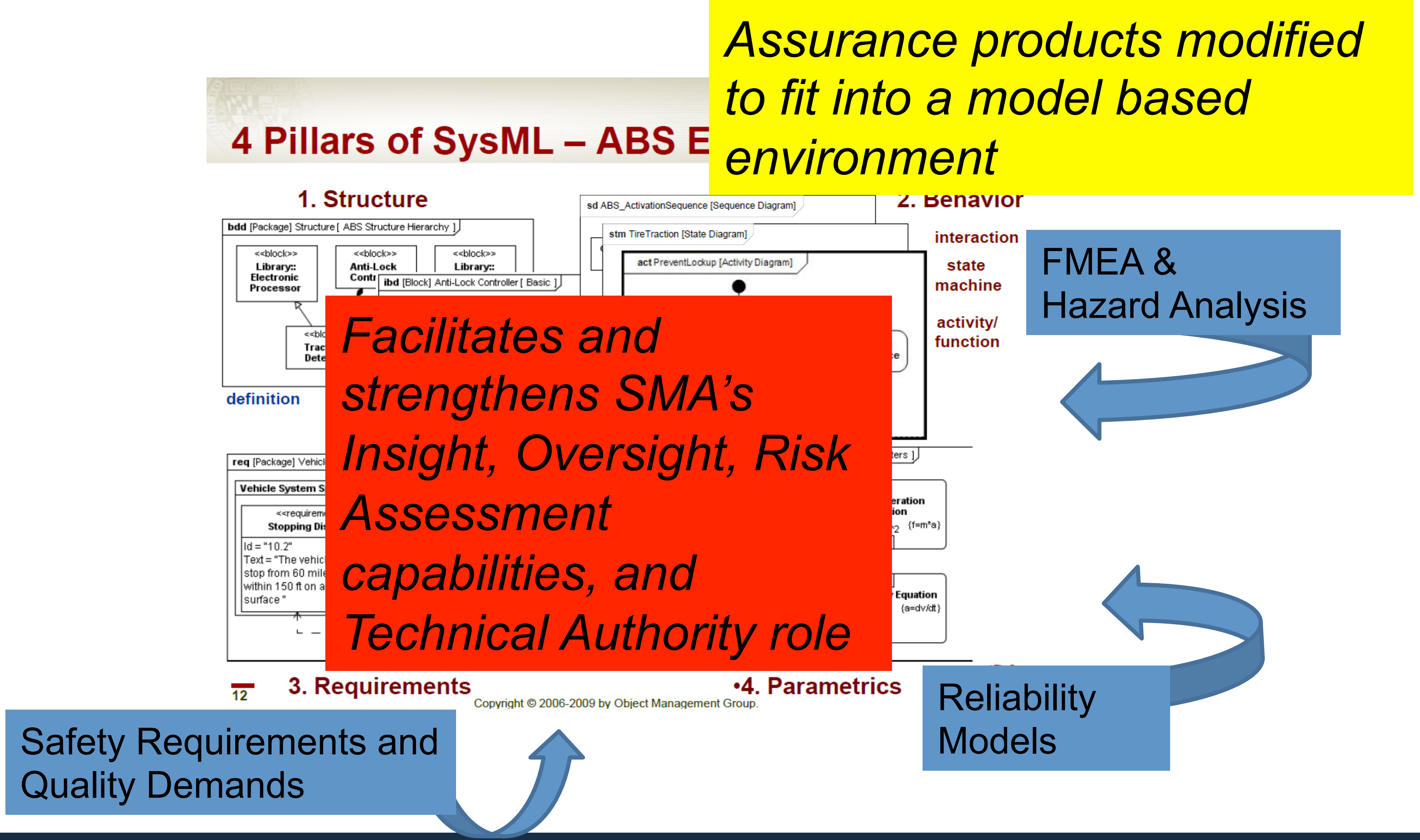
National Aeronautics and Space Administration

Model Based Mission Assurance

Tony DiVenti, Branch Head – Reliability and Risk Analysis (Code 371), Goddard Space Flight Center

John W. Evans, Office of Safety and Mission Assurance, NASA HQ

MBSE – How does SMA fit in



Assurance products modified to fit into a model based environment

Facilitates and strengthens SMA’s Insight, Oversight, Risk Assessment capabilities, and Technical Authority role

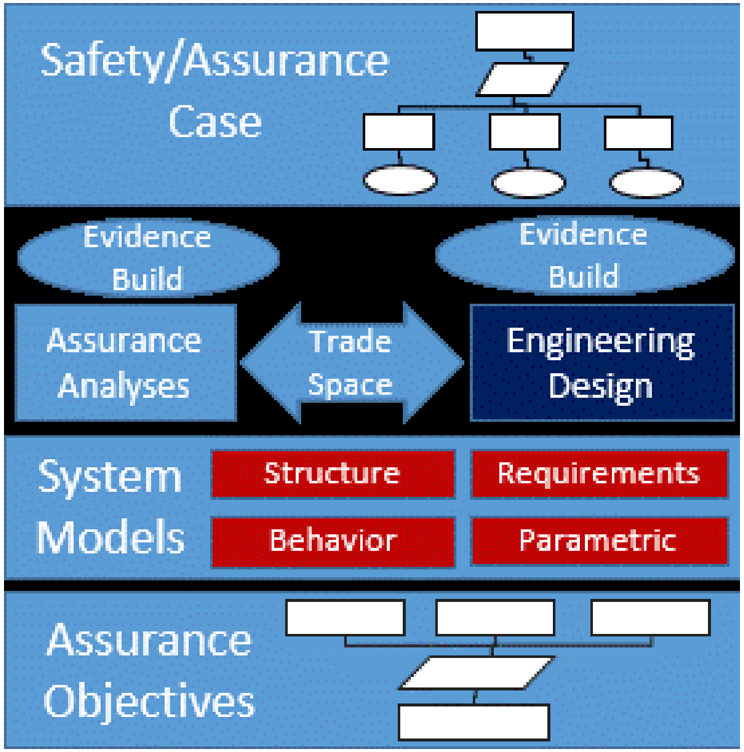
FMEA & Hazard Analysis

Reliability Models

Safety Requirements and Quality Demands

4 Pillars of SysML – ABS E
1. Structure
bdd [Package] Structure [ABS Structure Hierarchy]
<<block>> Library:: Electronic Processor
<<block>> Anti-Lock Contr
<<block>> Library::
ibd [Block] Anti-Lock Controller [Basic]
<<blo Trac Dete
definition
sd ABS_ActivationSequence [Sequence Diagram]
stm TireTraction [State Diagram]
act PreventLockup [Activity Diagram]
2. Behavior
interaction
state machine
activity/ function
req [Package] Vehicl
Vehicle System S
<<requirem
Stopping Dis
Id = "10.2"
Text = "The vehic stop from 60 mil within 150 ft on a surface "
eration ion
{f=m*a}
Equation {a=dv/dt}
12
3. Requirements
•4. Parametrics
Copyright © 2006-2009 by Object Management Group.

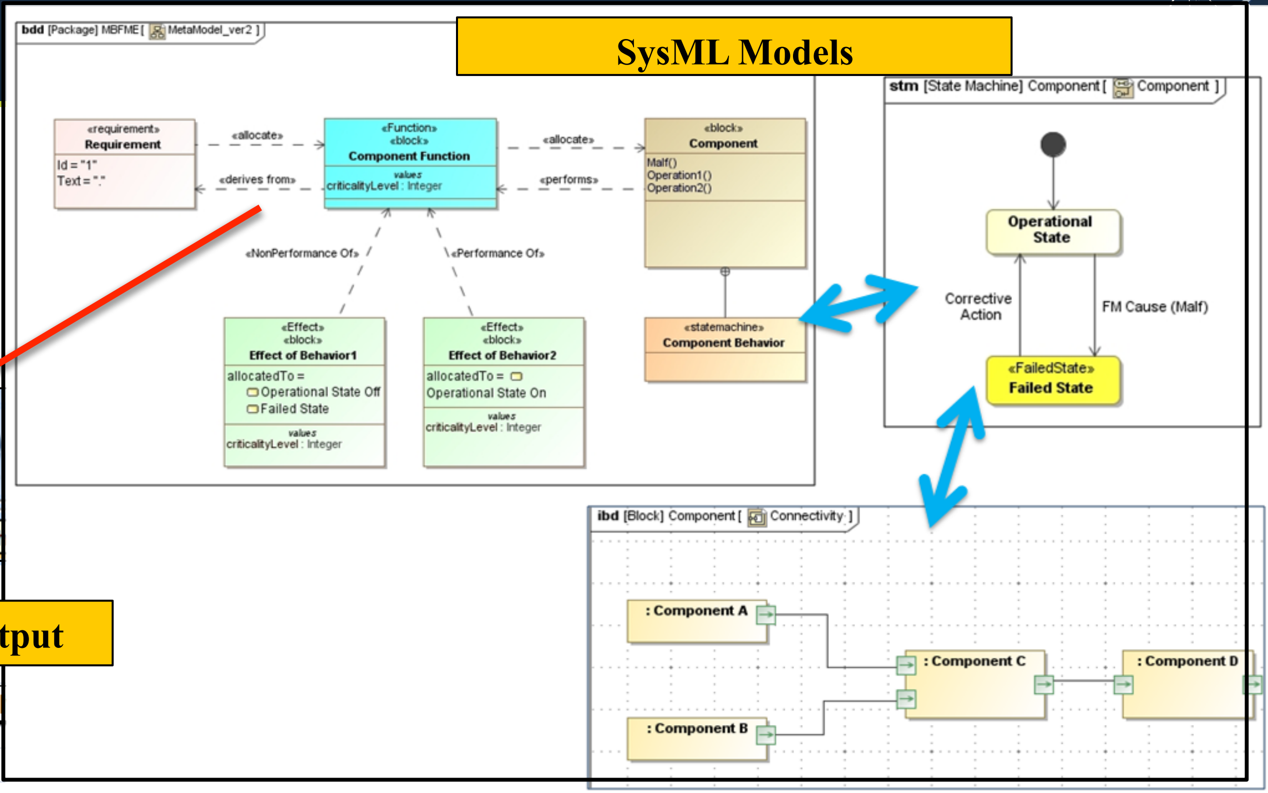
MBMA – Model Based Mission Assurance



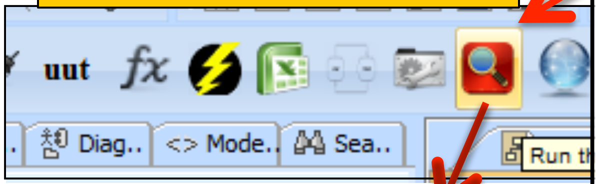
Example - MBSE FMEA

Courtesy Lui Wang
Johnson Space Center

SysML Models



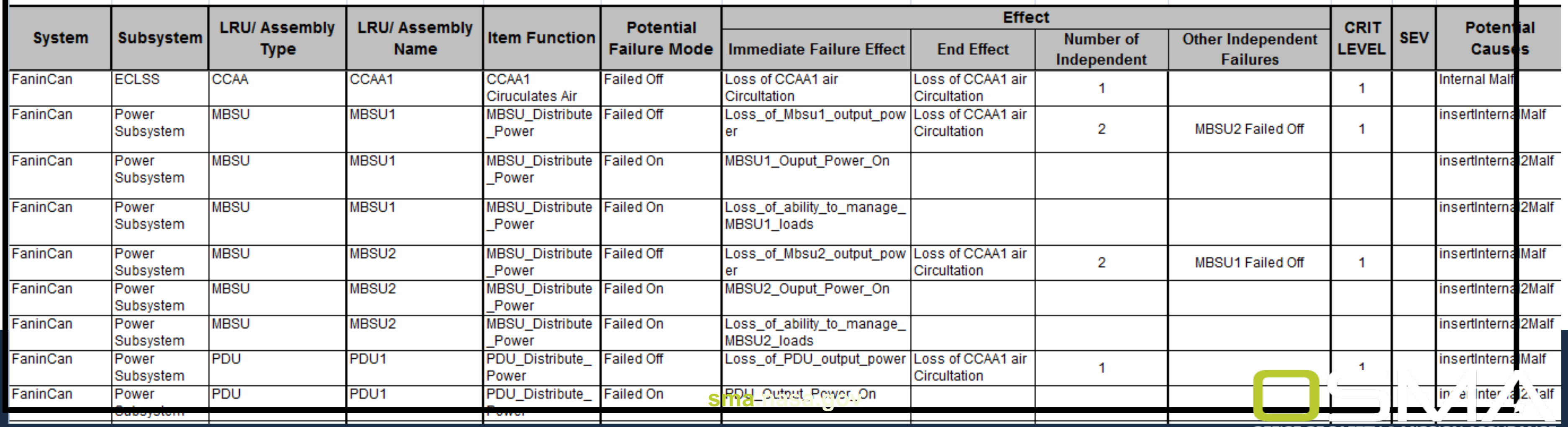
Magic Draw Plug-Ins



FMECA Output

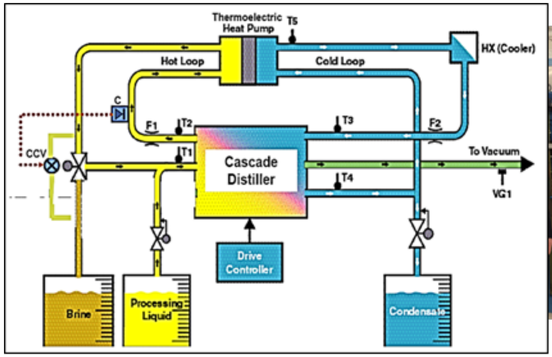
Failure Modes and Effects Criticality Ana

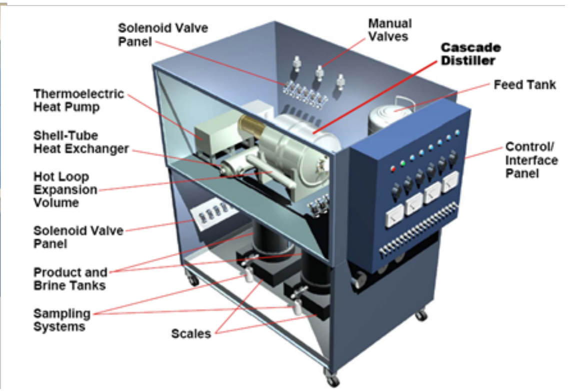
Project Name:	Fan in the Can SysML Model

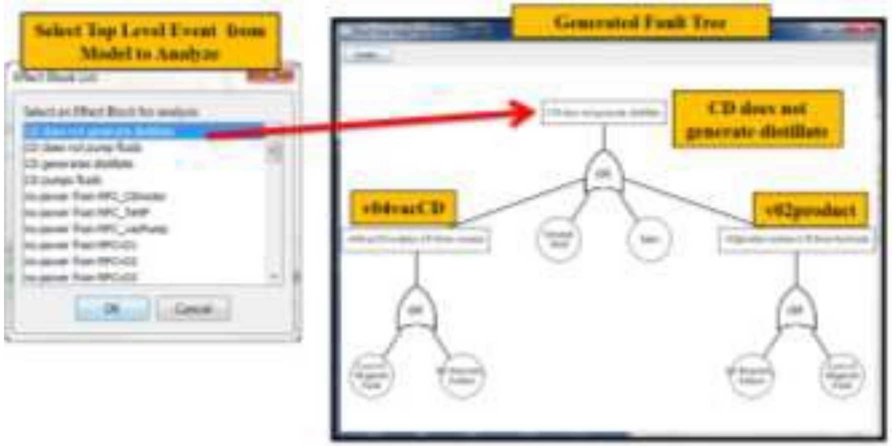


System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent	Other Independent Failures			
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Ciruculates Air	Failed Off	Loss of CCAA1 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

Example - CDS System Fault Tree






Select an Effect Block for analysis

CD does not generate distillate
CD does not pump fluids
CD generates distillate
CD pumps fluids

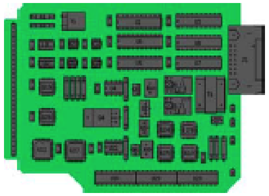
Select Top Level Event from Model to Analyze
Generated Fault Tree
CD does not generate distillate
v04earCD
v02product
OR
OK
Cancel

Courtesy Lui Wang
Johnson Space Center

Future Example - Physics of Failure Model Integration

FY16 Planned Collaboration – UMD Center for Advanced Life Cycle Engineering (CALCE)

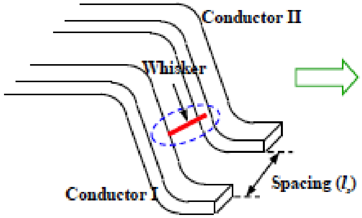
Simulation Assisted Reliability Assessment (SARA®) Software



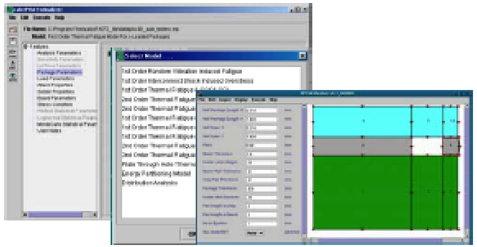
calcePWA
Circuit Card Assemblies

Thermal Analysis
Vibrational Analysis
Shock Analysis
Failure Analysis

calceEP
Device andPackage
Failure Analysis



calceTinWhisker FailureRiskCalculator

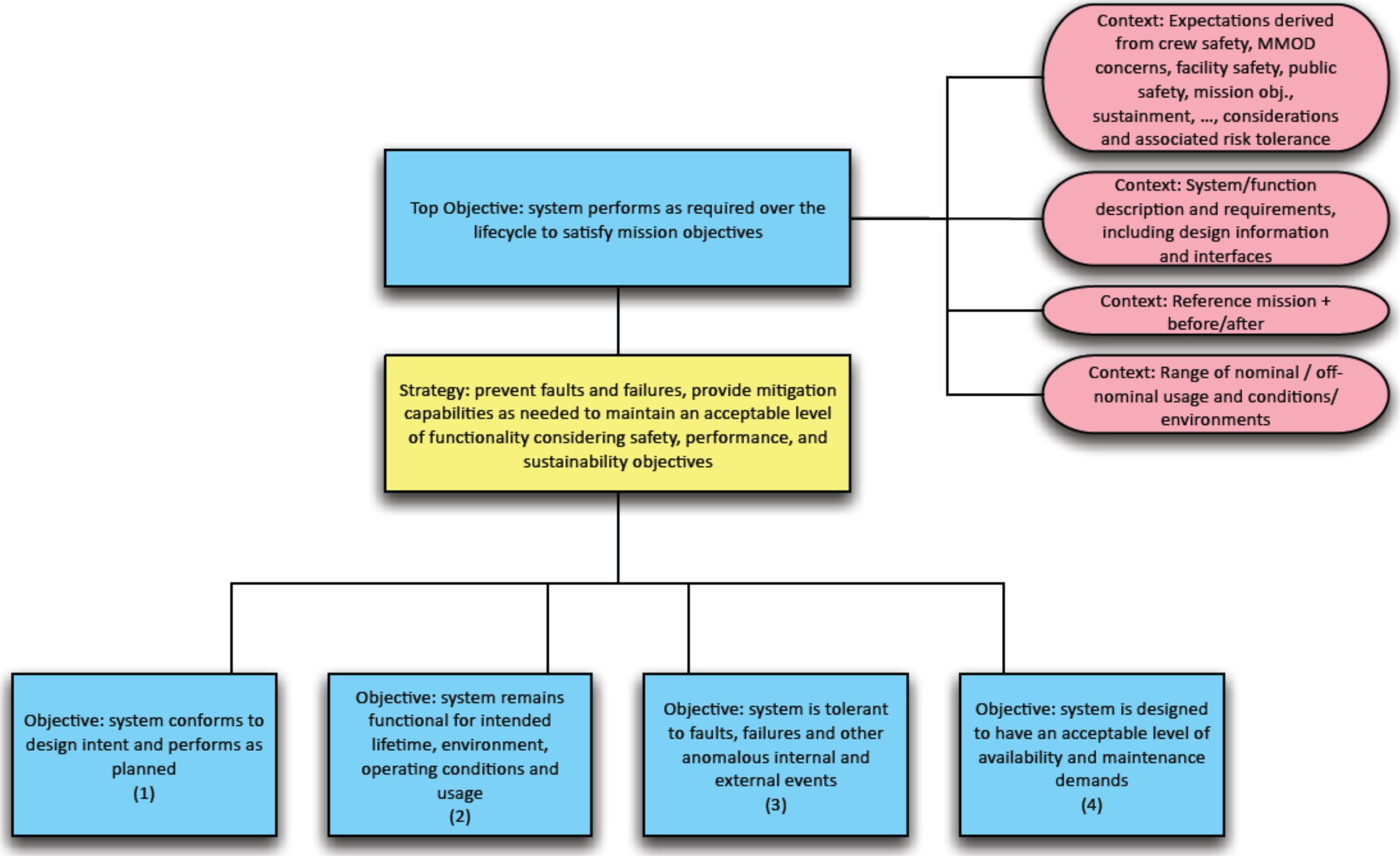


calceFAST
Failure Assessment
Software Toolkit

- GSFC has access to CALCE SARA® software to perform in depth parts reliability analysis
- A system model that links to SARA® could produce more accurate reliability analyses
- MBSE provides a framework to support this activity

Objectives Based Assurance

R&M Objectives Structure – Top-Level



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)

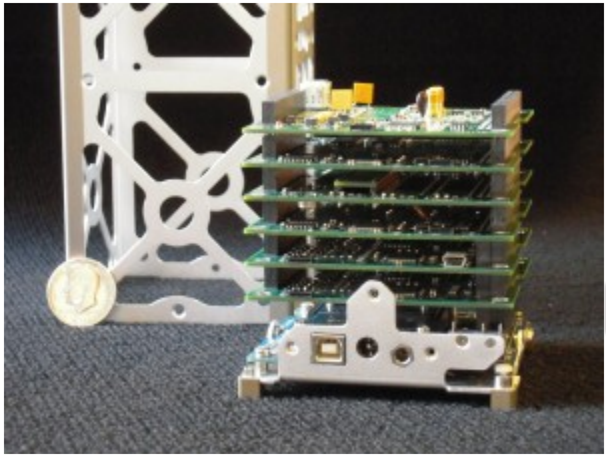
Objective: system is designed to have an acceptable level of availability and maintenance demands (4)

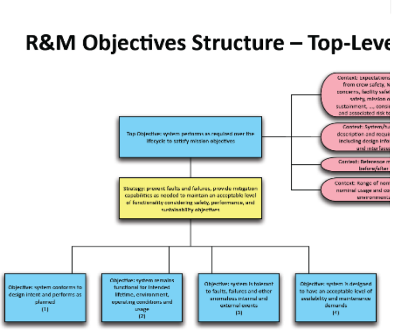
Laying the Foundation

- Logically decompose top-level R&M objective
  - Use elements of the Goal Structuring Notation
  - Structure shows why strategies are to be applied

- Structure forms basis for a proposed R&M standard
  - Specifies the technical considerations to be addressed by projects
  - Forms basis for evaluation of plans, design, and assurance products

Assurance Case





R&M Objectives Structure – Top-Leve

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

Context: Expectations from crew safety, N concerns, facility safe safety, mission a sustainment, ..., consi and associated risk to

Context: System/h description and requi including design infor and interfaces

Context: Reference m before/after

Context: Range of nom nominal usage and co environmenta

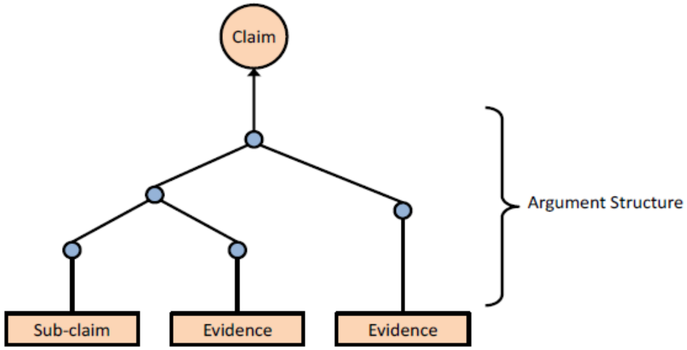
Strategy: prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives

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)



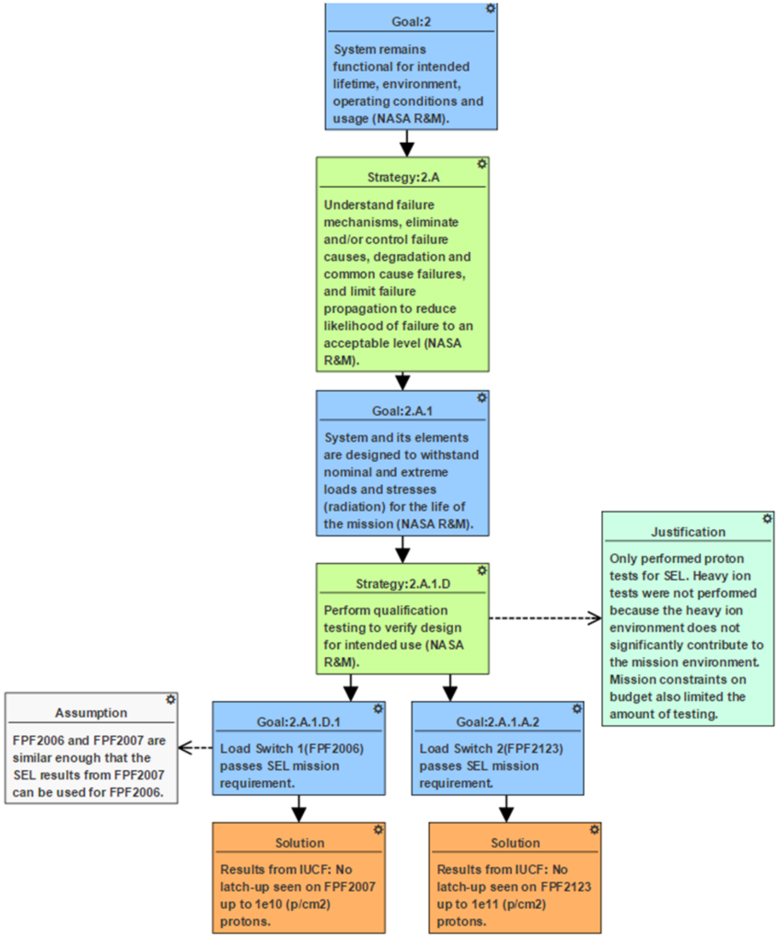
Claim

Argument Structure

Sub-claim

Evidence

Evidence



Goal:2

System remains functional for intended lifetime, environment, operating conditions and usage (NASA R&M).

Strategy:2.A

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 (NASA R&M).

Goal:2.A.1

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Strategy:2.A.1.D

Perform qualification testing to verify design for intended use (NASA R&M).

Justification

Only performed proton tests for SEL. Heavy ion tests were not performed because the heavy ion environment does not significantly contribute to the mission environment. Mission constraints on budget also limited the amount of testing.

Assumption

FPF2006 and FPF2007 are similar enough that the SEL results from FPF2007 can be used for FPF2006.

Goal:2.A.1.D.1

Load Switch 1(FPF2006) passes SEL mission requirement.

Goal:2.A.1.A.2

Load Switch 2(FPF2123) passes SEL mission requirement.

Solution

Results from IUCF: No latch-up seen on FPF2007 up to 1e10 (p/cm2) protons.

Solution

Results from IUCF: No latch-up seen on FPF2123 up to 1e11 (p/cm2) protons.

Summary

- MBSE provides an unprecedented opportunity to integrate SMA and Engineering Analysis concurrently as part of a common modeling framework.
- MBMA, part of the MBSE environment, facilitates and enhances SMA's analytical and risk assessment capabilities.
- MBSE and MBMA fully supports GSFC's Risk Based SMA Approach and the Agency's R&M Objectives Structure and as part of a larger Safety/Assurance Case.