

NAVAL Postgraduate School

Verification and Validation of Behavior Models using Lightweight Formal Methods

An Overview for the SoSECIE Webinar

Kristin Giammarco, Ph.D. NPS Department of Systems Engineering 8 August 2017

This work was made possible by sponsorship from CRUSER, NRP, NAVAIR, and MCSC.



Monterey, California WWW.NPS.EDU



- 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 | 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

MP Analyzer Layout



NAVAL

....

SCHOOL

POSTGRADUATE



- 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 detect, classify, predict and control emergent behaviors [4][7]

POSTGRADUATE Emergent Behaviors Found using MP Modeling

An order processing system enters a waiting state after a transaction is cancelled. (Pilcher 2015)

NAVAI

- A first responder administers rescue medication to an unconscious patient, ۲ unaware that the medication was already administered. (Bryant 2016)
- The International Space Station is unaware of a hazardous condition ۲ 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.





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

Pilcher, Joanne D. "Generation of department of defense architecture framework (DODAF) models using the Monterey Phoenix behavior modeling approach." <u>Master's Thesis</u>, Naval Postgraduate School, Monterey, CA. September 2015.



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.

Bryant, Jordan. "Using Monterey Phoenix to analyze an alternative process for administering Naloxone." <u>Capstone Research Project</u>, Science and Math Academy, Aberdeen, MD. June 2016.



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

track a new target





Detection: Initial discovery of emergent behavior.

Classification:

- **Simple:** derived from element properties and relationships in noncomplex 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].

<u>**Prediction</u>**: Postulation of potential future states of emergence based on detected behaviors.</u>

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



Example Analysis of Emergent Behaviors with MP

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



11

- 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







- Giammarco, Kristin. "Practical Modeling Concepts for Engineering Emergence in Systems of Systems." Proceeding of the 12th Annual System of Systems Engineering Conference, Waikoloa, HI, June 18-21, 2017.
- Giammarco, Kristin, Kathleen Giles, and Clifford A. Whitcomb. "Comprehensive use case scenario generation: An approach and template for modeling system of systems behaviors." Proceeding of the 12th Annual System of Systems Engineering Conference, Waikoloa, HI, June 18-21, 2017.
- 3. Farah-Stapleton, Monica. "Executable behavioral modeling of system- and software- architecture specifications to inform resourcing decisions." Doctoral Dissertation, Naval Postgraduate School, September 2016.
- 4. Rainey, Larry and Mo Jamshidi. "Introduction and Overview for Engineering Emergence: A Modeling and Simulation Approach," Chapter 1 in *Engineering Emergence: A Modeling and Simulation Approach*, edited by Larry Rainey and Mo Jamshidi. Boca Raton, FL: CRC Press Taylor & Francis Group.
- 5. Page, S.E. 2009. *Understanding Complexity*. The Great Courses. Chantilly, VA, USA: The Teaching Company.
- SEBoK authors. 2017. "System of Systems (SoS)," in BKCASE Editorial Board. 2016. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 1.8. R.D. Adcock (EIC). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. Released 27 March 2017, http://sebokwiki.org/wiki/Systems_of_Systems_(SoS)#Definition_and_Characteristics_of_Systems_of_Syste ms (accessed 12 July 2017).
- 7. Giammarco, Kristin and Mikhail Auguston. "Behavior modeling approach for the early verification and validation of system of systems emergent behaviors," Chapter 18 in *Engineering Emergence: A Modeling and Simulation Approach*, edited by Larry Rainey and Mo Jamshidi. Boca Raton, FL: CRC Press Taylor & Francis Group.