2021 Annual INCOSE international workshop
Virtual Event
January 29 - 31, 2021
Premier Systems Engineering Workshop

Treadstone + 1: The First Anniversary of the SAIC Digital Engineering Validation Tool

Michael J. Vinarcik, ESEP-Acq, P.E., FESD
Chief Systems Engineer
SAIC Strategy, Growth, and Innovation Organization (Digital Engineering)

www.incose.org/iw2021/

MBSE Lightning Round

Status Quo: Document-Intensive SE

- Leads to siloed, disconnected views of a system
- No guarantee of consistency between requirements or views
- Often delivered as PDFs, Excel, or other disjointed artifacts
- Difficult to review thoroughly

A coherent picture
is difficult to assemble!

How Modeling Can Help

MBSE Lightning Round

Lessons Learned and Recommended Best Practices from Model-Based Systems Engineering (MBSE) Pilot Projects
Ryan Noguchi, Aerospace Corporation (2016)

- The Ability to Interrogate the Data:
  "The modeling tools provide mechanisms for users to query the model to navigate this "mesh" of elements, attributes, and relationships to obtain more focused slices of insight into the architecture of the system."
- An Increased Focus on Content/Data:
  "Stakeholders and practitioners often did not understand the implications of this new approach, or take advantage of the benefits it can provide."
- Automated Reviews:
  "…many syntactical errors that would have been caught had they used the built-in model validation capabilities of their tools, but the problem would also have been apparent upon visual inspection by an experienced modeler…it is critical that model reviews be performed frequently by experienced modelers, particularly to check for semantic mistakes—those that won't be caught by the modeling tools' validation checks… Model reviews performed in a briefing format or through static captures of the model (typically via PDF files or HTML files) are much less effective at ferreting out errors."

MBSE Lightning Round

Our Challenge: MBSE Missteps

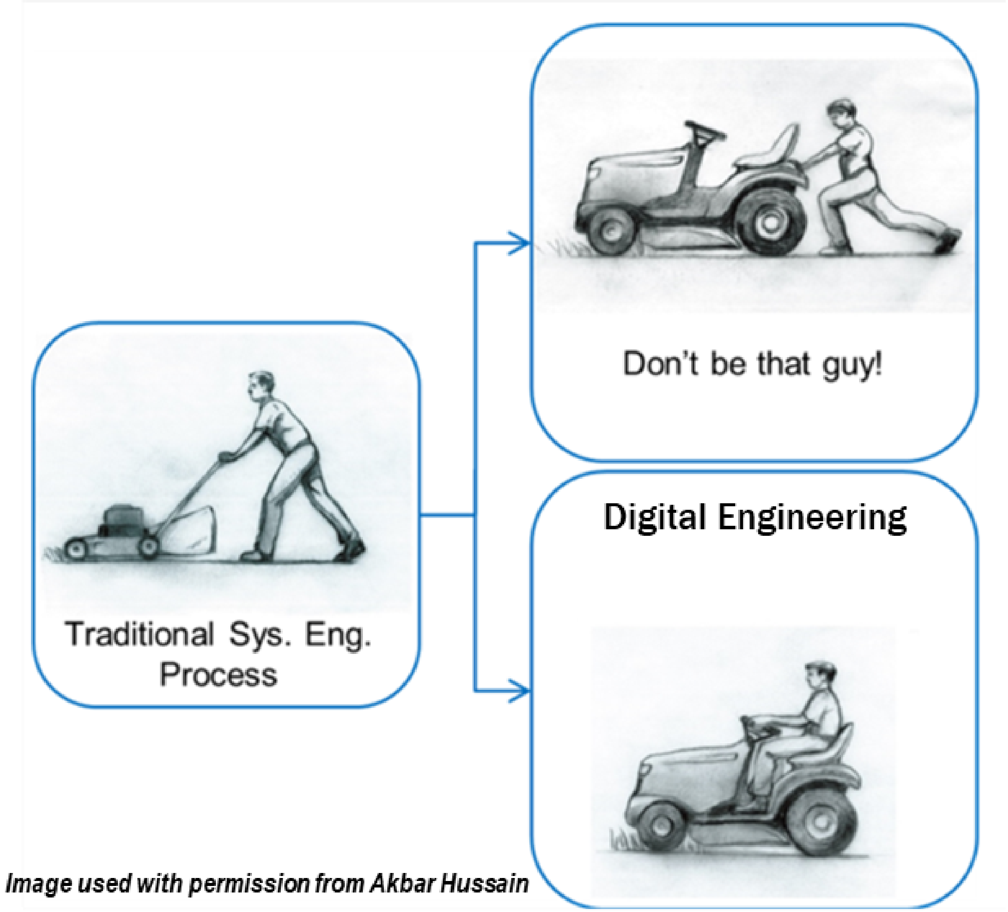


Image used with permission from Akbar Hussain

- MBSE efforts stall because they fail to grasp the opportunities inherent in the new approach
  - Confounding the *outcome* with the *means*
  - Excessive focus on diagrams/views vs. data
- Models *can* be more consistent and coherent…but it takes skill and effort to achieve that end

MBSE Lightning Round

SAIC's SysML Modeling Style

MBSE Lightning Round

SAIC's SysML Modeling Style and Pragmatism

"…this involves a willingness to trade off theoretical purity or future perfection in favor of getting things done today." p. 26

"…a willingness to experiment and be proven wrong.
This means we try stuff. We fail.
Then we use the lessons from that failure
in the next experiment." p.27

Apprenticeship Patterns: Guidance for the Aspiring Software Craftsman (2009)
David H. Hoover & Adewale Oshineye. O'Reilly Media

MBSE Lightning Round

SAIC's SysML Modeling Style

- Focused on the integration of behavior and structure through the creation of well-formed blocks:
  - Behaviors
    - Operations (what functions the block *can* do) + Parameters (inputs/outputs of each function)
    - State machine (what the block *does* under various conditions)
  - Structure
    - Part properties defining its components
    - Proxy ports defining what can flow into/out of the block
    - Internal block diagram (optional)
    - Item flows / flow sets defining flows into/within the block's structure
  - Attributes
    - Value properties defining characteristics of interest
- The focus on operations as the atomic behavioral element eliminates ambiguity (1:1 ownership) and facilitates metachain queries.
- The use of signals as conveyed elements, inputs/outputs (parameters), and triggers enables a richer understanding of system behavior than traditional functional decomposition.

MBSE Lightning Round

SAIC’s SysML Modeling Style

- Limited to a subset of SysML:
  - All ports are proxy ports
  - Reference properties, allocations, and swimlanes are prohibited
  - Item flows are used to integrate behavioral and structural views
- A minimal set of customizations is used:
  - <<logical>> and <<physical>> stereotypes are used to separate abstraction levels
  - <<flow set>> customizations allow the linking of deeply nested parts/ports
- The style focuses on usage and inferences *from usage*, not manual creation of relationships:
  - Example 1: Calling an operation on an activity diagram allows the inference that the block that owns the operation participates in the activity
  - Example 2: Realizing an object flow with an item flow establishes the source/target port (so send and accept events can infer *ports* and *parts*)
  - Example 3: The calling of operations in state do/entry/exit or transition behaviors allows inference of what states/transitions are able to support mission threads (activities)…or the impact of failures

MBSE Lightning Round

SAIC's Digital Engineering Validation Tool

MBSE Lightning Round

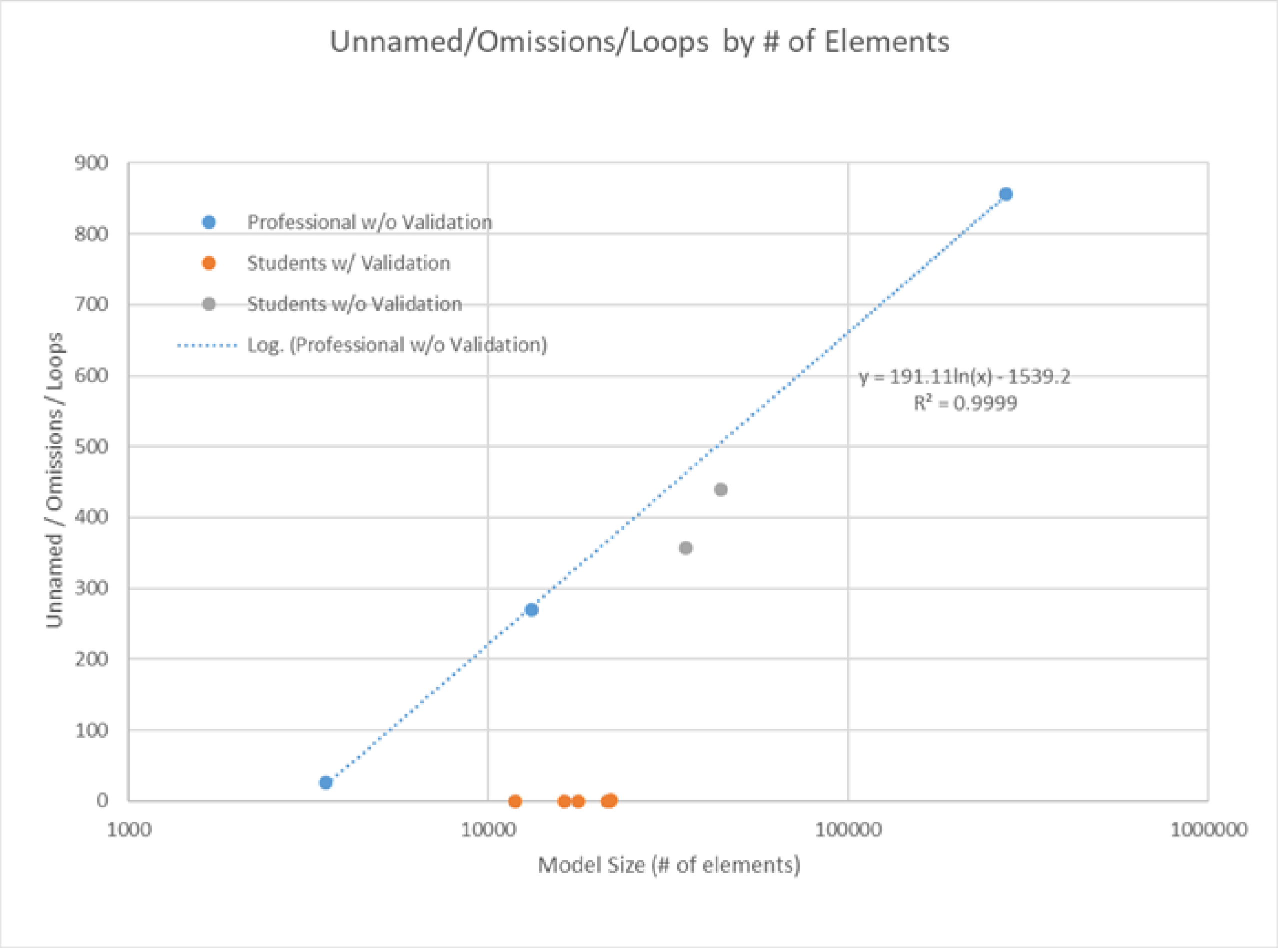
SAIC Digital Engineering Validation Tool

- *Shipshape and Bristol Fashion: Model Documentation and Curation to Facilitate Reuse* (Vinarcik/Jugovic, 2019 NDIA Systems and Mission Engineering Conference) discussed the use of automated validation in systems modeling: "When a model passes validation, you KNOW it is compliant…Validation is fast and consistent, Seconds/Minutes vs. Hours"

- SAIC released its Digital Engineering Validation Tool in December 2019:
  - V1.0 (December 2019—126 rules):
    - Initial customizations
    - Videos
  - V1.5 (April 2020—153 rules)
    - Model-based Style Guide
    - Example model (*Ranger* lunar probe)
    - Rhapsody rules
  - V1.6 (August 2020—164 rules)
    - Classification/Data Rights customization
  - V1.7 (January 2021—184 rules)
    - FMEA customization

MBSE Lightning Round

2020 ASEE Paper:
Treadstone: A Process for Improving Modeling Prowess Using Validation Rules



MBSE Lightning Round

Classification / Data Rights Profile
FMEA Profile

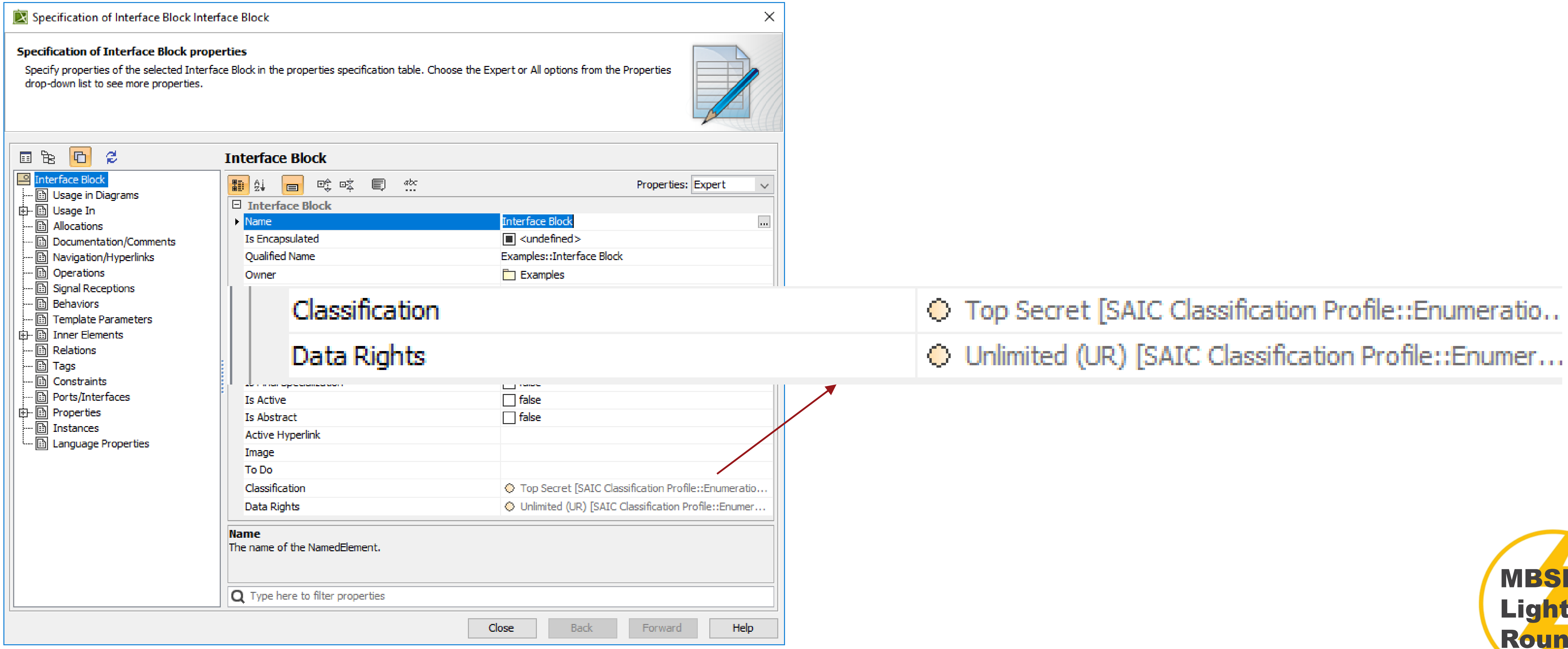
MBSE Lightning Round

SAIC Classification Profile: Restriction Relationships

#	Client	Supplier	Classification	Data Rights
1	Classification Guide	Signal 2	Top Secret	Unlimited (UR)
2	Classification Guide	value1	Secret	Limited Rights (LR)
3	Classification Guide	Signal	FOUO	Specifically Negotiated License Rights (
4	Classification Guide	Operation...	Unclassified	Specifically Negotiated License Rights (
5	Classification Guide	ON	Confidential	Specifically Negotiated License Rights (
6	Classification Guide	Test 2 Value	Confidential	Limited Rights (LR)
7	Classification Guide	Test	FOUO	Limited Rights (LR)
8	Classification Guide	Test 2	Secret	Limited Rights (LR)
9	Classification Guide	inout Port...	FOUO	Restricted Rights (RR)
10	Classification Guide	Test	Confidential	Restricted Rights (RR)
11	Contract B	Test 2		Government Purpose (GPR)
12	Classification Guide	Test	Secret	
13	Classification Guide	Top Secret	Top Secret	
14	Contract B	X	Secret	Unlimited (UR)

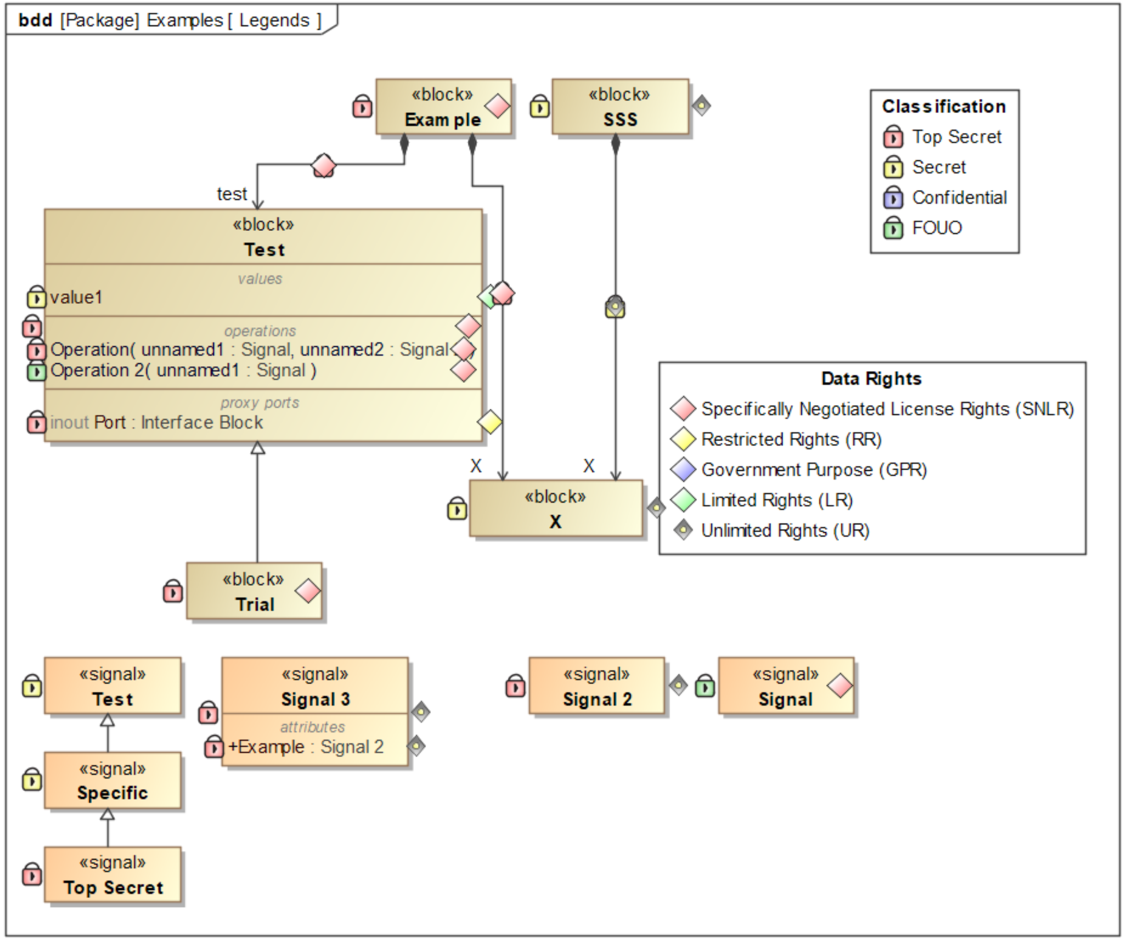
MBSE Lightning Round

SAIC Classification Profile: Inherent Classification/Data Rights Properties



MBSE Lightning Round

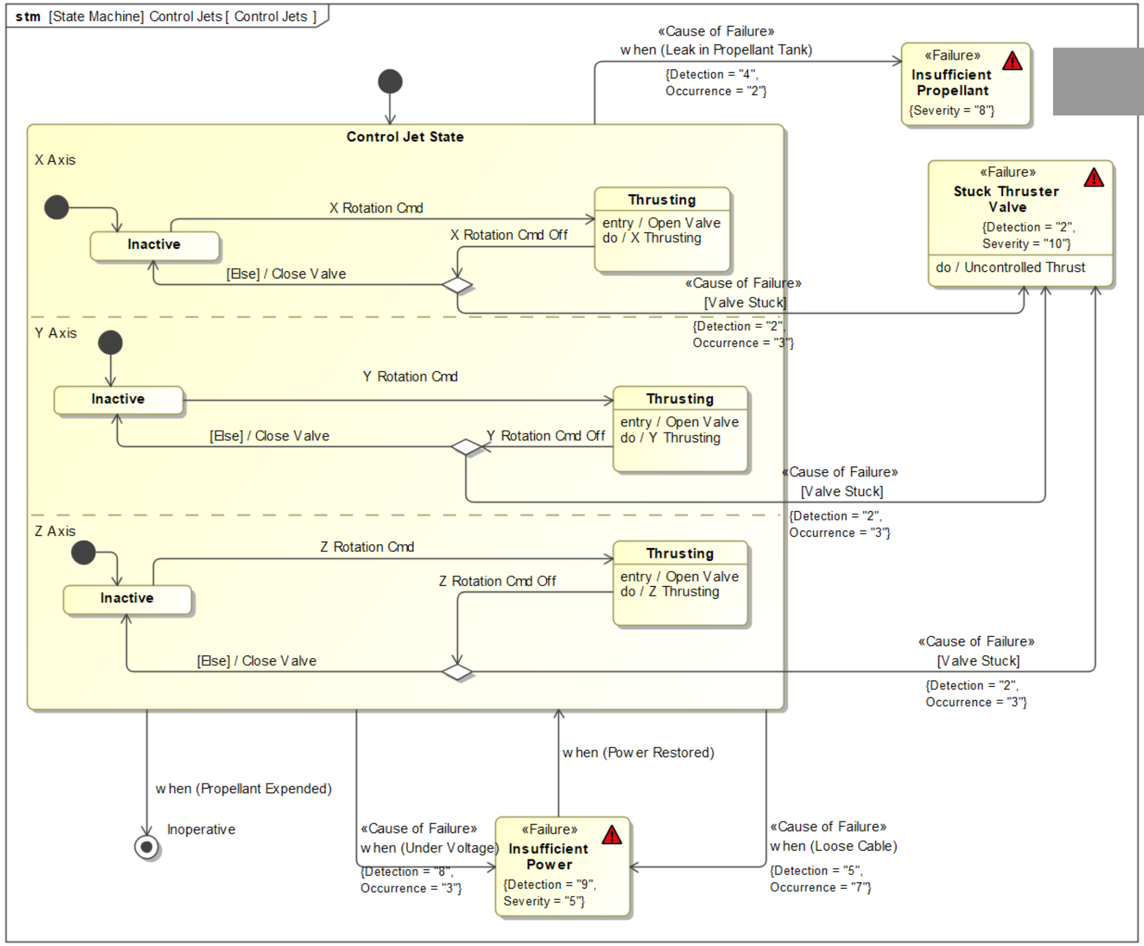
SAIC Classification Profile

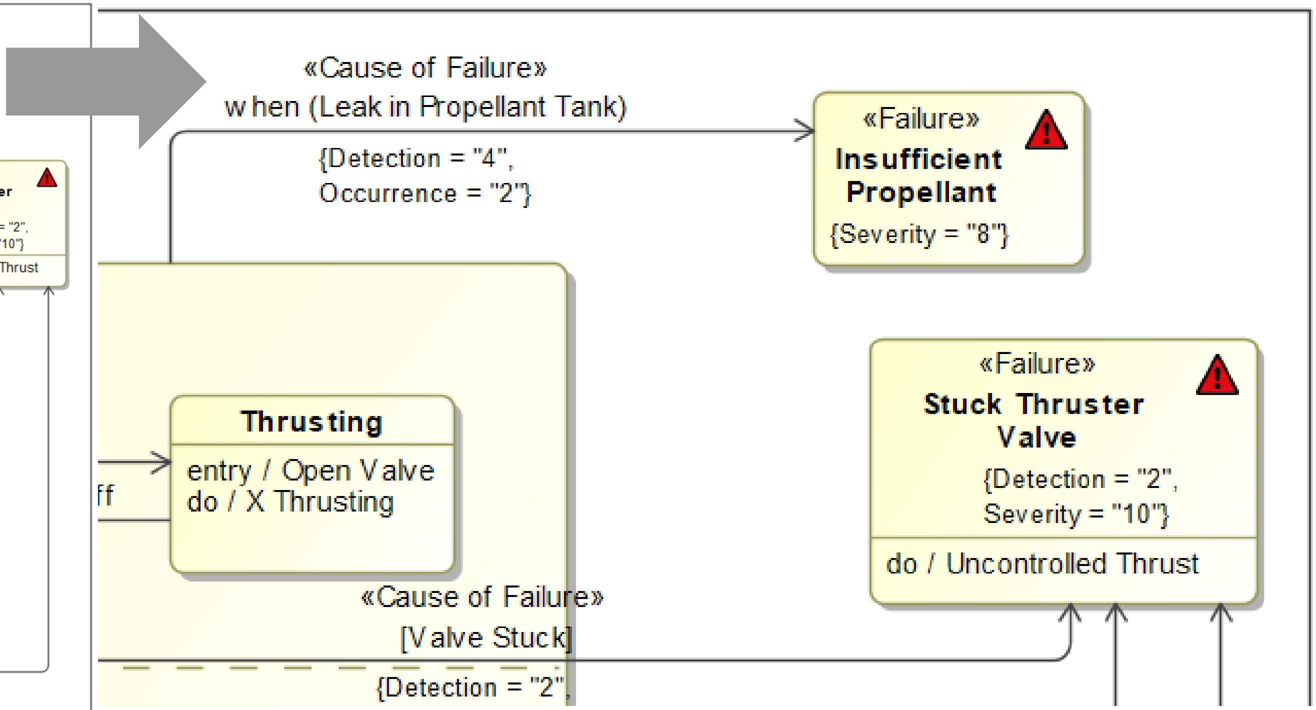


#	Name	Classification	Classification Aggregator	Data Rights	Data Aggregator
1	Activity	FOUO	FOUO	Specifically N...	Specifically Negotiated License
2	Port	Top Secret	FOUO Top Secret	Restricted Ri...	Restricted Rights (RR) Unlimited (UR)
3	Test	Top Secret	FOUO Confidential Top Secret Secret Unclassified	Specifically N...	Limited Rights (LR) Restricted Rights (RR) Unlimited (UR) Specifically Negotiated License Unspecified
4	Interface Block	Top Secret	Top Secret	Unlimited (UR)	Unlimited (UR)
5	flow1	Top Secret	Top Secret	Unlimited (UR)	Unlimited (UR)
6	unnamed1	FOUO	FOUO Top Secret	Specifically N...	Specifically Negotiated License
7	Signal	FOUO	FOUO	Specifically N...	Specifically Negotiated License
8	Operation	Top Secret	Unclassified FOUO Top Secret	Specifically N...	Specifically Negotiated License Unlimited (UR)

MBSE Lightning Round

SAIC FMEA Profile





SAIC FMEA Profile:
State and Mission-Thread Driven Analysis

#	Name	Owned Parameter	Available in State	Unavailable in State	Unavailable in Failures	Called On	Participates in (1st level up)	Participates in (2nd level up)	Participates in (3rd level up)	Possible Failures	Hazard	Hazard Severities
1	Close Valve	in parameter : Orientation Control Power		Inactive Thrusting Control Jet State Thrusting Thrusting Inactive Inactive	Insufficient Power Stuck Thruster Valve Insufficient Propellant	Close Valve Close Valve Close Valve						
2	Open Valve	in parameter : Orientation Control Power	Thrusting Thrusting Thrusting	Inactive Control Jet State Inactive Inactive	Insufficient Power Stuck Thruster Valve Insufficient Propellant	Open Valve Open Valve Open Valve						
3	Change X Axis Rotation	out : Control Thrust X Axis in : Orientation Propellant out result : Orientation Propellant	Thrusting	Inactive Thrusting Control Jet State Thrusting Inactive Inactive	Insufficient Power Stuck Thruster Valve Insufficient Propellant	Orientate Ranger (X Thrusting	Maneuver	Perform Automatic Mar Perform Manual Maneu Correct Course Fire Main Engine	Perform Automatic Maneuver Perform Manual Maneuver	Cannot Target Uncontrolled Thrus Cannot Target Uncontrolled Thrus	Suboptimal Data Collection Mission Failure	6 10
4	Change Y Axis Rotation	out : Control Thrust Y Axis out : Orientation Propellant in : Orientation Propellant	Thrusting	Inactive Control Jet State Thrusting Thrusting Inactive Inactive	Insufficient Power Stuck Thruster Valve Insufficient Propellant	Orientate Ranger (Y Thrusting	Maneuver	Perform Automatic Mar Perform Manual Maneu Correct Course Fire Main Engine	Perform Automatic Maneuver Perform Manual Maneuver	Cannot Target Uncontrolled Thrus Cannot Target Uncontrolled Thrus	Suboptimal Data Collection Mission Failure	6 10
5	Change Z Axis Rotation	in argument : Orientation Propellant out parameter : Orientation Propellant out parameter1 : Control Thrust Z Axis	Thrusting	Inactive Thrusting Control Jet State Thrusting Inactive Inactive	Insufficient Power Stuck Thruster Valve Insufficient Propellant	Orientate Ranger (Z Thrusting	Maneuver	Perform Automatic Mar Perform Manual Maneu Correct Course Fire Main Engine	Perform Automatic Maneuver Perform Manual Maneuver	Cannot Target Uncontrolled Thrus Cannot Target Uncontrolled Thrus	Suboptimal Data Collection Mission Failure	6 10

MBSE Lightning Round

SAIC FMEA Profile: Automatic RPN Calculation

#	Name	Severity	Maximum Occurrence	Maximum RPN	Causes of Failure	Cause Detection	Cause Occurence	Cause Criticality	Cause RPN	Malfunctions	Unavailable Functions	Affected Use Cases	Failures	Hazard	Hazard Severity
1	Insufficient Power	5	7	175	Trigger:when (Under Voltage) Trigger:when (Loose Cable)	8 5	3 7	24 35	120 175		Close Valve(parameter : C Open Valve(parameter : C Change X Axis Rotation(: Change Y Axis Rotation(: Change Z Axis Rotation(ar Uncontrolled Thrust(: Thr	Perform Automatic Maneu Perform Manual Maneuver	Cannot Target Uncontrolled Thrust Cannot Target Uncontrolled Thrust	Suboptimal Data Collection Mission Failure	6 10
2	Insufficient Propellant	8	2	64	Trigger:when (Leak in Propellant	4	2	8	64		Close Valve(parameter : C Open Valve(parameter : C Change X Axis Rotation(: Change Y Axis Rotation(: Change Z Axis Rotation(ar Uncontrolled Thrust(: Thr	Perform Automatic Maneu Perform Manual Maneuver	Cannot Target Uncontrolled Thrust Cannot Target Uncontrolled Thrust	Suboptimal Data Collection Mission Failure	6 10
3	Stuck Thruster Valve	10	3	60	Valve Stuck Valve Stuck Valve Stuck	2	3	6	60	Uncontrolled Thrust(: T	Close Valve(parameter : C Open Valve(parameter : C Change X Axis Rotation(: Change Y Axis Rotation(: Change Z Axis Rotation(ar	Perform Automatic Maneu Perform Manual Maneuver	Cannot Target Uncontrolled Thrust Cannot Target Uncontrolled Thrust	Suboptimal Data Collection Mission Failure	6 10

MBSE Lightning Round

From *Treadstone: A Process for Improving Modeling Prowess Using Validation Rules*

2020 American Society for Engineering Education Annual Conference

Teaching SysML Modeling at the University of Detroit Mercy

MBSE Lightning Round

Pedagogy of the SysML Modeling Class at UDM

Phase I:

- Construction of small models
- Creation of simple diagrams
- Experience with collaboration on TeamWork Cloud

“System modeling is not a conceptually simple or straightforward task…building models using these tools is not always straightforward, and like software programming, is a skill that not everyone can learn equally well.”

R. A. Noguchi, *Lessons Learned and Recommended Best Practices from Model-Based Systems Engineering (MBSE) Pilot Projects*, Aerospace Corporation, 2016

Phase II:

- Collaborative modeling of representative systems
- Focused on experiencing the subtleties of working together on a large system model
- Showcases best practices for collaboration
- Cultivates a visceral understanding of how modeling tools work and how to make a model serve a systems engineering effort
- Past topics for Phase II include notional nuclear submarines, next generation Mars orbiters, and simulated Mars rovers

MBSE Lightning Round

Managing Phase II

- Classroom sessions are suspended, and a laboratory format is adopted
- Weekly meetings are conducted with each team
  - Answer questions
  - Recommend next steps
  - Shepherd the team to completion
- Instructor serves as a senior modeler/reviewer for each team
  - Excessive time spent on semantic issues and method deviations
  - Less time available for focusing on the intellectual content

MBSE Lightning Round

Pre-Release Digital Engineering Validation Tool

- A pre-release version of the Digital Engineering Validation Tool was used during the Fall 2019 term.
- This allowed encoding of the instructor’s knowledge/review process and enabled rapid grading/review of assignments.
- Model errors that “leaked” past rules spawned new rules.
- Automation is important:
  - 21 students Fall 2019
  - 40 students Fall 2020

MBSE Lightning Round

2019 Topic: Mars Society University Rover Challenge

- College competition run by the Mars Society (includes testing in Utah desert)
- 2020 challenge consisted of 79 requirements and these milestones:
  - Preliminary Design Review (PDR)
  - System Acceptance Review (SAR)
  - Science Plan
- 36 teams passed SAR (competition cancelled due to COVID-19)

- How complete were the requirements?

MBSE Lightning Round

Requirements Count / Increase By Team

Team	Initial	Final	% Increase
Curiosity	76	205	170%
JARS	76	216	184%
Strike Force Alpha	76	142	87%
Team Bolt	76	172	126%
Team Chimps	76	284	274%
Team Voodoo	76	110	45%

Growth driven by use of extended requirement types and two rules:
all requirements must be satisfied and verified.

MBSE Lightning Round

Fall 2019 Model Size vs. Checkpoint

	Model Elements				Validation		
Team	Initial	Checkpoint	Final	End of Term	Errors	Info	Pages
Curiosity	8,587	22,550	17,588	21,483	0	0	198
JARS	9,548	16,291	18,357	21,905	1	214	237
Strike Force Alpha	7,070	8,963	13,351	16,204	0	0	193
Team Bolt	8,,262	19,440	15,206	17,773	0	39	199
Team Chimps	10,015	22,050	18,732	21,768	0	0	242
Team Voodoo	5664	8,583	9,846	11,836	0	76	175

Note: The ruleset grew from 72 rules at kickoff to 127 rules at completion
Rules instability led to rework in addition to model maturation/growth

MBSE Lightning Round

Fall 2020: Mars Octet

- Federated model used to integrate eight individual models:
  - Collection Rover
  - Retrieval Lander
  - Fetch Rover
  - Ascent Rocket
  - Return Orbiter
  - Mars Expedition Ice Mapper
  - Mars NAVCOM
  - Mission Control/Deep Space Network
  - Integration Model

- Models were based upon publicly available mission websites and documents

MBSE Lightning Round

Mars Octet Model Sizes (3 DEC 2020: 74 Days)

Model	Info	Errors	Size	Pages
Collection Rover	0	0	25,614	246
Retrieval Lander	0	0	11,259	153
Fetch Rover	0	0	15,343	139
Ascent Rocket	0	0	23,721	301
Return Orbiter	0	0	16,572	117
Mars Expedition Ice Mapper	0	0	24,970	243
Mars NAVCOM	72	167	18,127	262
Mission Control/Deep Space Network	474	0	12,271	148
Integration Model	13	12	5,892	1,651

MBSE Lightning Round

Mars Octet: Lessons Learned

- Rules stability reduced rework (174 at start, 184 at conclusion)
- Six mission models are 0/0 (zero info/zero errors)
- “Flow-heavy” communications models have errors:
  - Late “freeze” of interfaces / flows to boundaries
  - Late introduction of two rules that test for conveyed signal loss/gain at interfaces
- Bug in TeamWork Cloud model synchronization caused spurious recovered elements

- Outcome:
  - 40 Students
  - 74 Days
  - 153,769 model elements
  - 3,260 pages of content (Requirements Reports used to generate this count)
  - Fully integrated and consistent mission models
  - Communications/integration models not fully matured

MBSE Lightning Round

Conclusion

MBSE Lightning Round

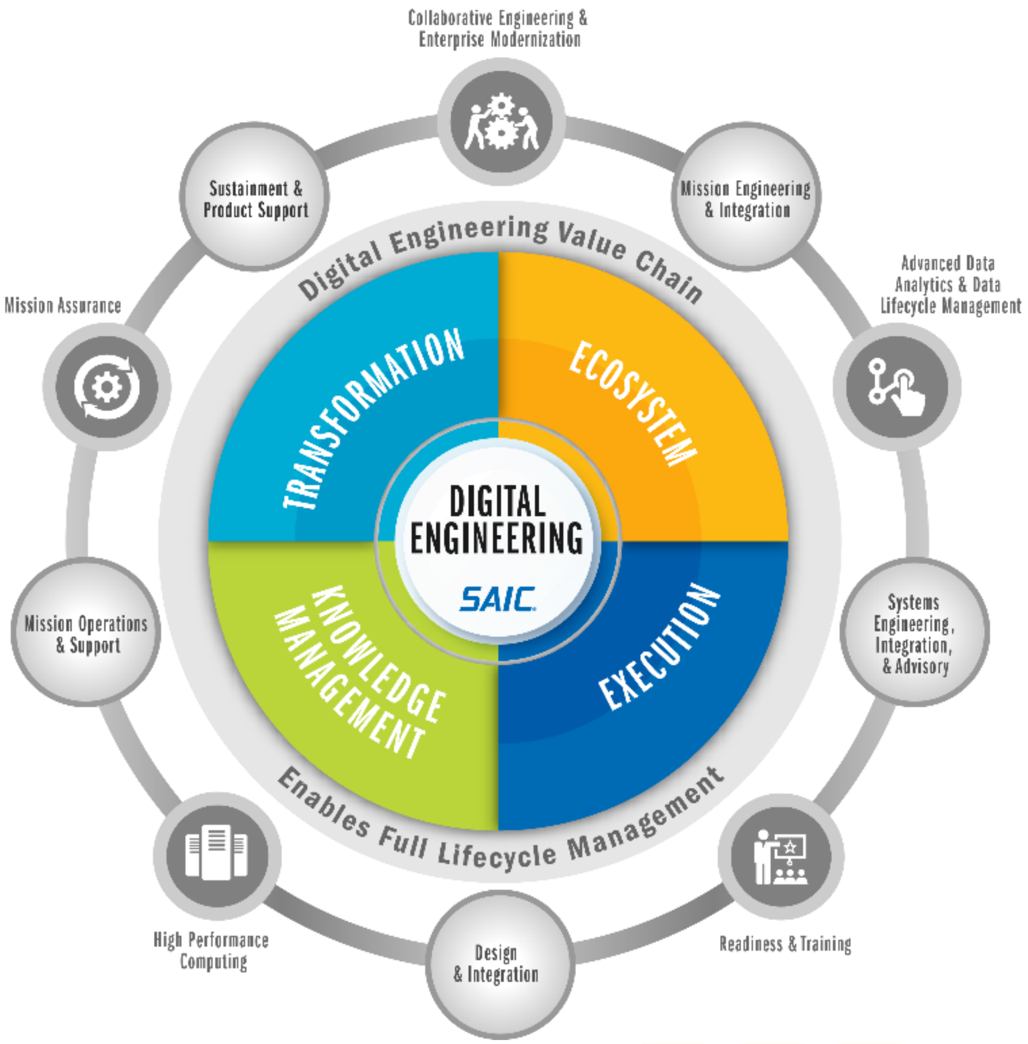
Conclusion

- Automated validation rules have a significant impact on model quality
- Rules must be tested with real-world modeling to detect corner cases/bugs and ensure usefulness
- Hands-on modeling (in a laboratory format supported by automated validation) enables novices to rapidly develop skill and confidence (and generate high-quality models)
- Relationship-based analysis has impact and traceability advantages vs. tag- or property-based approaches
- Real-time integration of multiple system models is facilitated by automated validation
  - Good systems engineering practices can reduce pain points (such as late interface/flow changes)

- Mars Octet models will be published at https://hypermodeling.systems

MBSE Lightning Round

SAIC Digital Engineering



Online: saic.com/digital-engineering

Email: digitalengineering@saic.com

MBSE Lightning Round

SAIC Digital Engineering

SAIC DE Profile & Validation Rules:

https://www.saic.com/digital-engineering-validation-tool

2021 Annual INCOSE international workshop
Virtual Event
January 29 - 31, 2021

Premier Systems Engineering Workshop

www.incose.org/iw2021/

MBSE Lightning Round