HYBRIDGE

Distributed Control and Stochastic Analysis of Hybrid Systems
Supporting Safety Critical Real-Time Systems Design

WP7: Error Evolution Control

# *Critical Observability for a Class of Stochastic Hybrid Systems and Application to Air Traffic Management*

**Maria D. Di Benedetto, Stefano Di Gennaro, Alessandro D'Innocenzo[1]**

***30 May 2005***

***Version:*** *0.4*
***Task number:*** *7.5*
***Deliverable number:*** *D7.5*
***Contract:*** *IST-2001-32460 of European Commission*

[1] University of L'Aquila

# DOCUMENT CONTROL SHEET

***Title of document:*** *Critical Observability for a Class of Stochastic Hybrid Systems and Application to Air Traffic Management*

***Authors of document:*** *Maria D. Di Benedetto, Stefano Di Gennaro, Alessandro D'Innocenzo*

***Deliverable number:*** *D7.5*

***Contract:*** *IST-2001-32460 of European Commission*

***Project:*** *Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design (HYBRIDGE)*

## DOCUMENT CHANGE LOG

| Version # | Issue Date | Sections affected | Relevant information |
|---|---|---|---|
| 0.1 | 31 Dec 2004 | All | First draft |
| 0.2 | 15 Mar 2005 | All | Second draft |
| 0.3 | 23 April 2005 | All | Third draft |
| 0.4 | 30 May 2005 | All | Fourth draft |

| Author(s) and Reviewers | | Organisation | Signature/Date |
|---|---|---|---|
| **Authors** | M.D. Di Benedetto | AQUI | |
| | S. Di Gennaro | AQUI | |
| | A. D'Innocenzo | AQUI | |
| | | | |
| | | | |
| **Internal reviewers** | E. De Santis | AQUI | |
| | G. Pola | AQUI | |
| | H. Blom | NLR | |
| | S. N. Strubbe | TWEN | |
| | | | |
| | | | |

**Abstract**

The purpose of Work Package WP7, "Error Evolution Control", of the HYBRIDGE project is developing algorithms with guaranteed performances for assisting human operators in detecting critical situation and avoiding the propagation of errors and other non–nominal events. In this report, the results of Deliverable 7.4, which were obtained in a deterministic setting, are extended 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. An observer is proposed for estimating the probability of a critical state to be active. The obtained results are related to previous work on observability of deterministic hybrid systems, and are applied to an ATM case study: a clearance to change the flight plan.

# Contents

# 1 Introduction

The purpose of Work Package WP7, "Error Evolution Control", of the HYBRIDGE project is developing algorithms with guaranteed performances for assisting human operators in detecting critical situation and avoiding the propagation of errors and other non–nominal events.

Various aspects need to be taken into account in the study of error detection for ATM. In the first four tasks of WP7, different aspects were considered. In particular, in Task 7.1, we dealt with a review of some of the psychological models that are in use for the study of air traffic management. In Task 7.2, in addition to the study of a stochastic hybrid model to describe the dynamics involved in error evolution control (see Deliverable 1.2 [3]), we addressed the issue of observability and observer design for hybrid systems (see Deliverable 7.2 [7]). In Task 7.3: we investigated the applicability of the theoretical results on observers obtained in Deliverable 7.2 to a realistic ATM situation, the active runway crossing control problem, for the detection of situation awareness errors (see Deliverable 7.3 [8]). The work carried out in Deliverable 7.3 also showed that new theoretical investigations were necessary to represent the error detection problem better. The observer construction methods proposed in Deliverable 7.2 and applied in Deliverable 7.3 are based on the notion of $K$–current–state observability [2] (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). The number $K$ is generic. In our application, it is necessary to identify *immediately* those discrete locations – called *critical* – that correspond to dangerous situations. Unfortunately, the notion of $K$–current–state observability is of no use in this case. In fact, if a critical state occurs before $K$ transitions take place, then the corresponding critical situation is not identified even though the system is current–state observable[1]. Thus, we extended the definition of observability to a subset of critical states of the agent hybrid system to yield the concept of *critical observability* (see Deliverable 7.4 [9]). We then presented how to design an observer based on this definition to verify the observability of critical states. The results were applied to the runway crossing problem and experimental results based on Matlab simulations were obtained.

In this report, the results of D7.4, which were obtained in a deterministic setting, are extended 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. *Situation Awareness [19], [10]* may be erroneous for several reasons, e.g., wrong perception of relevant information, wrong interpretation of perceived information, wrong prediction of a future state and propagation of error due to agent communication. Statistic data retrieved by the analysis of real cases of ATM procedures may be used to define specific error probability in ATM operations. Hence, we believe that a stochastic hybrid framework is well suited to analyzing error propagation. The current operational mode of

[1] In the case of the runway crossing example, the theory applies well because, after the signatures generation, the hybrid system model is current–state observable with $K = 1$.

each agent is not always known and may be represented by a partially observable discrete event system. An observer is proposed for estimating the probability of a critical state to be active. The obtained results are related to previous work on observability of deterministic hybrid systems, and are applied to an ATM case study: a clearance to change the flight plan.

The report is organized as follows. In Section 2, we define a class of stochastic hybrid systems, similar to the one considered in [18], namely a Markov Chain with continuous time dynamics associated with each node. The discrete layer of the stochastic hybrid system is assumed to be partially observable. For this class of systems, we propose in Section 3 the following definition of $\bar{P}$ - observability with respect to a set of critical states: the system is said to be $\bar{P}$-observable (observable with probability $\bar{P}$) if, whenever the measurable system output yields an estimate of the current discrete state that is ambiguous (i.e. we do not have perfect knowledge of the discrete state, but we have a set of states that are undistinguishable as actual active states), then the probability that a critical state is active is either zero or greater than $\bar{P}$ for each execution of the system. We then show how an estimator of the discrete state of the stochastic hybrid system may be designed for verifying $\bar{P}$ - observability. In Section 4, we show that 1- observability (observability with probability $\bar{P} = 1$) is equivalent to current-location observability of [2] for the deterministic hybrid system associated with the stochastic hybrid system. In Section 5, we present as a case study a clearance changing the flight plan, where partial discrete information is used to get a conditional probability distribution of the *SA* error evolution. Section 6 offers conclusions and a glimpse at further work.

## 2 Definitions and Setting

We consider a hybrid system $\mathcal{H}$ with $N$ locations $q_1, \cdots, q_N$. A continuous dynamic is associated to each location, described by the equations

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

with $A_i \in \mathbb{R}^{n\times n}$, $B_i \in \mathbb{R}^{n\times m}$, $C_i \in \mathbb{R}^{p\times n}$, $x \in X \subseteq \mathbb{R}^n$ the continuous state, $y \in Y \subseteq \mathbb{R}^p$ the continuous output, and $u \in U \subseteq \mathbb{R}^m$ the system input. As in [2], we suppose here that systems (1) are observable, although this assumption may be relaxed.

The discrete dynamics are described by a non-deterministic generator of formal language [17]:

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

with $k \in \mathbb{N}$, $q(k) \in Q$, the discrete state space, $\sigma(k) \in \Sigma = \{\sigma_1, \cdots \sigma_M\}$, the input symbol set, $\psi(k) \in \Psi = \{\varepsilon, \psi_1, \cdots \psi_P\}$, the output symbol set that includes $\varepsilon$, the null event. The

transition, input and output functions

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

are in general partial functions.

The functions $\delta$, $\eta$ can be extended as $\delta^*$, $\eta^*$ in the usual way to accept sequences $s = \sigma_1 \cdots \sigma_k \in \Sigma^*$, with $\Sigma^*$ the monoid on $\Sigma$ [17]:

$$\delta^*(q, s) = \bigcup_{q'} \delta(q', \sigma_k)$$

for $q' \in \delta^*(q, \sigma_1 \cdots \sigma_{k-1})$ and $\delta(q', \sigma_k)!$ ("!" indicates that the partial function is defined for the given arguments). If $s$ is an input sequence of length $l$, the measured output is $p = \eta^*(s) = \psi_1 \psi_2 \cdots \psi_{\bar{k}}$, where $\bar{k} \leq l$ since some $\psi_i$ can be the null event $\varepsilon$. There may exist strings of different length $s_1$ and $s_2$ (and hence with a different number of transitions) such that $\eta^*(s_1) = \eta^*(s_2)$. Let $Q_0$ be the set of possible initial discrete states; given an output string $p = \psi_1 \psi_2 \cdots \psi_{\bar{k}}$, we define

$$succ_p(Q_0) := \left\{ q \in Q : \exists q' \in Q_0, \exists s \in \Sigma^* \text{ such that } q = \delta^*(q', s)! \text{ and } \eta^*(s) = p \right\}$$

the set of all states that may be reached from an initial state $q' \in Q_0$ with an output string $p$.

The reset function

$$R\colon Q \times \Sigma \times Q \times X \to X$$

associates to each transition in $Q \times \Sigma \times Q$ a reset of the continuous state.

The evolution in time, also called *execution*, of the hybrid system $\mathcal{H}$, can be defined as in [13]. In particular, a hybrid time basis $\tau = \{I_k\} \in \mathcal{T}$, $k \in \mathbb{N}$, of $\mathcal{H}$ is a finite or infinite sequence of intervals $I_j = [t_k, t'_k]$ such that

1. $I_j$ is closed if $\tau$ is infinite; $I_k$ might be right–open if it is the last interval of a finite sequence $\tau$;
2. $t_k \leq t'_k$ for all $k \in \mathbb{N}$ and $t'_k = t_{k+1}$ for $k \geq 0$.

The cardinality of the hybrid time basis is denoted by $|\tau|$.

We assume here that discrete transitions are produced at unknown times $t'_k$ by a discrete uncontrollable input $\sigma$ (thus $\Sigma = \{\sigma\}$ and $\phi(q) = \sigma$ for each $q \in Q$). We also assume the existence of a *minimum dwell time* before which no discrete input causes a discrete transition. The association of $q(k), \sigma(k)$ and $\psi(k)$ with time can be written, by abusing notation, as $q(I_k), \sigma(t'_{k-1})$ and $\psi(t'_{k-1})$.

To characterize the stochastic behavior of $\mathcal{H}$, we define

1. A transition probability matrix $\Pi$ such that the $(i,j)$ element is

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

where $\mathcal{P}[q(k+1) = q_j \mid q(k) = q_i]$ is constant for each $k$ and $\sum_{j=1}^{N} \Pi_{ij} = 1$ for each $i = 1, \cdots, N$

2. An initial probability

$$\Pi_0 = \begin{bmatrix} \mathcal{P}_0[q_1] & \mathcal{P}_0[q_2] & \cdots & \mathcal{P}_0[q_N] \end{bmatrix}^T$$

where $\Pi_{0i} = 0$ if $q_i \notin Q_0$ and $\sum_{i=1}^{N} \Pi_{0i} = 1$.

We associate to $\mathcal{H}$ a stochastic hybrid system $\mathcal{S} := (\mathcal{H}, \ \Pi, \Pi_0)$ such that the sequence of discrete states $q(0), q(1), q(2), \cdots q(k), \cdots$, $k \in \mathbb{N}$, of $\mathcal{S}$ is a discrete time stationary Markovian Stochastic process with initial probability distribution $\Pi_0$ and transition probability matrix $\Pi$. This setting is similar to the one considered in [18] for investigating a class of stochastic optimal control problems. 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 $(\Omega, \mathcal{F}, \mathcal{P})$, on which the stationary Markov chain $q(0), q(1), q(2), \cdots$ exists. $\Omega$ is the space of all possible values that $q(0), q(1), q(2), \cdots$ can assume, and $\mathcal{F}$ the associated sigma-algebra. $\mathcal{P}$ is uniquely defined by the transition probability matrix $\Pi$ and the initial probability vector $\Pi_0$. Let $\pi_i(k) \colon = \mathcal{P}[q(k) = q_i]$ and

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

the corresponding dynamics. $\mathcal{S}$ will be called a *Markov hybrid system.*

We now introduce a formalism already used in [11] and that will be necessary in the following sections to define the probability distribution of $\mathcal{S}$ conditioned to a partial observation of the discrete state:

**Definition 1** *A digraph $D$ (or directed graph) is an ordered pair of disjoint sets $D = (Q, E)$ such that $E \subseteq Q \times Q$. A stochastic digraph is a digraph together with a transition probability matrix.*

**Definition 2** *Given a stochastic digraph $D = (Q, E)$ and a subset $Q' \subset Q$, $D' = (Q', E')$ is the stochastic subdigraph induced by $Q'$ on $D$, where $E'$ contains all edges of $E$ such that both ends are in $Q'$. The normalization of a stochastic subdigraph is the procedure of scaling all weights to obtain a stochastic digraph.*

A Markov Chain may be formalized as a digraph, and in the following we will refer to the subdigraph of the stochastic digraph associated to $\mathcal{S}$ as the subdigraph of $\mathcal{S}$.

# 3 $\bar{P}$-Observability w.r.t. Set of Critical States

There are important papers on the topic of diagnosability of stochastic systems. Debouk et al., in [4], analyze an optimization problem for sensor selection for failure diagnosis: a stochastic framework is used to minimize the number of tests and of sensors. Yoo and Lafortune, in [20], analyze diagnosability and the related control problems for partially observable discrete event systems, and propose a polynomial verification method. The definition of diagnosability does not require the detection of errors in real time, while in an ATM context it is necessary to diagnose a dangerous situation immediately. In this section, we propose a definition of observability for a Markov hybrid system with respect to a set of critical states. We then show how to design an observer for verifying $\bar{P}$-observability.

## 3.1 $\bar{P}$-Observability definition

Using the discrete output string $\psi_1 \cdots \psi_k$, it is possible to evaluate $\mathcal{P}[q(k) = q_i]$ conditioned to a subset of trajectories, namely all the trajectories whose output is the measured output. Consider the probability space $(\Omega, \mathcal{F}, \mathcal{P})$. Whenever a new output event at time $k$ is generated, it is possible to define a sequence $\{\mathcal{G}_k\}_{k\geq 0}$ (where $\mathcal{G}_k \subset \Omega \ \forall k \geq 0$), generated by the set of paths that may be associated to the output string $\psi_1 \cdots \psi_k$, and evaluate $\mathcal{P}[q(k) = q_i \mid \psi_1 \cdots \psi_k] := \mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]$. Let a set $Q_c \subseteq Q$ of critical states of $\mathcal{S}$ be given, namely a set of states associated to dangerous operations. We can give the following definition:

**Definition 3** *Given a Markov hybrid system $S$, it is $\bar{P}$-observable (with probability $\bar{P}$) for some $\bar{P} \in [0, 1]$ w.r.t. $Q_c$ if, $\forall q_i \in Q_c$ and for $k \in \mathbb{N}$:*

$$\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k] > \bar{P}, \text{ or}$$
$$\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k] = 0$$

When a discrete output string $p$ restricts the possible active state of $\mathcal{S}$ in the set $succ_p(Q_0) \subset Q$ such that $succ_p(Q_0) \cap Q_c \neq \varnothing$, the probability that the discrete state is $q_c$ may be either higher than $\bar{P}$ or zero, that is either we are sure that we are not in a critical state (thus we don't have to worry) or the probability of being in a critical state is higher than a given bound $\bar{P}$, and it is reasonable to start an alarm signal. This particular case is interesting because, in the ATM context, it corresponds to give an alert each time there is a possibility of being in a critical situation: we guarantee that we detect all critical situations with a probabilty of generating a false alarm less than $1 - \bar{P}$. We reach the limit case when the output function is rich enough that $\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]$ assumes only the values 1 or 0 for each $k > 0$, that is we know at each time with probability 1 if state $q_i$ is active or not. Clearly, it is possible that $\mathcal{G}_k$ allows to identify a state with probability 1 and $\mathcal{G}_{k+1}$ does not, because if an output string $\psi_1 \cdots \psi_k$ can only be generated by a unique path, the string $\psi_1 \cdots \psi_k \psi_{k+1}$ could instead be associated to more than one path of $S$.

### 3.2 $\bar{P}$-Observability verification

We now propose a method for the construction of a hybrid system $\mathcal{O}$ whose discrete input is the measurable discrete output of $\mathcal{S}$ (namely $\hat{\Sigma} = \Psi \setminus \{\varepsilon\}$), and whose continuous state is $\hat{\pi}(t) = [\hat{\pi}_1, \hat{\pi}_2, \cdots, \hat{\pi}_N] \in [0,1]^N$, where $\hat{\pi}_i(t) = \mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]$ for $t \in [t_k, t_{k+1})$. The discrete layer of $\mathcal{O}$ may be constructed as in [9]. Given an output string $\psi_1 \cdots \psi_k$ of $\mathcal{S}$, the associated discrete execution of $\mathcal{O}$, $\hat{q}(0), \hat{q}(1), \hat{q}(2), \cdots$, where $\hat{q}(k) \subset 2^Q$, is the set of states of $Q$ that may be active at time $k$ for the given string. In such a construction, the discrete input set $\hat{\Sigma}$ may be enriched exploiting the knowledge coming from the continuous dynamics to create further discrete signals (called "signatures"), as proposed in [2], which provide additional information to discriminate the discrete locations. The task of the signature generator is similar to that of a fault detection algorithm and is not discussed here (see [14] for a tutorial). The key point from the observability point of view is that signatures have to be generated before the system leaves the discrete state. This idea is carried out in [2] as follows: appropriate Luenberger's observers are designed for each of the continuous dynamics (1). Then, the signatures $\bar{\psi}_1, \cdots, \bar{\psi}_{\bar{N}}$ are obtained by feeding the observer outputs into a decision function block. In [2], it is shown how the observers' gains have to be chosen so that the signatures are generated within a finite and fixed time, namely the minimum dwell–time. Each label $\bar{\psi}_i \in \bar{\Psi} = \{\bar{\psi}_1, \cdots, \bar{\psi}_{\bar{N}}\}$ is characteristics of a set of locations associated to the same continuous dynamics, and is added as output $h(q)$ to the arcs entering the states $q$ contained in such set. Therefore, the input set of $\mathcal{O}$ can be defined as

$$\hat{\Sigma} = \left\{ \ \Psi \cup \bar{\Psi} \ \right\} \setminus \{\varepsilon\}$$

Clearly, it is possible that $h(q_i) = h(q_j)$ for some $i, j$, therefore $\bar{N} \leq N$.

By construction, the discrete dynamics of $\mathcal{O}$ are deterministic: thus, the transition function may be defined as $\hat{\delta} : \hat{Q} \times \ \hat{\Sigma} \to \hat{Q}$.

In order to give conditions for $\bar{P}$-observability of $\mathcal{S}$, it is reasonable to reduce the complexity in the construction of $\mathcal{O}$, namely erasing all the states of $\mathcal{S}$ (and their successors) such that critical states are not reachable from them. For notational simplicity, we still call $\mathcal{S}$ the reduced system. Then, to guarantee that the continuous state of $\mathcal{O}$ is equal to $\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k]$ for each $k \in \mathbb{N}$, we need to detect all $\varepsilon$ transitions on the reduced system $\mathcal{S}$. Since we are only interested in the detection of the null-output transitions, and not in the resolution of the ambiguity about which discrete state of $\mathcal{S}$ is currently active at each time, we require that, for each couple $(q, q')$ such that $\eta(q, \sigma, q') = \varepsilon$,

$$h(q) \neq h(q')$$

This is a weaker condition than the ones given in [9], where the generation of the signatures is used to steer $\mathcal{O}$ to singleton states, and thus to obtain the perfect knowledge of the state $q(k)$ for each $k$. Another way of detecting an $\varepsilon$ transition can be the presence of a reset of the continuous state.

The continuous dynamics associated with each discrete state of $\mathcal{O}$ are trivially flat, namely $\hat{\pi}(t_k)$ is constant until the next measured output resets the probability measure. Thus $\hat{\pi}(t) = \hat{\pi}(I_k)$ is constant for $t \in [t_k, t'_k), \forall k \in \mathbb{N}$. To complete the definition of the continuous layer of $\mathcal{O}$, we now define a reset function of the continuous state, whose interpretation is that we use the information given by the the discrete output $\psi$ of $\mathcal{S}$ to reset the probability measure of each state of $Q$. Let $t_k$ be the switching time for a transition of $\mathcal{O}$ induced by the output event $\psi$ such that $\hat{\delta}(\hat{q}_1, \psi) = \hat{q}_2$ (the event $\psi$ steers the observer from state $\hat{q}_1$ to state $\hat{q}_2$ at time $t_k$). We define a $N_{q_2} \times N_{q_1}$ dimensional matrix $\hat{R}_{\hat{q}_1,\hat{q}_2}$ such that $\hat{\pi}(t_{k+1}) = \hat{R}_{\hat{q}_1,\hat{q}_2}\hat{\pi}(t'_k)$. First, we define $\hat{q}'_1 \subseteq \hat{q}_1$ the set of states of $\hat{q}_1$ such that in $\mathcal{S}$ there exists an outgoing transition with $\psi$ output. The vector $\hat{\pi}(t'_k)$ must be normalized as $\hat{\pi}'(t'_k)$ in order to set probability 0 for all states in $\hat{q}_1 \setminus \hat{q}'_1$. Consider now the subdigraph induced by $(\hat{q}_1 \cup \hat{q}_2)$ (let $N_{1,2}$ be the cardinality of such a set) on $\mathcal{S}$; we assign probability 0 to all transitions whose output is not $\psi$ and normalize the subdigraph, obtaining an $N_{1,2} \times N_{1,2}$ dimensioned transition matrix $\hat{\Pi}$. We define $\hat{\pi}_j(t_{k+1}) = \sum_{i:q_i \in \hat{q}_1} \hat{\Pi}_{ij}\ \hat{\pi}'_i(t'_k)$ for each $j : q_j \in \hat{q}_2$, else $\hat{\pi}_j(t_{k+1}) = 0$. $\hat{R}_{\hat{q}_1,\hat{q}_2}$ is well defined.

Let $\hat{\xi}(t,k) = (\hat{\pi}(t), \hat{q}(k))$ be the hybrid state of $\mathcal{O}$, where $\hat{\xi} \in [0,1]^N \times \hat{Q}$. $\hat{\xi}_0 = (\Pi_0, Q_0)$ is the initial state.

Let $\{\mathcal{G}_k\}_{k\geq 0}$ be such that

$$\mathcal{G}_0 = \Omega \quad and \quad \mathcal{G}_{k+1} = \mathcal{G}_k \cap [q(k+1) \in \hat{q}(k+1)]$$

where the event $[q(k+1) \in \hat{q}(k+1)]$ is a subset of $\Omega$, and $\mathcal{G}_k$ is the set of all paths that may be associated to the system output until $k+1$.

We can state the following

**Theorem 4** *Given a system $S$ and the associated system $O$. Then, for each execution of $S$,*

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

$\forall t \in [t_k, t_{k+1}), \forall i = 1 \cdots N.$

**Proof.** *(by induction)* Let $q_i(k)$ be a compact notation for $q(k) = q_i$. Since $\hat{\pi}_i(t)$ is constant for each $t \in [t_k, t_{k+1})$, we refer to $\hat{\pi}_i(I_k)$ as the value on such intervals. For $k = 0$

$$\hat{\pi}(t_0) = \Pi_0$$

by construction, thus

$$\hat{\pi}_i(t_0) = \Pi_{0i} = \mathcal{P}[q_i(0)] = \mathcal{P}[q_i(0)|\ \mathcal{G}_0]$$

for all $i = 1, \cdots, N$ being $\mathcal{G}_0 = \Omega$.

We will now prove the induction step, namely that $\hat{\pi}_i(I_k) = \mathcal{P}[q_i(k)|\ \mathcal{G}_k]$ implies that $\hat{\pi}_i(I_{k+1}) = \mathcal{P}[q_i(k+1)|\ \mathcal{G}_{k+1}]$, $\forall i = 1, \cdots, N$. Let $\hat{q}(k) = \hat{q}_1$. By construction $\hat{\pi}_i(I_{k+1}) =$

$\hat{R}_{\hat{q}_1,\hat{q}_2}\hat{\pi}_i(I_k)$ if a transition $(\hat{q}_1, \hat{q}_2)$ occurs at time $k$ by an output $\psi$ of $\mathcal{S}$. The additional information given by the output $\psi$ restricts the possible paths in two ways: first, the current probability $\mathcal{P}[q_i(k)|\ \mathcal{G}_{k+1}]$ is normalized to the only states from which a $\psi$ output may be generated. Then, the transition probabilities $\mathcal{P}[q_i(k+1)|\ q_j(k), \mathcal{G}_{k+1}]$ must also be normalized (subdigraph normalization) to consider only the transitions with $\psi$ output. Thus, by construction

$$\hat{\pi}_i(I_{k+1}) = \sum_{j=1}^{N} \mathcal{P}[q_i(k+1)|q_j(k), \mathcal{G}_{k+1}]\ \mathcal{P}[q_j(k)|\ \mathcal{G}_{k+1}] = \mathcal{P}[q_i(k+1)|\ \mathcal{G}_{k+1}]$$

■

The following result states that, given a system $\mathcal{S}$ and the associated system $\mathcal{O}$, the $\bar{P}$-observability property is associated to a reachability problem on $\mathcal{O}$. Let $Reach_{\mathcal{O}}$ be the set of reachable hybrid states $\hat{\xi} \in \hat{X} \times \hat{Q}$ of $\mathcal{O}$, for the initial state $\hat{\xi}_0$ and for the output strings of all executions of $\mathcal{S}$. Then,

**Corollary 5** *A Markov hybrid system $S$ is $\bar{P}$-observable w.r.t. $\bar{Q} \subseteq Q$ if, for the associated observer $O$ the following is true:*

$$\left\{\hat{\xi} = (\hat{\pi}, \hat{q}) : \hat{\pi}_i \in (0, \bar{P})\ \forall i : q_i \in Q_c\right\} \cap Reach_{\mathcal{O}} = \varnothing$$

# 4 $\bar{P}-$ Observability for $\bar{P} = 1$

In this section, we introduce an equivalence relation between $\bar{P}$ - observability of $\mathcal{S}$ and current-location observability [2] of $\mathcal{H}$. More precisely, we prove that, given a system $\mathcal{S}$, the $\bar{P}$ - observability conditions for $\bar{P} = 1$ on the associated observer $\mathcal{O}_{\mathcal{S}}$ are equivalent to the current location observability conditions [2] on the observer $\mathcal{O}_{\mathcal{H}}$ of $\mathcal{H}$. Note that the construction of the discrete evolution of $\mathcal{O}$ is identical, thus $\mathcal{O}_{\mathcal{S}}$ and $\mathcal{O}_{\mathcal{H}}$ have the same discrete dynamics and therefore the same topological structure of the associated automata. We first recall the definitions given in [2] and [9] for a hybrid system $\mathcal{H}$ w.r.t. a subset of states $Q_c \subseteq Q$:

**Definition 6** *A hybrid system $H$ is current-location observable w.r.t. a subset of states $Q_c \subseteq Q$ if there exists a positive integer $K$ such that for every $k \geq K$, and for any initial state $q(0) \in Q$, a state $q_i \in Q_c$ can be determined from the output sequence $\psi(1), \cdots, \psi(k)$ for every possible input sequence $\sigma(1), \cdots, \sigma(k)$*

**Theorem 7** *A hybrid system $H$ is current-location observable w.r.t. a subset of states $Q_c \subseteq Q$ for $K = 1$ if, for each non-singleton state $\hat{q}$ of the corresponding observer $O_{\mathcal{H}}$, $\hat{q} \cap Q_c = \varnothing$*

We can now state the following:

**Theorem 8** *Given the systems $H$ and $S$, and the corresponding observers $O_{\mathcal{H}}$ and $O_{\mathcal{S}}$, the following are equivalent:*

1. *$S$ is $\bar{P}$-observable w.r.t. $Q_c$ with probability $\bar{P} = 1$*
2. *$H$ is current-location observable w.r.t. $Q_c$ for $K = 1$*

**Proof.** 2) $\Longrightarrow$ 1): $\mathcal{H}$ is current-location observable w.r.t. $Q_c \subseteq Q$ and $K = 1$ if and only if, for each non-singleton state $\hat{q}$ of the corresponding observer $\mathcal{O}_{\mathcal{H}}$, $\hat{q} \cap Q_c = \emptyset$. This is also true for $\mathcal{O}_{\mathcal{S}}$, since the construction of the discrete layers of $\mathcal{O}_{\mathcal{H}}$ and $\mathcal{O}_{\mathcal{S}}$ is identical. Thus, by construction,

$$\begin{aligned} \hat{\pi}_i(I_k) = 1 \quad &if \quad \hat{q}(k) = \{q_i\} \\ \hat{\pi}_i(I_k) = 0 \quad &if \quad \hat{q}(k) \neq \{q_i\} \end{aligned}$$

for each $k \geq 1$.

1) $\Longrightarrow$ 2) $\mathcal{S}$ is $\bar{P}$-observable w.r.t. $Q_c \subseteq Q$ with probability $\bar{P} = 1$ if and only if the following property holds for $\mathcal{O}_{\mathcal{S}}$ for each $i$ such that $q_i \in Q_c$ :

$$\hat{\pi}_i(I_k) \in \{0, 1\} \qquad \forall k \geq 1$$

Thus, for each $q_i \in Q_c$ and each $k \geq 1$, either

$$\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k] = 0$$

or

$$\mathcal{P}[q(k) = q_i \mid \mathcal{G}_k] = 1$$

In the first case, the statement implies that the event $[q(k) = q_i] \notin \mathcal{G}_k$ almost surely, thus for the measured output there exists no path such that $q(k) = q_i$; thus, by construction of $\mathcal{O}_{\mathcal{S}}$, $\hat{q}(k) \cap Q_c = \emptyset$. In the second case, the statement implies that the event $[q(k) = q_i] \equiv \mathcal{G}_k$ a.s., thus for the measured output all the compatible paths are such that $q(k) = q_i$. By construction of $\mathcal{O}_{\mathcal{S}}$, $\hat{q}(k) = \{q_i\}$. Thus, being the discrete layer of $\mathcal{O}_{\mathcal{S}}$ equal to the discrete layer of $\mathcal{O}_{\mathcal{H}}$, we proved that for each execution of $\mathcal{O}_{\mathcal{H}}$ and for each $k \geq 1$, if $\hat{q}(k)$ is a non-singleton state of $\mathcal{O}_{\mathcal{H}}$, then $\hat{q}(k) \cap Q_c = \emptyset$. By construction of $\mathcal{O}_{\mathcal{H}}$, for each $\hat{q} \in \hat{Q}$ there exists at least one execution of $\mathcal{H}$ such that the corresponding execution of $\mathcal{O}_{\mathcal{H}}$ visits $\hat{q}$, thus the previous assertion on $\hat{q}(k)$ holds true for each $\hat{q} \in \hat{Q}$. ■

## 5 Case study: Clearance Changing the Flight Plan

In the following, we consider the ATM procedure consisting of a clearance changing the flight plan. A description of the agents involved is presented and the procedure is modeled

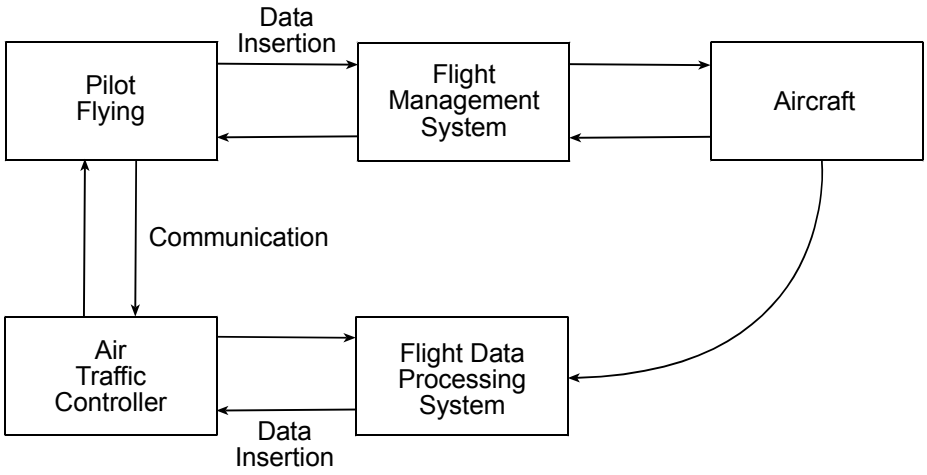


Figure 1: Clearance Changing the Flight Plan procedure

as a Markov hybrid system. A Clearance Changing the Flight Plan involves a pilot of a flying aircraft and an air traffic controller. We suppose that the procedure is started by a decision of the controller because of a conflict resolution. The agents involved (see Figure 1) and the specific behaviour of each of them are described in the following:

- The **Flight Management System** *(FMS)* is a technical system that contains the flight plan, modeled as a list of operations to be executed. Each element of the list consists of a position (for simplicity, and without loss of generality, we suppose a classical Cartesian Coordinates System $s = (x, y, z)$ ), and an arrival time $t$, which is the time the position $s$ is supposed to be reached. 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, that may be 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 informations (position, velocity, altitude, direction, aircraft code etc) on the *FDPS*.

A Clearance Changing 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 may be considered:

1. Communication error
2. *FMS* configuration error
3. *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 intent *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. The old flight plan (**Old**)
2. The 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* ($\mathbf{E}_{ATS}$)

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 following agents:

1. Pilot Flying (*PF*)
2. Flight Management System (*FMS*)
3. Fligh Data Processing System (*FDPS*)

At the beginning of the Clearance Changing the Flight Plan, the *Situation Awareness* of *PF*, *FMS* and *FDPS* is **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 *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 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: for example, if the correct flight 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, and an error could be detected when the aircraft has already entered a prohibited flight level. This means that the use of continuous dynamics to detect the current discrete state [2] 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 Changing the Flight-Plan procedure can be described by the following system $\mathcal{S}$, which models the *Situation Awareness* error evolution:

- $Q = \{q_1, q_2, \cdots, q_{12}\}$ is the set of discrete states. See Figure 2 for the interpretation of each state
- $\Sigma = \{\sigma\}$, $\Psi = \{0, 1, \varepsilon\}$ where $\varepsilon$ is the null 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 the flight plans are not equal ($SA_{\ FMS} \neq SA_{FDPS}$); *SA* stays for *Situation Awareness*.
- $\delta, \phi, \eta$ are defined according to the automata in Figure 2
- $X = \mathbb{R}^3 \times \mathbb{R}^3$ is the continuous state space, where $x = (s, v)$ specifies the aircraft position $s$ and the velocity $v$
- $U = \mathbb{R}^3$ is the control on the velocity of the aircraft, $Y = \mathbb{R}^3$ is the measure of the position of the aircraft
- $A_i, B_i, C_i$ :

$$A_i = \begin{bmatrix} 0 & I_3 \\ 0 & 0 \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ I_3 \end{bmatrix}, C_i = \begin{bmatrix} I_3 & 0 \end{bmatrix}$$

  $\forall q_i \in Q$ are the continuous dynamics. The velocity vector $v_{q_i}$ depends on the flight plan configured on the *FMS* and is controlled by $u$.

- $\Pi$ is the transition probability matrix, which may be defined according to ATM statistics. In this analysis, it is not important to define the numerical values of $\Pi_{ij}$ since our aim here is to define a framework more than solving specific cases.

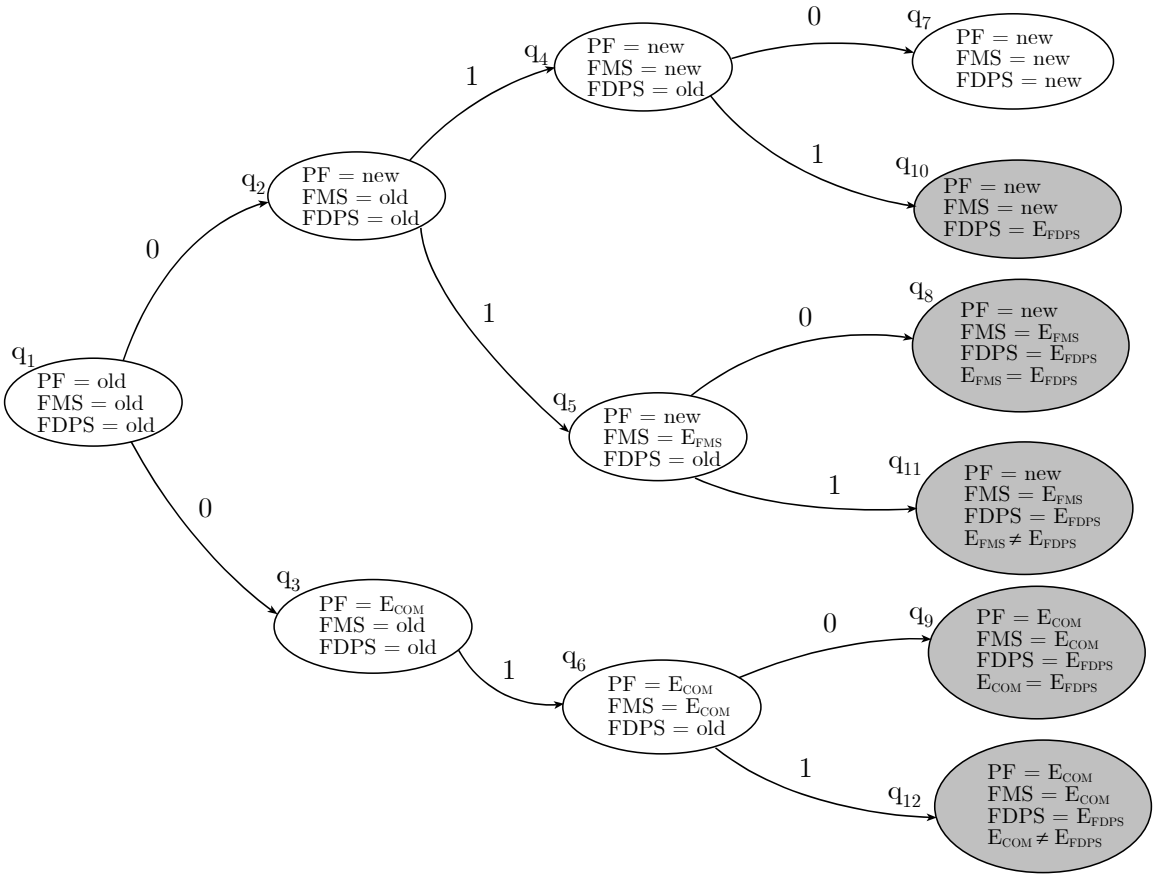


Figure 2: Situation awareness error evolution model $\mathcal{S}$

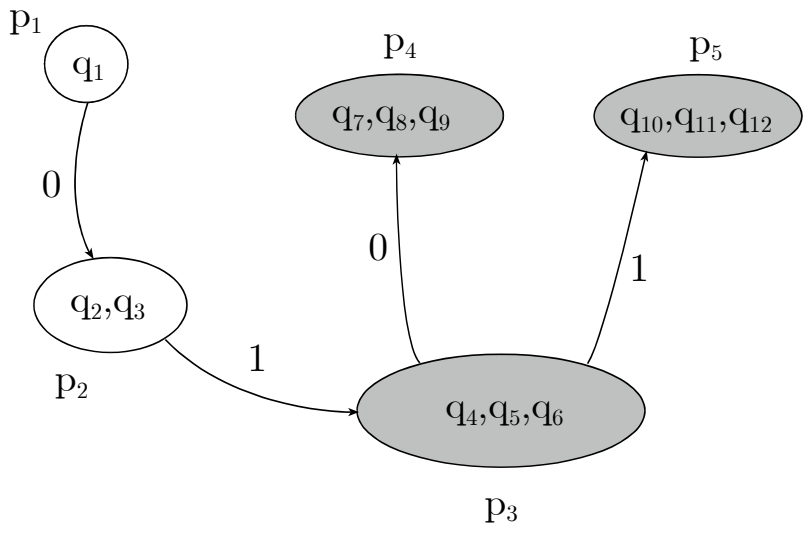


Figure 3: System $\mathcal{O}$ automaton

- $\Pi_0 = [1\ 0\ \cdots\ 0]^T$
- $x(0)$ are the aircraft continuous position and velocity when the Clearance Changing the Flight Plan procedure starts.

The construction procedure previously described leads to the following system $\mathcal{O}$, where:

- $\hat{Q} = \left\{ \begin{array}{lll} \hat{q}_1 = \{q_1\}, & \hat{q}_2 = \{q_2, q_3\}, & \hat{q}_3 = \{q_4, q_5, q_6\}, \\ \hat{q}_4 = \{q_7, q_8, q_9\}, & \hat{q}_5 = \{q_{10}, q_{11}, q_{12}\} & \end{array} \right\}$
- $\hat{\Sigma} = \{0, 1\}$
- $\hat{\delta}, \hat{\phi}$ are defined according to the discrete event system in Figure 3
- $\hat{\pi}(t) \in [0,1]^N$ is the continuous state, such that $\hat{\pi}_i(t) = \mathcal{P}[q(k) = q_i \mid \psi_1 \cdots \psi_k], \forall t \in [t_k, t_{k+1})$
- $\hat{\Pi}_{\hat{q}} = I,\ \forall \hat{q} \in \hat{Q}$

$\hat{R}$ is the reset map:

$$\hat{R}_{(\hat{q}_1,\hat{q}_2)}: \begin{cases} \hat{\pi}_2(k) = \hat{\pi}_1(k-1)\cdot\ \Pi_{1,2} \\ \hat{\pi}_3(k) = \hat{\pi}_1(k-1)\cdot\ \Pi_{1,3} \\ \hat{\pi}_i(k) = 0\ for\ i \neq 2,3 \end{cases}$$

$$\hat{R}_{(\hat{q}_2,\hat{q}_3)}: \begin{cases} \hat{\pi}_4(k) = \hat{\pi}_2(k-1)\cdot\ \Pi_{2,4} \\ \hat{\pi}_5(k) = \hat{\pi}_2(k-1)\cdot\ \Pi_{2,5} \\ \hat{\pi}_6(k) = \hat{\pi}_3(k-1)\cdot\ \Pi_{3,6} \\ \hat{\pi}_i(k) = 0\ for\ i \neq 4,5,6 \end{cases}$$

$$\hat{R}_{(\hat{q}_3,\hat{q}_4)}: \begin{cases} \hat{\pi}_7(k) = \hat{\pi}_4(k-1)\cdot\ \Pi_{4,7} \\ \hat{\pi}_8(k) = \hat{\pi}_5(k-1)\cdot\ \Pi_{5,8} \\ \hat{\pi}_9(k) = \hat{\pi}_6(k-1)\cdot\ \Pi_{6,9} \\ \hat{\pi}_i(k) = 0\ for\ i \neq 7,8,9 \end{cases}$$

$$\hat{R}_{(\hat{q}_3,\hat{q}_5)}: \begin{cases} \hat{\pi}_{10}(k) = \hat{\pi}_4(k-1)\cdot\ \Pi_{4,10} \\ \hat{\pi}_{11}(k) = \hat{\pi}_5(k-1)\cdot\ \Pi_{5,11} \\ \hat{\pi}_{12}(k) = \hat{\pi}_6(k-1)\cdot\ \Pi_{6,12} \\ \hat{\pi}_i(k) = 0\ for\ i \neq 10,11,12 \end{cases}$$

From the analysis of the system $\mathcal{O}$, system $\mathcal{S}$ is not $1-$observable since non-critical states $q_4$ and $q_7$ are indistinguishable from critical states $q_5, q_6$ and $q_8, q_9$, respectively, even when comparing the FMS and the FDPS data. Therefore, to distinguish critical states from non-critical ones, additional discrete outputs must be introduced. Finding the set of extra discrete outputs necessary to obtain 1 - observability is a combinatorial problem on the structure of the system $\mathcal{S}$, and may be trivially solved by adding all possible combinations of additional outputs to the set of edges of $\mathcal{S}$, and verifying the required conditions of 1 - observability on the system with the new outputs. Some optimization criterium can be introduced, as done in [4]. To obtain $P$-observability, a similar procedure should be followed. Since $P$ - observability conditions are weaker than deterministic current state observability conditions, the necessary number of additional outputs would be lower than in that case.

For the particular example considered here, suppose $p(k) = p_4$. Then

$$\begin{aligned} \mathcal{P}[q(k) = q_7] &= \Pi_{1,2}\cdot\Pi_{2,4}\cdot\Pi_{4,7} \\ \mathcal{P}[q(k) = q_8] &= \Pi_{1,2}\cdot\Pi_{2,5}\cdot\Pi_{5,8} \\ \mathcal{P}[q(k) = q_9] &= \Pi_{1,3}\cdot\Pi_{3,6}\cdot\Pi_{6,9} \end{aligned}$$

Since the values $\Pi_{1,3}$ (communication error probability, transit ion $(q_1, q_3)$) and $\Pi_{2,5}$ (FMS data insertion error probability, transition $(q_2, q_5)$) are very low, $P$ - observability does not hold for a reasonable value of $P$. Thus, we have to add new outputs, denoted $E_{COM}$ and $E_{FMS}$, to the transitions $(q_1, q_3)$ and $(q_2, q_5)$. To generate the output $E_{COM}$, since the VHF channel cannot be "measured", and the continuous state of the aircraft does not give any useful information, the only possibility is changing the procedure and introducing a protocol for the flight plan information data transmission, such that an error in the data transfer can be observed. The resulting observer $\mathcal{O}'$ constructed using these additional outputs is

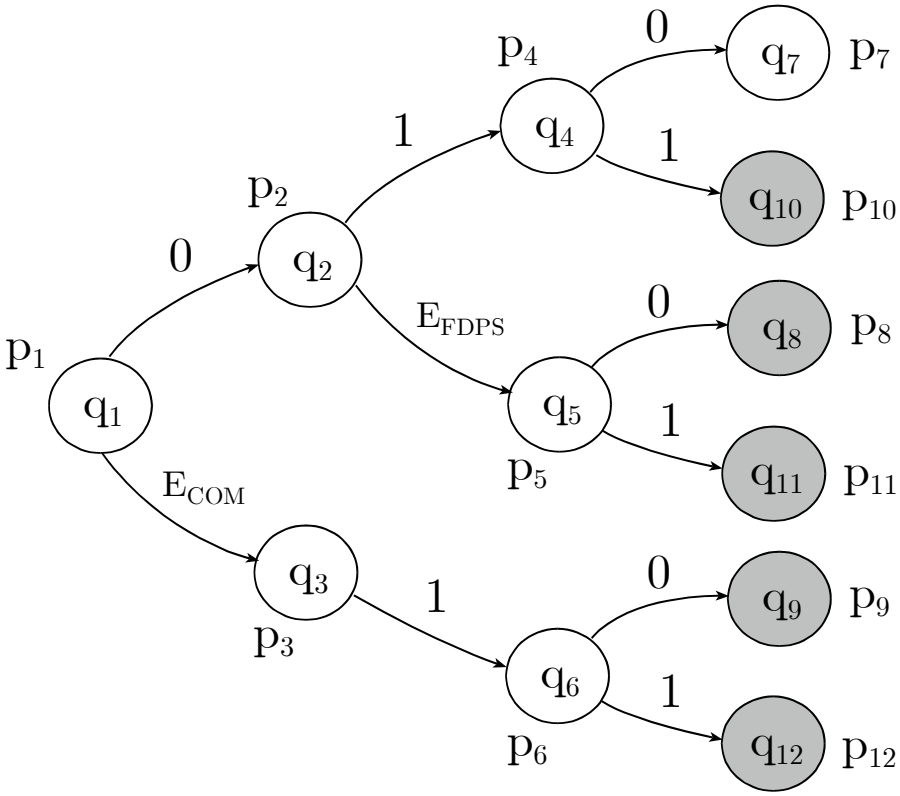


Figure 4: System $\mathcal{O}'$ automaton

shown in Figure 4, and fulfills 1-observability conditions. It is easy to see that with all other combinations of additional outputs, it is not possible to achieve $P$ - observability for a reasonable value of $P$.

The observability analysis presented here offers the advantage of obtaining an estimate of the probability distribution of the critical states: it can be used to determine the probability of a *Situation Awareness* error for the next transition, by examining all possible one-step transitions from the actual state of $\mathcal{O}$ and analyzing the probability of the next state of $\mathcal{S}$ to be critical.

## 6 Conclusions

In this report, we show that estimating and mitigating the probability of SA error in ATM may be supported by observability analysis. We proposed a definition of critical observability for a class of stochastic hybrid systems, namely for a Markov Chain with continuous time dynamics associated with each node. For this class of systems, conditions for checking critical observability were given, and an algorithm to design an observer was illustrated. The equivalence of 1 - observability conditions presented here and current location observ-

ability conditions given in [2] for non stochastic hybrid systems was proven. This stochastic framework was then used to analyze error evolution in an ATM example and to define probability measures on the transitions of the hybrid system model. The framework proposed in this report may 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 (and certainty of detecting a dangerous situation), 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.

# References


[1] A. Balluchi, L. Benvenuti, M.D. Di Benedetto, A.L. Sangiovanni- Vincentelli, "A Hybrid Observer for the Driveline Dynamics", *European Control Conference ECC'01*, Porto (Portugal), September 4–7, 2001, pp.618–623.

[2] A. Balluchi, L. Benvenuti, M.D. Di Benedetto, A.L., Sangiovanni-Vincentelli, "Design of Observers for Hybrid Systems", *In Lecture Notes in Computer Science 2289, C.J. Tomlin and M.R. Greensreet Eds.*, Springer-Verlag, 2002, pp.76–89.

[3] M.L. Bujorianu, J. Lygeros, W. Glover and G. Pola, "A Stochastic Hybrid System Modeling Framework", *Deliverable 1.2*, Project IST-2001-32460 HYBRIDGE, February 1, 2003, http://www.nlr.nl/public/hosted-sites/hybridge.

[4] R. Debouk, S. Lafortune, D. Teneketzis, "On an Optimization Problem in Sensor Selection for Failure Diagnosis", *Proceedings of the 38th Conference on Decision & Control* , Phoenix, Arizona USA, December 1999, pp. 4990-4995.

[5] E. De Santis, M.D. Di Benedetto, M.D., G. Pola, "On Observability and Detectability of Continuous–time Linear Switching Systems", *42nd IEEE Conference on Decision and Control CDC 2003*, Maui, Hawaii, December, 2003.

[6] M.D. Di Benedetto, G. Pola, "Inventory of Error Evolution Control Problems in Air Traffic Management", *Deliverable D7.1*, Project IST-2001-32460 HYBRIDGE, November 4, 2002.

[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.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.

[9] 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.

[10] Endsley, M.R., "Towards a theory of situation awareness in dynamic system", *Human Factors*, 1995, vol.37, No.1, pp.32-64.

[11] Xiao-Rong Li, Yaakov Bar-Shalom, "Multiple–Model Estimation with Variable Structure", *IEEE Transactions on automatic control*, April, 1996, vol.41, No.4, pp.478-492.

[12] D.G. Luenberger, "An introduction to observers", *IEEE Transactions on Automatic Control*, December, 1971, vol.16, 6, pp.596-602.

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

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

[15] C. M.Ozveren and A. S. Willsky, "Observability of discrete event dynamic systems", *IEEE Trans. on Automatic Control*, July, 1990, 35, 7, pp.797-806.

[16] C. M. Ozveren and A. S. Willsky and P. J. Antsaklis, "Stability and stabilizability of discrete event dynamic systems", *Journal of the Association for Computing Machinery*, July, 1991, 38, 3, pp.730-752.

[17] P. J. Ramadge, "Observability of Discrete Event–Systems", *25th IEEE Conference on Decision and Control*, Athens, Greece, 1986, pp.1108–1112.

[18] Ling Shi, A. Abate, S. Sastry, "Optimal Control for a Class of Stochastic Hybrid Systems", *43rd IEEE Conference on Decision and Control*, Atlantis, Paradise Island, Bahamas, December 14-17 2004, pp.1842–1847.

[19] 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/*

[20] T.-S. Yoo, S. Lafortune, "On the Computational Complexity of some Problems arising in Partially-Observed Discrete-Event systems", *Proceedings of the American Control Conference*, Arlington, VA, June 25-27 2001, pp. 307-312.