

---

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

Elena De Santis, Maria D. Di Benedetto, Stefano Di Gennaro,  
Alessandro D’Innocenzo, and Giordano Pola

Department of Electrical Engineering, Center of Excellence DEWS  
University of L’Aquila, Poggio di Roio, 67040 – L’Aquila, Italy  
desantis, dibenede, digennar, adinnoce, pola@ing.univaq.it

**Summary.** We present a novel observability notion for switching systems that model safety-critical systems, where a set of states – called critical states – must be detected within a prescribed delay since they correspond to hazards that may yield catastrophic events. Some sufficient and some necessary conditions for critical observability are derived. An observer is proposed for reconstructing the hybrid state evolution of the switching system whenever a critical state is reached. We apply our results to the runway crossing control problem, i.e., the control of aircraft that cross landing or take-off runways. In the hybrid model of the system, five agents are present; four are humans, each modeled as hybrid systems, subject to situation awareness errors.

## 1 Introduction

The class of hybrid control problems is extremely broad (it contains continuous control problems as well as discrete event control problems as special cases). Hence, it is very difficult to devise a general yet effective strategy to solve them. Research in the area of hybrid systems addresses significant application domains to develop further understanding of the implications of the hybrid model on control algorithms and to evaluate whether using this formalism can be of substantial help in solving complex, real-life, control problems (see e.g. [12] and the references therein).

An application that has benefited greatly from this modelling paradigm is the design of embedded controllers for transportation systems. In particular, power-train control is one of the most interesting and challenging problem in embedded system design. In [2], we presented a general framework for power-train control based on hybrid models and demonstrate that it is possible to find effective control laws with guaranteed properties without resorting to average-value models. By using hybrid systems modelling and synthesis, solutions to

several challenging control problems were proposed (see e.g. the Fast Force Transient problem [3], the cut-off problem [1], the digital idle speed control problem [10] ). These problems were solved by means of a power-train full state feedback. Since, in most cases, state measurements are not available, the synthesis of a state observer is of fundamental importance to make the hybrid control algorithms really applicable.

Another application of hybrid modelling in transportation systems that can potentially improve the quality of present solutions is the design of Air-Traffic Management systems. The objective of Air-Traffic Management is to ensure the safe and efficient operation of aircraft. The stress placed on the present systems by the ever increasing air traffic has forced the authorities to plan for an overhaul of ATM to make them more reliable, safer and more efficient. A move in this direction requires more automation and a more sophisticated monitoring and control system. Automation and control require in turn a precise formulation of the problem. In this context, variables that can be measured or estimated have to be identified together with safety indices and objective functions. To make things more complex, the behavior of ATM depend critically on the actions of humans who control the operations that are very difficult to observe, measure, model, and predict.

Error detection and control must rely upon robust state estimation techniques, thus providing a strong motivation for a rigorous approach to observability and detectability based on tests of affordable computational complexity. Other motivations are the necessity of developing controllers for assisting human operators in detecting critical situation and avoiding propagation of errors that could lead to catastrophic events. In fact, in an 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 which has to identify critical 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.

Observability has been extensively studied both in the continuous ([22], [25]) and in the discrete domains (see e.g. [29], [30]). In particular, Sontag in [32] defined different observability concepts and analyzed their relations for polynomial systems. More recently, various researchers have approached the study of observability for hybrid systems, but the definitions and the testing criteria for it varied depending on the class of systems under consideration and on the knowledge that is assumed at the output. Vidal et al. [35] considered autonomous switching systems and proposed a definition of observability based on the concept of indistinguishability of continuous initial states and discrete state evolutions from the outputs in free evolution. Incremental observability was introduced in [6] for the class of piecewise affine (PWA) systems. Incremental observability implies that different initial states always give different outputs independently of the applied input. In [8], we introduced a notion of observability and detectability for the class of switching systems,

based on the reconstructability of the hybrid state evolution, knowing the hybrid outputs, for some suitable continuous inputs. In [4], a methodology was presented for the design of dynamic observers of hybrid systems, which reconstructs the discrete state and the continuous state from the knowledge of the continuous and discrete outputs. In [17],[18], extensions of [4] were derived. In [21] the definitions of observability of [34] and the results of [4] on the design of an observer for deterministic hybrid systems were extended to discrete-time stochastic linear autonomous hybrid systems. In [5], the notion of generic final-state determinability proposed by Sontag [32] was extended to hybrid systems and sufficient conditions were given for linear hybrid systems. In [36] the Diagnosability problem for Discrete Event Systems was studied, and a polynomial verification procedure was proposed.

In some applications such as Air Traffic Management (ATM) systems and automotive control, we need to determine the actual state of the system immediately, as a delay in determining the state may lead to unsafe or even catastrophic behavior of the system. For this reason, some authors [28] extended the definition of observability to capture this urgency. In particular, in [14], [15] a notion of critical observability referred to the discrete dynamics was introduced, considering a subset of critical (discrete) states of the hybrid system. An observer based on this definition of observability was designed for fault and error detection in prescribed time horizon.

In this paper, we extend the work presented above to a class of hybrid systems, linear switching systems with minimum and maximum dwell time. The choice of this particular subclass of hybrid systems is motivated by the following considerations:

- i) switching systems are an appropriate abstraction for modelling important complex systems such as ATM systems (e.g. [14], [15]) or automotive engines (e.g. [1], [2], [10]);
- ii) the semantics of switching systems allows the derivation of necessary and sufficient computable observability conditions that become sufficient for the general class of hybrid systems where the transitions may depend on the continuous component of the hybrid state.

The paper is organized as follows. In Section 2, we review a set of formal definitions for switching systems. In Section 3, we propose a general definition of observability, based on the possibility of reconstructing the hybrid system state. We then give some necessary and sufficient testable conditions for observability. As a special case, we introduce the notion of *critical observability* and in Section 4, we offer conditions for the existence of critical observers. Furthermore, we consider in Section 5 as a non trivial case-study, the so-called active runway crossing control problem. In particular, we concentrate on the design of an observer for generating an alarm when critical situations occur, e.g., an aircraft crossing the runway when another aircraft is taking off. In Section 6, we offer some concluding remarks.

## 2 Linear Switching Systems

In this paper, we consider the class of linear switching systems that are a special case of hybrid systems, as defined in [26].

In a general hybrid system, an invariance condition may be associated with each discrete state. Given a discrete location, when the continuous state does not satisfy the corresponding invariance condition, a transition has to take place. A guard condition may be associated with each transition and has to be satisfied for that transition to be enabled. Switching systems may be seen as abstractions of hybrid systems, where we assume that the transitions do not depend on the value of the continuous state (that is, for any transition, the ‘guard condition’ is the continuous state space) and, for any discrete state, the ‘invariance condition’ is the continuous state space associated to that discrete state. The continuous state space associated with each discrete state is characterized by its own dimension that is not necessarily the same for all the discrete states.

**Definition 1.** *A linear switching system  $\mathcal{S}$  is a tuple  $(\Xi, \Xi_0, \Theta, S, E, R, \Upsilon)$  where:*

- $\Xi = \bigcup_{q_i \in Q} \{q_i\} \times \mathbb{R}^{n_i}$  is the hybrid state space, where
  - $Q = \{q_i, i \in J\}$  is the discrete state space and  $J = \{1, 2, \dots, N\}$ ;
  - $\mathbb{R}^{n_i}$  is the continuous state space associated with  $q_i \in Q$ ;
- $\Xi_0 = \bigcup_{q_i \in Q_0} \{q_i\} \times X_i^0 \subset \Xi$  is the set of all initial hybrid states;
- $\Theta = \Sigma \times \mathbb{R}^m$  is the hybrid input space, where
  - $\Sigma = \{\sigma_1, \dots, \sigma_r\}$  is the finite set of discrete uncontrolled inputs;
  - $\mathbb{R}^m$  is the continuous input space;
- $S$  is a mapping that associates to any discrete state  $q_i \in Q$ , the following continuous-time linear system

$$\dot{x}(t) = A_i x(t) + B_i u(t), \quad y(t) = C_i x(t), \quad i \in J \quad (1)$$

with  $A_i \in \mathbb{R}^{n_i \times n_i}$ ,  $B_i \in \mathbb{R}^{n_i \times m}$ ,  $C_i \in \mathbb{R}^{p \times n_i}$ ,  $x \in \mathbb{R}^{n_i}$  the continuous state,  $u \in \mathbb{R}^m$  the continuous input and  $y \in \mathbb{R}^p$  the continuous output;

- $E \subset Q \times \Sigma \times Q$  is a collection of transitions;
- $R: E \times \Xi \rightarrow \Xi$  is the reset function;
- $\Upsilon = \Psi_E \times \Psi_Q \times \mathbb{R}^p$  is the output space, where:
  - $\Psi_E = \{\epsilon, \psi_E^1, \dots, \psi_E^{N_1}\}$  is the output space associated with the transitions by means of the function  $\eta: E \rightarrow \Psi_E$ ;  $\epsilon$  is the unobservable output;
  - $\Psi_Q = \{\psi_Q^1, \dots, \psi_Q^{N_2}\}$  is the output space associated with the discrete states by means of the function  $h: Q \rightarrow \Psi_Q$ ;
  - $\mathbb{R}^p$  is the continuous output space.

We now formally define the semantics of linear switching systems. First of all we assume throughout the paper that *the discrete disturbance is not available for measurements*, thus yielding a non-deterministic system and, that the class of admissible continuous inputs is the set  $\mathcal{U}$  of piecewise continuous control functions  $u : \mathbb{R} \rightarrow \mathbb{R}^m$ . Following [26], we recall that a hybrid time basis  $\tau$  is an infinite or finite sequence of sets  $I_j = \{t \in \mathbb{R} : t_j \leq t \leq t'_j\}$ , with  $t'_j = t_{j+1}$ ; let be  $\text{card}(\tau) = L + 1$ . If  $L < \infty$ , then  $t'_L$  can be finite or infinite. Time  $t'_j$  is said to be a *switching time* and the symbol  $\mathcal{T}$  denotes the set of all hybrid time bases. The switching system temporal evolution is then defined as follows.

**Definition 2.** *An execution of  $\mathcal{S}$  is a collection  $\chi = (\xi_0, \tau, \sigma, u, \xi)$  with  $\xi_0 = (q_0, x_0) \in \Xi_0$ ,  $\tau \in \mathcal{T}$ ,  $\sigma : \mathbb{N} \rightarrow \Sigma$ ,  $u \in \mathcal{U}$ ,  $\xi : \mathbb{R} \times \mathbb{N} \rightarrow \Xi$ , where the hybrid state evolution  $\xi$  is defined as follows:*

$$\begin{aligned} \xi(t_0, 0) &= \xi_0, \\ \xi(t_{j+1}, j+1) &= R(e_j, \xi(t'_j, j)), \\ e_j &= (q(j), \sigma(j), q(j+1)) \in E, \\ x(t, j) &= x(t), \end{aligned}$$

where  $q : \mathbb{N} \rightarrow Q$ ,  $e_j = (q(j), \sigma(j), q(j+1)) \in E$  and  $x(t)$  is the (unique) solution at time  $t$  of the dynamical system  $S(q(j))$ , with initial time  $t_j$ , initial condition  $x(t_j, j)$  and control law  $u$ . The observed output evolution of  $\mathcal{S}$  is defined by the function  $y^\circ : \mathbb{R} \rightarrow \mathcal{Y}$ , such that

$$y^\circ(t) = \begin{cases} (\eta(e_{j-1}), h(q(j)), C_i x(t, j)), & \text{if } t = t_j, \\ (\epsilon, h(q(j)), C_i x(t, j)), & \text{if } t \in (t_j, t'_j), \end{cases}$$

where  $\eta(e_{-1}) = \epsilon$ .

We denote by  $\mathcal{Y}^\circ$  the class of functions  $y^\circ : \mathbb{R} \rightarrow \mathcal{Y}$ . Given a control  $u \in \mathcal{U}$  and the initial hybrid state  $\xi_0 = (q_0, x_0)$ , the resulting executions are called executions of  $\mathcal{S}$  with initial hybrid state  $\xi_0$ .

We assume the existence of a *minimum dwell time* [27] before which no discrete input causes a transition, and of a *maximum dwell time* [8] before which a transition certainly occurs.

**Assumption 1.** (*Minimum and maximum dwell time*) Given the linear switching system  $\mathcal{S}$ , there exist  $\Delta_m > 0$  and  $\Delta_M > 0$ , called respectively minimum and maximum dwell time, so that any execution  $\chi = (\xi_0, \tau, \sigma, u, \xi)$  has to satisfy the condition

$$\Delta_m \leq t'_j - t_j \leq \Delta_M, \quad \forall j = 0, 1, \dots, L-1. \quad (2)$$

The existence of a minimum dwell time is a widely used assumption in the analysis of switching systems (e.g. [27], [24] and the references therein),

and models the inertia of the system to react to an external (discrete) input. The existence of a maximum dwell time is related to the so-called liveness property of the system and is widely used in the context of Discrete Event Systems (e.g. [29]). Moreover, as shown in [10], minimum and maximum dwell times offer a method for approximating hybrid systems by means of switching systems.

An execution is *infinite* if  $\text{card}(\tau) = \infty$  or  $t'_L = \infty$ . The value  $\Delta_M$  can be finite or infinite. If  $\Delta_M = \infty$ , without loss of generality (w.l.o.g.) all executions may be assumed to be infinite. Otherwise we assume that  $\mathcal{S}$  is alive [29], i.e. for any discrete state  $q \in Q$  there exists a discrete state  $q^+$  and  $\sigma \in \Sigma$  such that  $(q, \sigma, q^+) \in E$ , so that again all the executions may be assumed w.l.o.g. to be infinite.

We will use the following notation:  $f^{-1}(\cdot)$  denotes the inverse image operator of  $f(\cdot)$ ,  $\text{reach}(Q_0)$  denotes the set of discrete states that can be reached from  $Q_0$ , i.e. such that there exists an execution, with initial discrete state in  $Q_0$ , which steers the discrete state in  $\text{reach}(Q_0)$  in a finite number of switchings. We assume w.l.o.g. that  $Q = \text{reach}(Q_0)$ .

### 3 Observability Notions

A rather complete discussion on different definitions of observability for some subclasses of hybrid systems can be found in [7], [8]. In particular, we based our definition in [8] on the reconstructability of the hybrid state evolution from some instant of time on and after a finite number, namely  $k$ , of transitions for some suitable continuous input. However, in some important applications, as for example in Air Traffic Management, it is necessary to identify within a prescribed delay and before a transition occurs, those discrete states – that we may call *critical* – that can lead to unsafe situations [14], [15]. In that case, even if the system is observable in the sense of [8], if a critical state is reached before  $k$  transitions take place, the corresponding critical situation is not identified. We therefore need to extend the definition of [8] by requiring, in addition to observability, the immediate detection of the critical states.

As already pointed out, all the definitions presented here can be given for general hybrid systems. Let  $Q_c \subset Q$  denote the set of critical states associated with the linear switching system  $\mathcal{S}$ . We assume w.l.o.g. that  $Q_0 \subset \text{reach}^{-1}(Q_c)$ .

**Definition 3.** *A linear switching system  $\mathcal{S}$  is  $Q_c$ -observable if there exist a function  $\hat{u} \in \mathcal{U}$ , a function  $\hat{\xi} : \mathcal{Y}^o \times \mathcal{U} \rightarrow \Xi$ , a real  $\Delta \in (0, \Delta_m)$  and for any  $\xi_0 \in \Xi_0$  there exists  $\hat{t} \in (t_0, \infty)$  such that for any execution of  $\mathcal{S}$  with  $u = \hat{u}$ ,*

$$\hat{\xi}\left(y^o|_{[t_0, t]}, \hat{u}|_{[t_0, t]}\right) = \xi(t, j),$$

*for any  $j$  such that  $q(j) \in Q_c, \forall t \in [t_j + \Delta, t'_j]$  and for any  $j$  such that  $j \geq \min\{j : \hat{t} \in I_j\}, \forall t \in [\hat{t}, \infty) \cap [t_j + \Delta, t'_j]$ .*

*Remark 1.* The meaning of the above definition is that any hybrid evolution has to be reconstructed at any time but a finite interval after a transition occurs, and any current state belonging to a critical set has to be detected before the next switching. If  $Q_c$  is the empty set ( $Q_c = \emptyset$ ), i.e. if there are no critical discrete states, Definition 3 of  $\emptyset$ -observability is equivalent to the notion of observability given in [8].

*Remark 2.* Definition 3 of observability is based on the existence of a control law that ensures the reconstruction of the hybrid state evolution. One could object that if a state is critical, it should be observable for all inputs. The results that we obtained in [11] answer this question: under the conditions of Theorem 1 (see Section 4), the class of control laws for which the hybrid state evolution cannot be reconstructed is a ‘thin’ set in the class of control laws  $\mathcal{U}$ . Consequently, our notion of observability is an ‘almost everywhere’ notion with respect to the chosen control law.

If one is interested in observing only the hybrid state related to the critical locations  $Q_c$ , Definition 3 can be relaxed as follows.

**Definition 4.** A linear switching system  $\mathcal{S}$  is  $Q_c$ -critically observable if there exist a function  $\hat{u} \in \mathcal{U}$ , a function  $\hat{\xi}: \mathcal{Y}^o \times \mathcal{U} \rightarrow \Xi$  and a real  $\Delta \in (0, \Delta_m)$  such that for any execution of  $\mathcal{S}$  with  $u = \hat{u}$ ,

$$\hat{\xi}\left(y^o|_{[t_0,t]}, \hat{u}|_{[t_0,t]}\right) = \xi(t, j),$$

for any  $j$  such that  $q(j) \in Q_c, \forall t \in [t_j + \Delta, t'_j]$ .

The definition of  $Q_c$ -critical observability can be further relaxed, by requiring the reconstruction only of the discrete component of the critical states.

**Definition 5.** A linear switching system  $\mathcal{S}$  is  $Q_c$ -critically location observable if there exist a function  $\hat{u} \in \mathcal{U}$ , a function  $\hat{q}: \mathcal{Y}^o \times \mathcal{U} \rightarrow Q$  and a real  $\Delta \in (0, \Delta_m)$  such that for any execution of  $\mathcal{S}$  with  $u = \hat{u}$ ,

$$\hat{q}\left(y^o|_{[t_0,t]}, \hat{u}|_{[t_0,t]}\right) = q(j),$$

for any  $j$  such that  $q(j) \in Q_c, \forall t \in [t_j + \Delta, t'_j]$ .

The relations among the different observability notions introduced above are summarized hereafter:

$$\begin{array}{c} Q_c\text{-observability} \\ \Downarrow \\ Q_c\text{-critical observability} \\ \Downarrow \\ Q_c\text{-critical location observability.} \end{array}$$

Moreover, as a direct consequence of the definitions, we have the following

**Proposition 1.** A linear switching system  $\mathcal{S}$  is  $Q_c$ -observable if and only if it is  $Q_c$ -critically observable and  $\emptyset$ -observable.

## 4 Main Results

This section is devoted to the characterization of the observability notions introduced in the previous section, and in particular of  $Q_c$ -critical observability. In view of Proposition 1, we address first  $\emptyset$ -observability and then  $Q_c$ -critical observability. For the various observability notions of interest, a set of sufficient and, under some assumptions on the switching systems, necessary and sufficient conditions are given. If there is a minimum dwell time, these conditions are sufficient also for the more general class of hybrid systems, where transitions can be forced by the value of the current continuous state (invariance transitions) or are enabled by appropriate conditions (guard conditions). In fact, it is always possible to associate a switching system to a hybrid system, by replacing invariance transitions with switching transitions (i.e. due to external discrete uncontrollable input) and by removing guard conditions (see e.g. [10]). An observer (if it exists) for this switching system is also an observer for the original hybrid system.

### 4.1 Characterization of $\emptyset$ -Observability

Given the semantics of linear switching systems and the definition of the observed output, the reconstruction of the discrete state evolution is based on both the discrete and the continuous components of the observed output. If the same discrete output is associated to two discrete states  $q_i$  and  $q_j$  of  $\mathcal{S}$ , i.e.  $h(q_i) = h(q_j)$ , then one may consider to discriminate  $q_i$  and  $q_j$  by means of the input-output behaviour of  $S(q_i)$  and  $S(q_j)$ . In particular, if

$$\exists k \in \mathbb{N} \cup \{0\} : C_i A_i^k B_i \neq C_j A_j^k B_j, \quad (3)$$

there always exists a control law  $u \in \mathcal{U}$ , such that for any initial states of  $S(q_i)$  and  $S(q_j)$ , the continuous outputs of  $S(q_i)$  and  $S(q_j)$  are different.

The following result gives a sufficient condition for  $\emptyset$ -observability.

**Theorem 1.** *A linear switching system  $\mathcal{S}$  is  $\emptyset$ -observable if the following conditions are satisfied*

- (i, 1)  $\forall q_i, q_j \in Q_0, q_i \neq q_j$ , such that  $h(q_i) = h(q_j)$ , condition (3) holds;
- (ii, 1)  $\forall q_i, q_j \in \text{reach}(Q_0), q_i \neq q_j$ , such that  $e = (q_i, \sigma, q_j) \in E$ ,  $h(q_i) = h(q_j)$  and  $\eta(e) = \epsilon$ , condition (3) holds;
- (iii, 1)  $\forall q_i \in Q, S(q_i)$  is observable.

The proof of the result above is a direct consequence of the results established in [11].

As already pointed out (see Remark 2), conditions of Theorem 1 guarantee the reconstruction of the hybrid state evolution not only for a particular control law but for ‘almost all’ control laws in the class  $\mathcal{U}$ .

It is easy to see that condition  $(i, 1)$  ensures the reconstructability of the initial discrete state while condition  $(ii, 1)$  ensures the reconstructability of the switching times: these two conditions guarantee that the discrete state evolution may be determined. The third condition  $(iii, 1)$  ensures the reconstructability of the continuous component of the hybrid state, once the discrete state evolution is known.

If the space of initial conditions  $\Xi_0$  coincides with the whole hybrid state space, i.e.  $\Xi_0 = \Xi$ , then condition  $(i, 1)$  implies condition  $(ii, 1)$ . Moreover, if the system  $\mathcal{S}$  is characterized by infinite maximum dwell time, i.e.  $\Delta_M = +\infty$ , then conditions  $(i, 1)$  and  $(iii, 1)$  are also necessary. Therefore, a consequence of Theorem 1 is

**Corollary 1.** *A linear switching system  $\mathcal{S}$  with  $\Xi_0 = \Xi$  and  $\Delta_M = +\infty$ , is  $\emptyset$ -observable if and only if conditions  $(i, 1)$  and  $(iii, 1)$  hold.*

In [8], the notion of  $\emptyset$ -observability was characterized for a linear switching system  $\mathcal{S}$  with  $\Xi_0 = \Xi$ ,  $\Delta_M = +\infty$ , and  $\eta(e) = \epsilon, \forall e \in E$ . The conditions given in [8] coincide with those of Corollary 1, since, if the maximum dwell time is infinite, the information that we get from the transitions plays no role.

## 4.2 Characterization of $Q_c$ -Critical Observability

The characterization of the notion of  $Q_c$ -critical observability is addressed by abstracting the continuous outputs of a given switching system to a suitable discrete domain. More precisely, we embed the information coming from the continuous component of the observed output into the discrete component of the observed output.

For this reason, following [4], we introduce a so-called *signature generator*. We consider here a particular signature generator consisting of a system whose inputs are the continuous input and output of  $\mathcal{S}$  and whose output is a ‘signature’ that can be considered as an additional discrete output  $h_c(q)$  associated with a discrete state  $q$  of  $\mathcal{S}$ . The signature  $h_c(q)$  has to be generated before the system leaves the discrete state  $q$  and therefore in a time interval  $\Delta < \Delta_m$ . Once this signature is generated, it remains constant until a new signature is generated.

If two dynamical systems  $S(q_i)$  and  $S(q_j)$  satisfy condition (3), there exists a control law  $u \in \mathcal{U}$  such that different signatures can be associated with  $S(q_i)$  and  $S(q_j)$ . Therefore, we assume that for any pair of distinct discrete states  $q_i, q_j \in Q$ ,  $h_c(q_i) = h_c(q_j)$  if and only if  $C_i A_i^k B_i = C_j A_j^k B_j, \forall k \in \mathbb{N} \cup \{0\}$ . This assumption allows to state *a priori* conditions for a signature to be generated, even if the information that we can collect from the continuous evolution could be richer. Indeed, even if  $S(q_i)$  and  $S(q_j)$  do not satisfy (3), there may exist initial conditions  $x_i^0$  for  $S(q_i)$  and  $x_j^0$  for  $S(q_j)$  such that, for any  $u \in \mathcal{U}$ , the continuous outputs of  $S(q_i)$  and  $S(q_j)$  are different. This is why the observability conditions presented in this section are in general sufficient, although there are cases in which they are also necessary, as shown later.

We now define, starting from the given switching system  $\mathcal{S}$ , a suitable switching system  $\mathcal{S}_d$  whose discrete output gives also informations about the input–output behavior of the continuous systems associated with the discrete locations of  $\mathcal{S}$ . Formally, given  $\mathcal{S} = (\Xi, \Xi_0, \Theta, S, E, R, \Upsilon)$ , we define the following linear switching system:

$$\mathcal{S}_d = (\Xi, \Xi_0, \Theta, S_d, E, R, \Upsilon_d),$$

where:

- $S_d$  is a mapping that associates to any discrete state  $q_i \in Q$ , the following continuous–time linear system:

$$\dot{x}(t) = A_i x(t) + B_i u(t), \quad y = \mathbf{0}, \quad i \in J$$

where  $\mathbf{0}$  is the zero vector in  $\mathbb{R}^p$  and the matrices  $A_i$  and  $B_i$  are as in (1);

- $\Upsilon_d = \bar{\Psi}_E \times \bar{\Psi}_Q \times \{0\}$ , where:
  - $\bar{\Psi}_Q = \bar{\Psi}_Q \times \bar{\Psi}$  for some set  $\bar{\Psi}$  such that  $\bar{\Psi}_Q \cap \bar{\Psi} = \emptyset$  is the extended output space associated with the discrete states by means of the function  $\bar{h} : Q \rightarrow \bar{\Psi}_Q$  such that

$$\bar{h}(q_i) = \bar{h}(q_j) \iff (h(q_i) = h(q_j) \text{ and } h_c(q_i) = h_c(q_j));$$

- $\bar{\Psi}_E = \bar{\Psi}_E \cup \{\bar{\psi}_E\}$  such that  $\bar{\psi}_E \notin \bar{\Psi}_E$  and  $\bar{\eta} : E \rightarrow \bar{\Psi}_E$  such that for any  $e = (q_i, \sigma, q_j) \in E$ ,

$$\bar{\eta}(e) := \begin{cases} \bar{\psi}_E & \text{if } \eta(e) = \epsilon \text{ and } \bar{h}(q_i) \neq \bar{h}(q_j), \\ \eta(e) & \text{otherwise.} \end{cases}$$

Two locations  $q_i$  and  $q_j$  of a switching system  $\mathcal{S}$  may be distinguished either because  $h(q_i) \neq h(q_j)$  or because condition (3) holds, i.e. equivalently, because  $\bar{h}(q_i) \neq \bar{h}(q_j)$ . Therefore,

**Proposition 2.** *Given a linear switching system  $\mathcal{S}$ , consider the associated linear switching system  $\mathcal{S}_d$ . Assume  $0 \in X_i^0$  for any  $q_i \in Q_0 \cap Q_c$ . Then,  $\mathcal{S}$  is  $Q_c$ –critically observable only if for any  $q_c \in Q_0 \cap Q_c$ ,*

(i,2)  $S(q_c)$  is observable;

(ii,2) for any  $q_0 \in Q_0 \setminus \{q_c\}$ ,  $\bar{h}(q_c) \neq \bar{h}(q_0)$ .

*Proof.* (i,2) By definition of  $Q_c$ –critical observability, for any  $q(0) = q_c \in Q_0 \cap Q_c$  it is necessary to reconstruct the continuous component of the hybrid state from the observed output, within the time interval  $I_0$ . Therefore  $S(q_c)$  has to be observable. (ii,2) By contradiction, suppose  $\bar{h}(q_c) = \bar{h}(q_0)$ , for some  $q_c \in Q_0 \cap Q_c$  and  $q_0 \in Q_0 \setminus \{q_c\}$ . Since the continuous component of the initial hybrid state can be zero, then, by definition of the function  $\bar{h}$ , it is not possible to distinguish  $q_c$  and  $q_0$ , and hence the system is not  $Q_c$ –critically observable.

Sufficient conditions for  $Q_c$ -critical observability can be given as follows:

**Proposition 3.** *The linear switching system  $\mathcal{S}$  is  $Q_c$ -critically observable if:*

- (i, 3)  $\mathcal{S}$  is  $Q_c$ -critically location observable;
- (ii, 3) for any  $q_c \in Q_c$ ,  $\mathcal{S}(q_c)$  is observable.

By definition, condition (i, 3) is also necessary and condition (ii, 3) is necessary if  $Q_c \subset Q_0$  for a switching system to be  $Q_c$ -critically observable.

Necessary and sufficient conditions for  $Q_c$ -critical observability may be given on the basis of an observer  $\mathcal{O}$  for  $\mathcal{S}_d$ , which detects the critical states in the sense of Definition 5 whenever those critical states are reached. The construction of the observer  $\mathcal{O}$  (see also [14], [15]), is inspired by [29], where a procedure was given for the construction of a finite state machine that, under appropriate conditions, allows an intermittent observation of the discrete state of  $\mathcal{S}$ , and by [4], where hybrid observers were proposed for reconstructing the hybrid state evolution of a hybrid system, in the sense of  $k$ -current state observability, namely after a certain fixed  $k > 0$ .

The observer  $\mathcal{O}$  is a discrete event system [20], that takes as inputs the observed output of  $\mathcal{S}_d$  and gives back as outputs all and only the discrete states of  $\mathcal{S}_d$  that match that observed output. The basic idea is as follows. Suppose the switching system  $\mathcal{S}_d$  starts its evolution from a location  $q_0 \in Q_0$ . When the discrete output  $\bar{h}(q_0)$  associated with  $q_0$  is available, this output is captured as an input by the observer. This first piece of information allows the observer to discriminate among all the discrete states of  $Q_0$  that are compatible with  $\bar{h}(q_0)$ . This actually implies that once this information is acquired, the observer gives back as output

$$Q_1 = \{q \in Q_0 : \bar{h}(q) = \bar{h}(q_0)\}.$$

If a transition  $e_1 \in E$  occurs, the system  $\mathcal{S}_d$  provides a discrete output  $\bar{\eta}(e_1)$  that will be an additional input for the observer. On the basis of  $\bar{\eta}(e_1)$ , the observer provides the set  $Q_2$  of all discrete states that can be reached by a state in  $Q_1$  through a transition  $e$  whose discrete output coincides with  $\bar{\eta}(e_1)$ . Therefore,

$$Q_2 = \left\{ q \in Q \mid \exists q_1 \in Q_1, \exists \sigma \in \Sigma : e = (q_1, \sigma, q) \in E, \bar{\eta}(e) = \bar{\eta}(e_1) \right\}.$$

By iterating this two-step procedure the observer can be built.

For later use, it is convenient to rewrite the discrete dynamics associated with  $\mathcal{S}_d$  by means of a non-deterministic generator of formal language [31],

$$\begin{aligned} q(j+1) &\in \delta(q(j), \sigma(j)), \\ \sigma(j) &\in \phi(q(j)), \\ \psi_E(j) &= \eta(e_{j-1}), \quad \eta(e_{-1}) = \epsilon, \\ \psi_Q(j) &= \bar{h}(q(j)), \end{aligned} \tag{4}$$

where  $\delta: Q \times \Sigma \rightarrow 2^Q$  and  $\phi: Q \rightarrow 2^\Sigma$  are respectively the transition and the input functions. Moreover, let  $s_\epsilon \in \Sigma^*$  be the input strings whose output is a sequence of empty strings  $\epsilon$ .

The following algorithm defines the observer

$$\mathcal{O} = (\hat{Q}, \hat{Q}_0, \hat{\Sigma}, \hat{\Psi}, \hat{\delta}, \hat{\phi}, \hat{h}),$$

where  $\hat{Q} \subset 2^Q$  is the state space,  $\hat{Q}_0 \subset \hat{Q}$  is the set of initial states,  $\hat{\Sigma}$  is the set of inputs that coincides with the set of outputs of  $\mathcal{S}_d$ ,  $\hat{\Psi}$  is the set of outputs that coincides with  $\hat{Q}$ ,  $\hat{\delta}: \hat{Q} \times \hat{\Sigma} \rightarrow \hat{Q}$  is the transition function,  $\hat{\phi}: \hat{Q} \rightarrow 2^{\hat{\Sigma}}$  is the input function and  $\hat{h}: \hat{Q} \rightarrow \hat{\Psi}$  is the output function.

**Algorithm 1.**

Begin

```

 $\hat{q}_0 := Q_0 \cup \{\delta(q_0, s_\epsilon) \in Q \mid q_0 \in Q_0\}$ 
 $\hat{Q}_0 := \{\hat{q}_0\}$ 
 $\hat{Q} := \hat{Q}_0$ 
 $\hat{\Sigma} := (\bar{\Psi}_E \setminus \{\epsilon\}) \cup \bar{\Psi}_Q$ 
 $j := 0$ 
repeat
   $\hat{Q}_{j+1} = \emptyset$ 
  for any  $\hat{q} \in \hat{Q}_j$ 
     $\hat{\phi}(\hat{q}) := \{\psi_Q \in \bar{\Psi}_Q \mid \exists q \in \hat{q}: \bar{h}(q) = \psi_Q\}$ 
    for any  $\psi_Q \in \hat{\phi}(\hat{q})$ 
       $\hat{\delta}(\hat{q}, \psi_Q) := \{q \in \hat{q}: \bar{h}(q) = \psi_Q\} \neq \emptyset$ 
      if  $\hat{\delta}(\hat{q}, \psi_Q) \notin \hat{Q}$ 
         $\hat{Q}_{j+1} := \hat{Q}_{j+1} \cup \{\hat{\delta}(\hat{q}, \psi_Q)\}$ 
         $\hat{Q} := \hat{Q} \cup \hat{Q}_{j+1}$ 
      end if
    end for
  end for
end for
for any  $\hat{q} \in \hat{Q}_{j+1}$ 
   $\hat{\phi}(\hat{q}) := \{\psi_E \in \bar{\Psi}_E \setminus \{\epsilon\} \mid \exists q \in \hat{q}, \exists \sigma \in \phi(q):$ 
     $\eta_E((q, \sigma, q^+)) = \psi_E, \text{ for some } q^+ \in \delta(q, \sigma)\}$ 
  for any  $\psi_E \in \hat{\phi}(\hat{q})$ 
     $\hat{\delta}(\hat{q}, \psi_E) := \left\{ q \in Q \mid \exists \bar{q} \in \hat{q}, \exists s \in \Sigma^*:$ 
       $q \in \delta(\bar{q}, s) \text{ and } \eta_E(s) \in \psi_E \epsilon^* \right\}$ 
    if  $\hat{\delta}(\hat{q}, \psi_E) \notin \hat{Q}$ 
       $\hat{Q}_{j+1} := \hat{Q}_{j+1} \cup \{\hat{\delta}(\hat{q}, \psi_E)\}$ 
       $\hat{Q} := \hat{Q} \cup \hat{Q}_{j+1}$ 
    end if
  end for
end for
end for

```

```

        j: = j + 1
    until  $\hat{Q}_{j+1} = \emptyset$ 
     $\hat{\Psi}: = \hat{Q}$ 
     $\hat{h}(\hat{q}): = \hat{q}, \forall \hat{q} \in \hat{Q}$ 
End
    
```

The finite convergence of Algorithm 1 is guaranteed by the finiteness of the discrete state space  $Q$  of  $\mathcal{S}_d$ . The set of critical states  $Q_c$  of the system  $\mathcal{S}$  induces a set of critical states  $\hat{Q}_c$  on the observer  $\mathcal{O}$ , whose analysis is fundamental for assessing critical location observability.  $\hat{Q}_c$  is formally defined as follows:

$$\hat{Q}_c: = \{\hat{q} \in \hat{Q} \mid \hat{q} \cap Q_c \neq \emptyset \wedge \hat{\phi}(\hat{q}) \cap \bar{\Psi}_Q = \emptyset\}$$

The following result holds.

**Theorem 2.**  $\mathcal{S}_d$  is  $Q_c$ -critically location observable if and only if for any  $\hat{q}_c \in \hat{Q}_c$ ,  $\text{card}(\hat{q}_c) = 1$ .

The proof of the result above is a straightforward consequence of the definition of  $\mathcal{O}$  and of the notion of  $Q_c$ -critical location observability. Moreover, Theorem 2 allows us also to give some sufficient conditions for characterizing the  $Q_c$ -critical location observability of  $\mathcal{S}$ , as follows.

**Theorem 3.** Consider the linear switching systems  $\mathcal{S}$  and  $\mathcal{S}_d$ . The following statements hold:

(i,3)  $\mathcal{S}$  is  $Q_c$ -critically location observable if  $\mathcal{S}_d$  is  $Q_c$ -critically location observable.

(ii,3) If  $Q_c \subset Q_0$  and for any  $q_i \in Q_c$ ,  $0 \in X_i^0$ , then  $\mathcal{S}$  is  $Q_c$ -critically location observable only if  $\mathcal{S}_d$  is  $Q_c$ -critically location observable.

*Proof.* (i,3) The statement follows by definition of system  $\mathcal{S}_d$ . (ii,3) By applying Proposition 2, if  $Q_c \subset Q_0$  and for any  $q_i \in Q_c$ ,  $0 \in X_i^0$ , then any two critical states  $q_i$  and  $q_j$  in  $Q_c$  can be distinguished only if  $\bar{h}(q_i) \neq \bar{h}(q_j)$ . Since this last condition implies the  $Q_c$ -critical location observability of  $\mathcal{S}_d$ , the result follows.

### 4.3 Example

We now analyze an example of application of the methodology proposed in the previous section for checking critical observability.

Consider a switching system

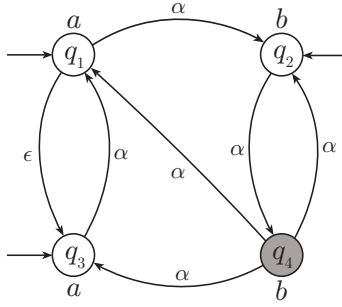
$$\mathcal{S} = (\Xi, \Xi_0, \Theta, S, E, R, \Upsilon),$$

where:

- $\Xi = Q \times \mathbb{R}^n$  where  $Q = \{q_1, q_2, q_3, q_4\}$ ;
- $\Xi_0 = \{q_1, q_2, q_3\} \times \mathbb{R}^n$ ;
- $\Theta = \Sigma \times \mathbb{R}^m$  where  $\Sigma = \{\sigma\}$ ;
- $S(q) = S$  for any  $q \in Q$ , where  $S$  is a linear dynamical system  $\dot{x} = Ax + Bu$ ,  $y = Cx$  that is supposed to be observable;
- $E = \{(q_1, \sigma, q_2), (q_1, \sigma, q_3), (q_3, \sigma, q_1), (q_2, \sigma, q_4), (q_4, \sigma, q_1), (q_4, \sigma, q_2), (q_4, \sigma, q_3)\}$ ;
- $R(e, (q_i, x)) = (q_j, x)$ ,  $\forall e = (q_i, \sigma, q_j) \in E$ ,  $\forall x \in \mathbb{R}^n$ ;
- $\Upsilon = \Psi_E \times \Psi_Q \times \mathbb{R}^p$ , is the output space, where  $\Psi_E = \{\epsilon, \alpha\}$ ,  $\Psi_Q = \{a, b\}$  and

$$h(q) = \begin{cases} a, & \text{if } q \in \{q_1, q_3\} \\ b, & \text{if } q \in \{q_2, q_4\} \end{cases}$$

$$\eta(e) = \begin{cases} \epsilon, & \text{if } e = (q_1, \sigma, q_3) \\ \alpha, & \text{otherwise.} \end{cases}$$



**Fig. 1.** Discrete event system associated with the switching system  $\mathcal{S}$

The discrete event system associated with  $\mathcal{S}$  is depicted in Figure 1, where the discrete inputs driving the transitions are omitted. We suppose that the set of critical states is  $Q_c = \{q_4\}$ . Since dynamical systems associated with each of the locations of  $\mathcal{S}$  coincide, the signatures play no role and therefore the discrete dynamics of  $\mathcal{S}_d$  coincide with the discrete dynamics of  $\mathcal{S}$ .

By applying Algorithm 1, the observer  $\mathcal{O}$  depicted in Figure 2 is obtained. It is easily seen that  $\hat{Q}_c = \{\{q_4\}\}$  and therefore conditions of Theorem 2 are fulfilled: thus  $\mathcal{S}_d$  is  $Q_c$ -critically location observable. By combining Proposition 3 and Theorem 3, we can conclude that  $\mathcal{S}$  is  $Q_c$ -critically observable. For the sake of explanation, locations  $q_2$  and  $q_4$  are characterized by the same discrete output and the same continuous dynamics  $S$ , hence  $\bar{h}(q_2) = \bar{h}(q_4)$ . This implies that there is no way of discriminating locations  $q_2$  and  $q_4$ . However, since the topological properties of the discrete event system associated to  $\mathcal{S}$  do not allow to reach  $q_4$  before reaching  $q_2$  and since the transitions

connecting the states  $q_2$  and  $q_4$  have no unobservable output, the observer  $\mathcal{O}$  is able to detect if the current location is  $q_2$  or  $q_4$ .

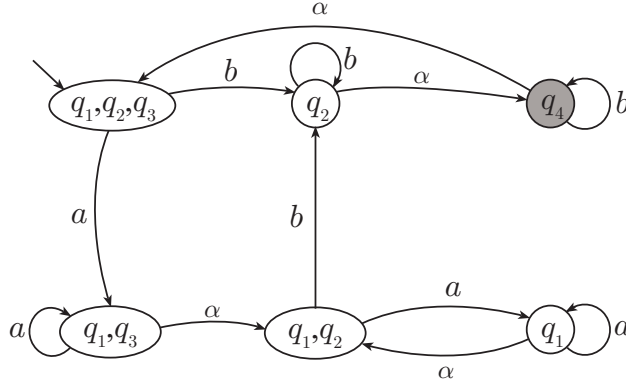


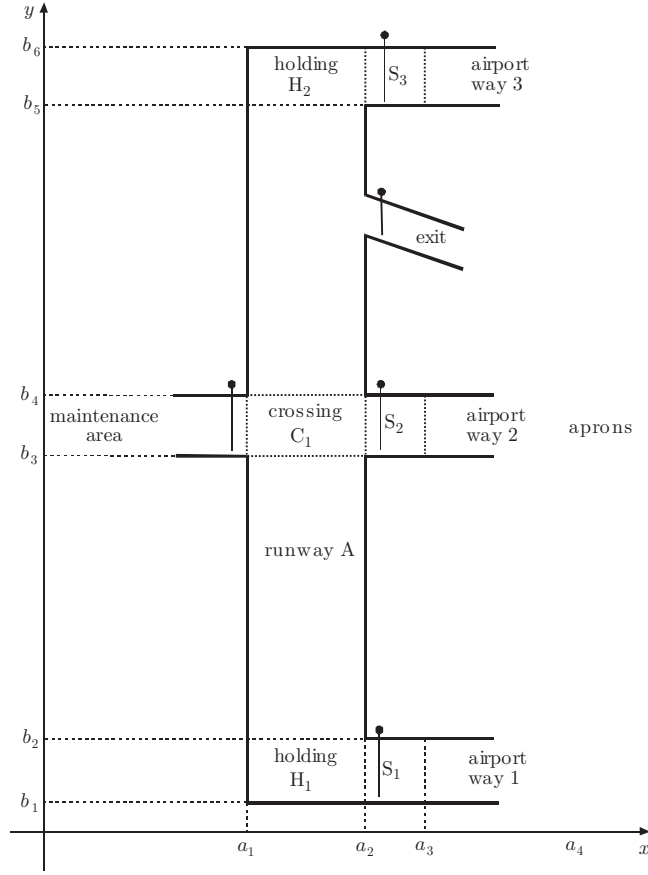
Fig. 2. Observer  $\mathcal{O}$  associated with the switching system  $\mathcal{S}$

### 5 A Case Study: the Active Runway Crossing System

In this section, we consider the example proposed in [33] and [23], and analyzed in [14], [16], of an active runway crossing with the intent of testing the applicability of the theoretical results on observers to a realistic ATM situation for the detection of situation awareness errors. This will be a sufficiently simple case study that summarizes the main difficulties in the formulation, analysis and control of a typical accident risk situation for ATM. The active runway crossing will be decomposed into various subsystems, each with hybrid dynamics modeling its specific operations.

The active runway crossing environment consists of a runway  $A$  (with holdings, crossings and exits), a maintenance area and aprons. The crossings connect the aprons and the maintenance area. Crossings (on both sides) and holdings have remotely controlled stopbars to access the runway, and each exit has a fixed stopbar (see Figure 3).

The following relevant areas can be defined:



**Fig. 3.** Airport configuration

$$\begin{aligned}
 \Omega_{Ap} &= \{(x, y) \mid x > a_4, y \in [b_1, b_6]\} \\
 \Omega_{AW_1} &= \{(x, y) \mid x \in [a_3, a_4], y \in [b_1, b_2]\} \\
 \Omega_{AW_2} &= \{(x, y) \mid x \in [a_3, a_4], y \in [b_3, b_4]\} \\
 \Omega_{AW_3} &= \{(x, y) \mid x \in [a_3, a_4], y \in [b_5, b_6]\} \\
 \Omega_{S_1} &= \{(x, y) \mid x \in [a_2, a_3], y \in [b_1, b_2]\} \\
 \Omega_{S_2} &= \{(x, y) \mid x \in [a_2, a_3], y \in [b_3, b_4]\} \\
 \Omega_{S_3} &= \{(x, y) \mid x \in [a_2, a_3], y \in [b_5, b_6]\} \\
 \Omega_{H_1} &= \{(x, y) \mid x \in [a_1, a_2], y \in [b_1, b_2]\} \\
 \Omega_{H_2} &= \{(x, y) \mid x \in [a_1, a_2], y \in [b_5, b_6]\} \\
 \Omega_{C_1} &= \{(x, y) \mid x \in [a_1, a_2], y \in [b_3, b_4]\} \\
 \Omega_{RWA} &= \{(x, y) \mid x \in [a_1, a_2], y \in [b_1, b_6]\} \\
 \Omega_M &= \{(x, y) \mid x < a_1, y \in [b_3, b_4]\}
 \end{aligned}$$

where ‘ $Ap$ ’ stands for aprons, ‘ $AW$ ’ for airport way, ‘ $S$ ’ for stopbar, ‘ $H$ ’ for holding, ‘ $C$ ’ for crossing, ‘ $RW_A$ ’ for runway A and ‘ $M$ ’ for maintenance area.

Humans may not have a correct ‘Situation Awareness’ (SA) [19], [33] and the consequent errors can then evolve to create hazardous situations. Our goal is to identify these errors and possibly correct them before they may cause catastrophic event. To do so, we need to define Situation Awareness, as follows.

**Definition 6.** *Situation Awareness (SA) is the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. The projection in the near future of the perception of the actual environment is referred to as intent SA.*

Within an ATM system, Stroeve *et al.* [33] define an *agent* as an entity, such as a human operator or a technical system, characterized by its SA of the environment. Following [33], SA can be incomplete or inaccurate, due to three different situations. An agent may:

1. wrongly perceive task-relevant information or miss them completely;
2. wrongly interpret the perceived information;
3. wrongly predict a future status.

An important source of error that has to be considered when analyzing multi-agent environments is the propagation of erroneous situation awareness due to agents interactions, e.g. via VHF communication.

### 5.1 Agents in an active runway crossing

The runway crossing operation consists of:

1. a pilot flying ( $P_t$ ) directed to  $RW_A$  to perform a take off operation;
2. a pilot flying ( $P_c$ ) directed to the  $M$ , taxing through  $AW_2$  and the runway crossing  $C_1$ ;
3. a ground controller ( $C_g$ );
4. a tower controller ( $C_t$ );
5. the airport technical support system ( $ATS$ ).

The pilot  $P_t$  proceeds towards the holding area (regular taxiway) with the intent of completing a take off operation, while the pilot  $P_c$  is approaching the crossing area. The tower controller  $C_t$  and ground controller  $C_g$ , with the aid of visual observation of the runway and VHF communication, respectively, are responsible of granting take off and crossing, avoiding the use of the runway by two aircraft simultaneously. Technical support systems help the pilots and the controllers to communicate (VHF) and detect dangerous situations (alerts).

The specific behavior of these agents in the runway crossing operation can be described as follows:

1. *Pilot flying of taking off aircraft  $P_t$ .* Initially  $P_t$  executes boarding and waits for start up grant by  $C_g$ . He begins taxiing on  $AW_1$ , stops at stopbar  $S_1$  and communicates with the  $C_t$  at the reserved frequency to obtain take off grant. Depending on the response,  $P_t$  waits for grant or executes take off immediately. Because of a *SA* error, the take off could be initiated without grant. For simplicity, we will not consider this kind of error in this work. When the aircraft is airborne, he confirms 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. If a crossing aircraft is visible, or in reaction to an emergency braking command by the controller the  $P_t$  starts a braking action and take off is rejected.
2. *Pilot Flying of crossing aircraft  $P_c$ .* When start up is granted by  $C_g$ , the  $P_c$  proceeds on the  $AW_2$  and stops at stopbar  $S_2$ . He asks to  $C_g$  crossing permission and crosses when granted. While proceeding towards the  $AW_2$ , he may have the *intent SA* that the next airport way point is either a regular taxiway (erroneous *intent SA*) or a runway crossing. In the first case,  $P_c$  enters  $RW_A$  without waiting for crossing permission. In the second case,  $P_c$  could have the *SA* that crossing is allowed while it is not. Then, he would enter the runway performing an unauthorized runway crossing. The reaction of  $P_c$  to the detection of a collision risk, due to visual observation or a tower controller call, is an emergency braking action.
3. *Ground Controller  $C_g$ .*  $C_g$  is a human operator supported by visual observation and by the *ATS* system. He grants start up both to  $P_t$  and  $P_c$ , and handles crossing operations on  $RW_A$ . If  $C_g$  has *SA* of a collision risk,  $C_g$  specifies an emergency braking action to the crossing aircraft.
4. *Tower Controller  $C_t$ .*  $C_t$  is a human operator supported by visual observation and by the *ATS* system. The  $C_t$  handles take off operations on  $RW_A$ . If the  $C_t$  has *SA* of a collision risk, he specifies an emergency braking action to the taking off aircraft.
5. *ATS system.* This is the technical system supporting the decisions of the controllers, and consists of a communication system, a runway incursion alert and a stopbar violation alert.

## 5.2 Pilot flying observation problem

The agents previously described can be modeled either as Hybrid Systems [26] or as Discrete Event Systems (DES) [16].

The pilot flying  $P_t$  can be modeled as a non-deterministic hybrid system  $\mathcal{H}_{P_t}$  with

- $Q_1 = \{q_{1,1}, q_{1,2}, q_{1,3}, q_{1,4}, q_{1,5}, q_{1,6}, q_{1,7}, q_{1,8}\}$  the set of discrete states with  $q_{1,1}$  the  $P_t$  communicating with  $C_g$  and waiting for start up grant,  $q_{1,2}$  the  $P_t$  taxiing on  $AW_1$ ,  $q_{1,3}$  the  $P_t$  aborting taxi,  $q_{1,4}$  the  $P_t$  at stopbar  $S_1$ ,  $q_{1,5}$  the  $P_t$  executing an authorized take off on  $RW_A$ ,  $q_{1,6}$  the  $P_t$  lined up

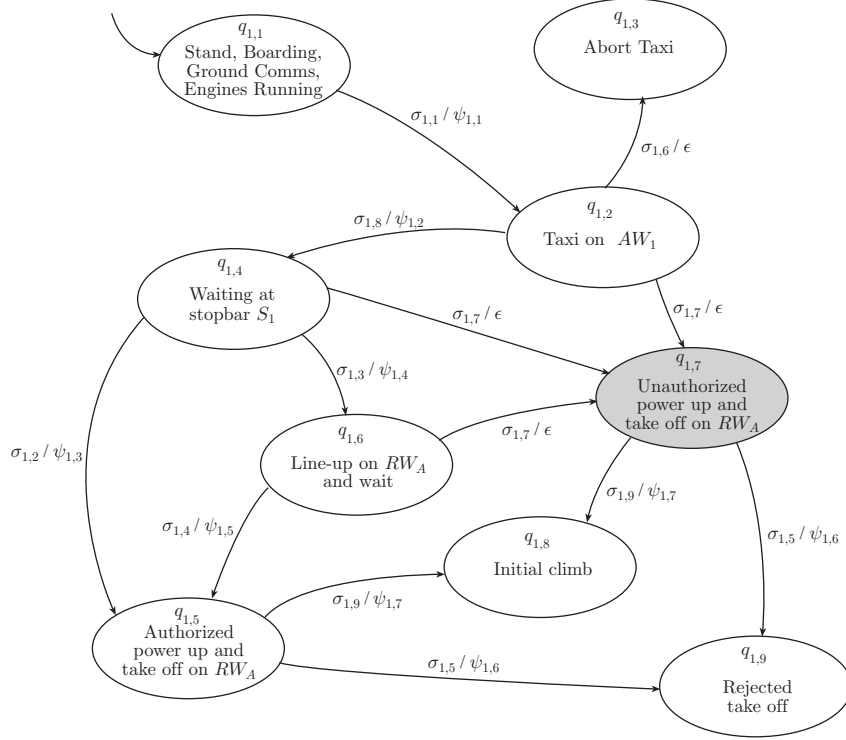


Fig. 4. Hybrid system  $\mathcal{H}_{P_t}$  modelling  $P_t$

and waiting for take off grant,  $q_{1,7}$  the  $P_t$  executing an unauthorized take off on  $RW_A$ ,  $q_{1,8}$  the  $P_t$  executing the initial climb,  $q_{1,9}$  the  $P_t$  aborting take off (emergency braking);

- $\Sigma_1 = \{\sigma_{1,1}, \sigma_{1,2}, \sigma_{1,3}, \sigma_{1,4}, \sigma_{1,5}, \sigma_{1,6}, \sigma_{1,7}\}$  the set of discrete inputs, where  $\sigma_{1,1}$  models the start up clearance by  $C_g$ ,  $\sigma_{1,2}$  the command for immediate take off by  $C_t$ ,  $\sigma_{1,3}$  the command to line up and wait by  $C_t$ ,  $\sigma_{1,4}$  the take off clearance by  $C_t$ ,  $\sigma_{1,5}$  an emergency braking command by  $C_t$ ,  $\sigma_{1,6}$  is a disturbance that causes a taxi abort, and  $\sigma_{1,7}$  models a situation awareness error as a disturbance that causes an ungranted take off;
- $\Psi_1 = \{\psi_{1,1}, \psi_{1,2}, \psi_{1,3}, \psi_{1,4}, \psi_{1,5}, \psi_{1,6}, \psi_{1,7}, \psi_{1,8}\} \cup \{\epsilon\}$  the set of discrete outputs, with  $\psi_{1,1}$  the start up confirmation to  $C_g$ ,  $\psi_{1,2}$  the take off request,  $\psi_{1,3}$  the immediate take off confirmation,  $\psi_{1,4}$  the line-up and wait confirmation,  $\psi_{1,5}$  the take off confirmation,  $\psi_{1,6}$  the emergency braking confirmation,  $\psi_{1,7}$  the airborne confirmation;
- $X_1 = \{(s_1, v_1) : s_1 \in \mathbb{R}^2, v_1 \in \mathbb{R}^2\}$ , is the set of the continuous state values, where  $s_1$  indicates the position and  $v_1$  the velocity of the agent;
- $U_1 = \mathbb{R}^2$ , is the set of the continuous input  $u_1$  values,  $D_1 = \mathbb{R}^2$  is the set of the continuous disturbance  $d_1$  values;

- The initial discrete state is  $q_{1,1}$ ;
- The invariant conditions are defined as

$$\begin{aligned}
I_{q_{1,1}} &= \{(s_1, v_1) : s_1 \in \Omega_{Ap}, \|v_1\| = 0\} \\
I_{q_{1,2}} &= \{(s_1, v_1) : s_1 \in \Omega_{AW_1} \cup \Omega_{S_1}, \|v_1\| > 0\} \\
I_{q_{1,3}} &= \{(s_1, v_1) : s_1 \in \Omega_{AW_1} \cup \Omega_{S_1}, \|v_1\| = 0\} \\
I_{q_{1,4}} &= \{(s_1, v_1) : s_1 \in \Omega_{S_1}, \|v_1\| = 0\} \\
I_{q_{1,5}} &= \{(s_1, v_1) : s_1 \in \Omega_{RW_A}, \|v_1\| > 0\} \\
I_{q_{1,6}} &= \{(s_1, v_1) : s_1 \in \Omega_{H_1}, \|v_1\| \geq 0\} \\
I_{q_{1,7}} &= \{(s_1, v_1) : s_1 \in \Omega_{RW_A} \cup \Omega_{S_1}, \|v_1\| > 0\} \\
I_{q_{1,8}} &= \{(s_1, v_1) : s_1 \in \Omega_{RW_A}, \|v_1\| > v_t\} \\
I_{q_{1,9}} &= \{(s_1, v_1) : s_1 \in \Omega_{RW_A}, \|v_1\| \geq 0\}
\end{aligned}$$

where  $v_t$  is the take off velocity and  $\Omega$ 's are defined by the airport configuration geometry;

- $S_{C_1} = \{f_{q_{j,1}} : q_{j,1} \in Q_1\}$ ,  $f_{q_{j,1}} : X_1 \times U_1 \times D_1 \rightarrow T_{X_1}$ , the sets of the continuous (simplified) dynamics  $\dot{s}_1 = v_1$ ,  $\dot{v}_1 = u_1 + d_1$ , where  $d_1$  represents possible disturbance forces acting on the aircraft (e.g. wind);
- $E_1 \subseteq Q_1 \times Q_1$  the set of transitions, given by the graph in Figure 4;
- $\eta_1 : E_1 \rightarrow \Psi_1$  the discrete output function, defined by the graph in Figure 4, where the outputs corresponding to transitions due to situation awareness errors ( $\{q_{1,2}, q_{1,7}\}$ ,  $\{q_{1,4}, q_{1,7}\}$  and  $\{q_{1,6}, q_{1,7}\}$ ) are unobservable ( $\epsilon$  output);
- $R_1(e, x, u, v) = x$ ,  $\forall (e, x, u, v) \in E_1 \times X_1 \times U_1 \times D_1$  are the reset mappings;
- The guard conditions are

$$\begin{aligned}
G(q_{1,2}, q_{1,4}) &= \{(s_1, v_1) : s_1 \in S_1, \|v_1\| = 0\} \\
G(q_{1,5}, q_{1,8}) &= G(q_{1,7}, q_{1,8}) = \{(s_1, v_1) : s_1 \in RW_A, \|v_1\| > v_t\}.
\end{aligned}$$

As shown above the pilot flying model is a hybrid system that cannot be cast in the framework of switching systems as in Definition 1. However it is possible to define an abstraction of  $\mathcal{H}_{P_t}$  that is a switching system and whose executions contain the executions generated by  $\mathcal{H}_{P_t}$ . Thus conditions outlined in the previous section for characterizing observability become sufficient conditions for characterizing observability of the hybrid system  $\mathcal{H}_{P_t}$ . The key idea is to associate to the original hybrid system  $\mathcal{H}_{P_t}$  a hybrid system  $\mathcal{H}'_{P_t}$  whose tuple coincides with tuple formally defining  $\mathcal{H}_{P_t}$  except for invariance and guard sets that are set to be the whole continuous state space. It is easily seen that the obtained hybrid system  $\mathcal{H}'_{P_t}$  is in fact a switching system in the sense of Definition 1. Therefore an observer for the pilot flying model can be constructed upon the obtained switching system  $\mathcal{H}'_{P_t}$ .

The observer  $\mathcal{O}_{P_t}$  for  $\mathcal{H}_{P_t}$  is given in Figure 5. It is clear that the system  $\mathcal{H}_{P_t}$  is not critically observable. In fact, the states of the observer  $\{q_{1,2}, q_{1,3}, q_{1,7}\}$ ,  $\{q_{1,4}, q_{1,7}\}$ ,  $\{q_{1,6}, q_{1,7}\}$  with cardinality greater than 1 are critical.

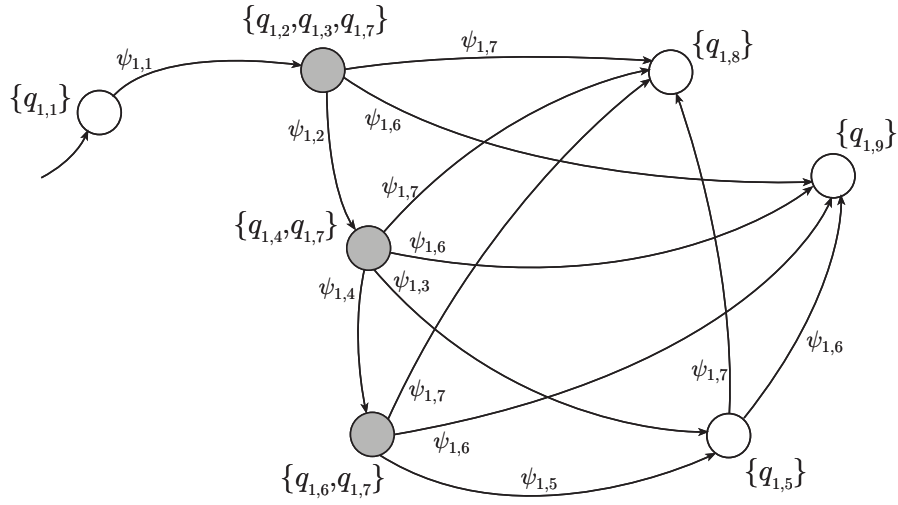


Fig. 5. Observer  $\mathcal{O}_{P_t}$

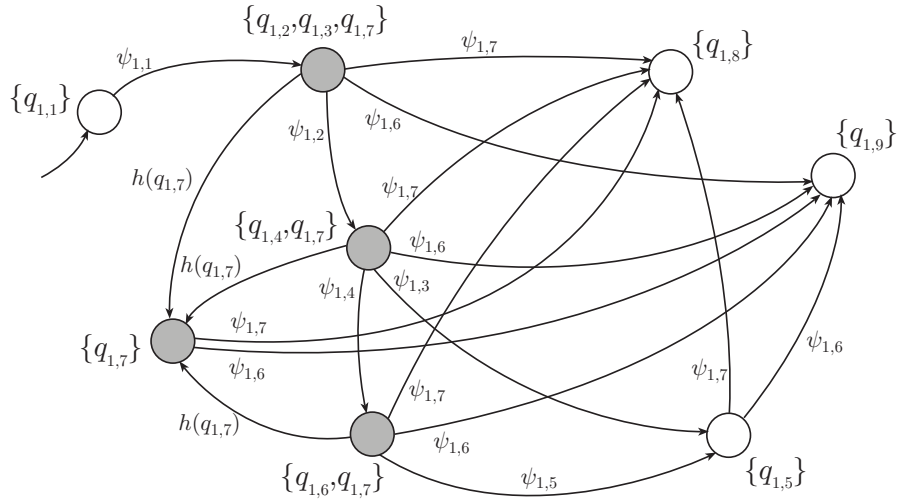


Fig. 6. Observer  $\mathcal{O}'_{P_t}$

If an additional signal  $h(q_{1,7})$  is generated to distinguish  $q_{1,7}$ , then we obtain an observer  $\mathcal{O}'_{P_t}$  (see Figure 6). It is easy to see that the introduction of the output  $h(q_{1,7})$  yields the system  $\mathcal{H}_{P_t}$  critically observable. This signal  $h(q_{1,7})$  could be generated if  $s_1 \in \Omega_{RWA}$ , assuming the continuous output  $y(t) = s_1(t)$  is available. This shows how we can solve the observation problem for  $P_t$ .

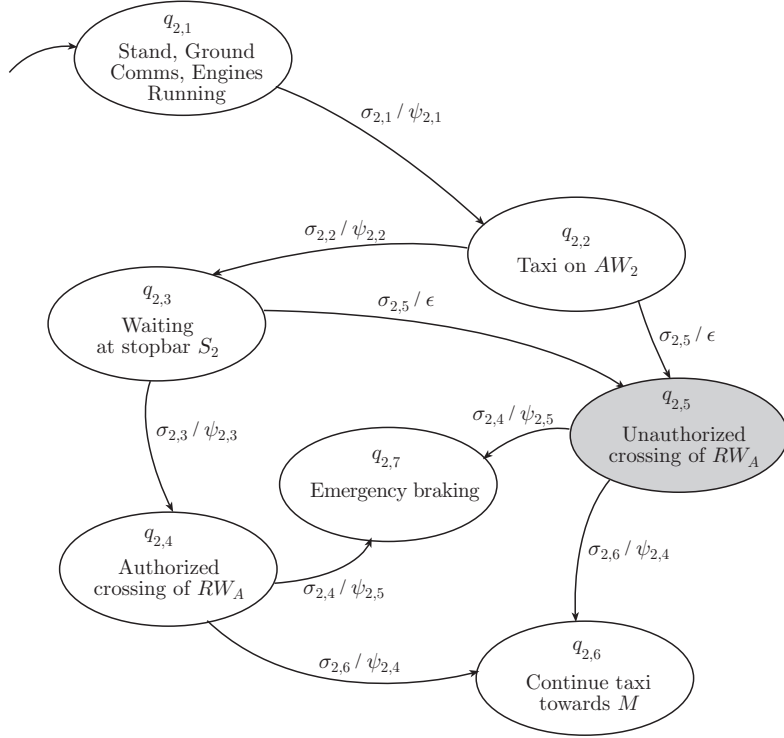


Fig. 7. Hybrid system  $\mathcal{H}_{P_c}$  modelling  $P_c$

An analogous model and a similar procedure can be followed also in the observation problem for  $P_c$  (see Figure 7), where  $P_c$  can be modeled by a hybrid system with

- $Q_2 = \{q_{2,1}, q_{2,2}, q_{2,3}, q_{2,4}, q_{2,5}, q_{2,6}, q_{2,7}\}$ , are the sets of discrete states where  $q_{2,1}$  corresponds to  $P_c$  communicating with  $C_g$  and waiting for start up grant,  $q_{2,2}$  to  $P_c$  taxiing on  $AW_2$ ,  $q_{2,3}$  to  $P_c$  waiting at stopbar  $S_2$ ,  $q_{2,4}$  to  $P_c$  executing an authorized crossing of  $RW_A$ ,  $q_{2,5}$  to  $P_c$  executing an unauthorized crossing of  $RW_A$ ,  $q_{2,6}$  to  $P_c$  taxiing towards  $M$ ,  $q_{2,7}$  to  $P_c$  performing an emergency braking operation;
- $\Sigma_2 = \{\sigma_{2,1}, \sigma_{2,2}, \sigma_{2,3}, \sigma_{2,4}, \sigma_{2,5}\}$ , is the set of discrete inputs, where  $\sigma_{2,1}$  models the start up clearance by the  $C_g$ ,  $\sigma_{2,2}$  the command by  $C_g$  to wait at stopbar  $S_2$ ,  $\sigma_{2,3}$  the crossing grant by  $C_g$ ,  $\sigma_{2,4}$  the emergency braking command by  $C_g$ ,  $\sigma_{2,5}$  models situation awareness error as a disturbance that causes an ungranted crossing;
- $\Psi_2 = \{\psi_{2,1}, \psi_{2,2}, \psi_{2,3}, \psi_{2,4}, \psi_{2,5}\} \cup \{\epsilon\}$ , is the set of discrete outputs, with  $\psi_{2,1}$  the start up confirmation,  $\psi_{2,2}$  the crossing request,  $\psi_{2,3}$  the  $RW_A$  crossing grant confirmation,  $\psi_{2,4}$  the crossing complete confirmation,  $\psi_{2,5}$  the emergency braking confirmation;

- $X_2 = \{(s_2, v_2) : s_2 \in \mathbb{R}^2, v_2 \in \mathbb{R}^2\}$ , is the set of the continuous state values, where  $s_2$  indicates the position and  $v_2$  the velocity of the agent;
- $U_2 = \mathbb{R}^2$ , is the set of the continuous input  $u_2$  values,  $D_2 = \mathbb{R}^2$  is that of the continuous disturbance  $d_2$  values;
- The initial discrete state is  $q_{2,1}$ ;
- The invariant conditions are defined as follows

$$\begin{aligned} I_{q_{2,1}} &= \{(s_2, v_2) : s_2 \in \Omega_{Ap}, \|v_2\| = 0\} \\ I_{q_{2,2}} &= \{(s_2, v_2) : s_2 \in \Omega_{AW} \cup \Omega_{S_2}, \|v_2\| > 0\} \\ I_{q_{2,3}} &= \{(s_2, v_2) : s_2 \in \Omega_{S_2}, \|v_2\| = 0\} \\ I_{q_{2,4}} &= \{(s_2, v_2) : s_2 \in \Omega_{C_1}, \|v_2\| > 0\} \\ I_{q_{2,5}} &= \{(s_2, v_2) : s_2 \in \Omega_{S_2} \cup \Omega_{C_1}, \|v_2\| > 0\} \\ I_{q_{2,6}} &= \{(s_2, v_2) : s_2 \in \Omega_M, \|v_2\| > 0\} \\ I_{q_{2,7}} &= \{(s_2, v_2) : s_2 \in \Omega_{C_1}, \|v_2\| \geq 0\} \end{aligned}$$

- $S_{C_2} = \{f_{q_{j,2}} : q_{j,2} \in Q_2\}$ ,  $f_{q_{j,2}} : X_2 \times U_2 \times V_2 \rightarrow T_{X_2}$ ,  $j = 1, 2$ , are the sets of the continuous (simplified) dynamics  $\dot{s}_2 = v_2$ ,  $\dot{v}_2 = u_2 + d_2$ , and  $d_2$  represents possible disturbance forces acting on the aircraft (e.g. wind);
- $E_2 \subseteq Q_2 \times Q_2$  the set of transitions, given by the graph in Figure 7;
- $\eta_2 : E_2 \rightarrow \Psi_2$  the discrete output function, defined by the graph in Figure 7, where the outputs corresponding to transitions due to situation awareness errors ( $\{q_{2,2}, q_{2,5}\}$  and  $\{q_{2,3}, q_{2,5}\}$ ) are unobservable, and are the source of the observability problems that we need to address;
- $R_2(e, x, u, v) = x$ ,  $\forall (e, x, u, v) \in E_2 \times X_2 \times U_2 \times D_2$  are the reset mappings;
- The guard conditions are

$$G(q_{2,4}, q_{2,6}) = (q_{2,5}, q_{2,6}) = \{(s_2, v_2) : s_2 \in M, \|v_2\| > 0\}.$$

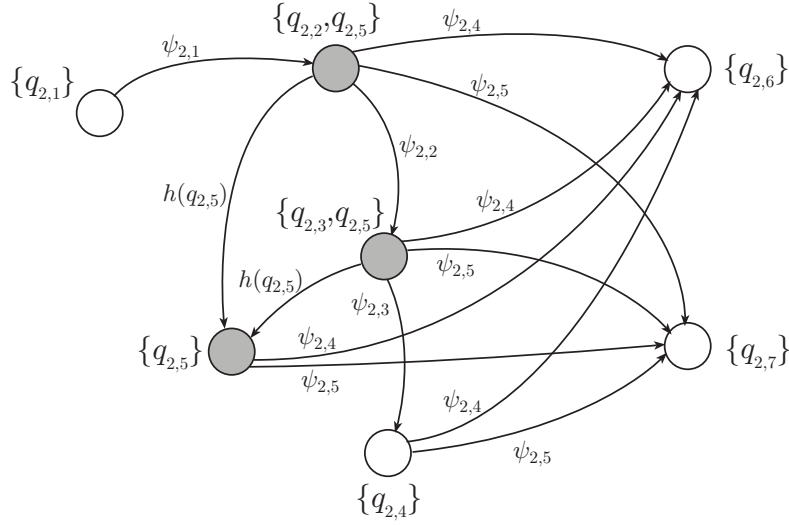
As done for  $\mathcal{H}_{P_t}$ , one works out an observer  $\mathcal{O}_{P_c}$  such that the states  $\{q_{2,2}, q_{2,5}\}$ ,  $\{q_{2,3}, q_{2,5}\}$  with cardinality greater than 1 are critical. Considering an additional discrete signal  $h(q_{2,5})$ , one obtains an observer  $\mathcal{O}'_{P_c}$ , and the system  $\mathcal{H}_{P_c}$  is critically observable (see Figure 8).

More complicated observation problems involving the two pilots acting together can be formalized considering the shuffle product of  $\mathcal{H}_{P_t}$  and  $\mathcal{H}_{P_c}$  [20], and determining the induced critical states on this new system  $\mathcal{H}$ . Indeed, in the case of the two pilots acting together, an emergency braking action may result into a halt of the aircraft on the runway, an unsafe situation to avoid. For the sake of simplicity, the models presented here do not consider this situation, but the methods developed to solve the observability problem can indeed be extended to these more complex models.

### 5.3 Controller observation problem

Consider now the observation problem of the controllers.

The ground controller  $C_g$  can be modeled by a discrete event system  $\mathcal{D}_{C_g}$  where:



**Fig. 8.** Critical observer  $\mathcal{O}'_{P_c}$

- $Q_3 = \{q_{3,1}, q_{3,2}, q_{3,3}\}$  is the set of discrete states, with  $q_{3,1}$  corresponding to  $C_g$  in miscellaneous monitoring operations,  $q_{3,2}$  to  $C_g$  having granted crossing,  $q_{3,3}$  to an emergency braking action on the runway;
- $\Sigma_3 = \{\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3}, \sigma_{3,4}, \sigma_{3,5}\}$  is the finite set of input symbols, with  $\sigma_{3,1}$  the decision to give a crossing grant,  $\sigma_{3,2} = \psi_{2,4}$  the crossing completed confirmation,  $\sigma_{3,3}$  the stopbar violation alarm on,  $\sigma_{3,4}$  the decision to give a start up,  $\sigma_{3,5} = \psi_{2,2}$  the crossing request;
- $\Psi_3 = \{\psi_{3,1}, \psi_{3,2}, \psi_{3,3}, \psi_{3,4}\} \cup \{\varepsilon\}$  is the set of discrete outputs, with  $\psi_{3,1} = \sigma_{2,3}$  the crossing grant,  $\psi_{3,2} = \sigma_{2,4}$  the emergency braking command,  $\psi_{3,3} = \sigma_{1,1} = \sigma_{2,1}$  the start up grant,  $\psi_{3,4} = \sigma_{2,2}$  the command to wait for crossing grant at stopbar  $S_2$ ;
- The set  $E_3$  of transitions and the output function  $\eta_3$  are defined by the graph in Figure 9.

The tower controller  $C_t$  can also be modeled by a discrete event system  $\mathcal{D}_{C_t}$  where:

- $Q_4 = \{q_{4,1}, q_{4,2}, q_{4,3}\}$  is the set of discrete states, with  $q_{4,1}$  corresponding to  $C_t$  in miscellaneous operations,  $q_{4,2}$  to  $C_t$  having granted take off,  $q_{4,3}$  an emergency braking action on the runway;
- $\Sigma_4 = \{\sigma_{4,1}, \sigma_{4,2}, \sigma_{4,3}\}$  is the finite set of input symbols, with  $\sigma_{4,1} = \psi_{1,2}$  the take off request,  $\sigma_{4,2} = \psi_{1,5}$  the take off completed confirmation,  $\sigma_{4,3}$  the runway incursion alert on;
- $\Psi_4 = \{\psi_{4,1}, \psi_{4,2}\} \cup \{\varepsilon\}$  is the set of discrete outputs, with  $\psi_{4,1} = \sigma_{1,2}$  the take off grant,  $\psi_{4,2} = \sigma_{1,5}$  emergency braking command;

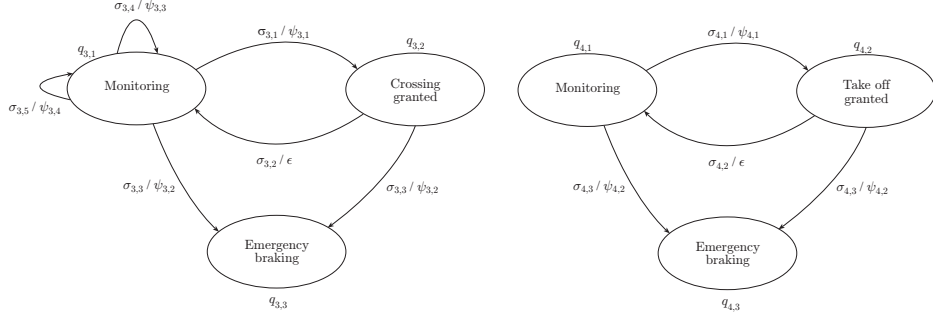


Fig. 9. Discrete event system modelling  $\mathcal{D}_{C_g}$  and  $\mathcal{D}_{C_t}$

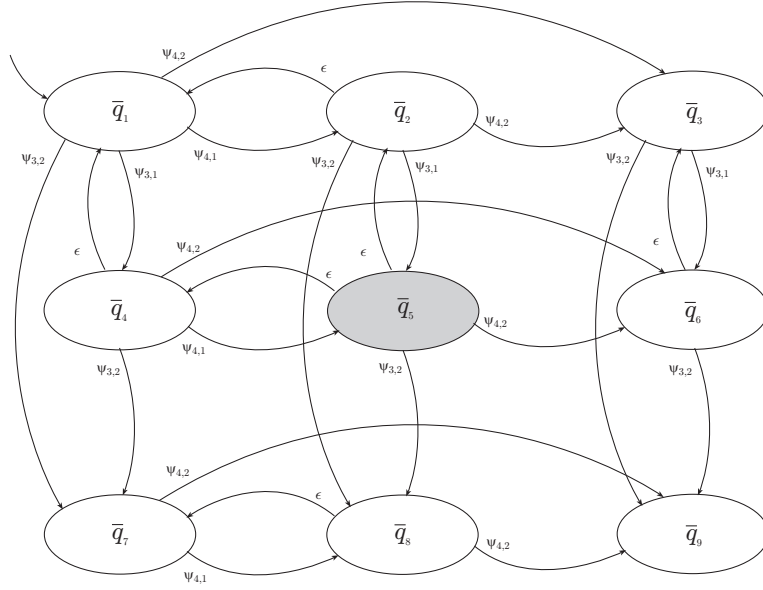
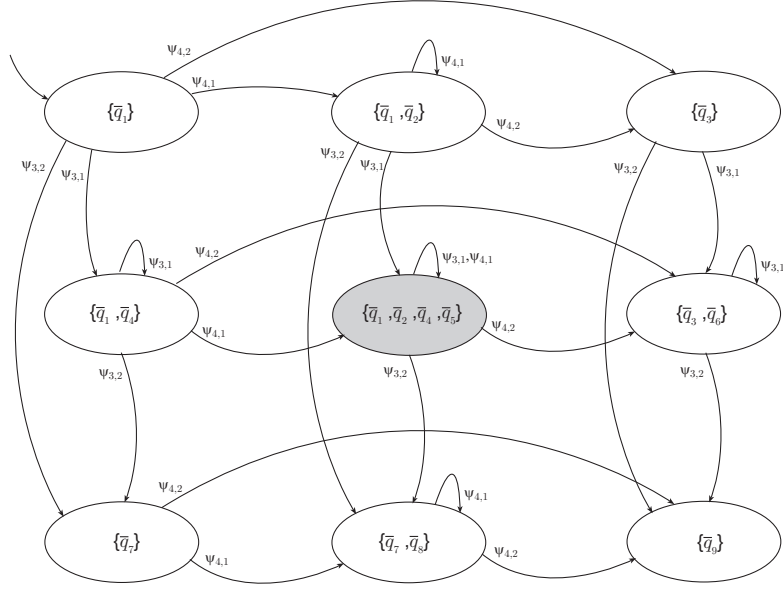


Fig. 10. Shuffle product  $\mathcal{D}_{C_g} || \mathcal{D}_{C_t}$  of  $\mathcal{D}_{C_g}$  and  $\mathcal{D}_{C_t}$

- The set  $E_4$  of transitions and the output function  $\eta_4$  are defined by the graph in Figure 9.

The hazardous situation of a crossing grant given by  $C_g$  and a take-off grant simultaneously given by  $C_t$  should be detected. However, the discrete event systems  $\mathcal{D}_{C_g}$  and  $\mathcal{D}_{C_t}$  have no critical states, because the hazardous situation arise when a crossing grant is given by  $C_g$  simultaneously with a take off grant given by  $C_t$ . Hence, the observation problem has to be considered for the composition (shuffle product)  $\mathcal{D}_{C_g} || \mathcal{D}_{C_t}$  of  $\mathcal{D}_{C_g}$  and  $\mathcal{D}_{C_t}$ , represented in Figure 10.



**Fig. 11.** Observer of  $\mathcal{D}_{C_g} || \mathcal{D}_{C_t}$

Since we are dealing with a DES, that can be viewed as a subclass of switching systems, observability conditions presented in previous sections can be applied to the system  $\mathcal{D}_{C_g} || \mathcal{D}_{C_t}$ . The observer associated with this system is illustrated in Figure 11. The state  $\bar{q}_5 = \{q_{3,2}, q_{4,2}\}$  that corresponds to simultaneous crossing grant and take off grant, is critical. One can see that additional information are needed to detect the critical state  $\bar{q}_5$ .

However, in a discrete event system, no continuous information are available. Hence, the only way for solving the observability problem of the critical states is the introduction of new discrete outputs, e.g. the confirmation that crossing ( $\bar{\psi}_3$ ) or take off ( $\bar{\psi}_4$ ) are completed, as shown in Figure 12. This corresponds to a change in the procedure the controllers have to follow.

After the addition of new outputs, the observer of the shuffle product satisfies the critical observability criteria with respect to the critical state  $\bar{q}_5$  (see Figure 13). In this case, the observer coincides with the original DES, because every transition has an observable discrete output.

## 6 Conclusions

We addressed the characterization of observability of linear switching systems. We derived some sufficient and some necessary conditions for assessing observability and critical observability, which can be checked by means of a computationally efficient procedure. We proposed an observer that under appropriate conditions is guaranteed to reconstruct the hybrid state evolution of

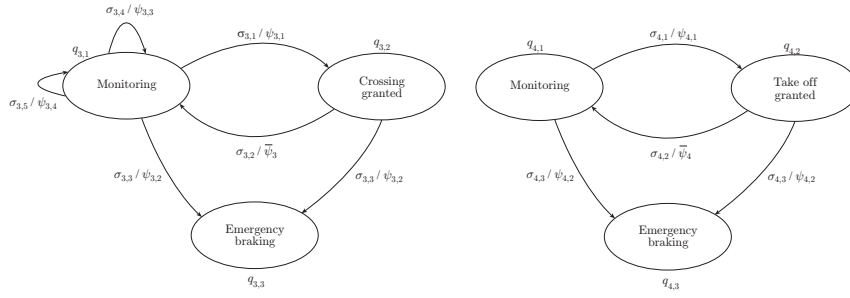


Fig. 12. DESs modelling  $\bar{D}_{C_g}$  and  $\bar{D}_{C_t}$

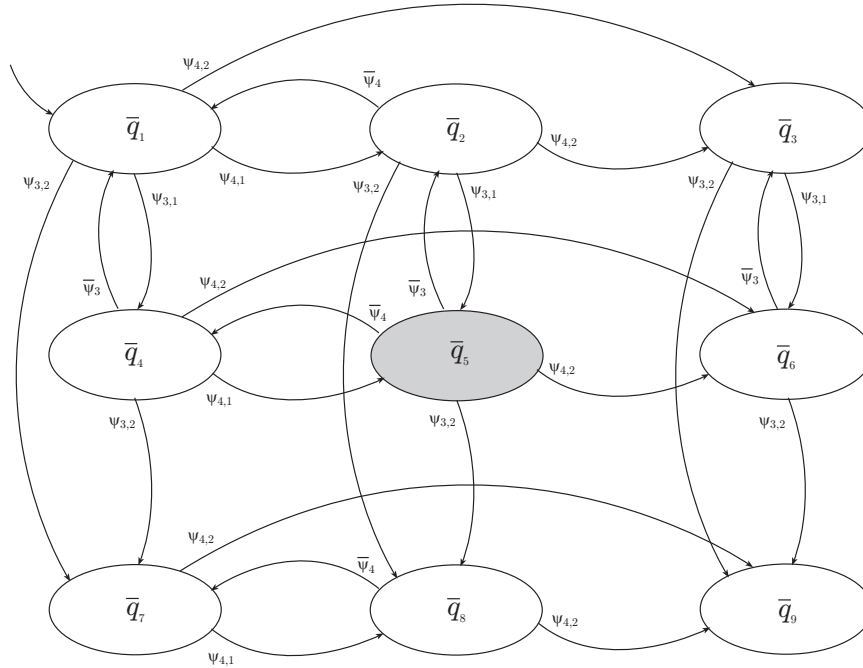


Fig. 13. Observer of  $\bar{D}_{C_g} || \bar{D}_{C_t}$

a given switching system whenever a critical state is reached. We showed how critical observability could be used in the runway crossing problem where four human agents interact in a system consisting of five subsystems. The human agents are subject to errors that may lead to catastrophic situations and are modeled as hybrid systems. We developed a hybrid observer to detect the hazardous situations corresponding to critical states. Starting from Matlab executions of the mathematical models, we also developed a framework for generating an animated simulation of the runway crossing. Future work will focus on the analysis of the topology of the discrete event system associated

with the linear switching system to find more efficient procedures for checking observability.

## Acknowledgement

The authors are grateful to Ted Lewis and Derek Jordan who provided the described scenario that relies on the UK Radio Telephony (RT) procedures CAP 413 (2002).

## References

1. A. Balluchi, M.D. Di Benedetto, C. Pinello, C. Rossi, A.L. Sangiovanni–Vincentelli, Hybrid Control in Automotive Applications: the Cut–off Control. *Automatica*, vol. 35, *Special Issue on Hybrid Systems*, March 1999, pp. 519–535.
2. A. Balluchi, L. Benvenuti, M.D. Di Benedetto, C. Pinello, A.L. Sangiovanni–Vincentelli, Automotive Engine Control and Hybrid Systems: Challenges and Opportunities. *Proceedings IEEE*, Invited Paper, Vol. 88, No. 7, July 2000, pp. 888–912.
3. A. Balluchi, M.D. Di Benedetto, C. Pinello, A.L. Sangiovanni–Vincentelli, A Hybrid Approach to the Fast Positive Force Transient Tracking Problem in Automotive Engine Control. *37<sup>th</sup> IEEE Conference on Decision and Control*, Tampa, FL, Dec. 98, pp. 3226–3231.
4. 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.
5. A. Balluchi, L. Benvenuti, M.D. Di Benedetto, A.L. Sangiovanni–Vincentelli, Observability for Hybrid Systems. *Proceedings of the 42<sup>nd</sup> IEEE Conference on Decision and Control* (CDC 03), Maui, Hawaii, USA, December 9–12, 2003.
6. A. Bemporad, G. Ferrari–Trecate, M. Morari, Observability and Controllability of Piecewise Affine and Hybrid Systems. *IEEE Transactions on Automatic Control*, Vol. 45, no. 10, October 2000, pp. 1864–1876.
7. E. De Santis, M.D. Di Benedetto, S. Di Gennaro, G. Pola, Hybrid Observer Design Methodology, WP7 Deliverable 7.2 Report, Project IST–2001–32460 HYBRIDGE, August 19, 2003.
8. E. De Santis, M.D. Di Benedetto, G. Pola, On Observability and Detectability of Continuous–time Linear Switching Systems, *Proceedings of the 42<sup>nd</sup> IEEE Conference on Decision and Control* (CDC 03), Maui, Hawaii, USA, December 9–12, 2003, pp. 5777–5782 (extended version in [www.diel.univaq.it/tr/web/web\\_search\\_tr.php](http://www.diel.univaq.it/tr/web/web_search_tr.php)).
9. E. De Santis, M.D. Di Benedetto, L. Berardi, Computation of Maximal Safe Sets for Switching Systems, *IEEE Transactions on Automatic Control*, Vol. 41 No. 10, February 2004, pp. 184–195.

10. E. De Santis, M.D. Di Benedetto, G. Pola, Digital Idle Speed Control of Automotive Engines: A Safety Problem for Hybrid Systems, *International Journal of Hybrid Systems*, 6th Special Issue on Nonlinear Analysis: Hybrid Systems and Applications, 2006, to appear.
11. E. De Santis, M. D. Di Benedetto, G. Pola, Observability and Detectability of Linear Switching Systems: A Structural Approach. Technical Report no. R.05–82, Department of Electrical Engineering and Computer Science, University of L’Aquila, Italy, January 2006. (submitted) (also available from [www.diel.univaq.it/tr/web/web\\_search\\_tr.php](http://www.diel.univaq.it/tr/web/web_search_tr.php)).
12. M.D. Di Benedetto and A. Sangiovanni–Vincentelli, Eds., Fourth International Workshop HSCC’01, Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, Springer–Verlag, Vol. 2034, 2001.
13. 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>.
14. M. D. Di Benedetto, S. Di Gennaro, A. D’Innocenzo, Critical Observability and Hybrid Observers for Error Detection in Air Traffic Management, *Proceedings of the 2005 International Symposium on Intelligent Control and 13<sup>th</sup> Mediterranean Conference on Control and Automation*, pp. 1303–1308, 27–29 June, Limassol, Cyprus, 2005.
15. M. D. Di Benedetto, S. Di Gennaro, A. D’Innocenzo, Error Detection within a Specific Time Horizon and Application to Air Traffic Management, 44<sup>th</sup> *IEEE Conference on Decision and Control*, pp. 7472–7477, Seville, Spain, December 12–15, 2005.
16. 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>.
17. S. Di Gennaro, Nested Observers for Hybrid Systems, *Proceedings of the Latin–American Conference on Automatic Control CLCA 2002*, Guadalajara, México, December 3–6, 2002.
18. S. Di Gennaro, Notes on the Nested Observers for Hybrid Systems, *Proceedings of the European Control Conference 2003 – ECC 03*, Cambridge, UK, 2003.
19. M. R. Endsley, Towards a Theory of Situation Awareness in Dynamic Systems, *Human Factors*, Vol. 37, No. 1, pp. 32–64, 1995.
20. J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages and Computation*, Addison–Wesley, Reading, MA, 1979.
21. I. Hwang, H. Balakrishnan, C. Tomlin, Observability Criteria and Estimator Design for Stochastic Linear Hybrid Systems. *Proceedings European Control Conference*, Cambridge, UK, Sept. 2003.
22. R.E. Kalman, A New Approach to Linear Filtering and Prediction Problems, *Transactions of the ASME – Journal of Basic Engineering*, Vol. D, pp. 35–45, 1960.
23. T. Lewis, D. Jordan, Personal communication, BAE Systems, 2004.
24. Liberzon, D., *Switching in systems and control*, Birkhauser 2003.
25. D.G. Luenberger, An Introduction to Observers. *IEEE Transactions on Automatic Control*, Vol. 16, no. 6, Dec. 1971, pp.596–602.
26. J. Lygeros, C. Tomlin, S. Sastry, Controllers for Reachability Specifications for Hybrid Systems, *Automatica*, Special Issue on Hybrid Systems, Vol. 35, 1999.

27. A.S. Morse, Supervisory Control of Families of Linear Set–point Controllers–Part 1: Exact Matching. *IEEE Transactions on Automatic Control*, Vol. 41, no. 10, October 1996, pp. 1413–1431.
28. M. Oishi, I. Hwang and C. Tomlin, Immediate Observability of Discrete Event Systems with Application to User–Interface Design, *Proceedings of the 42<sup>nd</sup> IEEE Conference on Decision and Control*, Maui, Hawaii USA, pp. 2665–2672, 2003.
29. C.M. Özveren, and A.S. Willsky, Observability of Discrete Event Dynamic Systems, *IEEE Transactions on Automatic Control*, Vol. 35, pp. 797–806, 1990.
30. P. J. Ramadge, Observability of Discrete Event Systems, *Proceedings of the 25<sup>th</sup> IEEE Conference on Decision and Control*, Athens, Greece, pp. 1108–1112, 1986.
31. 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.
32. E.D. Sontag, On the Observability of Polynomial Systems, I: Finite–time Problems. *SIAM J. Control and Optimization*, Vol. 17, No. 1, 1979, pp. 139–151.
33. 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>.
34. R. Vidal, A. Chiuso, S. Soatto, Observability and Identifiability of Jump Linear Systems. *Proceedings 41<sup>st</sup> IEEE Conference on Decision and Control*, Las Vegas, Nevada USA, December 2002, pp. 3614–3619.
35. R. Vidal, A. Chiuso, S. Soatto, S. Sastry, Observability of Linear Hybrid Systems, In *Lecture Notes in Computer Science 2623*, A. Pnueli and O. Maler Eds. (2003), Springer–Verlag Berlin Heidelberg, pp. 526–539.
36. T. Yoo and S. Lafortune, On The Computational Complexity Of Some Problems Arising In Partially-observed Discrete-Event Systems, In *Proceedings of the 2001 American Control Conference*, Arlington, Virginia, June, 25–27, 2001.