NAVAL ORDNANCE SAFETY & SECURITY ACTIVITY

3 November 2022

#24622 - Implementation Guide: Model-Based Systems Engineering (MBSE) for System Safety

Mr. Trung Hoang – NOSSA, N32D
trung.d.hoang2.civ@us.navy.mil

Mr. Robert Smith, CSP – Booz Allen Hamilton
smith_bob@bah.com / robert.e.smith1725.ctr@us.navy.mil

Approved for public release. Distribution is unlimited

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

Background – MBSE for System Safety

- System Safety is the application of engineering and management principles, criteria, and techniques to achieve acceptable safety risk within the constraints of operation effectiveness and suitability, time and cost throughout all phases of the system life-cycle.
  - Identify Hazards
  - Assess and Mitigate associated safety risk
  - Track, Control, Accept, and document safety risks
- Safety Community shall embrace Digital Engineering tools utilized by Engineering to facilitate safety assessments and risk characterization to efficiently support a rapid and accelerated program while maintaining the established safety principles that ensure the development and delivery of a safe systems.
  - Allows System Safety to be part of the DEVSECOP cycle
  - Enable streamline process, documentation and analyses
  - Tracking of safety risks, mitigations and verifications throughout the life cycle
  - Provide a single source of truth for all aspects of a system

Goals of MBSE - System Safety Implementation Guide

- Provide guidance to Program Managers to incorporate system safety programs into their MBSE driven programs
- Provide guidance to System, Software, and MBSE engineers on processes and tasks necessary to integrate system safety into program using MBSE
- Provide guidance to System Safety Engineering on how to execute their MIL-STD-882E tasks and applicable Level of Rigor (LOR) tasks in an MBSE environment
- Provide guidance to Review boards and stakeholders on providing, reviewing, and assessing Objective Quality Evidences from MBSE based programs
- Provide basic MBSE System Safety metamodel to highlight the architecture, rules, constraints, and models that are applicable and useful for safety practitioners

MBSE SSIG History

WSESRB Off-site Aug 2021

- MBSE analyses derived from WSESRB SOAR Workshop

Sep - Oct 2021

- POA&M for MBSE analyses
- Draft MBSE analyses White Paper

JWSWG Nov 2021

- Established Joint MBSE Working Group (bi-weekly)
  - NOSSA
  - OUSD (Specialty Engineering)
  - Army (Huntsville)
  - NSWCDD Safety

Dec 21 – Jan 22

- Scope focus on MBSE SSIG
- NAVAIR joined MBSE WG
- MBSE SSIG will included two end products
  - System Safety Implementation Guide
  - System Safety Metamodel (sandbox)

Feb 22 – Nov 22

- Development of the sandbox (on going)
- Air Force Joined MBSE WG
- Splinter Group Established to support the demand workloads

Today

- Provide MBSE SSIG Status
- Path forward into FY23

MBSE Working Group Overview

- Joint DoD MBSE analyses effort initiated by Joint Weapon Safety Working Group (JWSWG) in September 2021, MBSE Working Group established in November 2021
  - Members include System Safety, MBSE, Systems Engineering SMEs
  - Representatives from OSD, Navy, Army, Air Force
    - Membership is currently DoD and DoD Contractors
    - Will expand membership to include Industry representatives
    - ~50 members (as of November 2022)
- Two (2) recurring meetings
  - Bi-weekly MBSE Working Group
  - Weekly MBSE Splinter Working Group

Joint DoD Effort to meet Digital Engineering Requirement

Implementation (High Level) Overview

- Establish Ground Rules and Expectations
  - Maintain requirements of MIL-STD-882E
  - Understand the processes and methodologies of System Safety Program Plans
    - Prepare safety artifact formats and templates
- Communication
  - Need to communicate system safety needs/wants to MBSE developers
    - System Safety analysis process, methodology, and templates
  - System Safety needs to have a general understanding of the MBSE tools and SysML
- Collaboration
  - System Safety needs to collaborate with MBSE to understand the basics of the System model in the digital engineering tool
  - System Safety needs to interact with MBSE, Systems Engineering, Software Engineering , and other Stakeholders in order understand system information that is available
  - System Safety is “data hungry” and requires data to fully assess the system(s) under analysis
    - E.g., OV-1 diagram, Functional Block Diagram, Interface Block Diagrams, Requirements, Design Architecture, Schematics, etc.

Communication and Collaboration

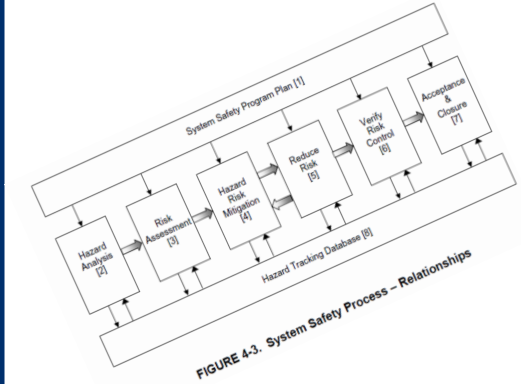


FIGURE 4-3. System Safety Process – Relationships

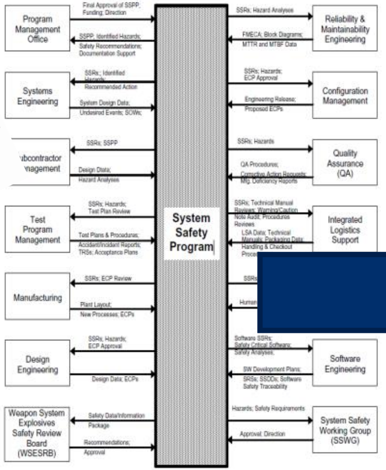

Program Management Office
Systems Engineering
Subcontractor Management
Test Program Management
Manufacturing
Design Engineering
Weapon System Explosives Safety Review Board (WSESRB)
System Safety Program
Reliability & Maintainability Engineering
Configuration Management
Quality Assurance (QA)
Integrated Logistics Support
Software Engineering
System Safety Working Group (SSWG)
Final Approval of SSPP; Funding; Direction
SSPP; Identified Hazards; Safety Recommendations; Documentation Support
SSRs; Hazard Analyses
FMECA; Block Diagrams; MTTR and MTBF Data
SSRs; Hazards; ECP Approval
Engineering Release; Proposed ECPs
SSRs; Hazards
QA Procedures; Corrective Action Requests; Mfg. Deficiency Reports
Software SSRs; Safety Critical Software; Safety Analyses
SW Development Plans; SRSs; SSDDs; Software Safety Traceability
Hazards; Safety Requirements
Approval; Direction
Safety Data/Information Package
Recommendations; Approval

FIGURE 4-5. Major SSP Interfaces and Data Exchange

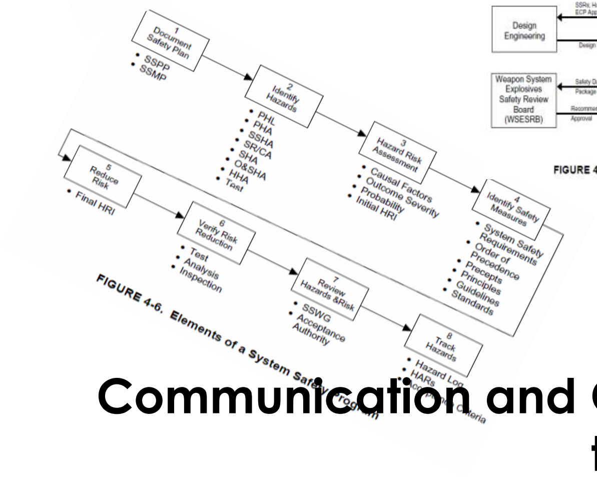
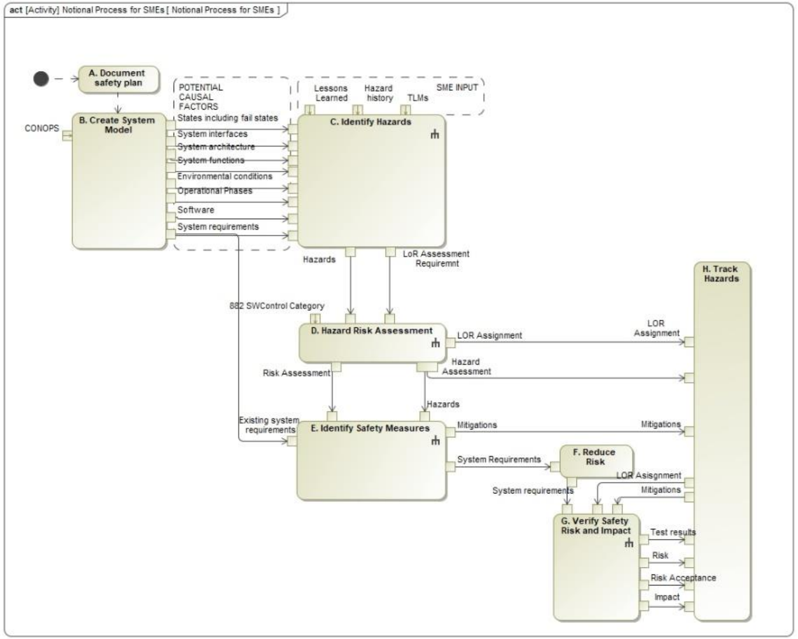


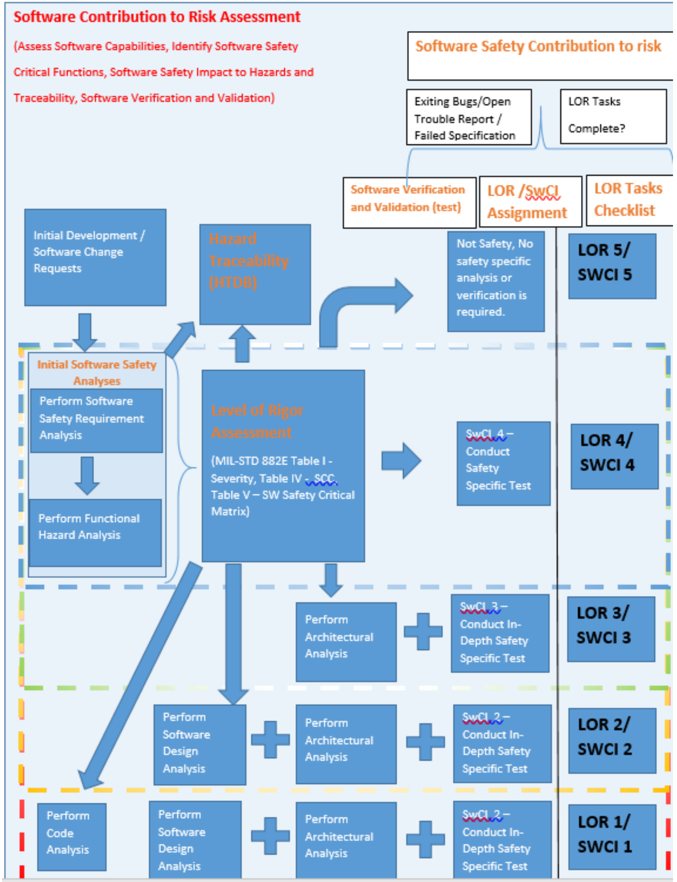
FIGURE 4-6. Elements of a System Safety Program



Communication and Collaboration are key to success throughout the program's lifecycle

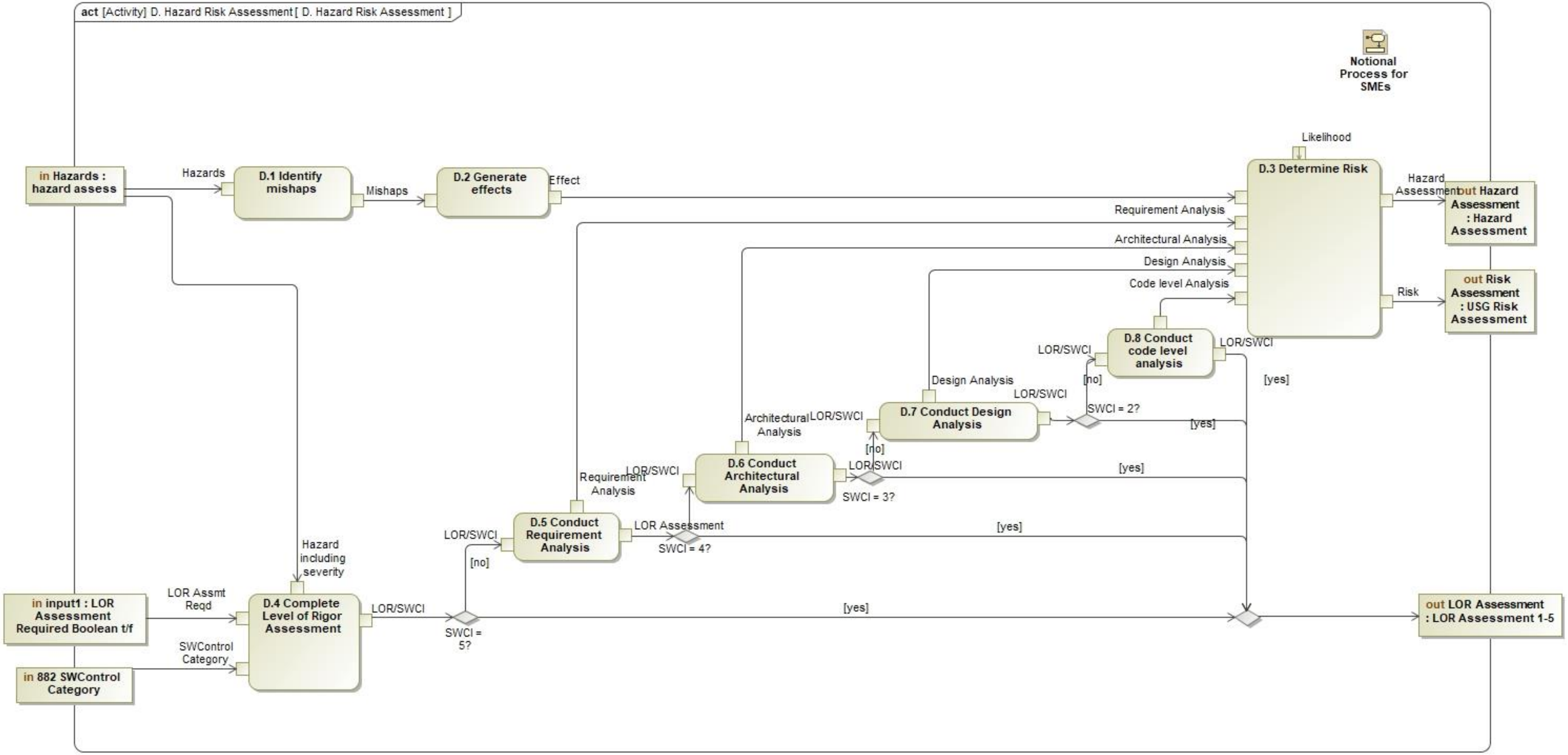
NOSSA

Example – Software Level of Rigor Process

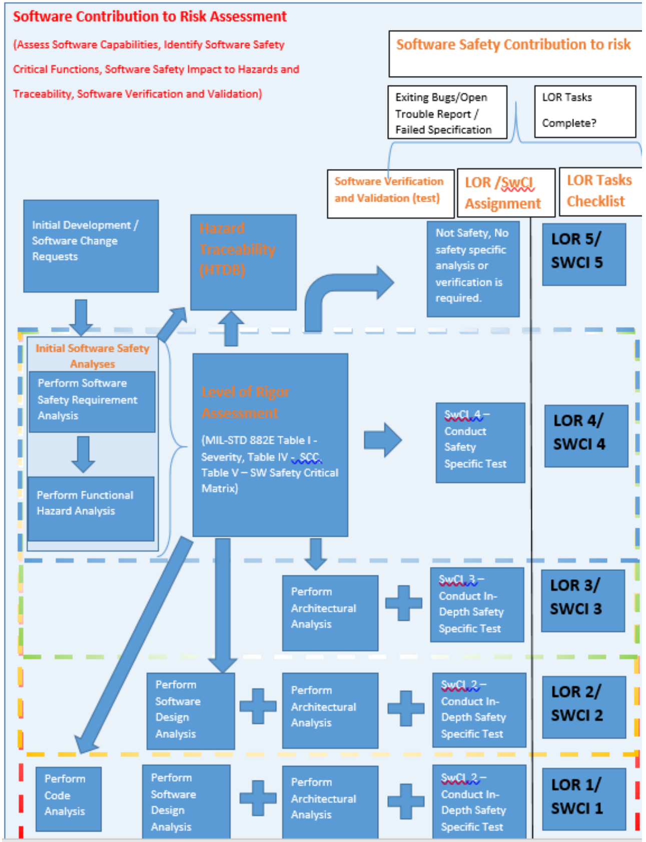

Software Contribution to Risk Assessment
(Assess Software Capabilities, Identify Software Safety Critical Functions, Software Safety Impact to Hazards and Traceability, Software Verification and Validation)
Software Safety Contribution to risk
Exiting Bugs/Open Trouble Report / Failed Specification
LOR Tasks Complete?
Software Verification and Validation (test)
LOR /SwCI Assignment
LOR Tasks Checklist
Initial Development / Software Change Requests
Hazard Traceability (HTDB)
Not Safety, No safety specific analysis or verification is required.
LOR 5/ SWCI 5
Initial Software Safety Analyses
Perform Software Safety Requirement Analysis
Perform Functional Hazard Analysis
Level of Rigor Assessment
(MIL-STD 882E Table I - Severity, Table IV - SCC, Table V – SW Safety Critical Matrix)
SwCI 4 – Conduct Safety Specific Test
LOR 4/ SWCI 4
Perform Architectural Analysis
SwCI 3 – Conduct In-Depth Safety Specific Test
LOR 3/ SWCI 3
Perform Software Design Analysis
Perform Architectural Analysis
SwCI 2 – Conduct In-Depth Safety Specific Test
LOR 2/ SWCI 2
Perform Code Analysis
Perform Software Design Analysis
Perform Architectural Analysis
SwCI 2 – Conduct In-Depth Safety Specific Test
LOR 1/ SWCI 1

- Software Safety Level of Rigor (LOR) provides a depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence for software's contribution to risk
  - Use as a Objective Qualitative Evidence (OQE) to support safety case or rationale
  - Demonstrate the software safety process to independent review boards, other program engineering activities, and/or stakeholders from a System Safety perspective

Example – Software Level of Rigor Process


act [Activity] D. Hazard Risk Assessment[D. Hazard Risk Assessment]
Notional Process for SMEs
in Hazards : hazard assess
Hazards
D.1 Identify mishaps
Mishaps
D.2 Generate effects
Effect
Likelihood
D.3 Determine Risk
Requirement Analysis
Architectural Analysis
Design Analysis
Code level Analysis
Hazard Assessment
out Hazard Assessment : Hazard Assessment
Risk
out Risk Assessment : USG Risk Assessment
LOR/SWCI
D.8 Conduct code level analysis
LOR/SWCI
[no]
[yes]
Design Analysis
LOR/SWCI
SWCI = 2?
D.7 Conduct Design Analysis
[yes]
Architectural Analysis
LOR/SWCI
[no]
D.6 Conduct Architectural Analysis
LOR/SWCI
[yes]
SWCI = 3?
Requirement Analysis
LOR/SWCI
D.5 Conduct Requirement Analysis
LOR Assessment
[yes]
SWCI = 4?
LOR/SWCI
[no]
Hazard including severity
in input1 : LOR Assessment Required Boolean t/f
LOR Assmt Reqd
D.4 Complete Level of Rigor Assessment
LOR/SWCI
SWCI = 5?
[yes]
out LOR Assessment : LOR Assessment 1-5
SWControl Category
in 882 SWControl Category

Example – Software Level of Rigor Process



Software Contribution to Risk Assessment

(Assess Software Capabilities, Identify Software Safety Critical Functions, Software Safety Impact to Hazards and Traceability, Software Verification and Validation)

Software Safety Contribution to risk

Exiting Bugs/Open Trouble Report / Failed Specification

LOR Tasks Complete?

Software Verification and Validation (test)

LOR /SwCI Assignment

LOR Tasks Checklist

Initial Development / Software Change Requests

Hazard Traceability (HTDB)

Not Safety, No safety specific analysis or verification is required.

LOR 5/ SWCI 5

Initial Software Safety Analyses

Perform Software Safety Requirement Analysis

Perform Functional Hazard Analysis

Level of Rigor Assessment

(MIL-STD 882E Table I - Severity, Table IV - SCC, Table V – SW Safety Critical Matrix)

SwCI 4 – Conduct Safety Specific Test

LOR 4/ SWCI 4

Perform Architectural Analysis + SwCI 3 – Conduct In-Depth Safety Specific Test

LOR 3/ SWCI 3

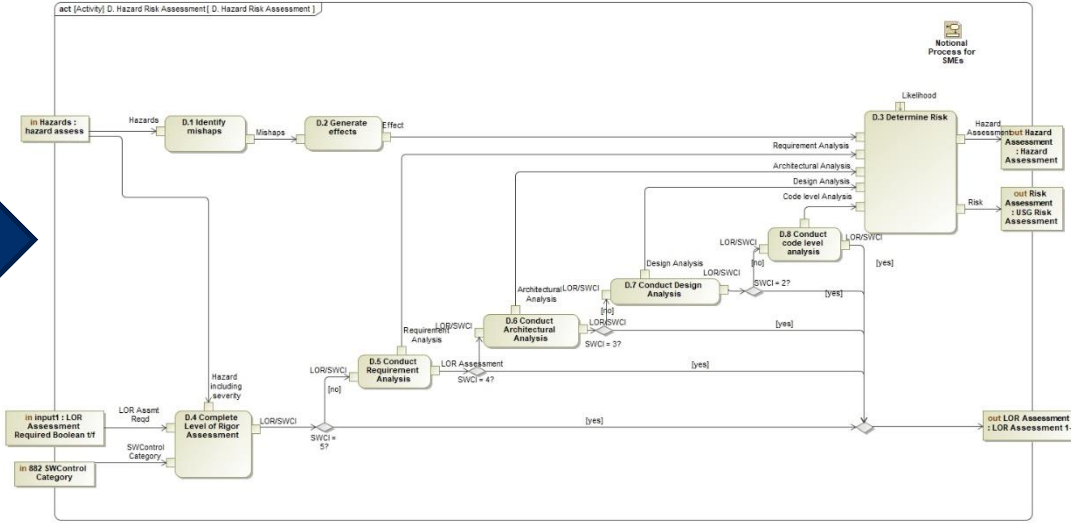
Perform Software Design Analysis + Perform Architectural Analysis + SwCI 2 – Conduct In-Depth Safety Specific Test

LOR 2/ SWCI 2

Perform Code Analysis

Perform Software Design Analysis + Perform Architectural Analysis + SwCI 2 – Conduct In-Depth Safety Specific Test

LOR 1/ SWCI 1


act [Activity] D. Hazard Risk Assessment [D. Hazard Risk Assessment]
Notional Process for SMEs
in Hazards : hazard assess
Hazards
D.1 Identify mishaps
Mishaps
D.2 Generate effects
Effect
Likelihood
D.3 Determine Risk
Requirement Analysis
Architectural Analysis
Design Analysis
Code level Analysis
Hazard Assessment
out Hazard Assessment : Hazard Assessment
Risk
out Risk Assessment : USG Risk Assessment
D.8 Conduct code level analysis
LOR/SWCI
[no]
[yes]
Design Analysis
D.7 Conduct Design Analysis
SWCI = 2?
Architectural Analysis
D.6 Conduct Architectural Analysis
SWCI = 3?
Requirement Analysis
D.5 Conduct Requirement Analysis
LOR Assessment
SWCI = 4?
Hazard including severity
in input1 : LOR Assessment Required Boolean t/f
LOR Assmt Reqd
D.4 Complete Level of Rigor Assessment
SWControl Category
in 882 SWControl Category
SWCI = 5?
out LOR Assessment : LOR Assessment 1-

- Safety Process is within MBSE Model
- Enhancement can be made to incorporate integration features with Software Engineering Team to allow a **single source of truth**
- Could serve as LOR OQE to provide to the Review Board to substantiate adequate completion of LOR

Challenges and Lessons Learned (so far)

- Maintaining System Safety perspective of “out-of-the-box” thinking for thorough safety analyses and risk characterization
  - MBSE provides a design perspective, limited operational perspective
- Communication between MBSE and System Safety
  - Need to cross reference of terminology between MBSE vs. System Safety vernacular
- Maintaining Configuration Management (CM) of models
  - Best to work in Teamwork Cloud environment to maintain CM
  - Safety Analyses are typically a snapshot in time, need to determine CM for organic, real-time data
- Determine if safety data will be fully digitized via Dashboard or exported to document file(s) (e.g., MSWord, Excel)
  - Need to have system safety dashboard (“Start Here”) to ensure external stakeholders can easily navigate models (containment trees, diagram trees, structure trees)
- Ability for all users to adapt and evolve from entrenched processes
  - Need to develop best practices for reviewing System Design information in DE environment
  - System Safety needs to learn from MBSE and Systems Engineering SMEs, and MBSE SMEs need to learn from System Safety
  - Instead of having separate hazards analyses such as a PHA, SRHA, FHA, SHA, SSHA, HHA, and O&SHA, have a single real-time Hazard Analysis that assesses all attributes of the 882E tasks in the digital engineering environment to gain efficiencies while not sacrificing system safety analysis rigor
- Need to know desired outputs from other engineering activities in order to be effective in MBSE environment
  - Integration between engineering activities and MBSE developers
  - Cross-engineering traceability between hazards, mitigations, system requirements, tests, verification, etc.

Challenges are being identified and understood
Our goal is to address these challenges in the Implementation Guide

Activities

- Phase 1 (Near-term)
  - Integrate into mock-up model to validate safety model and methodologies
    - Ensure safety attributes can be documented and tracked in model
    - FHA Template/Worksheet can be exported and viewed by third party reviewer
    - Interface Data can be cross-referenced with the model
  - Using Safety Sandbox to conduct "partial" Functional Hazard Analysis (FHA)
  - Developing System Safety Dashboard (landing page)
  - Complete Draft MBSE System Safety Implementation Guide (SSIG) to document lessons-learned, challenges, and recommendations for successful System Safety Program execution in MBSE environment
  - Draft MBSE SSIG to be reviewed and vetted through JWSWG

- Phase 2 (Future)
  - Expand Safety Sandbox to include more safety analysis tasks and Hazard Tracking System (HTS)
  - Collaborate with Warfare Centers to create plans for Workforce Development and training
  - Promulgate current MBSE SSIG for guidance to DoD and Industry

Summary & Conclusion

- MBSE Implementation Guide is a joint effort from all services and will be released under DOD documentation
- The objective of the Implementation Guide is to ease the system safety adaptation/transition to MBSE
- Both MBSE Implementation Guidance documentation and sand box model will be made available for all stakeholders once released
- New members (MBSE developers) are welcome to support the working groups
  - To include expanding MBSE Working Group Membership to Industry representatives to leverage best practices / lessons learned

NOSSA

Questions/Answers