A-P-T RESEARCH, INC.
AN EMPLOYEE-OWNED COMPANY

MODEL BASED MISSION ASSURANCE

Fayssal M. Safie, PhD, A-P-T Research, Inc., Huntsville, Alabama
RAM XII , Nov 13-14, 2019

AGENDA

- Objective
- Systems Engineering
- Model Based Systems Engineering (MBSE)?
- Model Based Mission Assurance (MBMA)
- System Modeling Language (SYSML) Examples
- MBSE and MBMA - The Integrated Picture
- MBSE/MBMA Anticipated Benefits
- Summary and Conclusions
- Bibliography

OBJECTIVE

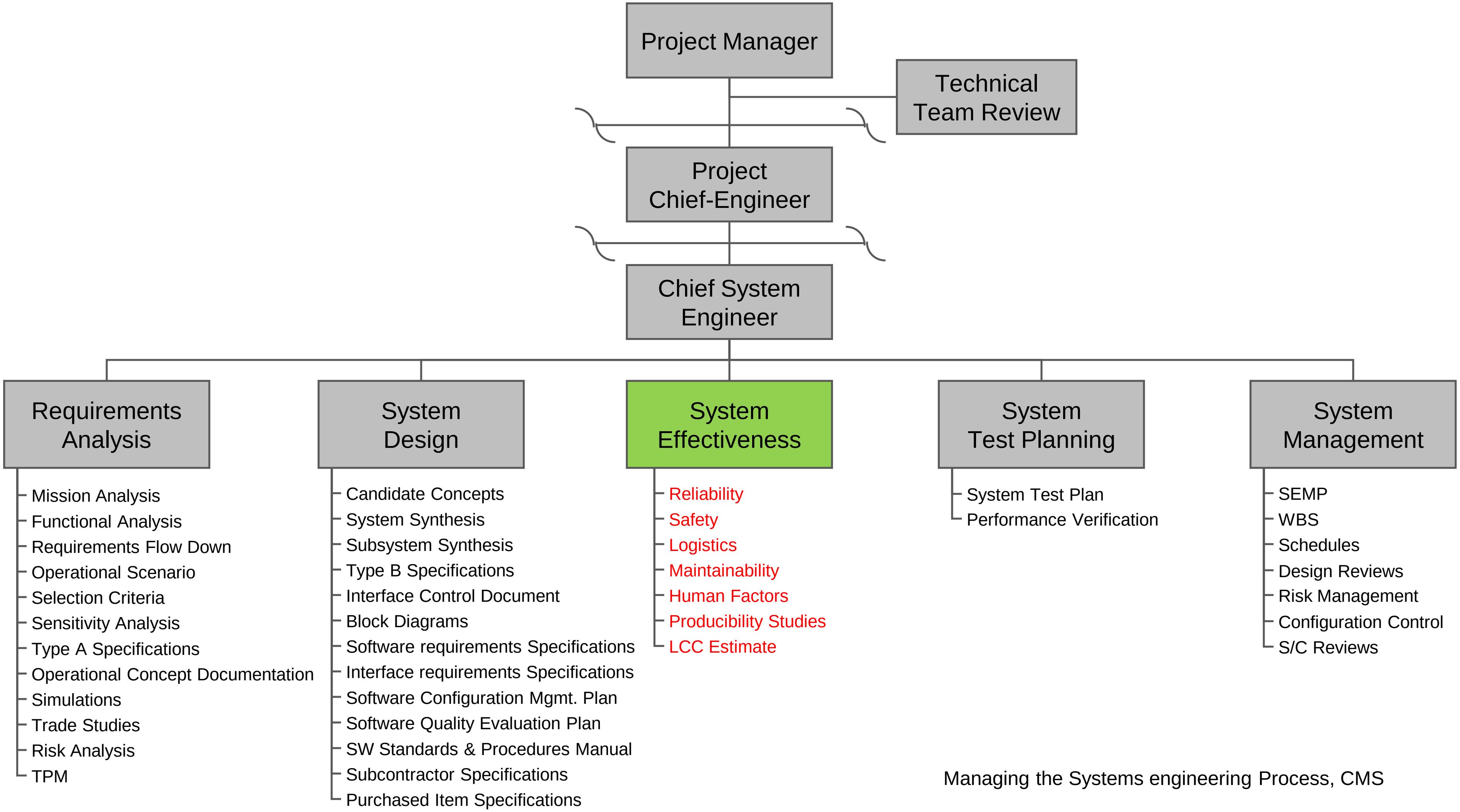
This presentation is intended to discuss the Model Based Mission Assurance (MBMA) concept in a Model Based Systems Engineering (MBSE) environment. It discusses what safety and mission assurance organizations need to do to participate and integrate in the MBSE environment (i.e. new skills, new role, training, requirements, etc..).

Note: It is important to acknowledge the significant contribution of Dr. John Evans of NASA/OSMA his contribution to the MBMA material used in this presentation.

SYSTEMS ENGINEERING

- **A system** is an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.
- **Systems Engineering** is an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient, and schedule compliant manner throughout a system's entire life cycle.

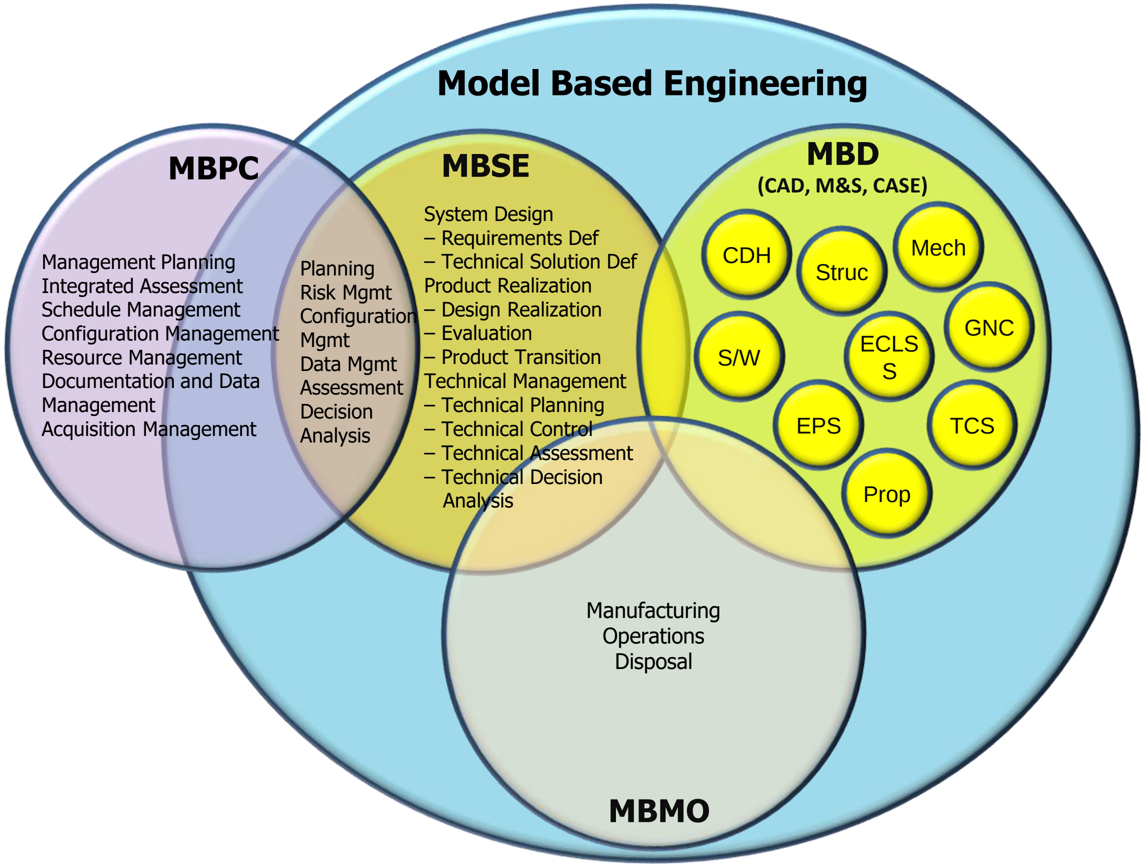
TYPICAL PROJECT SYSTEMS ENGINEERING ORGANIZATION



MODEL BASED SYSTEMS ENGINEERING (MBSE)?

- MBSE is a formalized application of modeling to support system requirements, design, analysis, technical management, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.
- MBSE is an environment that can be characterized as the collection of related processes, methods, and tools used to support the discipline of systems engineering in a “model-based” or “model-driven” context.
- MBSE is part of a long-term trend toward model-centric approaches. In particular, MBSE is expected to replace the document-centric approach that has been practiced by systems engineers in the past.
- Although it holds considerable promise for freeing systems engineering from the present document-centric environment, MBSE still has a long way to go before it is universally accepted and implemented.
- The International Council on Systems Engineering [INCOSE] vision for the future development of MBSE predicts that MBSE will be widely used throughout both academia and industry by the year 2025.

MODEL BASED CONCEPTS



MBSE (Model Based Systems Engineering) – A formalized application of modeling to support system requirements, design, analysis, *technical management*, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.

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

MBD (Model Based Design) – Mathematical and visual method of addressing problems associated with designing complex control signal processing and communication systems.

MBPC (Model Based Project Control) – A formalized application of modeling to support schedule, budget, organizational activities related to the system(s) of interest.

MBMO (Model Based Manufacturing and Operations) – A formalized application of modeling to support manufacturing and operations.

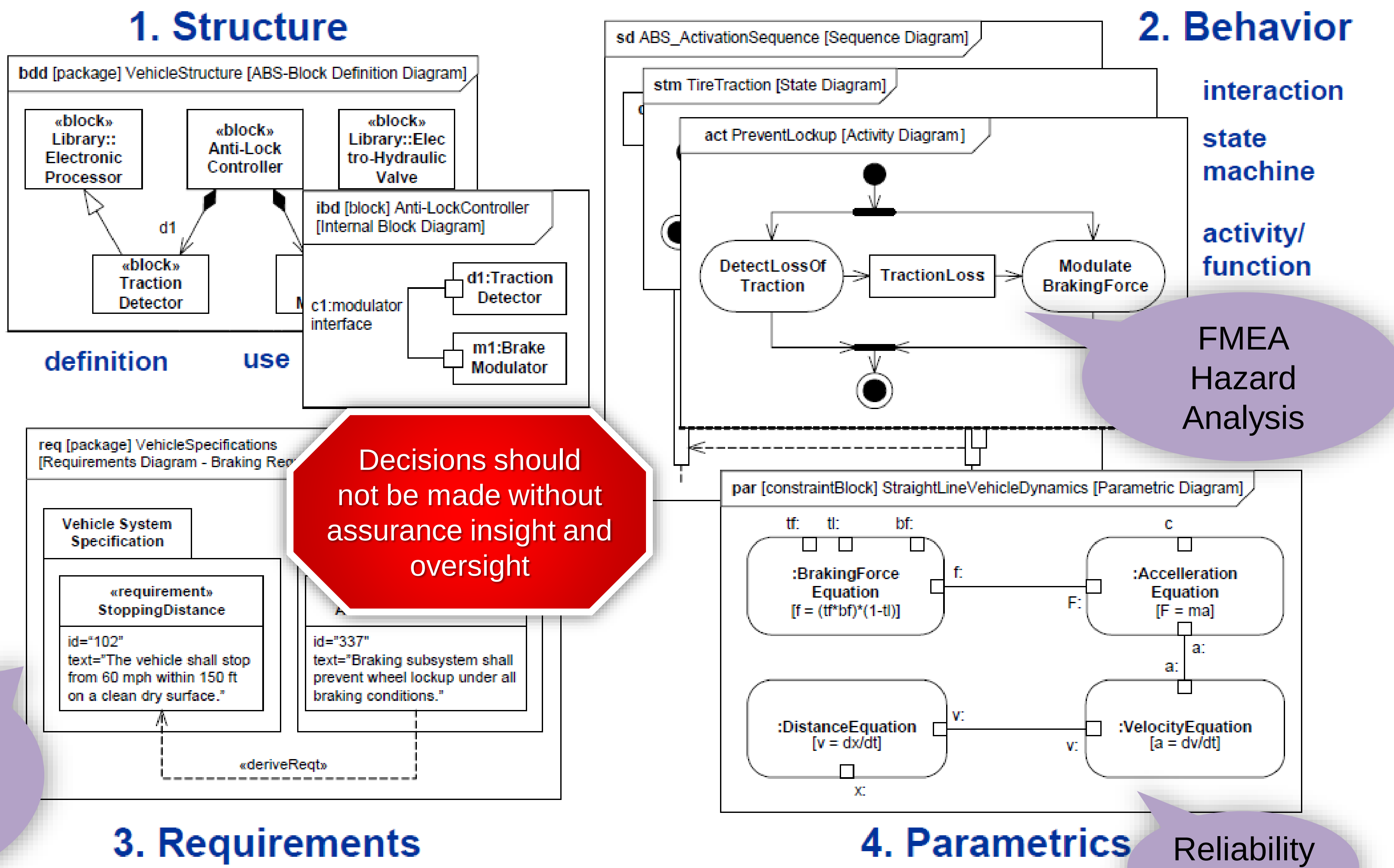
MODEL BASED MISSION ASSURANCE (MBMA)

- In MBSE, a virtual model of the system is created, typically while it is still in the designing and planning phase. The model is used as a singular reference source — a "single point of truth" — for system concept, requirements and design, and verification and validation and associated data.
- Safety and Mission Assurance (SMA) can leverage that model to perform a variety of assurance analyses earlier in the life cycle reducing the occurrence of costly changes after the system design hardens.
- We are calling the corresponding approach to mission assurance “Model-Based Mission Assurance (MBMA)”.

https://sma.nasa.gov/sma-disciplines/model-based-mission-assurance

SYSTEMS MODELING LANGUAGE (SYSML)- ABS EXAMPLE

- SysML sponsored by INCOSE/OMG with broad industry and vendor participation and adopted in 2006
- SysML provides a general purpose modeling language to support specification, analysis, design and verification of complex systems
- It allows linking different types of models that come from different engineering disciplines.
- 4 Pillars of SysML include modeling of requirements, behavior, structure, and parametrics



Safety Requirements and Quality Demands

Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA
Used with permission of OMG

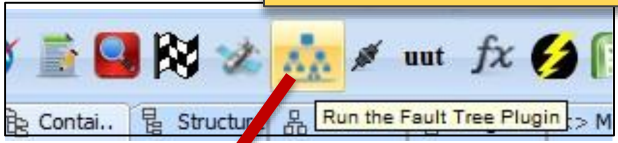
MODEL BASED MISSION ASSURANCE (MBMA)

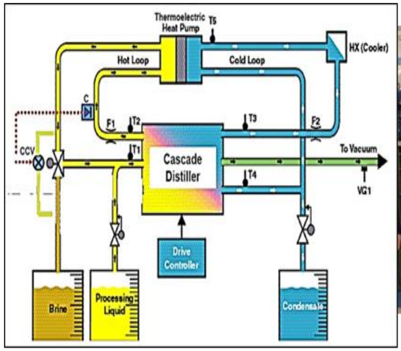
- Structure: Represents structural elements called blocks, and their composition and classification. Blocks provides a unifying concept for describing the structure of an entity: System, Hardware, Software, Facility, etc.
- Behavior: Activity diagrams represents behavior in terms of the ordering of actions based on the availability of inputs, outputs, and control, and how the actions transform the inputs to outputs. Machine diagrams represents behavior of an entity in terms of its transitions between states triggered by events. Sequence diagrams represents behavior in terms of a sequence of messages exchanged between parts.
- Parametrics: Parametric diagrams capture the analysis as a network of equations. They represents constraints on property values, such as F=m*a, used to support engineering analysis. They help in managing technical performance measures and ensuring consistency between the system design model and multiple engineering analysis models.
- Requirements: Requirement diagram represents text-based requirements and their relationship with other requirements, design elements, and test cases to support requirements traceability

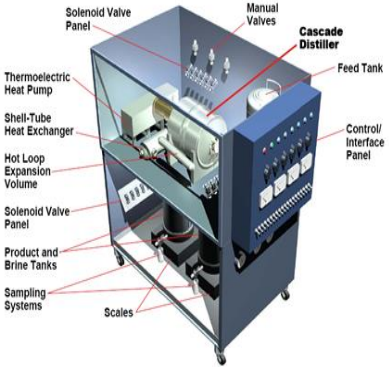
A FAULT TREE ANALYSIS EXAMPLE

Magic Draw introduces several customization engines

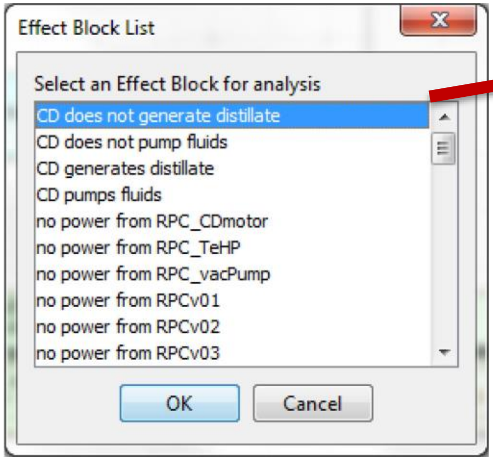
Magic Draw Plug-Ins



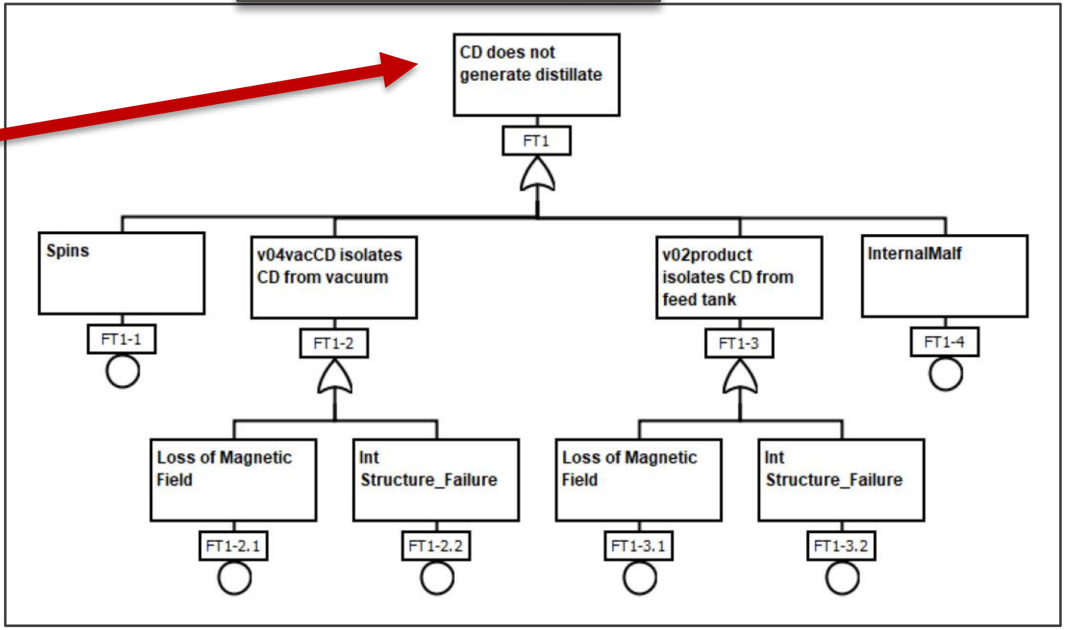




Select Top Level Event from Model to Analyze



Generated Fault Tree For the Cascade Distiller (CD)

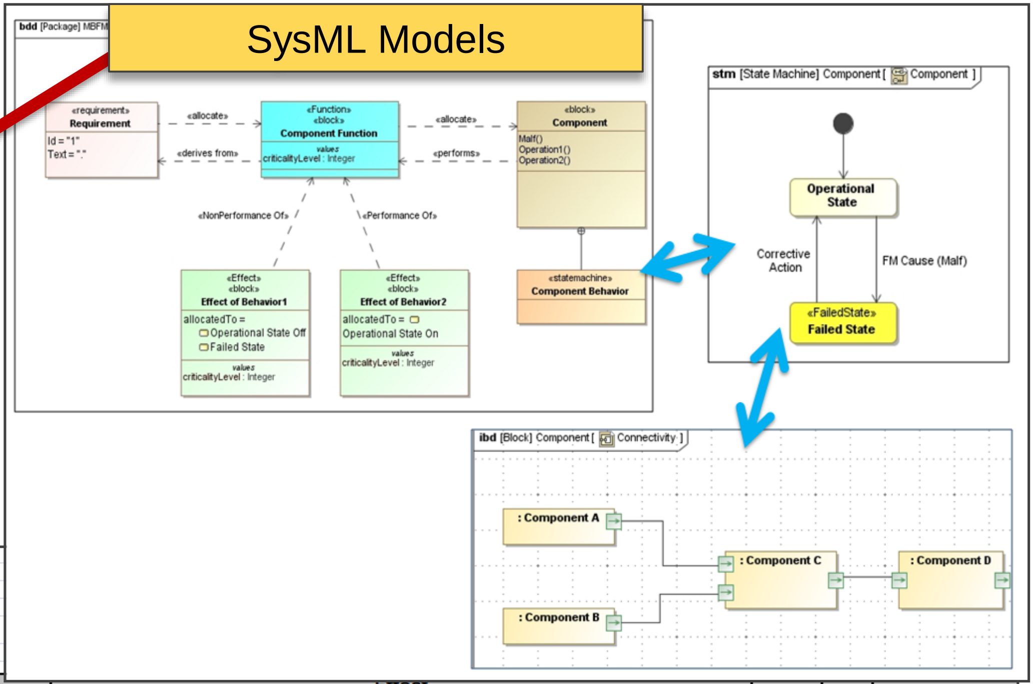


Courtesy Lui Wang
Johnson Space Center

A FMECA EXAMPLE

Courtesy Lui Wang
Johnson Space Center

Magic Draw introduces several customization engines



Magic Draw Plug-Ins

FMECA Output

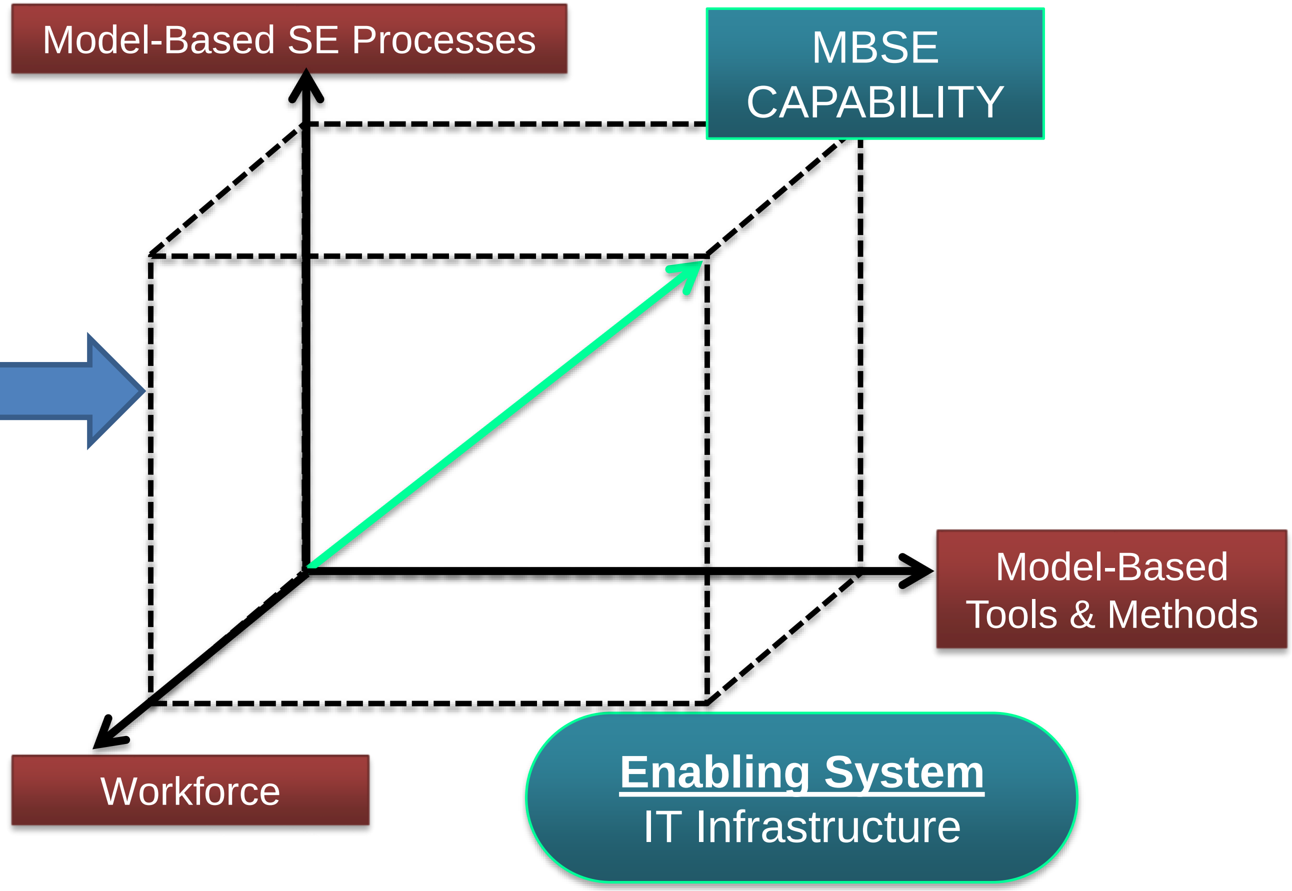
Failure Modes and Effects Criticality Analysis (FMECA)

Project Name: Fan in the Can SysML Model

System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect: Immediate Failure Effect	Effect: End Effect	Effect: Number of Independent	Effect: Other Independent Failures	CRIT LEVEL	SEV	Potential Causes
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Ciruculates Air	Failed Off	Loss of CCAA1 air Circultation	Loss of CCAA1 air Circultation	1		1		Internal Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu1_output_power	Loss of CCAA1 air Circultation	2	MBSU2 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	MBSU1_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU1_loads						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu2_output_power	Loss of CCAA1 air Circultation	2	MBSU1 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	MBSU2_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU2_loads						insertInternal2Malf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed Off	Loss_of_PDU_output_power	Loss of CCAA1 air Circultation	1		1		insertInternalMalf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed On	PDU_Output_Power_On						insertInternal2Malf

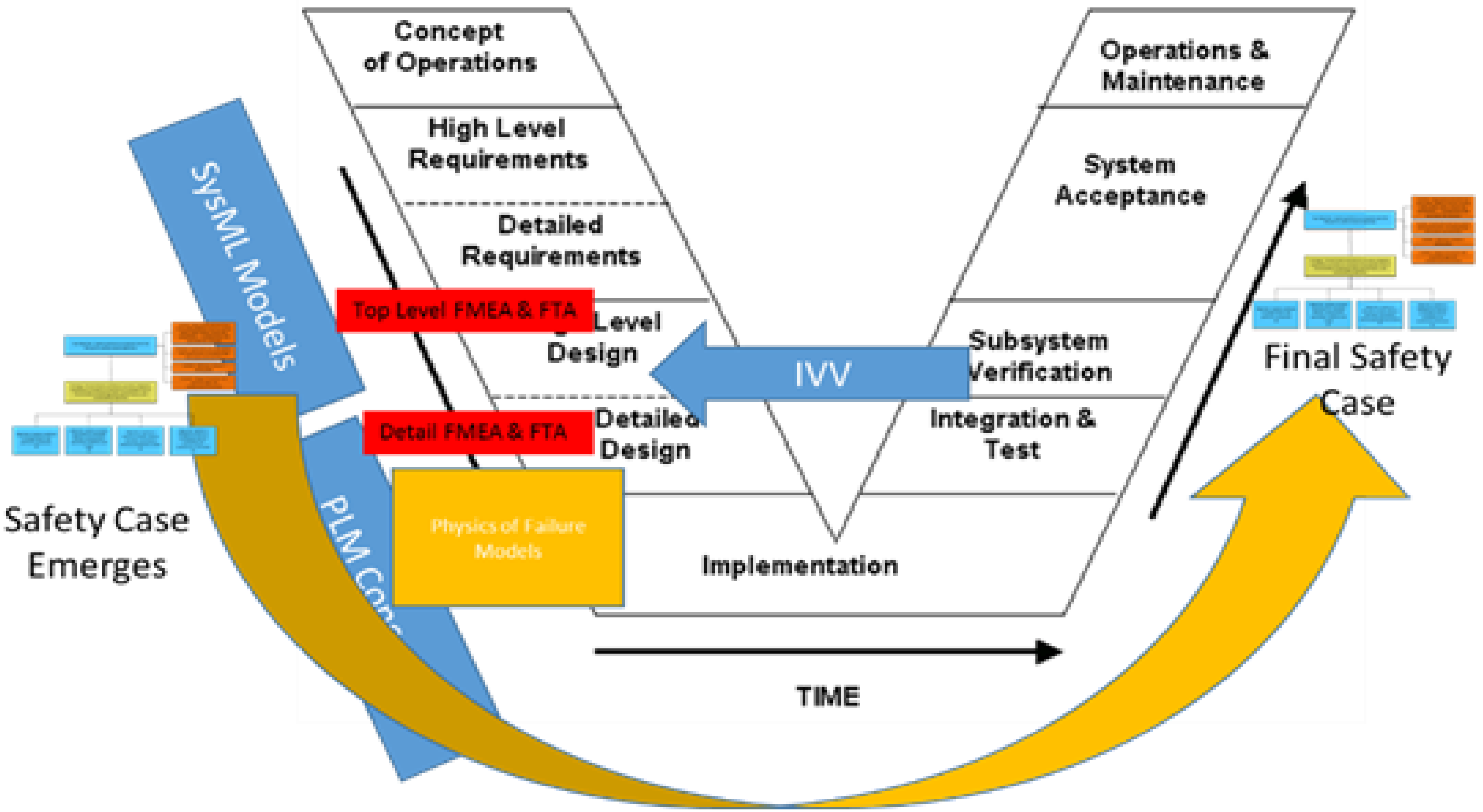
SAFETY AND MISSION ASSURANCE – THE CHANGE

Assurance organizations may need to modify their standards and requirements (e.g. safety case, objective driven requirement), define new roles, develop new skills, and train on new tools to engage in the Model Based Systems Engineering environment



Joe Hale/Fayssal M. Safie, MSFC/QD01 presentation 4/7/16

MBMA IN MBSE ENVIRONMENT



https://sma.nasa.gov/sma-disciplines/model-based-mission-assurance

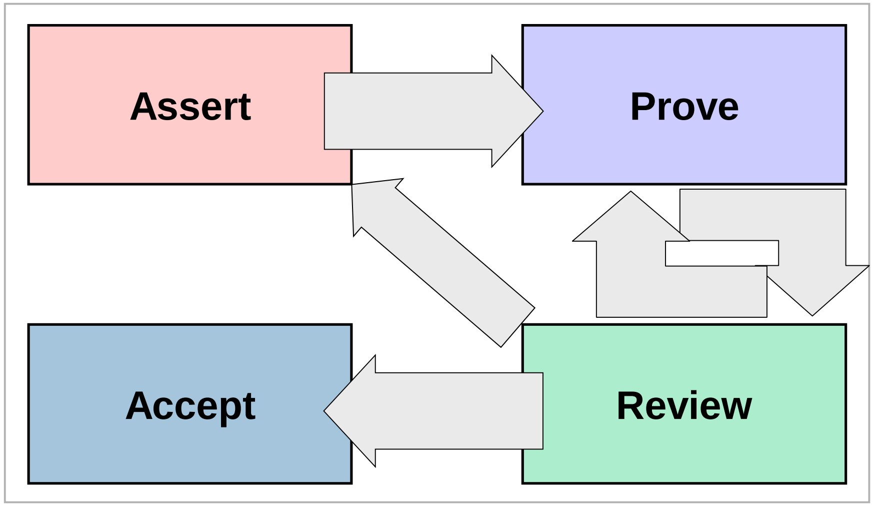
THE SAFETY CASE

A safety case is a documented body of evidence that provides a convincing and valid argument that the system is safe. It Involves:

- Making an explicit set of claims about the system(s)
  - E.g., probability of accident is low
- Producing supporting evidence
  - E.g., operating history, redundancy in design
- Providing a set of safety arguments that link claims to evidence

THE SAFETY CASE PROCESS

- Assert the case: This system is safe because it meets the following: (List requirements or claims which, if met, demonstrate the case that the system is adequately safe)
- Prove: Validate by demonstrations, tests, or analysis that each claim is met.
- Review: Independent reviewers examine the logical, legal, and scientific basis on which the validation is based. They then develop findings as to the adequacy of the validation.
- Accept: A properly designated decision authority then reviews the case, proofs, and finding of the reviewers, and makes an informed decision for acceptance of the risk or rejection.



Reference: APT safety course

R&M OBJECTIVES HIERARCHY – TOP LEVEL

"…NASA OSMA has developed an approach…to provide for flexibility … while focusing on a vision that is rooted in technical objectives rather than specifying specific products and processes. This approach uses the development of *objectives hierarchies with supporting strategies for implementation.* *The results promise the potential of improved effectiveness, flexibility, and* ***compatibility with Model Based Systems Engineering (MBSE)****…"*

Top Objective: System performs as required over the lifecycle to satisfy mission objectives

Context: Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, …, considerations and associated risk tolerance

Context: System/function description and requirements, including design information and interfaces

Context: Reference mission + before/after

Context: Range of nominal / off-nominal usage and conditions/environments

Strategy: Prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives

Objective: System conforms to design intent and performs as planned (1)

Objective: System remains functional for intended lifetime, environment, operating conditions and usage (2)

Objective: System is tolerant to faults, failures and other anomalous internal and external events (3)

Objective: System is designed to have an acceptable level of availability and maintenance demands (4)

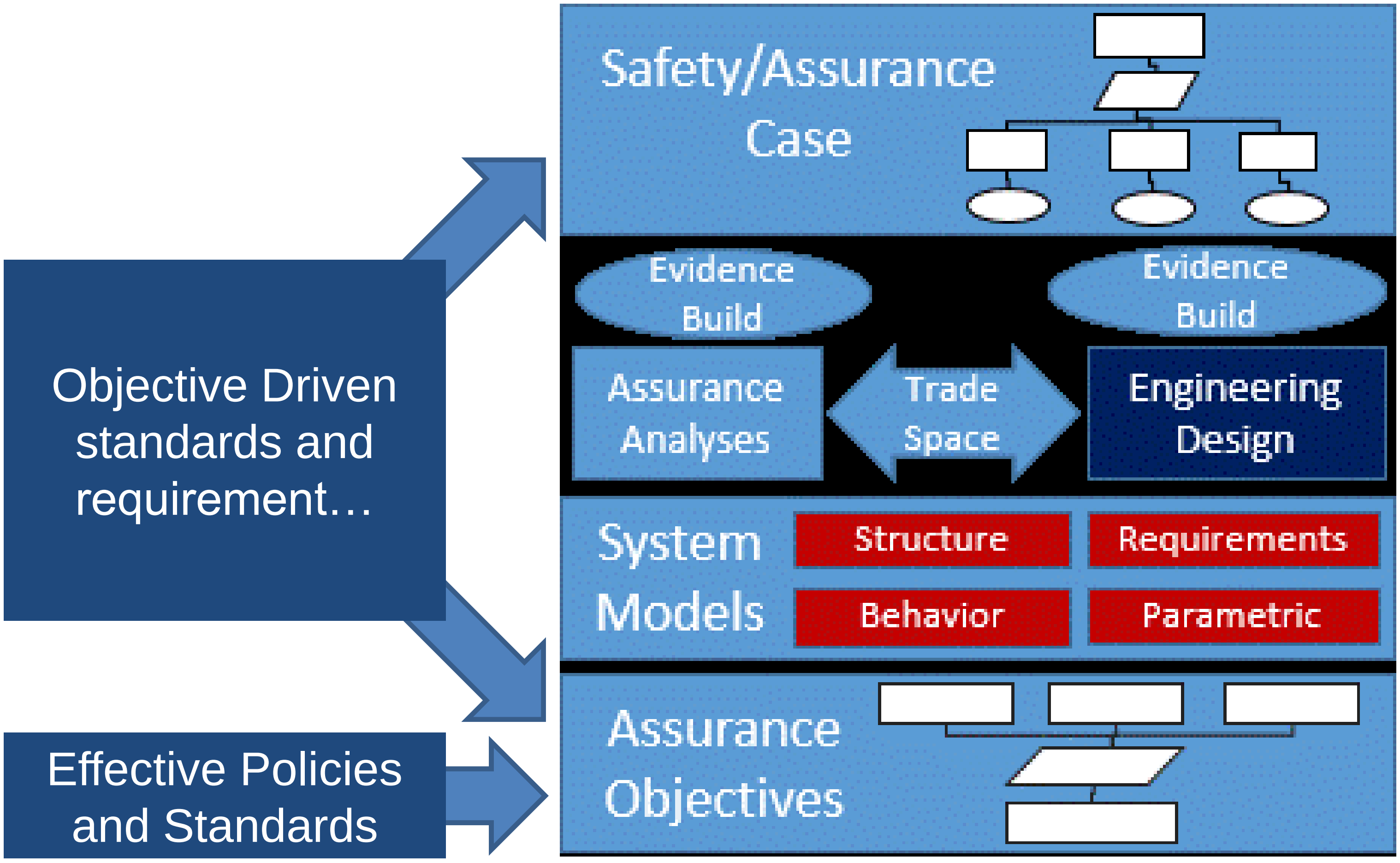
https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4

R&M OBJECTIVES HIERARCHY (CONTINUED)
SUB – OBJ. 2

- Objective: System remains functional for intended lifetime, environment, operating conditions and usage (2)
  - Context: Description of operating environment, including static, cyclical, and randomly varying loads
  - Strategy: Understand failure mechanisms, eliminate and/or control failure causes, degradation and common cause failures, and limit failure propagation to reduce likelihood of failure to an acceptable level (2.A)
    - Objective: system and its elements are designed to withstand nominal and extreme loads and stresses (radiation, temperature, pressure, mechanical, …) for the life of the mission (2.A.1)
      - Strategy: Apply design standards to incorporate margin to account for variable and unknown stresses (2.A.1.A)
      - Strategy: Evaluate and control nominal stresses and related failure causes (2.A.1.B)
      - Strategy: Evaluate and control potential for extreme stresses and related failure causes (2.A.1.C)
      - Strategy: Perform qualification testing and life demonstration to verify design for intended use (2.A.1.D)
    - Objective: System or its elements are not susceptible to common-cause failures (2.A.2)
      - Strategy: Evaluate and control coupling factors and shared causes between redundant (or dependent) components (2.A.2.A)
  - Strategy: Assess quantitative reliability measures and recommend or support changes to system design and/or operations (2.B)
    - Objective: System and its components meet quantitative reliability criteria (2.B.1)
      - Strategy: Determine reliability allocation (2.B.1.A)
      - Strategy: Estimate reliability based on applicable performance data, historical data of similar systems, and/or physics-based modeling (2.B.1.B)
      - Strategy: Support design trades based on reliability analysis (2.B.1.C)
      - Strategy: Plan and perform life testing (2.B.1.D)
      - Strategy: Track and monitor reliability performance over time (2.B.1.E)

https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4

MBSE AND MBMA - THE INTEGRATED PICTURE



Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA

MBSE/MBMA ANTICIPATED MAJOR BENEFITS

MBSE/MBMA Major Benefits

- Information consistency: reduced overhead, increased confidence
- No “where’s the latest” confusion
- Propagation of changes
- Changes tracked and versioned
- Ease of communicating and maintaining current project baseline
- Cross-training/experience for earlier-career engineers
- Enhanced stakeholder communication to enable better elicitation and validation
- Enhanced visibility into information gaps and system design integrity
- Rigorous traceability from need through solution
- Reduction in the number of requirements
- Early/on-going requirements validation and design verification

SUMMARY & CONCLUSION

- MBSE can provide the frame of work to support Model Based Mission Assurance activities.
- Mission Assurance Community must get engaged and integrate with the MBSE communities.
- Assurance organizations may need to define new roles, develop new skills, and their products may need to be different in a model-based environment.

BIBLIOGRAPHY

- Goddard Space Flight Center (GSFC) MBSE Workshop, February 17-18, 2016, (https://drive.google.com/open?id=0Bw3ikr90G7CVR01Wd0hTWjN5NjA)
- NASA Jet Propulsion Laboratory (JPL) Symposium and workshop on MBSE, January 28-30, 2015, (see Link 2 Below). https://drive.google.com/drive/folders/0B3hsmXWocH2JZVpTSzdzaUxYQzA
- Reliability and Maintainability Objective Driven Hierarchy (NASA, OSMA).
  - (https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4)
- Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA,
- MBSE presentation to MSFC S&MA, Joe Hale/Fayssal Safie, April 27, 2016
- Model Based Mission Assurance in a Model Based Systems Engineering (MBSE) Framework, Steve Cornford and Martin Feather, NASA/CR—2016–219272

A-P-T RESEARCH, INC.
AN EMPLOYEE-OWNED COMPANY

BACKUPS

COMPARISON OF EXISTING ANSI/GEIA-STD-0010, MIL-STD-882 TECHNIQUES AND THE SAFETY CASE

MIL-STD-882

1. Documentation of the system safety approach
2. Identification of hazards
3. Assessment of mishap risk
4. Identification of mishap risk mitigation measures
5. Reduction of mishap risk to an acceptable level
6. Verification of mishap reduction
7. Review and acceptance of residual mishap risk by the appropriate authority
8. Tracking hazards and residual mishap risk

ANSI/GEIA-STD-0010

1. Program Initiation
2. Hazard **I**dentification and Tracking
3. Risk **A**ssessment
4. Risk **R**eduction
5. Risk **A**cceptance

I-A-R-A

The eight program elements outlined in MIL-STD-882D and earlier versions were combined and simplified into five, to provide a more concise representation of current consensus practices.

Safety Case Approach

* 0. Articulate arguments (rationale & claims) to be used in safety case

1. Develop program to provide supporting evidence and independent review
2. Provide supporting evidence **(I – A – R)**

* 3. Independently review, verify and validate

4. Review for acceptance **(– A)**

* Feature not currently in Best Practices

Reference: APT Safety Case