Critical Observability and Hybrid Observers for Error Detection in Air Traffic Management

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

Department of Electrical Engineering, Center of Excellence DEWS
University of L'Aquila, 67040 Poggio di Roio, L'Aquila, Italy
E-mail: dibenede, digennar, adinnoce@ing.univaq.it

***Abstract*— A particular problem in Air Traffic control Management (ATM), the runway crossing control problem, is considered to motivate the extension of the notion of observability for hybrid systems to yield the notion of *critical observability*. In this problem, various agents are present, and some of them are humans, modelled as hybrid systems, subject to situation awareness errors that could lead to catastrophic events. The problem is to detect the errors *immediately* to prevent them to cause these catastrophic events. Hence, the classical notions of observability for hybrid systems need to be extended to consider *critical* observability, whereby hazardous states have to be detected in one step of the Finite–State Machine component of the hybrid system. Conditions for the existence of an observer for critical states are also given and a procedure for its computation presented.**

I. Introduction

In an Air Traffic Management (ATM) closed–loop system with mixed computer–controlled and human–controlled subsystems, recovery from non–nominal situations implies the existence of an outer control loop which has to identify these situations and act accordingly to prevent them to evolve into accidents. We present an algorithm for assisting human operators in detecting critical situations and avoiding propagation of errors that could lead to catastrophic events.

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. Various aspects need to be taken into account in the study of error detection for ATM:

1) Psychological models which can be used for the study of ATM;
2) Stochastic hybrid models describing the dynamics involved in error evolution control, capturing the essential features of ATM;
3) Observability and observer design for these hybrid models;
4) The applicability of theoretical results on observers to a realistic ATM situation.

In this paper, we focus on the last two aspects. More precisely, we consider 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.

This work was partially supported by European Commission under Project HYBRIDGE IST–2001–32460 and IST NoE HyCON contract n. 511368.

The observer construction methods present in literature, such as the observer proposed in [1], are based on the notion of K–current–state observability. A hybrid system is K–current–state observable if any discrete location of the hybrid system can be identified by the use of the discrete outputs, after a finite number $K > 0$ of discrete transitions.

In this definition, the number K is generic. However, in our application, we need the bound on K to be zero for *critical* states, to prevent the evolution of errors into catastrophic situations. To solve the problem of critical observability, we build on the work presented in [1], and the one on fault and error detection in prescribed time horizon [10], [14]. To do so, we extend the definition of observability to a subset of critical states of the agent hybrid system to yield the concept of *critical observability*. We then present how to design an observer based on this definition to verify the observability of critical states. A similar result is presented in [15], where a definition of *immediate observability* is introduced, and necessary and sufficient conditions are given to satisfy this property. However, our results differ from this paper in two aspects:

- Immediate observability is required for all the states of the system, while here we are looking for milder conditions regarding the observability of those discrete states marked as "critical", namely connected with a possible hazardous situation for the process the system is modelling.
- We are interested in the extra information needed to make the property of critical observability hold, more than on the analysis of a given system

The paper is organized as follows. In Section 2, we formulate the problem and we review results on observability for hybrid systems. In Section 3, we introduce the notion of *critical observability* and we offer conditions for the existence of critical observers for a class of hybrid systems. In Section 4, we apply these results to the runway crossing problem. In Section 5, we offer concluding remarks.

II. Definitions and Problem Setting

A. Preliminary Definitions

We consider a hybrid system $\mathcal{H}$ with N locations $q_1, \cdots, q_N$. Each location identifies the continuous dynamics described by the equations

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

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 [1], we

suppose here that systems (1) are observable, although this assumption may be relaxed.

The discrete event dynamics are given by a nondeterministic generator of formal language [18]

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

with $k = 0,1,2,\cdots$, $q(k) \in Q$ the discrete location, $\psi(k) \in \Psi$ the output symbol, $\sigma(k) \in \Sigma$ the k^{th} input symbol, which takes place at time t_k and forces the discrete evolution. Here $Q = \{q_1,\cdots,q_N\}$, $\Sigma = \{\sigma_1,\cdots,\sigma_s\}$, $\Psi = \{\epsilon,\psi_1,\cdots,\psi_r\}$, with ϵ the null event, are the finite sets of locations, input and output symbols. Moreover,

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

are the transition, the input, and the output functions (in general these are partial functions, i.e. not always defined). The initial state is a state $q_0 \in Q_0 \subseteq Q$. The function ϕ specifies the possible input events σ. The functions δ, η can be extended in the usual way to accept sequences $\sigma_0\sigma_1\cdots\sigma_{k-1}\sigma_k \in \Sigma^*$, with Σ^* the monoid on Σ [18]

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

for $q' \in \delta(q,\sigma_0\cdots\sigma_{k-1})$ and $\delta(q',\sigma_k)!$, $\eta(q',\sigma_k,q'')!$ ("!" indicates that the partial function is defined for the given arguments). If $s_m = \sigma_0\sigma_2\cdots\sigma_{m-1}$ is an input sequence of length $|s_m| = m$, the measured output is $p_{\bar m} = \psi_1\psi_2\cdots\psi_{\bar m}$, whose length is $|p_{\bar m}| = \bar m \le m$ since some $\eta(q',\sigma_k,q'')$ can be the null event ϵ.

The hybrid system $\mathcal{H}$ considered here is described by systems (1), (2). The action of the discrete dynamics on the continuous ones is the change of the equations (1) when a location transition takes place. On the other hand, the action of the continuous dynamics on the discrete ones is the change of location when the continuous state x and/or the continuous control u belong to some region or when the system trajectory hits some boundary. These reciprocal actions can be modelled by the so–called guard and reset functions (see [13] for details).

To define correctly the evolution of a hybrid system $\mathcal{H}$, one introduces a hybrid time basis [13] $\tau = \{I_k\} \in \mathcal{T}$, $k = 0,1,2,\cdots$, of $\mathcal{H}$ as a finite or infinite sequence of intervals $I_k = [t_k, t'_k]$ such that

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

The length of the hybrid time basis is $|\tau|$.

Given a hybrid system $\mathcal{H}$ and a time basis τ, we suppose that for each state $q \in Q$, there exists a minimum dwell time $\Delta_m(q)$ such that

$$t'_k - t_k \ge \Delta_m(q) > 0, \qquad \forall\, k \in \big[0, |\tau| - 1\big]$$

with $q(k)$ the state for $t \in I_k$, $\sigma(k)$ the input at $t = t'_k$, $\psi(k)$ the output at $t = t_k$ ($\psi(0) = \epsilon$). Roughly speaking, The minimum dwell time for $\mathcal{H}$ is the minimum time elapsed between two consecutive transitions, namely the minimum time of permanence in a given state q of $\mathcal{H}$.

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

B. Observer's Construction

The output sequences $\psi_1\psi_2\cdots\psi_k$ of $\mathcal{H}$ can be used to determine the current discrete state q, possibly at intermittent time instants (i.e. not at each time instant).

In [16], observability in the case of partial output observability was defined. A procedure was proposed for the construction of a finite state machine $\mathcal{O}$ that, under appropriate conditions, can provide intermittent observation of the discrete state of $\mathcal{H}$. In ATM, an intermittent detection of the discrete state is not acceptable because of the need of observing "hazardous states immediately. By the same token, K–current–state observability, presented in [1], is not suitable for ATM as well.

Nevertheless, an observer that gives an estimate of the discrete state of $\mathcal{H}$ will be the starting point of our developments. For this reason, we first present such an observer. The procedure for the construction of a (discrete) state observer

$$\mathcal{O} = \Big\{\hat Q, \hat\Psi, \hat\delta, \hat q_0, \hat\phi, \hat\eta\Big\} \tag{3}$$

for $\mathcal{H}$ is rather standard, although it is different from those given in [16] and [1], and is based on the iterative construction of the state transition function $\hat\delta\colon \hat Q\times\hat\Psi\to\hat Q$ induced by the function δ as follows

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

where $\hat\Psi = \Psi\setminus\{\epsilon\}$ is the set of inputs (the outputs of $\mathcal{H}$), and $\hat Q \subset 2^Q$ is the observer state set obtained as the set of states $\hat q$ for which $\hat\delta(\hat q,\psi)!$ for some $\psi\in\hat\Psi$. The initial state of the observer is

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

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

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

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

Roughly speaking, the function $\hat\delta$ is defined for each pair $(\hat q,\psi)$ such that there exist at least a state $\bar q\in\hat q$ and a transition from $\bar q$ to q, given by a sequence $\sigma s_k = \sigma\sigma_1\cdots\sigma_k$, such that the resulting output is ψ.

The observer $\mathcal{O}$ can be used to solve the following *observation problem.*

Definition 1. *Given a hybrid system $\mathcal{H}$, the system $\mathcal{O}$ is said to be an observer for the discrete states of $\mathcal{H}$ if there exists an integer K such that*

$$\hat q(k) = \{\bar q\} \qquad \text{if } q(k) = \bar q,\ \forall k \ge K \tag{4}$$

for every initial state $(q_0,x_0)\in Q_0\times X$ of the hybrid system $\mathcal{H}$, every continuous input function u, every discrete input $s_k = \sigma_1,\cdots,\sigma_k$. □

In [1], [3], [7], [8] conditions are given to characterize such an observer. Alternatively, one can give a characterization in terms of invariance and attractiveness [6].

Definition 2. *A set $\emptyset\ne\tilde Q\subseteq\hat Q$ is invariant with respect to a function $\tilde\delta\colon\tilde Q\times\tilde\Psi\to\tilde Q$, $\tilde\Psi\subseteq\hat\Psi$, if $\tilde\delta(\tilde q,\psi)\in\tilde Q$ for all $\tilde q\in\tilde Q$ and $\psi\in\tilde\Psi$ such that $\tilde\delta(\tilde q,\psi)!$.* □

Definition 3. *A set $\emptyset \neq \tilde{Q} \subseteq \hat{Q}$ is attractive with respect to a function $\tilde{\delta}: \tilde{Q} \times \tilde{\Psi} \to \tilde{Q}$, $\tilde{\Psi} \subseteq \bar{\Psi}$, if for all $\tilde{q} \notin \tilde{Q}$ there exists a $p \in \tilde{\Psi}^*$ with length $|p| < \infty$ such that $\tilde{\delta}(\tilde{q}, p) \in \tilde{Q}$.* □

Proposition 1. *Let $\tilde{Q}_1 = \hat{Q}_1 \cap \hat{Q} \neq \emptyset$, with*

$$\hat{Q}_1 := \Big\{ \hat{q} = \{q\},\ \forall q \in Q \Big\}. \tag{5}$$

$\mathcal{O}$ is an observer for the discrete states of $\mathcal{H}$ if and only if $\tilde{Q}_1$ is invariant and attractive with respect to the dynamics of $\hat{\delta}$. □

Proof. Let $\mathcal{O}$ be an observer. Since, according to (4), for any $q_0 \in Q_0$, if $q(k) = \bar{q} \in \delta(q_0, s)$, $\forall\, s \in \Sigma^*$, one has

$$\hat{q}(k) = \hat{\delta}(\hat{q}_0, \eta(q_0, s, \bar{q})) = \{\bar{q}\} \in \tilde{Q}_1, \quad \forall\, k \geq K$$

i.e. $\forall\, p = \eta(q_0, s, \bar{q})$ with $|p| \leq k$ generated by $\mathcal{H}$

$$\hat{\delta}(\hat{q}_0, p) \in \tilde{Q}_1.$$

Hence $\tilde{Q}_1$ must be attractive. Moreover, again from (4), one need that

$$\hat{\delta}(\{\bar{q}\}, \eta(\bar{q}, s, q')) \in \tilde{Q}_1, \qquad \forall\, s \in \Sigma^*$$

$q' \in \delta(\bar{q}, s)!$, namely $\tilde{Q}_1$ must be invariant.

Conversely, if $\tilde{Q}_1$ is attractive and invariant (4) must hold true for a finite K. □

The conditions above are quite intuitive: the first one requires that $\mathcal{O}$ has a state set including some of the singleton states of Q, and that the discrete event dynamics do not bring the state out of this set $\hat{Q}_1 \cap \hat{Q}$ of singletons; the second one requires that all the evolutions go inside this set. These conditions are necessary and sufficient for determining, after a transient, the exact discrete state of $\mathcal{H}$.

C. Extra Information to Recover Observability

When the conditions given in Proposition 1 are violated, it is not possible to determine the discrete state of $\mathcal{H}$ for k greater than a certain positive integer K, at least with a pure discrete event–driven observer. This is due to the fact that either an invariant set $\tilde{Q}$ does not exist, namely $\hat{\delta}$ drives to a state $\hat{q} = \{q_{i_1}, \cdots, q_{i_r}\}$ with cardinality greater than 1, or this set $\tilde{Q}$ is not attractive.

One way to recover from these cases is to exploit the knowledge coming from the continuous dynamics to create further discrete signals (called "signatures"), as proposed in [1], which provide additional information to discriminate the discrete locations. Clearly, this extra information must be "rich enough" to determine an observer.

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 [1] as follows: appropriate Luenberger's observers are designed for each of the continuous dynamics (1). Then, the signatures $\bar{\psi}_1, \cdots, \bar{\psi}_s$ are obtained by feeding the observer outputs into a decision function block. In [1], it is shown how the observer's gains have to be chosen so that the signatures are generated within a finite and fixed time, namely the minimum dwell–time. Each label $\bar{\psi} \in \bar{\Psi} = \{\bar{\psi}_1, \cdots, \bar{\psi}_s\}$ is characteristics of a specific location q and is added as output to the arcs entering q. Hereinafter, we will consider an alternative way to associate $\bar{\psi}$ to $\mathcal{H}$.

III. Critical Observers

As already pointed out, the notion of observability introduced in the previous section does not capture the urgency of a dangerous situation that may be created by an error in an ATM system. In this case, we need to identify the states corresponding to these errors immediately, i.e., K must be 0. This will be accomplished using the recalled signature generation mechanism.

Our point of view on the signature generation mechanism is slightly different from [1]: instead of associating signatures to the transitions, we associate to each state $q \in Q$ an additional output value $\bar{\psi} = h(q) \in \bar{\Psi}$ depending on the state q and we suppose that $\bar{\psi}$ is generated within the minimum dwell–time $\Delta_m(q)$. In this way the generation dynamics is "hidden" inside the delay necessary to generate $\bar{\psi} = h(q)$, and we can neglect the signatures generator dynamics. Note that in general $h: Q \to \bar{\Psi}$ is a partial function. The signals $h(q)$ can be used to modify the observer $\mathcal{O}$ introduced in (3).

Let us now define $q_c \in Q$ a *critical state* for $\mathcal{H}$ if it corresponds to a hazardous operation. Let Q_c be the set of critical states for $\mathcal{H}$. A critical state for $\mathcal{H}$ induces the notion of *critical states for the observer* $\mathcal{O}$ as follows. Consider the system $\mathcal{O}$ defined in (3). We recall that each discrete state $\hat{q} \in \hat{Q} \subseteq 2^Q$ of $\mathcal{O}$ is a non–empty set of states $q_{j_1}, \cdots, q_{j_r}$ of $\mathcal{H}$, and we can define its cardinality $|\hat{q}| = r$.

Definition 4. *A state $\hat{q} \in \hat{Q}$, with cardinality is $|\hat{q}| > 1$, is critical for $\mathcal{O}$ if $\hat{q} \cap Q_c \neq \emptyset$.* □

The critical states $\hat{q}_c \in \hat{Q}_c$ can be refined, i.e. partitioned, by means of the values $h(\bar{q})$, $\bar{q} \in \hat{q}_c$. Defining as refinement

$$\hat{q}_c|_{h(\bar{q})} \subseteq \hat{q}_c, \qquad \bar{q} \in \hat{q}_c$$

the subset of states $\bar{q}$ of $\hat{q}_c$ with associated the value $h(\bar{q})$, with obviously

$$\bigcup_{\bar{q} \in \hat{q}} \hat{q}_c|_{h(\bar{q})} = \hat{q}_c$$

starting from the observer $\mathcal{O}$ one can define a new system $\hat{\mathcal{O}}$ where the state transition function, the state set, etc., can be defined as follows.

Algorithm 1. *Let us determine $\mathcal{O}$ as in (3).*

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

Let $\hat{\mathcal{O}}$ be the obtained system. □

A more formal definition of $\hat{\mathcal{O}}$ is obvious and is therefore omitted. Nevertheless, note that since the events $\bar{\psi} = h(q)!$ are considered as new input events for $\hat{\mathcal{O}}$, the hybrid time basis is refined because some intervals I_k may be given by $I_k = I_{1,k} \cup I_{2,k}$, with $I_{1,k} = [t_k, t_k + \rho_k)$, $I_{2,k} = [t_k + \rho_k, t'_k)$, and with $\bar{\psi}(k)$ generated at time $t_k + \rho_k$, where $\rho_k \leq \Delta_m(q)$. If $h(q)$ is not defined, then this means that $\rho_k \geq t'_k - t_k \geq \Delta_m(q)$, i.e. I_k is not refined. With some abuse of notation, we let $\hat{q}(I)$ be the value of $\hat{q}$ for $t \in I$. With this in mind, consider the following.

Definition 5. *Given a hybrid system $\mathcal{H}$ and a subset $Q_c \subseteq Q$, the system $\hat{\mathcal{O}}$ is said to be a* critical observer *for $\mathcal{H}$ with respect to the set of states Q_c if*

$$\hat{q}(I_k^\varepsilon) = \{\bar{q}\} \qquad \forall\, \bar{q} \in Q_c, \quad \forall\, k\colon q(k) = \bar{q} \tag{6}$$

with

$$I_k^\varepsilon = [t'_k - \varepsilon, t'_k), \qquad \text{for some } \varepsilon > 0$$

for every initial state $(q_0, x_0) \in Q \times X$ of the hybrid system $\mathcal{H}$, every continuous input function u, every discrete input $s_k = \sigma_1, \cdots, \sigma_k$. □

It is clear that an observer ensuring K–current state observability with $K = 0$, or 0–current state observer for short, is also a critical observer since

$$\hat{q}(k) = \{\bar{q}\} \qquad \text{if } q(k) = \bar{q},\ \forall k\ \geq 0.$$

However, a critical observer is not in general a 0–current state observer, and therefore represents a generalization of the 0–current state observer. In fact, according to Proposition 1, the attractiveness of $\tilde{Q}_1$ is a necessary condition, while it is not necessary for a critical observer.

Let us determine when the observer (3) is also a critical observer.

Proposition 2. *The observer (3) is a critical observer for $\mathcal{H}$ if and only if*

$$\hat{Q}_c \subseteq \hat{Q}_1$$

with $\hat{Q}_1$ defined as in (5). □

Proof. If (3) is a critical observer, (6) is valid. Since $\rho_k \geq t'_k - t_k$, it is necessary that (6) is valid with $I_k^\varepsilon = I_k$. This implies that $\hat{Q}_c \subseteq \hat{Q}_1$. On the contrary, if $\hat{Q}_c \subseteq \hat{Q}_1$ then (6) is valid with $I_k^\varepsilon = I_k$, i.e. (3) is a critical observer. □

When Proposition 2 is violated (3) is not a critical observer. The following proposition gives a condition under which Algorithm 1 gives a system $\hat{\mathcal{O}}$ that is a critical observer for $\mathcal{H}$.

Proposition 3. *$\hat{\mathcal{O}}$ is a critical observer for $\mathcal{H}$ with respect to a set $Q_c \subset Q$ if and only if for each induced critical state $\hat{q}_c \in \hat{Q}_c$*

$$\left|\hat{q}_c|_{h(\bar{q})}\right| = \begin{cases} 1 & \text{if } \bar{q} \in \hat{q}_c \cap Q_c \\ C \geq 1 & \text{if } \bar{q} \in \hat{q}_c \backslash \left(\hat{q}_c \cap Q_c\right) \end{cases} \tag{7}$$

for the refinements induced by h. □

Proof. If (7) holds, then (6) is valid for $I_k^\varepsilon = I_{2,k}$, and $\hat{\mathcal{O}}$ is critical for $\mathcal{H}$. Conversely, if $\hat{\mathcal{O}}$ is critical for $\mathcal{H}$ (6) and hence (7) holds. □

According to Proposition 3, there is an infinite number of functions $h\colon Q \to \bar{\Psi}$ that satisfy (7). In particular, one is interested in the following design problem: determine h such that the number of refined states for each $\hat{q}_c \in \hat{Q}_c$ is minimum. This allows to consider "nonzero" signatures only when it is strictly necessary for the design of the observer. The criterium used to determine such a function h will be the violation of Proposition 3.

Proposition 4. *Given an observer $\mathcal{O}$ as in (3), Algorithm 1 gives a critical observer $\hat{\mathcal{O}}$ for $\mathcal{H}$ with respect to a set $Q_c \subset Q$ if and only if there exists a function $h\colon Q \to \bar{\Psi}$ such that for each critical state $\hat{q}_c \in \hat{Q}_c$ (7) holds true with*

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

Proof. Straightforward. □

IV. A Case Study: the Active Runway Crossing System

In this section, we consider the example proposed in [19] and [12], and analyzed in [6], of an active runway crossing with the intent of testing the applicability of the theoretical results on critical 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 1).

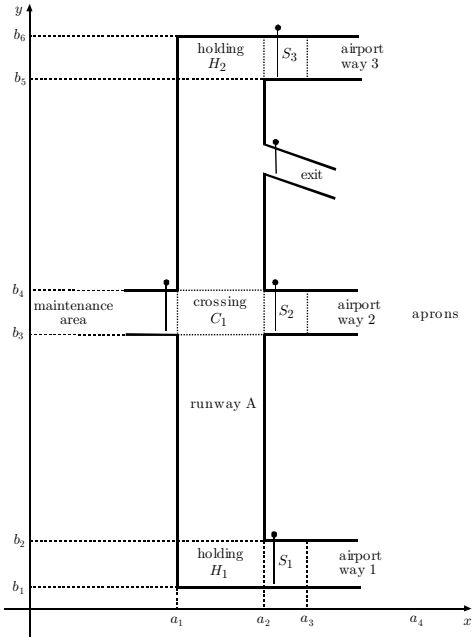

Fig. 1. Airport configuration

The following relevant areas can be defined

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

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*) [9], [19]. 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.* [19] define an *agent* as an entity, such as a human operator or a technical system, characterized by its *SA* of the environment. Following [19], *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.

A. 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 aircrafts 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 observed or in reaction to an emergency braking command by the controller the P_t starts a braking action and so 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, he may have the *intent SA* that the next AW 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 to 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.

B. Pilot flying observation problem

The agent P_t can be modelled as a hybrid system $\mathcal{H}_{P_t}$, see Figure 2 [5], [6]. Referring the reader to [6] for the complete description of $\mathcal{H}_{P_t}$, here we just note that the input $\sigma_{1,1}$ 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. Moreover, the output $\psi_{1,1}$ denotes 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. Note the null output ϵ corresponding to $\sigma_{1,6}$, $\sigma_{1,7}$ due to situation awareness errors.

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

Propositions 3 or 4 can be used to determine a critical observer for $\mathcal{H}_{P_t}$. In particular, using Proposition 4, one sees that if $s_1 \in \Omega_{RW_A}$ a signature $r_{1,1} = h(q_{1,7})$ is generated to distinguish $q_{1,7}$, one gets the critical observer $\hat{\mathcal{O}}_{P_t}$, see Figure 4. This shows how we can solve the critical observation problem for P_t.

More complicated critical observation problems, involving the two pilots acting together (or even, more generally, the other agents C_g, C_t, ATS) can be formalized considering the shuffle product of $\mathcal{H}_{P_t}$ and $\mathcal{H}_{P_c}$ [11], and determining the induced critical states on this new system $\mathcal{H}$ (see [6]).

V. Conclusions

We introduced the notion of critical observability for hybrid systems to solve the problem of error propaga-

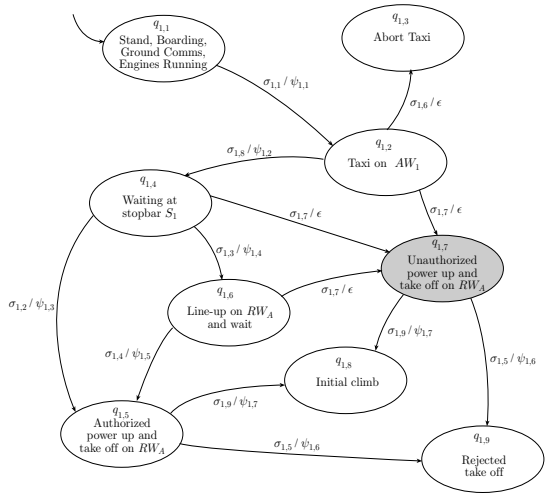

Fig. 2. Hybrid system $\mathcal{H}_{P_t}$ modelling P_t

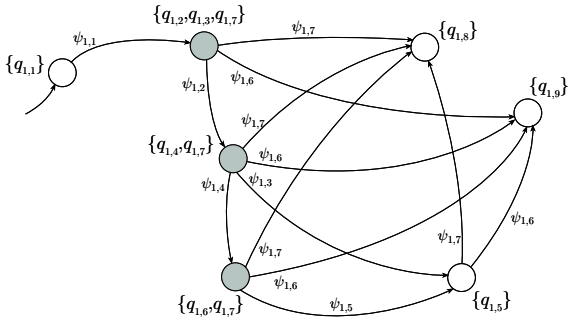

Fig. 3. Observer $\mathcal{O}_{P_t}$

tion control in Air Traffic Management. In particular, we gave conditions for the existence of a hybrid observer for critical states corresponding to hazardous situations. We demonstrated the use of critical observability in the runway crossing problem where human agents interact in a system consisting of various subsystems. The human agents, modelled as hybrid systems, are subject to errors that may lead to catastrophic situations. We developed hybrid observers to detect the hazardous situations corresponding to critical states.

The results seem to be easily obtainable by intuition. Indeed, in this particular example, an intuitive design would have solved the problem. However, errors that we try to prevent often originate from interactions among distributed systems that, albeit simple, can create risky situations that are difficult to discern without the help of automation. Several failures of complex systems can be traced back to unforeseen circumstances that are trivial to analyze after they become visible. We are now investigating some more complex ATM cases to demonstrate how difficult it is to enumerate the corner cases of real applications.

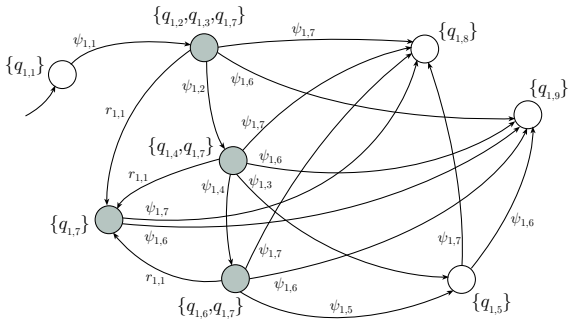

Fig. 4. Critical observer $\hat{\mathcal{O}}_{P_t}$

ACKNOWLEDGEMENTS

The authors thank Henk Blom (NLR), Ted Lewis (BAE Systems) and Derek Jordan (BAE Systems) for the suggestions received on the runway crossing problem. In particular, the authors are grateful to Ted Lewis and Derek Jordan who provided the scenario, relying on the UK Radio Telephony (RT) procedures CAP 413(2002).

REFERENCES

[1] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, A. L. Sangiovanni–Vincentelli, Design of Observers for Hybrid Systems, In Claire J. Tomlin and Mark R. Greenstreet, Editors, *Hybrid Systems: Computation and Control*, Vol. 2289 of Lecture Notes in Computer Science, pp. 76–89, Springer-Verlag, Berlin Heidelberg New York, 2002.

[2] 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.

[3] M. Cüneyt, C.M. Özveren and A.S. Willsky, Stability and Stabilizability of Discrete Event Dynamic Systems, *Journal of the Association for Computing Machinery*, Vol. 38, No. 3, pp. 730–752, July 1991.

[4] 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.

[5] 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.

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

[7] S. Di Gennaro, Nested Observers for Hybrid Systems, *Proceedings of the Latin–American Conference on Automatic Control CLCA 2002*, Guadalajara, México, December 3–6, 2002.

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

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

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

[11] J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages and Computation*, Addison–Wesley, Reading, MA, 1979.

[12] T. Lewis, D. Jordan, Personal communication, BAE Systems, 2004.

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

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

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

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

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

[18] 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.

[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/