Safety Criticality Analysis of Air Traffic Management Systems: A Compositional Bisimulation Approach

Elena De Santis, Maria Domenica Di Benedetto,
Davide Pezzuti, Giordano Pola and Luca Scarciolla
Department of Information Engineering, Computer Science and Mathematics,
Center of Excellence DEWS, University of L'Aquila, 67100, L'Aquila, Italy
Email: {elena.desantis,mariadomenica.dibenedetto,giordano.pola}@univaq.it,
davide.pezzuti@graduate.univaq.it,lucascarciolla@hotmail.com

Mariken Everdij
National Aerospace Laboratory NLR,
P.O. Box 90502, 1006 BM,
Amsterdam, The Netherlands
Email: mariken.everdij@nlr-atsi.nl

***Abstract*—Detecting safety critical situations that may arise in the evolution of Air Traffic Management (ATM) systems is of primary importance in the analysis of their behavior. The inherent complexity of ATM systems, typically involving a large number of agents, makes this analysis prohibitive today. Compositionality has been an effective way of tackling this problem. We present a compositional framework to accurately describe the behavior of the agents operating in ATM scenarios and of their interaction. We then expose some results that reduce the computational effort required in detecting safety critical situations. Benefits from the use of this approach are illustrated on a future Terminal Manoeuvring Area operation design.**

I. Introduction

The increasing in the volume of air traffic that is expected in the close future requires re–design of existing traffic flow worldwide. To this purpose researchers in the area of Air Traffic Management (ATM) systems are actually proposing new procedures with the aim of increasing capacity while preserving safety. Ensuring safety in ATM systems is a tough problem especially because the number of agents involved is large. Nowadays, several disciplines are being used to assist ATM experts in the design of robust novel procedures. Among some scientific disciplines, Resilience Engineering [14], [13], [21] deals with the design of efficient joint cognitive systems, as ATM systems are, both in nominal and non-nominal conditions. Since ATM joint cognitive systems are complex, resilience engineering in this regard is at an early stage of development. Formal mathematical models and analysis methods offer a key complementary approach that is needed to render resilience engineering effectively applicable to complex joint cognitive systems, such as ATM systems. This is the main goal of the project Mathematical Approach towards Resilience Engineering in ATM (MAREA) [2]. A research issue of the MAREA project is the *safety criticality analysis* of novel procedures within the new SESAR 2020 concept of operation. In this paper we approach the modeling and analysis of safety critical situations by using the notion of critical observability as introduced and studied in [7], [16]. Critical observability is a structural property of hybrid systems, that corresponds to the possibility of detecting if the current state of a hybrid system is in a set of critical states, representing unsafe, forbidden or non–nominal situations. This approach has been investigated before in [6], [17], [10], [22]. More specifically, in [6] a hybrid system framework has been proposed to model and analyze situation awareness inconsistencies in the Airborne Separation In–Trail Procedure. In [17], formal verification of the Airborne Separation In–Trail Procedure [19] has been carried out with software toolbox UPPAAL [15]. A limitation of [6] is that the different agents acting in ATM scenarios are considered as isolated systems. This assumption is particularly worrisome because agents' interaction may play a role in the occurrence of unsafe situations that cannot be captured when considering different agents in isolation. For this reason, we proposed in [22], [10] a compositional hybrid-system framework that provides a formal model of the agents and *of their interaction* as well. The proposed compositional hybrid systems framework has been successfully applied to the analysis of the ASAS Lateral Crossing Procedure in [10] and the Airborne Separation In–Trail Procedure in [22]. Building on the results established in [22], [10], we proposed in [23] a novel class of non–flat systems [4], [3] termed Arenas of Finite State Machines (AFSMs). AFSMs are a collection of finite state machines that interact concurrently through a communication network.

In this paper we propose an approach to the analysis of safety criticality in large–scale complex ATM systems which is based on a generalization of the results reported in [23]. The AFSM mathematical framework is shown to be appropriate in describing the behavior of each agent in an ATM system in both nominal and non–nominal conditions of operation and in describing their interaction. Moreover, this formalism provides a homogeneous representation of the diverse agents acting in the scenario. By generalizing the notion of compositional bisimulation in [23] we propose a method to the safety criticality analysis of complex ATM systems. The proposed approach is illustrated in the analysis of a future Terminal Manoeuvring Area operation [11], [18], which is a case study exhibiting most of the key features arising in the novel SESAR 2020 Concept of Operations.

This paper is organized as follows. In Section II we describe the TMA operation considered. In Section III we introduce the mathematical framework. In Section IV we model and analyse the TMA operation considered. Finally Section V offers some concluding remarks.

II. Terminal Manoeuvring Area T1 Operation

In this paper we consider the Terminal Manoeuvring Area (TMA) T1 operation that has been selected within the project MAREA as a benchmark to describe key features arising in the novel SESAR 2020 concept of operation [1]. For a detailed description of this scenario the interested reader is referred to [11], [9] and the references therein. We only mention here that the TMA T1 operation considers a busy TMA in which all aircraft fly according to Reference Business Trajectories (RBT), which allow pilots to follow their assigned trajectories with a sensible reduction of tactical controller interventions. The RBTs are typically Standard Instrument Departure (SID) routes, Standard Terminal Arrival Routes (STAR) and also cruise routes at a lower flight level. To allow for a significant capacity increase, in the TMA T1 operation, the minimum spacing between (the centerlines of) the SIDs, STARs and cruise routes has been reduced to 5 Nautical Miles (NM). The radar separation minimum is as today, i.e. 3NM laterally and 1000 feet vertically. In this context we identify five types of agents: *Aircraft*, *Aircraft crew*, including their actions, performance and situation awareness, *Cockpit Human Machine Interface (Cockpit HMI)* for each aircraft, *Tactical controller*, including his/her actions, performance and situation awareness, and *Air traffic Controller Human Machine Interface (ATCo HMI) system*, including all technical equipments of the air traffic controller. The interaction among the aforementioned agents is depicted in Figure 1.

The evolution of the TMA T1 operation can be subject to a number of hazards that could cause unsafe and/or unallowed operations. In this paper we consider a number of hazards that have been selected from [24], as relevant in the SESAR 2020 concept of operation. More specifically:

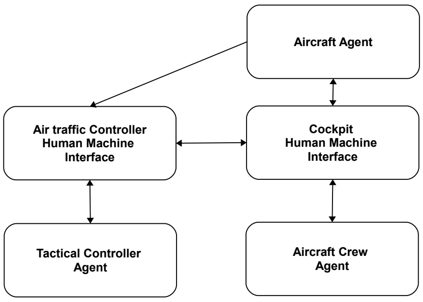
Aircraft Agent
Air traffic Controller Human Machine Interface
Cockpit Human Machine Interface
Tactical Controller Agent
Aircraft Crew Agent

Fig. 1. Interaction among agents in TMA T1 scenario.

- *Failure of Flight Management System (FMS)* (hazard[1] no. 19). Failure of FMS is immediately obvious, through multiple indications on the flight deck. The impact is high workload. To deal with the situation, the pilot would revert to conventional navigation (VOR/DME), and inform the controller and request radar vectors.
- *Failure of cockpit display and failure of the Controller Pilot Data Link Connection (CPDLC)* (hazards no. 5, 63, 115 and 137). In this context, one of the effects could be that the pilots would not get an alert of a deviation from their RBT, not even through an ATCo HMI message by CPDLC. It could also lead to the pilots losing situation awareness, which could lead to the pilots making mistakes, or performing their tasks with a delay.
- *False alert of an airborne system* (hazard no. 21). If the pilots get a false alert from the airborne system, for example an alert that they deviated from their RBT even though they are still on their RBT, then this could lead to pilots having wrong situation awareness. It could even lead to pilots taking a control action while they should not, or making mistakes, or performing their tasks with a delay. If false alerts happen often, the pilots would ultimately lose trust in the system and second-guess all alerts, even the correct ones, thus performing their tasks with a delay.
- *Short Term Conflict Alert (STCA) or conflict alert is underestimated or ignored by the ATCo* (hazards no. 254, 322 and 326). In this particular case, the controller can become aware of the problem with delay through other devices of the ATCo HMI or colleagues could warn him about the problem. Then, the ATCo will communicate the control instructions to the crew. The delay between the STCA alarm and the awareness of the alarm by the controller may cause the pilots involved not getting instructions to recover from the conflict, or they would get these instructions with a delay. Eventually, the aircraft could even collide.
- *Misunderstanding of controller instruction by pilot* (hazard no. 292). The ATCo sends, through radio communication, control directions to the pilot. The pilot answers immediately, because such information could lead to urgent change of direction. The pilot gets the information communicated by the controller and executes it. The hazard can occur when the pilot misreads the instruction, without realizing that it is wrong, and executes it. In this case, the controller could detect, for example through the radar display, that the aircraft is going off course and then re-contacts the pilot to resolve the conflict. Alternatively, the pilot could realize that he misunderstood and request a new communication from the ATCo to get control instructions.

[1] Numbering of hazards has been taken from [24].

III. Mathematical framework

In this paper we model agents acting in ATM systems by means of finite state machines.

Definition 3.1: [20] A Finite State Machine (FSM) is a tuple $M = (Q, q_0, \Sigma, \Psi, \eta, E)$, where Q is a finite set of states, $q_0 \in Q$ is an initial state, Σ is a finite set of input symbols, Ψ is a finite set of output symbols, $\eta : Q \to 2^{\Psi}$ is an output map and $E \subseteq Q \times 2^{\Sigma} \times Q$ is a transition relation.

We model interaction of agents in ATM systems by the notion of Arenas of Finite State Machines (AFSMs) [23]. AFSMs are a collection of FSMs that interact concurrently through a communication network. More formally, an AFSM is specified by a directed graph

$$\mathbb{A} = (\mathbb{V}, \mathbb{E}),$$

where:

- $\mathbb{V}$ is a collection of N FSMs M_i $(i = 1, 2, ..., N)$;
- $\mathbb{E} \subseteq \mathbb{V} \times \mathbb{V}$ describes the communication network of the FSMs M_i.

By expanding each vertex $M_i \in \mathbb{V}$ of $\mathbb{A}$ an ordinary FSM is obtained, which is denoted by $\mathbb{M}(\mathbb{A})$, see [23] for details. In this paper we are interested in detecting possible unsafe and/or non-nominal operations of agents acting in ATM systems, including those operations caused by the hazards described in the previous section. The formal tool that we use to detect these operation is the notion of critical observability [7], [16]. Given an FSM M, let $\mathfrak{R}_c \subset Q$ be the set of *critical states* of M corresponding to unsafe or non-nominal actions of M. We say that M is $\mathfrak{R}_c$–critically observable if it is possible to construct a system that is able to detect whether the current discrete state of M belongs to $\mathfrak{R}_c$ or not on the basis of the observations. Given a FSM M, we refer to a $\mathfrak{R}_c$–critical observer of M as an FSM $\mathcal{O} = (\hat{Q}, \hat{Q}_0, \hat{\Sigma}, \hat{\Psi}, \hat{\eta}, \hat{E})$, where $\hat{Q} \subseteq 2^Q$ is a set of states, $\hat{Q}_0 \subseteq \hat{Q}$ is a set of initial states, $\hat{\Sigma} = \Psi$ is a set of inputs, $\hat{\Psi} = \{0, 1\}$ is a set of outputs, $\hat{\eta} : \hat{Q} \to \{0, 1\}$ is an output function such that $\hat{\eta}(q) = 1$ if $q \subseteq \mathfrak{R}_c$, and $\hat{\eta}(q) = 0$ if $q \cap \mathfrak{R}_c = \varnothing$, and $\hat{E} \subseteq \hat{Q} \times 2^{\hat{\Sigma}} \times \hat{Q}$ is a transition relation. The construction of such observers is rather standard within the community of discrete event systems, see e.g. [5] for details.

Definition 3.2: FSM M is said to be $\mathfrak{R}_c$–critically observable if an $\mathfrak{R}_c$–critical observer $\mathcal{O}_{\mathfrak{R}_c}$ exists.

The notion of critical observability of FSMs naturally generalizes to AFSMs, as follows. Given an AFSM $\mathbb{A} = (\mathbb{V}, \mathbb{E})$, consider the tuple $\mathfrak{R}_c = (\mathfrak{R}_c^1, \mathfrak{R}_c^2, ..., \mathfrak{R}_c^N)$, where $\mathfrak{R}_c^1$ is the collection of sets $\mathfrak{R}_{i_1} \subseteq Q_{i_1}$ $(i_1 = 1, 2, ..., N)$ of critical states for M_{i_1}, $\mathfrak{R}_c^2$ is the collection of sets $\mathfrak{R}_{i_1,i_2} \subseteq Q_{i_1} \times Q_{i_2}$ $(i_1, i_2 = 1, 2, ..., N)$ of critical states arising from the interaction of M_{i_1} and M_{i_2}, ..., $\mathfrak{R}_c^N$ is the collection of sets $\mathfrak{R}_{1,2,...,N} \subseteq Q_1 \times Q_2 \times \ldots \times Q_N$ of critical states arising from the interaction of M_i with $i = 1, 2, ..., N$. The above critical relation involving states of FSMs naturally induces suitable critical relations $\mathcal{R}_c = (\mathcal{R}_c^2, ..., \mathcal{R}_c^N)$ on the corresponding FSMs, where $\mathcal{R}_c^2 \subseteq \mathbb{V} \times \mathbb{V}$ is such that $(M_{i_1}, M_{i_2}) \in \mathcal{R}_c^2$ if $\mathfrak{R}_{i_1,i_2} \neq \varnothing$, ..., $\mathcal{R}_c^N \subseteq \mathbb{V} \times ... \times \mathbb{V}$ is such that $(M_1, M_2, ..., M_N) \in \mathcal{R}_c^N$ if $\mathfrak{R}_{1,2,...,N} \neq \varnothing$. Checking critical observability on AFSMs is in general demanding from a computational complexity point of view because of the large number of agents involved. The notion of compositional bisimulation can be used as a tool to reduce complexity of large–scale ATM systems while preserving the critical observability property.

Definition 3.3: Consider a pair of AFSMs $\mathbb{A}^j = (\mathbb{V}^j, \mathbb{E}^j)$ of FSMs M_1^j, M_2^j, ..., $M_{N^j}^j$ $(j = 1, 2)$ and a pair of critical relations $\mathcal{R}_{cj} = (\mathcal{R}_{cj}^2, ..., \mathcal{R}_{cj}^{N^j})$, $j = 1, 2$. A relation $\mathbb{R} \subseteq \mathbb{V}^1 \times \mathbb{V}^2$ is a $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional simulation relation of $\mathbb{A}^1$ by $\mathbb{A}^2$ if for any $(M_{i_1}^1, M_{j_1}^2) \in \mathbb{R}$ the following conditions are satisfied:

(i) $M_{i_1}^1$ and $M_{j_1}^2$ are isomorphic;

(ii) existence of $(M_{i_1}^1, M_{i_2}^1) \in \mathbb{E}^1$ implies existence of $(M_{j_1}^2, M_{j_2}^2) \in \mathbb{E}^2$ such that $(M_{i_2}^1, M_{j_2}^2) \in \mathbb{R}$;

(iii) The following N conditions hold:

(iii,1) for any $M_{i_2}^1 \in \mathbb{V}^1$ such that $(M_{i_1}^1, M_{i_2}^1) \in \mathcal{R}_{c1}^2$, there exists $M_{j_2}^2 \in \mathbb{V}^2$ such that $(M_{j_1}^2, M_{j_2}^2) \in \mathcal{R}_{c2}^2$ and $(M_{i_2}^1, M_{j_2}^2) \in \mathbb{R}$;

(iii,2) for any $M_{i_2}^1, M_{i_3}^1 \in \mathbb{V}^1$ such that $(M_{i_1}^1, M_{i_2}^1, M_{i_3}^1) \in \mathcal{R}_{c1}^3$, there exist $M_{j_2}^2, M_{j_3}^2 \in \mathbb{V}^2$ such that $(M_{j_1}^2, M_{j_2}^2, M_{j_3}^2) \in \mathcal{R}_{c2}^3$, $(M_{i_2}^1, M_{j_2}^2) \in \mathbb{R}$ and $(M_{i_3}^1, M_{j_3}^2) \in \mathbb{R}$;

$\ldots$

(iii,N) for any $M_{i_2}^1, M_{i_3}^1, \ldots, M_{i_{N^1}}^1 \in \mathbb{V}^1$ such that $(M_{i_1}^1, M_{i_2}^1, \ldots, M_{i_{N^1}}^1) \in \mathcal{R}_{c1}^{N^1}$, there exist $M_{j_2}^2, M_{j_3}^2, \ldots, M_{j_{N^2}}^2 \in \mathbb{V}^2$ such that $(M_{j_1}^2, M_{j_2}^2, \ldots, M_{j_N}^2) \in \mathcal{R}_{c2}^{N^2}$ and $(M_{i_k}^1, M_{j_k}^2) \in \mathbb{R}$ for any $k = 1, ..., \min\{N^1, N^2\}$.

Relation $\mathbb{R}$ is a $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional bisimulation relation between $\mathbb{A}^1$ and $\mathbb{A}^2$ if $\mathbb{R}$ is a $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional simulation relation from $\mathbb{A}^1$ to $\mathbb{A}^2$ and $\mathbb{R}^{-1}$ is[2] a $(\mathcal{R}_{c2}, \mathcal{R}_{c1})$–compositional simulation relation from $\mathbb{A}^2$ to $\mathbb{A}^1$. AFSMs $\mathbb{A}^1$ and $\mathbb{A}^2$ are $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$-compositionally bisimilar if there exists a $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional bisimulation total[3] relation between $\mathbb{A}^1$ and $\mathbb{A}^2$.

By following the results in [23] it is possible to show under some technical assumptions that the notion of compositional bisimulation preserves the critical observability property, i.e. if AFSMs $\mathbb{A}^1$ and $\mathbb{A}^2$ are $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositionally bisimilar then $\mathbb{M}(\mathbb{A}^1)$ is $\mathfrak{R}_{c1}$–critically observable if and only if $\mathbb{M}(\mathbb{A}^2)$ is $\mathfrak{R}_{c2}$–critically observable.

The maximal $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional bisimulation relation between AFSMs $\mathbb{A}^1$ and $\mathbb{A}^2$ is an $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional bisimulation relation $\mathbb{R}^*(\mathbb{A}^1, \mathbb{A}^2)$ such that $\mathbb{R} \subseteq \mathbb{R}^*(\mathbb{A}^1, \mathbb{A}^2)$ for any $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$–compositional bisimulation relation $\mathbb{R}$ between $\mathbb{A}^1$ and $\mathbb{A}^2$. Consider an AFSM $\mathbb{A} = (\mathbb{V}, \mathbb{E})$ and a critical relation $\mathcal{R}_c$. Let $\mathbb{R}^*$ be the maximal $(\mathcal{R}_c, \mathcal{R}_c)$–compositional bisimulation relation between AFSM $\mathbb{A}$ and

[2] Symbol $\mathbb{R}^{-1}$ denotes the inverse relation of $\mathbb{R}$, i.e. $\mathbb{R}^{-1} = \{(M^2, M^1) \in \mathbb{V}^2 \times \mathbb{V}^1 | (M^1, M^2) \in \mathbb{R}\}$.

[3] A relation $\mathcal{R} \subseteq A \times B$ is said to be total if for any $a \in A$ there exists $b \in B$ such that $(a, b) \in \mathcal{R}$ and conversely, for any $b \in B$ there exists $a \in A$ such that $(a, b) \in \mathcal{R}$.

itself. Since $\mathbb{R}^*$ is an equivalence relation on the set $\mathbb{V}$ it is possible to partition $\mathbb{V}$ in the collection of sets M_k^*, called equivalence classes, such that $M_i, M_j \in M_k^*$ if and only if $(M_i, M_j) \in \mathbb{R}^*$. The quotient of $\mathbb{A}$ induced by $\mathbb{R}^*$ is the AFSM $\mathbb{A}^* = (\mathbb{V}^*, \mathbb{E}^*)$ where $\mathbb{V}^*$ is the collection of sets M_k^* and $\mathbb{E}^*$ is the collection of pairs $(M_k^*, M_{k'}^*)$ for which there exist $M_i \in M_k^*$ and $M_{i'} \in M_{k'}^*$ such that $(M_i, M_{i'}) \in \mathbb{E}$. The quotient $\mathbb{A}^*$ of $\mathbb{A}$ is the minimal (in terms of the number of the FSMs involved) $(\mathcal{R}_c, \mathcal{R}_c)$–compositionally bisimilar AFSM of $\mathbb{A}$. We denote by $\mathcal{R}_c^*$ the critical relation[4] obtained by quotienting the original critical relation $\mathcal{R}_c$ through $\mathbb{R}^*$.

IV. TMA T1 OPERATION

A. Modeling of the TMA T1 operation

In this section we use the mathematical formalism introduced in the previous section to model and analyse the TMA T1 operation. We start by providing the mathematical model of each agent acting in the scenario.

The mathematical model of the *Aircraft* is given by the following differential equation, taken from [12]:

$$\begin{cases} \dot{x_1} = x_4 \cos(x_5) \cos(x_6) \\ \dot{x_2} = x_4 \sin(x_5) \cos(x_6) \\ \dot{x_3} = x_4 \sin(x_6) \\ \dot{x_4} = \frac{1}{m} \left[u_1 \cos(\alpha) - D - mg \sin(x_6) \right] \\ \dot{x_5} = \frac{1}{m x_4} \left[L \sin(u_2) + u_1 \sin(\alpha) \sin(u_2) \right] \\ \dot{x_6} = \frac{1}{m x_4} \left[(L + u_1 \sin(\alpha)) \cos(u_2) - mg \cos(x_6) \right] \end{cases}$$

where x_1 and x_2 indicate the horizontal position, x_3 the altitude, x_4 the true airspeed, x_5 the heading angle, x_6 the angle of climb/descent, u_1 the engine thrust, u_2 the bank angle, L the lift force, D the drag force, α the angle of attack, g gravitational acceleration and m is the mass of the aircraft. As detailed in [8], an FSM M_{air} can be constructed which approximates the above differential equation with any desired precision; this step is essential in order to provide an homogeneous representation of diverse agents acting in the scenario.

In the sequel we illustrate the FSMs associated with the remaining agents acting in the TMA T1 operation. Due to lack of space we only describe the sets of states; the full model is described in detail in [8].

The FSM associated to the *Aircraft crew* agent, depicted in Figure 2, is described by $M_{crew} = (Q_{crew}, q_{0,crew}, \Sigma_{crew}, \Psi_{crew}, \eta_{crew}, E_{crew})$, with set of states $Q_{crew} = \{q_{1,crew}, \ldots, q_{13,crew}\}$, where $q_{1,crew}$ represents crew monitoring of flight according to RBT, $q_{2,crew}$, crew conflict resolution manoeuvre (In this state the situation awareness of the crew is assumed to be correct.), $q_{3,crew}$, crew updates of flight trajectory data (In this state the situation awareness of the crew is assumed to be correct.), $q_{4,crew}$, crew flight-plan deviation avoidance manoeuvre, $q_{5,crew}$, a radio communication requested by the crew, $q_{6,crew}$, crew updates of flight trajectory data (In this state the situation awareness of the crew is assumed to be incorrect with respect to his RBT. Due to heavy workload, the situation awareness of the crew may be different from the real one: the crew is not aware of a deviation from RBT when it occurs or assumes a deviation from RBT when there is none.), $q_{7,crew}$, VOR/DME navigation turned on, $q_{8,crew}$, heavy workload of the crew, $q_{9,crew}$, reception of radio communication from the ATCo, $q_{10,crew}$, wrongly implementation of a conflict resolution manoeuvre (hazard no. 292), (In this state, the situation awareness of the crew is assumed to be incorrect. Due to heavy workload, the situation awareness of the crew may be different from the real one: the pilot misinterprets the communication of control statements, and wrongly implements the maneuver.), $q_{11,crew}$, alert of a trajectory deviation not perceived, not even through an ATCo HMI message by the CPDLC (hazard no. 137) (In this state the situation awareness of the crew is assumed to be incorrect. Due to equipment malfunctioning the pilot does not realize a warning, and might experience an error of trajectory.), $q_{12,crew}$ RBT deviation alert by the airborne system, $q_{13,crew}$ cross-checking of independent sources leading to realize that it is a false alarm.

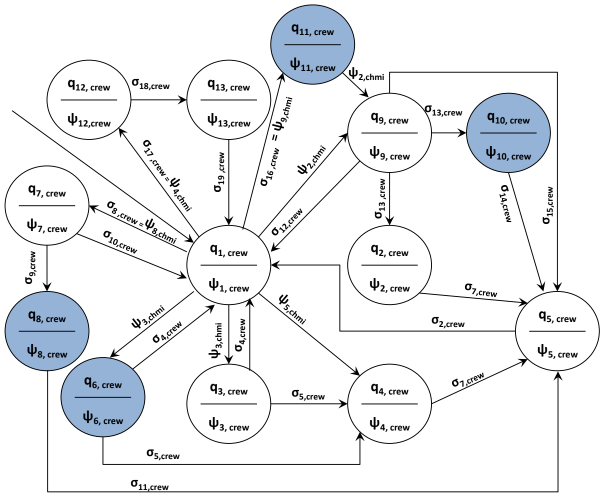

Fig. 2. FSM M_{crew} of Aircraft Crew agent.

The FSM associated to the *Tactical controller* agent, depicted in Figure 3, is described by $M_{atco} = (Q_{atco}, q_{0,atco}, \Sigma_{atco}, \Psi_{atco}, \eta_{atco}, E_{atco})$ with set of states $Q_{atco} = \{q_{1,atco}, \ldots, q_{6,atco}\}$, where $q_{1,atco}$ represents monitoring of assigned airspace (In this state the situation awareness of the ATCo is assumed to be correct.), $q_{2,atco}$, identification of a flight-plan deviation resolution manoeuvre, $q_{3,atco}$, identification of a conflict avoidance manoeuvre, $q_{4,atco}$, answer to crew radio communication, $q_{5,atco}$, radar vectors data sent to the pilot, $q_{6,atco}$, not detection of a STCA alarm (hazards no. 254, 322 and 326) (Due to high workload, the situation awareness of the ATCo may be different from the real one: the ATCo does not realize the STCA alarm and believes that he is still in the monitoring

[4] For the formal definition of the $\mathcal{R}_c^*$ we refer to [8].

state.).

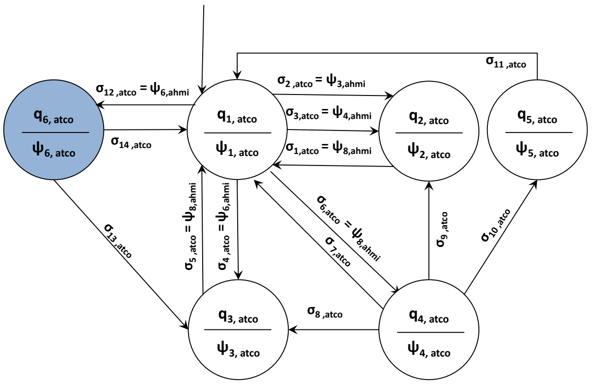

Fig. 3. FSM M_{atco} of Tactical Control agent.

The *ATCo HMI* is assumed to include also ground CPDLC and R/T communication equipment; its FSM, depicted in Figure 4, is described by $M_{ahmi} = (Q_{ahmi}, q_{0,ahmi}, \Sigma_{ahmi}, \Psi_{ahmi}, \eta_{ahmi}, E_{ahmi})$, with set of states $Q_{ahmi} = \{q_{1,ahmi}, \dots, q_{8,ahmi}\}$ where $q_{1,ahmi}$ represents monitoring of aircraft trajectory, $q_{2,ahmi}$, aircraft position and velocity acquired and comparison with planned RBT, $q_{3,ahmi}$, generation of an FPCM alarm due to a vertical deviation from RBT, $q_{4,ahmi}$, generation of an FPCM alarm due to a transversal deviation from RBT, $q_{5,ahmi}$, message to/from pilot sent/displayed through CPDLC, $q_{6,ahmi}$, generation of an STCA alarm due to a trajectory conflict, $q_{7,ahmi}$, radio communication to the crew turned on, $q_{8,ahmi}$, reception of radio communication from the crew.

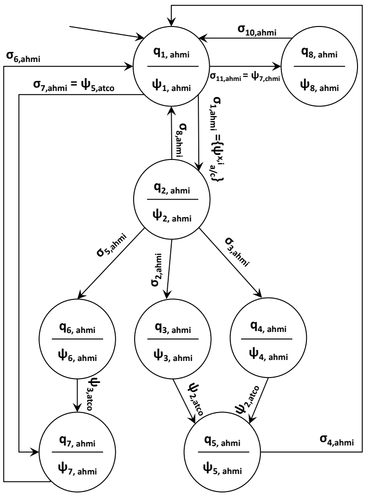

Fig. 4. FSM M_{ahmi} of ATCo HMI system agent.

The *Cockpit HMI* is assumed to include also airborne CPDLC and R/T communication equipment; its FSM, depicted in Figure 5, is described by $M_{chmi} = (Q_{chmi}, q_{0,chmi}, \Sigma_{chmi}, \Psi_{chmi}, \eta_{chmi}, E_{chmi})$, with set of states $Q_{chmi} = \{q_{1,chmi}, \dots, q_{9,chmi}\}$ where $q_{1,chmi}$ represents monitoring of current position and velocity of the aircraft, $q_{2,chmi}$, reception of radio communication from the ATCo, $q_{3,chmi}$, aircraft position and velocity acquired and displayed, $q_{4,chmi}$, false alert of airborne system (hazard no. 21), $q_{5,chmi}$, reception of an RBT deviation avoidance instruction by the controller via CPDLC, $q_{6,chmi}$, reception of a control action from the crew to the aircraft, $q_{7,chmi}$, radio communication to the ATCo turned on, $q_{8,chmi}$, FMS failure (hazard no. 19), $q_{9,chmi}$, is the state where the Cockpit HMI does not indicate display failure or display alert does not show or the CPDLC loses part of message sent by the ATCo (hazards no. 5, 63, 115).

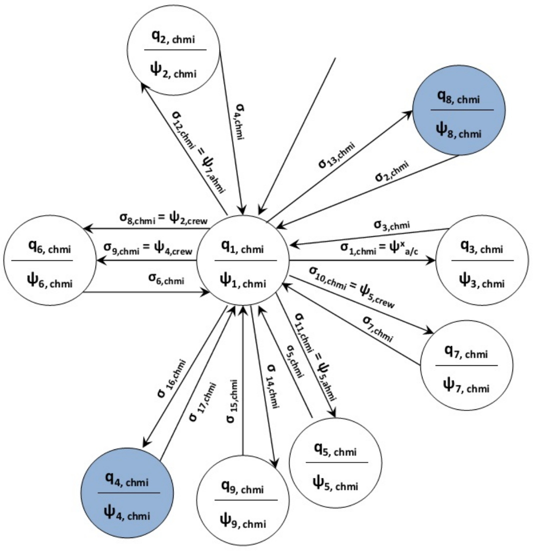

Fig. 5. FSM M_{chmi} of Cockpit HMI agent.

In the sequel we consider a scenario of TMA T1 operation involving 3 SID aircraft, 2 STAR aircraft, 3 cruise routes aircraft and 1 ATCo. This scenario is chosen for illustrative purposes; the proposed methodology can be applied to other scenarios. The communication scheme that models exchange of information among the agents involved can be described by the AFSM $\mathbb{A} = (\mathbb{V}, \mathbb{E})$ shown in Figure 6, where FSMs $M_{i,1}$, $i = 2, \dots, 9$, represent the crew (SIDs in green, STARs in red and cruise routes in blue), FSMs $M_{i,2}$, $i = 2, \dots, 9$, represent the Cockpit HMI of each aircraft-crew (SIDs in green, STARs in red and cruise routes in blue), FSM systems $M_{i,3}$, $i = 2, \dots, 9$, represent the Aircraft (SIDs in green, STARs in red and cruise routes in blue), FSM $M_{1,0}$ represents the ATCo HMI System (in white), FSM $M_{1,1}$ represents the ATCo (in orange). The notation $M_{i,j}$ is defined as follows: the first index i is associated to the i-th human agent and the index j to the j-th agent involved in the AFSM related to the i-th human agents.

We illustrate the evolution of the AFSM described above, through a simple example. Consider the flow of communication signals generated by the hazard related to failure of FMS (hazard no. 19):

- Starting from the initial state $q_{1,chmi}$ where the Cockpit HMI system is monitoring current position and velocity of the aircraft, a transition occurs to state $q_{8,chmi}$ where the Cockpit HMI system indicates FMS failure (Figure 5).
- The output $\psi_{8,chmi}$ (i.e. Cockpit HMI system indicates FMS failure) of state $q_{8,chmi}$ in the Cockpit HMI model triggers a transition in the crew agent from state $q_{1,crew}$ where the crew is monitoring the flight according to RBT to state $q_{7,crew}$ where the crew turns on the VOR/DME navigation. When in state $q_{7,crew}$ the crew can be either in absence of workload, in which case a transition occurs from state $q_{7,crew}$ to state $q_{1,crew}$ with input $\sigma_{10,crew}$ representing no high workload and returning to the monitoring state, or, in workload, in which case a transition occurs from state $q_{7,crew}$ to state $q_{8,crew}$ representing heavy workload of the crew with input $\sigma_{9,crew}$ representing high workload. In the second case, after a transition in the state $q_{5,crew}$, the pilot requires the radar vectors through a radio communication with the output $\psi_{5,crew}$ (representing the radio communication to the ATCo) and returns to the monitoring state (Figure 2).
- In the Cockpit HMI model, the output $\psi_{5,crew}$ (modeling the radio communication to the ATCo) generates a transition from $q_{1,chmi}$ to $q_{7,chmi}$ that represents the radio communication to the ATCo. (Figure 5)
- In the Aircraft model, the system sends the update data, position and velocity, to the ATCo HMI system.
- In the ATCo HMI system model, after the update of position and velocity of the aircraft $q_{2,ahmi}$, the output $\psi_{7,chmi}$ (modelling the radio communication to the ATCo) triggers a transition from $q_{1,ahmi}$ to $q_{8,ahmi}$ where the ATCo HMI system receives radio communication from the crew (Figure 4).
- In the ATCo model, the output $\psi_{8,ahmi}$ (i.e. the output indicating that the ATCo received the radio communication from the crew) leads to the state $q_{4,atco}$ where the controller answers to the radio communication of the crew. Then, the ATCo sends radar vectors data to the pilot with the output $\psi_{5,atco}$ of the state $q_{5,atco}$ and returns to the monitoring state (Figure 3).
- In the ATCo HMI system model, the output $\psi_{5,atco}$ (i.e. the output generated when the controller sends radar vectors data to the pilot) generates a transition from $q_{1,ahmi}$ to $q_{7,ahmi}$ where the ATCo HMI system turns on radio communication to the crew and return to the monitoring state (Figure 4).
- In the Cockpit HMI model, the output $\psi_{7,ahmi}$ (representing the radio communication to the crew) leads to the state $q_{2,chmi}$ where the Cockpit HMI system receives radio communication from the ATCo (Figure 5).
- In the end, in the crew agent, the output $\psi_{2,chmi}$ (i.e. the radio communication from ATCo) triggers a transition from $q_{1,crew}$ to $q_{9,crew}$ where the crew receives radio communication from the ATCo, executes them and returns to the monitoring state (Figure 2).

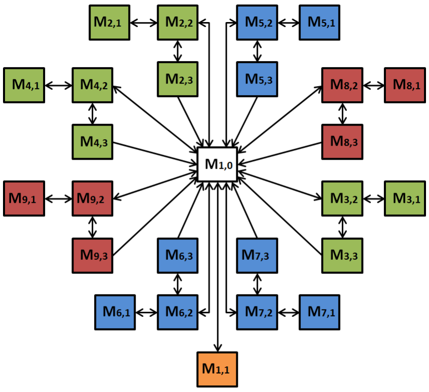

Fig. 6. AFSM $\mathbb{A}$ with 8 Aircraft, 8 Aircraft crew, 8 Cockpit HMI, 1 ATCo HMI and 1 ATCo.

B. Analysis of the TMA T1 operation

Whenever two aircraft are closer than 3NM apart in horizontal direction, while being closer than 1000ft apart in vertical direction, they are said to be in conflict. The conflicting area around each aircraft describes a cylinder in the Euclidean space. This cylinder naturally induces a critical relation among the aircraft involved: whenever two cylinders have not-empty intersection the corresponding aircraft are in conflict. This translates in considering the agents that model these aircraft as belonging to a certain critical relation. We consider the critical relation $\mathcal{R}_c = (\mathcal{R}_c^1, \mathcal{R}_c^2, \mathcal{R}_c^3)$, where:

- critical relation $\mathcal{R}_c^1$ contains the FSMs with critical states represented by the blue circles in the Figures 2, 3 and 5;
- critical relation $\mathcal{R}_c^2$ contains pairs of aircraft that are flying in each others vicinity, while they simultaneously perform a flight-plan deviation avoidance manoeuvre, or perform a conflict resolution manoeuvre, or where an aircraft performs a conflict resolution manoeuvre while the other one performs a flight-plan deviation avoidance manoeuvre, or one aircraft performs a conflict resolution manoeuvre while the other one is in the monitoring state, or one aircraft performs a flight-plan deviation avoidance manoeuvre while the other one is in the monitoring state;
- critical relation $\mathcal{R}_c^3$ contains triplets of agents, one of which is the ATCo, and two of which are aircraft flying in each other's vicinity while requiring a radio communication with the ATCo to receive instructions, but the ATCo is busy doing other activities (e.g. he is engaged in another radio communication of sending radar vectors to a third crew or he is engaged in another radio communication of manoeuvre conflict resolution),

or triplets of aircraft performing a deviation from their corresponding RBTs while flying in each other's vicinity.

We suppose that the geometry of the RBTs induces the critical relations $\mathcal{R}^2_c$ and $\mathcal{R}^3_c$, showed in Figure 7.

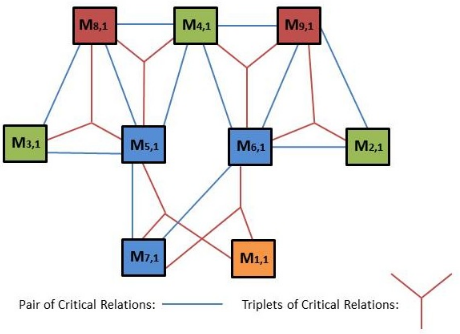

Fig. 7. Critical relations $\mathcal{R}^2_c$ and $\mathcal{R}^3_c$. A link between two FSMs M_{i_1,j_1} and M_{i_2,j_2} indicates that $(M_{i_1,j_1}, M_{i_2,j_2}) \in \mathcal{R}^2_c$. A link among three FSMs M_{i_1,j_1}, M_{i_2,j_2} and M_{i_3,j_3} indicates that $(M_{i_1,j_1}, M_{i_2,j_2}, M_{i_3,j_3}) \in \mathcal{R}^3_c$.

The size of the $\mathbb{M}(\mathbb{A})$ is very large and the construction of its critical observer is rather demanding from the computational complexity point of view. To avoid this problem we use the notion of compositional bisimulation. We computed the minimal AFSM $\mathbb{A}^*$ compositionally bisimilar to the original AFSM $\mathbb{A}$, depicted in Figure 8, and the corresponding critical relation $\mathcal{R}^*_c$, depicted in Figure 9.

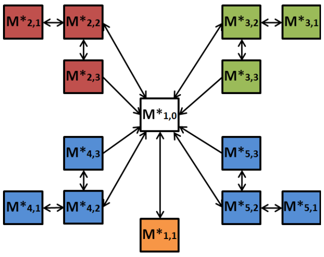

Fig. 8. Minimal AFSM $\mathbb{A}^*$.

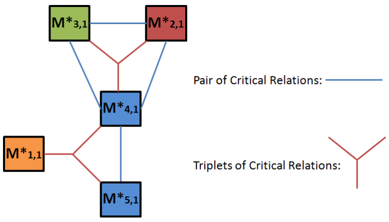

Fig. 9. Critical relation $\mathcal{R}^*_c$.

AFSM $\mathbb{A}^*$ is composed of 14 agents and critical relation $\mathcal{R}^*_c$ is composed of 6 elements (4 pairs and 2 triplets), whereas the original AFSM $\mathbb{A}$ is composed of 26 agents and the original critical relation $\mathcal{R}_c$ is composed of 8 elements (6 pairs and 2 triplets). Analysis of critical observability on the original AFSM can be then transferred to the minimal AFSM $\mathbb{A}^*$ with a consequence reduction in the computational effort. For checking critical observability we now construct the critical observers. We start by constructing an observer for the crew agents $M^*_{i,1,(i=2,3,4,5)} \in \mathcal{R}^1_c$. Critical states of $M^*_{i,1}$ are $q_{6,crew_i}, q_{8,crew_i}, q_{10,crew_i}, q_{11,crew_i}$, depicted as blue circles in Figure 2. The observer obtained is $\mathcal{O}_{crew_i} = (\hat{Q}_{crew_i}, \hat{Q}_{0,crew_i}, \hat{\Sigma}_{crew_i}, \hat{\Psi}_{crew_i}, \hat{E}_{crew_i}, \hat{\eta}_{crew_i})$, where $\hat{Q}_{crew_i} = \{\{q_{1,crew_i}, q_{11,crew_i}\}, \{q_{2,crew_i}, q_{10,crew_i}\}, \{q_{3,crew_i}, q_{6,crew_i}\}, \{q_{4,crew_i}\}, \{q_{5,crew_i}\}, \{q_{7,crew_i}\}, \{q_{8,crew_i}\}, \{q_{9,crew_i}\}, \{q_{12,crew_i}\}, \{q_{13,crew_i}\}\}$, $\hat{Q}_{0,crew_i} = \{q_{1,crew_i}\}$, $\hat{\Sigma}_{crew_i} = \Psi_{crew_i}$, $\hat{\Psi}_{crew_i} = \{0, 1\}$, $\hat{E}_{crew_i}$ and $\hat{\eta}_{crew_i}$ are depicted in Figure 10. The obtained observer $\mathcal{O}_{crew_i}$ illustrated in Figure 10, shows that $M^*_{i,1}$ is not $\{q_{6,crew_i}, q_{10,crew_i}, q_{11,crew_i}\}$–critically observable and is $\{q_{8,crew}\}$–critically observable. Indeed, for example, when the state of $\mathcal{O}_{crew_i}$ is in $\{q_{3,crew_i}, q_{6,crew_i}\}$ it is not possible to distinguish the critical state $q_{6,crew_i}$ from the non-critical state $q_{3,crew_i}$.

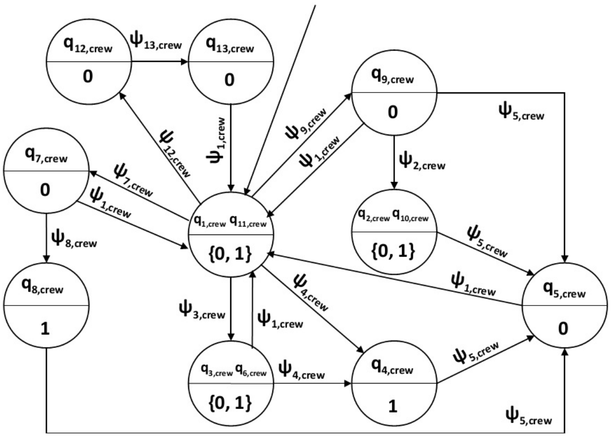

Fig. 10. Critical Observer $\mathcal{O}_{crew_i}$ for the Aircraft crew agent.

We now proceed with a further step and consider the critical relation $\mathcal{R}^2_c$. By following the results in [22], for the pair $(M^*_{i,1}, M^*_{j,1}) \in \mathcal{R}^2_c$ we need to check if $M^*_{i,1}$ is $\{q_{1,crew_i}, q_{2,crew_i}, q_{4,crew_i}\}$–critically observable and $M^*_{j,1}$ is $\{q_{1,crew_j}, q_{2,crew_j}, q_{4,crew_j}\}$–critically observable. Since the FSMs $M^*_{i,1,(i=2,\ldots,5)}$ coincide and the sets of critical situation states $\{q_{1,crew_i}, q_{2,crew_i}, q_{4,crew_i}\}$ coincide, it is sufficient to analyze critical observability of only one crew agent. By analysing critical observer $\mathcal{O}_{crew_i}$ in Figure 10, we conclude that $M^*_{i,1}$ is not critically observable with respect to the set of critical situation states $\{q_{1,crew_i}, q_{2,crew_i}\}$ and is critically observable with respect to the set of critical states $\{q_{4,crew_i}\}$. Indeed, the critical observer $\mathcal{O}_{crew_i}$ cannot distinguish the critical state $q_{2,crew_i}$ from the non-critical state $q_{1,crew_i}$. Observers for other agents can be constructed analogously. We do not report details in this regard here for lack of space; the interested reader is referred to [8]. Instead, we report hereafter the outcome of the overall analysis.

The hazards that cannot be detected on the basis of the available output signals (in the sense of critical observability) are:

- Failure of cockpit display and failure of the CPDLC (hazards no. 5, 63, 115 and 137).
- STCA or conflict alert is underestimated or ignored by the ATCo (hazards no. 254, 322 and 326).
- Misunderstanding of controller instruction by pilot (hazard no. 292).

The analysis that we performed also pointed out other safety critical situations that cannot be detected:

- Pairs of crew agents corresponding with aircraft that simultaneously perform a conflict resolution manoeuvre while flying in each other's vicinity, or where one of the aircraft performs a conflict resolution manoeuvre while the other one performs a flight-plan deviation avoidance manoeuvre while flying in each other's vicinity, or where one aircraft performs a conflict resolution manoeuvre while the other one is in the monitoring state while flying in each other's vicinity, or where one aircraft performs a flight-plan deviation avoidance manoeuvre while the other one is in the monitoring state while flying in each other's vicinity.
- Triplets of Crew agents, corresponding with three aircraft performing deviations from their corresponding RBTs while flying in each other's vicinity.

V. Conclusions

We used the notions of arenas of finite state machines and of compositional bisimulation as an effective tool for the complexity reduction in analysing safety–critical problems of large–scale ATM systems. The proposed framework has been applied to the analysis of the TMA T1 operation and interesting results were found which can assist ATM experts in rendering the TMA T1 procedure more robust with respect to (non critically observable) non-nominal operating modes.

VI. Acknowledgement

The authors thank Alessandro Petriccone, Henk Blom, and Sybert Stroeve for fruitful discussions of the topic of the present paper.

Disclaimer: This work is co-financed by the Center of Excellence DEWS and by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

References

[1] "SESAR. European Air Traffic Management Master Plan," March 2009, edition 1.

[2] "Mathematical Approach Towards Resilience Engineering in ATM (MAREA) Technical Tender Public version," March 2011.

[3] R. Alur, S. Kannan, and M. Yannakakis, "Communicating hierarchical state machines," in *Computer Science Automata, Languages and Programming*, ser. Lecture Notes in Computer Science. Springer Verlag, 1999, vol. 1644, pp. 169–178.

[4] R. Alur and M. Yannakakis, "Model checking of hierarchical state machines," *ACM Transactions on Programming Languages and Systems*, vol. 23, no. 3, pp. 273–303, 2001.

[5] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, 1999.

[6] M. Colageo and A. Di Francesco, "Composing specifications," in *ICRAT 2008 - 3rd International Conference on Research in Air Transportation, Fairfax, Virginia, USA*, June 01-04 2008.

[7] E. De Santis, M.D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, and G. Pola, "Critical observability of a class of hybrid systems and application to air traffic management," *Book Chapter of Lecture Notes on Control and Information Sciences, Springer Verlag*, 2005.

[8] E. De Santis, M.D. Di Benedetto, M. Everdij, A. Petriccone, D. Pezzuti, and G. Pola, "Final modelling and analysis of SESAR 2020 ConOps," Tech. Rep., May 2013, deliverable D4.4, MAREA.

[9] E. De Santis, M.D. Di Benedetto, A. Petriccone, D. Pezzuti, and G. Pola, "Initial modelling and analysis of SESAR 2020 ConOps," Tech. Rep., September 2012, deliverable D4.3, MAREA.

[10] E. De Santis, M.D. Di Benedetto, A. Petriccone, and G. Pola, "A compositional hybrid system approach to the analysis of air traffic management systems," in *Proc. of the 8th Innovative Research Workshop & Exhibition, EUROCONTROL, Paris, France*, December 2009.

[11] M. Everdij, H. Zmarrou, G. Bakker, and H. Blom, "D7.4 preliminary safety case – part 2 TMA T1," Tech. Rep., November 2010, http://reset.aena.es/start/frames.html.

[12] W. Glover and J. Lygeros, "A multi-aircraft model for conflict detection and resolution algorithm evaluation," Project IST-2001-32460 HYBRIDGE, Deliverable 1.3, 18 February 2004.

[13] E. Hollnagel and C. Nemeth, "Resilience engineering perspectives: Remaining sensitive to the possibility of failure." Ashgate, England, 2008, vol. 1.

[14] E. Hollnagel, D. Woods, and N. Leveson, "Resilience engineering: Concepts and precepts." Ashgate, Aldershot, England, 2006.

[15] K. G. Larsen, P. Pettersson, and W. Yi, "Uppaal in a nutshell," *International Journal on Software Tools for Technology Transfer*, vol. 1(1), pp. 134–152, December 1997.

[16] M.D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo, "Discrete state observability of hybrid systems," *International Journal of Robust and Nonlinear Control, Special Issue on Observability and Observer Design for Hybrid Systems*, vol. 19(14), pp. 1564–1580, 2008.

[17] M.D. Di Benedetto, A. D'Innocenzo, and A. Petriccone, "Automatic verification of temporal properties of air traffic management procedures using hybrid systems," in *EUROCONTROL Innovative ATM Research Workshop & Exhibition*, December 2008.

[18] M.D. Di Benedetto, A. Petriccone, and G. Pola, "Review of SESAR 2020 Conops," Tech. Rep., October 2011, deliverable D4.2, MAREA.

[19] C. Montijn, G. Graniero, and B. K. Obbink, "Qualitative Risk Assessment for ASEP-ITP," D6.1b ASSTAR Projects, 01 February 2007, v.1.0.

[20] E. Moore, "Gedanken–experiments on sequential machines," in *Annals of Mathematics Studies*, ser. Automata Studies, C. Shannon and J. McCarthy, Eds. Princeton University Press, Princeton, NJ, 1956, vol. 34, pp. 129–153.

[21] C. Nemeth, E. Hollnagel, and S. Dekker, "Resilience engineering perspectives, preparation and restoration." Ashgate, England, 2009, vol. 2.

[22] A. Petriccone, G. Pola, M.D. Di Benedetto, and E. De Santis, "A complexity reduction approach to the detection of safety critical situations in air traffic management systems," in *Proceedings of the 49th Conference on Decision and Control, Atlanta, USA*, December 2010, pp. 2081–2085.

[23] G. Pola, M. Di Benedetto, and E. De Santis, "Arenas of finite state machines," *Technical Report*, June 2011, available online at arXiv:1106.0342v1.

[24] S. Stroeve, M. Everdij, and H. Blom, "Hazards in ATM: model constructs, coverage and human responses," Tech. Rep., July 2011, deliverable D1.2, MAREA.