Reduction and Slicing of Hierarchical State Machines

Mats P.E. Heimdahl and Michael W. Whalen

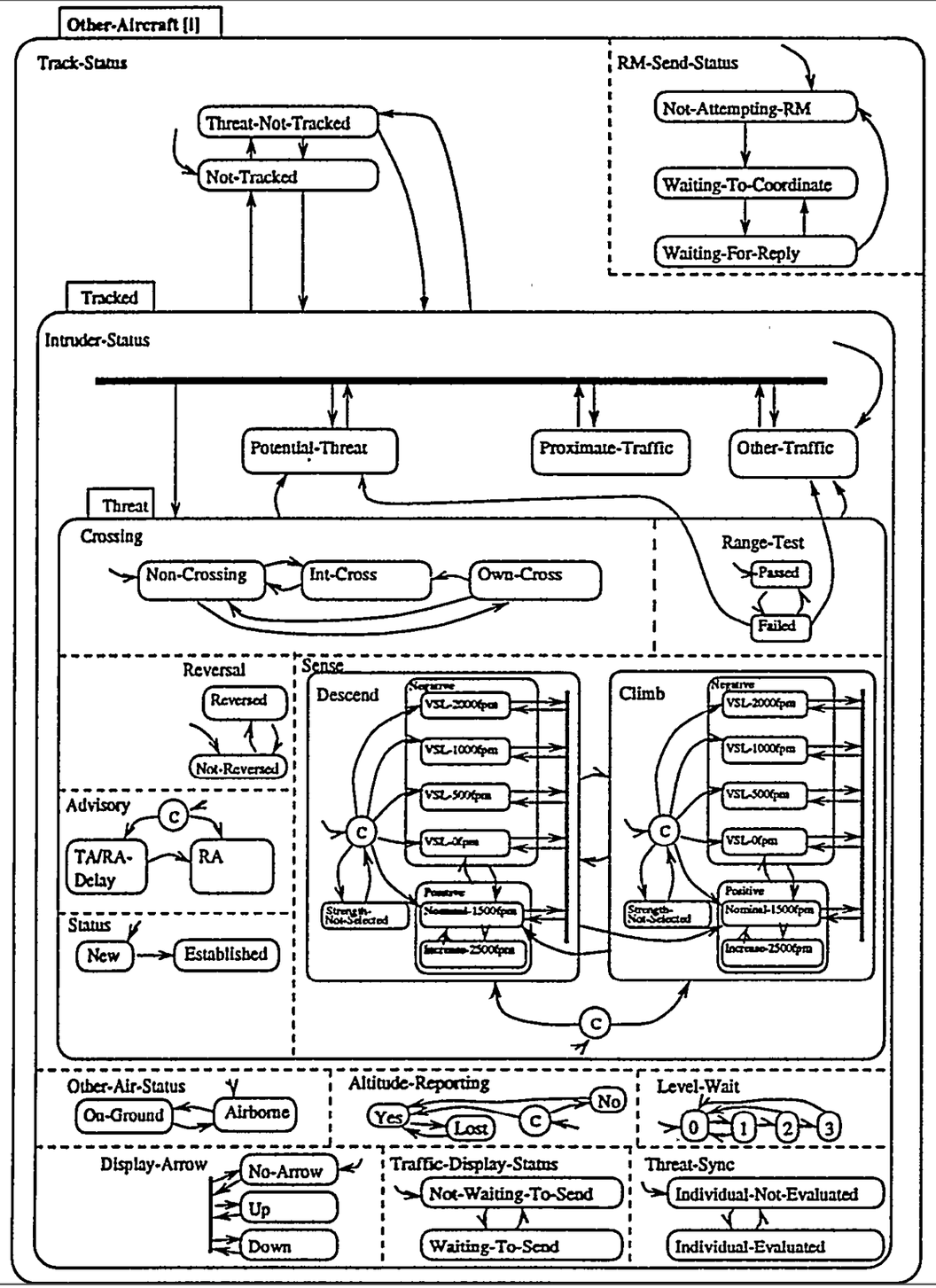
Presenter: David Gage

The Authors

- Mats P.E. Heimdahl
  - Professor at the University of Minnesota
  - Research in requirements specification
  - (page last updated in 2006)
- Michael W. Whalen
  - Program Director at UMN Software Engineering Center
  - Formal verification
  - A lot of work with avionics models

Motivation

- We want to write a specification to simplify things.
- But even a specification that is readable can get complicated and large.
- How can we accurately look at only “digestible chunks” of a specification?


Other-Aircraft [i]
Track-Status
Threat-Not-Tracked
Not-Tracked
RM-Send-Status
Not-Attempting-RM
Waiting-To-Coordinate
Waiting-For-Reply
Tracked
Intruder-Status
Potential-Threat
Proximate-Traffic
Other-Traffic
Threat
Crossing
Non-Crossing
Int-Cross
Own-Cross
Range-Test
Passed
Failed
Reversal
Reversed
Not-Reversed
Sense
Descend
Climb
Negative
VSL-2000fpm
VSL-1000fpm
VSL-500fpm
VSL-0fpm
Positive
Nominal-1500fpm
Increase-2500fpm
Strength-Not-Selected
Advisory
C
TA/RA-Delay
RA
Status
New
Established
Other-Air-Status
On-Ground
Airborne
Altitude-Reporting
Yes
No
Lost
Level-Wait
0
1
2
3
Display-Arrow
No-Arrow
Up
Down
Traffic-Display-Status
Not-Waiting-To-Send
Waiting-To-Send
Threat-Sync
Individual-Not-Evaluated
Individual-Evaluated

Program Slicing

- A projection of a program under specified conditions.
- What influences a variable?
- Or in this case
  - What influences transitions?
  - What allows them to happen?
- What triggers them?

RSML

- Requirements State Machine Language.
- Designed for readability and understandability.
- Based on hierarchical state machines.
- Guarding conditions are unavoidably complex.

AND/OR

Transition(s): Potential-Threat ⟶ Other-Traffic

Location: Other-Aircraft ▷ Intruder-Status$_{s\text{-}136}$

Trigger Event: Air-Status-Evaluated-Event$_{e\text{-}279}$
Condition:

		OR									
	Alt-Reporting$_{s\text{-}101}$ **in state Lost**	T	T	·	·	T	T	·	·	·	·
	RA-Mode-Cancelled$_{m\text{-}218}$	·	·	T	T	·	·	T	T	·	·
	Alt-Reporting$_{s\text{-}101}$ **in state No**	·	·	T	T	·	·	T	T	·	·
AND	Other-Bearing-Valid$_{v\text{-}130}$	F	·	F	·	F	·	F	·	·	·
AND	Other-Range-Valid$_{v\text{-}117}$ = True	·	F	·	F	·	F	·	F	·	·
AND	Potential-Threat-Range-Test$_{m\text{-}214}$	T	T	T	T	F	F	F	F	·	·
	Potential-Threat-Condition$_{m\text{-}213}$	·	·	·	·	·	·	·	·	F	·
	Proximate-Traffic-Condition$_{m\text{-}216}$	·	·	·	·	T	T	T	T	F	·
	Threat-Condition$_{m\text{-}224}$	·	·	·	·	·	·	·	·	F	·
	Other-Air-Status$_{s\text{-}101}$ **in state On-Ground**	·	·	·	·	·	·	·	·	·	T

Output Action: Intruder-Status-Evaluated-Event$_{e\text{-}279}$

Fig. 2. A transition definition from TCAS II with the guarding condition expressed as an AND/OR table.

Scenarios

- Defined by domain experts.
- Restricts the value of certain variables.
- Become interpretations after any behavior impossible in the scenario are removed.

TCAS II

- "In Intruder-Status, how does the threat classification logic work for an intruder that reports both valid range and valid bearing?"
- "How do we classify and intruder that has stopped reporting altitude?"
- "What happens with a threat that lands and is determined to be on the ground?"

Interpretations

- The collection of states that can still be reached given restrictions placed by the scenario.
- With the reduced AND/OR guarding conditions.

How it's done

- Remove any contradicting columns in each transitions AND/OR tables.
- Remove any columns that are left with all "don't care" values.
- Any transitions guarded by now empty AND/OR tables can be safely removed.

TCAS II

- "In Intruder-Status, how does the threat classification logic work for an intruder that reports both valid range and valid bearing?"

Reduction Scenario: Valid-Tracking

AND	Other-Bearing-Valid$_{v\text{-}130}$ = Valid	T
AND	Other-Range-Valid$_{v\text{-}133}$ = Valid	T

Fig. 6. An intruder reporting reliable tracking data expressed as an AND/OR table.

Transition(s): Potential-Threat ⟶ Other-Traffic

Location: Other-Aircraft ▷ Intruder-Status$_{s\text{-}136}$

Trigger Event: Air-Status-Evaluated-Event$_{e\text{-}279}$

Condition:

		OR									
	Alt-Reporting$_{s\text{-}101}$ **in state Lost**	T	T	·	·	T	T	·	·	·	·
	RA-Mode-Cancelled$_{m\text{-}218}$	·	·	T	T	·	·	T	T	·	·
	Alt-Reporting$_{s\text{-}101}$ **in state No**	·	·	T	T	·	·	T	T	·	·
	Other-Bearing-Valid$_{v\text{-}130}$	F	·	F	·	F	·	F	·	·	·
AND	Other-Range-Valid$_{v\text{-}117}$ = True	·	F	·	F	·	F	·	F	·	·
	Potential-Threat-Range-Test$_{m\text{-}214}$	T	T	T	T	F	F	F	F	·	·
	Potential-Threat-Condition$_{m\text{-}213}$	·	·	·	·	·	·	·	·	F	·
	Proximate-Traffic-Condition$_{m\text{-}216}$	·	·	·	·	T	T	T	T	F	·
	Threat-Condition$_{m\text{-}224}$	·	·	·	·	·	·	·	·	F	·
	Other-Air-Status$_{s\text{-}101}$ **in state On-Ground**	·	·	·	·	·	·	·	·	·	T

Output Action: Intruder-Status-Evaluated-Event$_{e\text{-}279}$

Fig. 2. A transition definition from TCAS II with the guarding condition expressed as an AND/OR table.

Transition(s): Potential-Threat ⟶ Other-Traffic

Location: Other-Aircraft ▷ Intruder-Status$_{s\text{-}136}$

Trigger Event: Air-Status-Evaluated-Event$_{e\text{-}279}$

Condition:

		OR	
AND	Potential-Threat-Condition$_{m\text{-}213}$	F	·
	Proximate-Traffic-Condition$_{m\text{-}216}$	F	·
	Threat-Condition$_{m\text{-}224}$	F	·
	Other-Air-Status$_{s\text{-}101}$ **in state** On-Ground	·	T

Output Action: Intruder-Status-Evaluated-Event$_{e\text{-}279}$

Fig. 8. The transition definition sliced based on the scenario Valid-Tracking in Figure 6.

Data Flow

- If we are interested in some transition
- What has to take place to release it's guarding condition?

Transition(s): Potential-Threat ⟶ Other-Traffic

Location: Other-Aircraft ▷ Intruder-Status$_{s\text{-}136}$

Trigger Event: Air-Status-Evaluated-Event$_{e\text{-}279}$
Condition:

		OR	
AND	Potential-Threat-Condition$_{m\text{-}213}$	F	·
AND	Proximate-Traffic-Condition$_{m\text{-}216}$	F	·
AND	Threat-Condition$_{m\text{-}224}$	F	·
	Other-Air-Status$_{s\text{-}101}$ **in state** On-Ground	·	T

Output Action: Intruder-Status-Evaluated-Event$_{e\text{-}279}$

Fig. 8. The transition definition sliced based on the scenario Valid-Tracking in Figure 6.

Control Flow

- If we're interested in an Event
- What can trigger it?

Transition(s): Potential-Threat ⟶ Other-Traffic

Location: Other-Aircraft ▷ Intruder-Status$_{s\text{-}136}$

Trigger Event: Air-Status-Evaluated-Event$_{e\text{-}279}$

Condition:

		OR	
AND	Potential-Threat-Condition$_{m\text{-}213}$	F	·
	Proximate-Traffic-Condition$_{m\text{-}216}$	F	·
	Threat-Condition$_{m\text{-}224}$	F	·
	Other-Air-Status$_{s\text{-}101}$ **in state** On-Ground	·	T

Output Action: Intruder-Status-Evaluated-Event$_{e\text{-}279}$

Fig. 8. The transition definition sliced based on the scenario Valid-Tracking in Figure 6.

Combining slices

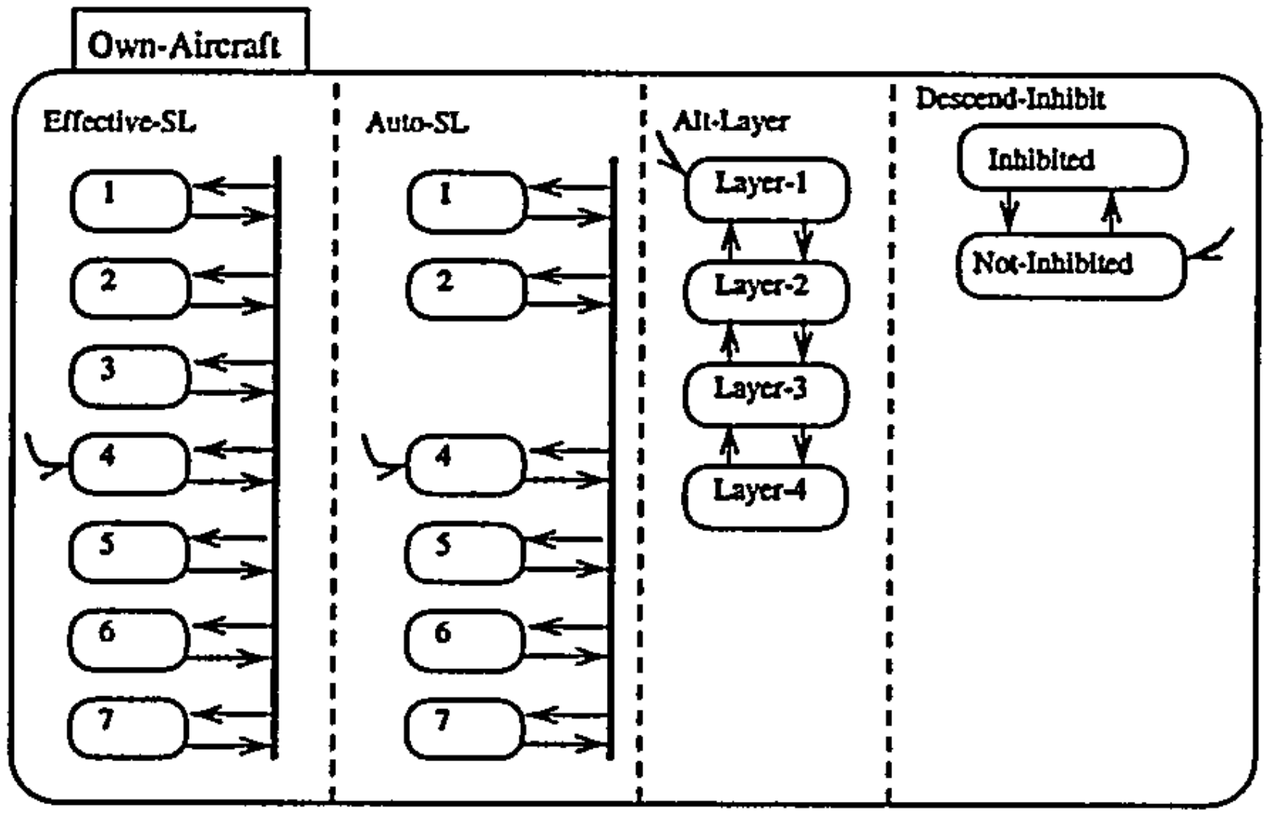


Fig. 10. Model of Own-Aircraft reduced

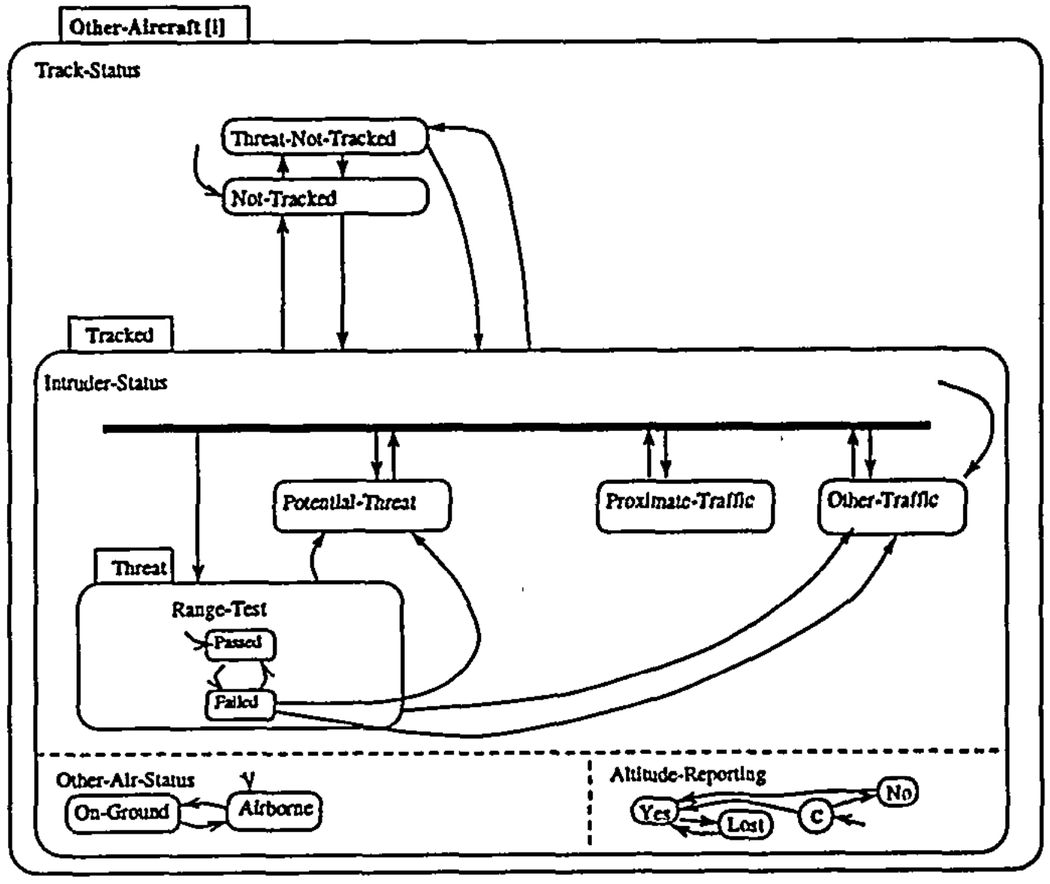
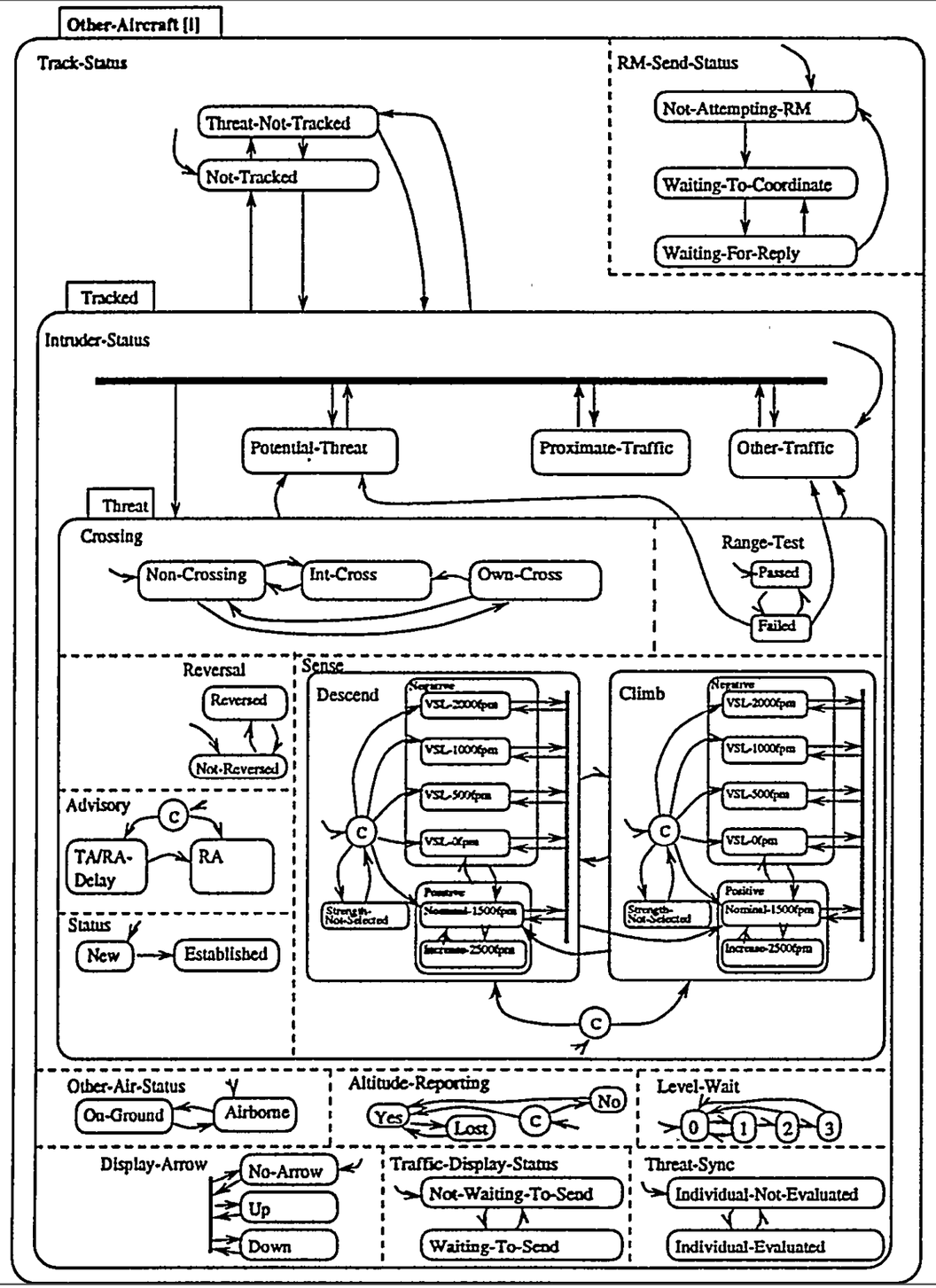


Fig. 11. Model of an intruding aircraft


Other-Aircraft [i]
Track-Status
Threat-Not-Tracked
Not-Tracked
RM-Send-Status
Not-Attempting-RM
Waiting-To-Coordinate
Waiting-For-Reply
Tracked
Intruder-Status
Potential-Threat
Proximate-Traffic
Other-Traffic
Threat
Crossing
Non-Crossing
Int-Cross
Own-Cross
Range-Test
Passed
Failed
Reversal
Reversed
Not-Reversed
Sense
Descend
Climb
Negative
VSL-2000fpm
VSL-1000fpm
VSL-500fpm
VSL-0fpm
Positive
Nominal-1500fpm
Increase-2500fpm
Strength-Not-Selected
Advisory
C
TA/RA-Delay
RA
Status
New
Established
Other-Air-Status
On-Ground
Airborne
Altitude-Reporting
Yes
No
Lost
Level-Wait
0
1
2
3
Display-Arrow
No-Arrow
Up
Down
Traffic-Display-Status
Not-Waiting-To-Send
Waiting-To-Send
Threat-Sync
Individual-Not-Evaluated
Individual-Evaluated

Case Study

- TCAS II RSML
- Metrics
  - Number of transitions
  - Perceived table size
  - Effective table size

Evaluation

- Scenarios
  - Reduced perceived table size from 1-80 to 0-40.
  - Reduced effective size from 10^8-10^10 to 0-10^8.
  - Does not significantly reduce transitions.
- Data and Control Flow
  - Significantly reduced the specification.

Discussion

- Can we use this?
- Are there changes that need to be made?