Modeling and Verification of an Air Traffic Concept of Operations

Sven Dražan
guided by Pavel Šimeček

ParaDiSe Seminar, March 3, 2008

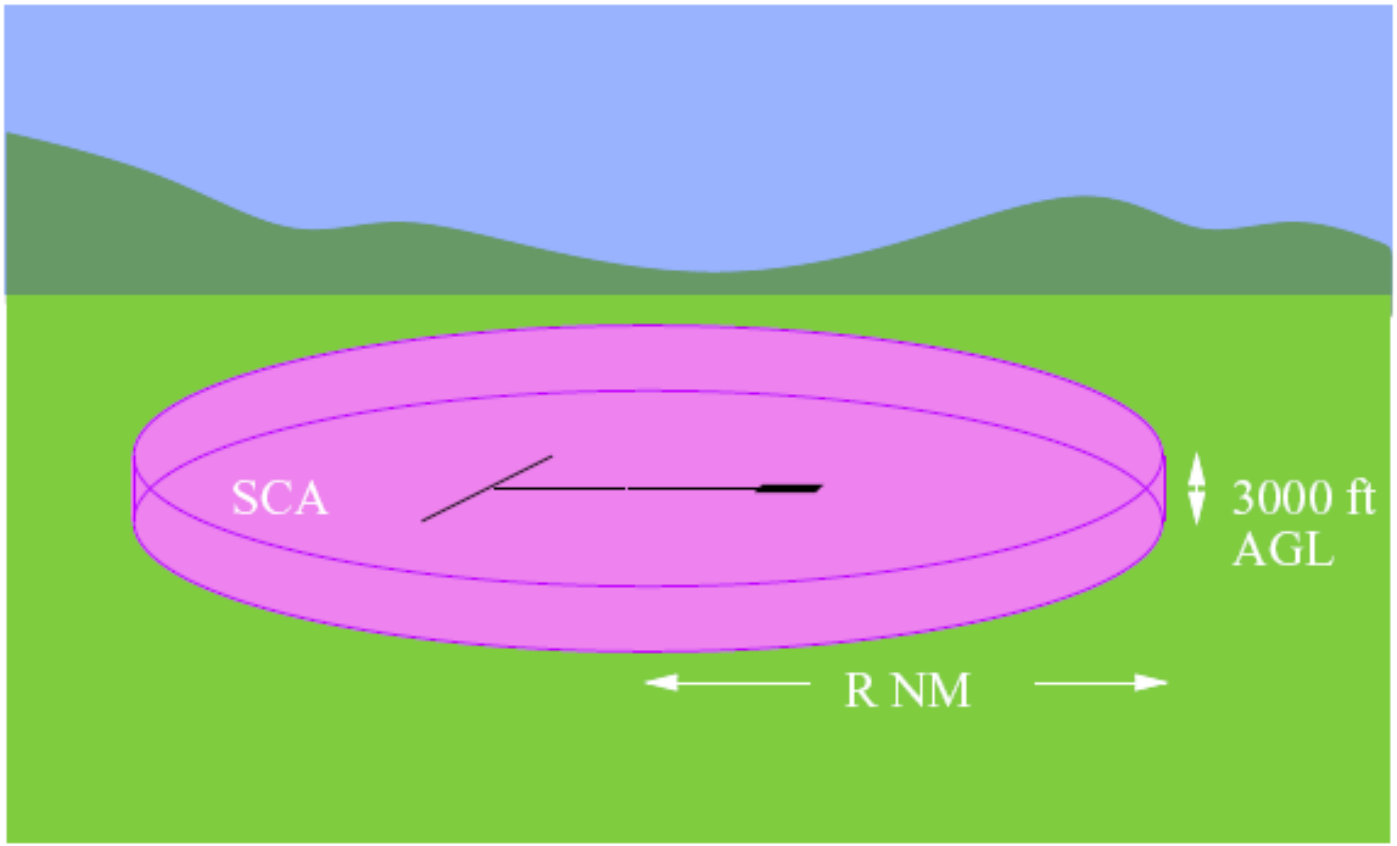
Overview

- Introduction of SATS-HVO concept
- Basic definitions
- Model
- Properties
- Verification
- Issues
- Discussion

SATS-HVO

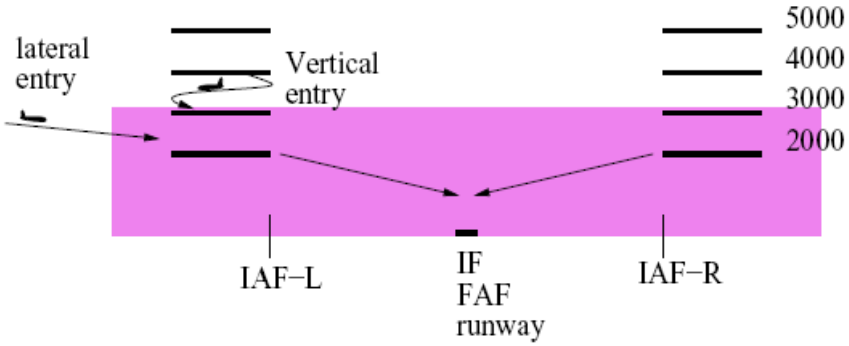
- Small Aircraft Transportation System
  - Nasa, Federal Aviation Admin, Industry, Airport authorities
- Higher Volume Operations concept
  - Problem of small airport underutilization
  - One-in/One-out separation
  - Higher throughput, same safety
- Responsibility change
  - Instrument Flight Rules, separation by Air Traffic Control
  - Separation by pilot inside Self Controled Area (SCA)

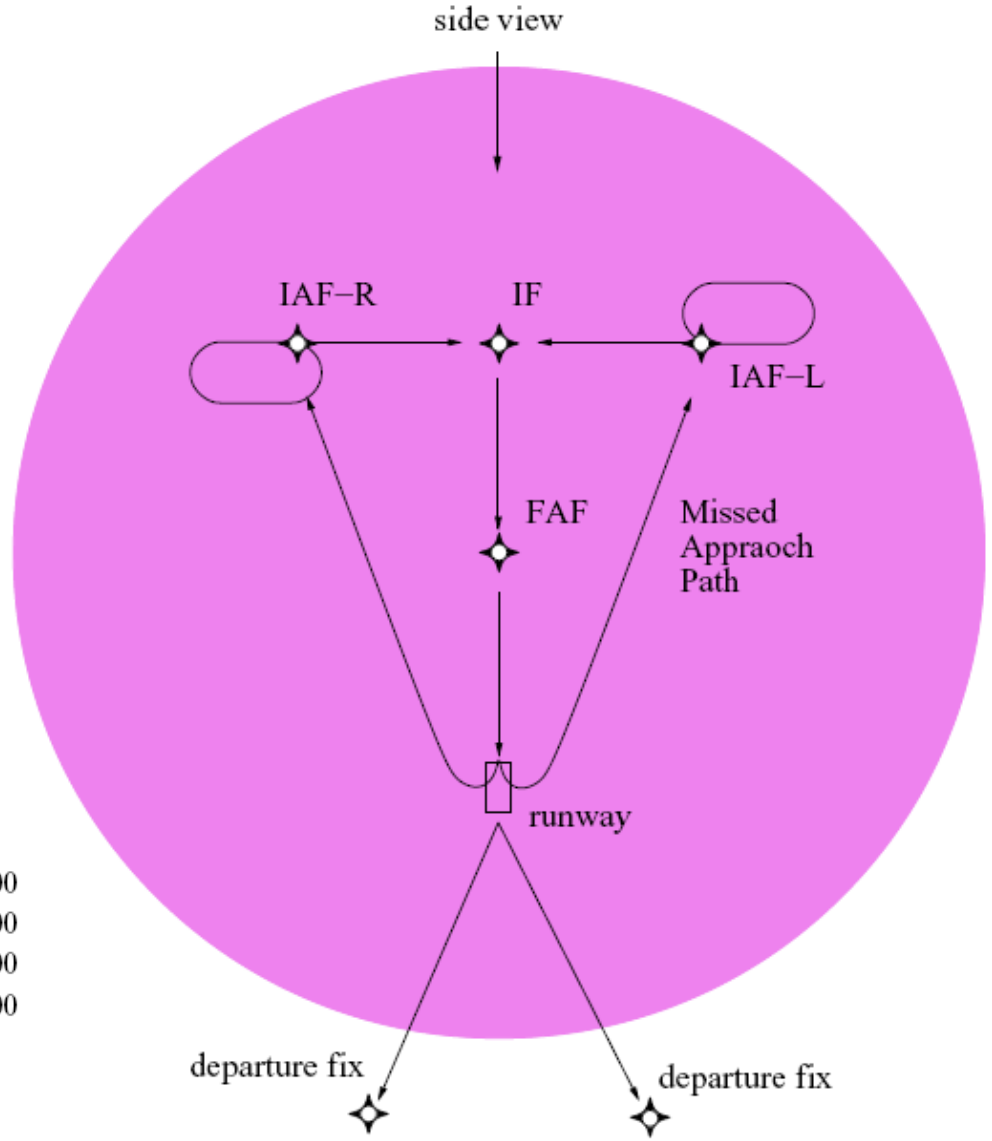
Self Controled Area – SCA



Self Controled Area – SCA

- Vertical entry
- Lateral entry
- Holding Fix
- Missed Aproach Holding Fix
- Initial Arrival Fix
- Initial Fix
- Final Approach Fix
- Runway
- Departure Fix





Airport Management Module (AMM)

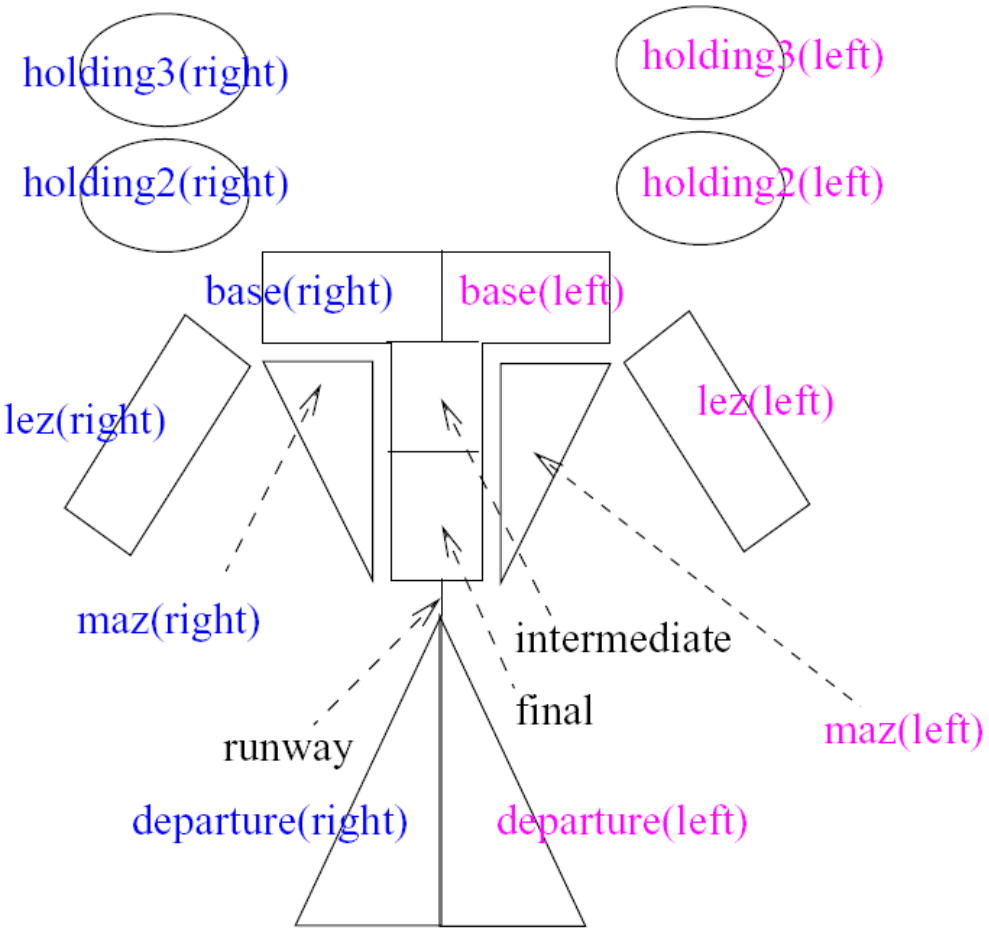
- Automated system at airport
- Data from and to aircraft via data link
- Grants entry to SCA
- Assigns Follow Notification and Missed Approach Holding Fix
- Reassigns Follow Notification and MAHF on missed approach
- Follows rules given by SATS-HVO

Rules example

- Vertical entries:
  - The AMM rules that determine if a normal (vertical) entry into the SCA is permitted are:
  - (1) There are less than 2 aircraft either at that fix or assigned to the fix, (i.e., as a missed approach holding fix), and
  - (2) no aircraft assigned to that fix as a missed approach holding fix on the approach".
  - Moreover, Alternating missed approach holding fixes are given (by the AMM) to sequential aircraft".

- Reassignments after a missed approach:
  - … once the aircraft gets within the proximity of the MAHF, the aircraft is reassigned (by the AMM) for another approach".

Model



SCA division zones

- Holding patterns at 2000 and 3000 feet
- Base segments
- Intermediate segment
- Final segment
- Runway
- Lateral entry zones
- Missed approach zones
- Departure zones
- 15 zones

Model - States

- State is defined by content of segments and state of AMM
- Each zone as FIFO of aircrafts (Follow and MAHF)

```
SCA : TYPE = [
   holding3,              % Holding Pattern 3kft
   holding2,              % Holding Pattern 2kft
   lez,                   % Lateral Entry Zone
   maz,                   % Missed Approach Zone
   base,                  % Base segment
   departure:             % Departure zone
   [Side→Zone],
   intermediate,          % Intermediate segment
   final,                 % Final segment
   runway:                % Runway
   Zone,
   nextmahf:Side,         % Next missed approach holding fix (AMM)
   nextseq:int,           % Next sequence number (AMM)
]
```

Model - Transitions

- Vertical entry (right, left)
- Lateral entry (right, left)
- Descend from 3000 to 2000 feet (right, left)
- Approach initiation for vertical entry (right, left)
- Approach initiation for lateral entry (right, left)
- Transition from base segment to intermediate segment (right, left)
- Transition from intermediate segment to final segment
- Landing
- Taxiing
- Missed approach initiation
- Determination of lowest available altitude (right, left)
- Emergency departure from SCA
- Departure initiation (right, left)
- Takeoff
- Departing from SCA (right,left)
- 24 transitions

Model - Transitions

Transitions are guided by formalised rules from SATS-HVO

Vertical entry example:

- For *side* ∈ {right, left}, a vertical entry transition may take place at the *side* IAF, only if all the following conditions hold:
- |holding3(*side*)| + |holding2(*side*)| + |maz(*side*)| + |lez(*side*)| + r < 2, where r is the number of aircraft in the opposite zones assigned to the *side* MAHF.
- No aircraft assigned to the *side* MAHF on base, intermediate, or final.
- No aircraft on maz(*side*), lez(*side*), or holding3(*side*).

Model - Transitions

Missed approach initiation example:

- A missed approach initiation transition may take place only if there is an aircraft on final.
- In the new state of the SCA, an aircraft is removed from the head of final and added to the tail of maz(side), where side is the MAHF assignment of the aircraft.
- The aircraft gets the next landing sequence from the AMM state.
- If it becomes the first aircraft, it keeps its MAHF assignment. Otherwise, it is reassigned to the next alternating missed approach fix.
- The state of the AMM and the landing sequence of the remaining aircraft are updated accordingly.

Model – Transitions

- Transitions as functions from states of SCA to lists of states of SCA
  - VerticalEntry(side:Side)(state:SCA):list[SCA] = ...
  - LateralEntry(side:Side)(state:SCA):list[SCA] = ...
  - ...
  - Landing(state:SCA):list[SCA] = ...
  - Taxiing(state:SCA):list[SCA] = ...
- Global transition Next as asynchronous composition:
  - Next(state:SCA):list[SCA] =
  - append(VerticalEntry(right)(state),
  - append(VerticalEntry(left)(state),
  - append(LateralEntry(right)(state),
  - append(LateralEntry(left)(state),
  - ...
  - append(Landing(state),Taxiing(state))))))
- Nondeterminism (Landing vs. Missed approach, Entry)

Properties

Explicitely stated from SATS-HVO or implied:

- There is always an altitude available at a missed approach holding fix for an aircraft on the arrival approach.
- Two MAHFs and two possible altitudes (2000 and 3000 feet) imply an upper bound of four simultaneous arrival operations.
- At any time and for *side* $\in$ {right, left}:
  - There are no more than two aircraft assigned to the side MAHF.
  - The number of aircraft on *side* is at most 2:
  - |holding3(*side*)| + |holding2(*side*)| + |maz(*side*)| + |lez(*side*)| $\leq$ 2
  - |holding3(*side*)|$\leq$1, |holding2(*side*)|$\leq$1, |maz(*side*)|$\leq$2
  - If there is an aircraft in lez(*side*), then holding3(*side*), holding2(*side*), and maz(*side*) are empty.

Properties

- The leader of an aircraft on base is either on the - final approach or the first aircraft on the opposite base segment.
- Aircraft land in order according to the landing sequences.
- There is at most one aircraft on the runway at any time.
- Consecutive departure operations are separated.
- Aircraft eventually land or depart the SCA.
- There are no operational deadlocks.

Verification

Prototype Verification System (PVS):

- Theorem proving, Model checking, Real time systems

Properties as state assertions:

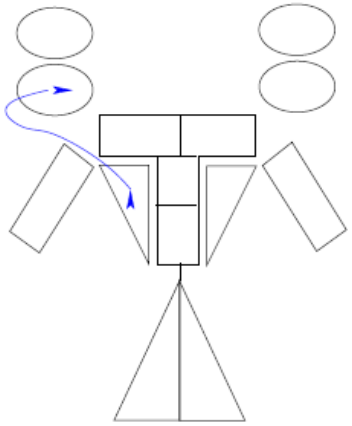
```
four_arrivals(state:SCA):bool =
   total_arrivals(state) ≤ 4

Invariant(state):bool =
   four_arrivals(state) AND
   well_assigned(state) AND
   ...
   non_incursion(state)
```

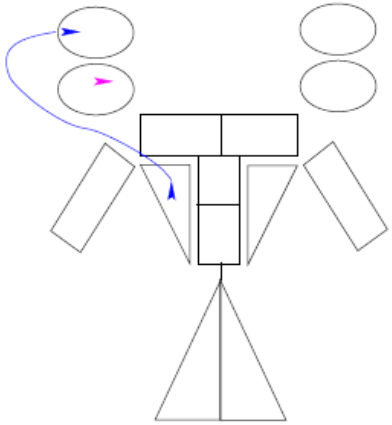
2811 reachable states, overaproximated

Issues

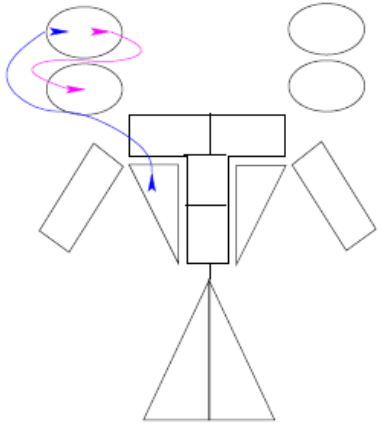
- Some transitions are actualy synchronous
- Available altitude determination



3000 and 2000 feet available



3000 feet available, 2000 feet occupied



3000 feet occupied, 2000 feet available

Discussion

Thank you for your attention.