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?
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):** \[\text{Potential-Threat} \rightarrow \text{Other-Traffic}\]

**Location:** Other-Aircraft \[\rightarrow\] Intruder-Status_{s.136}

**Trigger Event:** Air-Status-Evaluated-Event_c.279

**Condition:**

| Condition                                           | \[\begin{array}{cccccccc}
| Alt-Reporting_{s.101} in state Lost                  | T | T | T | T | T | T | T | T |
| RA-Mode-Cancelled_{m.218}                            | T | T | T | T | T | T | T | T |
| Alt-Reporting_{s.101} in state No                    | T | T | T | T | T | T | T | T |
| Other-Bearing-Valid_{v.130}                          | F | F | F | F | F | F | F | F |
| Other-Range-Valid_{v.117} = True                     | F | F | F | F | F | F | F | F |
| Potential-Threat-Range-Test_{m.214}                 | T | T | T | T | T | T | T | T |
| Potential-Threat-Condition_{m.213}                  | T | T | T | T | T | T | T | T |
| Proximate-Traffic-Condition_{m.216}                 | T | T | T | T | T | T | T | T |
| Threat-Condition_{m.224}                             | T | T | T | T | T | T | T | T |
| Other-Air-Status_{s.101} in state On-Ground          | T | T | T | T | T | T | T | T |
| \end{array}\] |

**Output Action:** Intruder-Status-Evaluated-Event_c.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.
“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**

\[
\begin{array}{c}
\text{AND} \\
\begin{array}{c}
\text{Other-Bearing-Valid}_{130} = \text{Valid} \\
\text{Other-Range-Valid}_{133} = \text{Valid}
\end{array}
\end{array}
\]

**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<sub>136</sub>

**Trigger Event:** Air-Status-Evaluated-Event<sub>e-279</sub>

**Condition:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>OR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt-Reportings&lt;sub&gt;101&lt;/sub&gt; in state Lost</td>
<td>T</td>
</tr>
<tr>
<td>RA-Mode-Cancelled&lt;sub&gt;m-218&lt;/sub&gt;</td>
<td>T</td>
</tr>
<tr>
<td>Alt-Reportings&lt;sub&gt;101&lt;/sub&gt; in state No</td>
<td>T</td>
</tr>
<tr>
<td>Other-Bearing-Valid&lt;sub&gt;v-130&lt;/sub&gt;</td>
<td>T</td>
</tr>
<tr>
<td>Other-Range-Valid&lt;sub&gt;v-117&lt;/sub&gt; = True</td>
<td>F</td>
</tr>
<tr>
<td>Potential-Threat-Range-Test&lt;sub&gt;m-214&lt;/sub&gt;</td>
<td>F</td>
</tr>
<tr>
<td>Potential-Threat-Condition&lt;sub&gt;m-213&lt;/sub&gt;</td>
<td>F</td>
</tr>
<tr>
<td>Proximate-Traffic-Condition&lt;sub&gt;m-216&lt;/sub&gt;</td>
<td>F</td>
</tr>
<tr>
<td>Threat-Condition&lt;sub&gt;m-224&lt;/sub&gt;</td>
<td>F</td>
</tr>
<tr>
<td>Other-Air-Status&lt;sub&gt;s-101&lt;/sub&gt; in state On-Ground</td>
<td>T</td>
</tr>
</tbody>
</table>

**Output Action:** Intruder-Status-Evaluated-Event<sub>e-279</sub>

Fig. 2. A transition definition from TCAS II with the guarding condition expressed as an AND/OR table.
**Transition(s):** Potential-Threat $\rightarrow$ Other-Traffic

**Location:** Other-Aircraft $\triangleright$ Intruder-Status$_{s-136}$

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

**Condition:**

$$A \quad \text{Potential-Threat-Condition}_{m-213} \quad \bigwedge \quad \text{Proximate-Traffic-Condition}_{m-216} \quad \bigwedge \quad \text{Threat-Condition}_{m-224} \quad \bigwedge \quad \text{Other-Air-Status}_{s-101} \quad \text{in state On-Ground}$$

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

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 $\rightarrow$ Other-Traffic

**Location:** Other-Aircraft $\triangleright$ Intruder-Status$_{s,136}$

**Trigger Event:** Air-Status-Evaluated-Event$_{e,279}$

**Condition:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>truth value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential-Threat-Condition$_{m,213}$</td>
<td>F</td>
</tr>
<tr>
<td>Proximate-Traffic-Condition$_{m,216}$</td>
<td>F</td>
</tr>
<tr>
<td>Threat-Condition$_{m,224}$</td>
<td>F</td>
</tr>
<tr>
<td>Other-Air-Status$_{s,101}$ in state On-Ground</td>
<td>T</td>
</tr>
</tbody>
</table>

**Output Action:** Intruder-Status-Evaluated-Event$_{e,279}$

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 $\rightarrow$ Other-Traffic

**Location:** Other-Aircraft $\triangleright$ Intruder-Status_{s-136}

**Trigger Event:** Air-Status-Evaluated-Event_{e-279}

**Condition:**

\[
\begin{align*}
\text{AND} & \quad \text{Potential-Threat-Condition}_{m-213} & \quad F \\
\text{AND} & \quad \text{Proximate-Traffic-Condition}_{m-216} & \quad F \\
\text{AND} & \quad \text{Threat-Condition}_{m-224} & \quad F \\
\quad \text{Other-Air-Status}_{s-101} & \quad \text{in state On-Ground} & \quad T
\end{align*}
\]

**Output Action:** Intruder-Status-Evaluated-Event_{e-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
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?