Formal Analysis of the Operational Concept for the Small Aircraft Transportation System

César Muñoz[1], Víctor Carreño[2], and Gilles Dowek[3]

[1] National Institute of Aerospace, 100 Exploration Way, Hampton VA 23666, USA
munoz@nianet.org
[2] NASA Langley Research Center, Hampton VA 23666, USA
victor.a.carreno@nasa.gov
[3] École polytechnique, 91128 Palaiseau Cedex, France
Gilles.Dowek@polytechnique.fr

Abstract. The Small Aircraft Transportation System (SATS) is a NASA project aimed at increasing access to small non-towered non-radar airports in the US. SATS is a radical new approach to air traffic management where pilots flying instrument flight rules are responsible for separation without air traffic control services. In this paper, the SATS project serves as a case study of an operational air traffic concept that has been designed and analyzed primarily using formal techniques. The SATS concept of operations is modeled using non-deterministic, asynchronous transition systems, which are then formally analyzed using state exploration techniques. The objective of the analysis is to show, in a mathematical framework, that the concept of operation complies with a set of safety requirements such as absence of dead-locks, maintaining aircraft separation, and robustness with respect to the occurrence of off-nominal events. The models also serve as design tools. Indeed, they were used to configure the nominal flight procedures and the geometry of the SATS airspace.

Acronyms	
AMM	Airport Management Module
FAF	Final Approach Fix
HVO	Higher Volume Operations
IAF	Initial Approach Fix
IF	Intermediate Fix
IMC	Instrument Meteorological Conditions
MAHF	Missed Approach Holding Fix
PVS	Prototype Verification System
SATS	Small Aircraft Transportation System
SCA	Self-Controlled Area

1 Introduction

The primary safety objective of an air traffic management system is to provide aircraft separation. This objective is achieved trough air/ground equipment and a set of flight rules and procedures, usually called *concept of operations*. Emerging

M. Butler et al. (Eds.): REFT 2005, LNCS 4157, pp. 306–325, 2006.

and more reliable surveillance and communication technologies have enabled new concepts where pilots and air traffic controllers share the responsibility for traffic separation. One of such concepts is NASA's *Small Aircraft Transportation System (SATS)*, *Higher Volume Operation (SATS HVO)* [1].

The SATS project aims to increase access to small airports in the US during instrument approach operations. Currently, under poor weather conditions, small airports are restricted to *one-in/one-out* operations. The SATS HVO concept enables up to four simultaneous arrival approaches and multiple departures. A key aspect of the concept is that, under nominal operations, aircraft are *self-separated*, i.e., pilots are responsible for separation without assistance of an air traffic controller. To this end, the SATS HVO concept designs the airspace surrounding the airport as a *Self-Controlled Area (SCA)*. A centralized, automated system, called the *Airport Management Module* (AMM), serves as an arbiter to aircraft entering the SCA. In this concept, aircraft constantly broadcast their locations and receive traffic aircraft locations. Therefore, they have an updated view of the airspace.

The SATS HVO operational concept is a collection of rules and procedures to be followed by aircraft operating or transitioning in/out of the SCA. For instance, the concept of operations states when and how an aircraft is allowed to enter (or leave) the SCA, when an aircraft is allowed to initiate the approach, and how to perform a missed approach. In order to alleviate pilot workload and increase situational awareness, on board navigation tools provide advisories that assist pilots in following these procedures. An overview of the SATS HVO operational concept is given in Section 2.

Because the operational concept is a safety critical element of the SATS project, the task of showing that it satisfies safety requirements is accomplished using formal mathematical analysis. A discrete mathematical model of the SATS HVO operational concept for nominal operations is described in [11]. That model was mechanically checked for safety and liveness properties. The discrete model, and its limitations, is presented in Section 3.

In this paper, we extend the discrete model in [11] in two orthogonal ways. First, in Section 4, we include off-nominal procedures such as closing of the SCA and re-sequencing of aircraft. We verify that most of the safety properties are still maintained with minimal modifications to the operational concept. Second, in Section 5, we study spacing and separation issues in the Self-Controlled Airspace. To this end, we describe a *hybrid* model that extends the discrete model to take into account the geometry of the SCA and the aircraft speed performances. Using this new model, we formally verified that the SATS HVO operational concept *effectively* achieves self-separation, i.e., aircraft performing nominal approaches are safely separated according to minimum spacing criteria.

2 Higher Volume Operations

In the SATS HVO concept, pilots operating within the Self-Controlled Area (SCA) are required to fly by latitude/longitude points in the space, called *fixes*.

Similar to a GPS-T approach, fixes are arranged as a T (see Figure 1).[1] The fixes at the extremes of the T are called *initial approach fixes* (IAF's) and they are the entry points to the SCA. The IAF's also serve as *missed approach holding fixes* (MAHF's), i.e., fixes where aircraft will proceed in case they have to perform a missed approach. The holding areas are located at 2000 feet and 3000 feet above ground level at the IAF's.

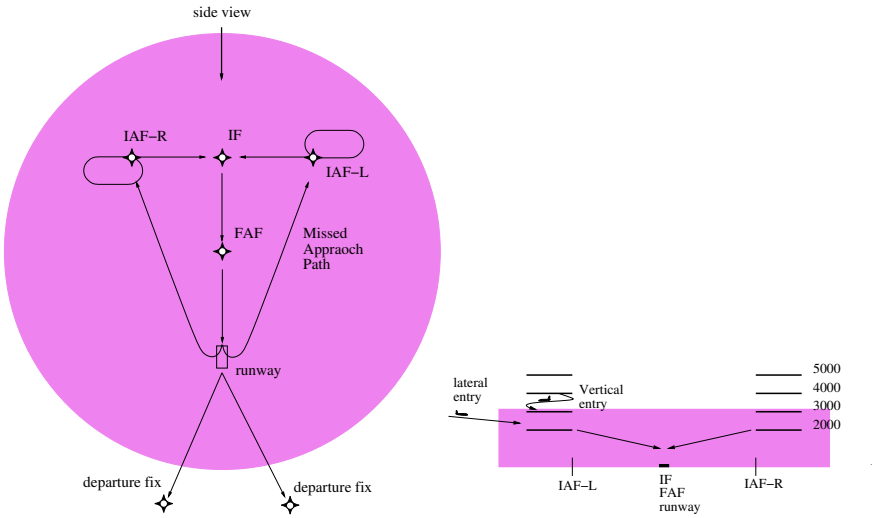

Fig. 1. Top and side view of SCA

There are two types of entry procedures: *vertical entry* and *lateral entry*. In a vertical entry, an aircraft at the IAF descends from 4000 feet to 3000 feet and holds at 3000 feet until it is enabled to descend to 2000 feet. In a lateral entry, an aircraft flies directly to its IAF at or above 2000 feet. When the aircraft is enabled to initiate the approach, it flies to the *intermediate fix* (IF), from there to the *final approach fix* (FAF), and finally to the runway threshold. In case of a missed approach, the aircraft flies to its assigned missed approach holding fix at the lowest available altitude (2000 or 3000 feet). Then, it re-initiates the approach and either follows a normal landing procedure or leaves the SCA. The linear segments between the IAFs and the IF are called *base segments*; the segment between the IF and the runway threshold is called the *final segment*. Henceforth, we say that an aircraft is *on final approach* if it is in the base or final segments.

The Airport Management Module (AMM) is an automated centralized system that resides at the airport grounds. It receives state information from aircraft in the vicinity of the airport and communicates with aircraft via data link. The AMM provides entry clearances (vertical or lateral) and assigns missed approach

[1] As it is usually depicted, right and left are relative to the pilot facing the runway, i.e., opposite from the reader's point of view.

holding fixes. When an entry is granted by the AMM, the aircraft receives a *follow notification* and a *missed approach holding fix assignment*. The follow notification is either *none*, if it is the first aircraft in the landing sequence, or the identification of a *lead* aircraft. Missed approach holding fixes are assigned by the AMM on an alternating basis. This technique ensures that consecutive aircraft on missed approach are not flying to the same missed approach holding fix.

For nominal arrival operations, self-separation is achieved by requiring an aircraft to hold at its IAF until it meets a spacing safety threshold with respect to its lead aircraft. The threshold guarantees a minimum separation during the approach and during a missed approach, in case of this eventuality.

The concept of operations also describes nominal departure operations. However, for simplicity, the analysis presented in this paper only considers arrival operations. This simplification does not affect the result of the formal verification as arriving aircraft are geographically separated from departing aircraft and an aircraft cannot depart if there is an aircraft on final approach. The fact that departing aircraft are separated was also verified using the techniques presented in this paper.

3 Discrete Model and Its Limitations

The discrete model described in [11] is a mathematical abstraction of the SATS HVO concept. A simple way to visualize that model is via an analogy with a board game where the board is a discretized SCA, the pieces that move across the board are the aircraft, and the rules of the game are given by the concept of operations. This analogy is illustrated in Figure 2.The places where an aircraft can be during an arrival operation are called *zones*. There are 12 zones:

- `holding3` (left, right): Holding patterns at 3000 feet.
- `holding2` (left, right): Holding patterns at 2000 feet.
- `lez` (left, right): Lateral entry zones.[2]
- `base` (left, right): Base segments.
- `maz` (left, right): Missed approach zones.
- `final` and `runway`: Final segment and runway.

An aircraft is always in one and only one zone, but several aircraft may be in the same zone. Aircraft leave the zones in the same order as they arrive. The arrows in Figure 2 are the valid moves and they represent 15 flight rules and procedures:

- Vertical entry (left, right): Initial move to `holding3`.
- Lateral entry (left, right): Initial move to `lez`.
- Descend (left, right): Move from `holding3` to `holding2`.
- Approach initiation (left, right): Move from `holding2` to `base`.
- Final approach (left, right): Move from `base` to `final`.

[2] Lateral entry zones start outside the SCA.

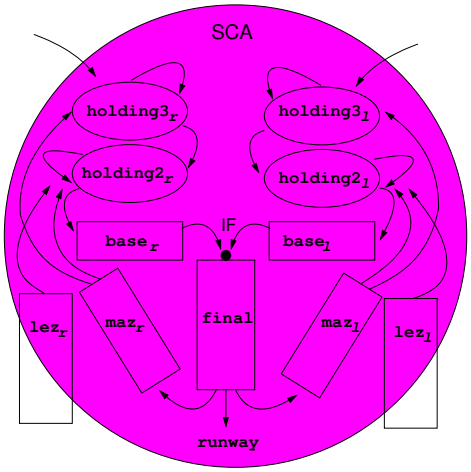

Fig. 2. Discrete view of SCA

- Landing: Move from `final` to `runway`.
- Missed approach initiation (left, right): Move from `final` to `maz`.
- Transition to lowest available altitude (left, right). Move from `maz` to either `holding3` or `holding2`.

The *state of the SCA* is then composed of the 12 zones, each one being a list of aircraft, the next available landing sequence (natural number), and the next alternating missed approach holding fix (left or right). Each aircraft is represented by its initial approach fix (left or right), landing sequence (natural number), and missed approach holding fix assignment (left or right). Aircraft identifications are implicit as aircraft can be distinguished from each other by their landing sequence.

The discrete model is conservative in the sense that it abstracts away the SCA geometry and physical performance parameters of the aircraft. Hence, it includes scenarios that may no physically occur in the real world. We argue that the model is complete, i.e., it includes all nominal operations. Indeed, the model has been extensively reviewed by the developers of the SATS HVO concept.

From a mathematical point of view, the discrete model is a state transition system where the states are snapshots of the zones at discrete times and the transitions describe how the states evolve when the flight procedures are applied. A priori, there are no bounds on the number of aircraft in each zone; therefore, the transition system is potentially infinite. However, an exhaustive exploration of the set of reachable states reveals that the transition system is finite. Indeed, the system was exhaustively explored [11] using an explicit model checker algorithm written and formally verified in the verification system PVS [12].

Using formal techniques, it has been shown in [11] that, under nominal operations, the concept satisfies the following safety properties:

- There are at most four arriving aircraft.
- There are no more than two aircraft assigned to a given missed approach holding fix.
- For an aircraft on missed approach, there is always an available altitude at the assigned MAHF.
- There are at most two aircraft on each side of the SCA.
- There is at most one aircraft holding at a given altitude of a holding fix.
- There are at most two aircraft on missed approach assigned to the same MAHF.
- There are no simultaneous lateral and vertical entries at a given fix.
- Aircraft land in order according to the landing sequence.

Furthermore, it has been verified that each reachable state evolves into an empty SCA when entry rules are inhibited, and that the concept of operations is free of dead-locks, i.e., all aircraft eventually land (or depart).

The rest of this section illustrates some limitations of the discrete model that are addressed by this paper.

3.1 Off-Nominal Operations

It is very difficult, if possible, to handle the occurrence of off-nominal events in a comprehensive way. For this reason, the operational concept for off-nominal SATS HVO operations [2] only addresses *pragmatic failures and operational errors*, i.e., conditions that have a practical expectation for occurrence. These conditions are further segregated in three categories:

1. *Routine non-normal conditions* due to pilot deviations from nominal operations.
2. *Equipment malfunction conditions* due to hardware failures.
3. *Emergency conditions* that cause a landing priority request.

In general, safety properties are not preserved under operations that are non-conforming to SATS HVO procedures. For example, if an aircraft returns to its incorrect missed approach holding fix, there is no guarantee that the aircraft will find an available altitude to hold. However, for this situation to occur, the pilot would have already ignored the information provided by the Multi-Function Display and the Pilot Adviser, which are components of the SATS HVO concept. Furthermore, the Conflict Detection and Alerting system provides an additional layer of safety to the overall system [4].

The discrete model presented in [11] does not include off-nominal operations. Given the complex nature of off-nominal events, a complete mathematical model of off-nominal operations is a major endeavor. In this work, we aim at a simpler objective. We extend the discrete SATS HVO model with procedures for SCA closing, re-sequencing, and re-assignment during a missed approach. These procedures are critical to several procedures for off-nominal conditions.

3.2 Self-separation Guarantees

Consider the two states depicted in Figure 3. Although these states do not satisfy the same separation requirements, they are indistinguishable by the discrete model. This behavior is due to the way the approach initiation procedure was written in the discrete model. The concept of operations states that an aircraft

(a) Aircraft A and B are separated (b) Aircraft A and B are not separated

Fig. 3. Indistinguishable discrete states

may initiate the approach if (a) it is the first aircraft in the landing sequence or (b) it meets a safety threshold with respect to the lead aircraft, which is already on approach [1]. There are several ways a pilot can check whether the safety threshold is satisfied or not. In the most conservative case, the pilot has to delay the approach initiation until the lead aircraft is within 6 nautical miles from the runway. The value 6 is for a nominal SCA where the base segments are 5 nautical miles and the final segment is 10 nautical miles. In the general case, the initial distance between an aircraft and its lead aircraft is configurable and could be calculated by on-board tools according to the geometry of the SCA and the speeds of the aircraft involved. Since the geometry of the SCA and speeds of the aircraft are not considered in the discrete model, the approach initiation transition rule was simplified. The condition (a) rests the same. However, the discrete model uses a weaker condition (b) where an aircraft can initiate the approach as soon as the lead aircraft is already on the final approach (base or final segments). Because the safety threshold is not checked, spacing properties cannot be verified using the discrete model.

In order to verify spacing properties, we need a more detailed modeling of the approach initiation procedure. To this end, we extend the discrete model of the SATS HVO concept with continuous variables that encode the geometry of the SCA and the aircraft speed performances.

4 Off-Nominal Procedures

To model off-nominal procedures, the state of the SCA is extended with a new field *status* of an enumeration type $\{OP, CLOSE, OFF\}$. The value OP is used to indicate normal operations, the value $CLOSE$ is used to indicate that the SCA is close, and the value OFF is used to indicate that the AMM is unavailable.

The status *CLOSE* and *OFF* differ in that in the former case the AMM is providing normal service to the aircraft already in the SCA but has inhibited new operations; in the latter case, the AMM is not providing any service. Transition rules are modified accordingly to cope with the extended state. For instance, entries are only allowed when *status* is *OP*, AMM services inside the SCA are provided only if *status* is different from *OFF*, etc.

4.1 SCA Closing

The following off-nominal conditions require the SCA to be closed to new operations:

- Change of approach direction.
- Loss of aircraft state data input/output on an arriving SATS aircraft.
- Loss of AMM.
- Loss of voice radio communication.
- Priority request from an aircraft on landing approach.

The SCA closing procedure is modeled as a transition rule that changes the status of the SCA to *CLOSE* and from *CLOSE* to *OP* in a non-deterministic asynchronous way.

4.2 Re-sequencing

Under normal operations, re-sequencing is only necessary for missed approach operations. In this case, the aircraft in the missed approach re-initiates the approach as the last aircraft in the landing sequence (or the first one, if it is the only aircraft in the SCA). Furthermore, if it is the first aircraft in the approach, it keeps its MAHF assignment. Otherwise, it gets an alternating MAHF with respect to its lead aircraft.

Off-nominal situations such as pilot cancellation of an approach request and priority request from an aircraft on approach, may require the AMM to remove one aircraft from the normal approach sequence and re-sequence the remainder aircraft. To handle these situations, the re-sequencing transition rule has been modified as follows. Assume that the removed aircraft had the landing sequence n:

- Aircraft with an approach sequence less than n keep their assigned approach sequence and MAHF.
- Aircraft with an approach sequence greater than n decrease their landing sequence by one. If $n \neq 1$, they get assigned to their opposite MAHF. Otherwise, they keep their MAHF.

4.3 Re-assignment During Missed Approach

Aircraft in missed approach get a new approach sequence and a MAHF assignment from the Airport Management Module. The concept of operations for off-nominal operations requires that, if the AMM output is lost, pilots use voice radio communication to complete the approach.

To support this procedure, we have designed a very simple transition rule for re-assignment during missed approach when *status* is *OFF*:

- Aircraft in a missed approach keep their relative landing sequence and their assigned MAHF.
- All other aircraft complete their normal approaches.

4.4 Verification of Off-Nominal Procedures

Exhaustive exploration of the discrete transition system extended with the previous off-nominal procedures shows that these procedures preserve all the safety properties in Section 3. In particular, it can be shown that in case of a AMM failure, aircraft in missed approach will always have a place to hold even if they perform a missed approach after the AMM has failed. However, in this case, MAHF are not necessarily assigned in an alternating way. We have not explored this issue further, but this may not be a major issue as, if the AMM is down, the SCA is closed for new operations and the probability of simultaneous consecutive missed approaches is relatively low.

5 Spacing Properties

The term *spacing* refers to linear separation of an aircraft with respect to the lead aircraft. If both aircraft are not flying the same approach, spacing is computed relative to the merging point of their linear trajectories. For instance, in a symmetric SCA, if the trail and lead aircraft are on opposite initial approach fixes their spacing is 0, although their Euclidean distance is twice the length of the of the base segments. Note that, independently of the initial Euclidean distance, if both aircraft start the approach at roughly the same time and speed, they will have a conflict at the merging point.

The geometry of the SCA is given by the lengths of the base segments, denoted $Lbase(s)$ where $s \in \{left, right\}$, the length of the final segment, denoted $Lfinal$, and the lengths of the missed approach zones, denoted $Lmaz(s)$ where $s \in \{left, right\}$. Henceforth, we write iaf_A and $mahf_A$ to denote, respectively, the initial approach fix and missed approach holding fix (*left* or *right*) of aircraft A.

We define $D_A(t)$ as the linear distance at time t of an aircraft A from its initial approach fix. In a symmetric SCA, i.e., $Lbase(left) = Lbase(right)$ and $Lmaz(left) = Lmaz(right)$, the spacing at time t between an aircraft A and its lead aircraft B is simply defined as $D_B(t) - D_A(t)$. However, in the general case, we must consider the difference in length of the base segments. Hence, if B is before A in the landing sequence, the spacing between A and B is defined as

$$S_{A \to B}(t) \equiv D_B(t) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B). \tag{1}$$

Now, we specify the spacing requirements to be formally verified.

Proposition 1. *Under nominal operations, aircraft A and B on final approach at time t, such that B is the lead aircraft of A, satisfy the following spacing requirement:*

$$S_T \ \leq \ S_{A \to B}(t). \tag{2}$$

Proposition 2. *Under nominal operations, A and B on final approach, on missed approach at the same fix at time t, such that B is before A in the landing sequence, satisfy the following spacing requirement:*

$$S_{MAZ} \ \leq \ S_{A \to B}(t). \tag{3}$$

The constants S_T and S_{MAZ} are the theoretical spacing that the concept guarantees on final approach and missed approach, respectively. These constants are determined by the geometry of the SCA, the minimum and maximum speed of the aircraft, $v_{\min}$ and $v_{\max}$, and the initial spacing between the aircraft, S_0, as follows:

$$S_T \equiv S_0 - (L_{max} + Lfinal - S_0)\Delta_v, \tag{4}$$

$$S_{MAZ} \equiv \min(L_{min} + Lfinal - L_{maz}\Delta_v, \\ 2S_0 - (L_{max} + Lfinal + L_{maz} - S_0)\Delta_v), \tag{5}$$

where

$$L_{min} \equiv \min(Lbase(left), Lbase(right)), \tag{6}$$

$$L_{max} \equiv \max(Lbase(left), Lbase(right)), \tag{7}$$

$$L_{maz} \equiv \max(Lmaz(left), Lmaz(right)), \tag{8}$$

$$\Delta_v \equiv \frac{v_{\max} - v_{\min}}{v_{\min}}. \tag{9}$$

5.1 Hybrid Model

In order to verify Propositions 1 and 2, we extend the discrete model of the SCA with the following continuous variables:

- A current time t that evolves in a continuous way.
- For each aircraft A on final approach or missed approach, the linear distance from its IAF, $D_A(t)$. We assume that the speed of an aircraft may vary with time in the interval $[v_{\min}, v_{\max}]$. Therefore, the value of $D_A(t)$ is constrained by

$$(t_1 - t_0)v_{\min} \leq \ D_A(t_1) - D_A(t_0) \ \leq \ (t_1 - t_0)v_{\max}, \tag{10}$$

  if $t_0 \leq t_1$ (t_0 and t_1 are measured in the same approach operation).

These continuous variables allow us to state the approach initiation rule in a more precise way:

- *Approach initiation for vertical and lateral entry (left and right)*: An aircraft A may initiate the approach when (a) it is the first aircraft in the landing sequence or (b) its lead aircraft B is already on the final approach (base or final segments) and

$$S_0 \ \leq \ S_{A \to B}(t). \tag{11}$$

Other transitions have to be modified to relate the continuous variables to the geometry of the SCA:

- *Merging*: An aircraft A in the base segment turns to the final segment when

$$D_A(t) = Lbase(iaf_A). \tag{12}$$

- *Missed approach initiation*: An aircraft A in the final segment may go to the missed approach zone when it is the first aircraft in the landing sequence and

$$D_A(t) = Lbase(iaf_A) + Lfinal. \tag{13}$$

- *Landing*: An aircraft A in the final segment may land if it is the first aircraft in the landing sequence, there is no other aircraft in the runway, and

$$D_A(t) = Lbase(iaf_A) + Lfinal. \tag{14}$$

- *Determination of lowest available altitude (left and right)*: An aircraft A on missed approach may go to the holding fix at the lowest available altitude when

$$D_A(t) = Lbase(iaf_A) + Lfinal + Lmaz(mahf_A). \tag{15}$$

We note that they hybrid transition system has been defined such that all the reachable states in the hybrid system are reachable in the discrete system (modulo the common discrete variables). Therefore, all the safety properties in Section 3 are satisfied on the hybrid transition system. Of course, the converse is not true: not all the reachable states of the discrete system are reachable in the hybrid system; in particular, those states violating the spacing requirement expressed by Formula (11) are not reachable in the hybrid system.

5.2 Mechanical Verification

The discrete model of the SATS HVO concept was written in PVS and verified using a state exploration PVS tool called Besc [11]. Roughly speaking, Besc is a basic explicit model checker, written and formally verified in PVS.[3] Early attempts to analyze the hybrid transition system described in this paper, using a hybrid model checker, e.g., HyTech [6], failed mainly due to the number of variables of the SATS HVO model. We tried a different approach: we encoded the hybrid transition system as a discrete one and explored it using Besc.

If we take all the reachable states in the discrete system and eliminate those that do not satisfy the continuous behavior expressed by Formulas (11)–(15), we have a valid abstraction of the SATS HVO concept. Instead of physically eliminating states during the state exploration, which would require a hybrid model checker, we collect for each state a set of constraints yielded by Formulas (11)–(15). Afterward, we process the set of reachable states and use the constraints

[3] Besc is available from `http://research.nianet.org/~munoz/Besc`

to discharge the spacing properties expressed by Propositions 1 and 2. As we will see, this process can be done using a discrete explicit model checker.

A *hybrid constrained state* of the SCA is a tuple $(\mathcal{D}, \mathcal{C})$, where $\mathcal{D}$ is the discrete state of the SCA and $\mathcal{C}$ is a set of constraints of the form $e \leq f$, where e and f are expressions described by the following grammar:

$$\begin{aligned} A, B &::= 1, 2, \ldots \\ s &::= \mathit{left} \mid \mathit{right} \mid \mathit{iaf}_A \mid \mathit{mahf}_A \\ T &::= t \mid T_A \\ e, f &::= T \mid D_A(T) \mid \mathit{Lbase}(s) \mid \mathit{Lfinal} \mid \mathit{Lmaz}(s) \mid S_0 \mid \\ &\quad L_{min} \mid L_{max} \mid L_{maz} \mid S_{A \to B}(T) \mid e + f \end{aligned}$$

Informally, a hybrid constrained state $(\mathcal{D}, \mathcal{C})$ represents an infinite set of hybrid states where all the constraints in $\mathcal{C}$ are satisfied.

A *hybrid constrained transition* is a rule that transforms a state $(\mathcal{D}, \mathcal{C})$ into a state $(\mathcal{D}', \mathcal{C}')$, i.e., in addition to modify the value of the discrete variables, a transition may also add or remove constraints from the previous state.

The continuous behavior described by Formulas (11)–(15) is expressed by hybrid constrained transitions. These transitions are discretized by encoding the constraints in a symbolic way. This is possible because the constraints only relate continuous variables.

- *Approach initiation for vertical and lateral entry (left and right)*: Let A be the aircraft that initiates the approach. The following symbolic constraints are added:
  - The fact that A is in the base segment:

$$T_A \leq t, \tag{16}$$
$$D_A(t) \leq \mathit{Lbase}(\mathit{iaf}_A). \tag{17}$$

  - If B is the lead aircraft of A, the fact that the aircraft are spaced at time T_A:

$$T_B \leq T_A, \tag{18}$$
$$S_0 \leq S_{A \to B}(T_A). \tag{19}$$

  - For all aircraft C on missed approach, the fact that C was ahead of A:

$$\mathit{Lbase}(\mathit{iaf}_A) + \mathit{Lfinal} \leq D_C(T_A). \tag{20}$$

- *Merging*: Let A be the aircraft that goes into the final segment. Constraint(17) is removed from the constraints. But, the fact that A is in the final segment is added to the constraints:

$$D_A(t) \leq \mathit{Lbase}(\mathit{iaf}_A) + \mathit{Lfinal}. \tag{21}$$

- *Missed approach initiation*: Let A be the aircraft that initiates the missed approach. Constraint (21) is removed from the constraints. But, the fact that A is on missed approach is added to the constraints:

$$D_A(t) \leq Lbase(iaf_A) + Lfinal + Lmaz(mahf_A). \tag{22}$$

- *Landing*: Let A be the aircraft that is landing. All constraints related to A are removed from the constraints, except instances of Constraints (18) and(19) when B, the previous lead aircraft of A, is on missed approach.
- *Determination of lowest available altitude (left and right)*: Let A be the aircraft that goes to the lowest available altitude. All constraints related to A are removed from the constraints.

Finally, to verify Propositions 1 and 2, we explicitly generate the set of reachable constrained states and for each state $s = (\mathcal{D}, \mathcal{C})$, we formally prove the following invariant properties.

Invariant 1. *For each pair of aircraft A and B in s such that A and B are on final approach at time t, and B is the lead of aircraft A,*

$$\mathcal{C} \vdash S_T \leq S_{A \to B}(t), \tag{23}$$

i.e., the minimum spacing S_T holds for A and B under the constraints $\mathcal{C}$.

Invariant 2. *For each pair of aircraft A and B in s such that they are on missed approach to the same fix at time t, and B is before A in the landing sequence,*

$$\mathcal{C} \vdash S_{MAZ} \leq S_{A \to B}(t), \tag{24}$$

i.e., the minimum spacing S_{MAZ} holds for A and B under the constraints $\mathcal{C}$.

We remark that, for the explicit model checker, the constraints $\mathcal{C}$ are just data without logical meaning. Thus, the invariant properties cannot be checked on the fly during the state exploration process. The mechanical verification proceeds in three different stages. In the first stage, the hybrid constrained transition system is fully explored in PVS using the explicit model checker Besc. In order to get a finite system, the constraints are implemented as a set rather than a list to avoid repetitions. Besc reports a total of 2768 reachable states and a diameter, maximum length of a path, of 27 states.

In the second stage, we process the set of reachable hybrid constrained states using an external tool called PVSio[4] and generate a PVS file where there is a lemma for each possible instance of Invariant 1 or Invariant 2. Without counting repetitions, 117 spacing lemmas were generated. From those, 73 lemmas are instances of the first invariant and the remaining 44 lemmas are instances of the second one.

[4] PVSio enhances the PVS ground evaluator with input/output operations. It is available from `http://research.nianet.org/~munoz/PVSio`

In addition to the spacing lemmas, proof scripts, which automatically discharge these lemmas, are also generated. In the final stage of the mechanical verification task, all 117 proof scripts are successfully checked in batch mode via the utilities provided by ProofLite.[5]

The proof scripts that are automatically generated are based on three lemmas. One lemma, called *T*, takes care of instances of Invariant 1. The other two lemmas, called *Maz1* and *Maz2*, handle particular cases of Invariant 2. These lemmas were checked in PVS. Afterward, they were integrated into a PVS strategy that mechanically discharges the automatically generated spacing lemmas. For completeness, the lemmas *T*, *Maz1*, and *Maz2* are included in the appendix.

The SATS HVO formal development, excluding the PVS tools Besc, PVSio and ProofLite, is about 2800 lines of PVS specification and lemmas and 6500 lines of proofs. From these, 1600 lines of lemmas and 5900 lines of proofs were automatically generated using the PVS tools.

6 Conclusion

Several air traffic management systems have been previously specified and analyzed using formal notations and tools. For instance, the collision avoidance system TCAS II, which is required on commercial aircraft with more than 30 seats, was formally specified in the Requirements State Machine Language (RSML) in [7]. A portion of this specification was translated to SMV and several general properties were studied using model checking [3]. Examples of these properties included identification of non-deterministic transitions, function consistency, and termination. In [9], reachability analysis is used to find optimal conflict-free trajectories for aircraft in a distributed air traffic management environment. A runway incursion monitoring algorithm is analyzed using the SMART model checker in [13]. This analysis resulted in the identification of suspicious scenarios that were not considered by the algorithm. All these works use discretized finite models of the airspace. Hence, the verification techniques are based on model checking.

Continuous infinite models that enable the verification of timing and spacing properties are used in [10] and [8]. The former work studies the minimum time prior to a collision after an alarm is issued by an alerting algorithm for parallel landing. The later one describes the formal proof of the correctness of a conflict detection and resolution algorithm for distributed air traffic management. In both cases, the verification effort was performed using the PVS verification system.

Another example of the use of formal methods in air traffic management is presented in [14]. In this case, components written in C++ of an aeronautical information systems are specified using pre- and post-conditions. The experience discovered ambiguities in the formal specification, but no major logical errors were found.

The work presented in this paper extends a previous work [11] in two orthogonal aspects: off-nominal procedures and spacing properties. The overall approach

[5] ProofLite is a PVS tool for non-interactive proof checking. It is available from `http://research.nianet.org/~munoz/ProofLite`

is novel in several aspects. First, it is not related to a particular piece of software but to a more general system: a concept of operations that defines the expected interactions beetween multiple components of an air traffic management system. Second, the analysis involves general safety properties, which are expressed using discrete variables, and precise spacing requirements, which are expressed using continuous variables. The complete approach is developed in PVS, but it involves both model checking and theorem proving techniques. Finally, the models presented in this paper served as design tools. Indeed, the verification effort resulted in the identification of 9 issues, including one major flaw, in the original concept. Ten recommendations were made to the concept development working group [5]. All the recommendations were accepted and incorporated into the final concept of operations, which was successfully demonstrated on a flight experiment.

The model of off-nominal procedures proposed in this paper does not capture all abnormal conditions described in [2]. One such model is a major endeavor. A hazard analysis may help to determine which conditions are the most critical. If these conditions are handled in a procedural way, they can be modeled using the formal techniques described in this paper.

From a practical point of view, the spacing analysis presented in this paper, e.g., Formulas (4) and (5), can be used to configure a nominal SCA and the parameters of the baseline procedure for self-separation. For instance, consider a symmetrical nominal SCA where $Lbase(left) = Lbase(right) = 5$ nm, $Lfinal = 10$ nm, and $Lmaz(left) = Lmaz(right) = 13$ nm. If the initial separation S_0 is 6 nm and $v_{\min} = 90$ kt, $v_{\max} = 120$ kt, then

$$L_{min} = L_{max} = 5 \text{ nm}, \tag{25}$$

$$L_{maz} = 13 \text{ nm}, \quad \text{and} \tag{26}$$

$$\Delta_v = \frac{120 - 90}{90} = \frac{1}{3}. \tag{27}$$

The value of S_T is computed using Formula (4):

$$S_T = 6 - \frac{5 + 10 - 6}{3} = 3 \text{ nm}. \tag{28}$$

This configuration of the SCA satisfies Formula (60). Therefore, the value of S_{MAZ} can be computed using Formula (59):

$$S_{MAZ} = 12 - \frac{5 + 10 + 13 - 6}{3} = 4.66 \text{ nm}. \tag{29}$$

Hence, if the initial spacing of the trail aircraft with respect to the lead aircraft is 6 nm, the SATS HVO concept of operations guarantees a minimum spacing of 3 nm on final approach and 4.66 nm on missed approach.

The work presented demonstrates that the formal analysis can be used to show compliance with safety requirements and also to explore design decisions concerning the concept of operation. The mechanical verification is necessary to make sure that no cases were forgotten. Formal proofs are the ultimate guarantee that the mathematical development presented here is correct.

References

1. T. Abbott, K. Jones, M. Consiglio, D. Williams, and C. Adams. Small Aircraft Transportation System, High Volume Operation concept: Normal operations. Technical Report NASA/TM-2004-213022, NASA Langley Research Center, NASA LaRC Hampton VA 23681-2199, USA, 2004.
2. B. Baxley, D. Williams, M. Consiglio, C. Adams, and T. Abbott. The Small Aircraft Transportation System (SATS), Higher Volume Operations (HVO) off-nominal operations. In *Proceedings of the AIAA 5th Aviation, Technology, Integration, and Operations Conference, AIAA-2005-7461*, Arlington, Virginia, 2005.
3. W. Chan, R. Anderson, P. Beame, S. Burns, F. Modugno, D. Notkin, and J. Reese. Model checking large software specifications. *IEEE Transactions on Software Engineering*, 24(7):498–520, 1998.
4. M. Consiglio, V. Carreño, D. Williams, and C. Muñoz. Conflict prevention and separation assurance method in the Small Aircraft Transportation System. In *Proceedings of the AIAA 5th Aviation, Technology, Integration, and Operations Conference, AIAA-2005-7463*, Arlington, Virginia, 2005.
5. G. Dowek, C. Muñoz, and V. Carreño. Abstract model of the SATS concept of operations: Initial results and recommendations. Technical Report NASA/TM-2004-213006, NASA Langley Research Center, NASA LaRC,Hampton VA 23681-2199, USA, 2004.
6. T. Henzinger, P.-H. Ho, and H. Wong-Toi. HyTech: A model checker for hybrid systems. *Software Tools for Technology Transfer*, 1:110–122, 1997.
7. N. Leveson, M. Heimdahl, H. Hildreth, and J. Reese. Requirements specification for process-control systems. *IEEE Transactions on Software Engineering*, 20(9):684–707, September 1994.
8. J. Maddalon, R. Butler, A. Geser, and C. Muñoz. Formal verification of a conflict resolution and recovery algorithm. Technical Report NASA/TP-2004-213015, NASA Langley Research Center, NASA LaRC,Hampton VA 23681-2199, USA, April 2004.
9. M. Massink and N. De Francesco. Modelling free flight with collision avoidance. In *Proceedings 7th IEEE International Conference on Engineering of Complex Computer Systems*, pages 270–280, 2001.
10. C. Muñoz, V. Carreño, G. Dowek, and R.W. Butler. Formal verification of conflict detection algorithms. *International Journal on Software Tools for Technology Transfer*, 4(3):371–380, 2003.
11. C. Muñoz, G. Dowek, and V. Carreño. Modeling and verification of an air traffic concept of operations. *Software Engineering Notes*, 29(4):175–182, 2004.
12. S. Owre, J. M. Rushby, and N. Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *11th International Conference on Automated Deduction (CADE)*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752, Saratoga, NY, 1992.
13. R. Siminiceanu and G. Ciardo. Formal verification of the NASA runway safety monitor. *Electronic Notes Theoretical Computer Science*, 128(6):179–194, 2005.
14. R. Yates, J. Andrews, and P. Gray. Practical experience applying formal methods to air traffic management software. In *Proceedings of the 8th Annual International Symposium of the International Council on Systems Engineering*, Vancouver, Canada, 1998.

Appendix

The lemmas described here were mechanically checked in PVS. Afterward, they were integrated into a PVS strategy that mechanically discharges the automatically generated spacing lemmas.

First, we present some auxiliary properties. The time when an aircraft A initiates the final approach, i.e., when it enters the base segment, is denoted T_A. Hence, by definition,

$$D_A(T_A) = 0. \tag{30}$$

Therefore, Constraint (19) is equivalent to

$$S_0 + Lbase(iaf_B) - Lbase(iaf_A) \leq D_B(T_A). \tag{31}$$

Furthermore, if A is on final approach at time t, Constraint (17) and Constraint (21) yield

$$D_A(t) \leq Lbase(iaf_A) + Lfinal. \tag{32}$$

Lemma 1 (T). *Let A and B be aircraft on final approach at time t such that B is the lead of aircraft A. It holds that*

$$S_0 - (L_{max} + Lfinal - S_0)\Delta_v \leq S_{A \to B}(t), \tag{33}$$

under the hypotheses

$$T_A \leq t \tag{34}$$

$$S_0 + Lbase(iaf_B) - Lbase(iaf_A) \leq D_B(T_A), \tag{35}$$

$$D_B(t) \leq Lbase(iaf_B) + Lfinal. \tag{36}$$

(Formula (34) is the Constraint (16), Formula (35) is the spacing constraint from Formula (31), and Formula (36) is the instantiation of Formula (32) on aircraft B, which is on final approach.)

Proof. Subtracting Formula (35) from Formula (36), we get

$$D_B(t) - D_B(T_A) \leq Lbase(iaf_A) + Lfinal - S_0. \tag{37}$$

Using Formula (10) on A and B,

$$(t - T_A)v_{\min} \leq D_B(t) - D_B(T_A), \tag{38}$$

$$D_A(t) - D_A(T_A) \leq (t - T_A)v_{\max}. \tag{39}$$

Formula 39 yields

$$D_A(t) \leq (t - T_A)v_{\max}. \tag{40}$$

From Formulas (37) and (38),

$$t - T_A \leq \frac{Lbase(iaf_A) + Lfinal - S_0}{v_{\min}}. \tag{41}$$

Hence,

$$\begin{aligned}
S_{A\to B}(t) &= D_B(t) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&= D_B(T_A) + (D_B(t) - D_B(T_A)) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&\geq S_0 + (D_B(t) - D_B(T_A)) - D_A(t), \quad \text{by Formula (35)}, \\
&\geq S_0 + (t - T_A)v_{\min} - (t - T_A)v_{\max}, \quad \text{by Formulas (38) and (40)}, \\
&\geq S_0 - (Lbase(iaf_A) + Lfinal - S_0)\frac{v_{\max} - v_{\min}}{v_{\min}}, \quad \text{by Formula (41)}, \\
&\geq S_0 - (L_{max} + Lfinal - S_0)\Delta_v, \quad \text{by Formulas (7) and (9)}.
\end{aligned}$$

Lemma 2 (Maz1). *Let A and B be aircraft on missed approach at time t such that B is before A in the landing sequence. Furthermore, assume that when A initiated the approach, B was on missed approach. It holds that*

$$L_{min} + Lfinal - L_{maz}\Delta_v \leq S_{A\to B}(t), \tag{42}$$

under the hypotheses

$$T_A \leq t \tag{43}$$

$$D_B(t) \leq Lbase(iaf_B) + Lfinal + Lmaz(mahf_B), \tag{44}$$

$$Lbase(iaf_B) + Lfinal \leq D_B(T_A). \tag{45}$$

(Formula (43) is the Constraint (16), Formula (44) is the instantiation of Constraint (22) on aircraft B, and Formula (45) is the additional assumption about aircraft A and B.)

Proof. Subtracting Formula (45) from Formula (44), we get

$$D_B(t) - D_B(T_A) \leq Lmaz(mahf_B). \tag{46}$$

Formulas (38)–(40) are derived as in Lemma 1. From Formulas (38) and (46),

$$t - T_A \leq \frac{Lmaz(mahf_B)}{v_{\min}}. \tag{47}$$

Hence,

$$\begin{aligned}
S_{A\to B}(t) &= D_B(t) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&= D_B(T_A) + (D_B(t) - D_B(T_A)) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&\geq Lbase(iaf_A) + Lfinal + (D_B(t) - D_B(T_A)) - D_A(t), \quad \text{by Formula (45)}, \\
&\geq Lbase(iaf_A) + Lfinal + (t - T_A)v_{\min} - (t - T_A)v_{\max}, \\
&\qquad\qquad \text{by Formulas (38) and (40)}, \\
&\geq Lbase(iaf_A) + Lfinal - Lmaz(mahf_B)\frac{v_{\max} - v_{\min}}{v_{\min}}, \quad \text{by Formula (47)}, \\
&\geq L_{min} + Lfinal - L_{maz}\Delta_v, \quad \text{by Formulas (6), (8), and (9)}.
\end{aligned}$$

Lemma 3 (Maz2). *Let A and B be aircraft on missed approach at time t such that B is before A in the landing sequence. Furthermore, assume that when A initiated the approach, aircraft B and X where on final approach, B was the lead of aircraft X, and X was the lead aircraft of A. It holds*

$$2S_0 - (L_{max} + Lfinal + L_{maz} - S_0)\Delta_v \leq S_{A\to B}(t), \tag{48}$$

under the hypotheses

$$T_A \leq t \tag{49}$$

$$T_X \leq T_A \tag{50}$$

$$D_B(t) \leq Lbase(iaf_B) + Lfinal + Lmaz(mahf_B), \tag{51}$$

$$S_0 + Lbase(iaf_B) - Lbase(iaf_X) \leq D_B(T_X), \tag{52}$$

$$S_0 + Lbase(iaf_X) - Lbase(iaf_A) \leq D_X(T_A). \tag{53}$$

(Formula (49) is the Constraint (16), Formula (50) is the instantiation of Constraint (18) on aircraft X and A, Formula (51) is the instantiation of Constraint (22) on aircraft B, and Formulas (52) and (53) are the additional assumptions about aircraft A, B, and X.)

Proof. Subtracting Formula (52) from Formulas (51), we get

$$D_B(t) - D_B(T_X) \leq Lbase(iaf_X) + Lfinal + Lmaz(mahf_B) - S_0. \tag{54}$$

Formula (40) is derived as in Lemma 1. From Formula (30), $D_X(T_X) = 0$. Therefore, using Formula (10) on X,

$$D_X(T_A) \leq (T_A - T_X)v_{\max}. \tag{55}$$

From Formulas (49) and (50), $T_X \leq t$. Using Formula (10) on B,

$$(t - T_X)v_{\min} \leq D_B(t) - D_B(T_X). \tag{56}$$

From Formulas (54) and (56),

$$t - T_X \leq \frac{Lbase(iaf_X) + Lfinal + Lmaz(mahf_B) - S_0}{v_{\min}}. \tag{57}$$

Hence,

$$\begin{aligned}
S_{A\to B}(t) &= D_B(t) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&= D_B(T_X) + (D_B(t) - D_B(T_X)) - D_A(t) + Lbase(iaf_A) - Lbase(iaf_B) \\
&\geq S_0 + Lbase(iaf_A) - Lbase(iaf_X) + (D_B(t) - D_B(T_X)) - D_A(t), \\
&\quad \text{by Formula (52)}, \\
&\geq S_0 + Lbase(iaf_A) - Lbase(iaf_X) + (t - T_X)v_{\min} - (t - T_A)v_{\max}, \\
&\quad \text{by Formulas (40) and (56)}, \\
&= S_0 + Lbase(iaf_A) - Lbase(iaf_X) - (t - T_x)(v_{\max} - v_{\min}) + \\
&\quad (T_A - T_X)v_{\max}
\end{aligned}$$

$$\geq S_0 + Lbase(iaf_A) - Lbase(iaf_X) - (t - T_x)(v_{\max} - v_{\min}) + D_X(T_A),$$
by Formula (55),
$$\geq 2S_0 - (t - T_x)(v_{\max} - v_{\min}), \quad \text{by Formula (53)},$$
$$\geq 2S_0 - (Lbase(iaf_X) + Lfinal + Lmaz(mahf_B) - S_0)\frac{v_{\max} - v_{\min}}{v_{\min}},$$
by Formula (57),
$$\geq 2S_0 - (L_{max} + Lfinal + L_{maz} - S_0)\Delta_v,$$
by Formulas (7), (8), and (9).

Note that the conclusions of Lemmas 2 and 3 could be replaced by

$$\min(L_{min} + Lfinal - L_{maz}\Delta_v, 2S_0 - (L_{max} + Lfinal + L_{maz} - S_0)\Delta_v) \leq S_{A\to B}(t). \quad (58)$$

Furthermore,

$$S_{MAZ} = 2S_0 - (L_{max} + Lfinal + L_{maz} - S_0)\Delta_v, \quad (59)$$

when

$$1 + \frac{v_{\min}}{v_{\max}} \leq \frac{L_{min} + Lfinal}{S_0}, \quad (60)$$

and

$$S_t \leq S_{MAZ}, \quad (61)$$

when

$$L_{maz}\Delta_v \leq S_0. \quad (62)$$