HYBRID VERIFICATION OF AN AIR TRAFFIC OPERATIONAL CONCEPT[*]

César A. Muñoz[†]
National Institute of Aerospace, USA
Gilles Dowek[‡]
École polytechnique, France

ABSTRACT

A concept of operations for air traffic management consists of a set of flight rules and procedures aimed to keep aircraft safely separated. This paper reports on the formal verification of separation properties of the NASA's Small Aircraft Transportation System, Higher Volume Operations (SATS HVO) concept for non-towered, non-radar airports. Based on a geometric description of the SATS HVO air space, we derive analytical formulas to compute spacing requirements on nominal approaches. Then, we model the operational concept by a hybrid non-deterministic asynchronous state transition system. Using an explicit state exploration technique, we show that the spacing requirements are always satisfied on nominal approaches. All the mathematical development presented in this paper has been formally verified in the Prototype Verification System (PVS).

Keywords. Formal verification, hybrid systems, air traffic management, theorem proving

INTRODUCTION

The safety objective of air traffic management 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 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)* [Ref. 1].

The SATS program [Ref. 6] 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, therefore, they have an updated view of the SCA.

The SATS HVO operational concept is a collection of rules and procedures to be followed by aircraft operating or transitioning in/out 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 situation awareness, on board navigation tools provide advisories that assist pilots in following these procedures.

Because the operational concept is a safety critical element of the SATS program, the task of showing that it satisfies safety requirements is acomplished using formal mathematical analysis. A discrete mathematical model of the SATS HVO operational concept is described in [Ref. 5]. That model was mechanically checked for safety and liveness properties. As result of this research, several modification were incorporated to the concept [Ref. 2].

[*] This work was supported by the National Aeronautics and Space Administration under NASA Cooperative Agreement NCC-1-02043.

[†] munoz@nianet.org
[‡] Gilles.Dowek@polytechnique.fr

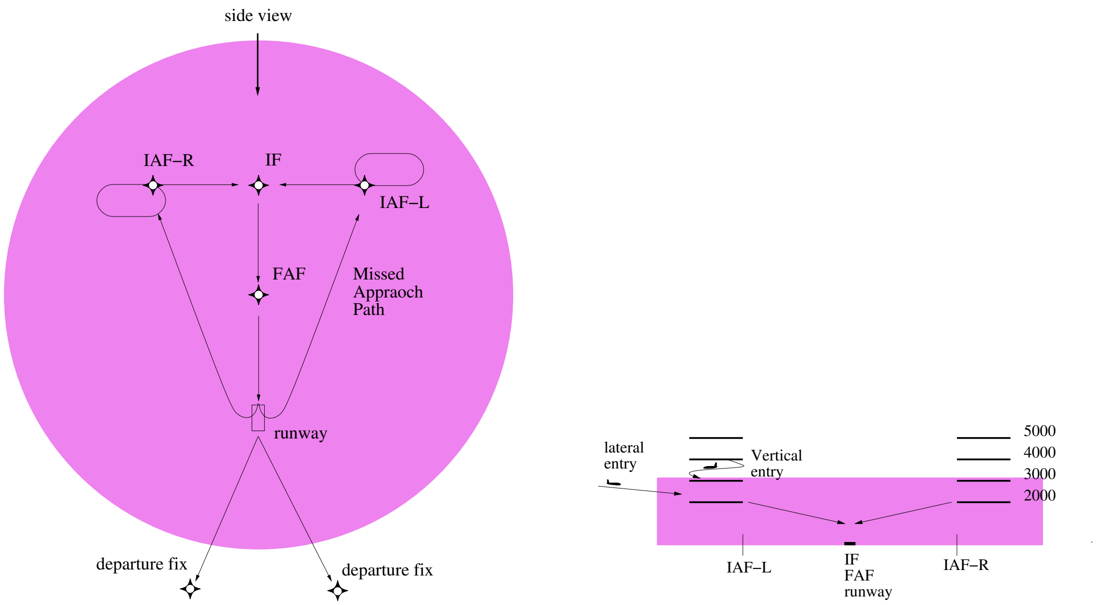


Figure 1: Top and side view of SCA

The discrete model in [Ref. 2, 5] is not precise enough to enable verification of spacing properties. In this paper, we described 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.

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 [Ref. 3], 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 at the IAF's.

There are two types of entry procedures: *vertical entry* and *lateral entry*. In a vertical entry, an aircraft 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 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* and the segment between the IF and the runway threshold is called *final segment*. Henceforth, we say that an aircraft is *on final approach* if it is in the base of 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 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 MAHF.

[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.

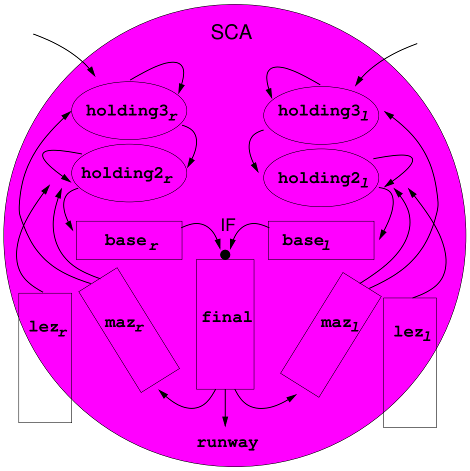


Figure 2: Discrete view of SCA

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 shall guarantee 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 also separated can be verified using the techniques presented in this paper.

DISCRETE MODEL AND ITS LIMITATIONS

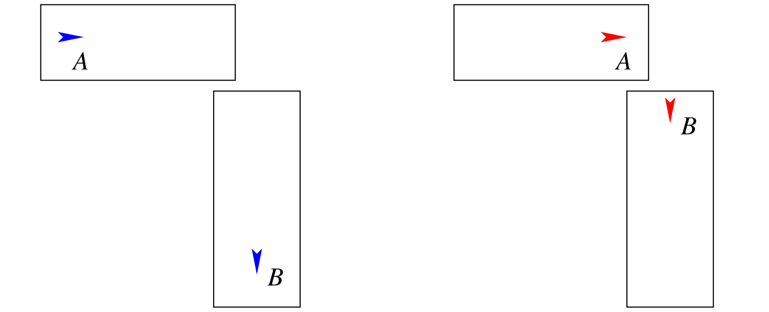
The discrete model described in [Ref. 2, 5] is a mathematical abstraction of the SATS HVO concept. A simple way to visualize that model is via an analogy with a board game where the board is a discretized SCA, the pieces that move across the board are the aircraft, and the rules of the game are given 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`.

[2] Lateral entry zones start outside the SCA.



(a) Aircraft A and B are separated

(b) Aircraft A and B are not separated

Figure 3: Indistinguishable discrete states

- Approach initiation (left, right): Move from `holding2` to `base`.
- Final approach (left, right): Move from `base` to `final`.
- 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`.

In this model, 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 AMM is modeled by the next available landing sequence (natural number) and the next alternating missed approach holding fix (left or right).

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. Of course, this cannot be proved formally. However, the model has been extensively reviewed by the developers of the SATS HVO concept as it was used as a designing tool of the final concept [Ref. 2].

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, it turns out that the transition system is finite. Indeed, it was exhaustively explored [Ref. 5] using the verification system PVS [Ref. 7]. Among several other properties, it was formally verified that the model of the SATS HVO concept allows up to four simultaneous arrival approaches, which is better than the current one-in/one-out mode of operation, and that eventually all aircraft land or depart, i.e., there are no deadlocks.

The discrete model does not support verification of spacing properties. In particular, the two states depicted in Figure 3 are indistinguishable by the discrete model, although they do not satisfy the same separation requirements. This behavior is due to the way the approach initiation procedure was written in the discrete model. Indeed, the concept of operations states that an aircraft 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 [Ref. 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, this value is configurable according to the geometry of the SCA. Since the geometry of the aircraft is not considered in the discrete model, the approach initiation procedure has to be modified. 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). As 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 accurate 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. Before that, we formally specify the spacing requirements.

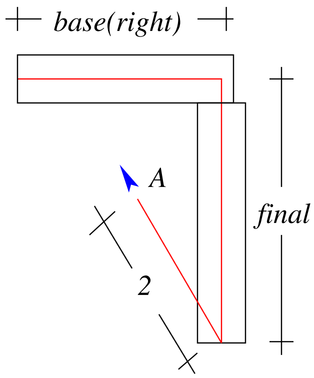


Figure 4: Linear distance from IAF

SPACING REQUIREMENTS

The term *spacing* refers to linear separation of an aircraft with respect to a lead aircraft. If both aircraft are not flying the same approach, spacing is usually computed relative 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.

Assume that the geometry of the SCA is described by $base(\mathit{left})$, $base(\mathit{right})$, *final*, $maz(\mathit{left})$, and $maz(\mathit{right})$, which are the lengths of the left and right base segments, final segment, and left and right missed approach zones, respectively. We define $D_A(t)$ as the linear distance at time t of an aircraft A from its initial approach fix. For instance, in Figure 4,

$$D_A(t) \quad = \quad base(\mathit{right}) + \mathit{final} + 2. \tag{1}$$

In a symmetric SCA, i.e., $base(\mathit{left}) = base(\mathit{right})$ and $maz(\mathit{left}) = maz(\mathit{right})$, 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

$$S_{A \to B}(t) \quad \equiv \quad D_B(t) - D_A(t) + base(\mathit{iaf}_A) - base(\mathit{iaf}_B). \tag{2}$$

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:*

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

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:*

$$S_{MAZ} \quad \leq \quad S_{A \to B}(t). \tag{4}$$

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, i.e., $v_{\min}$ and $v_{\max}$, and the initial spacing between the aircraft, i.e., S_0, as follows:

$$S_T \quad \equiv \quad S_0 - (L_{max} + \mathit{final} - S_0)\Delta_v, \tag{5}$$

$$S_{MAZ} \quad \equiv \quad \min(L_{min} + \mathit{final} - L_{maz}\Delta_v, 2S_0 - (L_{max} + \mathit{final} + L_{maz} - S_0)\Delta_v), \tag{6}$$

where

$$\begin{aligned} L_{min} &\equiv \min(\mathit{base}(\mathit{left}), \mathit{base}(\mathit{right})), & (7)\\ L_{max} &\equiv \max(\mathit{base}(\mathit{left}), \mathit{base}(\mathit{right})), & (8)\\ L_{maz} &\equiv \max(\mathit{maz}(\mathit{left}), \mathit{base}(\mathit{right})), & (9)\\ \Delta_v &\equiv \frac{v_{\max} - v_{\min}}{v_{\min}}. & (10) \end{aligned}$$

HYBRID MODEL

The hybrid model of the SATS HVO concept extends the discrete state of the original model 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, i.e., $D_A(t)$. 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

  $$(t_1 - t_0)v_{\min} \leq D_A(t_1) - D_A(t_0) \leq (t_1 - t_0)v_{\max}, \quad (11)$$

  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

  $$S_0 \leq S_{A \to B}(t). \quad (12)$$

Other transitions have to be modified as well to handle the new variables:

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

  $$D_A(t) = \mathit{base}(\mathit{iaf}_A). \quad (13)$$

- *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

  $$D_A(t) = \mathit{base}(\mathit{iaf}_A) + \mathit{final}. \quad (14)$$

- *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

  $$D_A(t) = \mathit{base}(\mathit{iaf}_A) + \mathit{final}. \quad (15)$$

- *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

  $$D_A(t) = \mathit{base}(\mathit{iaf}_A) + \mathit{final} + \mathit{maz}(\mathit{mahf}_A). \quad (16)$$

In the next section, we show how Propositions 1 and 2 can be mechanically verified on this hybrid transition system.

MECHANICAL VERIFICATION

The discrete model of the SATS HVO concept was written in PVS and verified using a state exploration PVS tool called Besc [Ref. 5]. 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 [Ref. 4], were unsuccessful due to the complexity 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.

We first note that the discrete system is a valid abstraction of the SATS HVO concept. From a high level, all the reachable states in the hybrid system are reachable in the discrete system (modulo the common discrete variables). 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 requirements should not be reachable in the hybrid system. Therefore, if we take all the reachable states in the discrete system and eliminate those that do not satisfy the continuous behavior expressed by Formulas (12)–(16), we should still have a valid abstraction of the SATS HVO concept.

Instead of eliminating states, we simply add the continuous behavior as constraints to the reachable states in the discrete system at the same time as the transitions take place. For instance, after a *Merging* rule, according to Formula (13), it should hold that

$$base(\mathit{iaf}_A) \ \leq\ D_A(t) \ \leq\ base(\mathit{iaf}_A) + \mathit{final}. \tag{17}$$

The semantics of a constrained state is that it is a valid reachable state if it is reachable in the discrete system and, moreover, all its constraints hold. The verification objective is to show that for each one of these hybrid reachable states, Propositions 1 and 2 hold.

Hybrid System as a Constrained Discrete System

In order to write the hybrid system as a discrete transition system, the continuous behaviors is encoded using *symbolic* constraints. A PVS data type, called `Constraint`, is inductively defined according to the following grammar:

$$\begin{aligned}
A, B &::= 1, 2, \ldots && (18)\\
s &::= \mathit{left} \mid \mathit{right} \mid \mathit{iaf}_A \mid \mathit{mahf}_A && (19)\\
T &::= t \mid T_A && (20)\\
e, f &::= T \mid D_A(T) \mid base(s) \mid \mathit{final} \mid maz(s) \mid S_0 \mid L_{min} \mid L_{max} \mid L_{maz} \mid S_{A\to B}(T) \mid e + f && (21)\\
\texttt{Constraint} &::= e \leq f && (22)
\end{aligned}$$

We use the variable T_A to denote the time when aircraft A initiates the approach.

The global state of the SCA is extended with a new field `constraints`, which is a list of `Constraints` that hold at a particular state. The hybrid transition system described before is encoded as follows:

- *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 to `constraints`:
  - The fact that A is in the base segment, i.e,

$$\begin{aligned} T_A &\leq t, && (23)\\ D_A(t) &\leq base(\mathit{iaf}_A). && (24)\end{aligned}$$

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

$$\begin{aligned} T_B &\leq T_A, && (25)\\ S_0 &\leq S_{A\to B}(T_A). && (26)\end{aligned}$$

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

$$base(\mathit{iaf}_A) + \mathit{final} \quad\leq\quad D_C(T_A). \tag{27}$$

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

- *Merging*: Let A be that aircraft that goes into the final segment. Constraint (24) is removed from `constraints`. Moreover, the fact that A is in the final segment is added to `constraints`:

$$D_A(t) \quad \leq \quad \mathit{base}(\mathit{iaf}_A) + \mathit{final}. \tag{28}$$

- *Missed approach initiation*: Let A be the aircraft that initiates the missed approach. Constraint (28) is removed from `constraints`. Moreover, the fact that A is on missed approach is added to `constraints`:

$$D_A(t) \quad \leq \quad \mathit{base}(\mathit{iaf}_A) + \mathit{final} + \mathit{maz}(\mathit{mahf}_A). \tag{29}$$

- *Landing*: Let A be the aircraft that is landing. All constraints related to A are removed from `constraints` except instances of Constraints (25) and(26) 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 `constraints`.

State Exploration

To verify Propositions 1 and 2, we have to prove the following invariant properties for every reachable state s.

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,*

$$\texttt{constraints}(s) \quad \Longrightarrow \quad S_T \ \leq \ S_{A \to B}(t). \tag{30}$$

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,*

$$\texttt{constraints}(s) \quad \Longrightarrow \quad S_{MAZ} \ \leq \ S_{A \to B}(t). \tag{31}$$

We remark that the constraints are just data without any 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 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 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.

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, the proof scripts are checked in batch mode via the utilities provided by ProofLite.[5] After a couple of minutes, ProofLite reports that all 117 lemmas are proved in PVS.

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. The rest of this section sketches the proof of these lemmas.

Three Lemmas

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,

$$D_A(T_A) \quad = \quad 0. \tag{32}$$

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

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

Therefore, Constraint (26) is equivalent to

$$S_0 + \mathit{base}(\mathit{iaf}_B) - \mathit{base}(\mathit{iaf}_A) \quad \leq \quad D_B(T_A). \tag{33}$$

Furthermore, if A is on final approach at time t, Constraint (24) and Constraint (28) yield

$$D_A(t) \quad \leq \quad \mathit{base}(\mathit{iaf}_A) + \mathit{final}. \tag{34}$$

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*

$$S_0 - (L_{max} + \mathit{final} - S_0)\Delta_v \quad \leq \quad S_{A\to B}(t), \tag{35}$$

under the hypotheses

$$\begin{aligned} T_A \quad &\leq \quad t && (36)\\ S_0 + \mathit{base}(\mathit{iaf}_B) - \mathit{base}(\mathit{iaf}_A) \quad &\leq \quad D_B(T_A), && (37)\\ D_B(t) \quad &\leq \quad \mathit{base}(\mathit{iaf}_B) + \mathit{final}. && (38)\end{aligned}$$

(Formula (36) *is the Constraint* (23)*, Formula* (37) *is the spacing constraint from Formula* (33)*, and Formula* (38) *is the instantiation of Formula* (34) *on aircraft B, which is on final approach.)*

Proof. Subtracting Formula (37) from Formula (38), we get

$$D_B(t) - D_B(T_A) \quad \leq \quad \mathit{base}(\mathit{iaf}_A) + \mathit{final} - S_0. \tag{39}$$

Using Formula (11) on A and B,

$$\begin{aligned} (t - T_A)v_{\min} \quad &\leq \quad D_B(t) - D_B(T_A), && (40)\\ D_A(t) - D_A(T_A) \quad &\leq \quad (t - T_A)v_{\max}. && (41)\end{aligned}$$

Formula 41 yields

$$D_A(t) \quad \leq \quad (t - T_A)v_{\max}. \tag{42}$$

From Formulas (39) and (40),

$$t - T_A \quad \leq \quad \frac{\mathit{base}(\mathit{iaf}_A) + \mathit{final} - S_0}{v_{\min}}. \tag{43}$$

Hence,

$$\begin{aligned} S_{A\to B}(t) \quad &= \quad D_B(t) - D_A(t) + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_B)\\ &= \quad D_B(T_A) + (D_B(t) - D_B(T_A)) - D_A(t) + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_B)\\ &\geq \quad S_0 + (D_B(t) - D_B(T_A)) - D_A(t), \quad \text{by Formula (37),}\\ &\geq \quad S_0 + (t - T_A)v_{\min} - (t - T_A)v_{\max}, \quad \text{by Formulas (40) and (42),}\\ &\geq \quad S_0 - (\mathit{base}(\mathit{iaf}_A) + \mathit{final} - S_0)\frac{v_{\max} - v_{\min}}{v_{\min}}, \quad \text{by Formula (43),}\\ &\geq \quad S_0 - (L_{max} + \mathit{final} - S_0)\Delta_v, \quad \text{by Formulas (8) and (10).}\end{aligned}$$

□

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*

$$L_{min} + \mathit{final} - L_{maz}\Delta_v \quad \leq \quad S_{A\to B}(t), \tag{44}$$

under the hypotheses

$$\begin{aligned} T_A \quad &\leq \quad t && (45)\\ D_B(t) \quad &\leq \quad \mathit{base}(\mathit{iaf}_B) + \mathit{final} + \mathit{maz}(\mathit{mahf}_B), && (46)\\ \mathit{base}(\mathit{iaf}_B) + \mathit{final} \quad &\leq \quad D_B(T_A). && (47)\end{aligned}$$

(Formula (45) *is the Constraint* (23)*, Formula* (46) *is the instantiation of Constraint* (29) *on aircraft B, and Formula* (47) *is the additional assumption about aircraft A and B.)*

Proof. Subtracting Formula (47) from Formula (46), we get

$$D_B(t) - D_B(T_A) \quad \leq \quad maz(\mathit{mahf}_B). \tag{48}$$

Formulas (40)–(42) are derived as in Lemma 1. From Formulas (40) and (48),

$$t - T_A \quad \leq \quad \frac{maz(\mathit{mahf}_B)}{v_{\min}}. \tag{49}$$

Hence,

$$\begin{aligned}
S_{A\to B}(t) &= D_B(t) - D_A(t) + base(\mathit{iaf}_A) - base(\mathit{iaf}_B)\\
&= D_B(T_A) + (D_B(t) - D_B(T_A)) - D_A(t) + base(\mathit{iaf}_A) - base(\mathit{iaf}_B)\\
&\geq base(\mathit{iaf}_A) + \mathit{final} + (D_B(t) - D_B(T_A)) - D_A(t), \quad \text{by Formula (47)},\\
&\geq base(\mathit{iaf}_A) + \mathit{final} + (t - T_A)v_{\min} - (t - T_A)v_{\max}, \quad \text{by Formulas (40) and (42)},\\
&\geq base(\mathit{iaf}_A) + \mathit{final} - maz(\mathit{mahf}_B)\frac{v_{\max} - v_{\min}}{v_{\min}}, \quad \text{by Formula (49)},\\
&\geq L_{min} + \mathit{final} - L_{maz}\Delta_v, \quad \text{by Formulas (7), (9), and (10).}
\end{aligned}$$

□

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*

$$2S_0 - (L_{max} + \mathit{final} + L_{maz} - S_0)\Delta_v \quad \leq \quad S_{A\to B}(t), \tag{50}$$

under the hypotheses

$$\begin{aligned}
T_A &\leq t & (51)\\
T_X &\leq T_A & (52)\\
D_B(t) &\leq base(\mathit{iaf}_B) + \mathit{final} + maz(\mathit{mahf}_B), & (53)\\
S_0 + base(\mathit{iaf}_B) - base(\mathit{iaf}_X) &\leq D_B(T_X), & (54)\\
S_0 + base(\mathit{iaf}_X) - base(\mathit{iaf}_A) &\leq D_X(T_A). & (55)
\end{aligned}$$

(Formula (51) *is the Constraint* (23)*, Formula* (52) *is the instantiation of Constraint* (25) *on aircraft X and A, Formula* (53) *is the instantiation of Constraint* (29) *on aircraft B, and Formulas* (54) *and* (55) *are the additional assumptions about aircraft A, B, and X.)*

Proof. Subtracting Formula (54) from Formulas (53), we get

$$D_B(t) - D_B(T_X) \quad \leq \quad base(\mathit{iaf}_X) + \mathit{final} + maz(\mathit{mahf}_B) - S_0. \tag{56}$$

Formula (42) is derived as in Lemma 1. From Formula (32), $D_X(T_X) = 0$. Therefore, using Formula (11) on X,

$$D_X(T_A) \quad \leq \quad (T_A - T_X)v_{\max}. \tag{57}$$

From Formulas (51) and (52), $T_X \leq t$. Using Formula (11) on B,

$$(t - T_X)v_{\min} \quad \leq \quad D_B(t) - D_B(T_X). \tag{58}$$

From Formulas (56) and (58),

$$t - T_X \quad \leq \quad \frac{base(\mathit{iaf}_X) + \mathit{final} + maz(\mathit{mahf}_B) - S_0}{v_{\min}}. \tag{59}$$

Hence,

$$
\begin{aligned}
S_{A\to B}(t) &= D_B(t) - D_A(t) + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_B) \\
&= D_B(T_X) + (D_B(t) - D_B(T_X)) - D_A(t) + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_B) \\
&\geq S_0 + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_X) + (D_B(t) - D_B(T_X)) - D_A(t), \\
&\quad \text{by Formula (54)}, \\
&\geq S_0 + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_X) + (t - T_X)v_{\min} - (t - T_A)v_{\max}, \\
&\quad \text{by Formulas (42) and (58)}, \\
&= S_0 + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_X) - (t - T_x)(v_{\max} - v_{\min}) + (T_A - T_X)v_{\max} \\
&\geq S_0 + \mathit{base}(\mathit{iaf}_A) - \mathit{base}(\mathit{iaf}_X) - (t - T_x)(v_{\max} - v_{\min}) + D_X(T_A), \\
&\quad \text{by Formula (57)}, \\
&\geq 2S_0 - (t - T_x)(v_{\max} - v_{\min}), \quad \text{by Formula (55)}, \\
&\geq 2S_0 - (\mathit{base}(\mathit{iaf}_X) + \mathit{final} + \mathit{maz}(\mathit{mahf}_B) - S_0)\frac{v_{\max} - v_{\min}}{v_{\min}}, \\
&\quad \text{by Formula (59)}, \\
&\geq 2S_0 - (L_{max} + \mathit{final} + L_{maz} - S_0)\Delta_v, \quad \text{by Formulas (8), (9), and (10).}
\end{aligned}
$$

□

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

$$\min(L_{min} + \mathit{final} - L_{maz}\Delta_v, 2S_0 - (L_{max} + \mathit{final} + L_{maz} - S_0)\Delta_v) \quad \leq \quad S_{A\to B}(t). \tag{60}$$

Furthermore,

$$S_{MAZ} \quad = \quad 2S_0 - (L_{max} + \mathit{final} + L_{maz} - S_0)\Delta_v, \tag{61}$$

when

$$1 + \frac{v_{\min}}{v_{\max}} \quad \leq \quad \frac{L_{min} + \mathit{final}}{S_0}, \tag{62}$$

and

$$S_t \quad \leq \quad S_{MAZ}, \tag{63}$$

when

$$L_{maz}\Delta_v \quad \leq \quad S_0. \tag{64}$$

CONCLUSION

This papers proposes a hybrid model that extends the discrete model presented in [Ref. 2]. In contrast to the original model, the proposed model enables the verification of safety spacing requirements of SATS HVO operations. To this end, aircraft performances, such as ground speed ranges, and information about the SCA geometry, such as length of the approach segments, were integrated into the original model. Thus, in the hybrid model, the concept of operations is described by the continuous dynamics of aircraft and the discrete events within the SCA. Using theorem proving and model checking techniques, we have exhaustively explored the hybrid model and mechanically verified spacing requirements over all nominal operations.

The SATS HVO 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.

From a practical point of view, the analytical formulas presented in this paper, e.g., Formulas (5) and (6), can be used to configure a nominal SCA and the parameters of the baseline procedure for self-separation. For instance, consider a

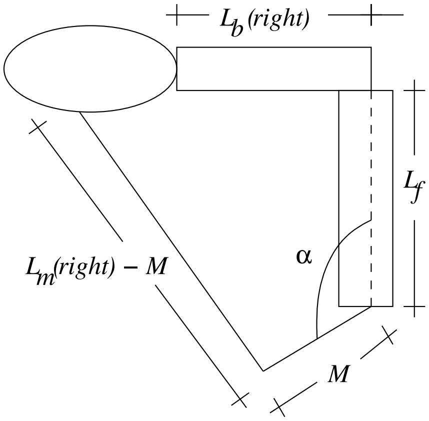


Figure 5: Nominal SCA

symmetric nominal SCA where $base(\textit{left}) = base(\textit{right}) = 5$ nm, $\textit{final} = 10$ nm, and $maz(\textit{left}) = maz(\textit{right}) = 13$ nm. If the initial separation S_0 is 6 nm and $v_{\min} = 90$ kt, $v_{\max} = 120$ kt, then

$$L_{min} = L_{max} = 5 \text{ nm}, \tag{65}$$

$$L_{maz} = 13 \text{ nm}, \quad \text{and} \tag{66}$$

$$\Delta_v = \frac{120 - 90}{90} = \frac{1}{3}. \tag{67}$$

The value of S_T is computed using Formula (5):

$$S_T = 6 - \frac{5 + 10 - 6}{3} = 3 \text{ nm}. \tag{68}$$

This configuration of the SCA satisfies Formula (62). Therefore, the value of S_{MAZ} can computed using Formula (61):

$$S_{MAZ} = 12 - \frac{5 + 10 + 13 - 6}{3} = 4.66 \text{ nm}. \tag{69}$$

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 analysis used in this paper can be extended to study Euclidean separation of aircraft on final approach and missed approach. Figure 5 illustrates a nominal SCA where aircraft on missed approach turn toward their missed approach zone α degrees with respect to the runway, fly a straight trajectory of M nautical miles, and then turn to their MAHF. A geometric analysis reveals that

$$M = \frac{\min(S_T, S_{MAZ})}{2} \tag{70}$$

achieves maximum separation for an arbitrary α. In this case, the minimum Euclidean distance D_α that the concept guarantees for an aircraft on final approach and an aircraft on missed approach is given by

$$D_\alpha = M\sqrt{2(1 - \cos\alpha)}. \tag{71}$$

In the example above, the optimal value of M, given by Formula (70), is 1.5 nm. The minimum Euclidean distance between an aircraft on final approach and an aircraft on missed approach, for different values of α, is computed using Formula (71):

- $D_{60^o} = 1.5$ nm.
- $D_{90^o} = 2.12$ nm.
- $D_{120^o} = 2.59$ nm.

Increasing the initial spacing S_0 to 7 nm yields the following values: $S_T = 4.33$ nm, $S_{MAZ} = 7$ nm, $M = 2.16$ nm, $D_{60^o} = 2.16$ nm, $D_{90^o} = 3.06$ nm, and $D_{120^o} = 3.75$ nm.

The mechanical verification is necessary to make sure that no cases were forgotten. For instance, the fact that Lemmas 1, 2, and 3 are sufficient to prove the spacing requirements for all nominal scenarios is shown by enumerating all the possibilities (in this case 117) and mechanically proving all of them using these 3 lemmas. 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. 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.

3. *Federal Aviation Regulations/Aeronautical Information Manual*, 1999.

4. 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.

5. 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.

6. SATS Program Office. Small aircraft transportation system program plan. http://sats.larc.nasa.gov/documents.html, 2001.

7. 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.