Safety Verification of the Small Aircraft Transportation System Concept of Operations

Victor Carreño [1]
NASA Langley Research Center, Hampton, Virginia, 23681

César Muñoz [2]
National Institute of Aerospace, Hampton, Virginia, 23666

A critical factor in the adoption of any new aeronautical technology or concept of operation is safety. Traditionally, safety is accomplished through a rigorous process that involves human factors, low and high fidelity simulations, and flight experiments. As this process is usually performed on final products or functional prototypes, concept modifications resulting from this process are very expensive to implement. This paper describe an approach to system safety that can take place at early stages of a concept design. It is based on a set of mathematical techniques and tools known as *formal methods*. In contrast to testing and simulation, formal methods provide the capability of exhaustive state exploration analysis. We present the safety analysis and verification performed for the Small Aircraft Transportation System (SATS) Concept of Operations (ConOps). The concept of operations is modeled using discrete and hybrid mathematical models. These models are then analyzed using formal methods. The objective of the analysis is to show, in a mathematical framework, that the concept of operation complies with a set of safety requirements. It is also shown that the ConOps has some desirable characteristic such as liveness and absence of dead-lock. The analysis and verification is performed in the Prototype Verification System (PVS), which is a computer based specification language and a theorem proving assistant.

I. Introduction

The Small Aircraft Transportation System (SATS) is a program with the objective of increasing the access to small airports, which might lack tower and radar services [1]. The SATS Concept of Operations for High Volume Operation (SATS ConOps-HVO) has been developed by a team at NASA Langley in partnership with industry and the FAA [2]. The SATS ConOps is a significant departure from conventional operations in controlled airspace. The SATS ConOps include three elements which makes it unconventional: 1. A special designation self controlled airspace (SCA) surrounding the airport where Air Traffic Control services are not provided and pilots have responsibility for separation in IMC; 2. An automated Airport Management Module (AMM) which grants or denies entry to the SCA and sequence aircraft; 3. On-board tools which provide collision avoidance advisories and guidance to the crew to comply with the ConOps rules.

The acceptability and viability of a concept of operation hinges on its safety. Proposed changes in operations or new concepts require verification of their safety and benefits. Operations that deviate from standard operations must demonstrate that they do not represent an increased risk to crew and passengers, people on the ground, and that they do not have a detrimental effect to the National Airspace System (NAS).

This paper describe the method used for the safety verification of the SATS ConOps. The method is based on

[1] Senior Research Engineer, SCASB, victor.a.carreno@nasa.gov, MS130 NASA Langley RC, Hampton, Virginia.
[2] Senior Research Scientist, Formal Methods Team, munoz@nianet.org, 100 Exploration Way, Hampton, Virginia.

formal methods, a set of mathematical techniques and computer aided tools based on logic, formal deduction, and exhaustive state exploration. The verification has been accomplished in two stages: 1. The development of a discrete model of the ConOps where the SCA is represented by a list of discrete regions and the nominal operations are represented by a state transition system. This model enables the verification of occupancy safety requirements, e.g., there is always a miss approaching holding fix open for an aircraft performing a miss approach, and liveness properties, e.g., all aircraft eventually land or depart the SCA; 2. The extension of the discrete model with continuous variables that represent the geometry of the SCA and the speed performance parameters of the aircraft. This hybrid model enables the verification of spacing properties, e.g., under nominal operations, all the aircraft are self-separated. The main contribution of this work is the formal assurance that under all possible arrival and departure sequences, key safety properties hold for the concept of operations and that some desirable efficiency properties are preserved.

The rest of this paper is organized as follows. Sections II gives an overview of the ConOps. Section III and IV describe the discrete and hybrid models, respectively. Section V presents the safety properties that have been formally verified using those models. The last section is the summary and conclusion.

II. Concept of Operations

The concept of operation is a set of rules and procedures which support separation, orderly arrival, and increased throughput during IMC to airports lacking radar coverage and control tower. The ConOps is implemented by means of the Self Control Airspace (SCA), the Airport Management Module (AMM), on-board navigation tools, and data communication including ADS-B (Automated Dependent Surveillance-Broadcast) and data link. The SCA is a special designation airspace surrounding the airport. Typically, the SCA covers a radius of 12 nautical miles and 3000 feet above ground. The approach is similar to a GPS T instrument approach [3]. Figure 1 shows a generic SCA approach with Initial Arrival Fixes (IAF) right and left, two holding altitudes at 2000 and 3000 feet above ground over the IAF, an intermediate fix (IF), a final approach fix (FAF), and the runway.

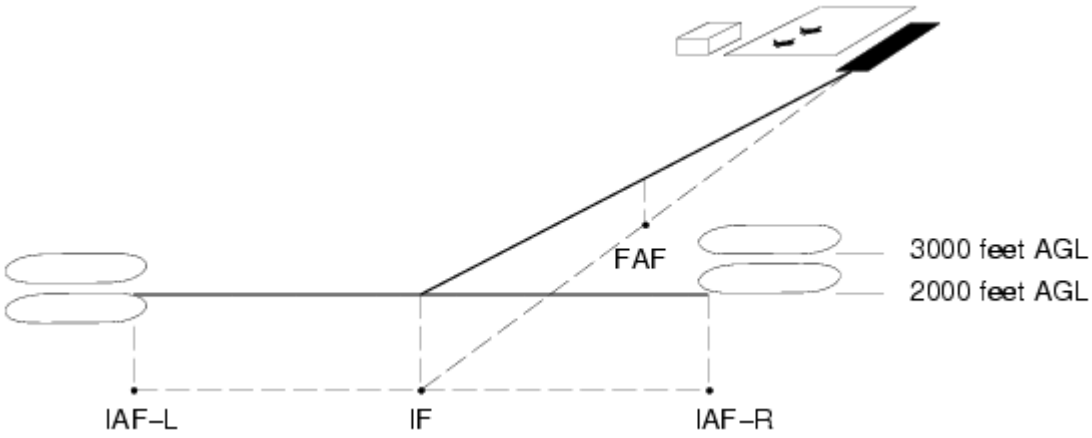

Figure 1. Generic SCA Approach.

Not shown in the generic SCA approach figure are the miss approach paths. In the generic SCA approach, the IAFs serve as the Miss Approach Holding Fixes (MAHF). An aircraft performing a miss approach will go to the MAHF that has been assigned to it by the AMM; either IAF-R or IAF-L. The aircraft will go the lowest available altitude, 2000 feet AGL or 3000 feet AGL. Part of the safety verification presented in this paper is to show that an aircraft performing a miss approach will always have a MAHF available, i.e., a MAHF that is not occupied by any other aircraft at the given altitude.

An aircraft performing an arrival approach to an airport implementing the SATS ConOps will go through the following steps:

- The aircraft will be cleared by ATC to a navigation fix near or above the SCA.

- In the vicinity of the SCA, the aircraft will request to the AMM entry to the SCA.
- If entry is not granted, the aircraft proceeds or stays at the navigation fix to which it has been cleared by ATC.
- When entry is granted by the AMM, the AMM will assign a type of entry (lateral or vertical), a lead aircraft (none if SCA is empty), and a Miss Approach Holding Fix (MAHF).
- The aircraft will perform a lateral or vertical entry (and notify ATC. ATC will terminate services.)
- The aircraft will hold at the Initial Arrival Fix (IAF) or proceed to the approach.
- The aircraft starts the approach when certain conditions are met regarding location and type of the lead aircraft.
- If aircraft does not land, it proceeds to its assigned MAHF or departs the SCA.
- Aircraft lands.

Departure operations are also described by the ConOps. For simplicity, those operations are not described in this document. A more detailed description of the concept of operations including the rules implemented by the AMM, how the vertical and lateral entry are selected, how the MAHF is selected, the criteria for starting and approach, and other conditions can be found in [2].

III. Discrete Model

The discrete model is a state transition system representing the concept of operations. The discrete model represents the operational zones of the SCA, the rules of the ConOps, and the rules implemented by the Airport Management Module. The operational zones of the SCA are shown in Figure 2.

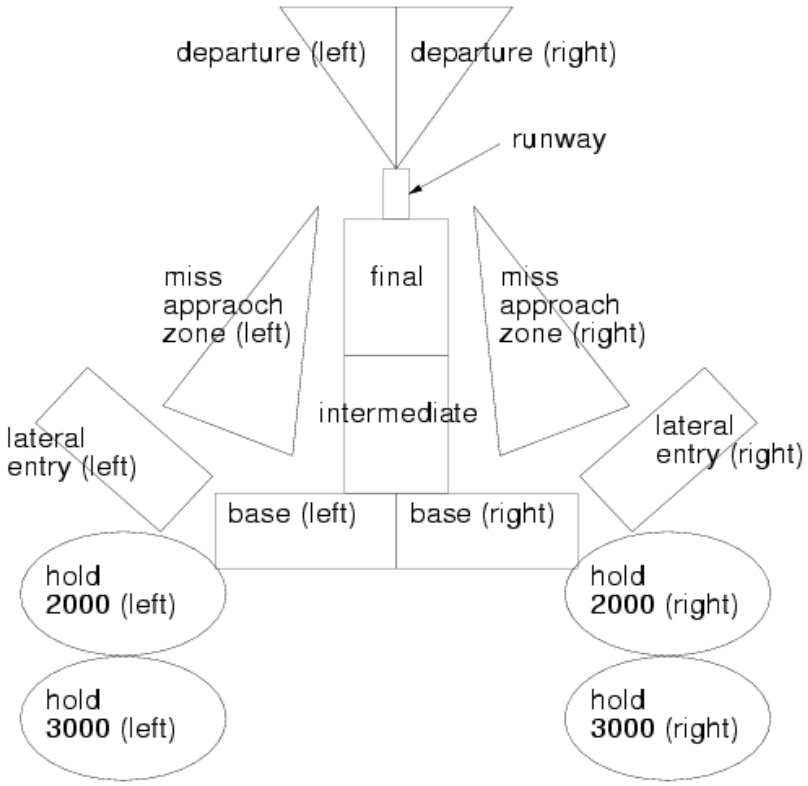

Figure 2. Operational Zones of the SCA.

Note that the operational zones might overlap geographically. For example, part of a volume might be covered both by the miss approach zone and the lateral entry zone. The state of the system is made of the state of the SCA and the state of the AMM. The state of the SCA and AMM are determined by the position of the aircraft, the lead-trail relationship between aircraft, and the miss approach holding fix assignments.

The ConOps rules determine how the system transitions from one state to the next. For example, Figure 3 shows a system state with four aircraft. Aircraft N123, N456, N789, and N101 are in the intermediate zone, hold 2000 left,

hold 3000 right, and hold 3000 left, respectively. The superscript on the aircraft identification (tail number) is its lead aircraft. The subscript is the miss approach holding fix assignment given by the AMM. The discrete model is an asynchronous and non-deterministic transition system, i.e., a discrete state can potentially transition to a new state in several ways. In this example, N123 could move to the final zone, or N456 can initiate its approach by going to base-left, or N789 could move to hold 2000 right. Therefore, the system has three new possible states. No other transitions are permitted by the ConOps rules. For example, N789 could not move to base-right because it must wait until N456 begin its approach. There are many other transitions that are disallowed by the ConOps or physically impossible; N101 should not move to hold 2000 left until the aircraft occupying this zone has departed the zone and N789 could not move to the runway zone because this is physically impossible before going through other operational zones.

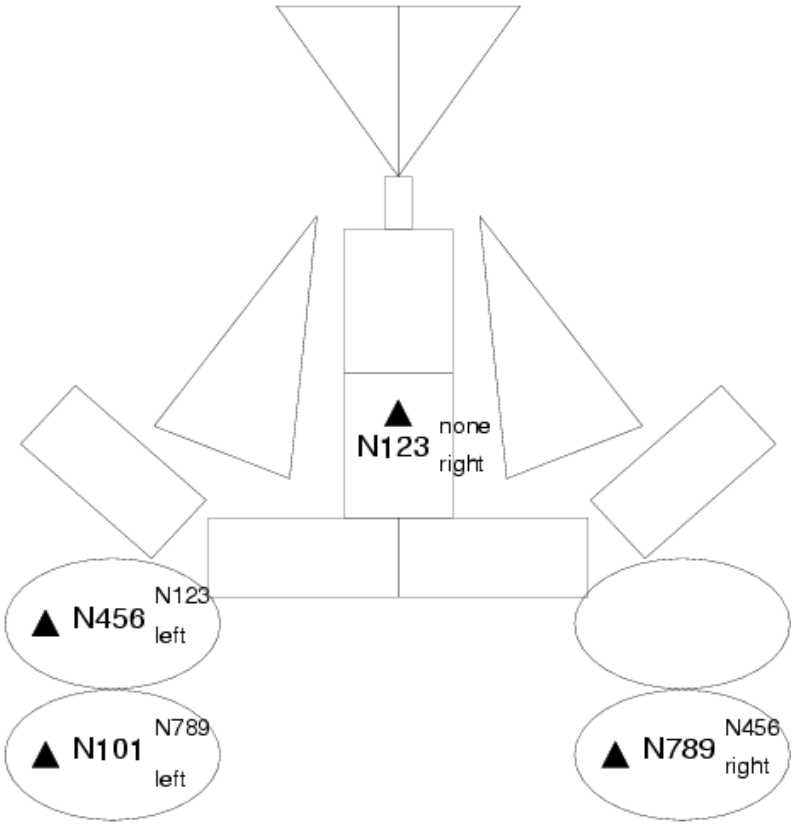

Figure 3. State Transition System Example.

The ConOps operational rules are encoded into 24 transitions. The sixteen transitions corresponding to arrival operations are:

- Vertical entry (left, right): Initial transition to hold at 3000 feet.
- Lateral entry (left, right): Initial transition to lateral entry.
- Descend (left, right): Transition from hold at 3000 feet to hold at 2000 feet.
- Approach initiation (left, right): Transition from hold at 2000 feet to base segment.
- Merging (left,right): Transition from base segment to intermediate segment.
- Final approach: Transition from intermediate segment to final segment.
- Landing: Transition from final segment to runway.
- Missed approach initiation (left, right): Move from final segment to missed approach zone.
- Lowest available altitude (left, right). Transition from missed approach zone to hold at 2000 feet or 3000 feet.

Using the transition system, an exhaustive state exploration analysis is performed to determine if the ConOps

meets all of the Safety requirements. Including departure operations, there is a total of 54280 reachable states for the system. A custom depth-first search algorithm has been developed to perform the state exploration analysis [4]. This search algorithm has been shown to be correct using the PVS proof assistant [5].

Figure 4. Indistinguishable Discrete States Showing Different Separation Distances.

IV. Hybrid Model

The discrete model does not support verification of spacing properties. For example, the two states depicted in Figure 4 are indistinguishable by the discrete model, although they do not satisfy the same spacing requirements. 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 usually 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 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.

In the ConOps, self-spacing is mainly achieved via the approach initiation procedure, i.e., the procedure that describes when an aircraft that is holding at 2000 feet is allowed to initiate the approach and transition to the base segment. This procedure shall guarantee that aircraft on final approach are separated all the way to the completion of the landing operation, even if they have to perform a missed approach. Therefore, under nominal operations, the second case in Figure 4 shall never occur.

The approach initiation procedure 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 (base, intermediate, or final segments) [2]. There are several ways a pilot can check whether the safety threshold is satisfied or not. In the most conservative case, the pilot delays the approach initiation until it is spaced S_o nautical miles with respect to the lead aircraft. The value S_o is a configurable parameter that depends on the geometry of the SCA and the speed performance parameters of the aircraft.

Since distances of SCA and performance of the aircraft are not considered in the discrete model, the discrete transition rule representing the approach initiation procedure uses a weaker condition (b) where an aircraft can initiate the approach as soon as the lead aircraft is already on the final approach. In order to verify spacing properties, a more accurate model of the approach initiation procedure is required. To this end, the discrete model of the SATS HVO concept is extended with continuous variables that encode the geometry of the SCA and the aircraft speed performances. In particular, the SCA is described by the lengths of the base, intermediate, and final segments, and the length of the missed approach zone. Furthermore, for each aircraft, we consider the time when the aircraft initiates the approach and the distance from its IAF at any given moment in time. Finally, we assume that ground speed of all aircraft is in a range defined by a minimum and maximum speed.

Via those continuous variables, the hybrid approach initiation rule takes into account the initial separation threshold S_o between the trail and the lead aircraft. Therefore, in the hybrid model, the states in Figure 4 are different. It can be proved that the aircraft in the first state satisfy the spacing requirement while the aircraft in the second state do not.

State exploration of a hybrid system is technically difficult due to the presence of continuous behavior which

yields an infinite transition system. An encoding technique was developed in [7] where continuous variables are symbolically represented by discrete variables. As a result, the hybrid model is rewritten as a discrete one that can be finitely explored.

V. Safety Properties

Using the discrete model described in Section III, the ConOps was shown to have the following properties:

- There are no more than two aircraft assigned to a MAHF (left or right).
- The number of aircraft inside the SCA at an IAF (left or right) is less than or equal to two.
- There is at most one aircraft at hold 2000 (left or right) and at hold 3000 (left or right).
- There are no more than two aircraft at the miss approach zone (left or right).
- When an aircraft is in the lateral entry (left or right) there are no aircraft in hold 3000, hold 2000 or miss approach zone (left or right), respectively.
- There is at most one aircraft on the runway.
- Consecutive departure operations are separated.
- Aircraft land in order according to the leader relation.
- Aircraft eventually land or depart the SCA.
- There are no operational deadlocks.

The first seven properties deal with limits on the number of aircraft occupying a zone and with always having an available altitude at a MAHF for an aircraft which is executing a missed approach. It is clear that any operation should minimize the risk of collision by not permitting two aircraft at the same altitude in one holding fix. The safety aspect of the last 3 properties are less obvious. Aircraft landing order precludes overtaking in the SCA and provides orderly arrival. An aircraft eventually landing or departing means that an aircraft will not be preempted by higher priority aircraft which could lead to an indefinite hold. An operational deadlock is a situation in which one or more aircraft cannot transition any further. Figure 5 is an example of an operational deadlock. In this state, aircraft N456 has aircraft N123 as its lead. Aircraft N456 must wait for N123 to start its approach before it can start its own approach. However, N123 must descend to hold 2000 before it can start its approach and hold 2000 is occupied by N456. The possibility of this condition occurring depends on how the AMM defines the lead-trail relationship when an aircraft returns to the IAF after executing a miss approach. Based on the AMM assignment rules and the operational rules in the SCA, it can be shown that the transition system cannot reach a deadlock state such as this one.

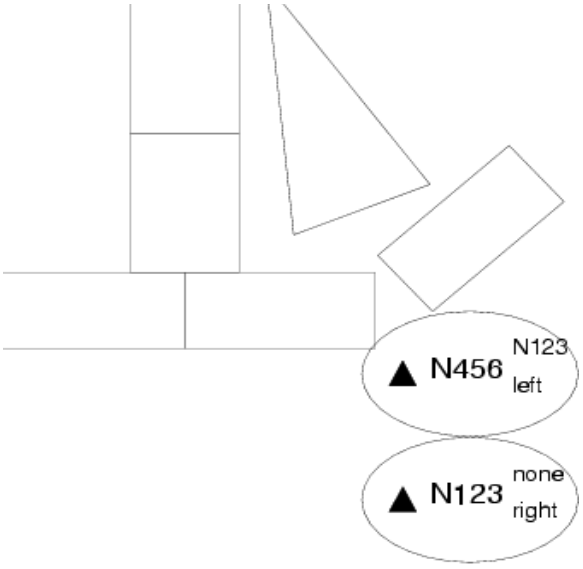

Figure 5. State Transition Deadlock Example.

The verification of spacing properties requires the hybrid system described in Section IV. The exhaustive exploration of the hybrid system has shown that the ConOps satisfies the following properties:

- Under nominal operations, all trail and lead aircraft on final approach, i.e., base, intermediate, and final segments, are separated S_t nautical miles.
- Under nominal operations, all trail and lead aircraft on missed approach are separated S_{maz} nautical miles.

The constants S_t and S_{maz} depend on the geometry of the SCA, the minimum and maximum speed of the aircraft, and the safety threshold used in the approach initiation rule. The actual formulas are described in reference [7]. For a symmetric SCA, where the base segments are 5 nautical miles, the combined intermediate and final segment is 10 nautical miles, the missed approach zone is 13 nautical, the minimum and maximum speed are 90 knots and 120 knots, respectively, and the safety threshold S_o is 6 nautical miles, the value of S_t is 3 nautical miles and the value of S_{maz} is 4.66 nautical miles. Therefore, the ConOps guarantees a minimum separation of 3 nautical miles for two aircraft, independently of these aircraft being in final approach or missed approach.

VI. Summary and Conclusion

The safety verification and analysis presented in this paper was performed in parallel with the ConOps development. The verification process influenced the ConOps through discussions and recommendations [6]. The authors believe that the verification performed in parallel with the development of the ConOps resulted in a more robust product and a more efficient development process.

Verification by exhaustive search and theorem proving have the added advantage over simulation and testing that it covers all possible system states. Simulation and testing only covers a fraction of the system state space. Two models were used in the verification of the SATS-HVO ConOps: a discrete model which captured the operations at a high level, and; a hybrid model which addressed the separation assurance inside and between the zones in the discrete model. The verification and analysis was able to demonstrate that the ConOps had the required safety properties.

7. Acknowledgments

The authors would like to thank the ConOps development team and the SATS project for discussions and cooperation with the safety and verification effort, and Gilles Dowek for his work in the development of the discrete and hybrid models presented in this paper.

8. References

[1] National Aeronautics and Space Administration Small Aircraft Transportation System (SATS) Program Planning White Paper, September, 2000.

[2] Abbot, T., Jones, K., Consiglio, M., Williams, D., Adams, C., "Small Aircraft Transportation System, Higher Volume Operations Concept: Normal Operations," NASA/TM-2004-213022, August, 2004.

[3] Jeppesen Sanderson Inc., "Federal Aviation Regulations / Aeronautics Information Manual", 1999.

[4] Muñoz, C., Dowek, G., Carreño, V., "Modeling and Verification of an Air Traffic Concept of Operations," International Symposium on Software Testing and Analysis, Boston, Massachusetts, July, 2004.

[5] Owre, S. , Rushby, J., Shankar, N., " PVS: A Prototype Verification System", International Conference on Automated Deduction, Saratoga, New York, 1992.

[6] Dowek, G., Muñoz, C., Carreño, V., "An Abstract Model of the SATS Concept of Operations: Initial Results and Recommendations", NASA/TM-2004-213006, March, 2004.

[7] Muñoz, C., Dowek, G., "Hybrid Verification of an Air Traffic Operational Concept", IEEE ISoLA Workshop on Leveraging Applications of Formal Methods, Verification, and Validation, Columbia, Maryland, September, 2005.

.