33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Case Studies in Disaster

Modern Digital Engineering Methods and Error Detection

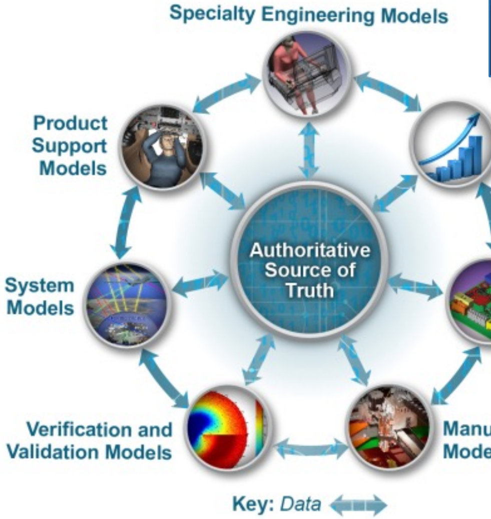
Heidi Jugovic & Chris Swickline

The Promise and Potential of MBSE

- Model Based Systems Engineering (MBSE) – "the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases" - *INCOSE SE Handbook v4*
- Benefits According to INCOSE
  - Improved Communication
  - Increased Ability to Manage System Complexity
  - Improved Product Quality
  - Enhanced Knowledge Capture
  - Improved Ability to Teach and Learn SE Fundamentals

How do we realize these benefits?

Digital Thread



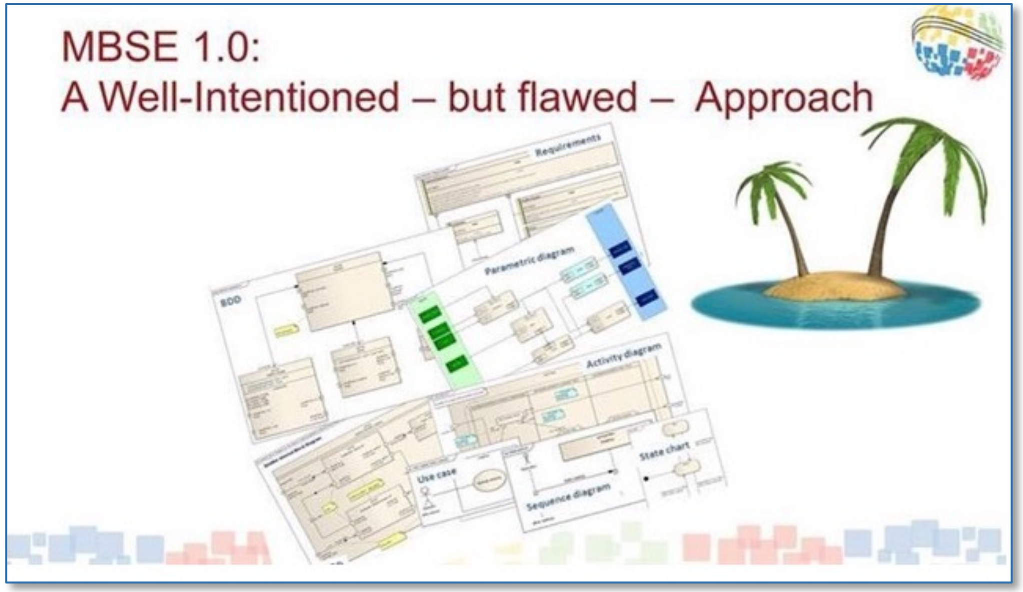
U.S. Space Force
Vision for a Digital Service
SF/CTIO
MAY 2021

DEPARTMENT OF DEFENSE
DIGITAL ENGINEERING STRATEGY
JUNE 2018

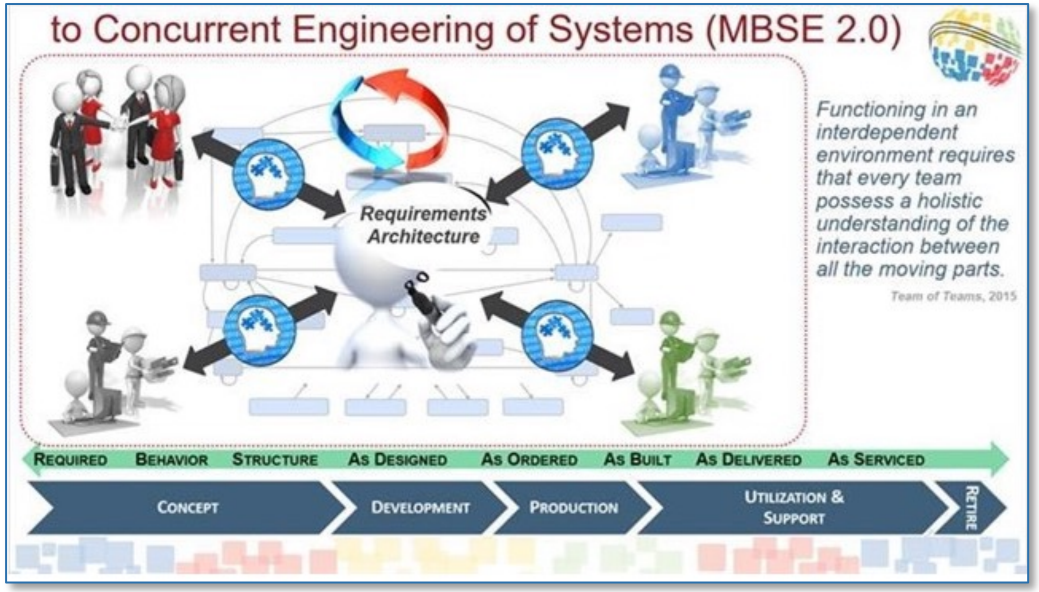
UNITED STATES
NAVY & MARINE CORPS
DIGITAL SYSTEMS
ENGINEERING
TRANSFORMATION
STRATEGY
United States Navy and Marine Corps
Digital Systems Engineering Transformation Strategy
2020
Washington, DC

Moving from MBSE 1.0 to MBSE 2.0

- Migrate from a diagram-centric approach (MBSE 1.0) to a **data-centric** approach (MBSE 2.0)
- MBSE 2.0 requires data to be well-structured to support structured queries, analysis, and linkages
  - https://www.saic.com/digital-engineering-validation-tool



MBSE 1.0:
A Well-Intentioned – but flawed – Approach



to Concurrent Engineering of Systems (MBSE 2.0)

Functioning in an interdependent environment requires that every team possess a holistic understanding of the interaction between all the moving parts.

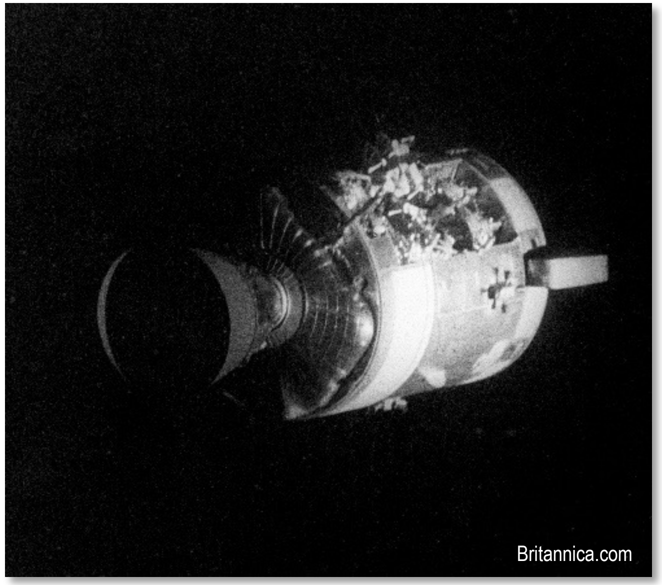
Team of Teams, 2015

https://community.aras.com/b/english/posts/mbse-2-0-what-s-that-all-about

- Model Validation
- Table / Matrix Generation
- Legend Visualization
- Interface Compatibility Checks
- Requirement Satisfaction & Verification
- Data Extraction for Analytics
- Model Federation for Systems of Systems
- Failure Analysis
- Integration, Verification, & Validation Planning

Case Study 1: Apollo XIII

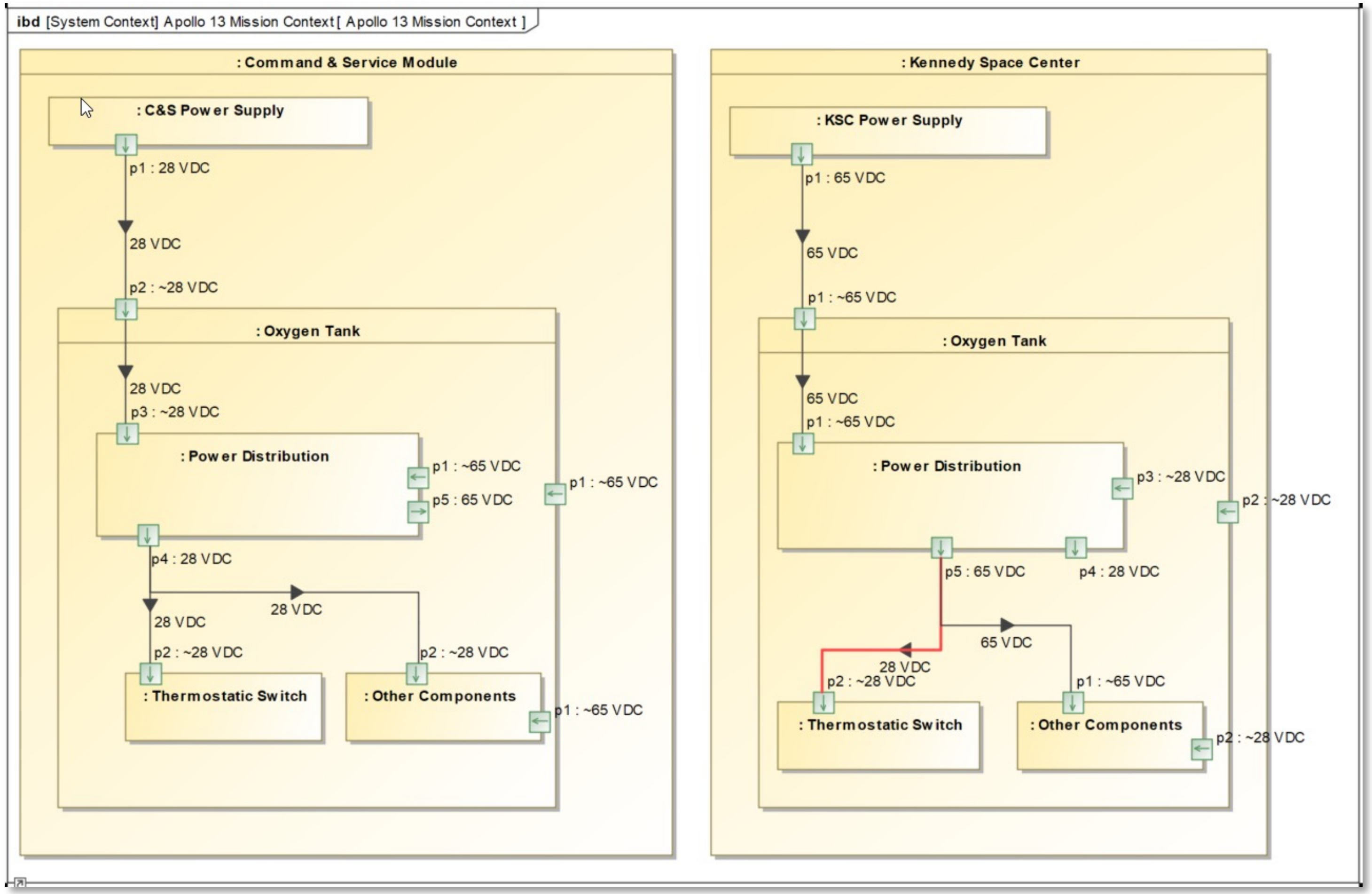
- Apollo XIII – seventh crewed mission in the Apollo space program and third meant to land on the Moon
- What went wrong?
  - An oxygen tank exploded, endangering the crew, and causing the moon landing to be aborted
  - The oxygen tanks were originally designed for 28 volt DC power, and redesigned to also support 65 volt DC power for the ground station. The heater thermostatic switches were **overlooked** and not upgraded.


Britannica.com

Wikipedia.com

- How MBSE would have helped?
  - A SysML model would have allowed for **pre-integration** of the oxygen tank with both the Command & Service Model (28 volt DC) as well as the Kennedy Space Center (65 volt DC)

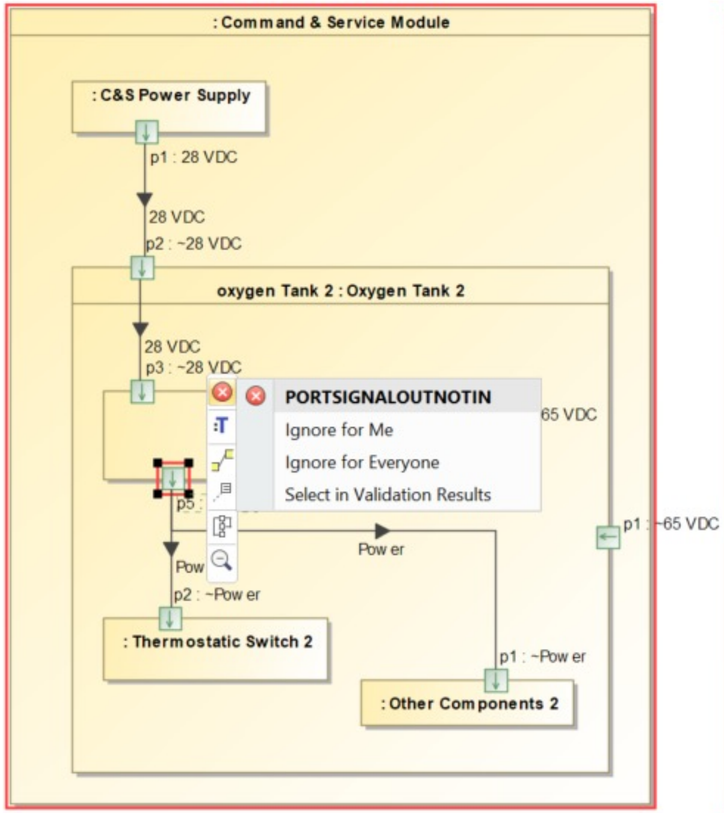
Apollo XIII – MBSE Scenario 1

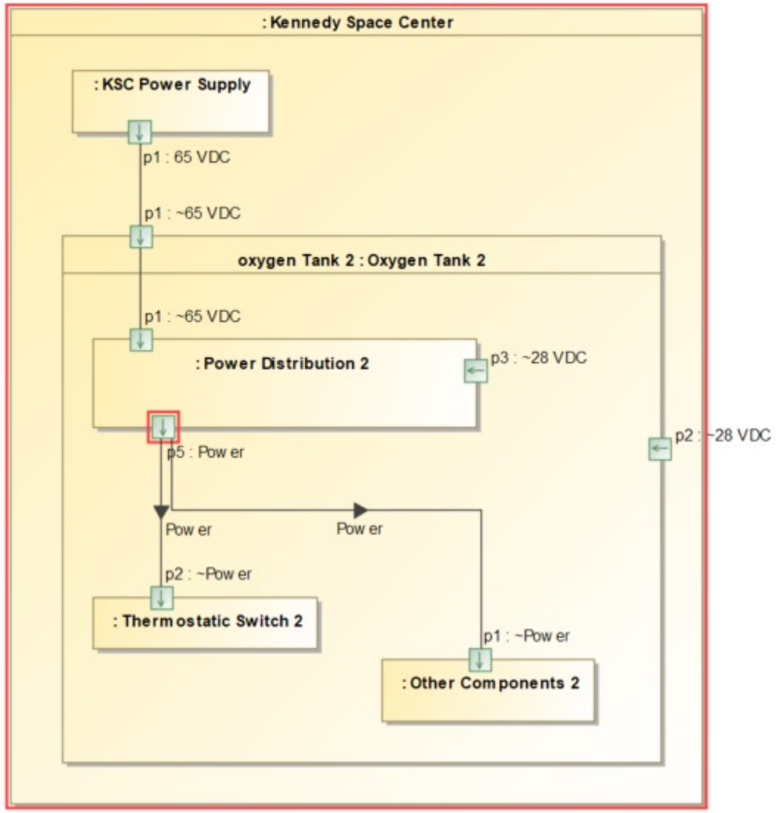


- In the case where the model specifies the voltage
  - As a pre-existing component, the oxygen tank block accepts 28 volts DC.
  - As the 65 volts DC adaptation is designed, it is **immediately** apparent that there is a power mismatch with the Thermostatic Switch
  - Cameo's inherent validation flags the error as soon as the connector is creator.

The model highlights the design defect early in the systems engineering process

Apollo XIII – MBSE Scenario 2





- In the case where the model only specifies "power" as the port type
  - In both cases shown, the specific voltage is shown as an input, however the owning block has no operation to convert it to a "Power" signal
  - This results in a **SAIC Validation Suite** error forcing engineers to include the power conversion in the design
  - This specific defect is extremely difficult to catch without validation

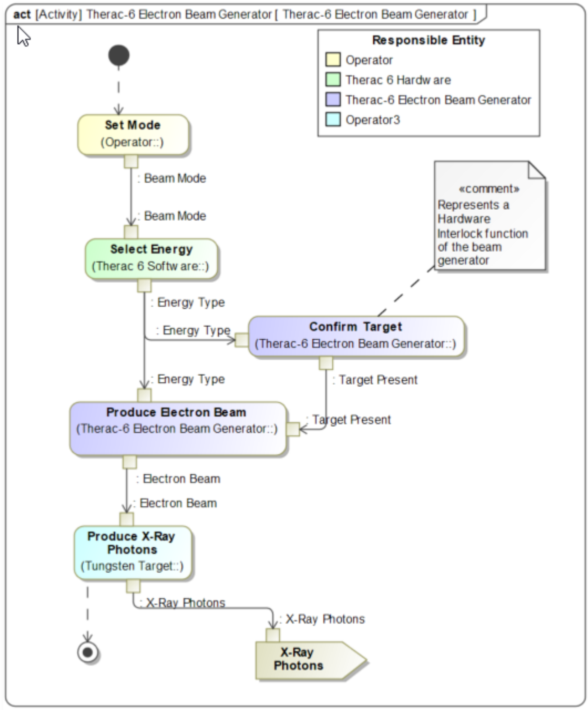
SAIC's Validation Suite provides additional model syntax checks to find defects early

Case Study 2: Therac-25

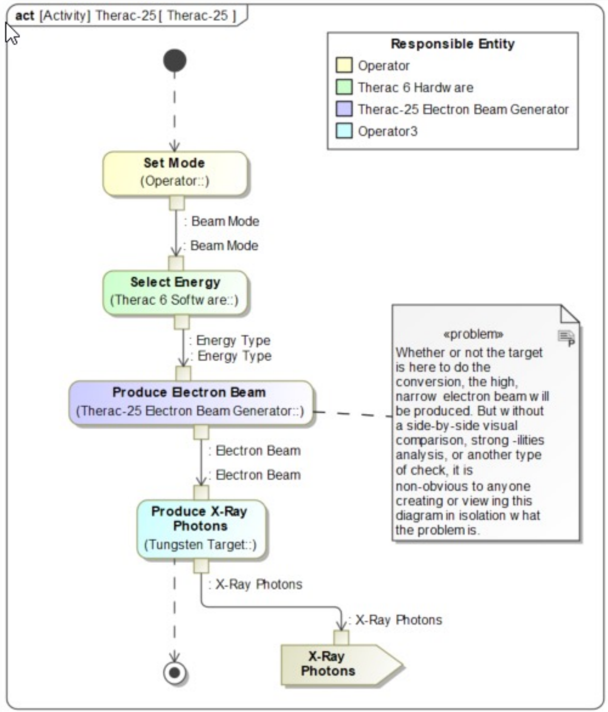
- Therac-25 – a computer-controlled radiation therapy system
- What went wrong?
  - At least six times patients were given **massive overdoses of radiation**
  - Developers opted not to duplicate the existing hardware safety interlocks from previous system incarnations, and instead to leverage software
  - Two software faults were to blame. When the operator incorrectly selected x-ray mode before quickly switching to electron model, the system allowed the beam to be set without the tungsten target being in place irradiating the patient
- How MBSE would have helped?
  - Modeling the functional architecture may have allowed developers to realize missing functionality when compared to previous system models
  - Mapping system functionality to requirements (based on previous system specifications) would have detected the defect

pvs-studio.com

Therac-25 - MBSE

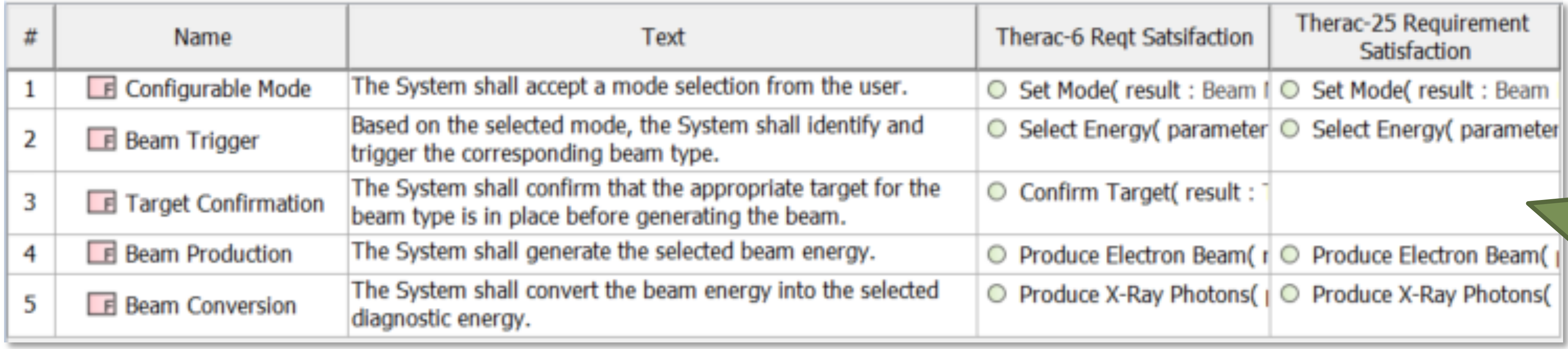


«comment»
Represents a Hardware Interlock function of the beam generator



«problem»
Whether or not the target is here to do the conversion, the high, narrow electron beam will be produced. But without a side-by-side visual comparison, strong -ilities analysis, or another type of check, it is non-obvious to anyone creating or viewing this diagram in isolation what the problem is.

- Without a side-by-side comparison of the modeled functional architectures for Therac-25 and previous versions of the system, it is not likely the defect would have been detected
- Creating SysML "satisfy" relationship between the functional safety requirements and the Therac-25 operations would have
  - Clearly appeared as a gap in a metachain based table
  - Thrown an **SAIC Validation Suite** error



#	Name	Text	Therac-6 Reqt Satsifaction	Therac-25 Requirement Satisfaction
1	Configurable Mode	The System shall accept a mode selection from the user.	○ Set Mode(result : Beam I	○ Set Mode(result : Beam
2	Beam Trigger	Based on the selected mode, the System shall identify and trigger the corresponding beam type.	○ Select Energy(parameter	○ Select Energy(parameter
3	Target Confirmation	The System shall confirm that the appropriate target for the beam type is in place before generating the beam.	○ Confirm Target(result :	
4	Beam Production	The System shall generate the selected beam energy.	○ Produce Electron Beam(r	○ Produce Electron Beam(
5	Beam Conversion	The System shall convert the beam energy into the selected diagnostic energy.	○ Produce X-Ray Photons(	○ Produce X-Ray Photons(

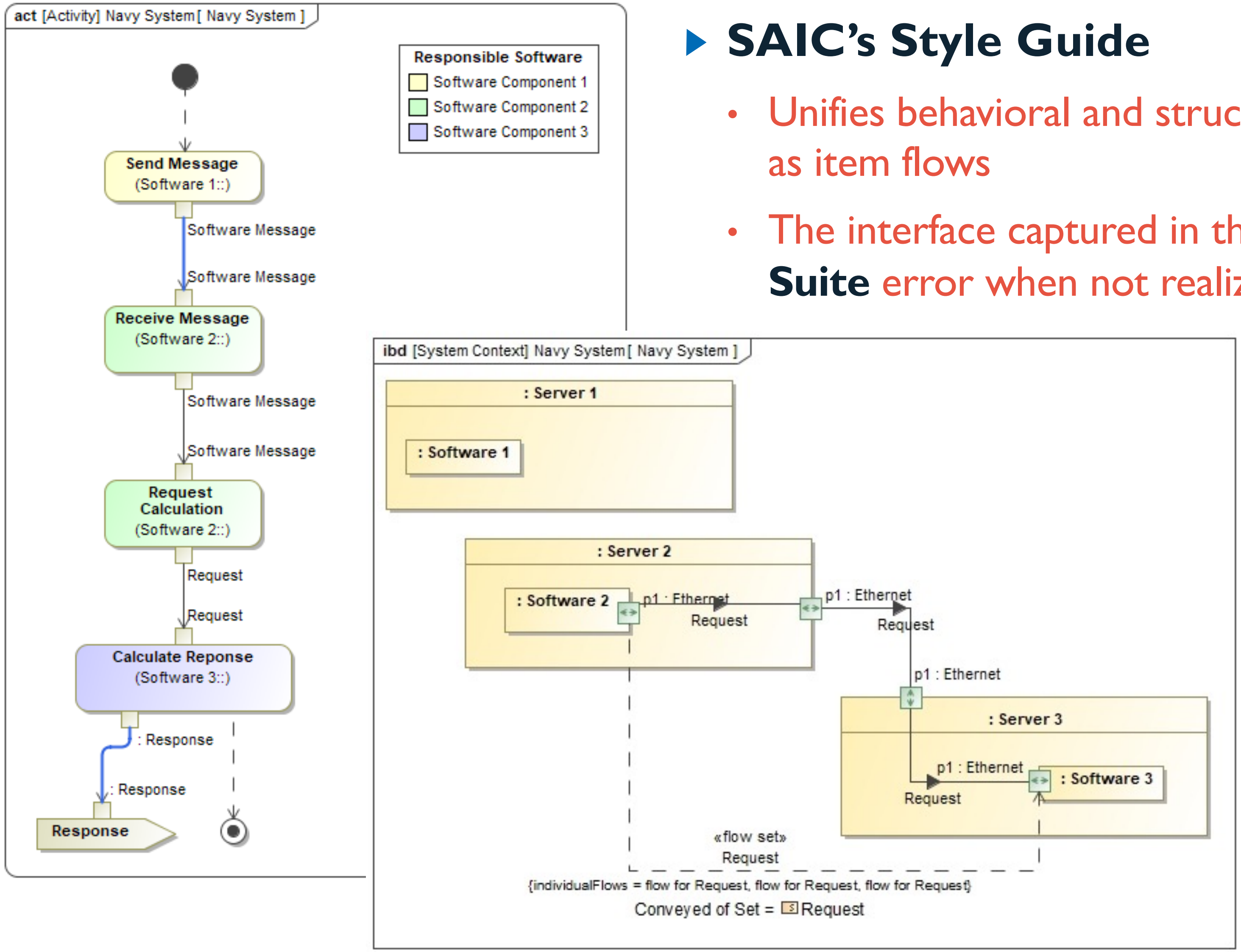
Unsatisfied requirements throw validation errors, detecting the missing safety function

Case Study 3: Naval System

- New systems development effort to support naval operations, leveraging MBSE from the onset
  - Anonymized to protect the innocent
  - Multiple teams building models with Systems Engineering responsible for model integration
- What went wrong?
  - The MBSE approach managed to catch a missing interface!
  - Unfortunately, an MBSE 1.0 styled approach was used in which diagrams from the model were **printed** and visually compared (with a highlighter) to find the error

- How MBSE would have helped?
  - An MBSE 2.0 approach would have identified the missing interfaces via automated validation
  - The program would have saved countless man hours of tedious effort to identify and correct the defects

Naval System – MBSE 2.0



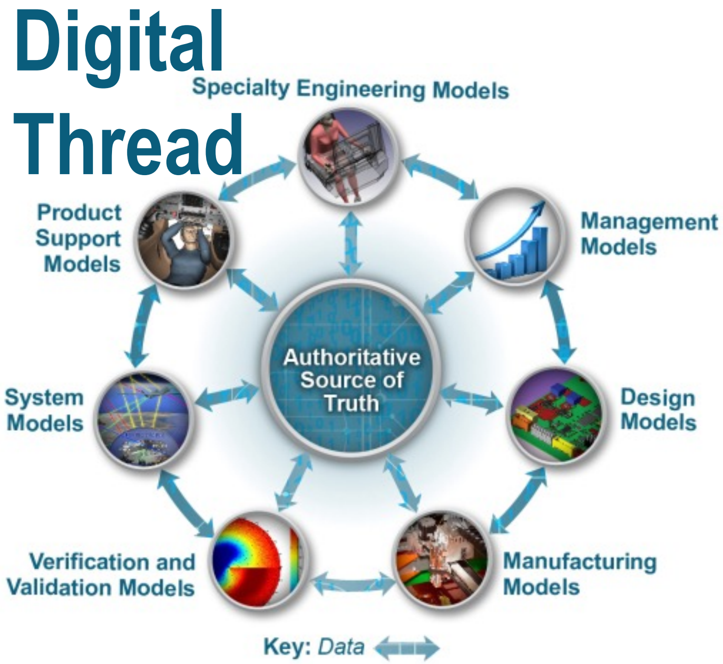
SAIC's Style Guide

- Unifies behavioral and structural content in part by realizing object flows as item flows
- The interface captured in the activity diagram causes an **SAIC Validation Suite** error when not realized by an item flow

- The "Software Message" is missing from the IBD and so throws an error
- The "Request" is consistent across behavioral and structural views and so passes validation

Data-centric modeling allows for cross checking across the design

Conclusions



- MBSE is about the data and the relationships between data
- Well structured SysML models can be used to detect defects early in development and prevent costly corrective maintenance and operational consequences down the line
- Cameo provides a wide variety of tools to support architecture/design analysis beyond basic SysML diagrams
- Checkbox modeling, exclusively to satisfy a Statement Of Work (SOW), is a missed opportunity to apply engineering rigor and support long term efforts such as Digital Thread and Digital Twin

SysML models leveraging automated validation can help your organization make the jump to MBSE 2.0

Questions

- Heidi Jugovic
  - Heidi.J.Jugovic@saic.com
- Chris Swickline
  - Chris.R.Swickline@saic.com
- SAIC Validation Suite
  - https://www.saic.com/digital-engineering-validation-tool

33rd Annual **INCOSE**
international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS