Verification and Validation of Behavior Models using Lightweight Formal Methods

An Overview for the INCOSE North Texas Chapter

Kristin Giammarco, Ph.D.
NPS Department of Systems Engineering
13 February 2018

This work was made possible by sponsorship from CRUSER, NRP, NAVAIR, and MCSC.
What is Monterey Phoenix?

- MP is a **Navy-developed** framework for modeling human, technology, and environment behaviors all in one framework.

- *Behavior* is defined as a set of *events* with two basic relations: precedence and inclusion.

A: B C;  
Ordered sequence of events (A includes B followed by C)

A: \(B \mid C\);  
Alternative events (A includes B or C)

A: \([B]\);  
Optional event (A includes B or no event at all)

A: \(* \ B \ *)\;  
Ordered sequence of zero or more occurrences of event B in A

A: \(+ \ B \ +\);  
Ordered sequence of one or more occurrences of event B in A

A: \{B, C\};  
Unordered set of events B and C in A (B and C may happen concurrently)

A: \{* B *\};  
Unordered set of zero or more occurrences of event B in A

A: \{+ B +\};  
Unordered set of one or more occurrences of event B in A
The Small Scope Hypothesis: most flaws in models can be demonstrated on small counterexamples.

1. Type model here.
2. Run the model.
3. Inspect event traces output.

- Model system behaviors separately
- System interactions treated as constraints
- Exhaustive generation of SoS behaviors up to a specified scope

2 possible SoS behaviors at scope 1
4 possible SoS behaviors at scope 2
6 possible SoS behaviors at scope 3
Some Use Cases for MP

- To verify and validate activity models developed in notations such as SysML [1]
- To generate comprehensive use case scenario variants for activity models [2]
- To count function points and estimate cost [3]
- To discover and document templates for behavior patterns [8]
- To detect, classify, predict and control emergent behaviors [7][9]
• **An order processing system** enters a waiting state after a transaction is cancelled. (Pilcher 2015)

• **A first responder** administers rescue medication to an unconscious patient, unaware that the medication was already administered. (Bryant 2016)

• The **International Space Station** is unaware of a hazardous condition within a supply spacecraft as that spacecraft approaches to dock. (Nelson 2015)

• **A UAV** on a search and track mission reaches a return-to-base condition, then finds and begins to track a new target. (Revill 2016)

• **A UAV** on a humanitarian assistance and disaster relief mission reports acceptable system status, then the operator suddenly commands the UAV to abort the mission without provocation (Reese 2017 on Beaufait, Constable, and Jent 2017).
An order processing system enters a waiting state after a transaction is cancelled.

**Valid Scenarios:** Orders conclude normally.

**Invalid Scenario:** This order hangs in a waiting state.

---

**Example Found Requirement:** The Order Processing System shall end all started transactions in either the Cancelled or Delivered state.

---

A first responder administers rescue medication to an unconscious patient, unaware that the medication was already administered.

Example Found Requirement: Any Bystander who administers Narcan to an Overdose Victim shall place a band around the Overdose Victim's wrist that indicates the amount and time of the Narcan dose administered.

A UAV on a search and track mission reaches a return-to-base condition, then finds and begins to track a new target.

**Valid Scenario:** Object detected, tracked, and determined by Swarm Operator to be a valid target

**Invalid Scenario:** Target tracked after bingo fuel condition

**Example Found Requirement:** A UAV that has reached a bingo fuel condition shall request permission from the Swarm Operator to track any new targets found.

**Example Found Requirement:** A UAV that has found a possible target after reaching bingo fuel shall relay the LKL of the target to the Swarm Operator, then continue to return to base.

**Example Found Requirement:** A UAV shall only track targets found before reaching bingo fuel conditions.
Detection: Initial discovery of emergent behavior.

Classification:
• Simple: derived from element properties and relationships in non-complex or ‘ordered’ systems [5].
• Weak: desired (or at least allowed) emergence produced by a complex system [5].
• Strong: unexpected emergence not observed until simulation, testing, or operations [6].

Prediction: Postulation of potential future states of emergence based on detected behaviors.

Control: Management of positive or negative emergent behaviors through M&S or other analysis.

Definition set paraphrased from [4]
### Example Analysis of Emergent Behaviors with MP

<table>
<thead>
<tr>
<th>Example</th>
<th>Slide</th>
<th>Detection</th>
<th>Classification</th>
<th>Prediction</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilcher’s Order Processing System</td>
<td>6 left</td>
<td>Automatic and scope-complete with MP</td>
<td>Simple positive emergence</td>
<td>Order Cancelled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 middle</td>
<td></td>
<td>Simple positive emergence</td>
<td>Order Delivered</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 right</td>
<td></td>
<td>Simple negative emergence</td>
<td>Order hangs in a Waiting state: Customer inconvenience; employee inconvenience; Cyber security vulnerability</td>
<td>Behavior logic modification in system model to prevent sequences that end in Waiting state</td>
</tr>
<tr>
<td>Revill’s UAV Mission</td>
<td>8 left</td>
<td>Automatic and scope-complete with MP</td>
<td>Weak positive emergence</td>
<td>Valid target detected and tracked</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 right</td>
<td></td>
<td>Strong positive emergence</td>
<td>UAV is successfully recovered after tracking an object of interest after bingo fuel</td>
<td>Add details to the model to be explicit about requirements to ensure this outcome</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strong negative emergence</td>
<td>UAV forced to emergency land / crash after tracking an object of interest after bingo fuel</td>
<td>Add details to the model to be explicit about requirements to mitigate this risk</td>
</tr>
</tbody>
</table>

Analysis from Table 1 in [7].
Conclusions

• Unspecified and potentially invalid behaviors have been exposed by students ranging from high school to graduate level education.

• Suggests that MP’s lightweight formal method approach is user friendly for practitioners with basic skills in logic and logical thinking.

• To expose emergent behaviors for analysis:
  – model possible events in systems, and
  – treat interactions among events in different systems as constraints that can be relaxed or restricted.
Questions?

Monterey Phoenix and Related Work:

https://wiki.nps.edu/display/mp

firebird.nps.edu

kmgiamma (at) nps.edu