# SysML and FMEA (Failure Modes Effects Analysis)

**James Hummell**
**Consultant**
MBSE Solutions, LLC

MBSESolutions
MAKING MODELS WORK FOR YOU

**October 18, 2018**

# Bio

- James Hummell is an expert trainer for SysML, UML, and UPDM/UAF, currently working as chief consultant for MBSE Solutions. He is an expert in software and systems engineering, specializing in modeling and simulation analysis using UML and SysML.

- James has extensive experience in embedded systems for safety critical systems (Do178b Level A), configuration management (CM), the software development life cycle (SDLC), and process engineering development. He has been developing software and systems in model-based design engineering (UML and SysML) for over 20 years.

- He is a member of the RTCA SC-205 subgroup developing Do-178C model-based development and verification supplement, and has worked with the Object Management Group (OMG) and the International Council on Systems Engineering (INCOSE) on many specifications and working groups.

http://MBSE.Solutions
jhummell@MBSE.Solutions
In/jameshummell
T: 480-463-4359
M: 480-521-2125

# Agenda

- What is FMEA
- How to Identify Failure Modes
- How to Mitigate Failure Modes
- How to Simulate Failure Modes
- Other Tools Available

# What is FMEA?

**Failure mode and effects analysis (FMEA)— was one of the first highly structured, systematic techniques for failure analysis. It was developed by reliability engineers in the late 1950s to study problems that might arise from malfunctions of military systems***

- A step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.
- **Failure Modes** means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual.
- **Effects Analysis** refers to studying the consequences of those failures.
- Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones.

# What Is FMEA?

**More and more companies and government agencies are required by contract to perform Failure Modes Effects Analysis (FMEA)**

- The Food and Drug Administration (FDA) has mandated that FMEAs must be done for any product that is put out on the market
- Original equipment manufacturers (OEMs) are now requiring FMEAs in the production of parts and in the making of devices
- Medical, aerospace, and automotive companies all understand the need to generate FMEA tables and forms in order to prove acceptability in the marketplace
- Any company that is producing any product should have a design and a FMEA, and that same design should trace to requirements, define any hazards that may exist, and should be able to demonstrate the failure modes

# How is Risk Assessment Different Than FMEA?

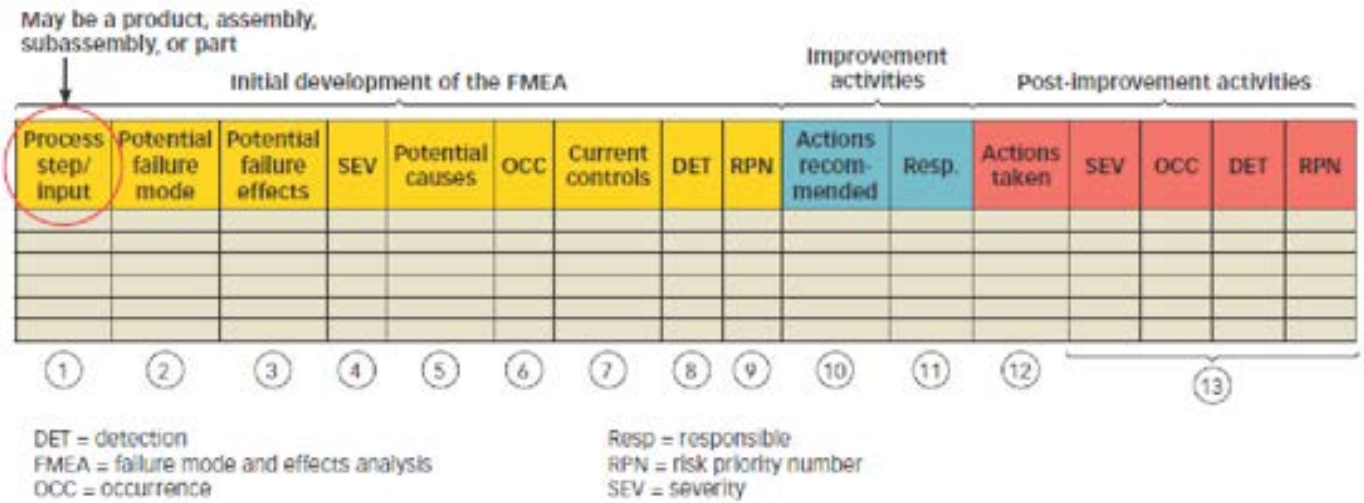
**Risk assessment has to do with looking at the product itself and assessing it, or quantifying it, in order to determine the likelihood of a certain risk.**

- **FMEA describes when you are doing analysis against your actual product, or the end thing. It is the process of identifying the failure mode of the system, analyzing it, and determining what to do when it happens.**
- **It asks the question, "what do I have to do to mitigate or resolve the failure, and how am I going to do that?"**
- **FMEA as a whole should include:**
  - the design (dFMEA)
  - the instructions for use (uFMEA)
  - the manufacturing process (pFMEA)
  - All of these can have failure modes, and they can all have effects. In order to figure out how to resolve these, analysis must be done.

# Other Tools Available

## Traditionally FMEAs are captured in a spreadsheet/table data format

- Windchill Quality Solutions
- ReliaSoft's Xfmea
- Excel



# Process Steps in FMEA

- Step 1: Identify potential failures and effects
- Step 2: Determine severity
- Step 3: Gauge likelihood of occurrence
- Step 4: Failure detection
- Risk priority number (RPN)

# Why Model Your FMEAs

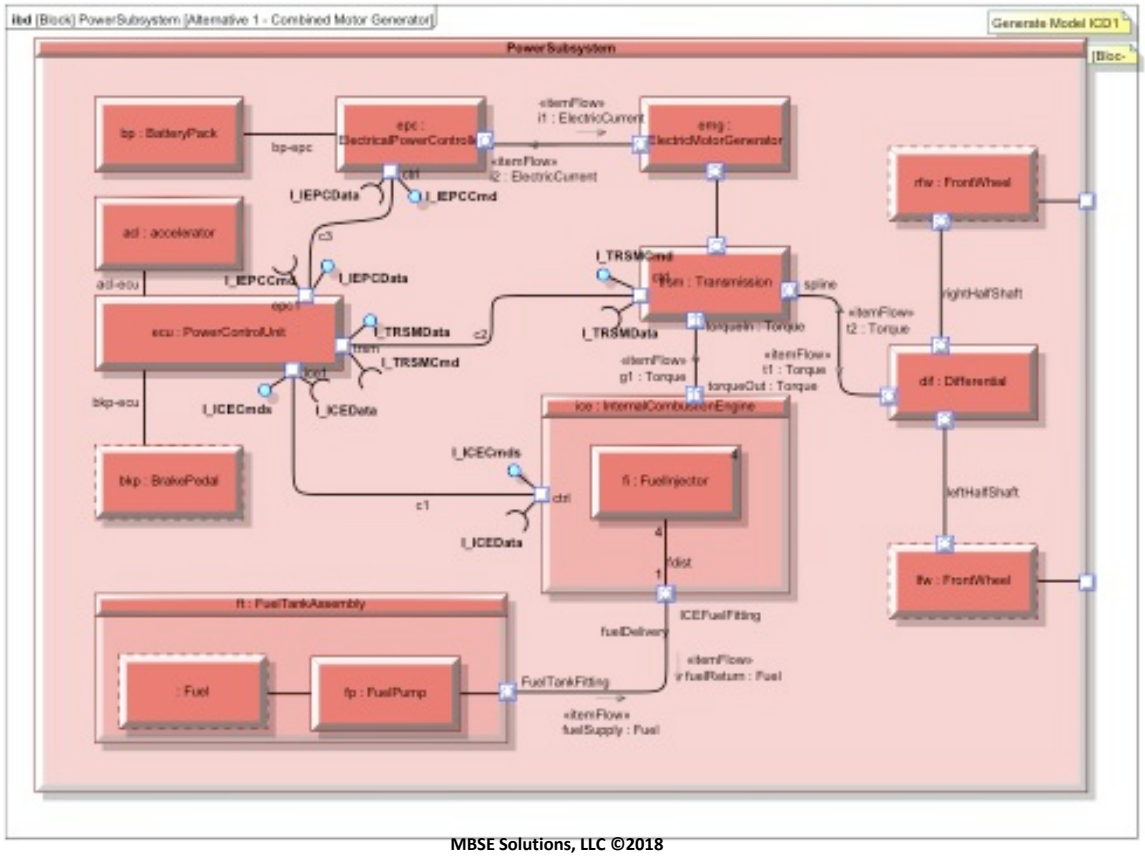
## FMEAs can be modeled to be tied to your systems

- By doing modeling, the review process will be much easier because everything will be traced to what is necessary.
- The model can be used during the review process and generate any answers the reviewer may ask about the product.
- After the model is generated, you can then do traceability to your systems, subsystems, and requirements.
- You can also list your failure modes and the estimated effects.
- In addition to structural design, you can draw a process in an activity diagram, and then generate those linked items into the traditional spreadsheet format, or tool of choice.

# How to Model Your FMEAs – Using SysML

**Using SysML you can model anything in the real world. You can model down to the wire on a circuit board and highlight the failure due to EMF issues and more**

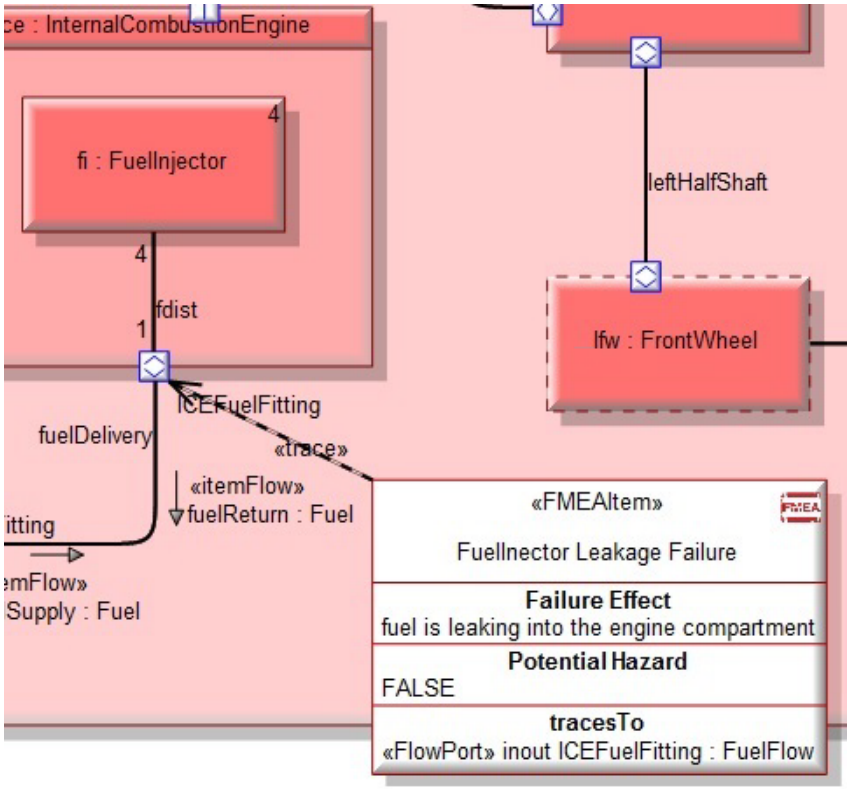
A Typical SysML Design With Physical Interfaces



# How to Identify Failures

## dFMEA - Using this profile, you can trace to your design or functions to create design FMEA

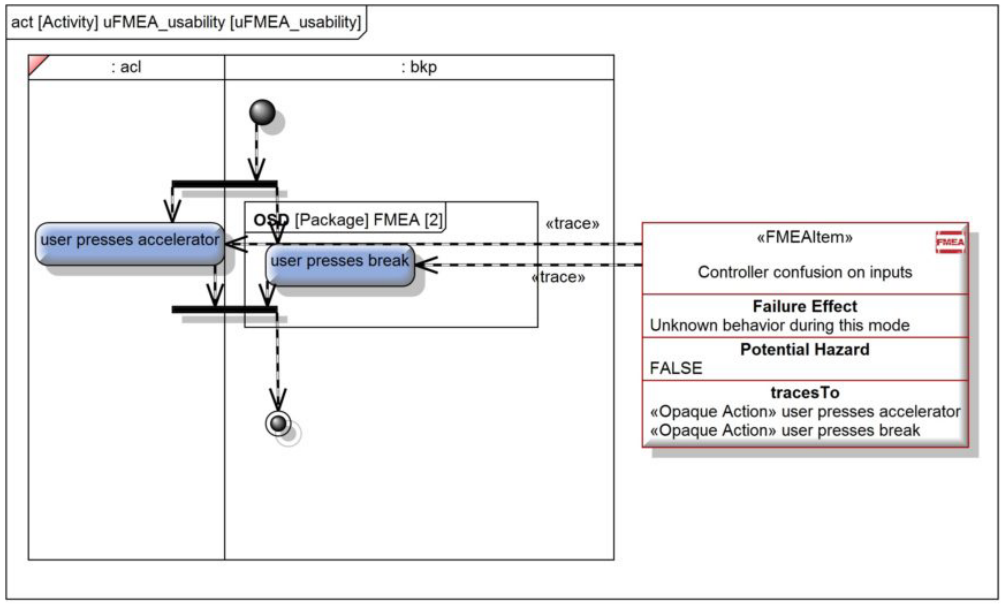
- Identify failures on any modeling item
- Create a trace relationship to set up the data relationship necessary to generate information into any FMEA tool or FMEA spreadsheet.



# How to Identify Failures

## uFMEA – Create a Usage FMEA to analyze how the user will use the system and the potential failure modes

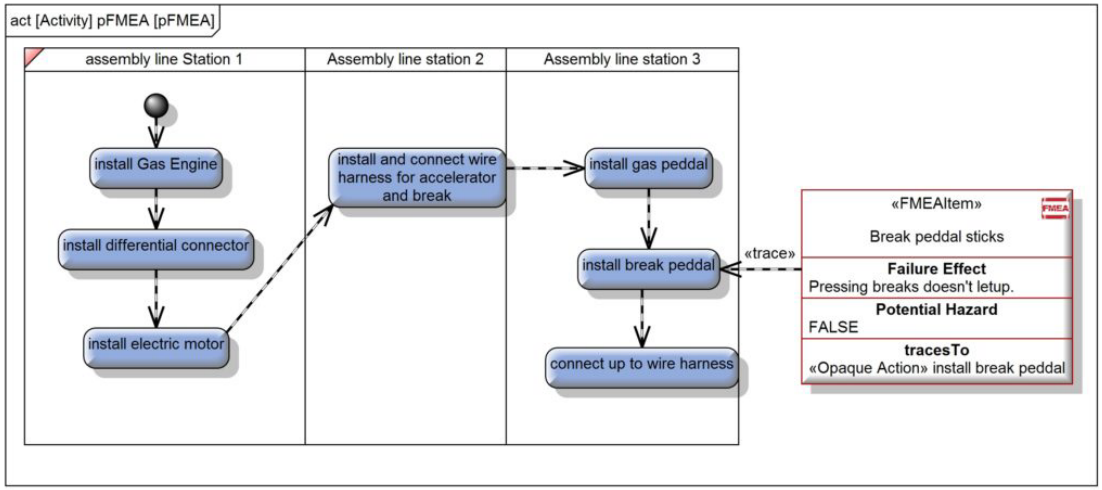
- The best way to show usability in modeling is to do a use case and an activity diagram to describe flow
- Swim-lanes will be the systems that the user interacts with for that failure
- This information can also be traced to the systems it may affect



# How to Identify Failures

## pFMEA —defines the process of building the system and identifies potential failure modes during construction

- This is best described as an activity diagram where each swim-lane identifies the person or equipment involved in doing that process step
- The effects detection will be directly identified in the activity step



# How to Mitigate Your Failure Modes

- Each FMEA Item will generate a row in the FMEA table tied to any modeling (MOF level) attribute that you need to identify as a failure in the system
- All values are generated into FMEA tools of your choosing or spreadsheet formats.

**Failure Mode and Effect Analysis**

| Item Name: | FMEA Team: | Prepared by: | |
|---|---|---|---|
| | | FMEA Date (Orig): | Revision: |

| Process Step or Variable or Key Input | Potential Failure Mode | Potential Effect on Customer Because of Defect | SEV | Potential Causes | OCC | Current Process Controls | DET | RPN | Actions Recommended | Resp.& Target Date | Actions Taken | SEV | OCC | DET | Future RPN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| What is the process step? Or Variable ? Or Input ? | In what ways can the Process Step, Variable, or Key Input go wrong? (chance of not meeting requirements) | What is the impact on the Key Output Variables (customer requirements) or internal requirements? | How Severe is effect to the | What causes the Key Input to go wrong? (How could the failure mode occur?) | How frequent is cause likely to | What are the existing controls that either prevent the failure mode from occurring or detect it should it occur? | How probable is Detection of cause? | Risk Priority # to rank order concerns | What are the actions for reducing the Occurrence of the cause, or improving Detection? Should have actions on high RPN's or Severity of 9 or 10 | Who's Responsible for the recommended action? What date? | What were the actions implemented? Include completion month/year. (Then recalculate resulting RPN.) | Future Severity | Future Occurance | Future Detection | |
| Customer Application | Checks Being Printed Incorrectly | Checks Have To Be Re-Issued | 6 | Incorrect Information On Application Form | 4 | Check of Application Form for Correct Information by Data Enty Operator | 8 | 192 | Clerk Reviews information with customer | Clerk Manager | Completed | 8 | 2 | 4 | 64 |
| Data Entry | Checks Being Printed Incorrectly | Checks Have To Be Re-Issued | | Data Entry Error | | | | | | | | | | | |

# How to Mitigate Your Failure Modes

**Each company has a unique set of FMEA columns or data that they want to capture with their failure modes**

- Using the same technique, you can model your controls to mitigate these failures by tracing controls to the corresponding FMEA item
- This generic FMEA profile can be modified to handle whatever the needs are.

# Why Create a FMEA |SysML System

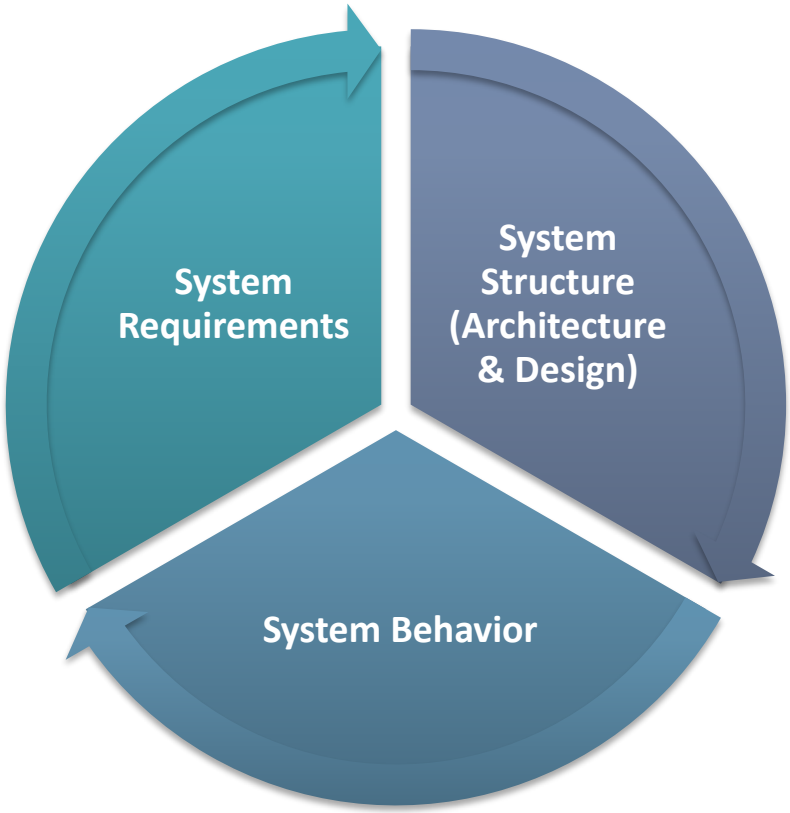
## SysML – a Modeling *Language*

- Standardization
- Reusability
- Documentation and Traceability Reports
- Understanding of the Complete System

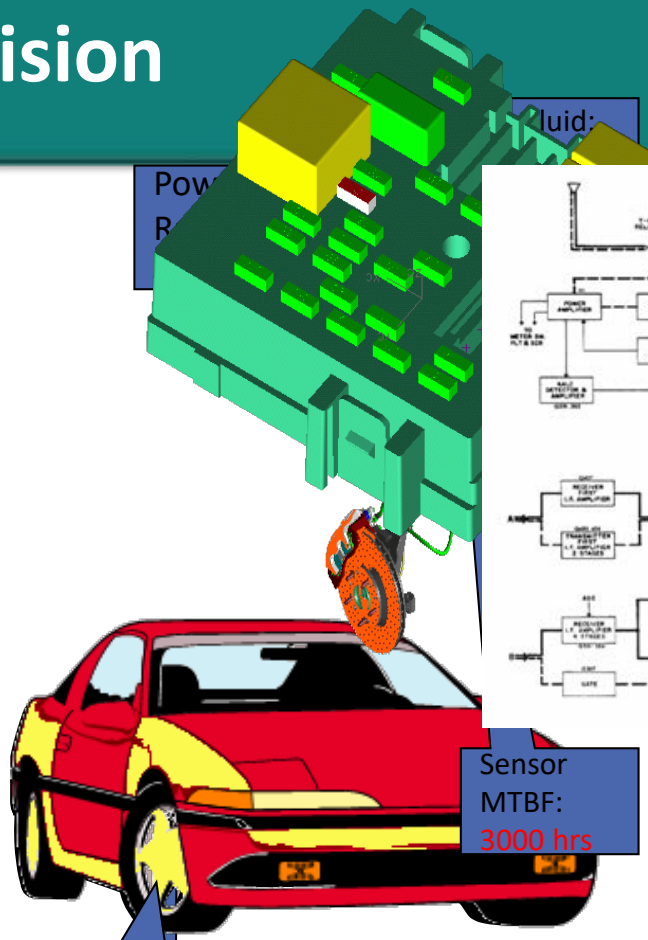
# Why Create a FMEA |SysML System

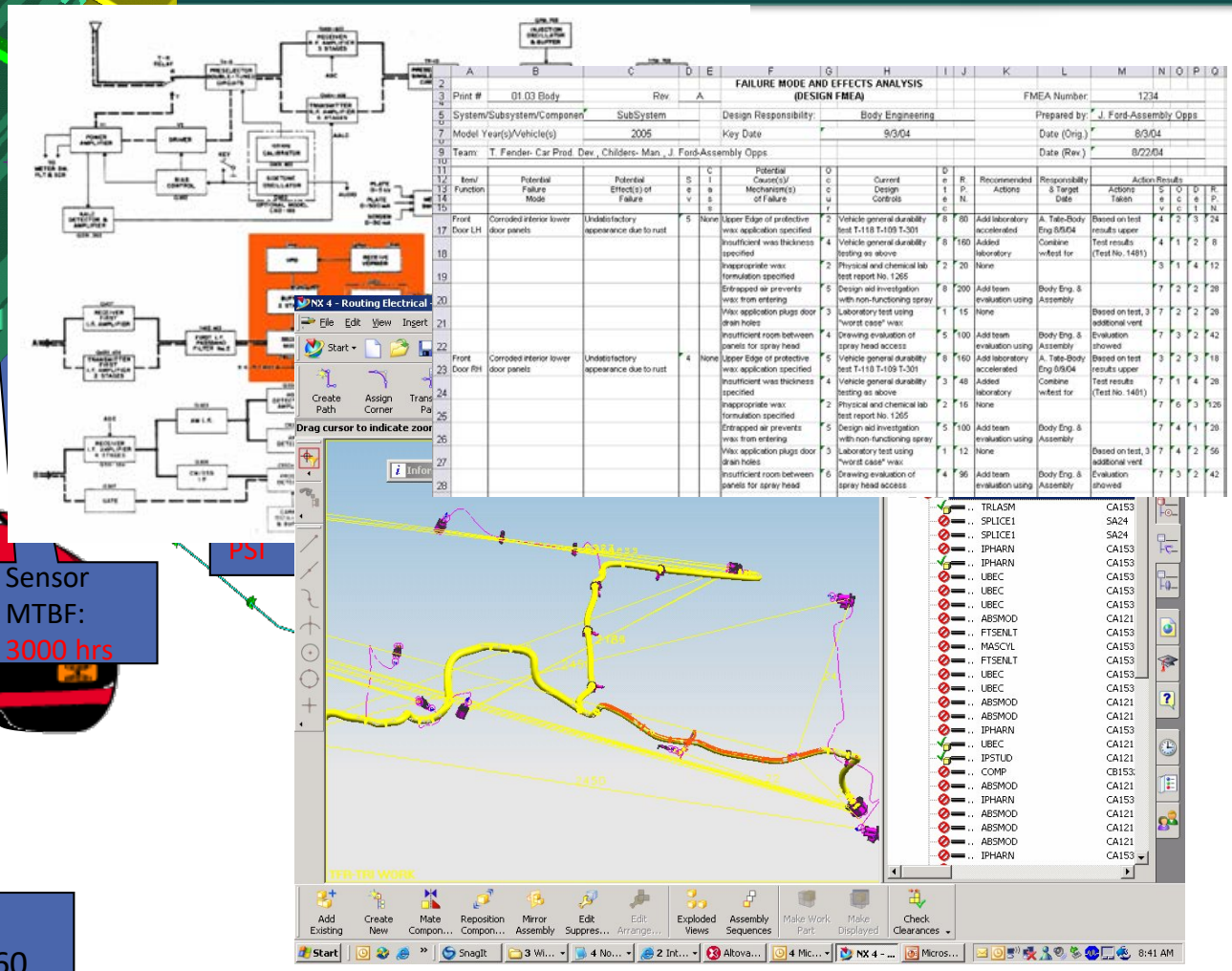
**SysML Allows for An Understanding of the Complete System**

**It Describes and Shows Interconnection of:**



# Integrated Systems Engineering Vision





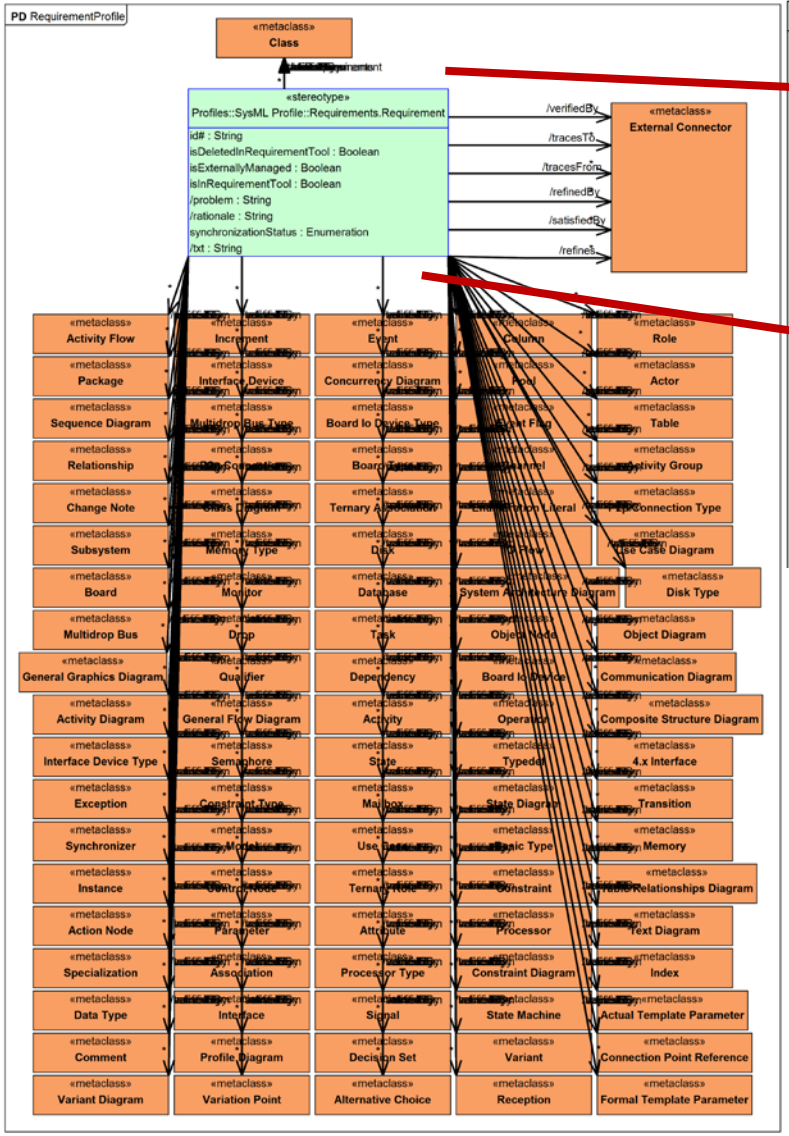

Sensor MTBF: 3000 hrs

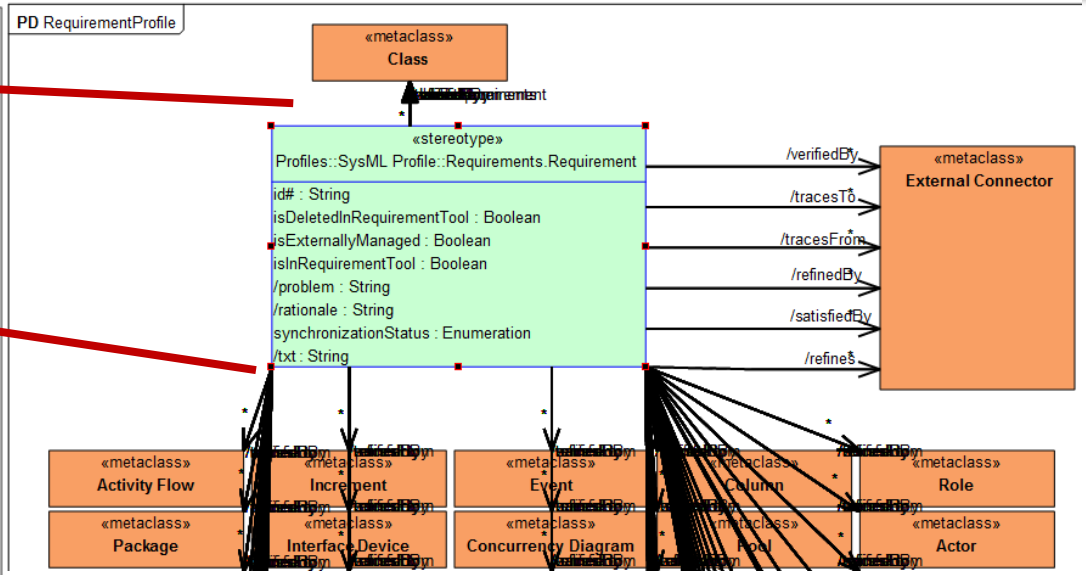
Minimum Turn Radius: 24 ft.
Dry Pavement Braking Distance at 60 MPH: 110 ft. ~~90~~ ft

# Solutions Descriptions

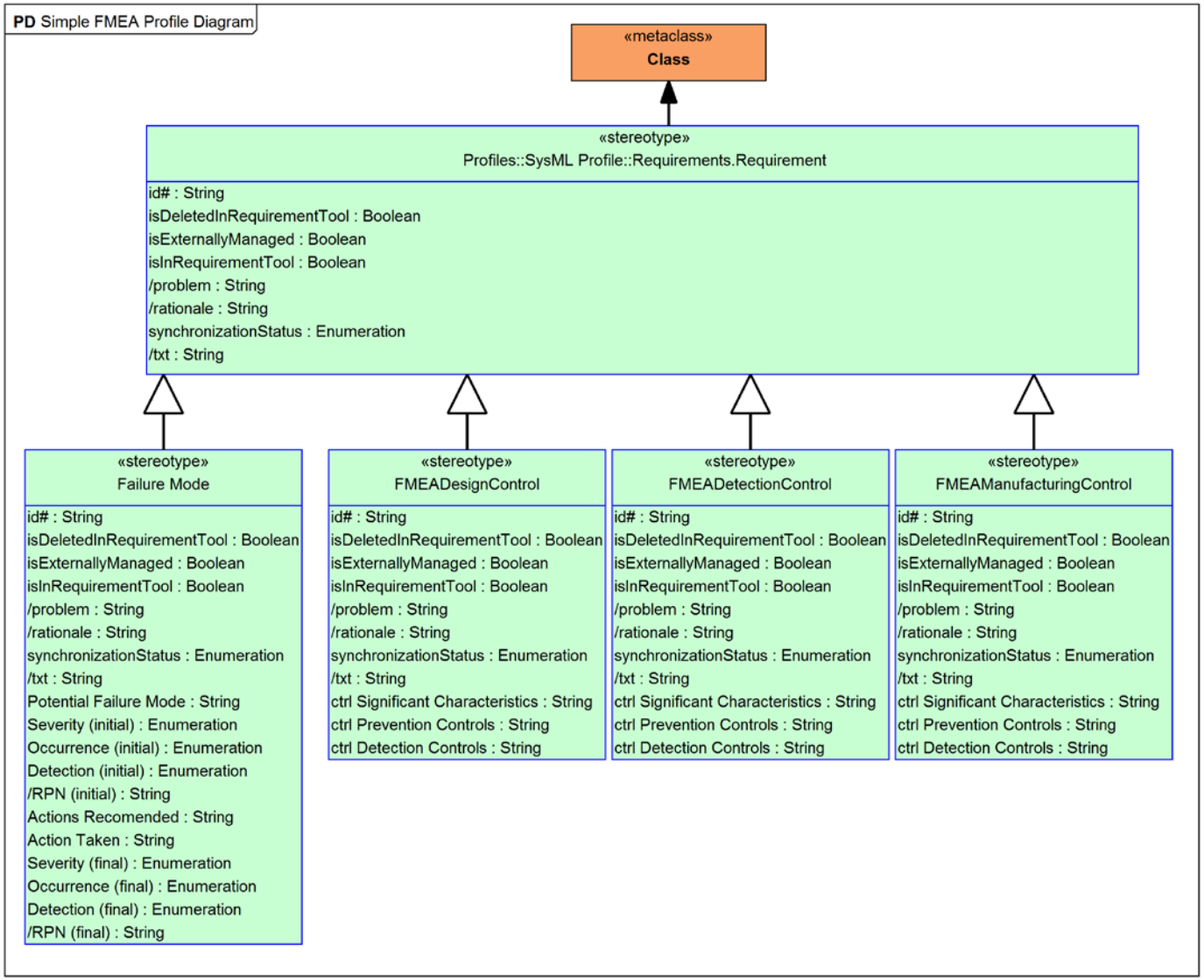
- MBSE Solutions Meta Structure
- Rolls-Royce FHA
- OMG What's happening.

# MBSE.Solutions Meta Structure

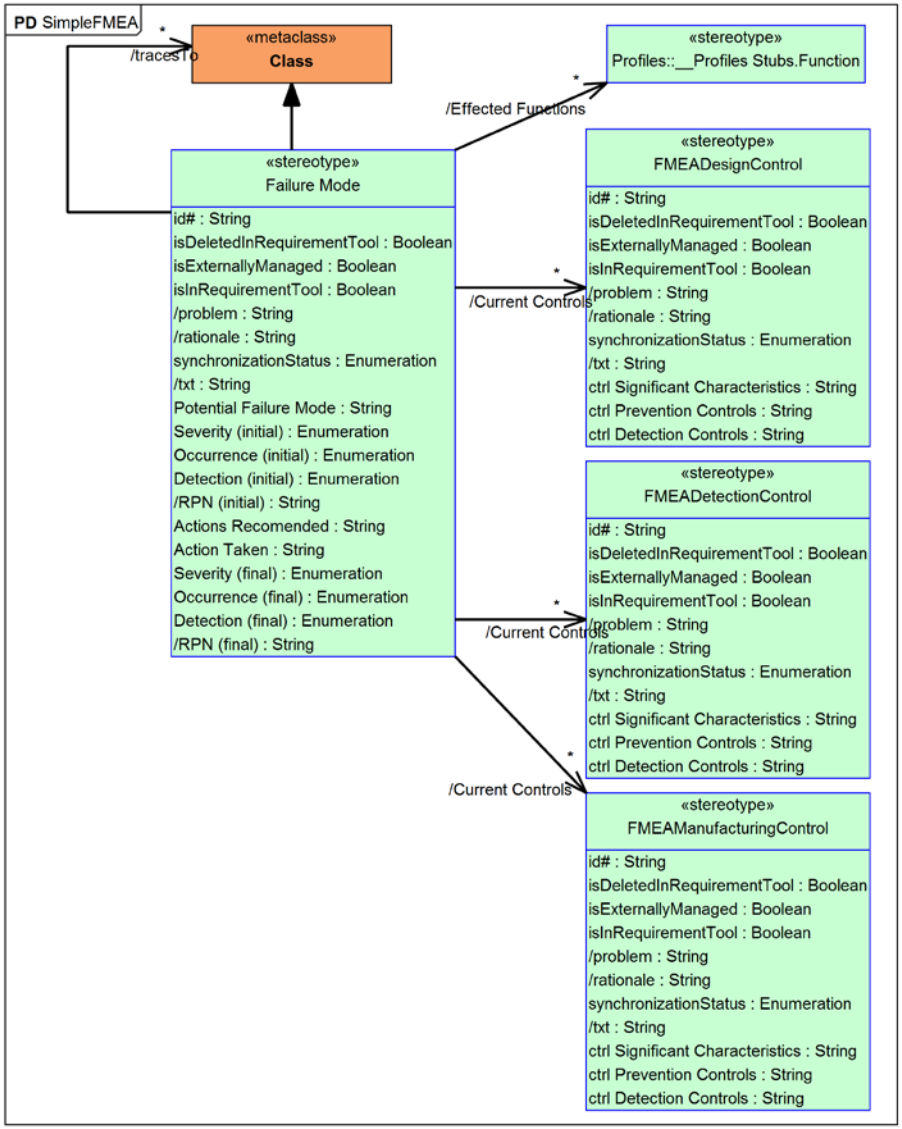


# MBSE.Solutions FMEA Meta Profile continued



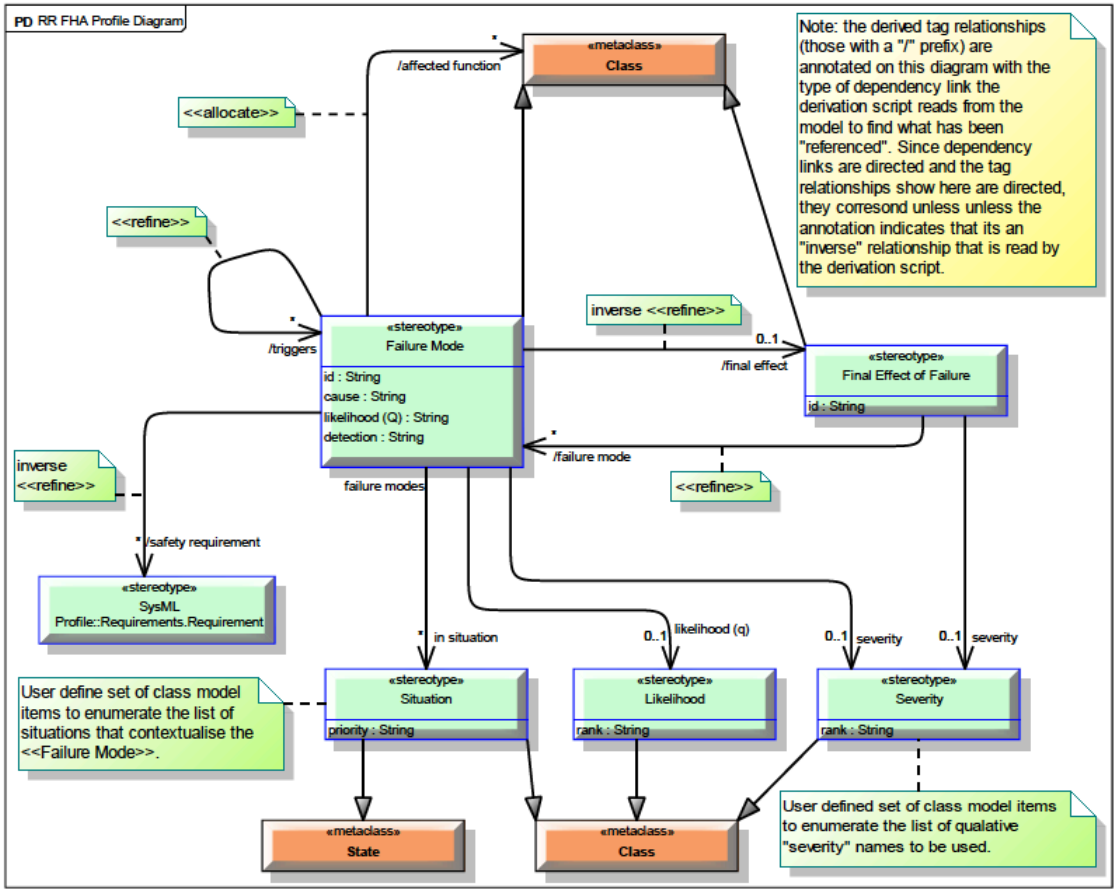
# MBSE.Solutions Meta FMEA Profile




- Tie Failure modes to anything in the model to identify the failing part.
- Or Tie it directly to your Function that is failing because of the form that is allocated to this. (Functional Decomposition/Allocation – see website for ideas.)
- Design Controls point to new requirements, new design elements.
- Detection Control will point to how you identify the failure to the user outputs, or flag errors and let user see them during maintenance
- Manufacturing Controls will point to manufacturing processes or design/behavior you identify in your modeling to help with manufacturability of your system.

# Other Meta FMEA models (Rolls-Royce)

## This profile diagram shows the FHA stereotypes, their value tags, and their reference tag relationships (Dave Banham Global Software Capability Group – Controls SCU Rolls-Royce)




- There are a number of relationships that need to be established between «Failure Mode» and «Final Effect» model items that require the use of «allocate» and «refine» dependency relationships
- These are noted on the affected reference tag connectors on this diagram
- As the reference tag connectors are directed (there is an arrowhead) and as the «allocate» and «refine» dependency relationships are directed, the intent is that the direction of use follows the direction between the stereotypes on the profile diagram, unless otherwise indicated by the use of the word "inverse"

# Safety & Reliability UML OMG submission

## What's happening at the OMG.

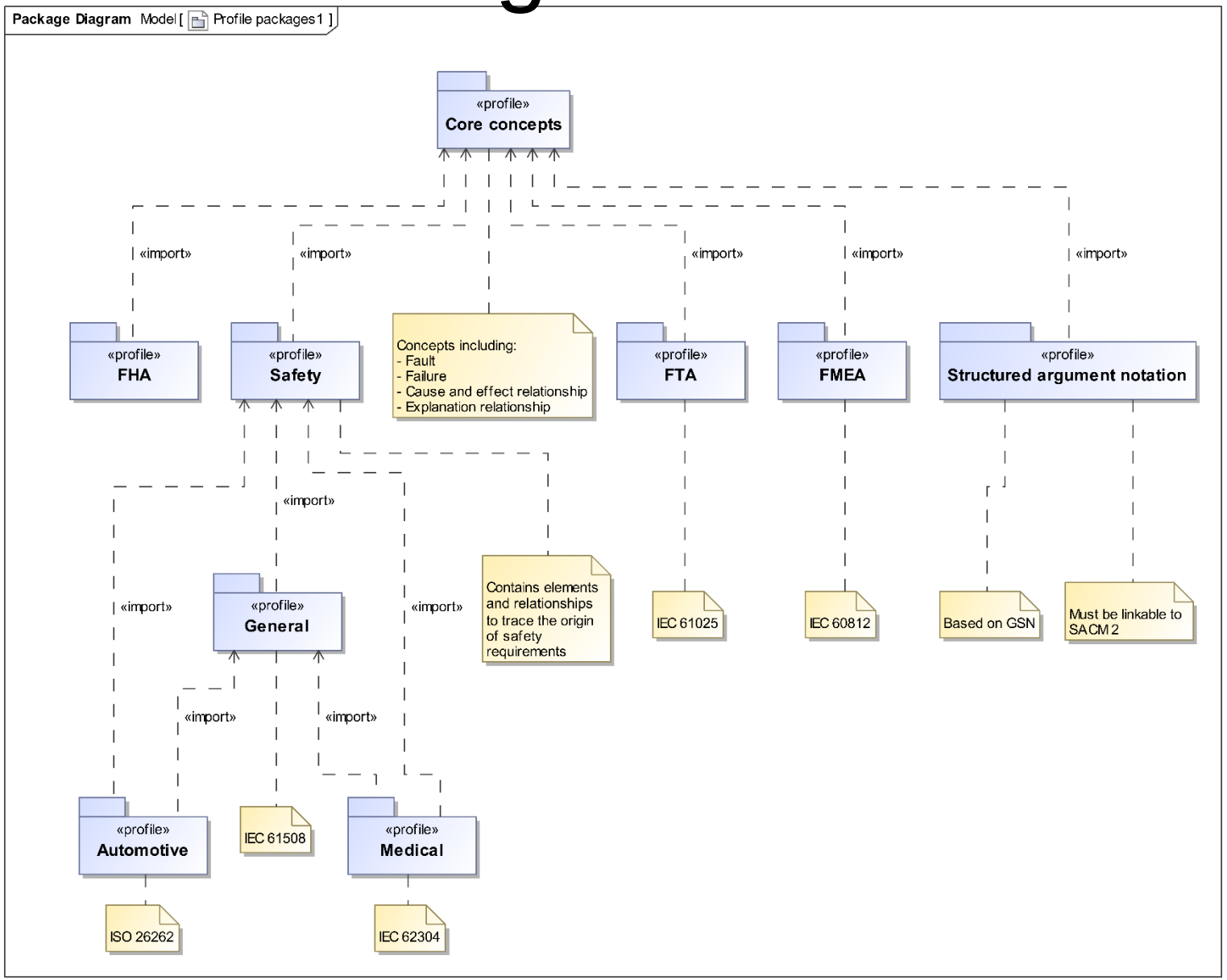
- Background
- Structure
- Mandatory Requirements
- Non-mandatory Requirements

Material is from OMG Briefing (06/25/2017)
Chair: Geoffrey Biggs, National Institute of Advanced Industrial Science and Technology, Japan

# Background

- RFP requests a UML profile for use with SysML
- Profile must provide for modelling:
  - Safety
  - Reliability (FTA, FMEA, fault modelling)
  - Structured assurance case argument visualisation
- Enable the above as an integrated part of a system model
- Enable automation of common tasks that are currently performed manually
- RFP issued in March 2017 meeting

# Package structure



# Mandatory Requirements

| Requirement - General | Status |
|---|---|
| Profile to extend SysML with safety and reliability features | In progress |
| Be compatible with ReqIF and don’t break SysML’s compatibility | Not started |
| Support traceability between system, safety and reliability | Supported |
| Be extensible to additional domains | Not started |
| Suitable diagrams for displaying safety and reliability information | Supported |
| Tabular views | Supported |
| Support model transforms | Supported |
| Model properties such as probabilities and severities | Supported |

Most supported features are nevertheless incomplete and subject to change

# Mandatory Requirements

| Requirement – Safety information | Status |
|---|---|
| Provide support for one or more domains from aerospace automotive, medical, railways | Supported |
| Comply with existing safety standards in relevant domains | Supported |
| Support the assignment of integrity levels | In progress |

| Requirement – Reliability information | Status |
|---|---|
| Support modelling Fault Tree Analysis in compliance with IEC 61025 | In progress |
| Provide a method to mark an FTA as complete or incomplete | Not started |
| Support modelling FMEA/FMECA in compliance with IEC 60812 | Supported |
| Provide a method to mark an FMEA/FMECA as complete or incomplete | Not started |

Most supported features are nevertheless incomplete and subject to change

# Mandatory Requirements

| Requirement – Model transformations | Status |
|---|---|
| APIs supporting the extraction of safety/reliability information from a combined system/safety/reliability model | Not started |
| Support for the reverse of the above | Not started |
| Make the above deterministic and repeatable | Not started |

| Requirement – Argument specification | Status |
|---|---|
| Support specifying safety assurance case arguments | Supported |
| Represent the above in a visual manner | Not started |
| Integration with the system model | Supported |
| Support for showing the derivation of a safety goal in a single diagram | Supported |
| Support modular safety assurance case arguments | Not started |

Most supported features are nevertheless incomplete and subject to change

# Mandatory Requirements

| Requirement – Fault modelling | Status |
|---|---|
| Support modelling faults in system elements | Not started |
| Allow modelling the propagation of faults | Not started |
| Integrate fault modelling features with FTA and FMEA/FMECA | Not started |
| Support modelling the context in which a fault occurs | Not started |
| Support modelling the connection between faults and their results | Not started |
| Support modelling the connection between faults and their counter-measures | Not started |

Most supported features are nevertheless incomplete and subject to change

# Non-mandatory features

| Feature | Status |
|---|---|
| Allow use with pure UML models | Will not support |
| Provide direct support for additional safety/reliability analysis methods | Supported (FHA) |
| Provide support for additional domains | None as yet |
| Structure profile so that concepts useful outside safety are usable by other profiles | Will support |
| Provide a mapping from structured argument models to SACM 2 | Intend to support |
| Use SACM 2 to provide structured argument modelling support | Will not support |

# Next Steps?

- **FMEA should be a team effort**
  - Members should be experts of every aspect affecting the process.
  - Every member should be able to establish the scope, boundaries and goal of the study
- **Better scoring system to ensure objectivity**
  - Tools rely on objectivity and eliminates the qualifying characteristics of variables
  - Scoring are only based on educated projections and arriving at the RPN is by multiplying the scores, slight variation will effectively double the RPN score.