A-P-T RESEARCH, INC.

MODEL BASED MISSION ASSURANCE (MBMA)

Dr. Fayssal M. Safie/APT-Research
Dr. John Evans/OSMA, NASA HQ

Model Based Systems Engineering
& Software System Safety Workshop
May 2-3, 2017

AGENDA

- Objective
- Definitions
- Why Model Based Systems Engineering (MBSE)
- Model Based Mission Assurance (MBMA)
- MBMA Case Studies
- Summary and conclusions
- References

OBJECTIVE

- This presentation is intended to discuss the MBMA concept in a MBSE environment. It addresses what safety and mission assurance organizations need to do to participate and integrate in the MBSE environment (i.e. new skills, new role, training, etc..). Examples are also discussed.

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.

Definitions

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.

Definitions

What Is Model Based Systems Engineering (MBSE)?

- **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.
- More Specifically, 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.

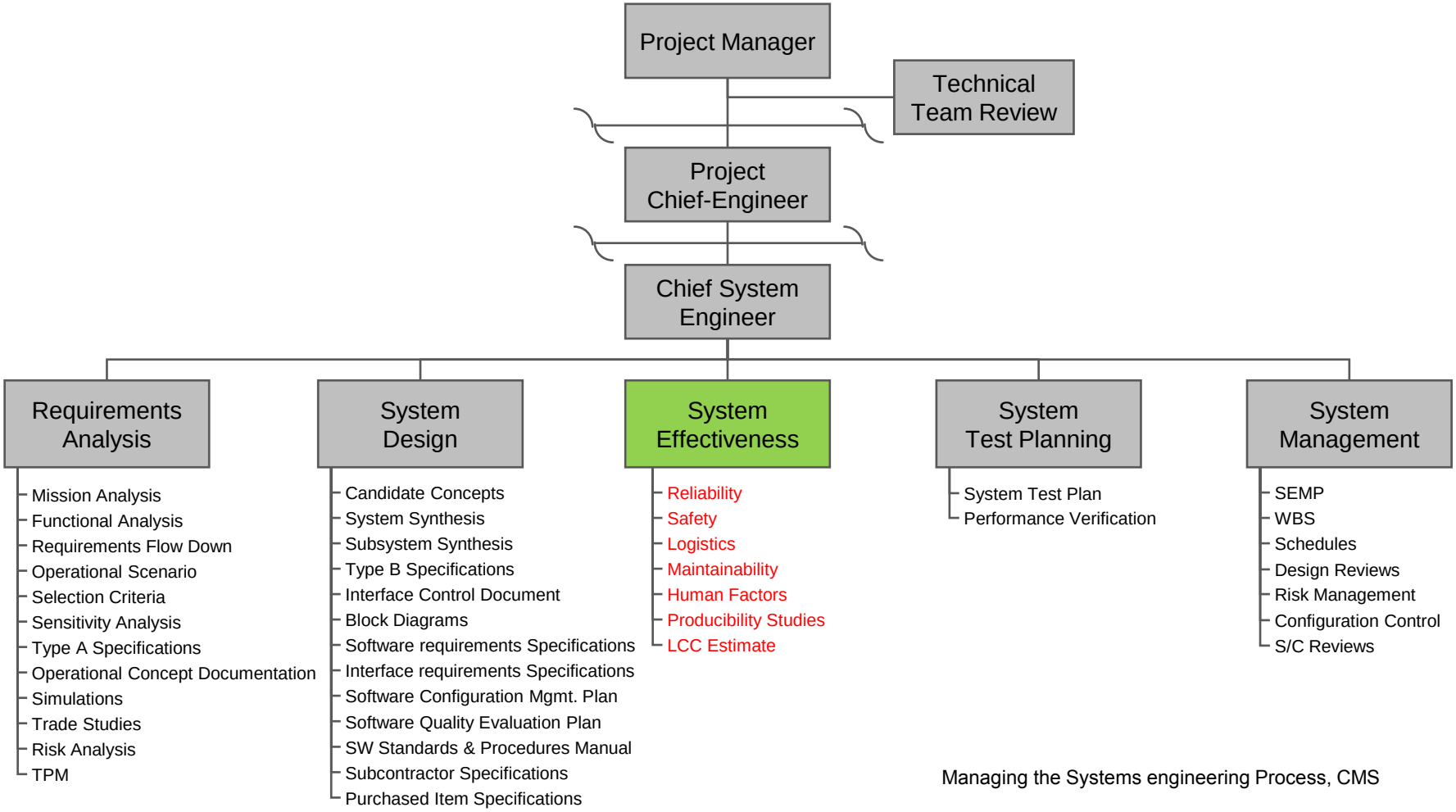
Why MBSE?

MBSE Anticipated 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

Model Based Mission Assurance

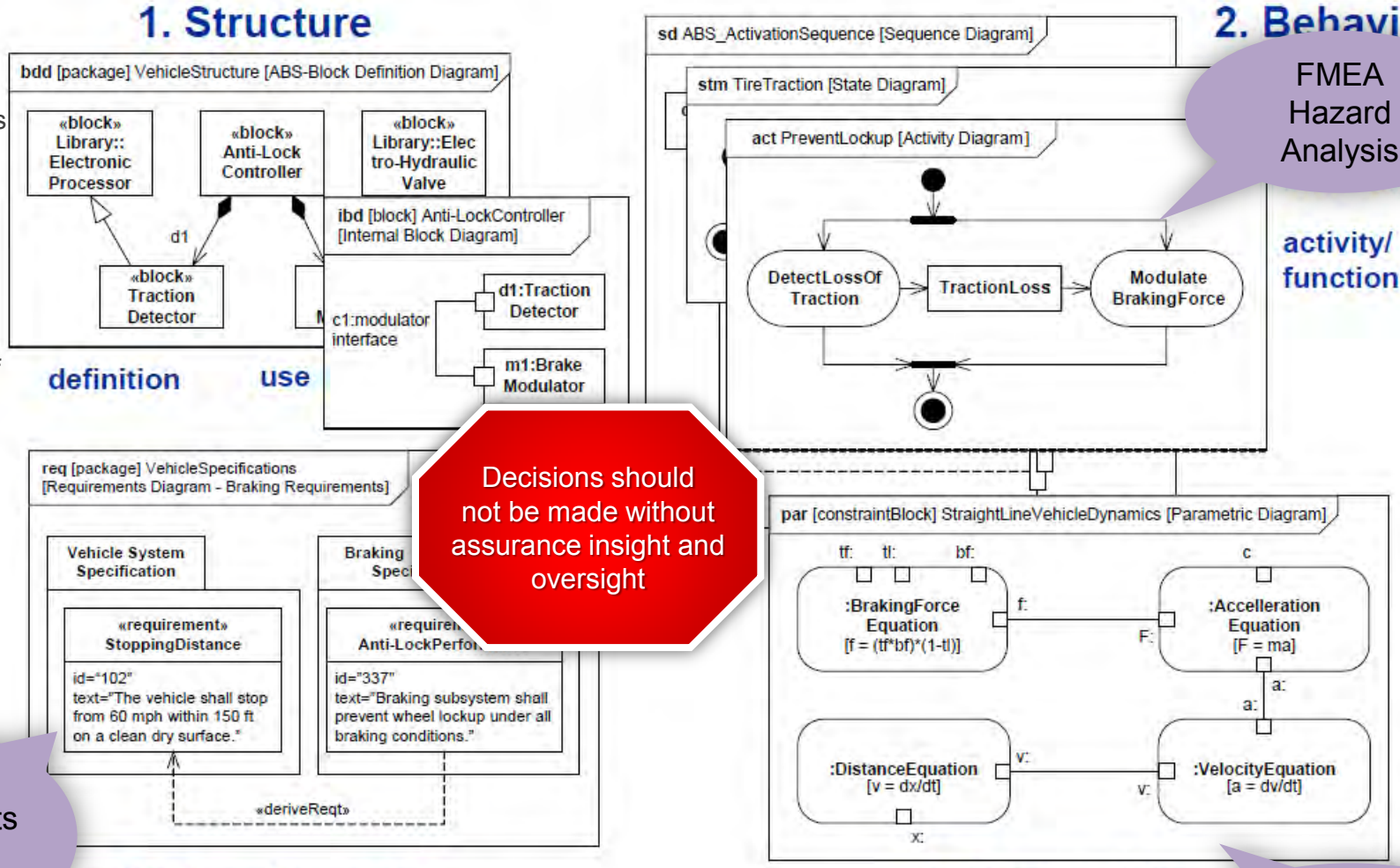
Typical Project Systems Engineering Organization



Managing the Systems engineering Process, CMS

SYSTEMS MODELING LANGUAGE (SYSML)- ABS EXAMPLE

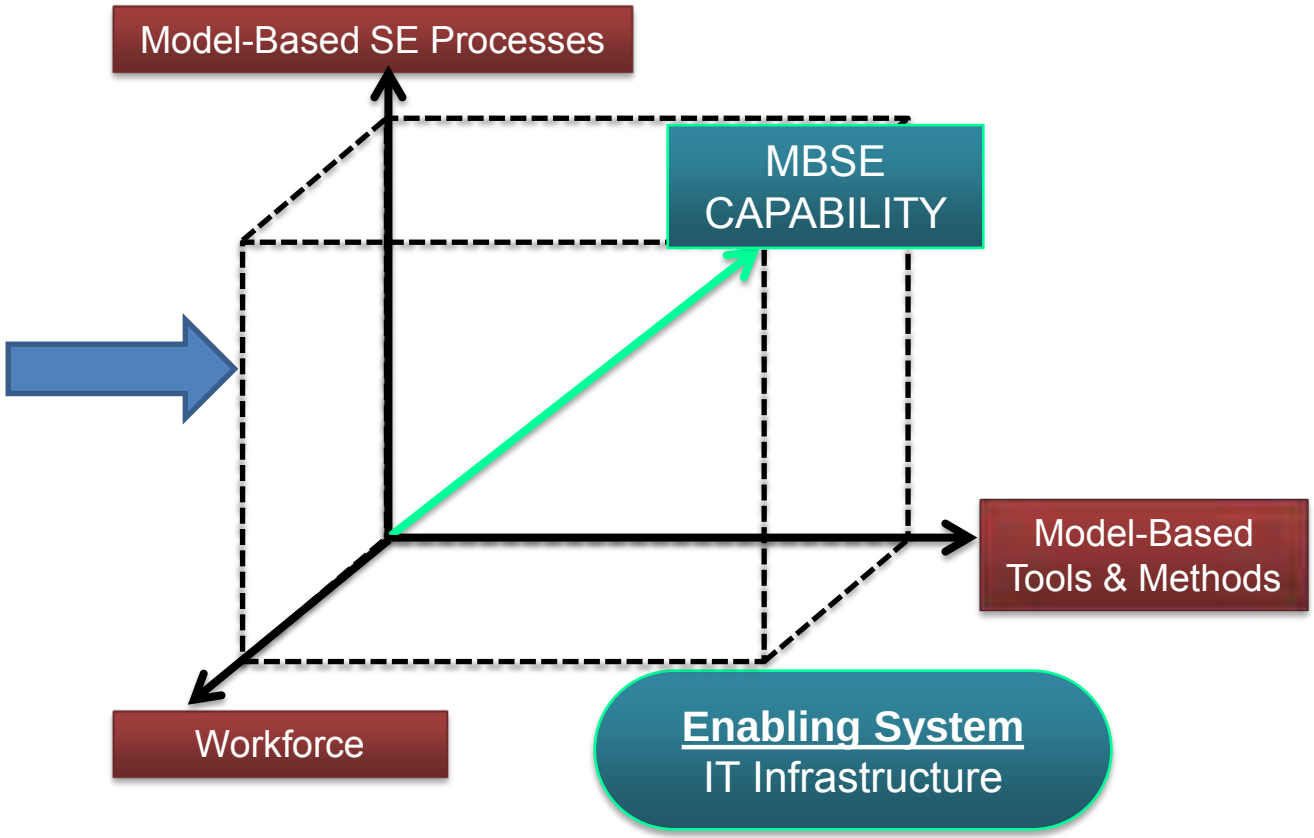
- SysML, being one of the key MBSE components, has a good foundation for capturing requirements, architecture, constraints, views and viewpoints.
- It allows linking different types of models that come from different engineering disciplines.



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

MBSE/MBMA Capability

Assurance organizations may need to define new roles, develop new skills, and train on new tools to engage in the Model Based Systems Engineering environment

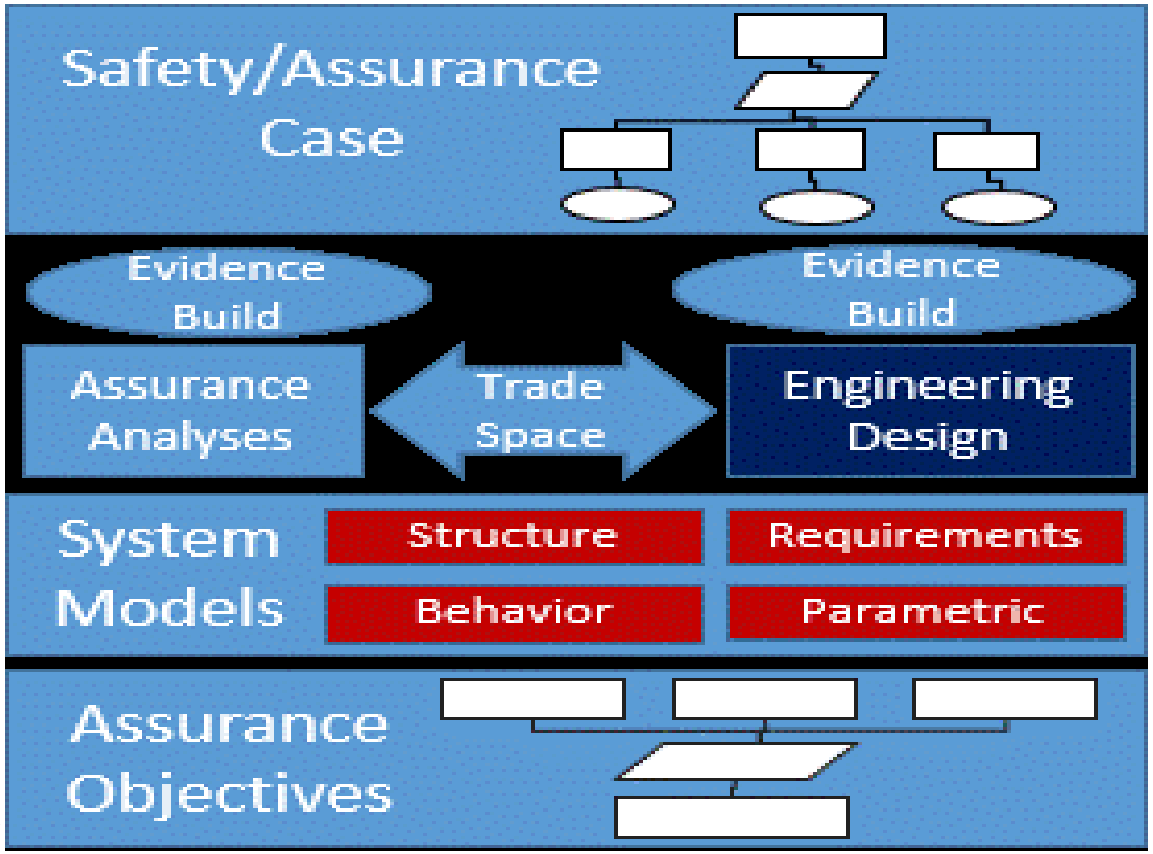


Joe Hale/Fayssal M. Safie,
MSFC/QD01 presentation 4/7/16

Model Based Mission Assurance

Mission Assurance products may need to be different in a model based environment (Objective Driven standards and requirement…)

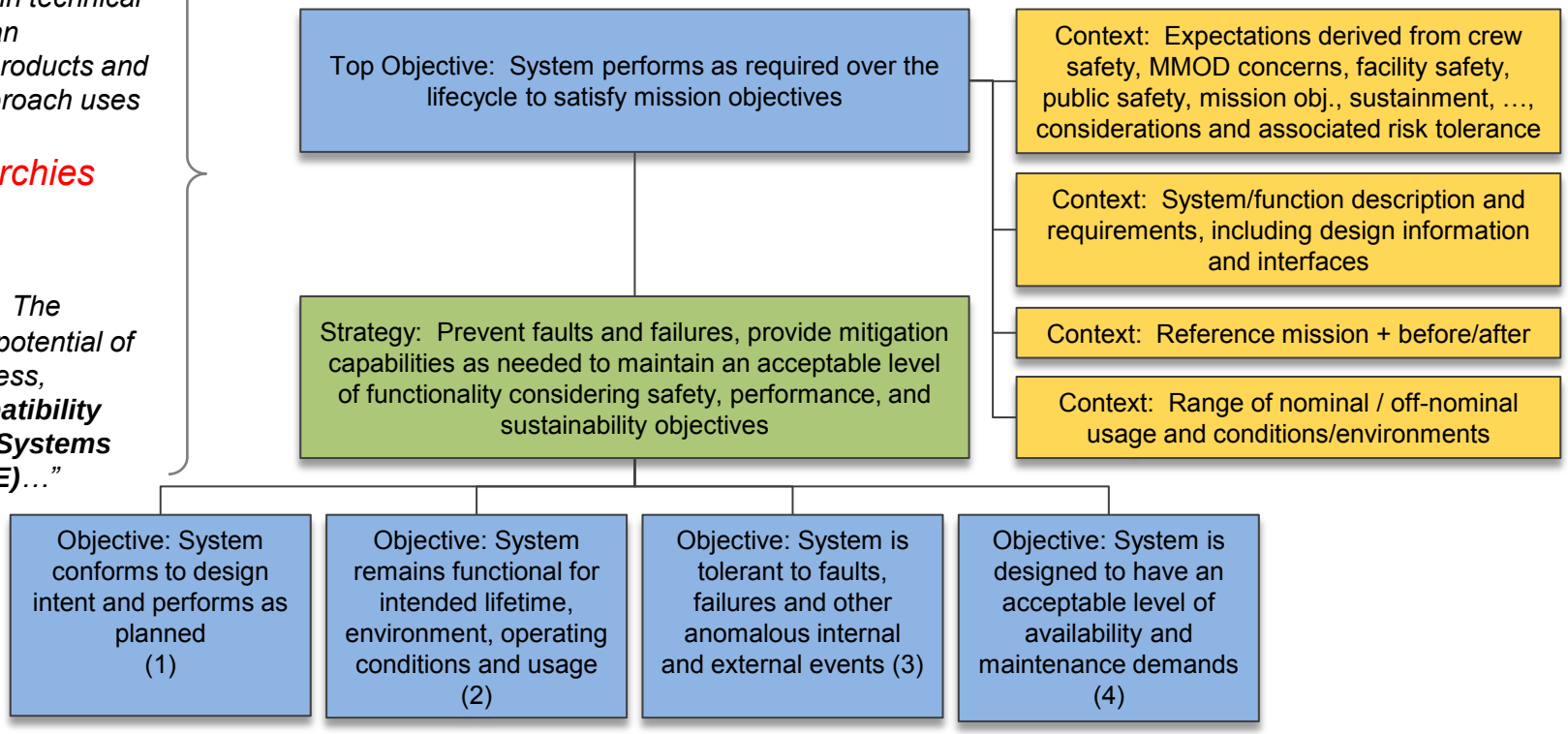
Effective Policies and Standards



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

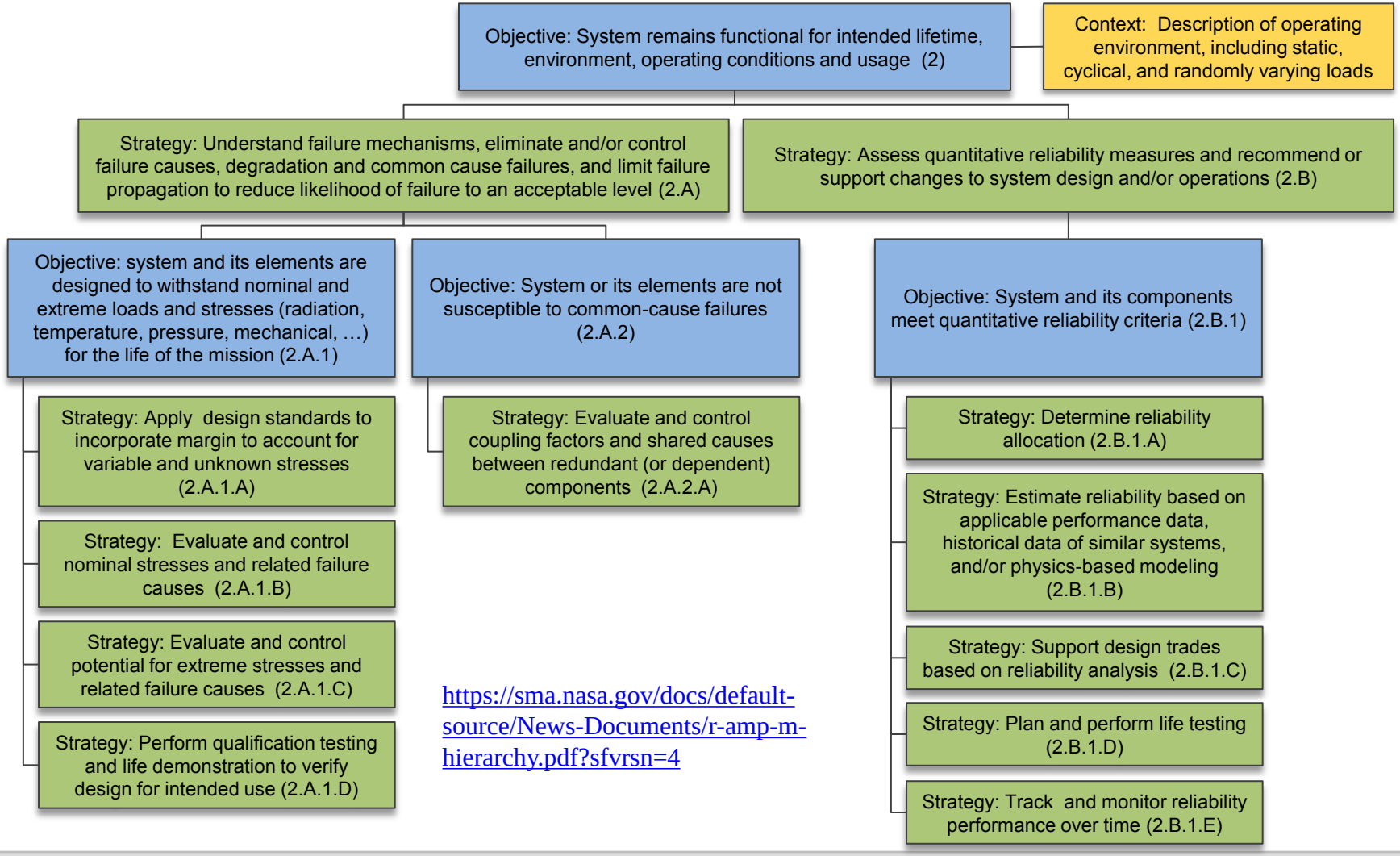
R&M Objectives Hierarchy – Top Level

"…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)****…"*



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

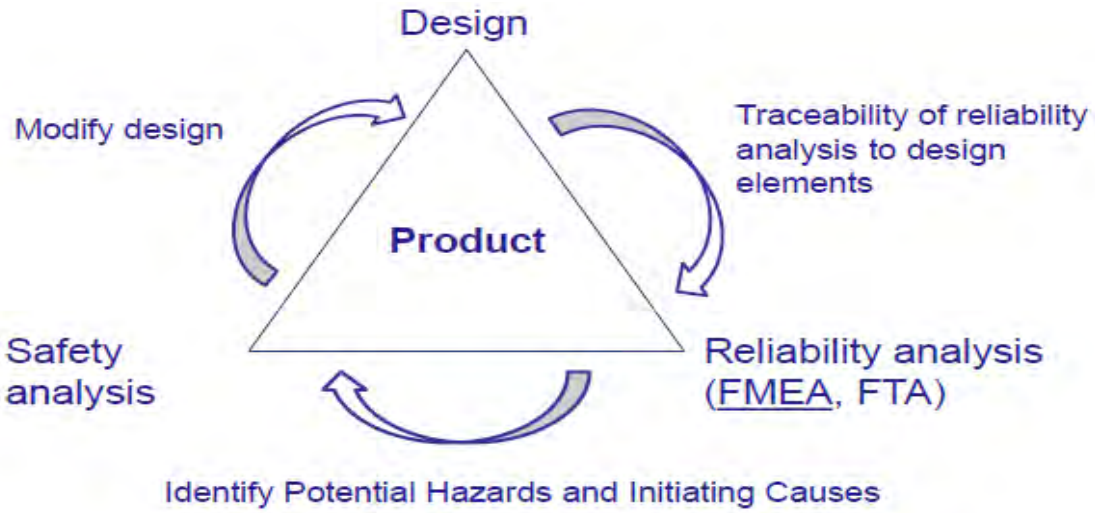
R&M Objectives Hierarchy (Continued)
SUB – OBJ. 2



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

Tying Design, Reliability & Safety Analyses

Linking designs to reliability analysis, reliability analysis to safety analysis, and safety analysis to designs



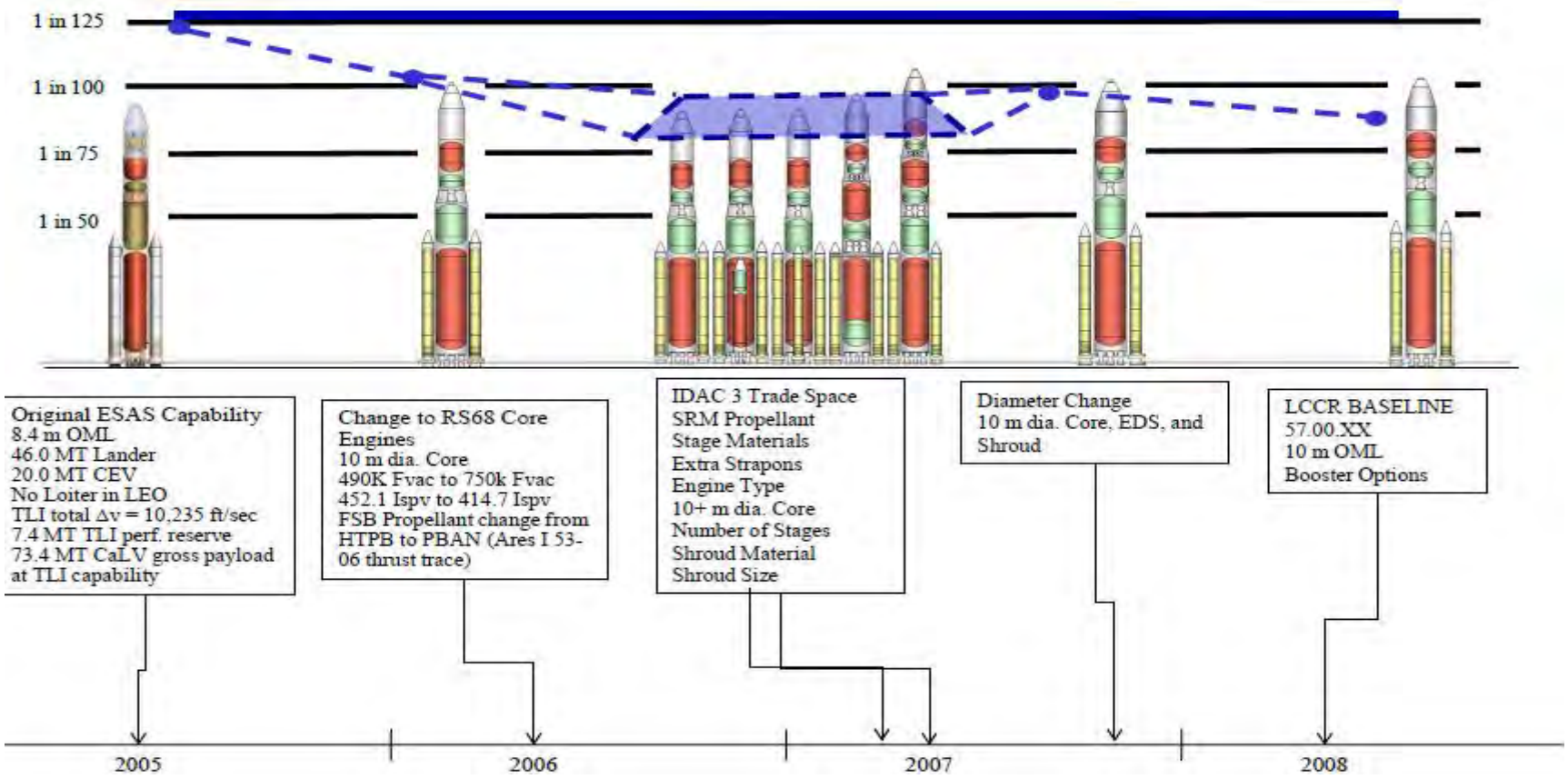
1. Integrating Safety and Reliability Analysis into MBSE Toolkit
   https://www.youtube.com/watch?v=NwuTV5-HAws

MBMA Case Studies - THE ARES V CASE

Performance-based Reliability and Safety Analysis

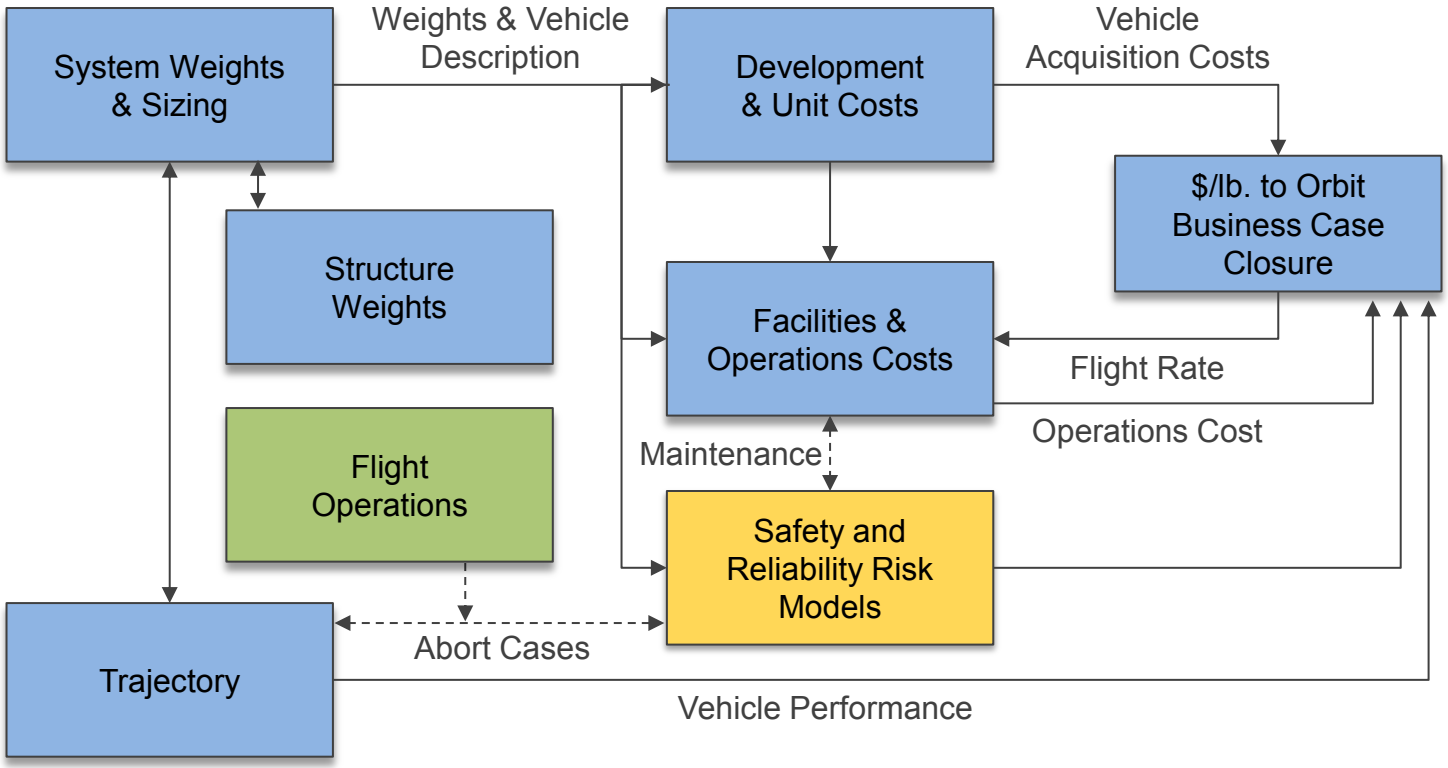
- Safety and Reliability analyses are an integral part of a program Design Analysis Cycles (DAC):
  - Launch System Architecture Assessments
  - Requirements evaluation and refinement
  - Assessment of progress toward program Goals

MBMA Case Studies
The ARES V Trades During Conceptual Design Phase

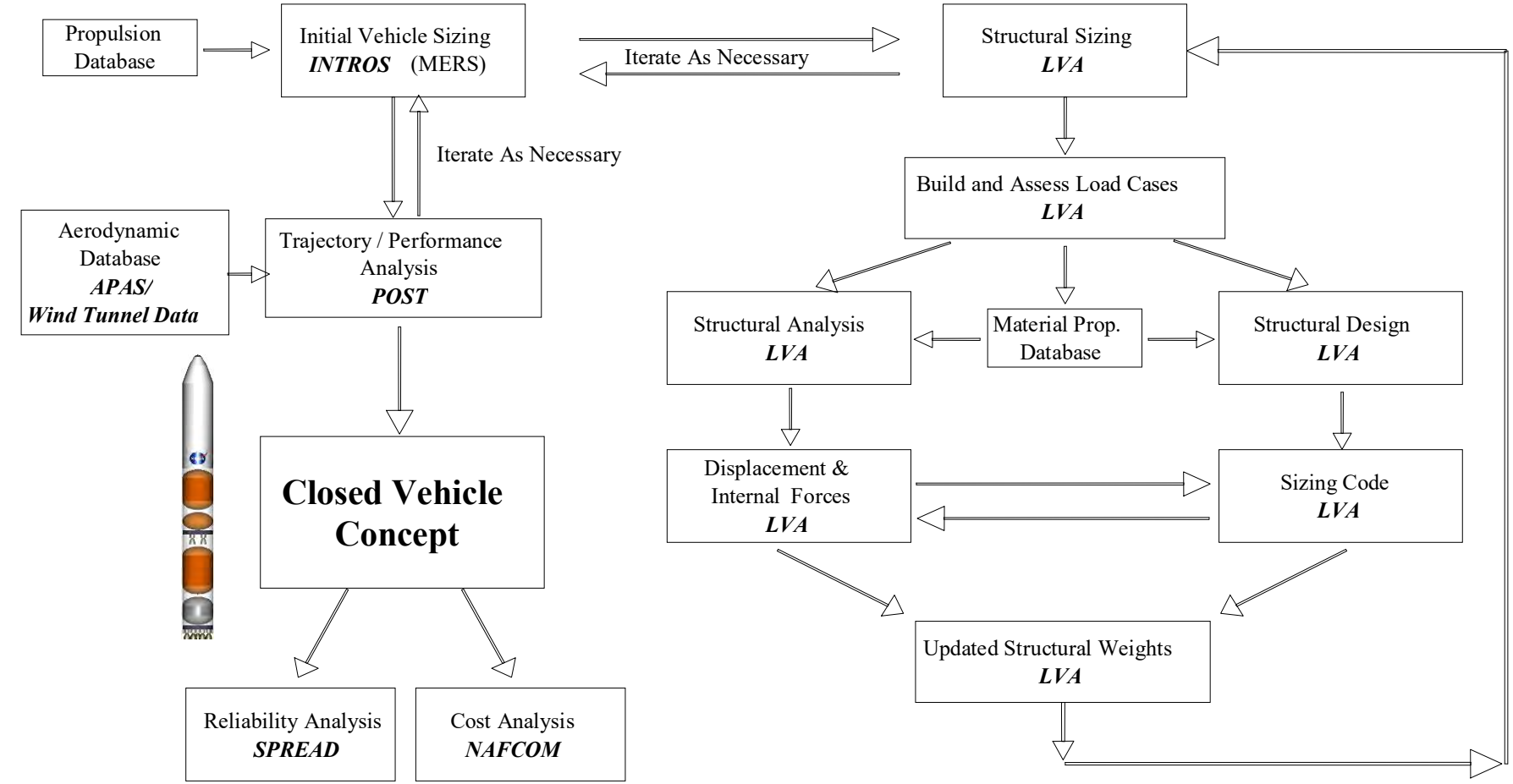


The ARES V launch vehicle is actually two vehicles in one since it serves both an ascent, or Earth launch function, and a trans-lunar injection (TLI), or Earth orbit departure function.

MBMA Case Studies - THE ARES V CASE
The ARES V Vehicle Concept Assessment Methodology

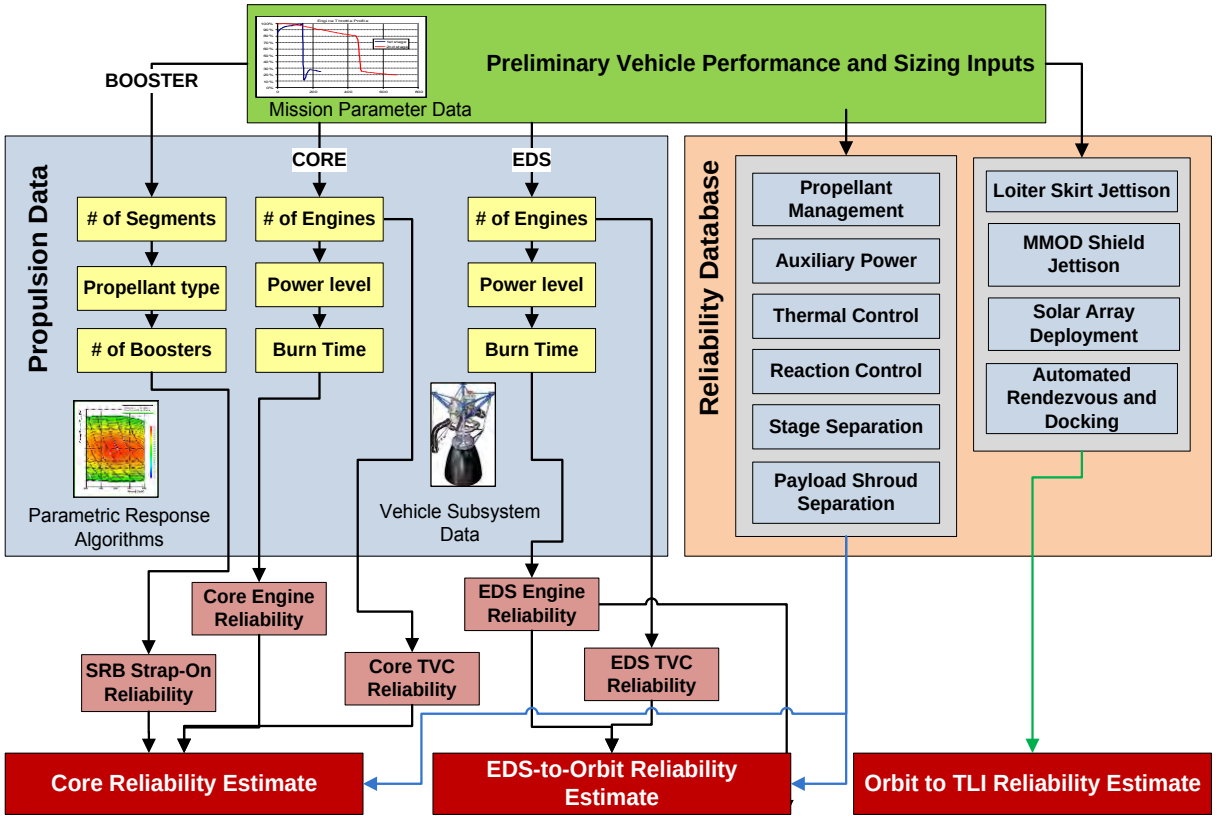


MBMA Case Studies - THE ARES V CASE
The ARES V Vehicle Concept Assessment Methodology



MBMA Case Studies - THE ARES V CASE
The ARES V Reliability Model Structure

Reliability Model Structure Schematic

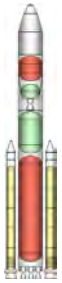


MBMA Case Studies - THE ARES V CASE
The ARES V Reliability Methodology

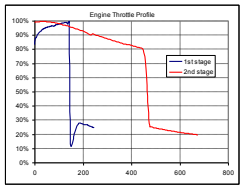
Mission Profile

Event	Time (sec)	Alt (km)
Liftoff		
Maximum Q		
SRB Separation		
Shroud Separation		
Main Engine Cutoff		
EDS Ignition		
EDS Engine Cutoff		

Vehicle Configuration



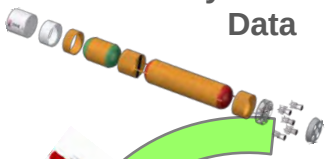
Subsystem Parameters



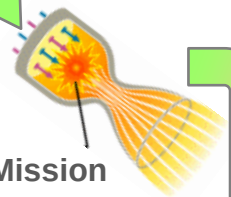
Advanced Concepts Office Design Input

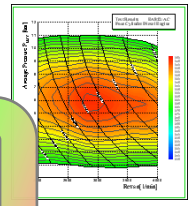
The Process

Ares V Subsystem Data



Reliability Database





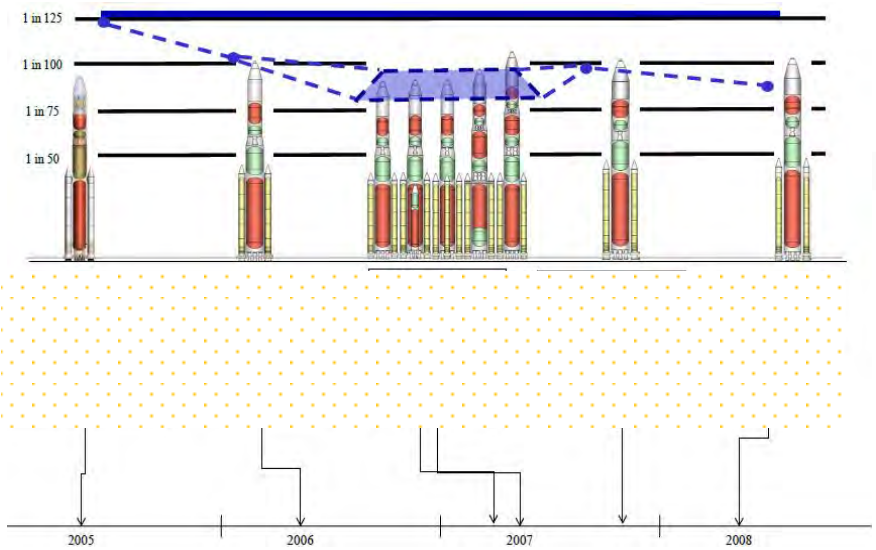
Reliability Algorithms

Mission Performance Data

System Analysis Integration

Reliability Evaluation Results

MBMA Case Studies - THE ARES V CASE
Within Concept Trade - Earth Departure Stage (EDS)

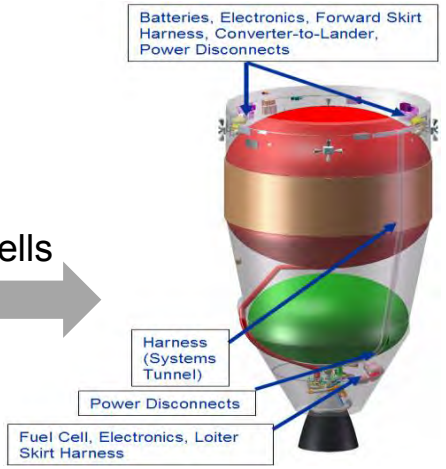


Performance-based reliability analysis provided supporting data in key architecture, element, subsystem, and component

design decisions.

Earth Departure Stage

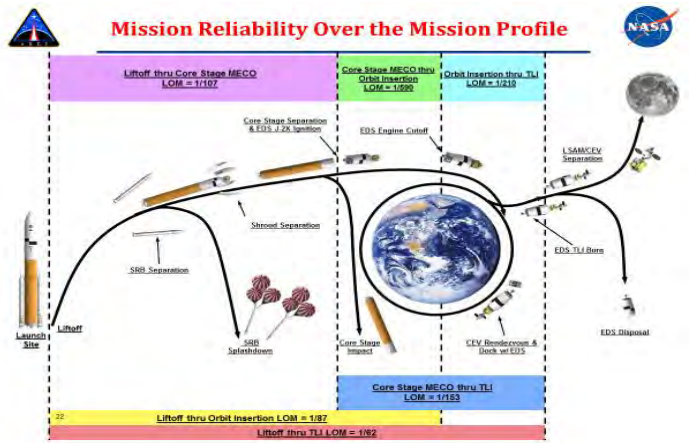
Solar Array to Fuel Cells



MBMA Case Studies - THE ARES V CASE
Reliability & Safety Predictions

Reliability and Safety Analyses Output

	Mean Failure Probability	MFBF (1 in)
SRB (2)	8.2118E-04	1,218
Core Stage engine CAT	1.1877E-03	842
Core Stage engine NCAT	6.9917E-03	143
Core Stage APU	2.3230E-05	43,048
Core Stage TCS	1.0800E-09	>1,000,000
Core Stage PMS	2.0907E-05	47,831
Core Stage TVC	2.2080E-04	4,529
Core Stage Separation	7.4003E-05	13,513
EDS engine CAT	1.0841E-04	9,224
EDS engine NCAT	5.9000E-04	1,695
EDS engine airstart	3.6000E-04	2,778
EDS APU	6.1794E-05	16,183
EDS TCS	1.0800E-09	>1,000,000
EDS PMS	5.7845E-06	172,876
EDS RCS	6.2540E-04	1,599
EDS TVC	3.6810E-05	27,167
Shroud	3.2464E-04	3,080
Ascent LOM (Loss of Mission)	**1.1452E-02**	**87**



Safety Condition

1	Inability to rendezvous with Orion and continue mission
2	Inability to perform mission critical operations in LEO
3	Undesired vehicle translation or rotation in LEO
4	Undesired vehicle translation or rotation during lunar coast
5	Undesired vehicle rotation during TLI burn
6	Uncontained release of energy and debris in LEO
7	Vehicle enters off nominal cis-lunar trajectory
8	Uncontained release of energy and debris during lunar coast
9	Uncontained release of energy and debris during TLI burn

Likelihood Estimate	1	2	3	4	5
Greater than 1 in 100					
Greater than 1 in 1,000	1			7	
Greater than 1 in 10,000	2	3			9
Greater than 1 in 100,000		4	6		
Greater than 1 in 1,000,000			5	8	

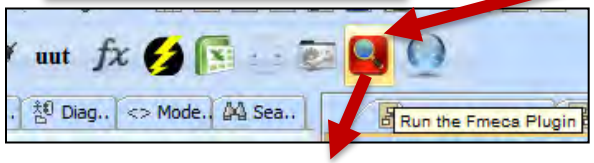
Consequence Level

Can We Customize Reliability and Safety Analyses to Fit in The MBSE Environment?

- Can reliability and safety analyses can be customized to fit in a MBSE?
- Can MBSE provide the frame of work to support Reliability and safety analyses?

SysML Models

Magic Draw Plug-Ins



Integrating Safety and Reliability Analysis into MBSE Toolkit
https://www.youtube.com/watch?v=NwuTV5-HAws

Reliability and safety predictions output

	Mean Failure Probability	MFBF (1 in)
SRB (2)	8.2118E-04	1,218
Core Stage engine CAT	1.1877E-03	842
Core Stage engine NCAT	6.9917E-03	143
Core Stage APU	2.3230E-05	43,048
Core Stage TCS	1.0800E-09	>1,000,000
Core Stage PMS	2.0907E-05	47,831
Core Stage TVC	2.2080E-04	4,529
Core Stage Separation	7.4003E-05	13,513
EDS engine CAT	1.0841E-04	9,224
EDS engine NCAT	5.9000E-04	1,695
EDS engine airstart	3.6000E-04	2,778
EDS APU	6.1794E-05	16,183
EDS TCS	1.0800E-09	>1,000,000
EDS PMS	5.7845E-06	172,876
EDS RCS	6.2540E-04	1,599
EDS TVC	3.6810E-05	27,167
Shroud	3.2464E-04	3,080
Ascent LOM (Loss of Mission)	**1.1452E-02**	**87**

Safety Condition

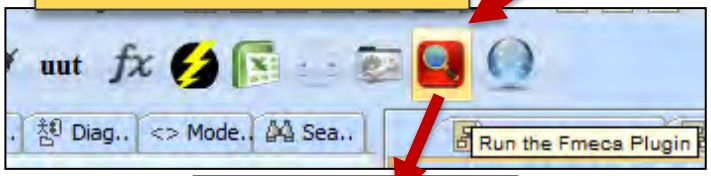
1	Inability to rendezvous with Orion and continue mission
2	Inability to perform mission critical operations in LEO
3	Undesired vehicle translation or rotation in LEO
4	Undesired vehicle translation or rotation during lunar coast
5	Undesired vehicle rotation during TLI burn
6	Uncontained release of energy and debris in LEO
7	Vehicle enters off nominal cis-lunar trajectory
8	Uncontained release of energy and debris during lunar coast
9	Uncontained release of energy and debris during TLI burn

A FMECA Synthesis Example

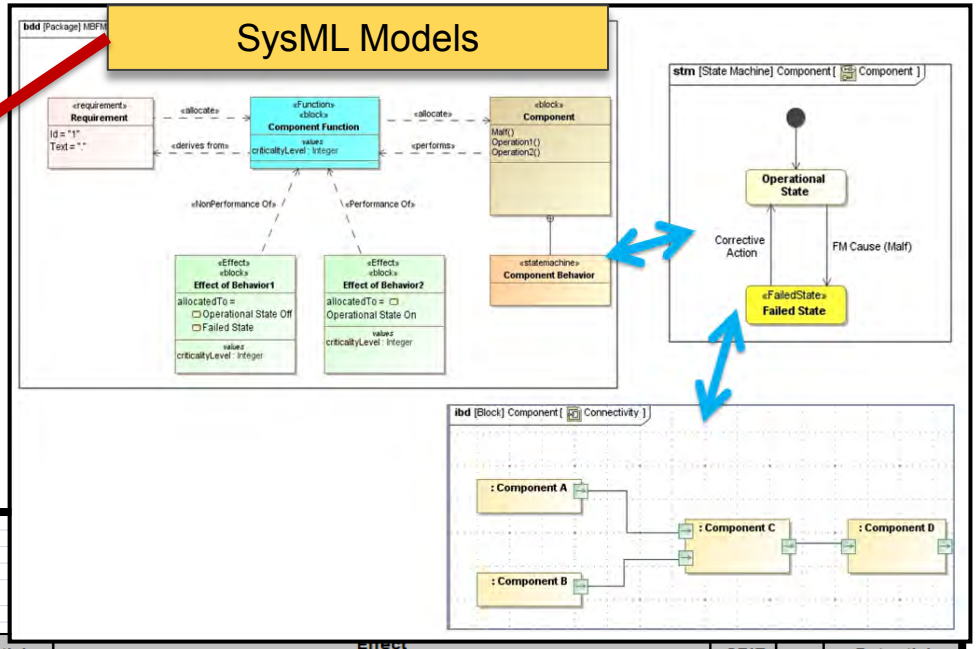
Courtesy Lui Wang
Johnson Space Center

SysML Models

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				CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent	Other Independent Failures			
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

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

References

- Goddard Space Flight Center (GSFC) MBSE Workshop, February 17-18, 2016, (See Link 1 Below).
- NASA Jet Propulsion Laboratory (JPL) Symposium and workshop on MBSE, January 28-30, 2015, (See Link 2 Below).
- Integrating Safety and Reliability Analysis into MBSE Toolkit, (See Link 3 Below)
- Reliability and Maintainability Objective Driven Hierarchy (NASA, OSMA), (See Link 4 Below).
- Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA
- 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

1. https://drive.google.com/open?id=0Bw3ikr90G7CVR01Wd0hTWjN5NjA
2. https://drive.google.com/drive/folders/0B3hsmXWocH2JZVpTSzdzaUxYQzA
3. ttps://www.youtube.com/watch?v=NwuTV5-Haws
4. https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4