U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – AVIATION & MISSILE CENTER

MBSE Methodologies for System Safety Analyses

Jason Rogers

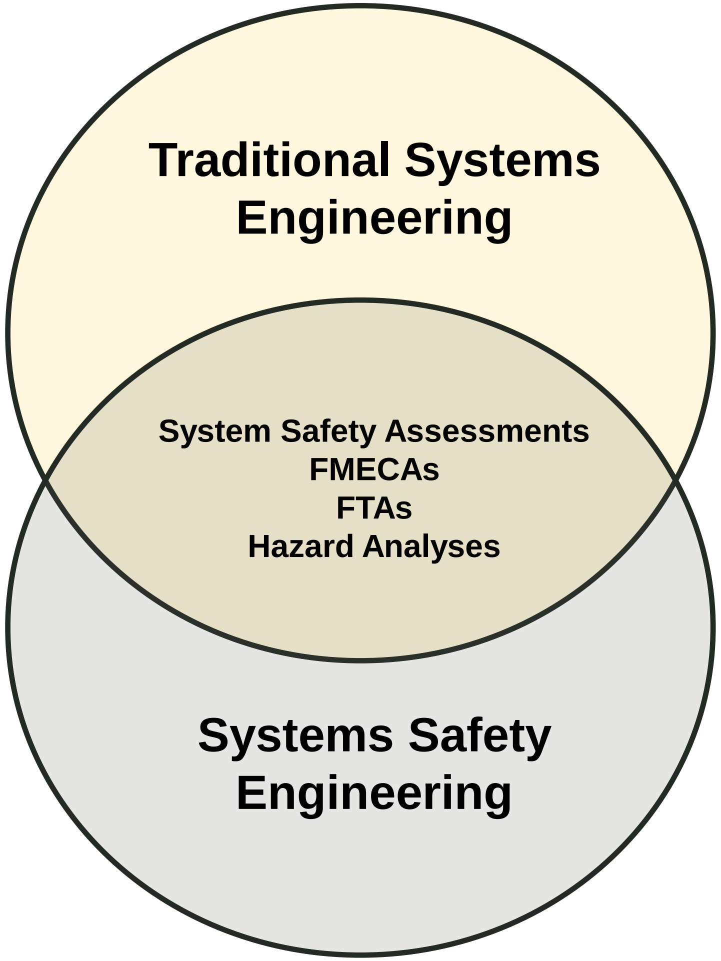
Senior Model-Based Systems Engineer

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; 10 April 2019. Other requests for this document shall be referred to the Director, CCDC-AVM, Engineering Directorate, FCDD-AME-O, Redstone Arsenal AL 35898-5000.

02 Nov 2022

OVERVIEW

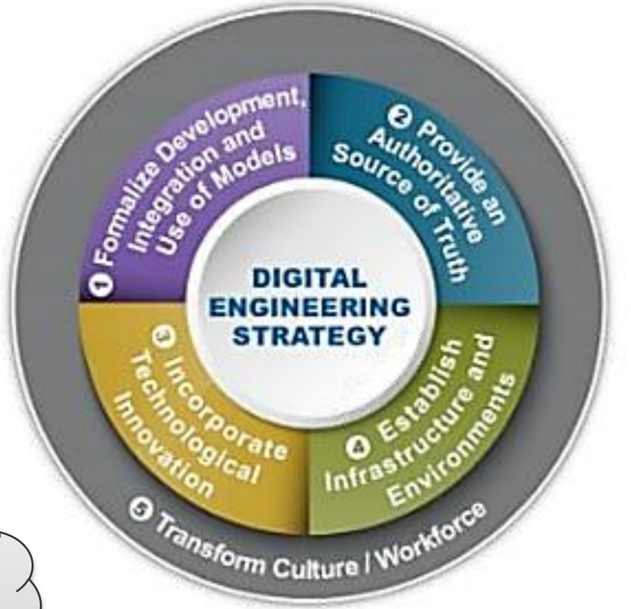
- How Systems Safety Analysis can be successful using MBSE to implement DoD Digital Engineering (DE) Strategies
- Improving how we document system safety information by bridging the gap between Traditional Systems Engineering and Systems Safety Engineering
- How to utilize MBSE to capture MIL-STD-882 artifacts

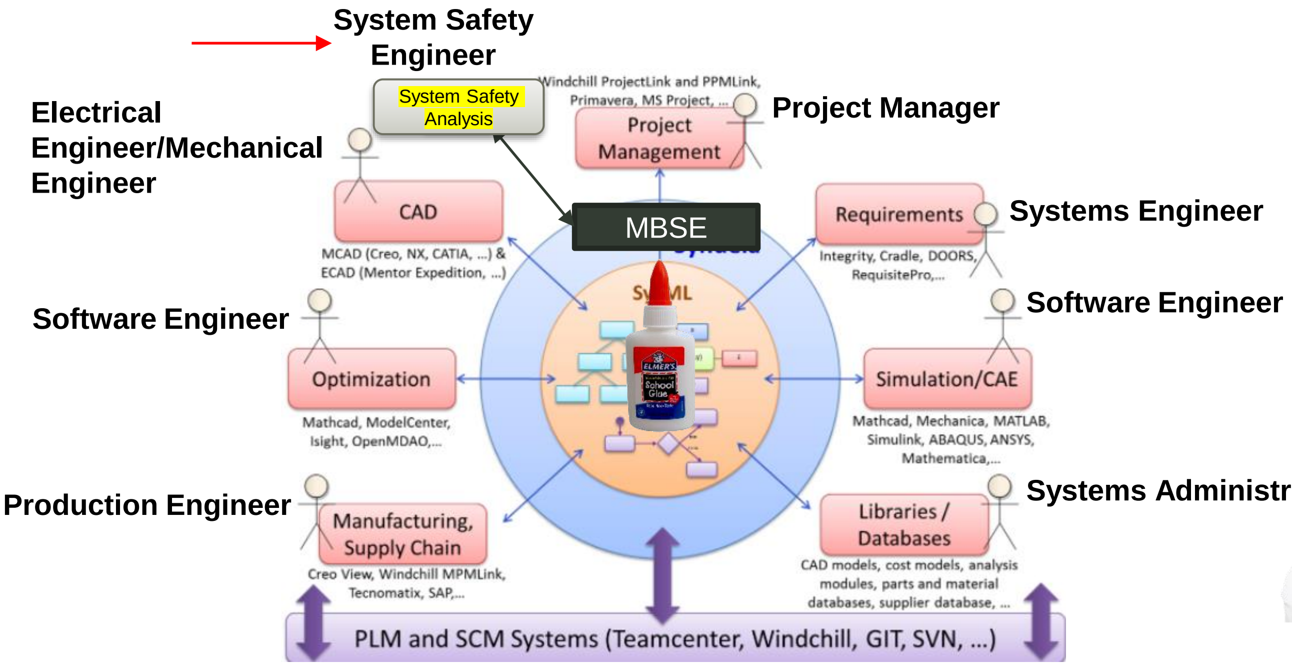

Traditional Systems Engineering
System Safety Assessments
FMECAs
FTAs
Hazard Analyses
Systems Safety Engineering

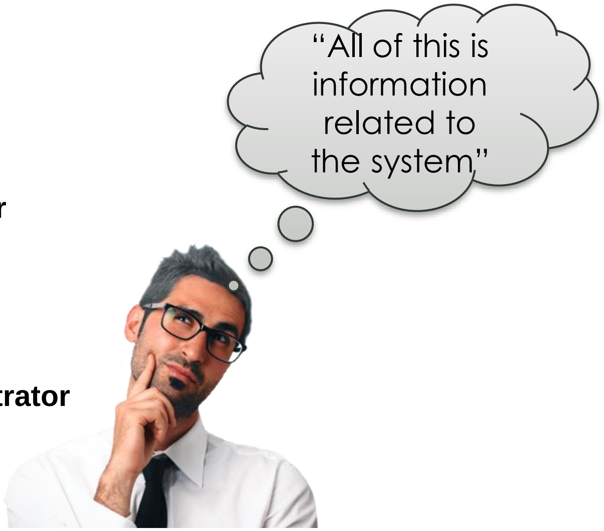
WHAT IS MBSE?

Digital Engineering (DE) is the use of digital artifacts, digital environment, and digital tools in the performance of engineering functions.

Model-Based Engineering (MBE) is an approach to engineering that uses models as an integral part of the technical baseline that includes the requirements, analysis, design, and verification of a capability, system or product throughout the acquisition lifecycle.


DIGITAL ENGINEERING STRATEGY
1 Formalize Development, Integration and Use of Models
2 Provide an Authoritative Source of Truth
3 Incorporate Technological Innovation
4 Establish Infrastructure and Environments
5 Transform Culture / Workforce


System Safety Engineer
System Safety Analysis
Electrical Engineer/Mechanical Engineer
Windchill ProjectLink and PPMLink, Primavera, MS Project, ...
Project Management
Project Manager
CAD
MCAD (Creo, NX, CATIA, ...) & ECAD (Mentor Expedition, ...)
MBSE
Requirements
Integrity, Cradle, DOORS, RequisitePro,...
Systems Engineer
Software Engineer
Optimization
Mathcad, ModelCenter, Isight, OpenMDAO,...
Simulation/CAE
Mathcad, Mechanica, MATLAB, Simulink, ABAQUS, ANSYS, Mathematica,...
Software Engineer
Production Engineer
Manufacturing, Supply Chain
Creo View, Windchill MPMLink, Tecnomatix, SAP,...
Libraries / Databases
CAD models, cost models, analysis modules, parts and material databases, supplier database, ...
Systems Administrator
PLM and SCM Systems (Teamcenter, Windchill, GIT, SVN, ...)

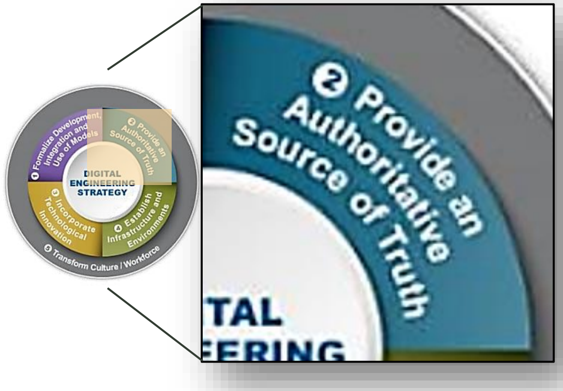


MBSE is a critical incorporation within Digital Engineering

MBSE SYSTEM INFORMATION VIEWS

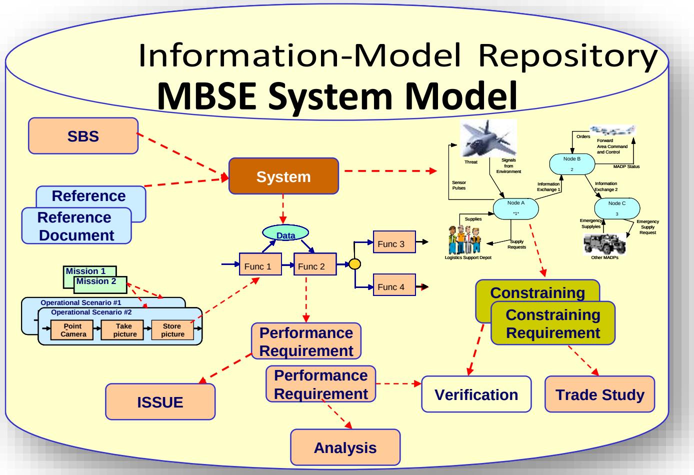
MBSE System Information Views

- Behavior
  - Mission and Stakeholder Requirements
  - System Functional Architecture
  - System States and Modes
  - Functional Allocations
- Structure
  - System Logical and Physical Architectures
  - External and Internal Interfaces and Definitions
- Requirements
  - System Requirements Definition
  - System Traceability Matrices
  - Verification Requirements
- Parametrics
  - Trade studies
  - Performance and design analysis calculations

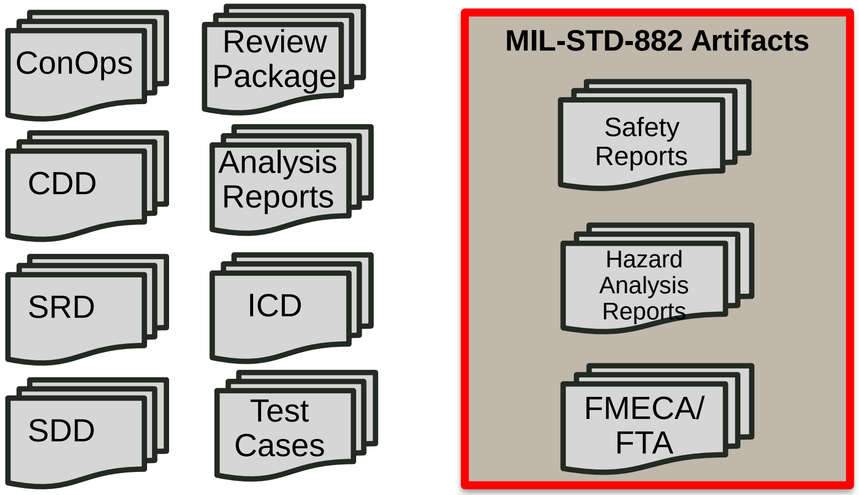


DIGITAL ENGINEERING STRATEGY
Formalize Development, Integration and Use of Models
Provide an Authoritative Source of Truth
Incorporate Technological Innovation
Establish Infrastructure and Environments
Transform Culture / Workforce
2 Provide an Authoritative Source of Truth
TAL
ERING

The MBSE System Model is the Authoritative Source of Truth



Developed using tools that support Systems Modeling Language (SysML)



ConOps

CDD

SRD

SDD

Review Package

Analysis Reports

ICD

Test Cases

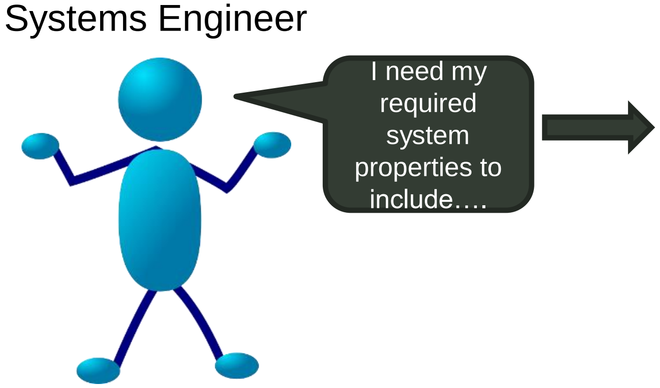
MIL-STD-882 Artifacts

Safety Reports

Hazard Analysis Reports

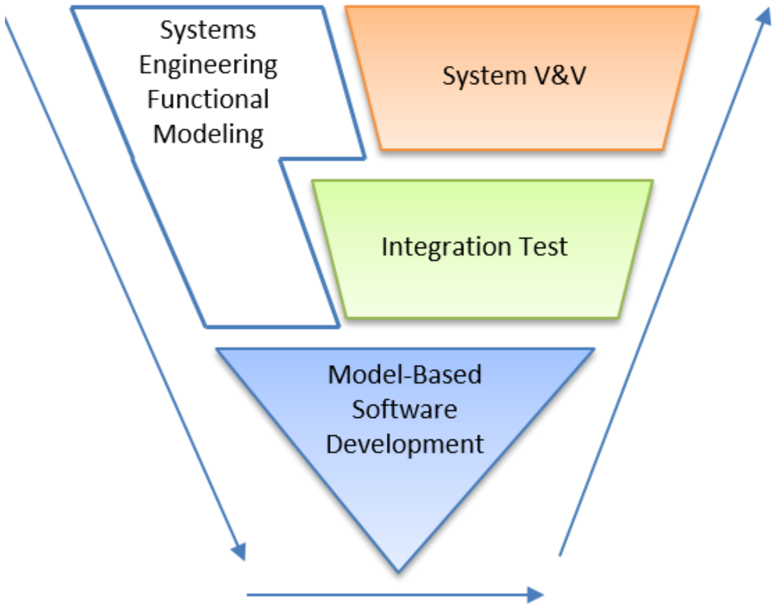
FMECA/ FTA

SYSTEMS AND SYSTEMS SAFETY ENGINEERING



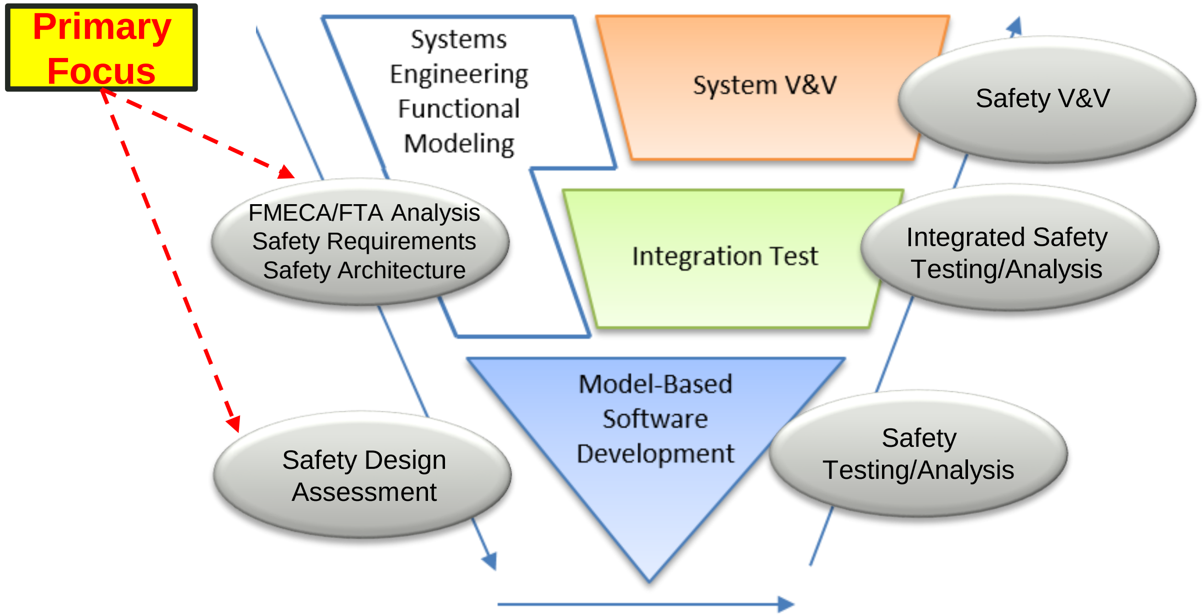
1. How my system interacts with its interfaces
2. The CONOPS and functionality of my system
3. The performance of my system
4. System Requirements
5. The system dependability constraints such as ***<u>Safety, Reliability,</u>*** and *Security*

SE V-Model (MBSE)


Systems Engineering Functional Modeling
System V&V
Integration Test
Model-Based Software Development

1. FMECA/FTA Modeling
2. Safety/RAM Requirements
3. Safety Design Analysis
4. Safety Reviews of Work Products
5. Safety Verification and Validation
6. ***<u>MIL-STD-882 Practices</u>***

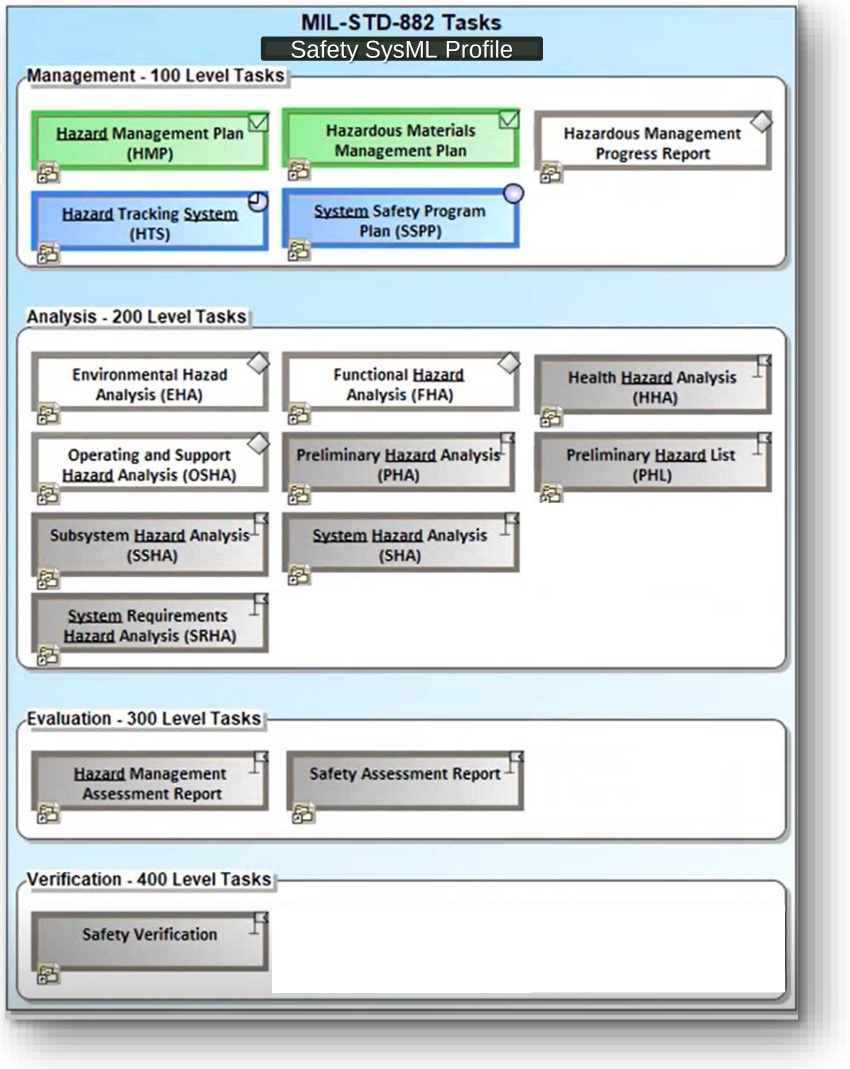
SE V-Model (Safety)



MIL-STD-882 REPRESENTATION IN MBSE MODEL

MIL-STD-882 Tasks (System Safety Standard Practices)

- 100 Level Tasks (Management)
  - Hazard Management Plans
  - Hazard Management Progress Reporting
  - System Safety Plans
- 200 Level Tasks (Analysis)
  - Hazard Analyses (FMECAs, FTAs, RAM Analysis)
  - Hazard Lists
  - System Safety Requirements Analysis
- 300 Level Tasks (Evaluation)
  - Safety Reports (Safety Assessment Reports (SAR))
- 400 Level Tasks (Verification)
  - Safety Verification (Test/Analysis Events)



MIL-STD-882 Tasks

Safety SysML Profile

Management - 100 Level Tasks

Hazard Management Plan (HMP)

Hazardous Materials Management Plan

Hazardous Management Progress Report

Hazard Tracking System (HTS)

System Safety Program Plan (SSPP)

Analysis - 200 Level Tasks

Environmental Hazad Analysis (EHA)

Functional Hazard Analysis (FHA)

Health Hazard Analysis (HHA)

Operating and Support Hazard Analysis (OSHA)

Preliminary Hazard Analysis (PHA)

Preliminary Hazard List (PHL)

Subsystem Hazard Analysis (SSHA)

System Hazard Analysis (SHA)

System Requirements Hazard Analysis (SRHA)

Evaluation - 300 Level Tasks

Hazard Management Assessment Report

Safety Assessment Report

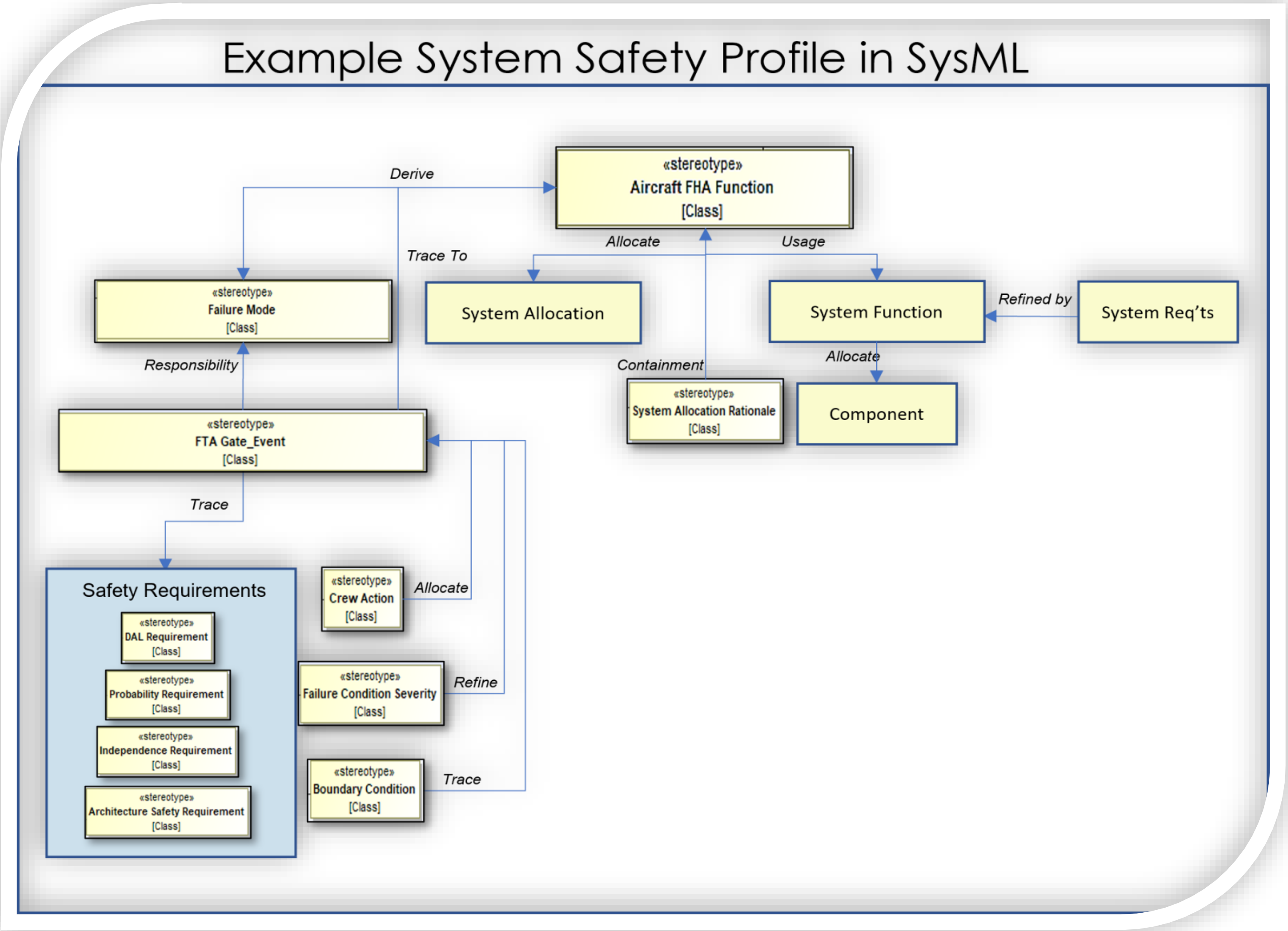
Verification - 400 Level Tasks

Safety Verification

SYSTEM SAFETY SYSTEMS MODELING (SYSML) PROFILES

SysML Profiles

- Cameo Safety and Reliability Analyzer Profile
- Risk Analysis and Assessment Modeling Language (RAAML)
  - Object Management Group (OMG) developed
  - Published March 2022
- Customizable Profiles based on Government-Furnished documentation (Profile Extension)



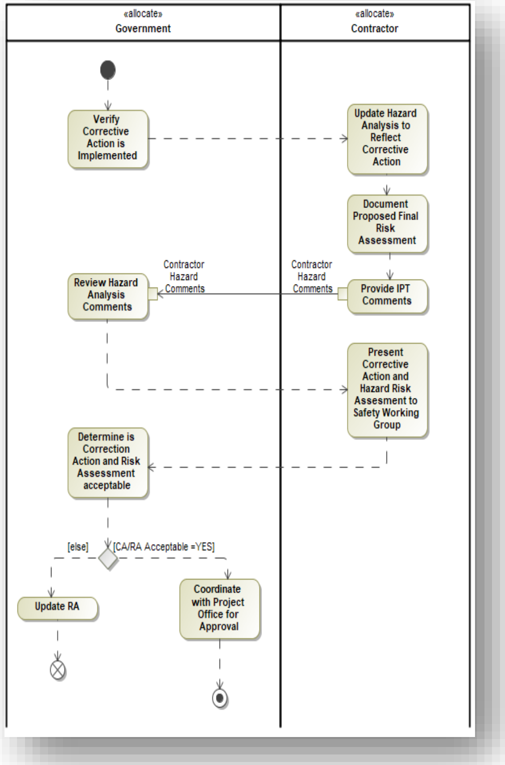
Example System Safety Profile in SysML

MBSE MIL-STD-882 100 LEVEL TASK EXAMPLE

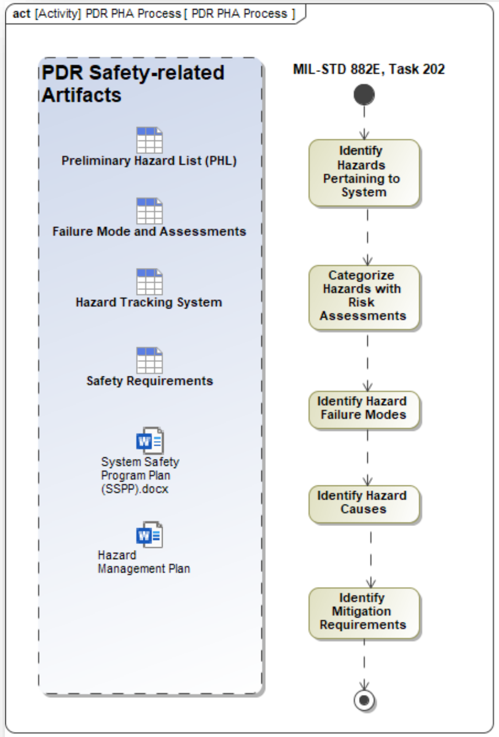
MIL-STD-882 100 Level Tasks

- Hazard Risk Assessment (HRA) Process
  - What processes are in my Hazardous Management Plan
  - How government and contractors support the HRA process
- PDR Preliminary Hazard Assessment (PHA) Process
  - What do I need for safety-related PDR artifacts
  - What steps do I perform to implement MIL-STD-882 Tasks
  - System Safety Requirements Analysis

Hazard Risk Assessment Process


«allocate»
Government
«allocate»
Contractor
Verify Corrective Action is Implemented
Update Hazard Analysis to Reflect Corrective Action
Document Proposed Final Risk Assessment
Contractor Hazard Comments
Review Hazard Analysis Comments
Contractor Hazard Comments
Provide IPT Comments
Present Corrective Action and Hazard Risk Assesment to Safety Working Group
Determine is Correction Action and Risk Assessment acceptable
[else]
[CA/RA Acceptable =YES]
Update RA
Coordinate with Project Office for Approval

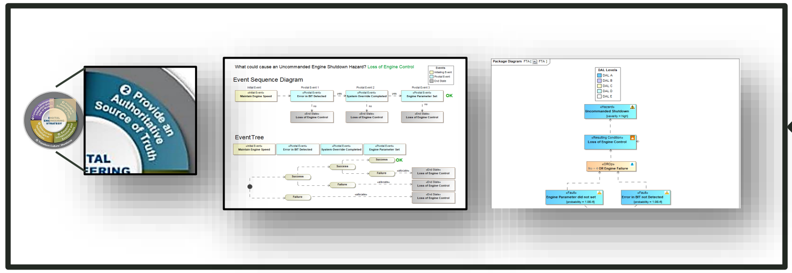
PDR Preliminary Hazard Assessment (PHA) Process


act [Activity] PDR PHA Process [PDR PHA Process]
PDR Safety-related Artifacts
Preliminary Hazard List (PHL)
Failure Mode and Assessments
Hazard Tracking System
Safety Requirements
System Safety Program Plan (SSPP).docx
Hazard Management Plan
MIL-STD 882E, Task 202
Identify Hazards Pertaining to System
Categorize Hazards with Risk Assessments
Identify Hazard Failure Modes
Identify Hazard Causes
Identify Mitigation Requirements

MBSE MIL-STD-882 200 LEVEL TASK EXAMPLE (1 OF 3)

MIL-STD-882 200 Level Tasks

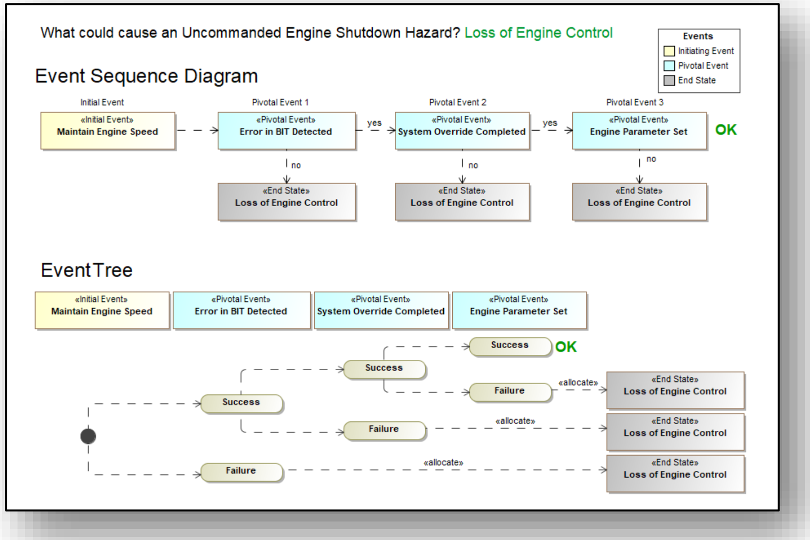
- Hazard Analysis
  - Event Tree/Sequence Diagram
  - Fault Tree Analysis (FTA)
  - We have tools that do this already
    - MBSE Integration opportunity between MBSE System Model and current hazard analysis tools
    - Where can we establish tool integration touch points between digital model elements



MBSE Integration

Existing Safety Analysis Tools

❶ Formalize Development, Integration and Use of Models
❷ Provide an Authoritative Source of Truth
DIGITAL ENGINEERING STRATEGY
❸ Incorporate Technological Innovation
❹ Establish Infrastructure and Environments
❺ Transform Culture / Workforce
❷ Provide an Authoritative Source of Truth
TAL
ERING



What could cause an Uncommanded Engine Shutdown Hazard? Loss of Engine Control

Events
- ▢ Initiating Event
- ▢ Pivotal Event
- ▢ End State

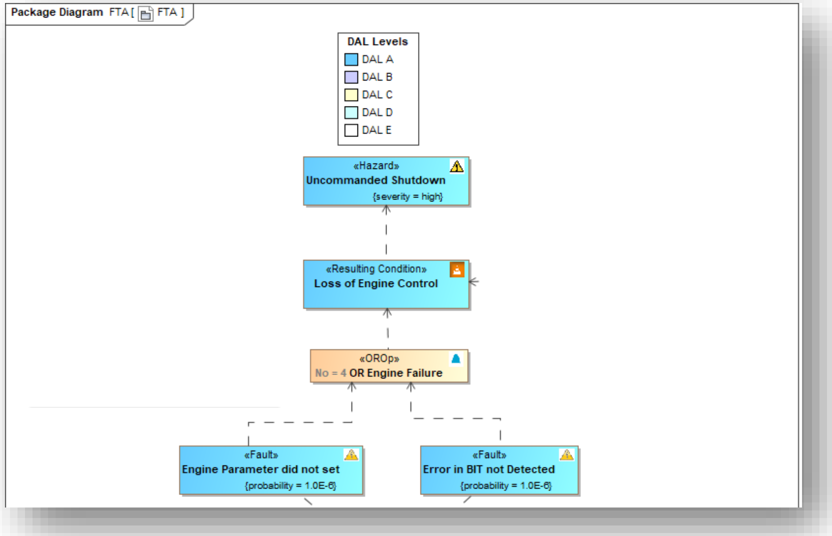
Event Sequence Diagram

Initial Event: «Initial Event» Maintain Engine Speed
Pivotal Event 1: «Pivotal Event» Error in BIT Detected
yes
Pivotal Event 2: «Pivotal Event» System Override Completed
yes
Pivotal Event 3: «Pivotal Event» Engine Parameter Set
OK
no: «End State» Loss of Engine Control
no: «End State» Loss of Engine Control
no: «End State» Loss of Engine Control

EventTree

«Initial Event» Maintain Engine Speed
«Pivotal Event» Error in BIT Detected
«Pivotal Event» System Override Completed
«Pivotal Event» Engine Parameter Set

Success
Success
Success OK
Failure «allocate» «End State» Loss of Engine Control
Failure «allocate» «End State» Loss of Engine Control
Failure «allocate» «End State» Loss of Engine Control



Package Diagram FTA [FTA]

DAL Levels
- ▢ DAL A
- ▢ DAL B
- ▢ DAL C
- ▢ DAL D
- ▢ DAL E

«Hazard» Uncommanded Shutdown {severity = high}
«Resulting Condition» Loss of Engine Control
«OROp» No = 4 OR Engine Failure
«Fault» Engine Parameter did not set {probability = 1.0E-6}
«Fault» Error in BIT not Detected {probability = 1.0E-6}

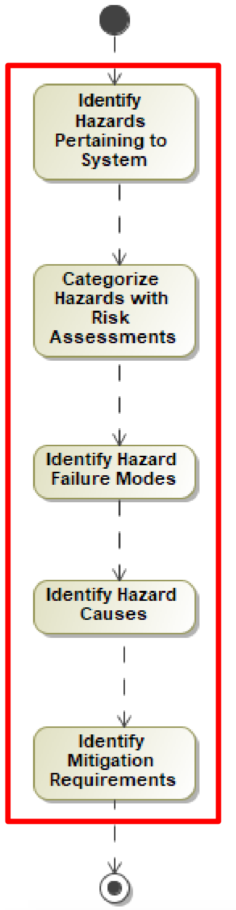
MBSE MIL-STD-882 200 LEVEL TASK EXAMPLE (2 OF 3)

MIL-STD-882 200 Level Tasks

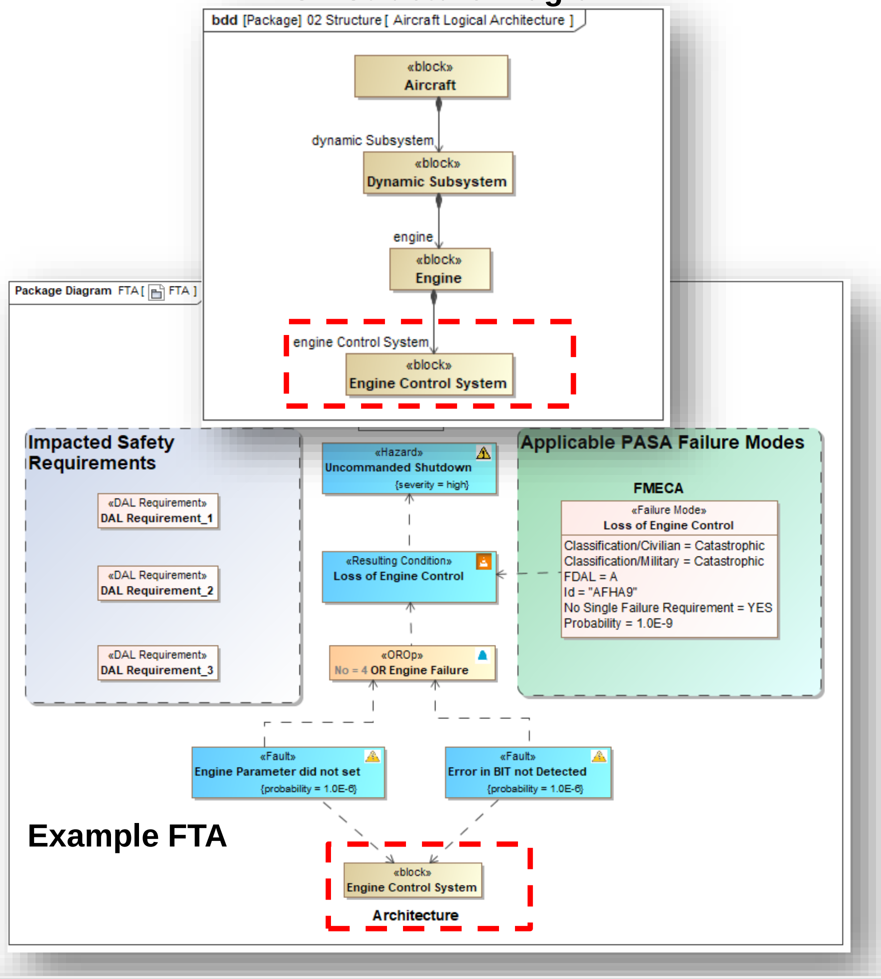
- Hazard Identification and tracking
- Identify failure modes within FTA
- Categorization of Failure Modes
  - Risk Assessments
  - DAL Assessments
- Safety requirement effectivity to FTA/FMECAs
- System Architecture fault allocations

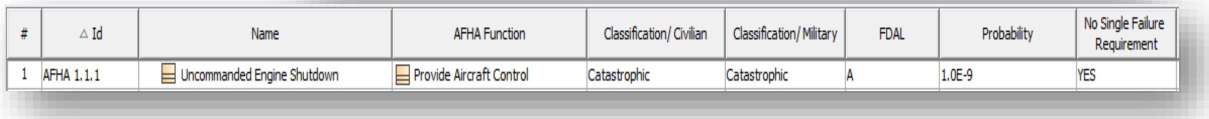
System Logical/Physical Architectures goes hand-in-hand with system safety processes.

MIL-STD 882E, Task 202


Identify Hazards Pertaining to System
Categorize Hazards with Risk Assessments
Identify Hazard Failure Modes
Identify Hazard Causes
Identify Mitigation Requirements

MBSE Structure Diagram


bdd [Package] 02 Structure [Aircraft Logical Architecture]
«block» Aircraft
dynamic Subsystem
«block» Dynamic Subsystem
engine
«block» Engine
engine Control System
«block» Engine Control System
Package Diagram FTA [FTA]
Impacted Safety Requirements
«DAL Requirement» DAL Requirement_1
«DAL Requirement» DAL Requirement_2
«DAL Requirement» DAL Requirement_3
«Hazard» Uncommanded Shutdown {severity = high}
«Resulting Condition» Loss of Engine Control
«OROp» No = 4 OR Engine Failure
Applicable PASA Failure Modes
FMECA
«Failure Mode» Loss of Engine Control
Classification/Civilian = Catastrophic
Classification/Military = Catastrophic
FDAL = A
Id = "AFHA9"
No Single Failure Requirement = YES
Probability = 1.0E-9
«Fault» Engine Parameter did not set {probability = 1.0E-6}
«Fault» Error in BIT not Detected {probability = 1.0E-6}
Example FTA
«block» Engine Control System
Architecture



#	△ Id	Name	AFHA Function	Classification/ Civilian	Classification/ Military	FDAL	Probability	No Single Failure Requirement
1	AFHA 1.1.1	Uncommanded Engine Shutdown	Provide Aircraft Control	Catastrophic	Catastrophic	A	1.0E-9	YES

MBSE MIL-STD-882 200 LEVEL TASK EXAMPLE (3 OF 3)

MIL-STD-882 200 Level Tasks

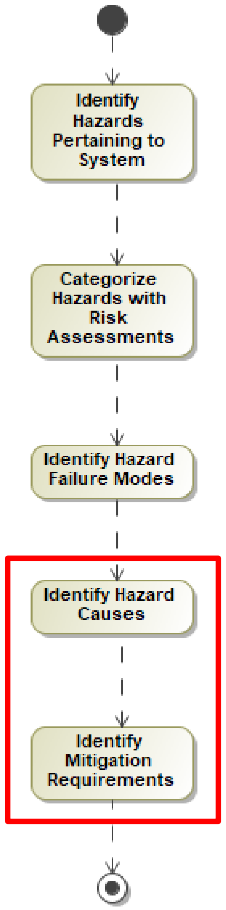
- Mitigation Requirements Analysis
  - Analyzing functionality of the system to determine potential failure causes that contribute to hazards
  - MBSE provides the capability to support “identify mitigation requirements” within the documented PDR PHA Process

System Functional Architecture

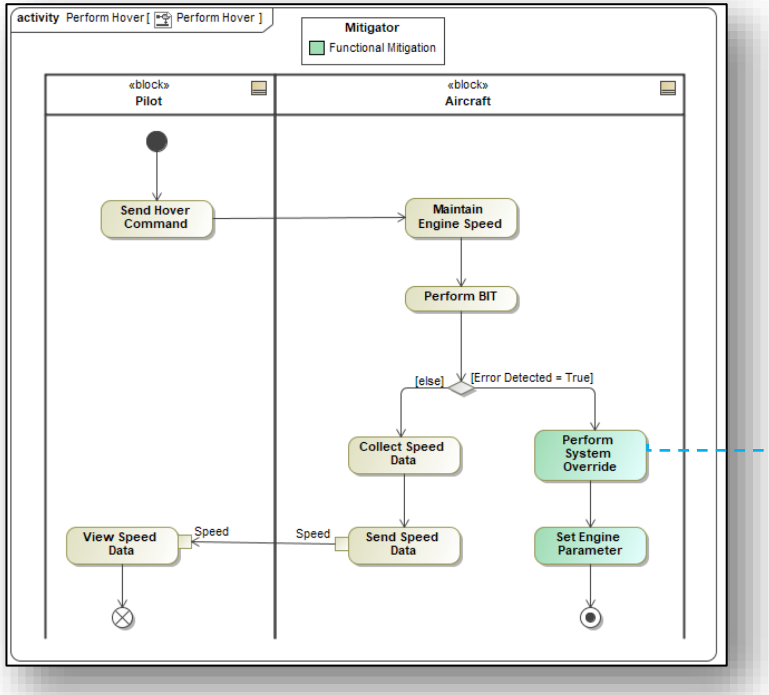
System Safety Process

System Functional Architecture goes hand-in-hand with system safety processes

MIL-STD 882E, Task 202


Identify Hazards Pertaining to System
Categorize Hazards with Risk Assessments
Identify Hazard Failure Modes
Identify Hazard Causes
Identify Mitigation Requirements

MBSE Behavior Diagram



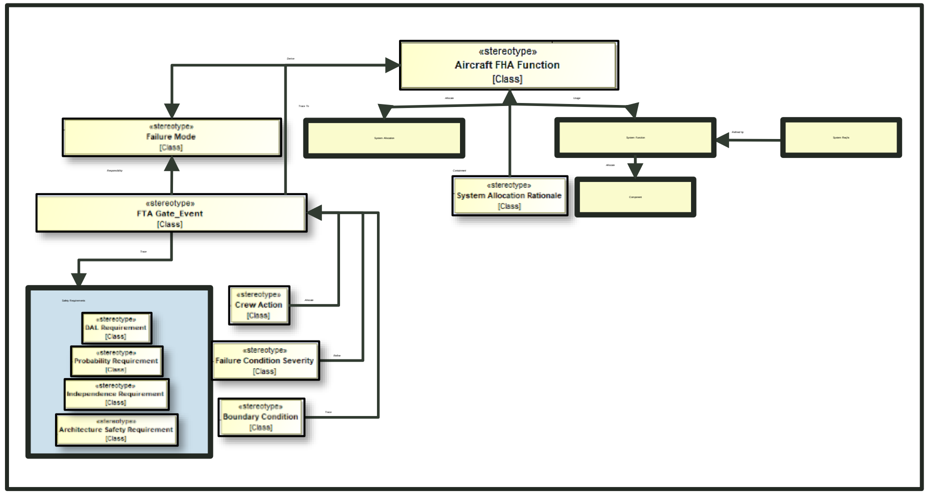
Mitigation Requirements (Functional):
When an error is detected during an engine BIT during hover, the system shall *perform a system override*.

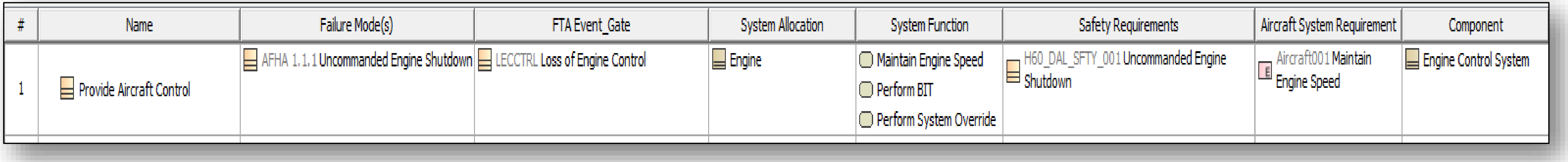
EXAMPLE AIRCRAFT FHA MODEL TRACE TABLE

Aircraft FHA Function Trace Table

- Traceable Safety attributes
  - ✓ Aircraft Mission Critical Functions
  - ✓ Failure Modes
  - ✓ FTA Events
  - ✓ System Allocations
  - ✓ System Functions
  - ✓ System Requirements
  - ✓ Safety Requirements
  - ✓ System Architecture

Example System Safety Profile in SysML





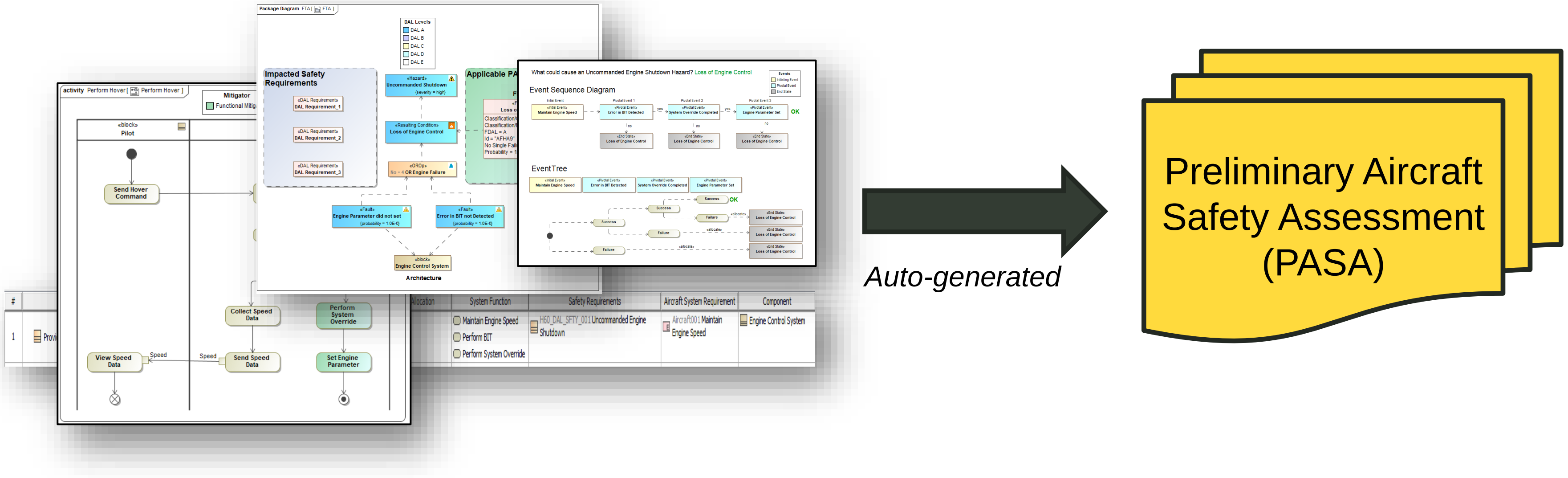
#	Name	Failure Mode(s)	FTA Event_Gate	System Allocation	System Function	Safety Requirements	Aircraft System Requirement	Component
1	Provide Aircraft Control	AFHA 1.1.1 Uncommanded Engine Shutdown	LECCTRL Loss of Engine Control	Engine	Maintain Engine Speed Perform BIT Perform System Override	H60_DAL_SFTY_001 Uncommanded Engine Shutdown	Aircraft001 Maintain Engine Speed	Engine Control System

MBSE enables dynamic change propagation rather than manual.

MBSE MIL-STD-882 300 LEVEL TASK EXAMPLE

MIL-STD-882 300 Level Tasks

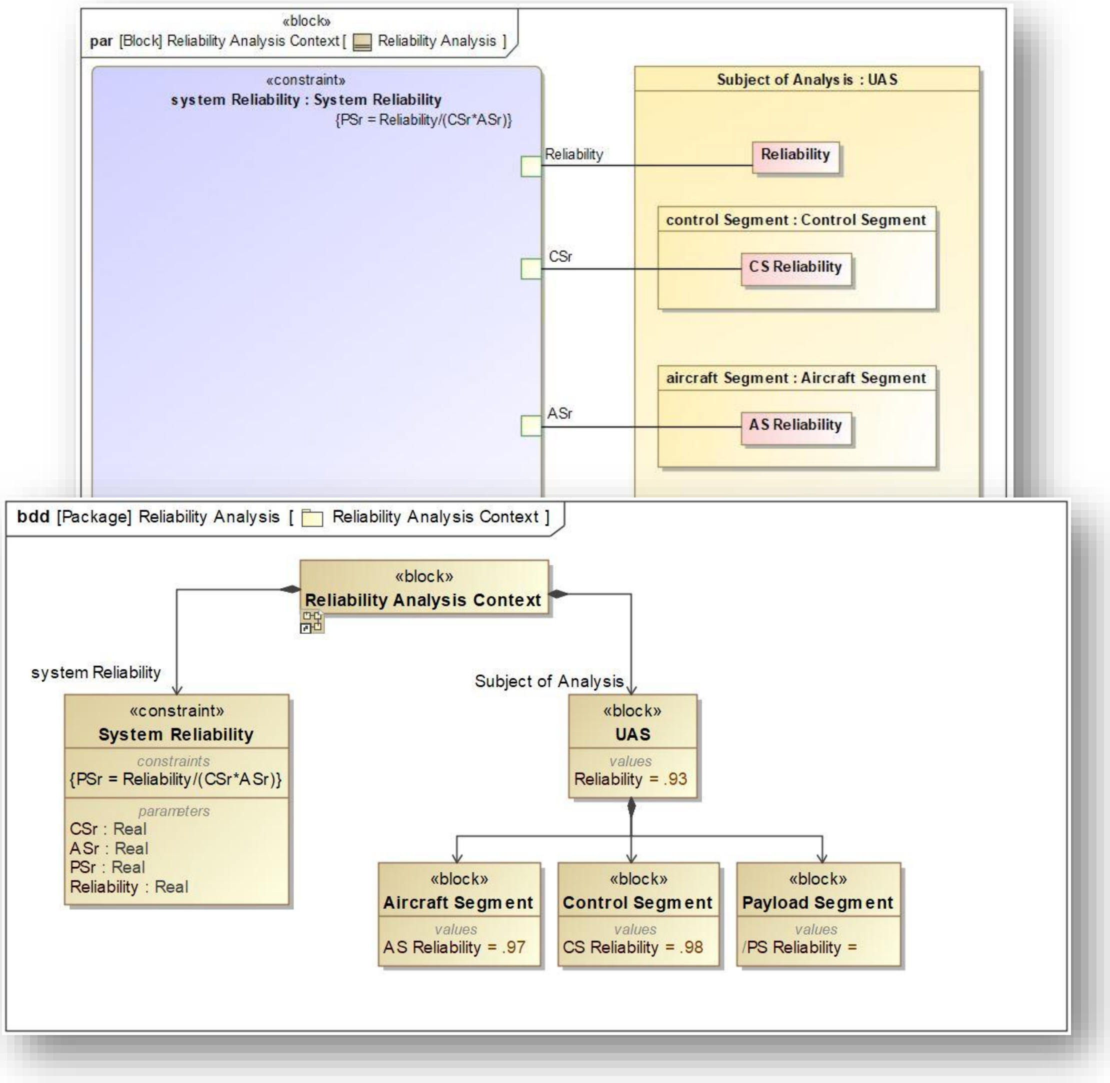
- Generate model integrated data into safety assessment reports (PASAs, PSSAs)
- Base generated documentation on templates



MBSE enables auto-generated documentation from model data.

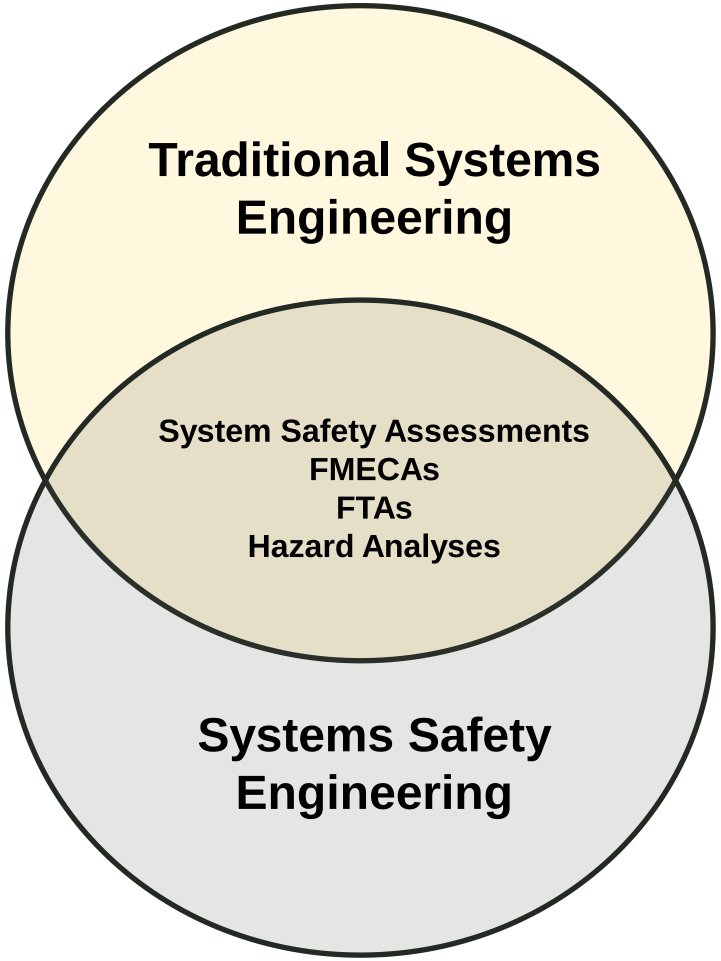
RELIABILITY PARAMETRIC ANALYSIS

- MBSE Parametric Views
  - Define System of Interest (SOI) mathematical constraints
  - Contain
    - Constraint block – Mathematical equations for reliability calculations
    - Constraint Parameters – used for calculating the equation
    - Value Properties – Represent model elements value (calculated or pre-defined)
    - Binding Connector – Links Constraint Parameters to Value Properties
  - Works in conjunction with an analysis context (Structure)
  - Supports MATLAB Integration



SUMMARY

- Successful robust System Safety Analysis requires the implementation of DoD Digital Engineering strategies using MBSE
- Bridging the gap between Traditional Systems Engineering and System Safety Engineering improves how we document system information
- MBSE provides the mechanism to produce MIL-STD-882 artifacts from a systems model


Traditional Systems Engineering
System Safety Assessments
FMECAs
FTAs
Hazard Analyses
Systems Safety Engineering

Web Site

www.avmc.army.mil

Facebook

www.facebook.com/ccdc.avm

Instagram

www.instagram.com/CCDC_AVM

Twitter

@CCDC_AVM

Public Affairs

usarmy.redstone.ccdc-avmc.mbx.pao@mail.mil