Safety not guaranteed:

Using formal methods in human factors engineering

Adam Houser

PhD Candidate, UB Department of Industrial and Systems Engineering

Inter-University Workshop 2014

Work Supported by Scenario Development Through Computational and Formal Modeling for Verification and Validation of Authority and Autonomy (A&A) Constructs in Aviation, subcontract from the Georgia Institute of Technology, sponsored by the NASA Ames Research Center.

Safety and simulation

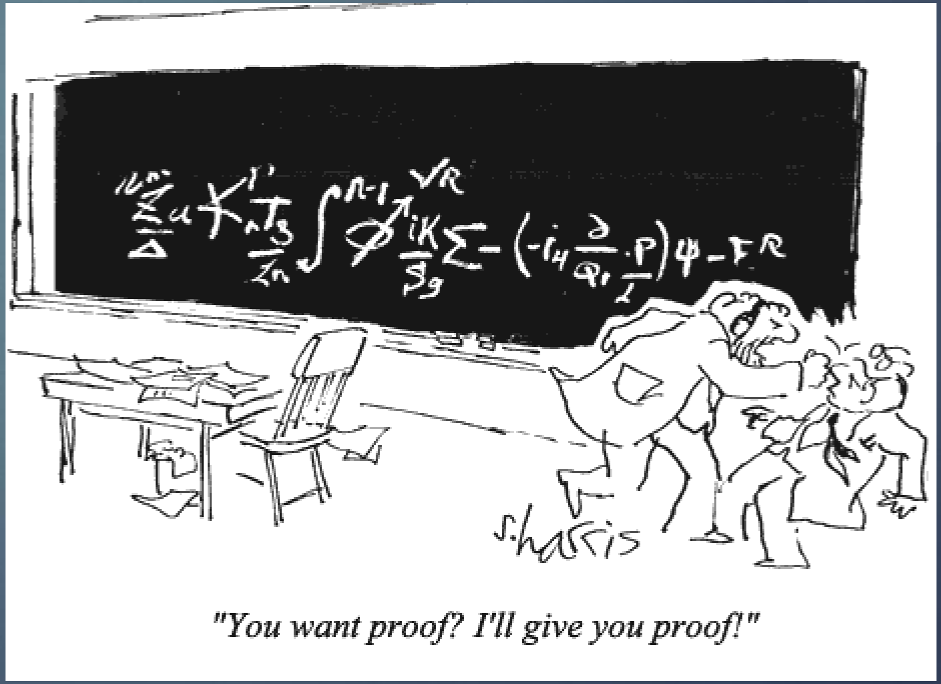
- Safety-critical systems: our lives and safety depend on them
- More specifically, on their correctness and robustness (among other attributes)
- Size and complexity concerns
- The use of simulation

Safety and simulation

- Why simulate?
  - Cost-effective (comparatively)
  - Useful event traces
  - Scalable
  - Diverse scenario exploration
- Why not simulate?

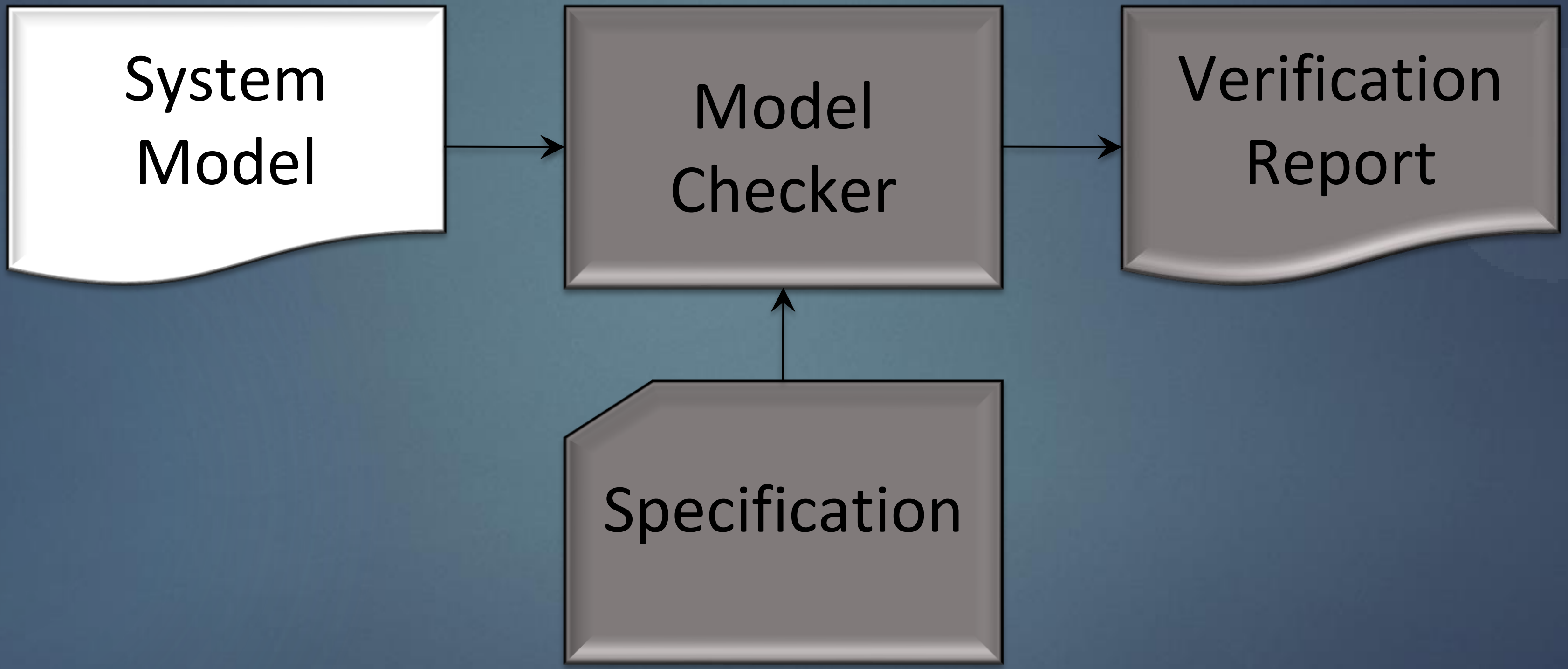
Formal Methods

- Formal methods: collections of tools and techniques to prove (*guarantee*) a system will perform as intended
  - Modeling
  - Specification
  - Verification

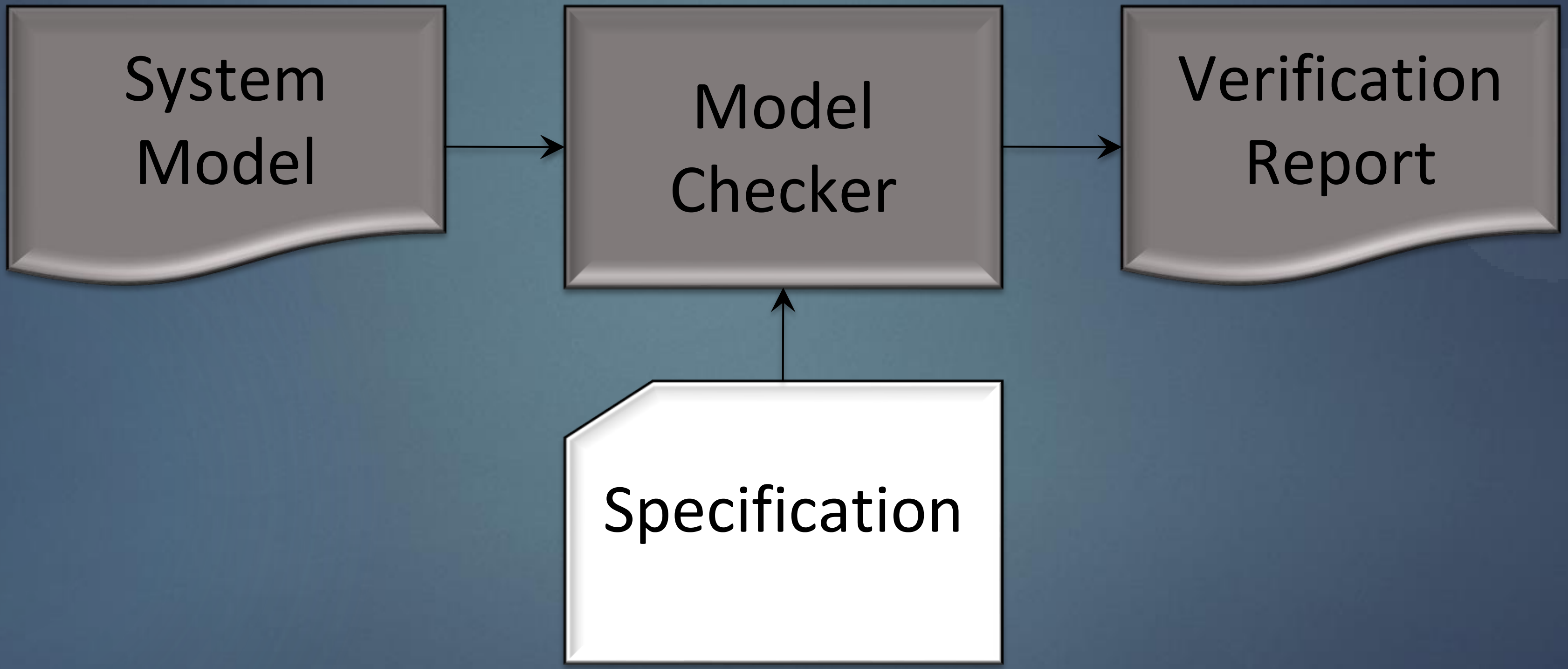


"You want proof? I'll give you proof!"

Formal Methods



Formal Methods



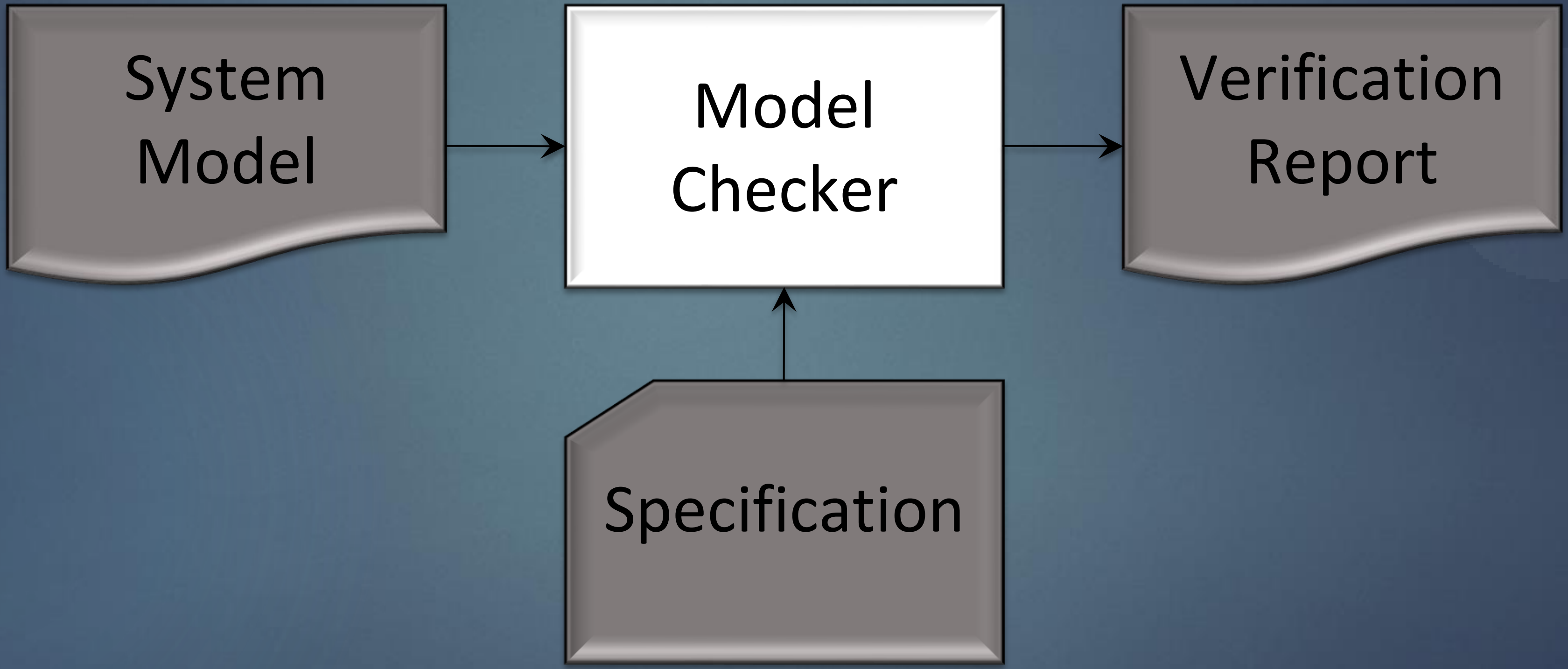
System Model

Model Checker

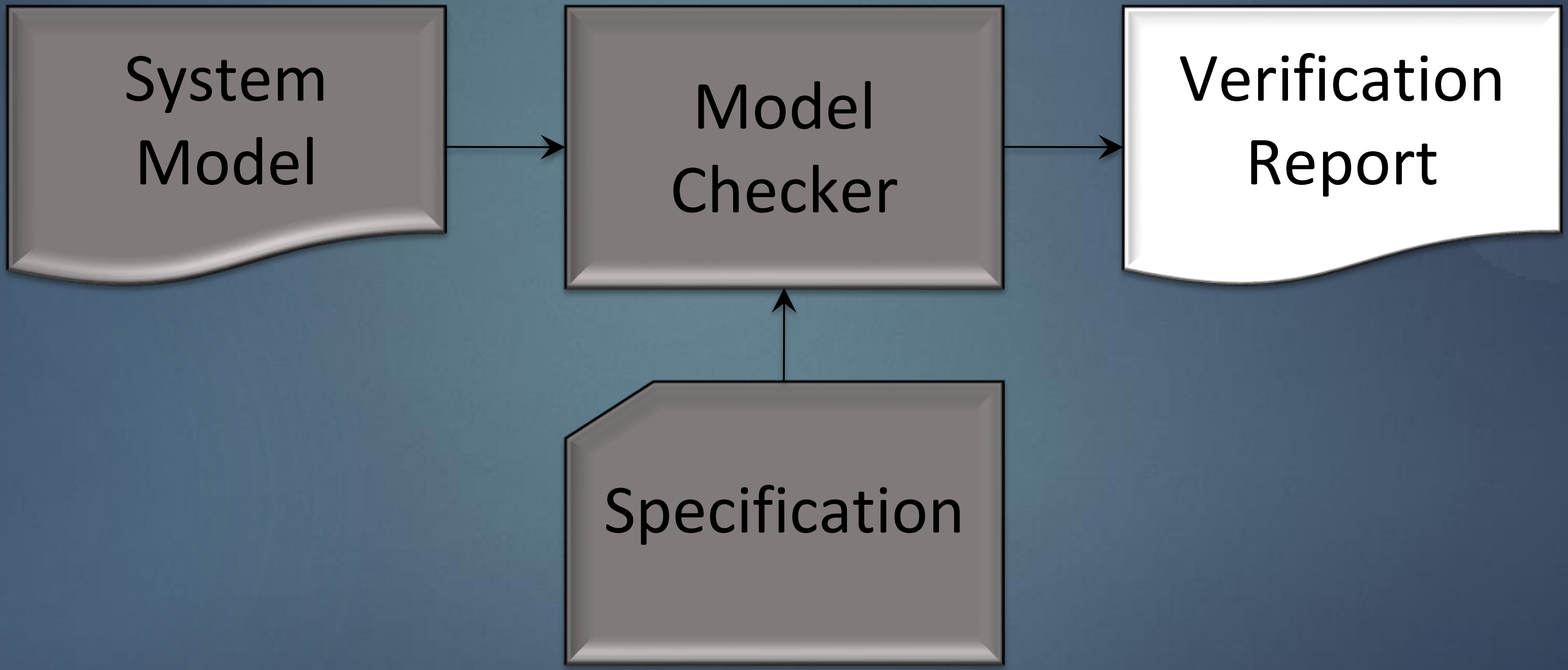
Verification Report

Specification

Formal Methods



Formal Methods



Simulation and Formal Methods

Simulations are better at…

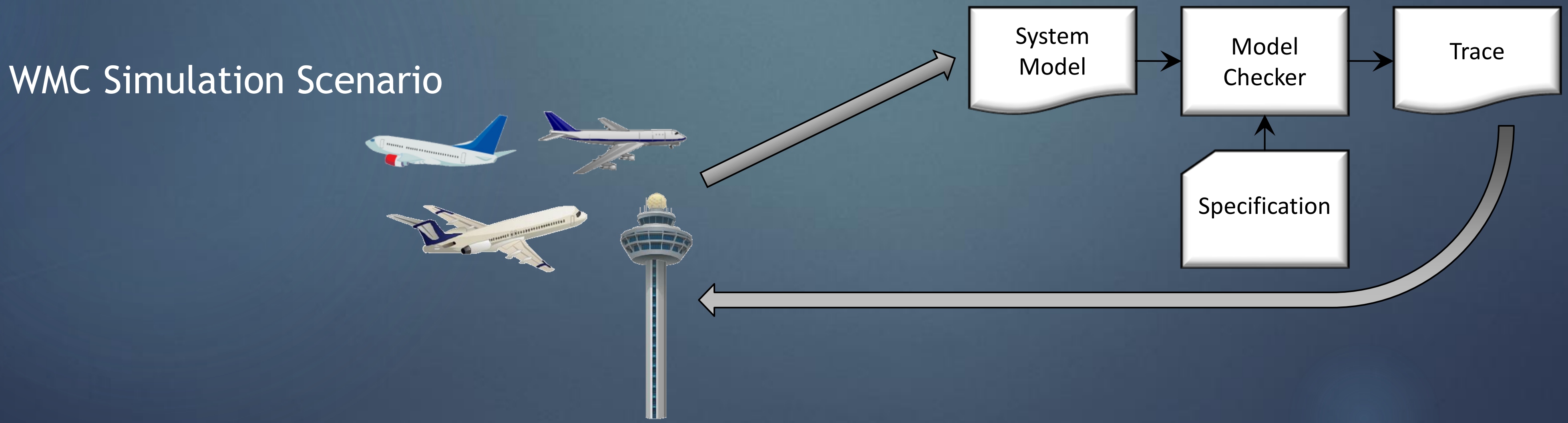
- Scalable computability
- Large-scope, scenario exploration
- Producing diverse performance and/or stochastic measures of system performance

Formal methods are better at …

- Complete state-space evaluation
- Small-scope, area of interest exploration
- Making specific guarantees about system model behavior or finding specific (potential unusual) occurrences of system conditions

Current Research

- Working with Georgia Tech, Honeywell, and Drexel U, sponsored by NASA
- Our slice: Using formal methods to do sensitivity analysis on simulation scenarios for evaluating authority and autonomy in NextGen Air Traffic Control



Current Research

- Modeling WMC concepts in SAL to facilitate WMC ↔ SAL scenario translations
  - Agents, a series of actions the agents must perform, a scheduler to arrange incoming actions, and flight “resources” (ex: altitude, speed)
- Developing formal specification properties capable of finding interesting authority and autonomy conditions in air traffic scenarios:
  - Authority-responsibility double-bind
  - Multistep action interruptions
  - Clumsy automation / bad function allocation
  - Excessive human task load

Conclusions and Future Work

- Automated translation: SAL ↔ WMC
- Examining real-world scenarios, backfeed into WMC
- Applications to novel scenarios at previously-unexplored levels of rigor
- Adam’s interests: autonomy, authority and responsibility;
  dynamic function allocation;
  trust (*guarantees?*) in automation.

Formal Methods

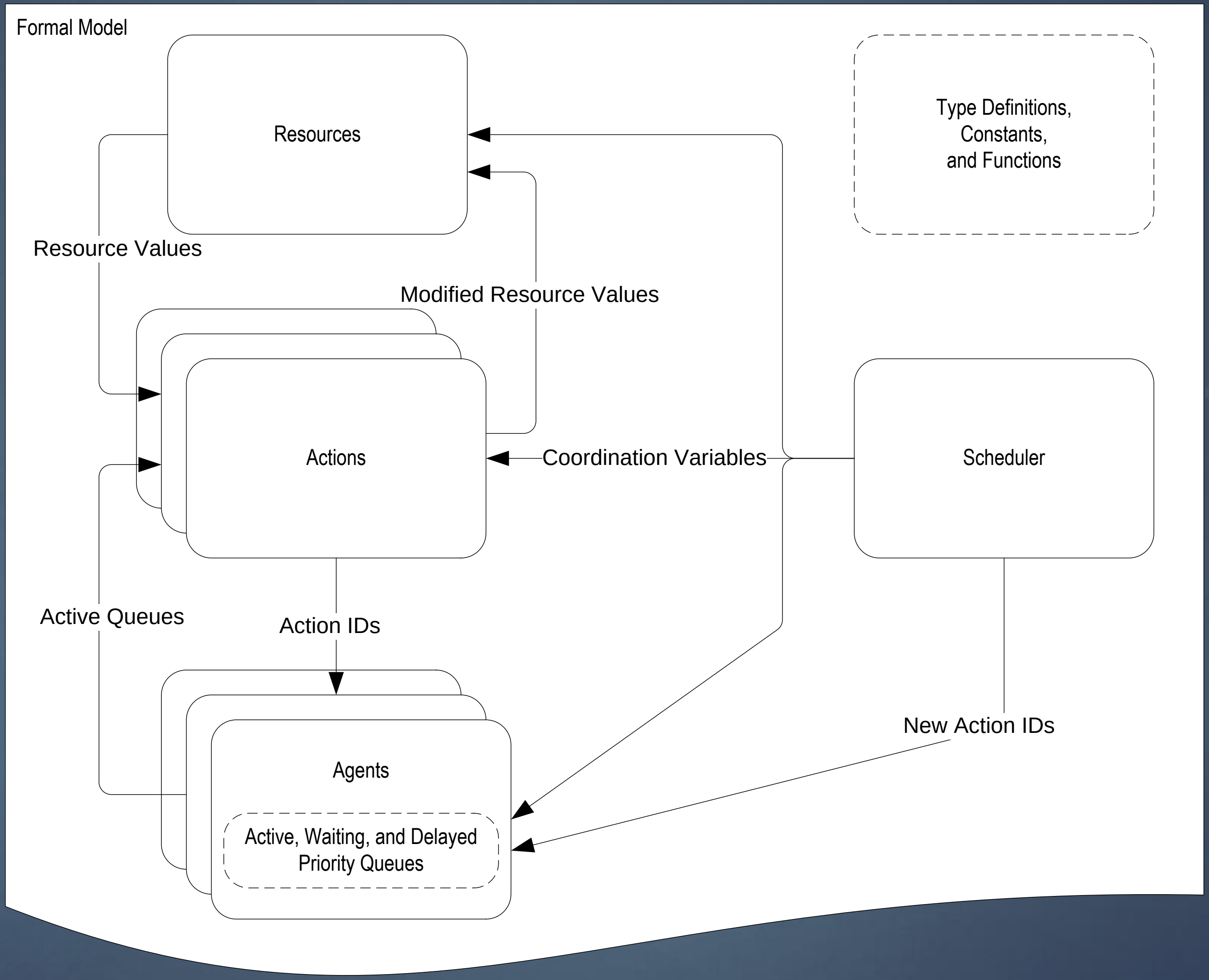
Fin.

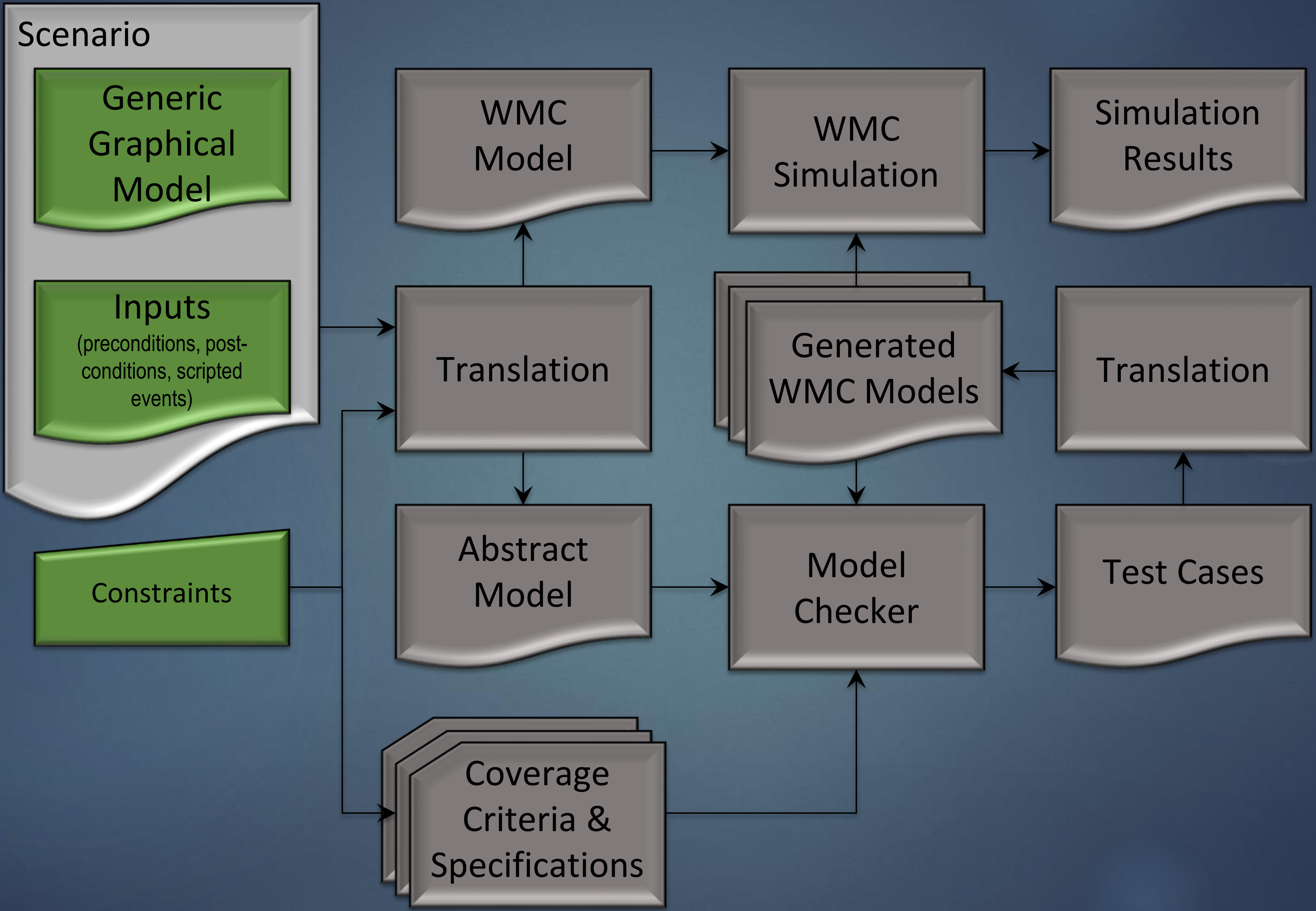
- References upon request.
- Constructive commentary and questions to:

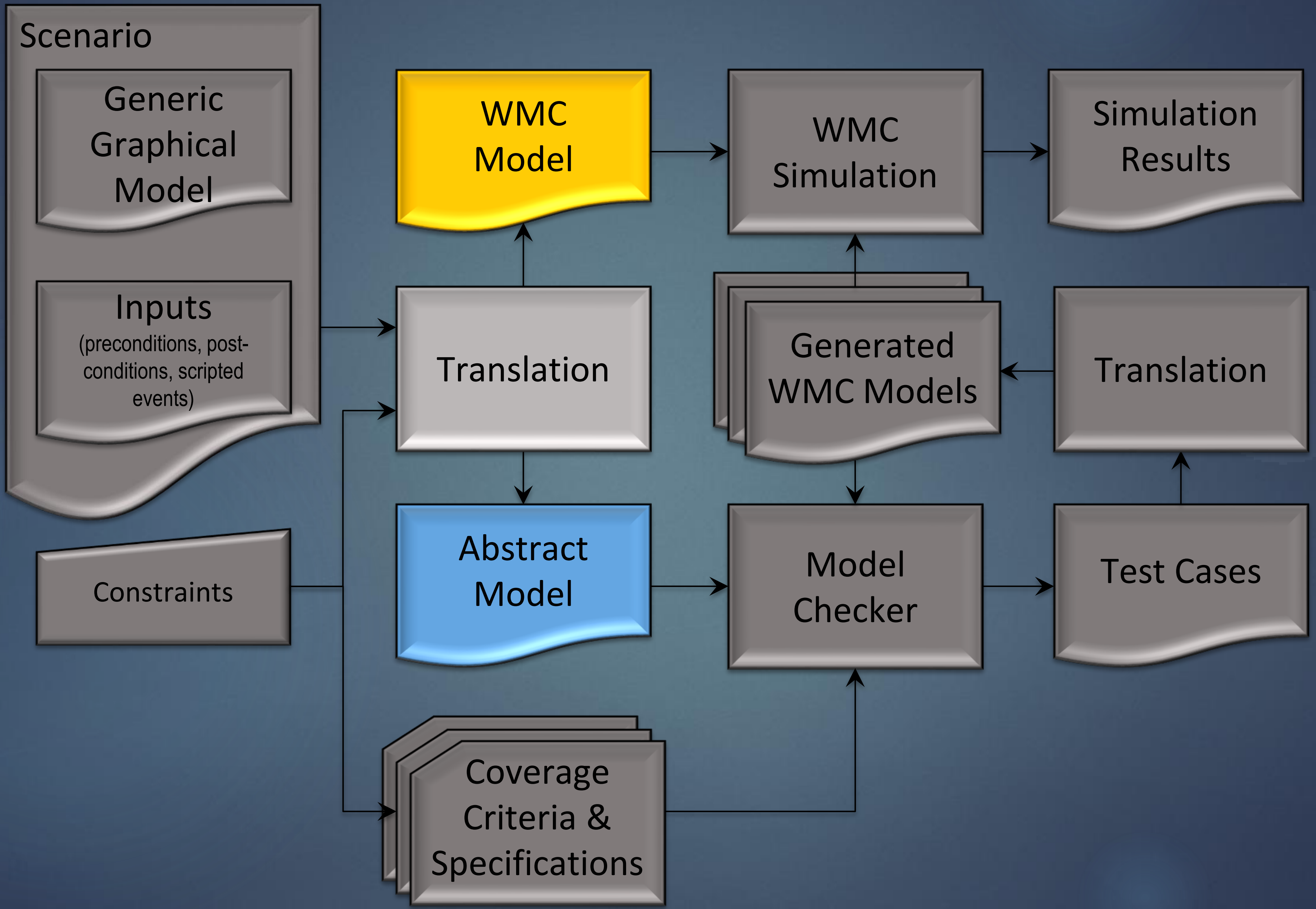
adamhous@buffalo.edu

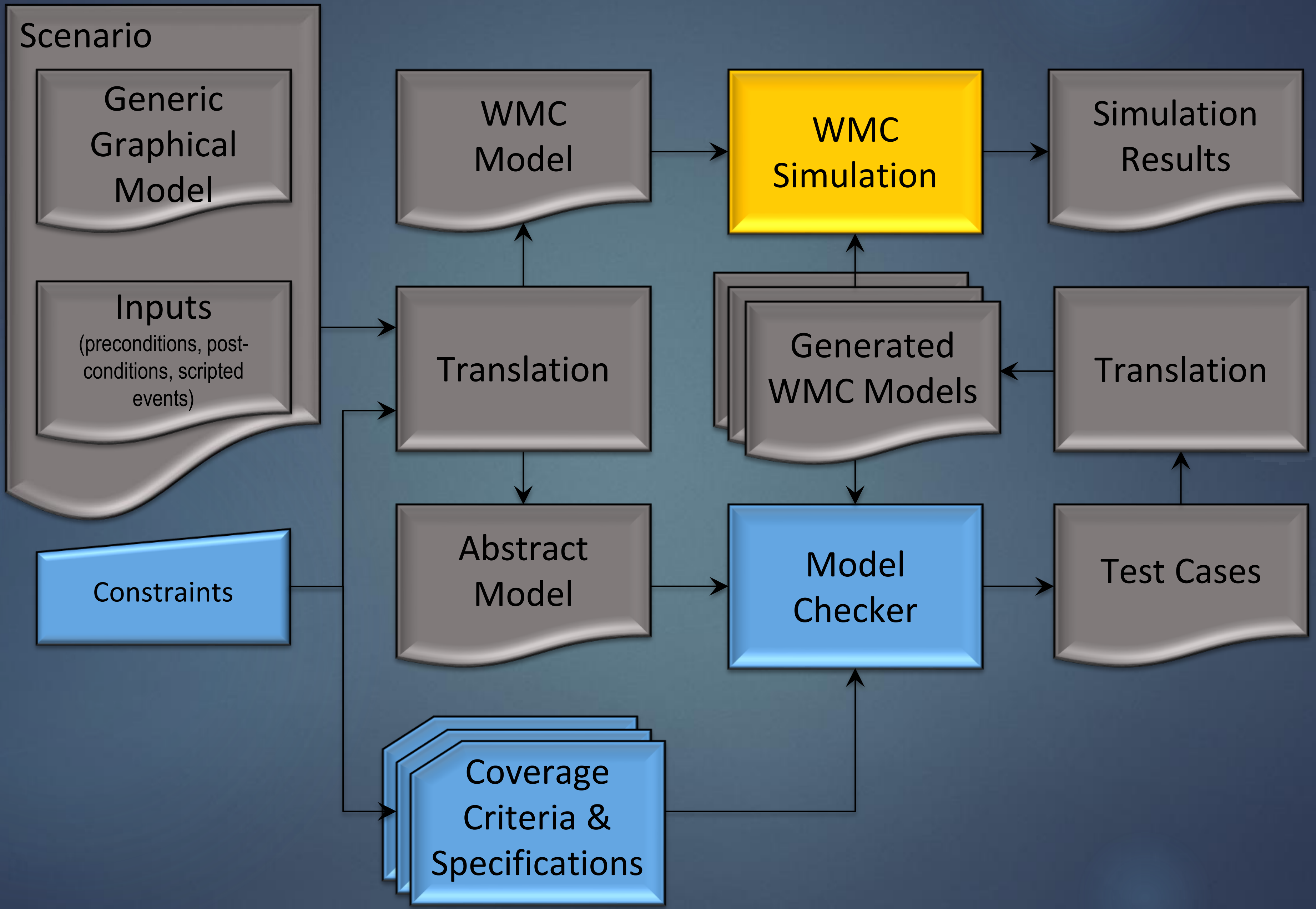
Thanks for listening!

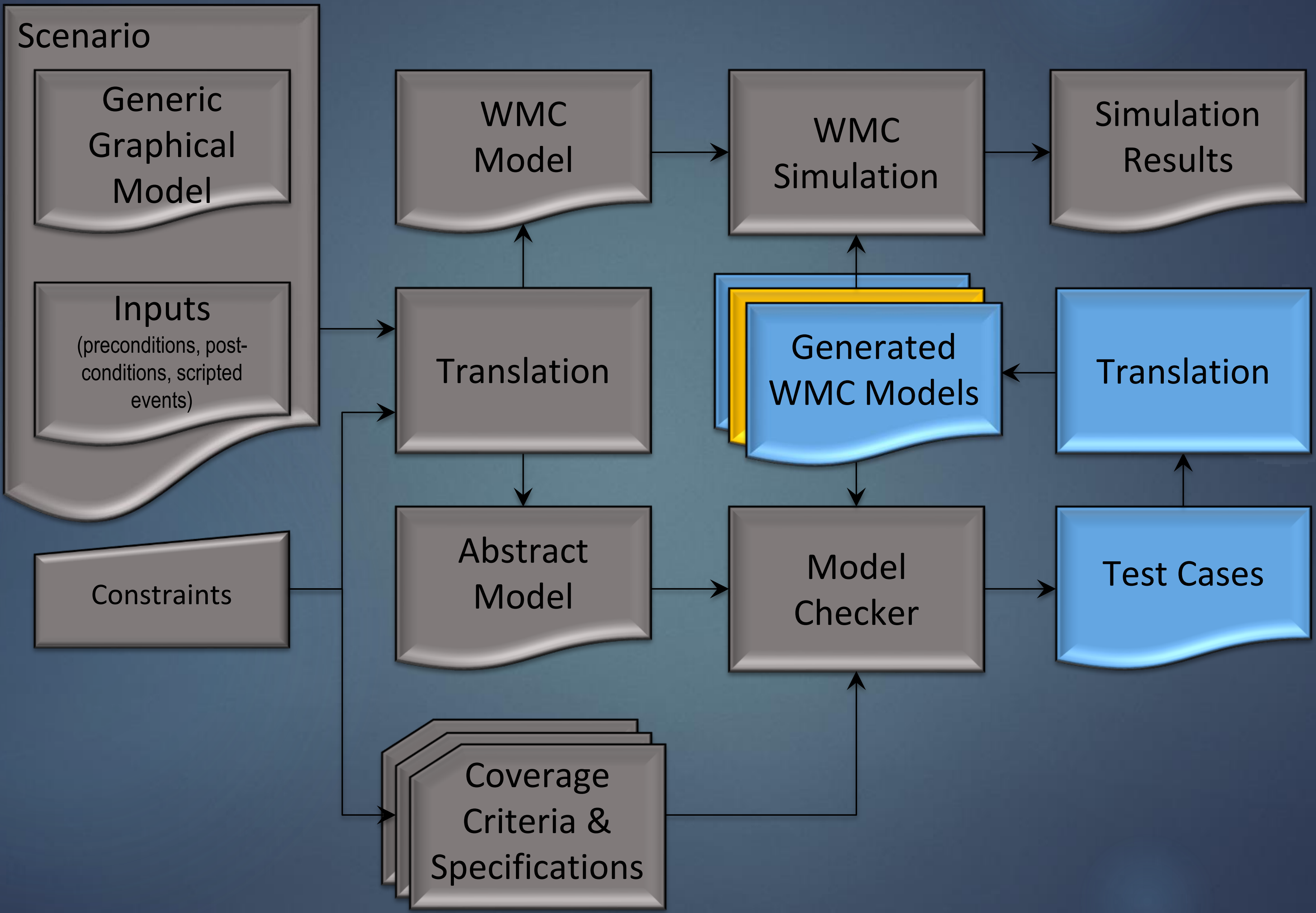
Additional Slides

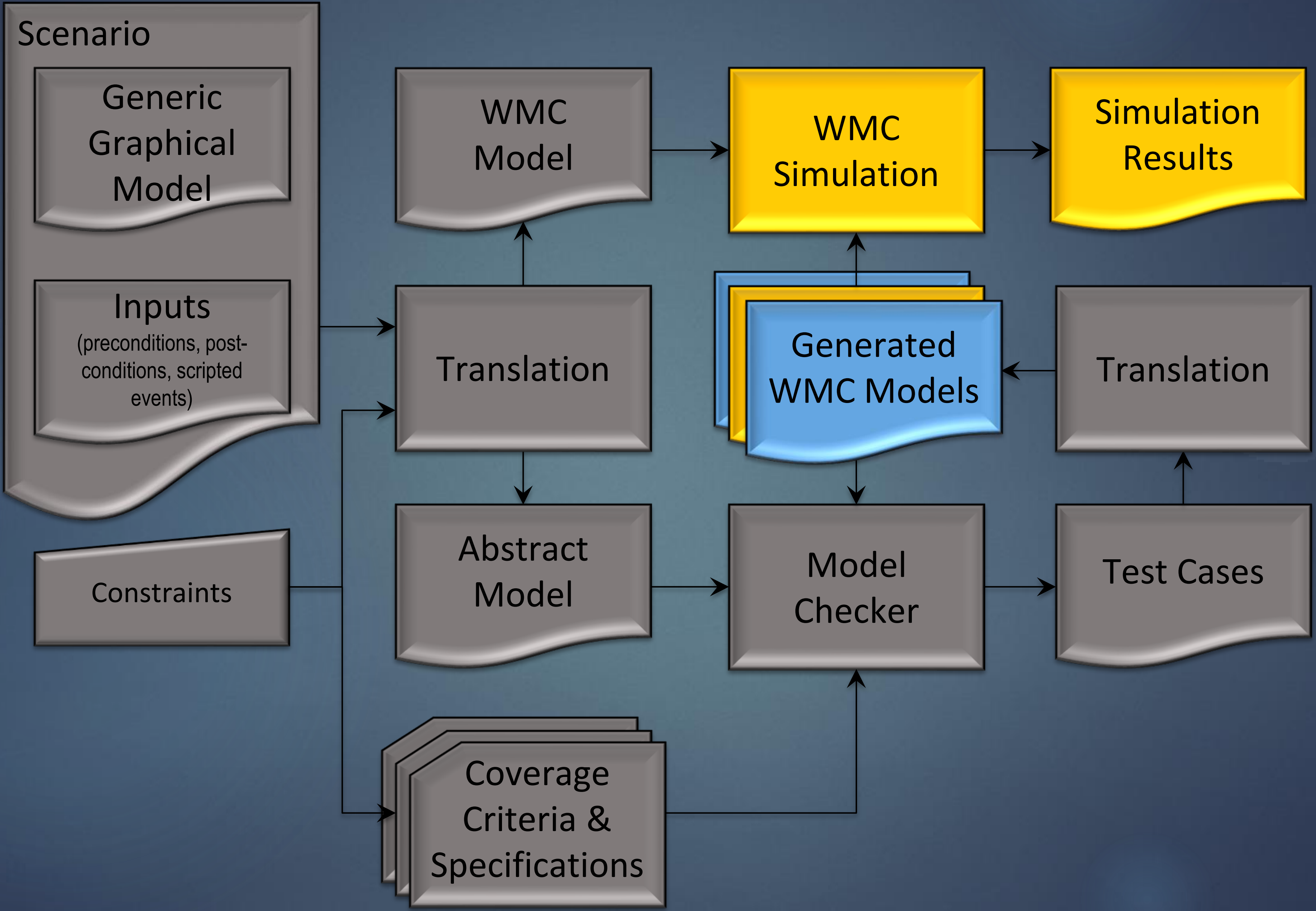

Formal Model
Resources
Type Definitions,
Constants,
and Functions
Resource Values
Modified Resource Values
Actions
Coordination Variables
Scheduler
Active Queues
Action IDs
Agents
Active, Waiting, and Delayed
Priority Queues
New Action IDs


Scenario
Generic Graphical Model
Inputs
(preconditions, post-conditions, scripted events)
Constraints
WMC Model
Translation
Abstract Model
Coverage Criteria & Specifications
WMC Simulation
Generated WMC Models
Model Checker
Simulation Results
Translation
Test Cases


Scenario
Generic Graphical Model
Inputs
(preconditions, post-conditions, scripted events)
Constraints
WMC Model
Translation
Abstract Model
Coverage Criteria & Specifications
WMC Simulation
Generated WMC Models
Model Checker
Simulation Results
Translation
Test Cases


Scenario
Generic Graphical Model
Inputs
(preconditions, post-conditions, scripted events)
Constraints
WMC Model
Translation
Abstract Model
Coverage Criteria & Specifications
WMC Simulation
Generated WMC Models
Model Checker
Simulation Results
Translation
Test Cases


Scenario
Generic Graphical Model
Inputs
(preconditions, post-conditions, scripted events)
Constraints
WMC Model
Translation
Abstract Model
Coverage Criteria & Specifications
WMC Simulation
Generated WMC Models
Model Checker
Simulation Results
Translation
Test Cases


Scenario
Generic Graphical Model
Inputs
(preconditions, post-conditions, scripted events)
Constraints
WMC Model
Translation
Abstract Model
Coverage Criteria & Specifications
WMC Simulation
Simulation Results
Generated WMC Models
Translation
Model Checker
Test Cases