



# Model-Based Systems Engineering (MBSE) for Iterative MIL-STD-882E Autonomous Ground Vehicle Safety Programs

Frank Fratrik  
VP & GM

Edge Case Defense

[ffratrik@ecr-defense.ai](mailto:ffratrik@ecr-defense.ai)



EDGE CASE DEFENSE  
ENABLING WARFIGHTER SAFETY



# Agenda

DoD Trends

Ground Vehicle Autonomy Challenges

ECD MBSE Safety Motivation

Related Work

Proposed MIL-STD-882E Safety Model

-Goals, Organization and Structure, Hazard Tracking

Iterating Hazard Analysis within the Safety Model

-Updating for Events from Fielded Systems, Updating for New Development Cycles

Conclusions and Future Work

# DoD: More Autonomy and Complexity

The DoD is increasingly building more modern, complex, and autonomous systems to maintain overmatch.



Common theme across the services – air, ground, maritime



Failure modes are designed into these systems which do not expose themselves until operation, disrupting schedules and budgets.



<https://rb.gy/lm3zs>



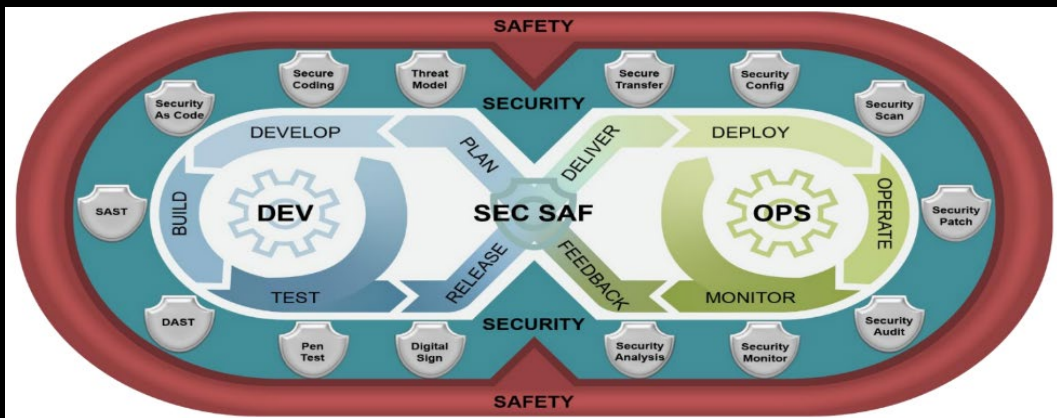
<https://rb.gy/7om50>



<https://rb.gy/afhor>

# DoD: More Agile Development

## Acquiring Fast, Faster, Fastest



Credit: Frank Marotta, US ATEC

Programs asked to accelerate acquisition, integrate existing functions, and deploy more frequently

MVP, iterate quickly, sort the backlog, and fill the CI/CD pipeline

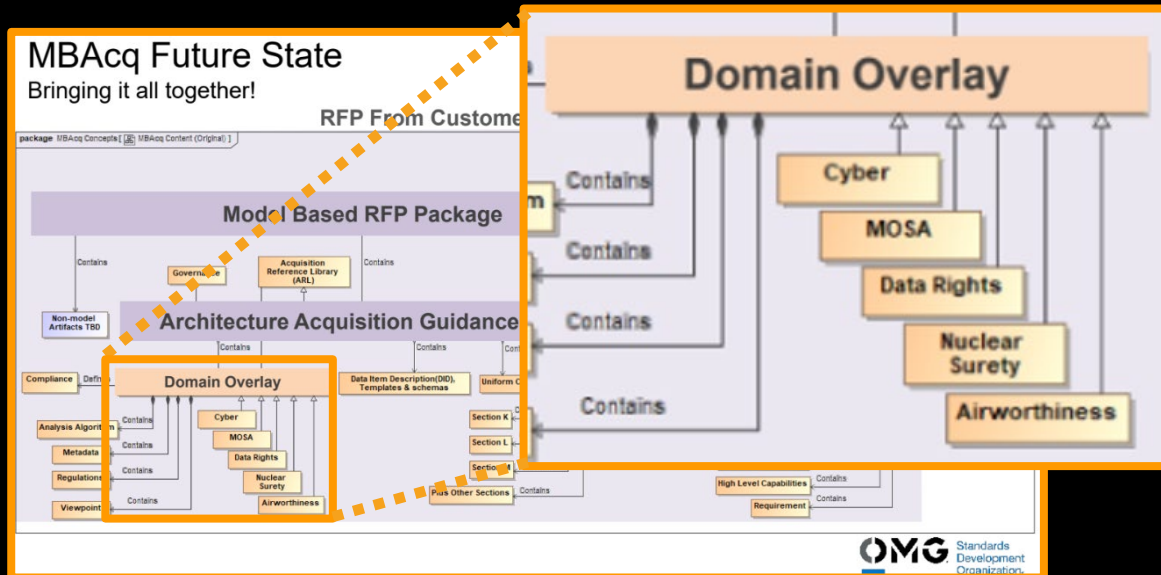
DevSecOps marketing is a win for Security

## MIL-STD 882E compliance via DevSecSafOps?



# DoD: More Digital Engineering

- Digital Engineering (DE) (re-)emerging as the preferred way to engineer complex systems
- Contracts requiring MBSE-based safety CDRLs; MB RFPs incoming
- Initial resourcing elevated: infrastructure, training, model initiation



- Returns increase during iterative lifecycle
- -ilities like System Safety likely best fit in MBSE as Domain Overlays



# Ground Vehicle Autonomy Challenges



<https://rb.gy/9pm2c>

Approved for Public Release

# Ground Vehicle Autonomy Challenges

- Push to use cutting edge technology with little time/space separation
- Mixed Tech Readiness Lvl stacks – Sense, Perceive, Predict, Plan, Act
- Dynamic safety concepts while technology matures  
Safety Driver -> E-stops & Isolation -> Obstacle Detection -> Obstacle Avoidance
- What functions enable the mission? What functions enable safety?



<https://rb.gy/hekte>

Approved for Public Release

- Learning from Mining Operators: Autonomous Ops Zone

# ECD MBSE Safety Motivation



How can we holistically address complexity, autonomy, agile, system safety?

*MBSE as a core enabler*

- MIL-STD 882E safety process using MBSE is analytical, rigorous, traceable AND scalable
- Source of Truth - System safety analyses in the same configuration controlled MBSE environment
- Faster Iteration - Safety change impact analysis execution made easy
- Rapid Safety Risk Tracking – Automated population, updates, and traceability



# Related Work: Modeling Language

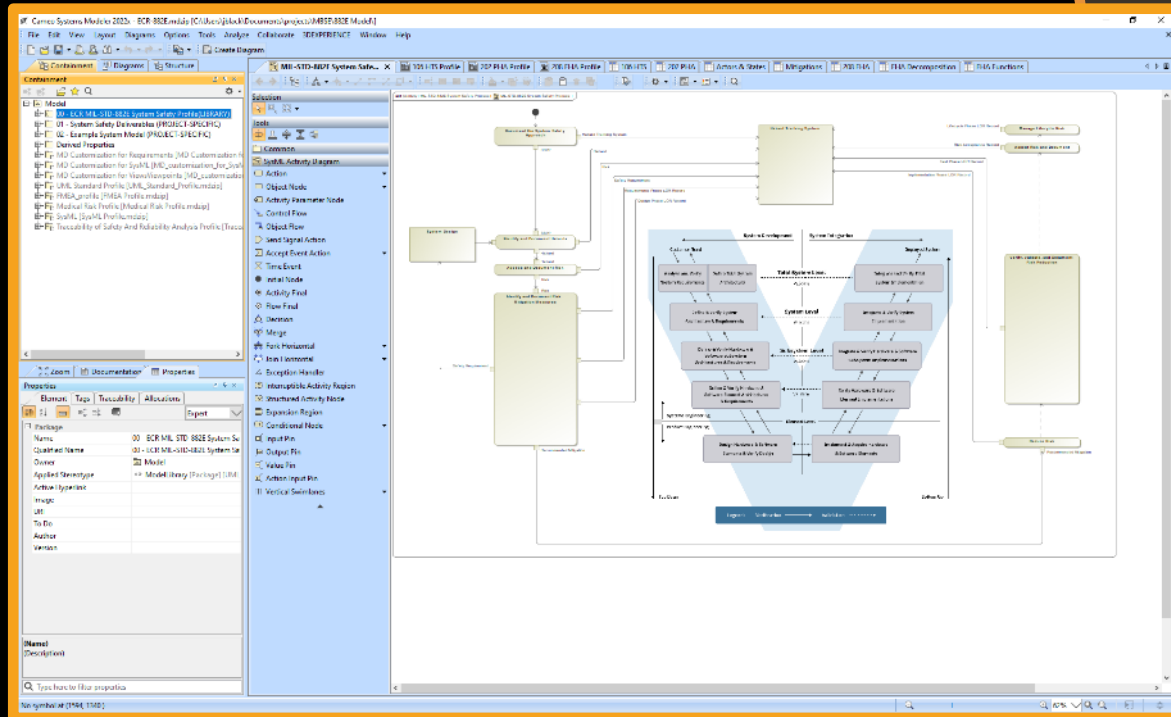
- Unified Modeling Language (UML®)
  - <https://www.omg.org/spec/UML/2.5.1/About-UML>
  - Graphical language for visualizing, specifying, constructing and documenting artifacts of distributed object systems
- Systems Modeling Language (SysML®)
  - <https://www.omg.org/spec/SysML/>
  - Extension of UML for systems engineering
- Risk Analysis and Assessment Modeling Language (RAAML)
  - <https://www.omg.org/spec/RAAML/1.0/About-RAAML>
  - Extension of SysML to support integration of generic safety analyses
    - Failure Modes & Effects Analysis (FMEA), Fault Tree Analysis (FTA), Systems Theoretic Process Analysis (STPA), Goal Structured Notation (GSN)
    - Includes stereotypes for ISO 26262
    - No stereotypes for MIL-STD-882E hazard analysis or hazard tracking



# Related Work: Cameo Systems Modeler™

<https://www.3ds.com/products-services/catia/products/no-magic/cameo-systems-modeler/>

- SysML
- Supports DoD Architecture Framework (DoDAF)
- Safety & Reliability Analyzer Plugin
  - ISO 26262
  - FMEA (IEC 60812:2006)
  - Hazard Analysis (IEC 62304, ISO 1497:2007)
  - No stereotypes for MIL-STD-882E hazard analysis or hazard tracking



# Related Work: MBSE for MIL-STD-882E

- Shevland, M. R. (2019). From Traditional to Digital: Integrating MIL-STD-882E System Safety Engineering into a Model Based Systems Engineering Environment. *37th International System Safety Conference*, (p. 16).
  - Proof of concept example
  - Package-based structure
  - System safety ontology
  - Preliminary Hazard Analysis w/ simple stereotypes
  - Hazard<->requirements and system element<->safety requirement traceability

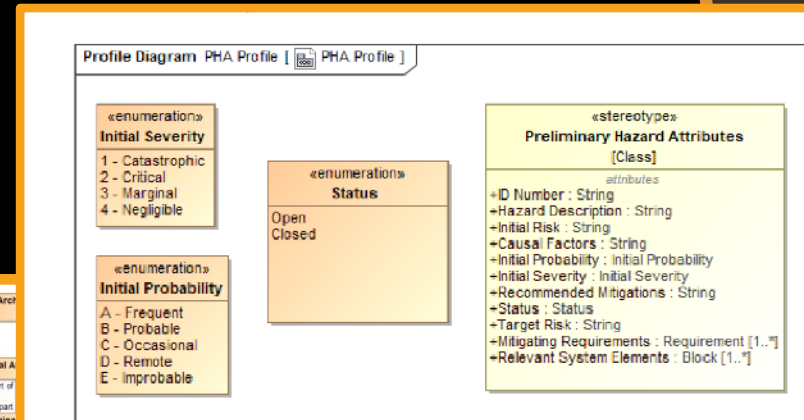


Figure 4 - DoD MIL STD 882E PHA Profile

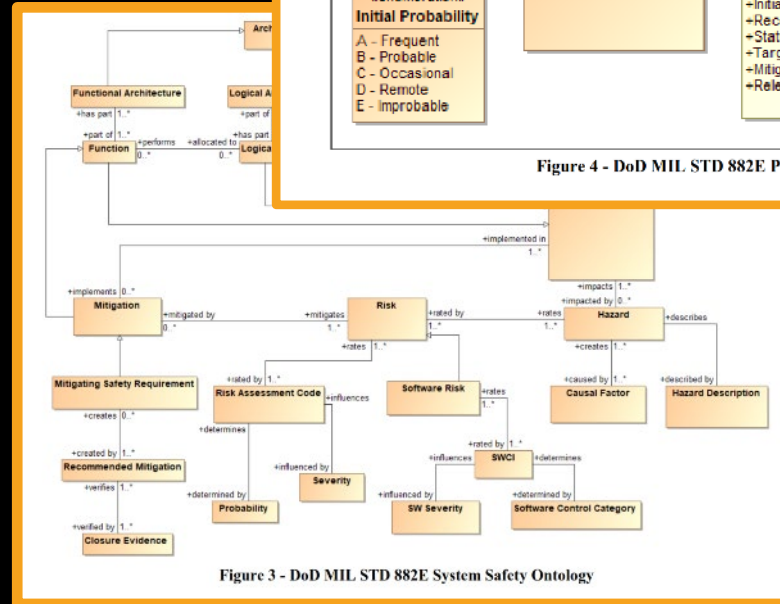


Figure 3 - DoD MIL STD 882E System Safety Ontology



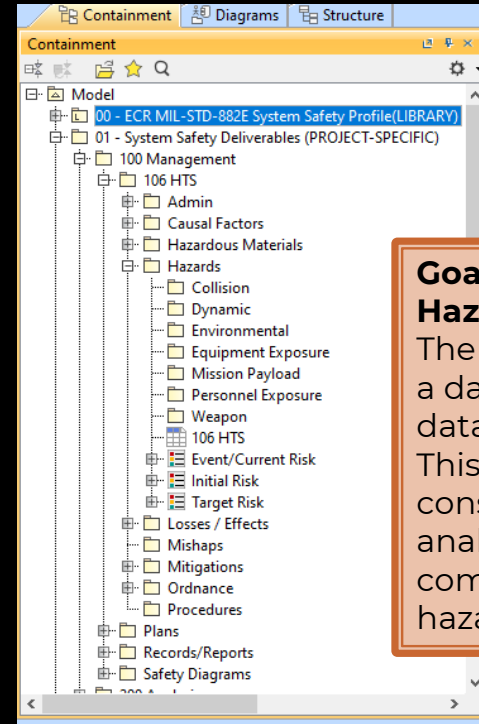


# Goals for Proposed MIL-STD-882E Model

1. Facilitate hazard tracking from analysis & requirements through design, implementation, V&V, post-deployment
  - HTS is foundation of MIL-STD-882E safety assessment
2. Facilitate rework
  - Update analyses & tracking quickly in new cycles
3. Standalone usability
  - Optimize safety processes even if system is not modeled
4. Portability
  - Need to apply it easily to new/multiple projects
5. Closely aligned to MIL-STD-882E
  - Require minimal customization for required work products

# Hazard Tracking – Data

- All associated data for the hazard has a defined stereotype, which is used to create a record in the HTS
  - Administration records (origination, update, risk acceptance, etc.)
  - Causal Factors
  - Losses/Effects
  - Mishaps
  - Mitigations
  - Hazardous Materials
  - Ordnance
  - Safety Procedures
- Requirements element is used as a base classifier to inherit traceability properties

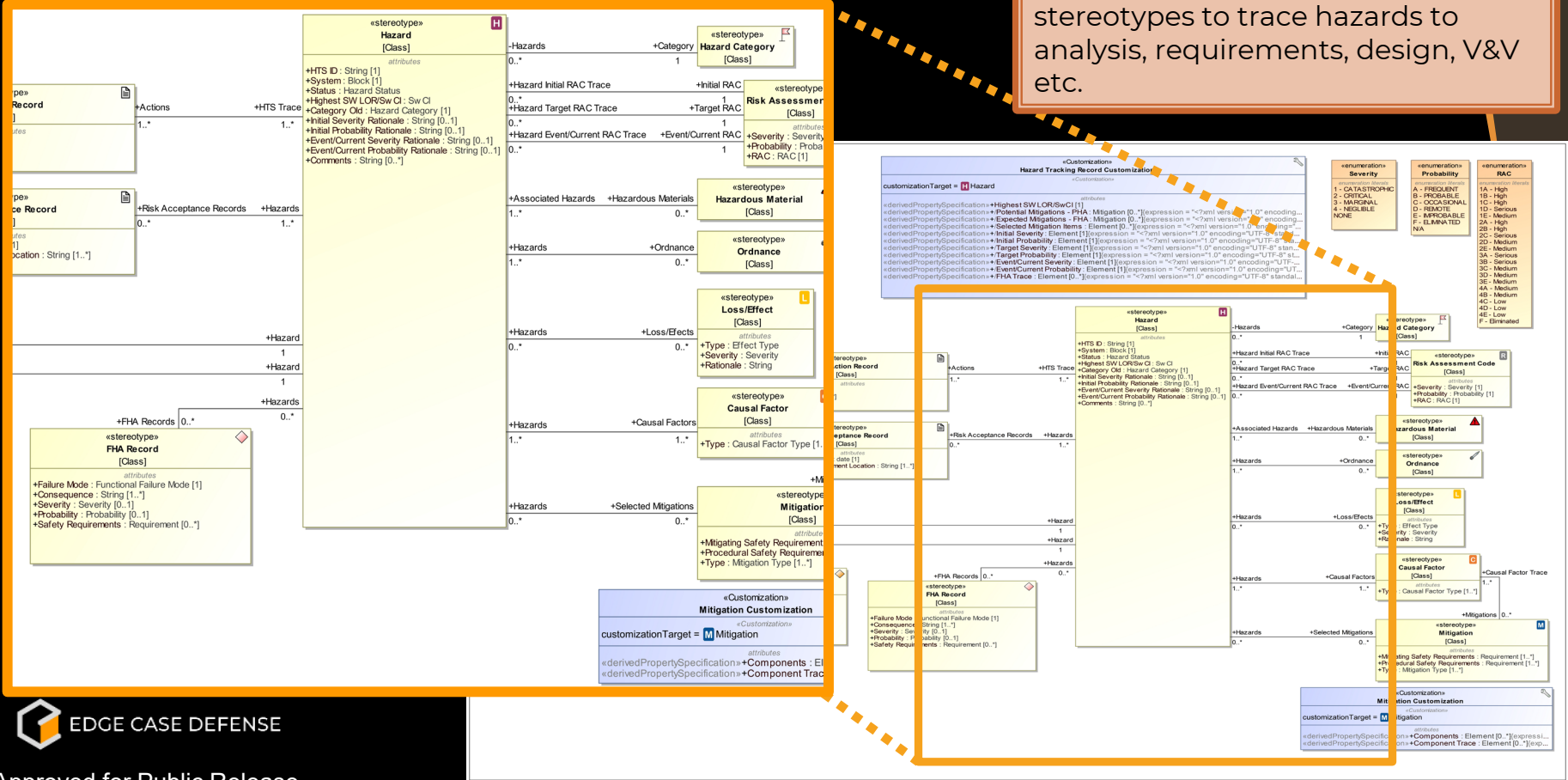


## Goal 1: Facilitate Hazard Tracking

The model becomes a database of related data for hazards. This increases consistency between analyses and completeness of hazard tracking

# Hazard Tracking – Traceability

**Goal 1: Facilitate Hazard Tracking**  
Model uses associations between stereotypes to trace hazards to analysis, requirements, design, V&V etc.



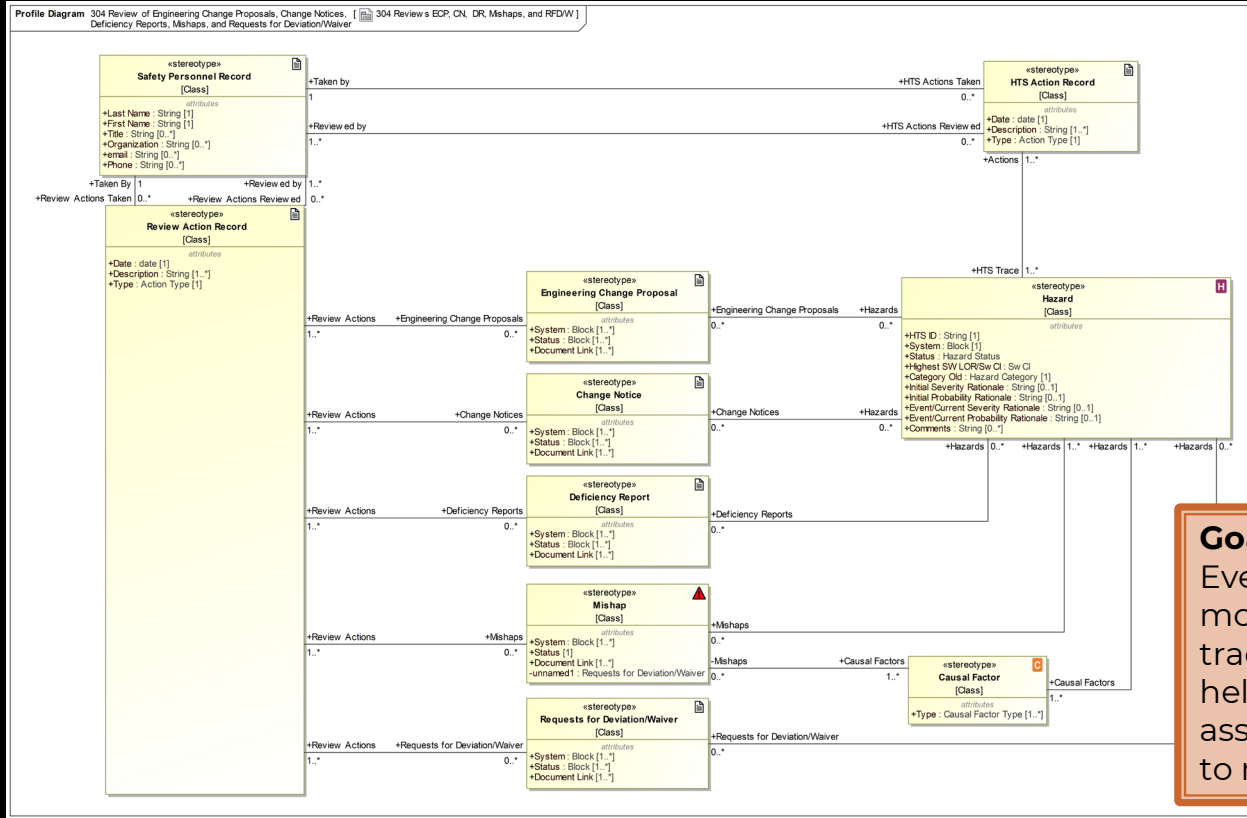
# Hazard Tracking – Data

#	△ Id	Name	Text	Type	Components	Functions of the Mitigation	Hazards	PHA Trace	FHA Trace
1	M-1	DBW Disablement	Mechanism to prevent Drive By Wire system control of the Vehicle 1 while operating manned.	Hardware Procedural	FHA-23 Safety Circuit	<ul style="list-style-type: none"> <li> FHA-23.8 Register signal from L</li> <li> FHA-23.10 Register signal from L</li> <li> FHA-23.9 Send signal to DBW S</li> <li> FHA-23.11 Send signal to DBW</li> </ul>	<ul style="list-style-type: none"> <li> H-1.1 Crewed collision with dismot</li> <li> H-1.2 Crewed collision with vehicle</li> </ul>	<ul style="list-style-type: none"> <li> PHA-1.1 Crewed collision with dismounted</li> <li> PHA-1.2 Crewed collision with vehicle</li> </ul>	<ul style="list-style-type: none"> <li> FHA-1.1.1 1 - mi</li> <li> FHA-1.1.3 3 - inc</li> <li> FHA-1.1.4 4 - inc</li> <li> FHA-1.1.5 5 - inc</li> </ul>
2	M-2	DBW E-Stop	Mechanism for the Drive By Wire to command the Vehicle 1 to cease motion, remain stationary, and bring payloads to a safe state.	Hardware Procedural	<ul style="list-style-type: none"> <li> FHA-10 Braking Subsystem</li> <li> FHA-21 E-Stop - Local</li> <li> FHA-23 Safety Circuit</li> </ul>	<ul style="list-style-type: none"> <li> FHA-10.1 Reduce vehicle speed</li> <li> FHA-10.2 Stop vehicle</li> <li> FHA-10.4 Allow vehicle speed</li> <li> FHA-21.1 Register signal from L</li> <li> FHA-21.3 Register signal from L</li> <li> FHA-23.3 Send signal to Braking</li> <li> FHA-23.7 Send signal to Braking</li> </ul>	<ul style="list-style-type: none"> <li> H-1.2 Crewed collision with vehicle</li> <li> H-1.1 Crewed collision with dismot</li> </ul>	<ul style="list-style-type: none"> <li> PHA-1.1 Crewed collision with dismounted</li> <li> PHA-1.2 Crewed collision with vehicle</li> </ul>	<ul style="list-style-type: none"> <li> FHA-1.1.1 1 - mi</li> <li> FHA-1.1.3 3 - inc</li> <li> FHA-1.1.4 4 - inc</li> <li> FHA-1.1.5 5 - inc</li> </ul>
3	M-3	Failsafe Mobility Control System	Mechanism(s) to ensure DBW vehicle mobility controls reliably execute the vehicle commands with no single point failures leading to unsafe conditions.	Hardware Software				<ul style="list-style-type: none"> <li> PHA-1.2 Crewed collision with vehicle</li> <li> PHA-1.1 Crewed collision with dismounted</li> </ul>	
4	M-4	Assured OEDR	Object and Event Detection and Response - functionality in the Autonomy subsystem that assures DBW mobility is controlled in a manner to avoid collisions.	Hardware Software				<ul style="list-style-type: none"> <li> PHA-1.1 Crewed collision with dismounted</li> <li> PHA-1.2 Crewed collision with vehicle</li> </ul>	

## Goal 2: Rework

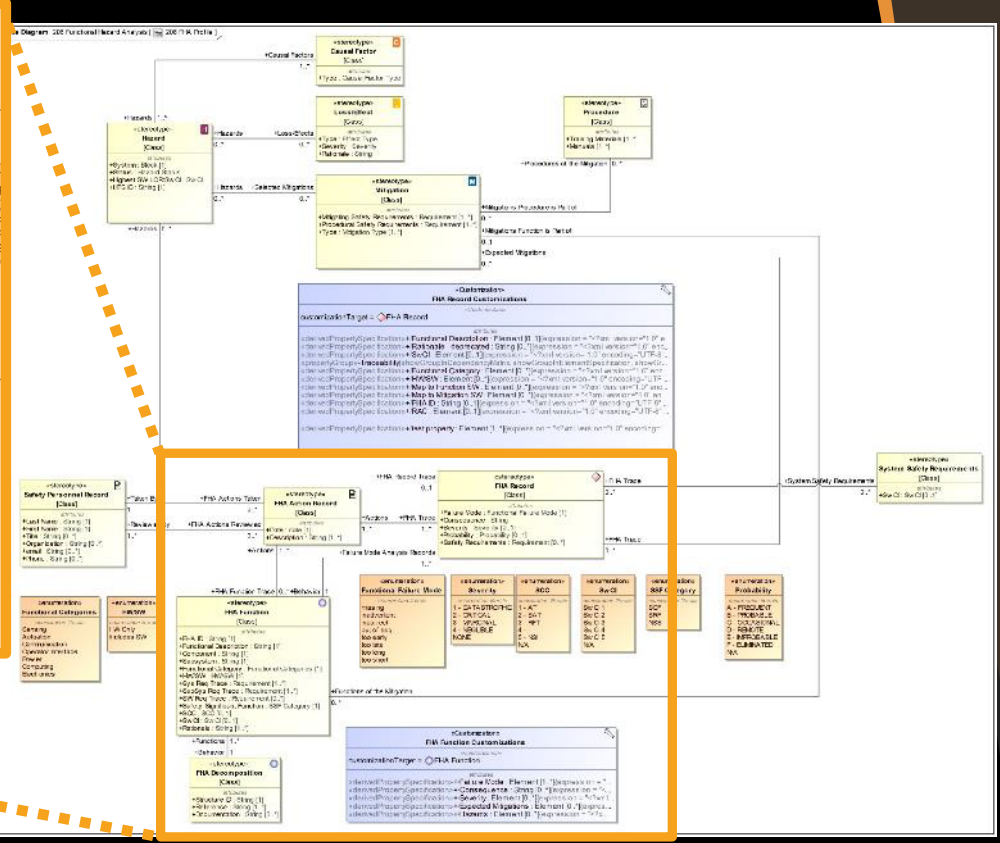
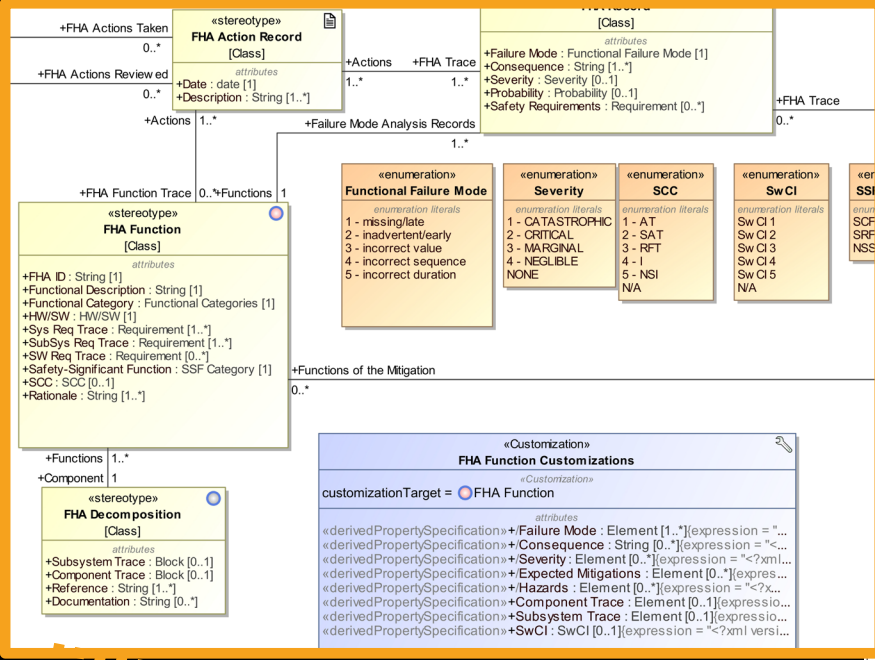
Design changes between Drive By Wire development cycles that are updated in the HTS are updated in all linked analyses. Rework of analysis can focus on records linked to the updated data.

# Event Tracking in Fielded Systems



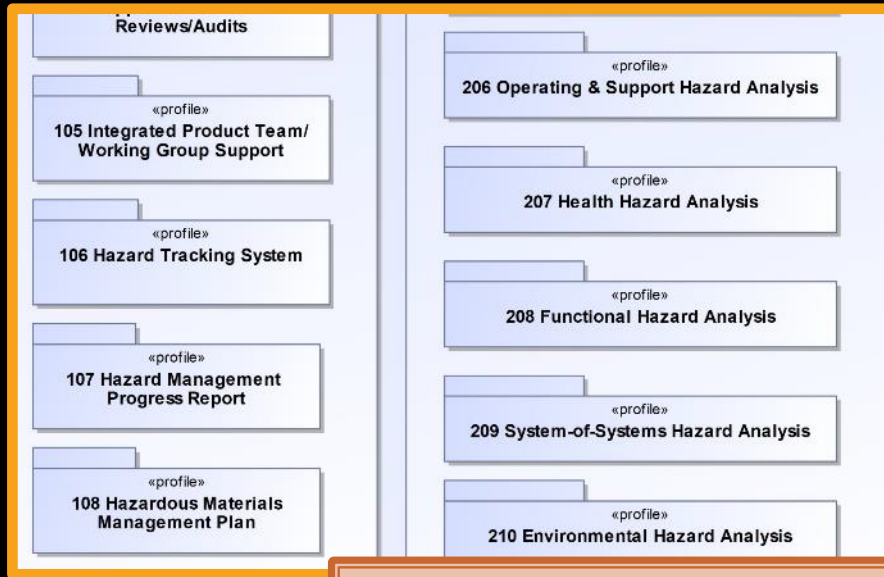
**Goal 2: Rework**  
 Event tracking is also modeled in the HTS and tracked to hazards. This helps quickly identify all associated analysis records to review.

# Hazard Analysis – Structures



**Goal 3: Standalone**  
Analysis structures  
can be used without  
a system model

# Model Organization & Structure



**Safety Profile**

**Safety Artifacts**

**System Model**

**Goal 3: Standalone**  
Ontology of stereotypes is defined separately from safety artifacts produced with them, and from the system model. Can be used without a system model for analysis of document-based system information

**Goal 4: Portable**  
Profile library can be used as a domain overlay for existing model

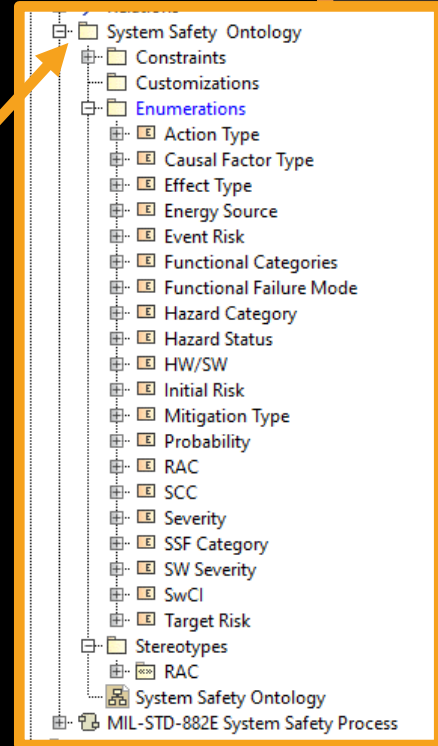
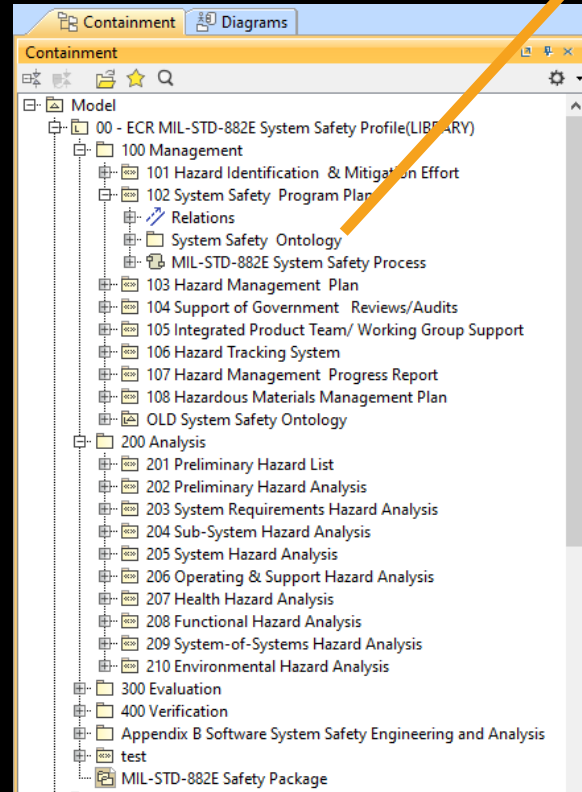


# Model Organization & Structure

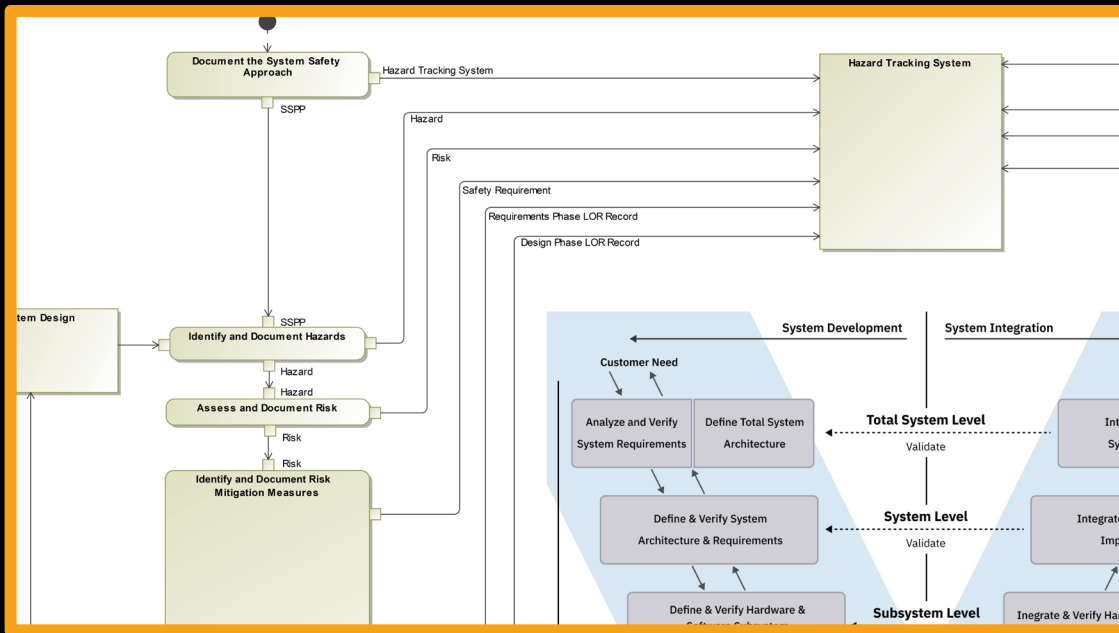
- Packages are organized by MIL-STD-882E Task #
- Enumerations & stereotypes for most definitions are stored in the System Safety Program Plan profile (task 102)
- Stereotypes for hazard tracking and analyses are stored in their profiles

## Goal 5: MIL-STD-882E alignment

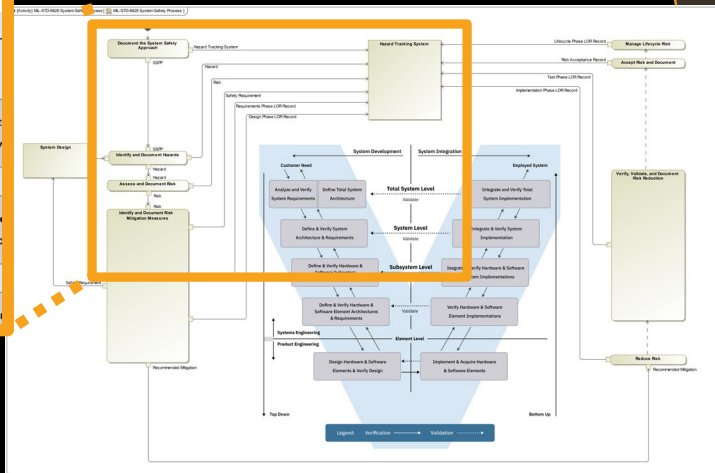
Profiles and packages organized by MIL-STD-882E task ID



# System Safety Process Modeling



**Goal 5: MIL-STD-882E alignment**  
 Can represent MIL-STD-882E Safety processes and workflows in activity diagrams







# Conclusions & Future Work


- Hazard tracking and table-based hazard analysis can be built in MBSE and improve traceability between analyses vs building in Excel
- Model of MIL STD 882 artifacts (PHL, PHA, FHA, HTS, etc) can be used without integration into a system model
- It is unclear if modeling fault trees in MBSE would be a net improvement over use of a dedicated fault-tree tool
- Next steps are application on additional systems and implementing lessons learned



For more information, find us at:

 [www.ecr-defense.ai](http://www.ecr-defense.ai) // [www.ecr.ai](http://www.ecr.ai)

 [info@ecr-defense.ai](mailto:info@ecr-defense.ai)

 Edge Case Defense

 Edge Case Research



Approved for Public Release

