MODEL BASED SYSTEM ENGINEERING USING VALIDATED EXECUTABLE SPECIFICATIONS AS AN ENABLER FOR COST AND RISK REDUCTION

George Fortney
SAIC

4 August 2014
Model-Based Engineering (MBE): An approach to engineering that uses models as an integral part of the technical baseline that includes the requirements, analysis, design, implementation, and verification of a capability, system, and/or product throughout the acquisition life cycle.

Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. (DoD 5000.59 -M 1998)

Preferred MBE Practices:
- Models are scoped to purpose/objectives
- Models are appropriate to the context (e.g., application domain, life cycle phase)
- The models represent the technical baseline that is delivered to customers, suppliers, and partners
- Models are integrated or interoperable across domains and across the lifecycle

Core to MBE is the integration of descriptive/design models with the computational models.
Performing requirements and design verification as early as possible, as opposed to waiting until “composition” activities begin, reduces cost and schedule risks.

Model-Based System Engineering Framework

- Design new systems or components, Build models with validated executable specifications.
- Mix and match simulation models with existing system or component implementations to instantiate a system of systems representation.
- Conduct analysis of alternatives by assessing performance of overall system at mission-level in representative operational scenarios.
- Optimize system and component design based on mission-level performance assessment.
- Allows performance and functionality assessment of overall system before code implementation.
- Generate code from optimized models
- Assess performance of integrated system at mission-level in operational scenarios prior to field tests; Identify integration issues before lab and field tests.
- Composable software to build hierarchical models of components, subsystems, and systems.

Agile Model-based System Engineering Framework

- Reduce Functionality Risk
- Reduce Integration Risk
- Reduce Schedule Risk
- Reduce Cost
• Systems specifications, developed after conceptual design, have a high degree of uncertainty.
• Specifications are not sufficiently validated in the early development process and no executable specification exists at the vehicle level (System of System)
• System designers cannot evaluate the impact of their design decisions at vehicle or vehicle application level.

A model-based design methodology together with a virtual test environment makes complex high level system specifications executable and testable during the very early levels of system design.

An integrated executable specification at Early Conceptual Architecture Level is developed and used to determine the impact of different system architecture decisions on system behavior and overall performance.
V-Model including percentages of where errors are likely to be introduced and found together with estimates of relative costs for error removal within the systems development lifecycle.

Source: C. Grimm, FDL’03, Springer Netherlands, 2004
MBSE with VES enables

• Resource availability and optimization modeling,
• Discrete event (DE) simulation with time correlation,
• Both synchronous and asynchronous data and signal flow
• Finite state machine (FSM) for control flow
• Continuous time modeling for analog effects
Limitations of UML & SysML

- Concepts for functional Modeling do not fully address architectural impact, dynamic networked feedback loops, and other resource sensitive aspects
- Primarily used for SW development in devices
- Does not provide for an integrated development environment.
- Does not accurately model resource availability – no multi-domain simulation environment that includes
- Does not have discrete event simulation
- Does not have event based time correlation
- Can model limited functional behavior, e.g. state chart behavior. However, you cannot model availability of resources. Therefore you cannot model architectures and cannot validate.
- SysML/UML adds some simulation capability to UML. However, you cannot model architecture together with functional behavior. You therefore cannot validate.

Validated Executable Specifications (VES) that take architectural models and add functional modelling capabilities can validate function, architecture and integrated architectural/functional behavior at mission/application level
All of the hard work that went into the current UML, UML/SysML models can be brought into an MBSE virtual test environment and then become the framework to add the logic to for the creation of VES.
MBSE
Real World Examples
PM MTS used software to track white vehicles (convoys) in an Area of Responsibility (AOR). This system used commercial SAT COMMS and the MTS hardware in the vehicles. The system would fail when the number of units reached 650 in an AOR.

Using MBSE to spawn vehicles in the NOC enabled the MBSE engineers to increase the number of units to the breaking point and then analyze the logs to determine the problems then test again. This iterative testing was done quickly and cost effective.

Without using vehicles, drivers or paying for SAT COMMS the SAIC MBSE team was able to find the problems and help correct them using only a NOC, 5 MTS units and the MBSE model. It took this team 2 months to get the number of MTS units in an AOR up to 3000. The fix was successfully fielded.
MBSE for Multi Mission Maritime Aircraft (MMMA) P8A Program

- Executable specification/Validated Platform of architecture, process and mission
- Formal executable specifications/Validated Platform at aircraft level
- Model based architectural trade-off at mission/operational level
- Automatically generated html-files of models are integrated in LCM (Life Cycle Management System) and viewable in Browser over Intranet

**Result/Impact**
Accelerated development at lower risk
First flight in April 25, 2009
Validated Platform used for coverage analysis during ‘flight test’
Validated Platform used for training
Validated Platform becomes key delivery for Navy + for future extensions + for future customers
Airbus A350 Civilian Aircraft

Traditional Avionics Network Layout

New Technology allows distributed Network layout

What is the minimum cost architecture that meets all requirements?

Optimized Architecture
### Performance Item

<table>
<thead>
<tr>
<th>Performance item</th>
<th>Reference system</th>
<th>Optimized system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of architecture [USD]</td>
<td>100%</td>
<td>28%</td>
</tr>
<tr>
<td>Reduction of cables [%]</td>
<td></td>
<td>68</td>
</tr>
<tr>
<td>Weight of architecture [kg]</td>
<td>280.06</td>
<td>201.00</td>
</tr>
<tr>
<td>Weight of cables [kg]</td>
<td>108.21</td>
<td>29.15</td>
</tr>
<tr>
<td>Length of cables [feet]</td>
<td>1,531.46</td>
<td>453.84</td>
</tr>
<tr>
<td>MTBF [h]</td>
<td>55,632.88</td>
<td>57,534.15</td>
</tr>
<tr>
<td>MTTR [h]</td>
<td>31.63</td>
<td>29.89</td>
</tr>
<tr>
<td>MTBUR [h]</td>
<td>49,164.46</td>
<td>50,874.30</td>
</tr>
<tr>
<td>Availability</td>
<td>0.99</td>
<td>0.9999999999999999</td>
</tr>
</tbody>
</table>

An optimized configuration will result in significant improvements in cost, weight, development time and risk level.
<table>
<thead>
<tr>
<th>Client</th>
<th>Problem</th>
<th>Solution</th>
<th>Result/impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOEING: Early</td>
<td>Validation of B777 avionics network and control system</td>
<td>Development of performance level executable specifications and simulation</td>
<td>Reduced development time for avionics system by factor 2; reliability analysis was moved to early design stages</td>
</tr>
<tr>
<td>BOEING: KC-46A</td>
<td>Tanker needed a way to model refueling sequencing to minimize time and optimize delivery process</td>
<td>MBSE was used to create a single executable I model with differential equations, FSM, discrete event. Purely model based approach was accepted by Air Force – a first</td>
<td>Integration model of refueling procedure of both tanker and aircraft eliminated the icing problem and decreased refueling operations by 20 seconds</td>
</tr>
<tr>
<td>MBSE Airborne</td>
<td>P-8A Program needed mission level performance validation. Aircraft level of complexity and sophistication of electronics required new methodology to validate aircraft at SoS level early in concept design.</td>
<td>Created a full unified aircraft SoS model as a FSM. Supply chain network was able to determine overall impact on components and sub stems. Digital thread enabled all contributors to view models through a browser simplifying integration</td>
<td>P8-A became the most successful aircraft in modern history developed on time, within budget, and exceeded performance specs set in 2004. MBSE models were accurate enough to be used for training saving $14Ms. For models sanctioned by NAVAIR</td>
</tr>
</tbody>
</table>
Integration of VICTORY on Vehicle Platforms

SYSTEMS ENGINEERING AND INTEGRATION

4 August 2014
Build a little, test a little.
Thank you

George Fortney
SAIC
VICTORY Program Manager/ Chief Engineer
MBSE Technical Lead
george.g.fortney@saic.com
732-642-4685