31st Annual INCOSE international symposium
virtual event
July 17 - 22, 2021

Myron Hecht, The Aerospace Corporation
Jaron Chen, The Aerospace Corporation

Verification and Validation of SysML Models

www.incose.org/symp2021

Need for SysML Model Validation and Verification (V&V)

- Model Based Systems Engineering (MBSE) will not succeed without correct and complete models.

- Consequences of incomplete or incorrect models
  - Integration failures due to erroneous or incomplete model interface blocks,
  - Violations of space weight or power constraints because of value properties leading in model block definitions and instantiations
  - Invalid analysis results because the model did not represent the system,
  - Inability to perform acceptance testing because requirements were not traced properly traced to the elements that satisfy them, and many others.

- Net result: cost overruns and delays – just as in programs using conventional systems engineering practices.

- V&V methods should be integrated into programs using MBSE in order to avoid the same or worse program impacts

Previous Work

Model Transformation

- Manzoor Ahmad, Iulia Dragomir, Jean-Michel Bruel, Iulian Ober, Nicolas Belloir., "Early Analysis of Ambient Systems SysML Properties using OMEGA2-IFx," in SIMULTECH 2013, Reykjavik, Iceland, Jul 2013 .
- Yosr Jarraya and Mourad Debbabi, "Formal Specification and Probabilistic Verification of SysML Activity Diagrams," in IEEE Sixth International Symposium on Theoretical Aspects of Software Engineering, 2012.
- Messaoud Rahim, Ahmed Hammad, Malika Boukala-Iuoaleln, "Towards the Formal Verification of SysML Specifications: Translation of Activity Diagrams into Modular Petri Nets," in 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence, 2015.

Evaluation Methods

- Julie Fant, et. al., Systems Engineering Model Assurance Levels (MALs) Scale & Detailed Criteria Aerospace Technical Report, ATR-2020-00232-Rev A, March, 2021
- Edward R. Carroll and Robert J. Malins, "What Questions Would a Systems Engineer Ask to Assess Systems Engineering Models as Credible?", Sandia Report SAND20XX-XXXX, September 2020
- Dominique Ernadote, (Airbus Defense and Space Company), "A Framework for Descriptive Models Quality Assessment," IEEE 978-1-5386-4446-1/18, 2018.

Modeling and Style Guides

- Michael Vinnarcik and Heidi Jugovic, Digital Engineering Validation Tool Enables Efficiency Gains, https://www.saic.com/blogs/digital-engineering-validation-tool-enables-efficiency-gains: SAIC Corporation, 2021
- "System Modeling Standards and Guidelines," US Navy, Strategic Systems Program, Systems Engineering, System Modeling IPT, 28 December 2018
- Eric M. Lautenschlager and Michael Munoz, B-52 Model Based Systems Engineering (MBSE) Model Style Guide, MITRE Report MTR190557, September, 2019
- Georgia Tech Research Institute Digitally Integrated Systems Engineering Model Style Guide (draft), March, 2021
- Boeing Corp., CERP MBSE Style Guide, March 2021

Model V&V is Governed by Requirements

- Types of requirements
  - Project Specific requirements
    - Correctness of requirements
    - Completeness and accuracy of representation
    - Accurate traceability of requirements to design and to verification methods
    - Utility of produced artifacts (for development, management, design reviews, testing and verification, and sustainment)
    - Completeness and correctness of internal data, exports and imports
  - Generic requirements
    - Organization
    - Ease of navigation and information retrieval
    - Internal and External Documentation
    - Descriptive names
    - Complete diagrams
    - Correct use of SysML

Model Requirements Catalog

1. **General:**

   – Requirements for language (.e.g., SysML vs, UPDM)

   – Incorporation of Government furnished profiles,

   – Production of artifacts for model development, design reviews, testing and verification, and sustainment,

2. **Requirements Diagrams and models:** amount and level of details needed for system requirements (very detailed requirements might be kept in a separate requirements management system)

3. **Structural Model Elements and Diagrams:** Requirements for the amount and level of detail for structural content

4. **Behavioral Model Elements and Diagrams:** Requirements for the amount and level of detail for behavioral content.

5. **Parametric Models:** Requirements for modeling and analyzing non-functional system attributes

   – Capacity and Response Time

   – Reliability, Maintainability, Availability

   – Cybersecurity

   – Other Specialized areas

Manual v. Automated Model Verification

- Manual V&V
  - Evaluation of model's human meaning (semantics)
    - Correctness of requirements allocation and verification
    - Completeness of model representation
    - Completeness and correctness of interfaces
    - Correctness of documentation
    - Correctness of value imports and exports
  - Inspection and demonstration are the primary methods
    - Test used for verification of quantitative results
- Automated V&V
  - Evaluation of model's conformance to language rules and modeling conventions
    - Requirements traceability
    - Structural and flow representations
    - Behavioral representations
  - Scripts are the primary method of verification
    - Analogous to static analyzers for software

Examples of Manually Verified Requirements

- The model shall be organized in a consistent manner (e.g. by organization, by hierarchy, or by subsystem)
  - Verified by inspection
  - Rationale: large models are difficult or impossible to understand unless their organization is clearly understood
  - Additional details to be specified in requirement: how model should be organized

- The model shall include package diagrams that capture and describes the model organization
  - Verified by inspection
  - Rationale: package diagrams are the primary means of depicting model organization
  - Additional details to be specified: how package diagrams should be organized

- The model shall include diagrams that depict links and enable navigation to all diagrams and views contained in the model
  - Verified by demonstration
  - Rationale: model navigation aids enable information to be found that might otherwise be missed
  - Additional details to be specified: what navigation aids should be provided

Example of Automatically Verifiable Requirement

The model shall have a different target state for each state/transition pair on the state machine diagram

Script language

Refers to element being validated

Edit Specification
Select language from the language list and specify body in a dedicated editor.

Language:
Jython

Body:
validate(THIS) : boolean

```
1  transitions=THIS.getOutgoing()  #Get all the transitions emanating from the state
2  result.set(True)
3  states=[]   # List containing all the target states
4  for transition in transitions:
5      state=transition.getTarget() #Get target state from transition
6      if state in states:     # If a state is the target of a transition twice, then two transitions go into the same state
7          result.set(False)   # Rule is violated
8      states.append(state)    # Add state to list of target states
9
```

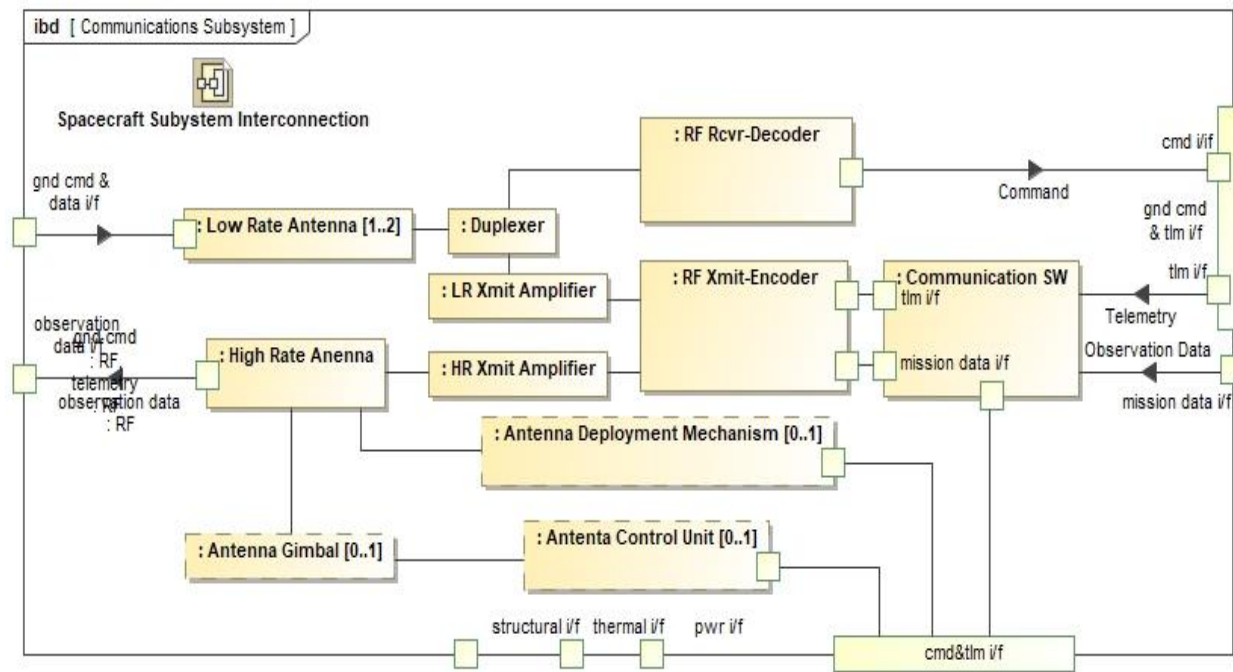Language instructions

Expert   OK   Cancel   Evaluation Mode

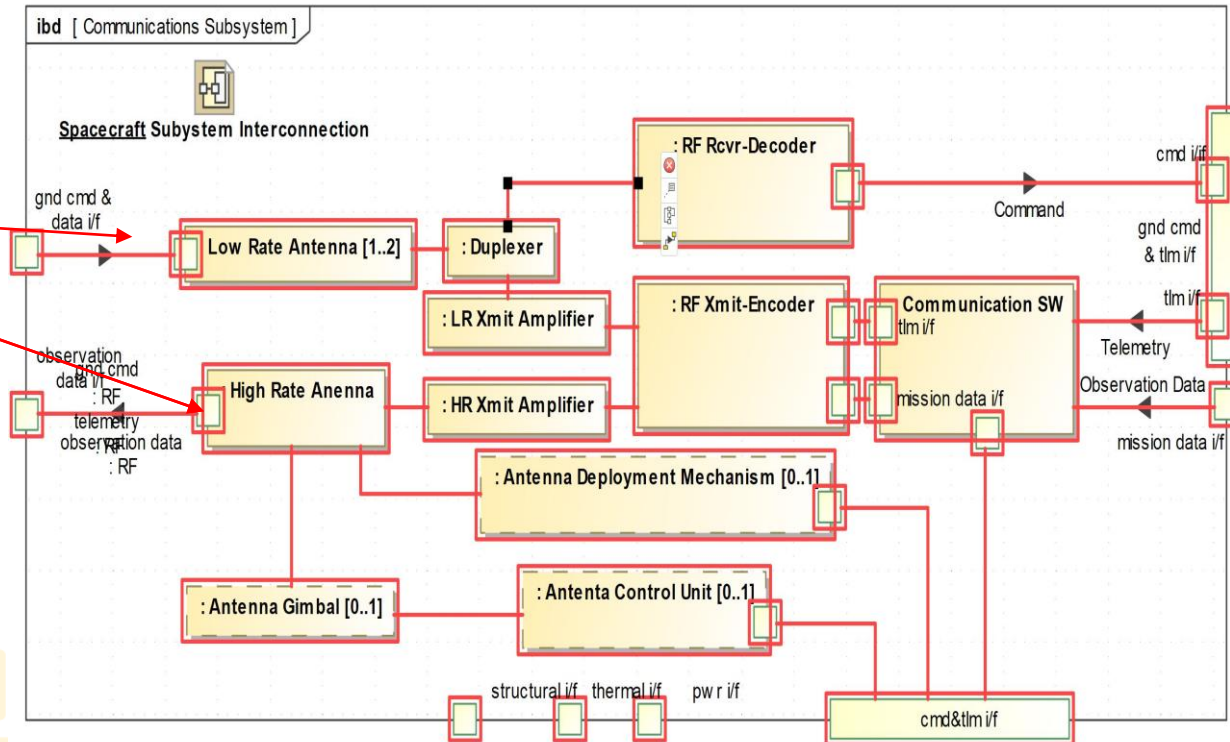Setting Boolean output to determine if validation rule is violated or not

Method from MagicDraw API that allows access to element properties
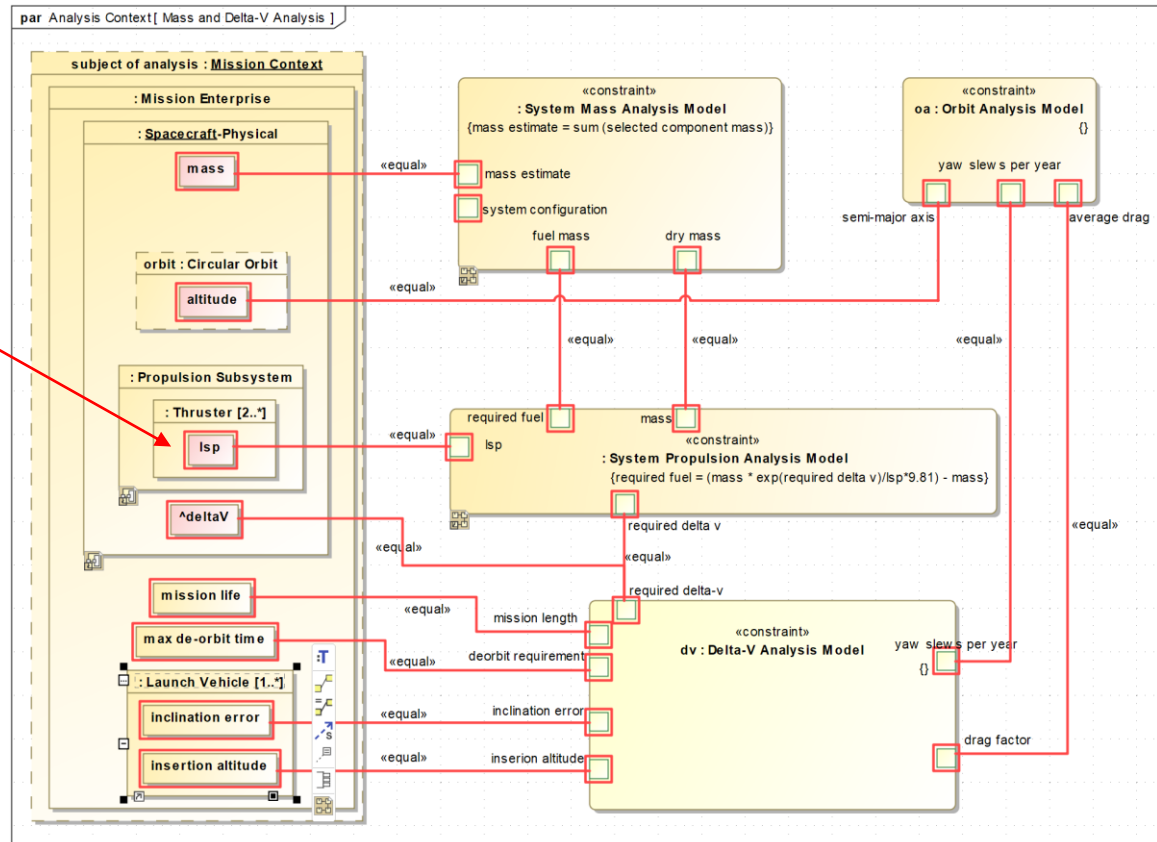
Check that all connections are through ports
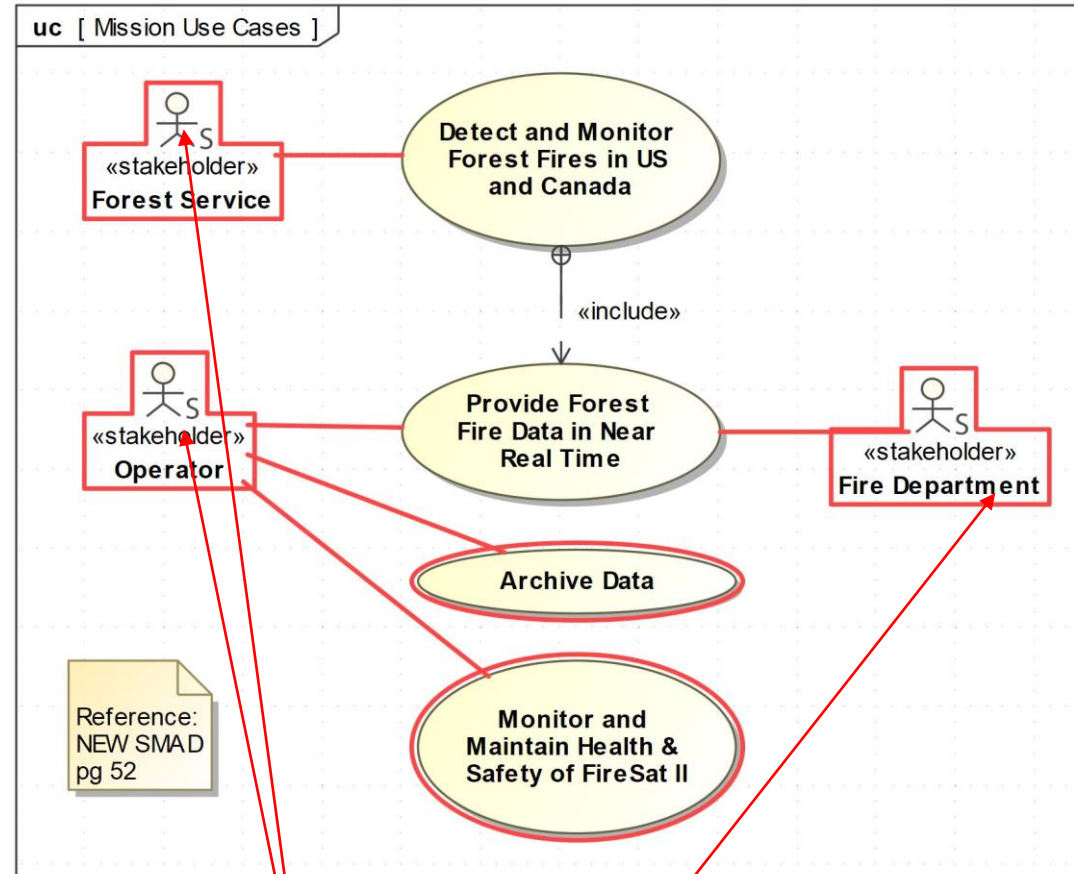
2 of many violations:

Typing of Value properties

Error: *"The model shall include data type for all attributes and properties"*
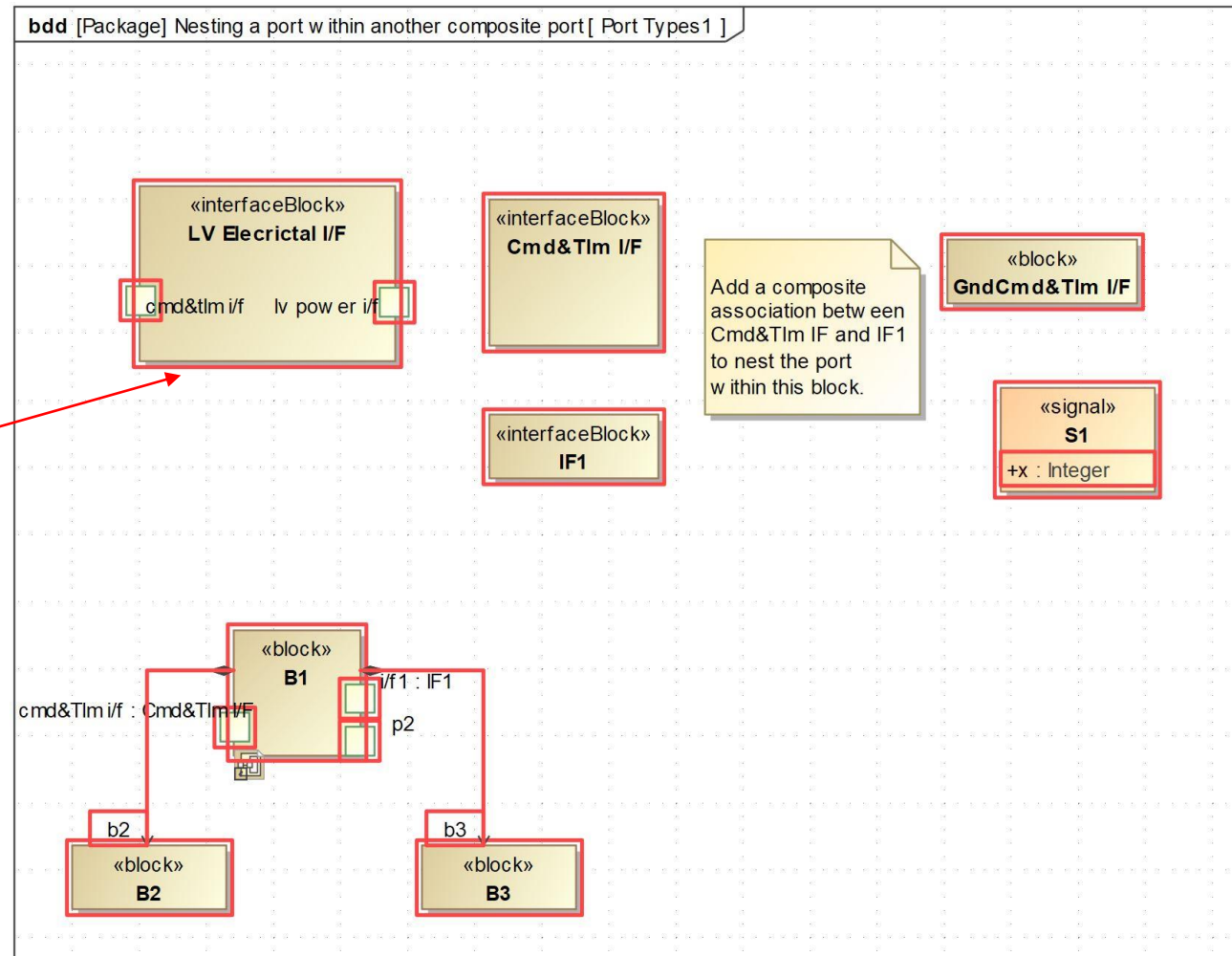
Documentation of Model Elements

Error: "All actors need documentation."

Traceability between blocks and requirements

Error: "All blocks representing system components shall be traceable to a requirement."

Element: *SysML Blocks*

Conclusions

- A necessary condition for MBSE and for Digital Engineering is that the models are correct
- Model Requirements are necessary for model verification and validation (V&V)
  - Model requirements and distinct form system requirements.
- V&V includes manual and automated methods
  - Manual methods are primarily inspection and validation, and are necessary to validate model requirements on aspects of the model that are interpreted by humans (natural language content, model navigation, and model output)
  - Automated methods can be used to check model syntax, relationships, and structure
- A catalog of candidate requirements and verification methods will soon be available to assist in development of model requirements