raise to $\psi_1 \cdots \psi_k$ if restricted to the time interval $[t_0, t'_k]$). The sequences $\{\mathcal{G}_k\}$, $k \geq 0$ are given by

$$\mathcal{G}_0 = \Omega, \qquad \mathcal{G}_k = \mathcal{G}_{k-1} \cap [q(k) \in \hat{q}(k) = \hat{\delta}(\hat{q}_0, \psi_1 \cdots \psi_k)]$$

where $[q(k) \in \hat{q}(k)] \subset \Omega$ represents the set of all the trajectories of $\mathcal{H}$ compatible with the state $q(k)$ being in $\hat{q}(k)$.

Define $\pi_i(k)$ conditioned to $\psi_1 \cdots \psi_k$ as

$$\mathcal{P}[q(k) = q_i \mid \psi_1 \cdots \psi_k] := \mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]. \quad (7)$$

We determine now an estimate $\hat{\pi}_i(k)$ of (7) as follows. Let $\hat{q}(k) = \hat{\delta}(\hat{q}(k-1), \psi(k))$ and let us compute a function $\hat{R}_{\hat{q}(k-1),\hat{q}(k)}$ such that

$$\hat{\pi}(k) = \hat{R}_{\hat{q}(k-1),\hat{q}(k)}(\hat{\pi}(k-1)). \quad (8)$$

For, we define $\hat{q}'(k-1) \subseteq \hat{q}(k-1)$ as the set of states of $\hat{q}(k-1)$ such that $\psi(k) \in \hat{\phi}(\hat{q}(k)$, we set to 0 the probability for all states in $\hat{q}(k-1) \setminus \hat{q}'(k-1)$, and finally we normalize $\hat{\pi}(k-1)$ to 1, obtaining a vector $\hat{\pi}'(k-1)$. Consider now the sub–graph induced on $\mathcal{S}$ by $\hat{q}(k-1) \cup \hat{q}(k)$ and assign probability 0 to all transitions whose output is not $\psi(k)$, and normalize to 1 the probabilities of the other transitions with output $\psi(k)$, obtaining the probability matrix $\hat{\Pi}$. Then, for all $i = 1, \cdots, N$ set

$$\hat{\pi}_i(k) = \begin{cases} \sum_{r: q_r \in \hat{q}(k-1)} \hat{\Pi}_{ir} \ \hat{\pi}'_r(k-1) & \text{if } q_i \in \hat{q}(k) \\ 0 & \text{if } q_i \notin \hat{q}(k) \end{cases}$$

thus obtaining the function $\hat{R}_{\hat{q}(k-1),\hat{q}(k)}$.

Theorem 3. *For each execution of $\mathcal{S}$ and for $i = 1 \cdots N$*

$$\hat{\pi}_i(k) = \mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]. \quad (9)$$

□

Proof. Let $q_i(k)$ be a compact notation for $q(k) = q_i$. For $k = 0$, $\hat{\pi}(0) = \pi_0$ by construction, so that

$$\hat{\pi}_i(0) = \mathcal{P}[q_i(0)] = \mathcal{P}[q_i(0) \mid \mathcal{G}_0], \qquad i = 1, \cdots, N$$

since $\mathcal{G}_0 = \Omega$. By induction, suppose that (9) holds for $k-1$. By construction, $\hat{\pi}_i(k)$ is given by (8), where the normalization operations (due to the knowledge of the output $\psi(k)$) of $\mathcal{P}[q_i(k-1) \mid \mathcal{G}_{k-1}]$, to consider only the states from which $\psi(k)$ can be generated, and of $\mathcal{P}[q_i(k) \mid q_j(k-1), \mathcal{G}_{k-1}]$, to consider only the transitions with output $\psi(k)$, give

$$\hat{\pi}_i(k) = \sum_{r=1}^{N} \mathcal{P}[q_i(k) \mid q_r(k-1), \mathcal{G}_k] \ \mathcal{P}[q_r(k-1) \mid \mathcal{G}_k]$$

$$= \mathcal{P}[q_i(k) \mid \mathcal{G}_k]$$

for all $i = 1, \cdots, N$. □

IV. Case Studies

A. The Active Runway Crossing System

In this subsection, we consider the runway crossing example described in detail in [6]. Among the agents acting in the system, we consider here the behavior of the pilot of a taking off aircraft (P_t). This agent may have erroneous Situation Awareness (*SA*), i.e. erroneous perception and/or comprehension of elements in the environment, and/or their projection of their status in the near future [8], [16], [3]. Referring to Figure 1 for the discrete dynamics of the hybrid system $\mathcal{H}_{P_t}$ modelling P_t, the pilot initially executes boarding and waits for start up grant by a ground controller C_g (event $\sigma_{1,1}$). He begins taxiing on the airport way AW_1, stops at stopbar S_1 (which controls AW_1) and communicates with the tower controller C_t to obtain take off grant. P_t waits for grant at the stopbar ($\sigma_{1,8}$) or, due to an *SA* error, executes an unauthorized take off ($\sigma_{1,7}$). From C_t the pilot receives the command of taking off immediately ($\sigma_{1,2}$), or to line up and wait ($\sigma_{1,3}$) and then to power up and take off ($\sigma_{1,4}$). After the initial climbing ($\sigma_{1,9}$), P_t confirms that the take off has been completed to C_t. During take off operations, P_t monitors the traffic situation on the runway visually and via VHF communications. If an aircraft, crossing the runway, is observed or in reaction to an emergency braking command C_t, the pilot starts a braking action and so take off is rejected ($\sigma_{1,5}$). An error of the pilot can bring to abort taxiing ($\sigma_{1,6}$). In Figure 1 $\psi_{1,1}$ is the start up confirmation to C_g, $\psi_{1,2}$ is the take off request, $\psi_{1,3}$ is the immediate take off confirmation, $\psi_{1,4}$ is the line–up and wait confirmation, $\psi_{1,5}$ is the take off confirmation, $\psi_{1,6}$ is the emergency braking confirmation, $\psi_{1,7}$ is the airborne confirmation. The outputs corresponding to the errors $\sigma_{1,6}$, $\sigma_{1,7}$ are null.

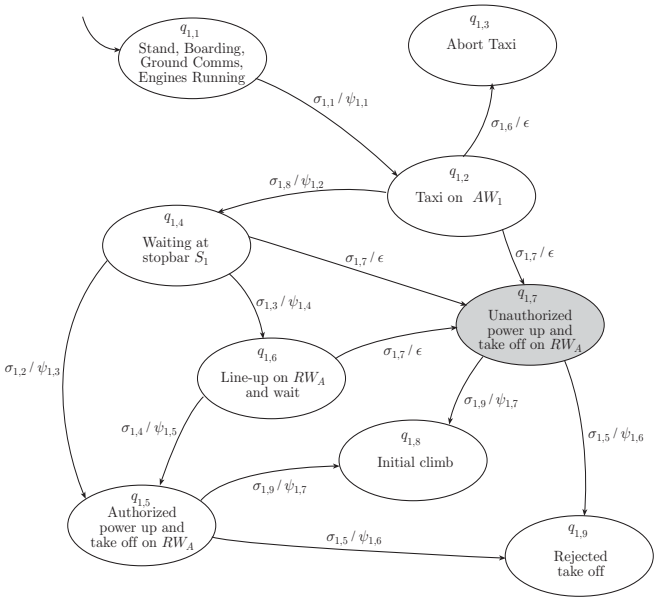

Fig. 1. Hybrid system $\mathcal{H}_{P_t}$ modelling P_t

The observer $\mathcal{O}_{P_t}$ for $\mathcal{H}_{P_t}$ is given in Figure 2. It is clear that $\mathcal{O}_{P_t}$ violates Proposition 1, and hence it is not a critical observer for $\mathcal{H}_{P_t}$. In fact, the induced critical states $\{q_{1,2}, q_{1,3}, q_{1,7}\}$, $\{q_{1,4}, q_{1,7}\}$, $\{q_{1,6}, q_{1,7}\}$ have cardinality

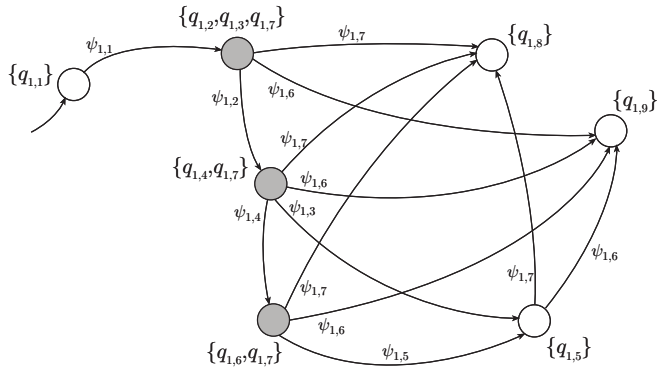

Fig. 2. Observer $\mathcal{O}_{P_t}$

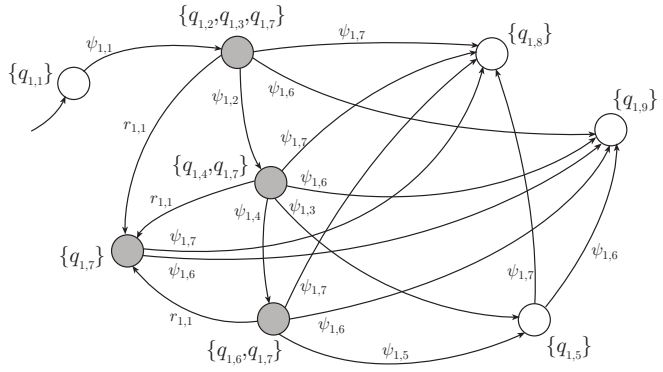

Fig. 3. Critical observer $\hat{\mathcal{O}}_{P_t}$

greater than 1. Theorems 1 or 2 can be used to determine a critical observer for $\mathcal{H}_{P_t}$. In particular if a signature $r_{1,1} = h(q_{1,7})$ is generated to distinguish $q_{1,7}$, one gets the critical observer $\hat{\mathcal{O}}_{P_t}$. Note that even if this model is simpler than reality, the propose method can be nevertheless applied to more complex models (see [4]).

B. The Clearance Changing the Flight–Plan

In this section we consider the ATM procedure consisting of a clearance changing the flight plan. This involves a pilot of a flying aircraft PF and an air traffic controller CO (see [5] for details). This procedure starts when the CO requests via VHF to PF to reconfigure the Flight Management System (FMS), which controls the aircraft direction, speed and flight mode, with a new position and arrival time. The PF inserts the new data on the FMS and gives confirmation to CO, who inserts the new data on the Flight Data Processing System ($FDPS$). This operation may be affected by situation awareness errors, which can bring to an erroneous flight–plan configuration. We consider only errors in VHF communication, FMS configuration and $FDPS$ configuration. The situation awareness of each agent can assume the following values

1) Old flight–plan (*old*);
2) New flight–plan decided by the controller (*new*);
3) Erroneous flight–plan due to VHF communication error (E_{COM});
4) Erroneous flight–plan due to erroneous FMS programming (E_{FMS});
5) Erroneous flight–plan due to erroneous $FDPS$ programming (E_{FDPS});

To simplify the number of states and transitions in the error evolution model, we suppose that a communication error and a FMS programming error can not occur simultaneously.

We consider the *SA* of PF (SA_{PF}), FMS (SA_{FMS}) and $FDPS$ (SA_{FDPS}). At the beginning of the procedure $SA_{PF} = SA_{FMS} = SA_{FDPS} = Old$. This will be considered the initial discrete state. Considering possible *SA* errors, we can construct an automaton where each discrete state is a different value of the *SA* vector of the three considered agents PF, FMS and $FDPS$. The discrete states of the *SA* propagation model are all possible permutations of the *SA* of the considered agents. We consider here only the most relevant states of the system.

In this case, the continuous aircraft dynamics of each location could be equal in case of correct or erroneous FMS configuration. For example, if the correct flight level given by the Air Traffic controller is 220 and the erroneous level understood by the pilot is 240, the rise dynamics of the aircraft can be identical. This means that the use of continuous dynamics for detecting the current discrete state can not solve the problem. Thus, in order to get extra 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 $FDPS$.

The clearance changing the flight–plan procedure can be described by the hybrid system $\mathcal{H}$ whose discrete dynamics are given in Figure 4. The arcs are labelled by the generated discrete outputs 0 (indicating that $SA_{FMS} = SA_{FDPS}$) and 1 (indicating that $SA_{FMS} \neq SA_{FDPS}$). For simplicity, the continuous dynamics are those of a material point moving in the space. The aircraft velocity vector depends on the flight–plan configured on the FMS and is controlled by a continuous input, and the initial position and velocity correspond to the occurrence of the clearance changing the flight–plan.

The construction procedure previously described leads to a system $\mathcal{O}$ as in Figure 5 (in this case $\hat{\mathcal{O}} = \mathcal{O}$). The analysis of the system $\mathcal{O}$ shows that, even if there are no unobservable outputs, $\mathcal{O}$ is not a critical observer for $\mathcal{H}$. More precisely, non–critical states q_4 and q_7 are indistinguishable respectively from critical states q_5, q_6 and q_8, q_9, while states q_{10}, q_{11}, q_{12} are not distinguishable among themselves. In the given example, the only way to distinguish critical states from non–critical ones is the introduction of new discrete outputs in the procedure. In other words, to obtain an automatic error detection in the clearance changing the flight–plan procedure, we need to introduce an automatic data transfer for the flight–plan information, because a VHF communication can not be automatically measured, and even if the FMS and the $FDPS$ data are compared, $\mathcal{O}$ is still not a critical observer.

If we accept a non zero probability of missing the detection of a critical state and/or of giving a false alarm, we can use the stochastic approach. A transition probability matrix Π can be defined according to ATM statistics. In this work it is not important to define the values of Π_{ri}, since the aim is to define a framework to analyze ATM procedures and not to study or solve a particular case. We consider $\pi_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$. Hence, a Markov hybrid

system $\mathcal{S} = (\mathcal{H}, \Pi, \pi_0)$ remains determined. Finally, to $\mathcal{O}$ we associate the continuous state $\hat{\pi}(k) \in [0,1]^N$, with the reset function $\hat{R}$ computed as explained in Section III.C

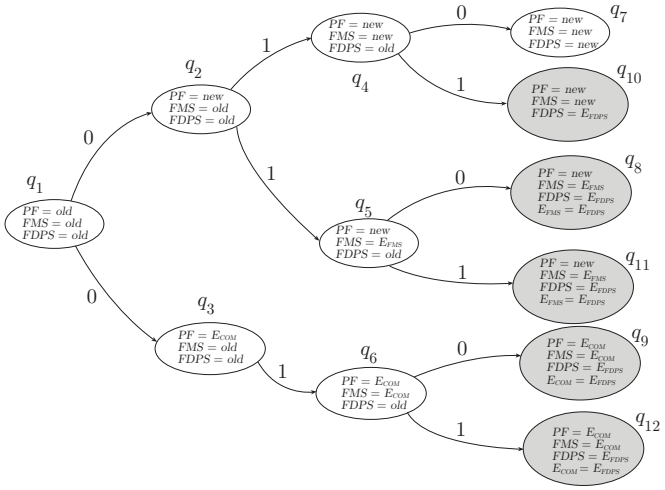

Fig. 4. Situation awareness error evolution model

With respect to the deterministic approach, the stochastic analysis offers as added value an estimate of the probability distribution of the critical states: it can be used to determine the risk of a *SA* error for the next transition, spanning on all possible one–step transitions from the actual state of $\mathcal{O}$ and associating the probability for the next state to be critical.

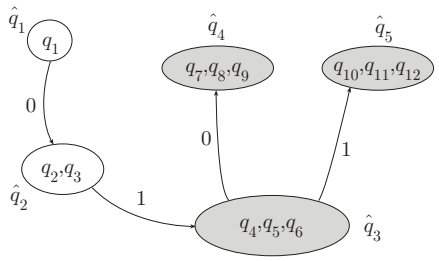

Fig. 5. System $\mathcal{O}$ automata

V. Conclusions

In this paper, we showed that estimating and mitigating the probability of errors in Air Traffic Management can be supported by observability analysis. We introduced the notion of critical observability for hybrid systems to solve the problem of error detection in prescribed time–horizon. In particular, we gave conditions for the existence of a hybrid observer for critical states and we developed the corresponding design procedure. We showed how a critical observer could be used in the runway crossing problem. Then, we extended the analysis to a class of stochastic hybrid systems, namely Markov Hybrid Systems. For this class of systems, an algorithm for the design of an observer was illustrated. This stochastic framework was used to analyze error evolution in a clearance changing the flight plan. The framework proposed in this paper may be used for simulating ATM procedures and verifying detectability of dangerous operations.

Acknowledgements

The authors thank H. Blom (NLR), T. Lewis and D. Jordan (BAE Systems) and R. Irvine (Eurocontrol) for the suggestions received on the case studies presented, which made them more realistic. In particular, the authors thank T. Lewis and D. Jordan who provided the scenario of the runway crossing based on present procedures, relying on the UK Radio Telephony (RT) procedures CAP 413(2002), that are largely similar for light and commercial aircraft. The authors also thank E. De Santis and G. Pola for useful discussions.

References

[1] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, A. L. Sangiovanni–Vincentelli, 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. 76–89, Springer-Verlag, Berlin Heidelberg New York, 2002.

[2] 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.

[3] M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, Situation Awareness Error Detection, Public Deliverable D7.3, Project IST–2001–32460 HYBRIDGE, August 18, 2004, http://www.nlr.nl/public/hosted–sites/hybridge.

[4] M.D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo, Critical Observability and Hybrid Observers for Error Detection in Air Traffic Management, *Joint 2005 International Symposium on Intelligent Control & 13^{th} Mediterranean Conference on Control and Automation (2005 ISIC–MED)*, Limassol, Cyprus, June 27–29, 2005.

[5] M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, Critical Observability for a Class of Stochastic Hybrid Systems and Application to Air Traffic Management, *Public Deliverable D7.5, Project IST–2001–32460 HYBRIDGE*, May 30, 2005, http://www.nlr.nl/public/hosted–sites/hybridge.

[6] M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, Error Detection within a Specific Time Horizon, *Public Deliverable D7.4, Project IST–2001–32460 HYBRIDGE*, January 26, 2005, http://www.nlr.nl/public/hosted–sites/hybridge.

[7] S. Di Gennaro, Notes on the Nested Observers for Hybrid Systems, *Proceedings of the European Control Conference 2003 – ECC 03*, Cambridge, UK, 2003.

[8] M. R. Endsley, Towards a Theory of Situation Awareness in Dynamic Systems, *Human Factors*, Vol. 37, No. 1, pp. 32–64, 1995.

[9] P. M. Frank, Fault Diagnosis in Dynamic Systems using Analytical and Knowledge–Based Redundancy – A Survey and Some New Results, *Automatica*, Vol. 26, No. 3, pp. 459–474, 1990.

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

[11] M. A. Massoumnia, G. C. Verghese, and A. S. Willsky, Failure Detection and Identification, *IEEE Transactions on Automatic Control*, Vol. 34, No.3, pp. 316–321, 1989.

[12] M. Oishi, I. Hwang and C. Tomlin, Immediate Observability of Discrete Event Systems with Application to User–Interface Design, *Proceedings of the 42^{nd} IEEE Conference on Decision and Control*, Maui, Hawaii USA, pp. 2665–2672, 2003

[13] C.M. Özveren, and A.S. Willsky, Observability of Discrete Event Dynamic Systems, *IEEE Transactions on Automatic Control*, Vol. 35, pp. 797–806, 1990.

[14] P. Ramadge, Observability of Discrete Event Systems, *Proceedings of the 25^{th} IEEE Conference on Decision and Control*, Athens, Greece, pp. 1108-1112, 1986.

[15] P. J. Ramadge, W. M. Wonham, Supervisory Control of a Class of Discrete–Event Processes *SIAM Journal of Control and Optimization*, Vol. 25, No. 1, pp. 206–230, Jan. 1987.

[16] S. Stroeve, H.A.P. Blom, M. van der Park, Multi–Agent Situation Awareness Error Evolution in Accident Risk Modelling, FAA–Eurocontrol, ATM2003, June 2003, http://atm2003.eurocontrol.fr/