U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – ARMAMENTS CENTER

Safe from the Start: Using MBSE for Safety Engineering

Ms. Daisy Bower & Ms. Kate Kovalovsky

System Architects

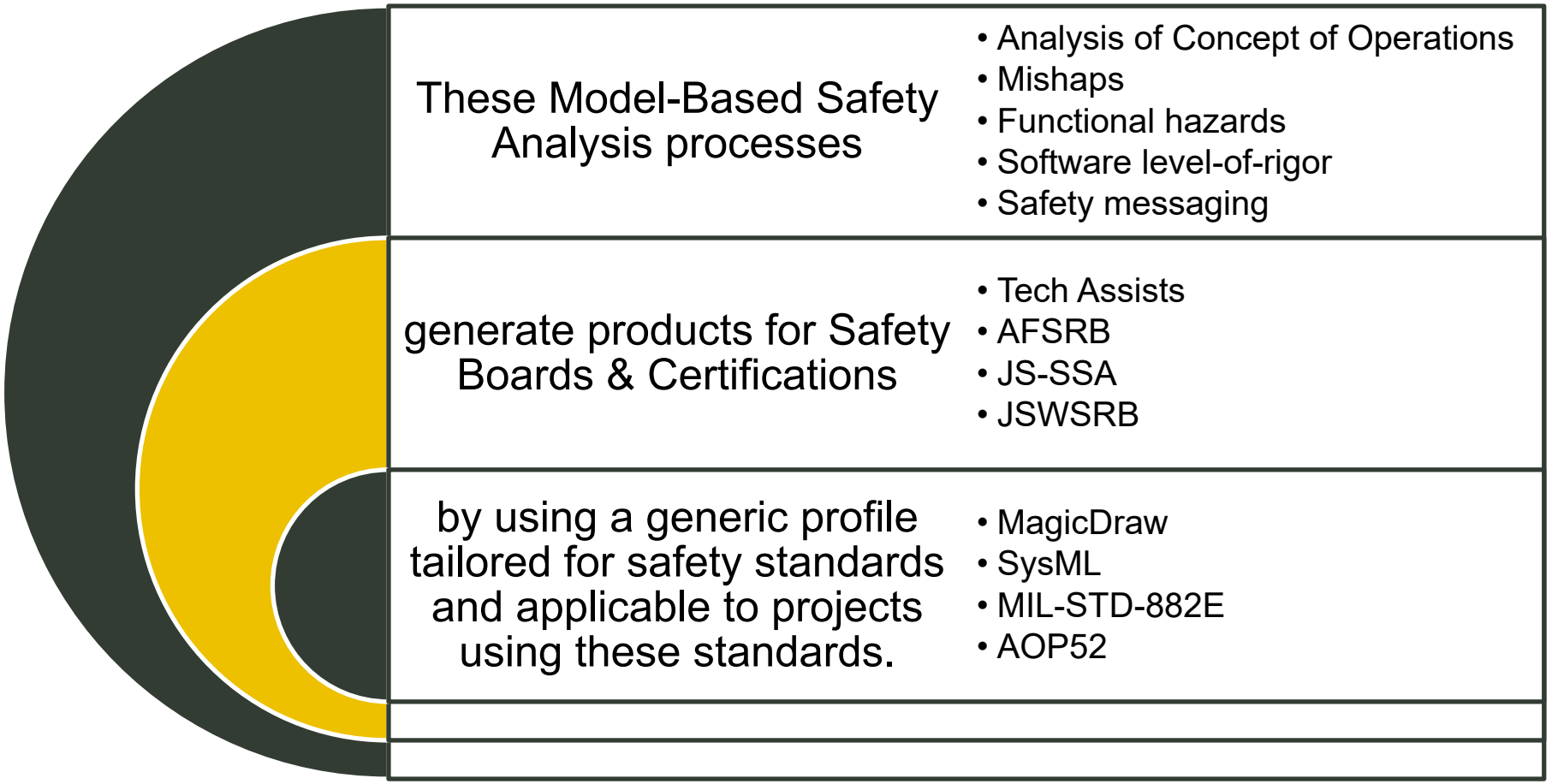
Systems Engineering Directorate

DISTRIBUTION STATEMENT A: Approved for Public Release

23 OCT 2019

SCOPE & CONTEXT

Safety Modeling makes for Happier Safety Engineers



STARTING POINT AND TEAMING

MIL-STD-882-E

Establish Safety Criteria and Requirements

Apply the Safety Order of Precedence

Hazard Mitigation/Testing/Verification

Guides Hazard Monitoring and Control

SSWG

Safety Plans

Safety Guidance and Design

Safety Board Presentations & Certifications

Identify & Mitigate Hazards

Identify Safety Related & Safety Critical Functions

Document Safety Analyses thoroughly

MBSE

Support Safety Analysis using SSWG Deliverables and the MBSE Models

Incorporate SSWG recommendations and supporting data into functional analysis

Create and publish model based deliverables

- Manage Mishaps
- Manage Functional Hazards
- Manage Safety Causes and Effects
- Manage Function Safety Ratings
- Manage Safety Requirements
- Traceability to Standards and Guidelines

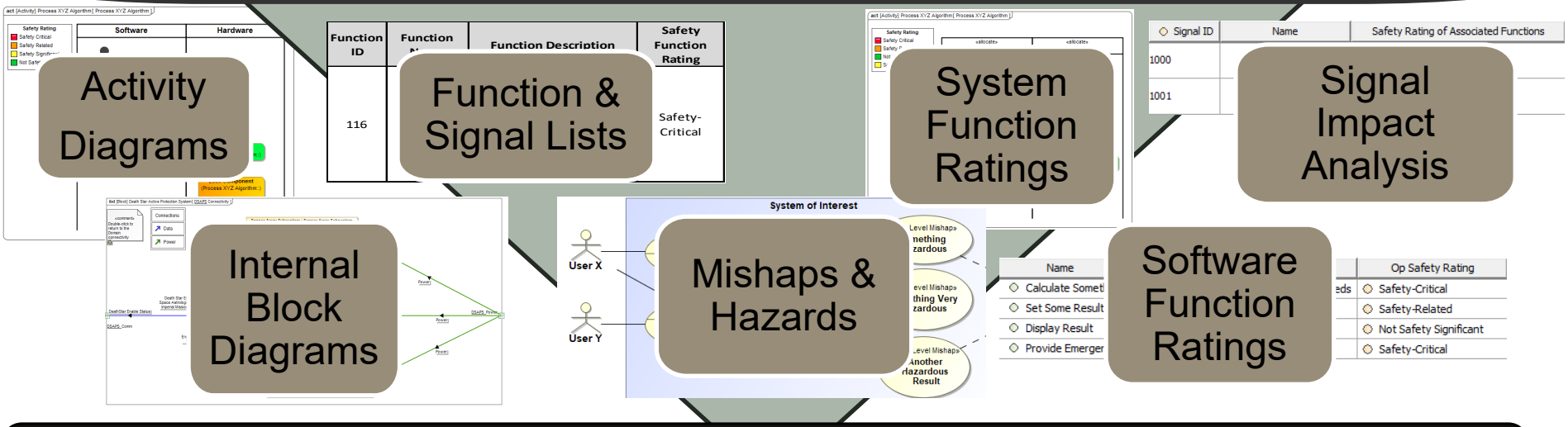
DEVELOPING THE SAFETY ARCHITECTURE

Inputs: System Need, Capability Gaps, ConOps, and/or Requirements

Functional Analysis

Safety Analysis

Outputs: Consistent views depicting the system and safety architecture



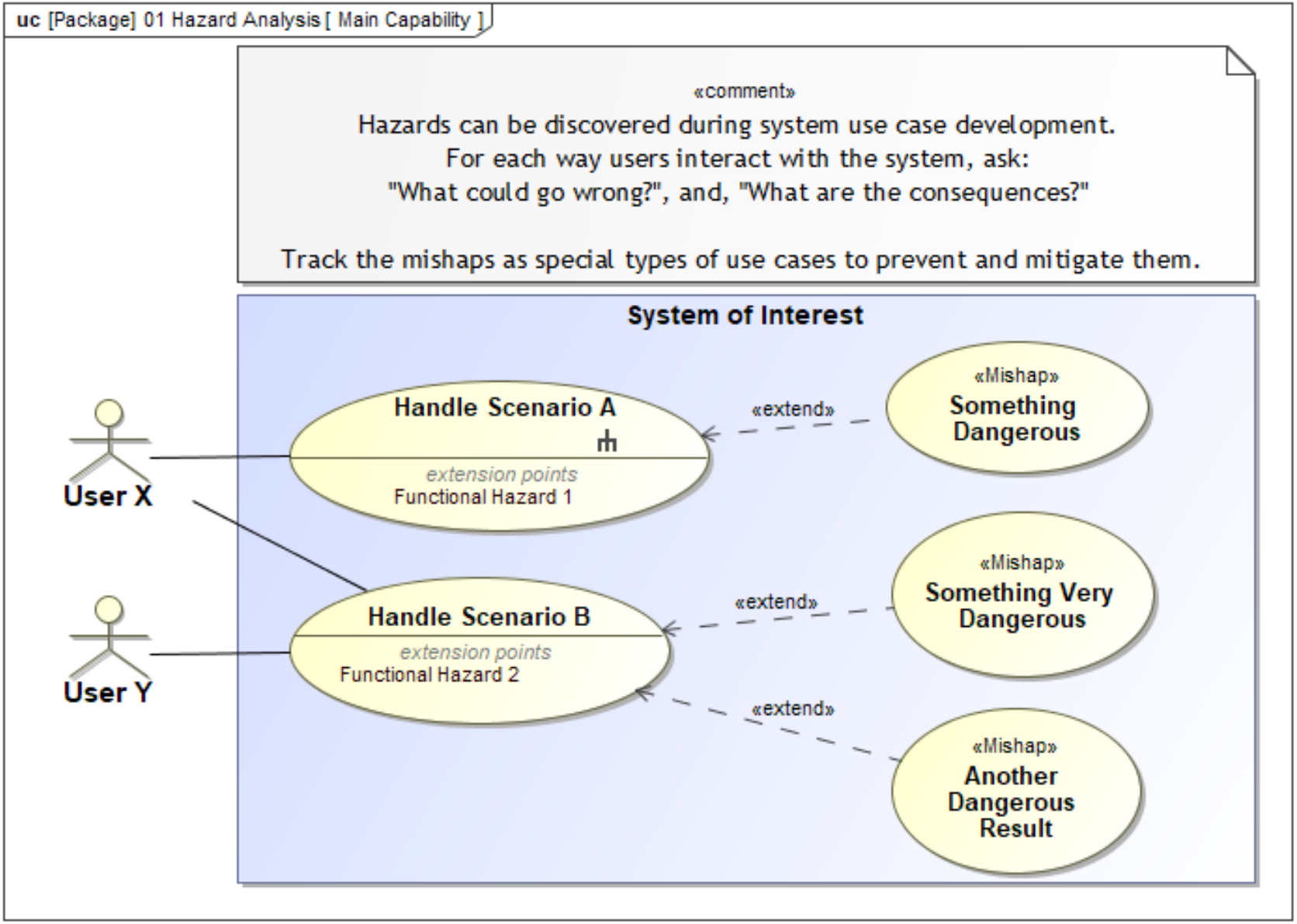
The Bottom Line: Functional & Safety Analyses are aligned with one another using Model-Based Systems Engineering techniques

SAFETY MODEL ELEMENTS

- **Use Case Elements are informed by the ConOps:**
  - Functional Hazards
  - Safety Causes
  - Safety Effects
  - Top Level Mishaps
- **System-Level Functions must have an 882E rating and the following attributes:**
  - Safety Rating: Safety Critical, Safety Related, Not Safety Significant (MIL-STD-882E)
  - Safety Rating Rationale: Detailed documentation of why the rating was assigned and the date of assignment
  - Needs Safety Review: TRUE or FALSE for tracking purposes
  - Safety Status: Additional Tag for any Notes on open actions or open questions the SSWG has
- **Software-Level Functions:**
  - Use stereotype tags to capture all SSWG information
  - These are used to support the development and management of FSHA and FMEA
- **Signals:**
  - AOP-52 dictates safety criticality of information and how it is consumed and supplied
  - Table created to automatically search signal usages and their interactions with function ratings

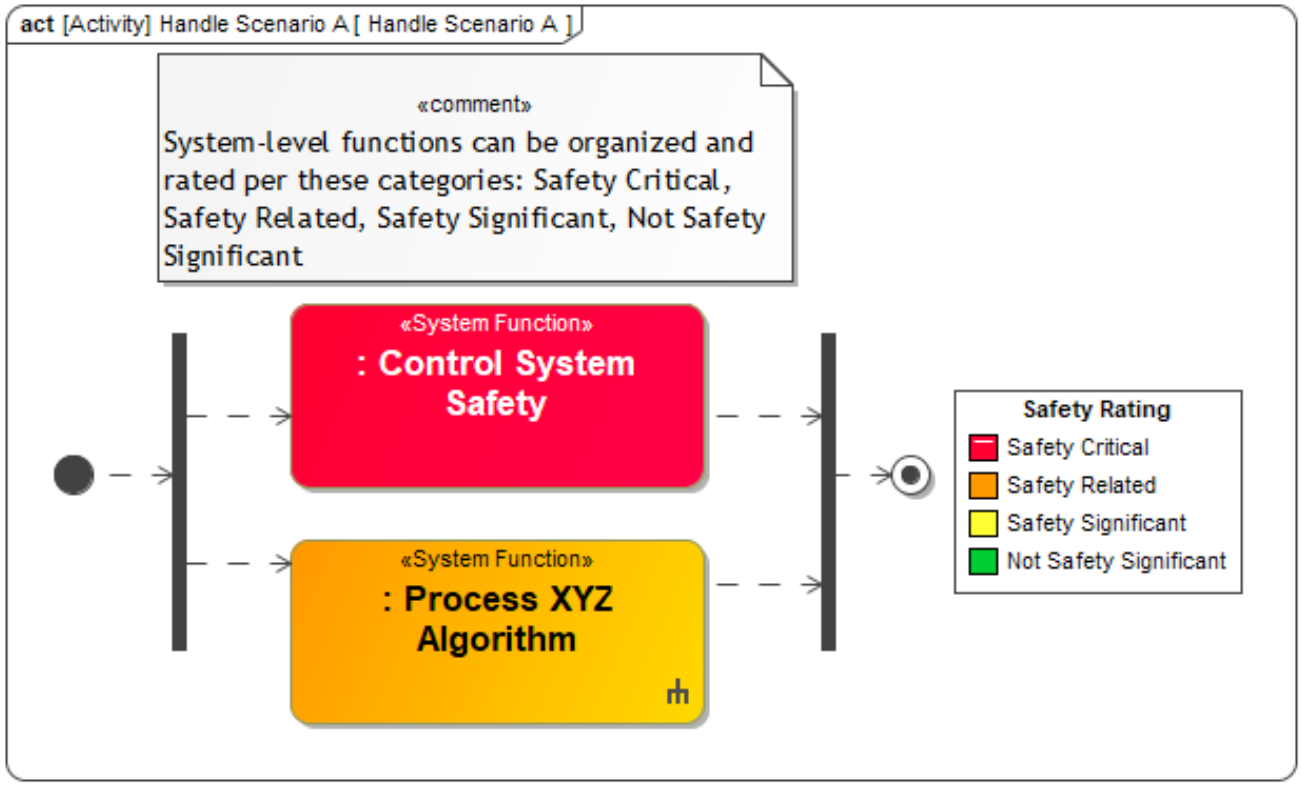
Model & Profile Demonstration

FUNCTIONAL HAZARDS AND MISHAPS



SYSTEM LEVEL FUNCTIONS

FunctionID	Name	Safety Function Rating	Safety Rating Rationale	Safety Status	Needs Safety Review
100	Process XYZ Algorithm	Safety-Related		17Oct2019: New input added t	true
101	Control System Safety	Safety-Critical			false
102	Stow System	Not Safety Significant	17Oct2019: Stowing is a featur		false



HARDWARE FUNCTION ANALYSIS

TABLE III. Risk assessment matrix

RISK ASSESSMENT MATRIX SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Model is aligned with the Risk Assessment Matrix for hardware items

Name	Safety Function Rating	Probability	Severity	Risk Assessment	Needs Safety Review	Safety Rating Rationale	Standard Status	Safety Status
Lock Component	Safety-Related	Remote	Marginal	Medium	☐ false	Because of important reasons	MIL-STD-882E	
Display Result	Not Safety Significant	Occasional	Negliglible	Low	☑ true	Rationale goes here	MIL-STD-882E	

SOFTWARE FUNCTION ANALYSIS

TABLE V. Software safety criticality matrix

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

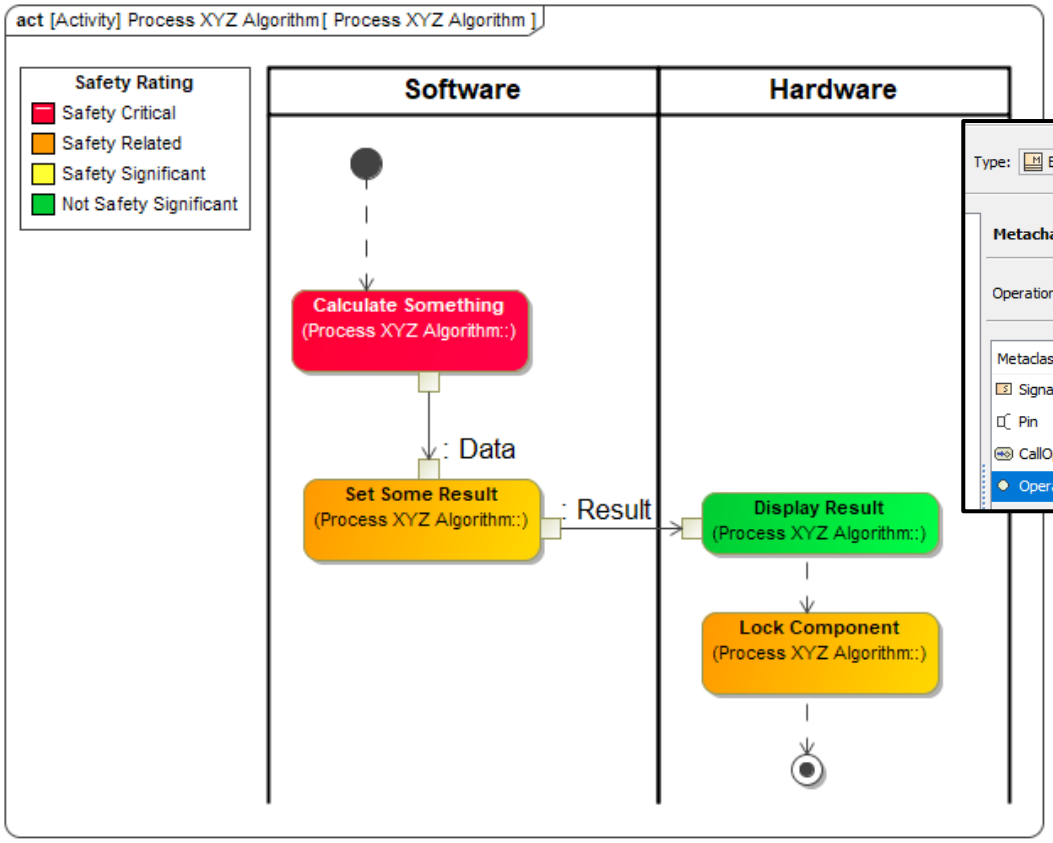
SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

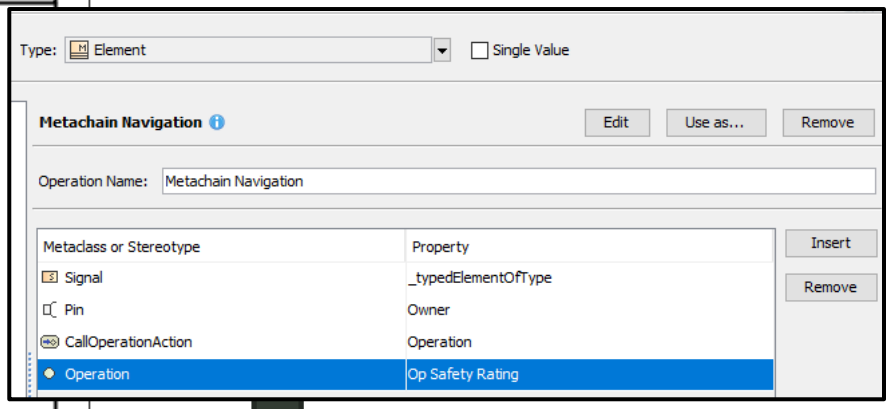
NOTE: Consult the Joint Software Systems Safety Engineering Handbook and AOP 52 for additional guidance on how to conduct required software analyses.

Model is aligned with the Software Safety Criticality Matrix and supporting text for software items.

Name	Software Control Category	Severity Category	SWCI	Safety Function Rating	Safety Status	Safety Rating Rationale	Needs Safety Review	Standard Status
Calculate Something	3	Critical	SwCI 3	Safety-Critical		17Oct2019: Rating was a	☐ false	AOP 52 Edition 1
Set Some Result	5	Marginal	SwCI 5	Safety-Related	17Oct2019: Need stan		☑ true	
Provide Emergency Stop				Safety-Critical			☑ true	MIL-STD-882E

SIGNAL IMPACT ANALYSIS





Signal ID	Name	Safety Rating of Associated Functions
1000	Data	Safety-Critical Safety-Related
1001	Result	Safety-Related Not Safety Significant

Metachains in MagicDraw find usages and relationships in the model.

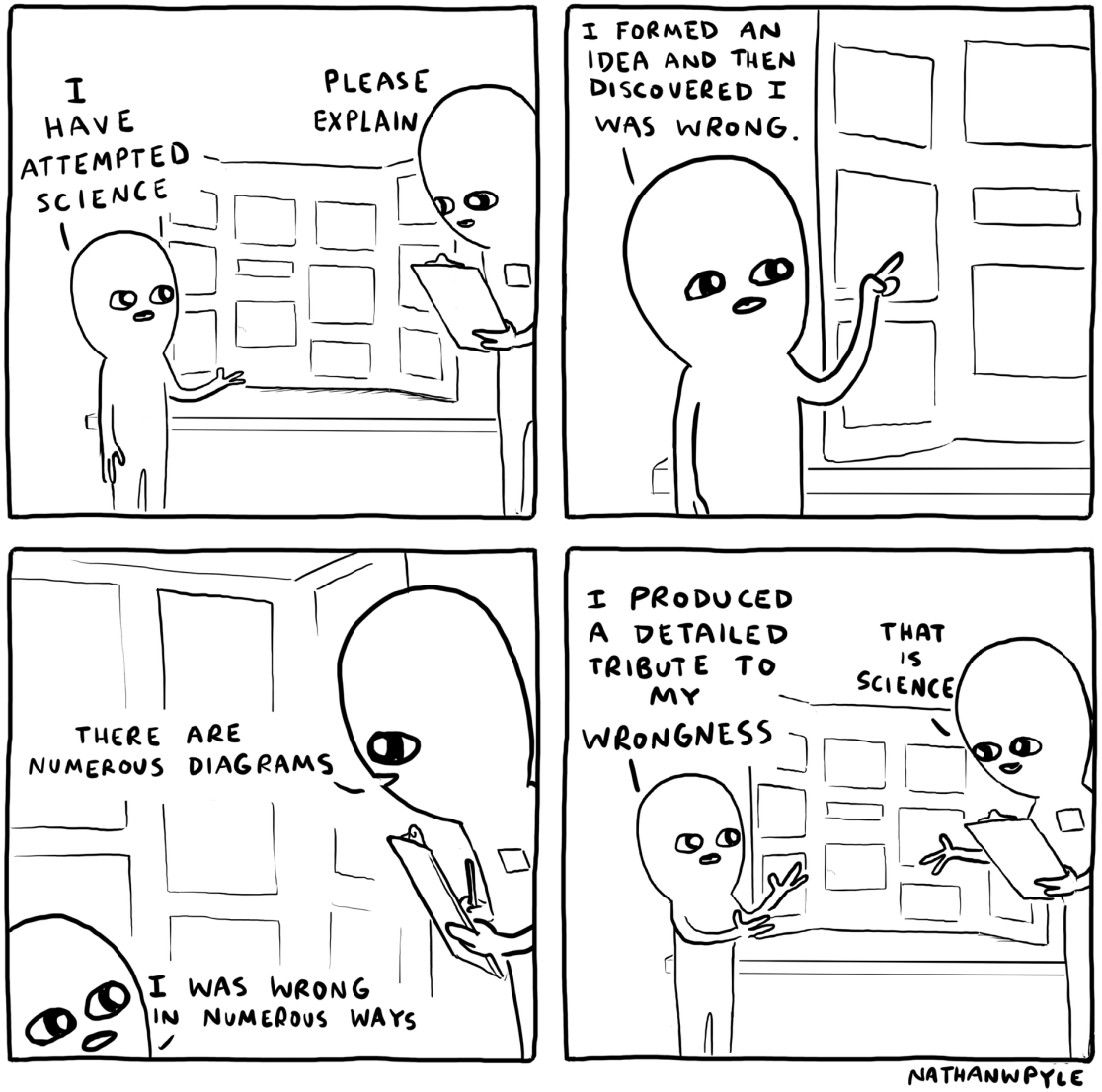
OUTCOMES OF ANALYSES

Re-usable profile can be leveraged to enable Safety Analyses

- Managing Functional Hazards and Mishaps
- Discovery of Safety Critical or Non-Safety Critical features
- Easy ID and quantification of safety criticality levels for system, hardware, and software level functions
- Clear delineation of Level of Rigor needed for SW development process: SWCI Level distinction
- Automated views that indicate potential problematic signal flows
- Clear communication of rationale
- Safety architecture → System architecture incorporation

Environment & Language: MagicDraw 18.5, SysML V1.4
Standards: MIL-STD-882E System Safety Military Standard,
AOP-52 Guidance on Software Safety Design

Questions?


I HAVE ATTEMPTED SCIENCE
PLEASE EXPLAIN
I FORMED AN IDEA AND THEN DISCOVERED I WAS WRONG.
THERE ARE NUMEROUS DIAGRAMS
I WAS WRONG IN NUMEROUS WAYS
I PRODUCED A DETAILED TRIBUTE TO MY WRONGNESS
THAT IS SCIENCE
NATHANWPYLE