29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

Geoffrey Biggs, Tier IV, Inc.

Andrius Armonas, No Magic / Dassault Systemes

OMG standard for integrating safety and reliability analysis into MBSE: Concepts and applications

Outline

- Motivation and history
- Current status of the specification for integrating safety and reliability analysis into MBSE
  - The structure of the specification
  - Methods covered
- Core concepts, implementation principles
- Demonstration of model-based FMEA
- Future plans

Terms and definitions

- Reliability
  - Ability of a functional unit to perform a required function under given conditions for a given time interval

ISO/IEC 2382:2015 Information Technology

- Safety
  - Freedom from unacceptable risk

IEC 61508:2010 EEPE safety-related systems

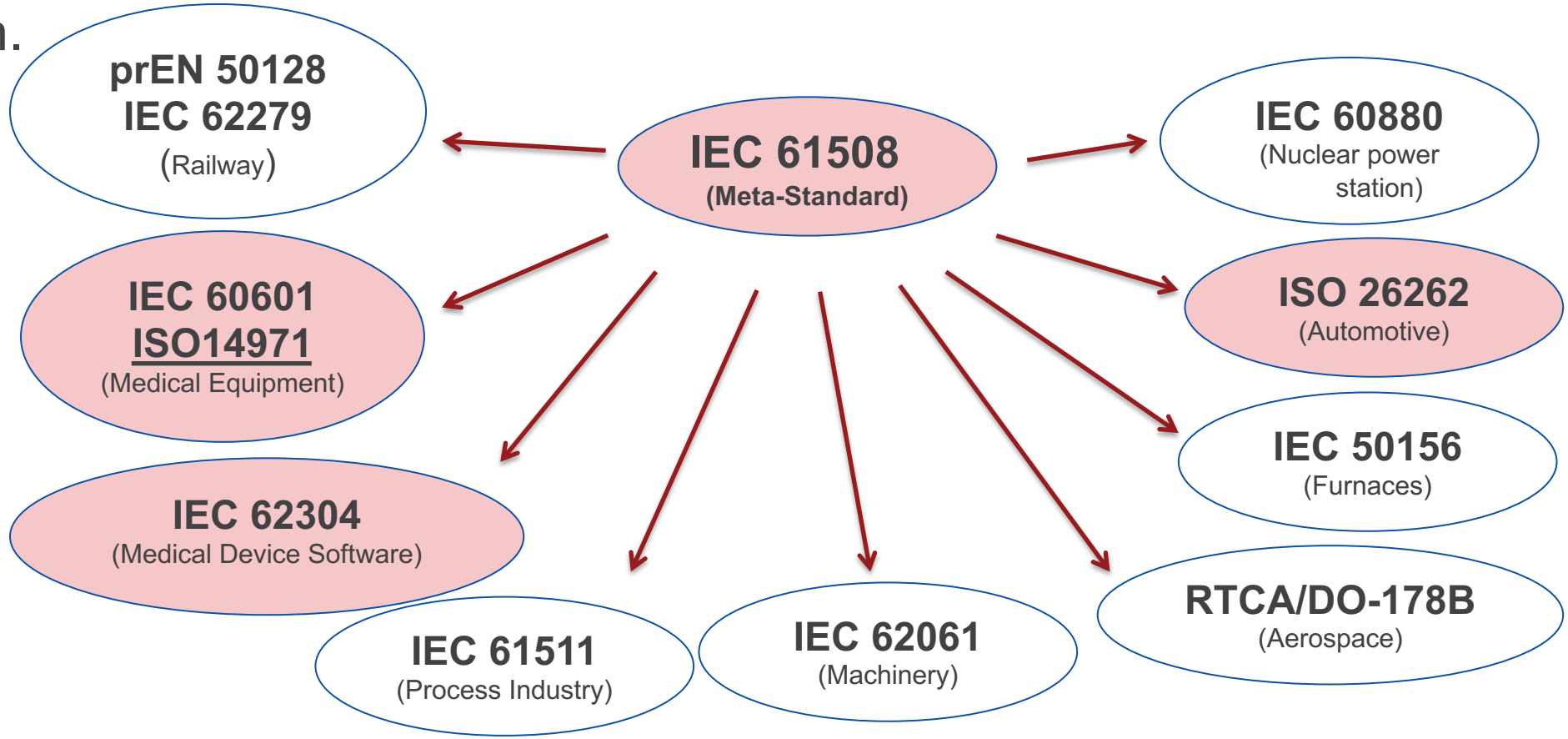
Terms and definitions

- The objective of functional safety is freedom from unacceptable risk of:
  - physical injury or
  - damage to the health of people either directly or indirectly (through damage to property or to the environment)

https://en.wikipedia.org/wiki/Functional_safety

Safety Standards

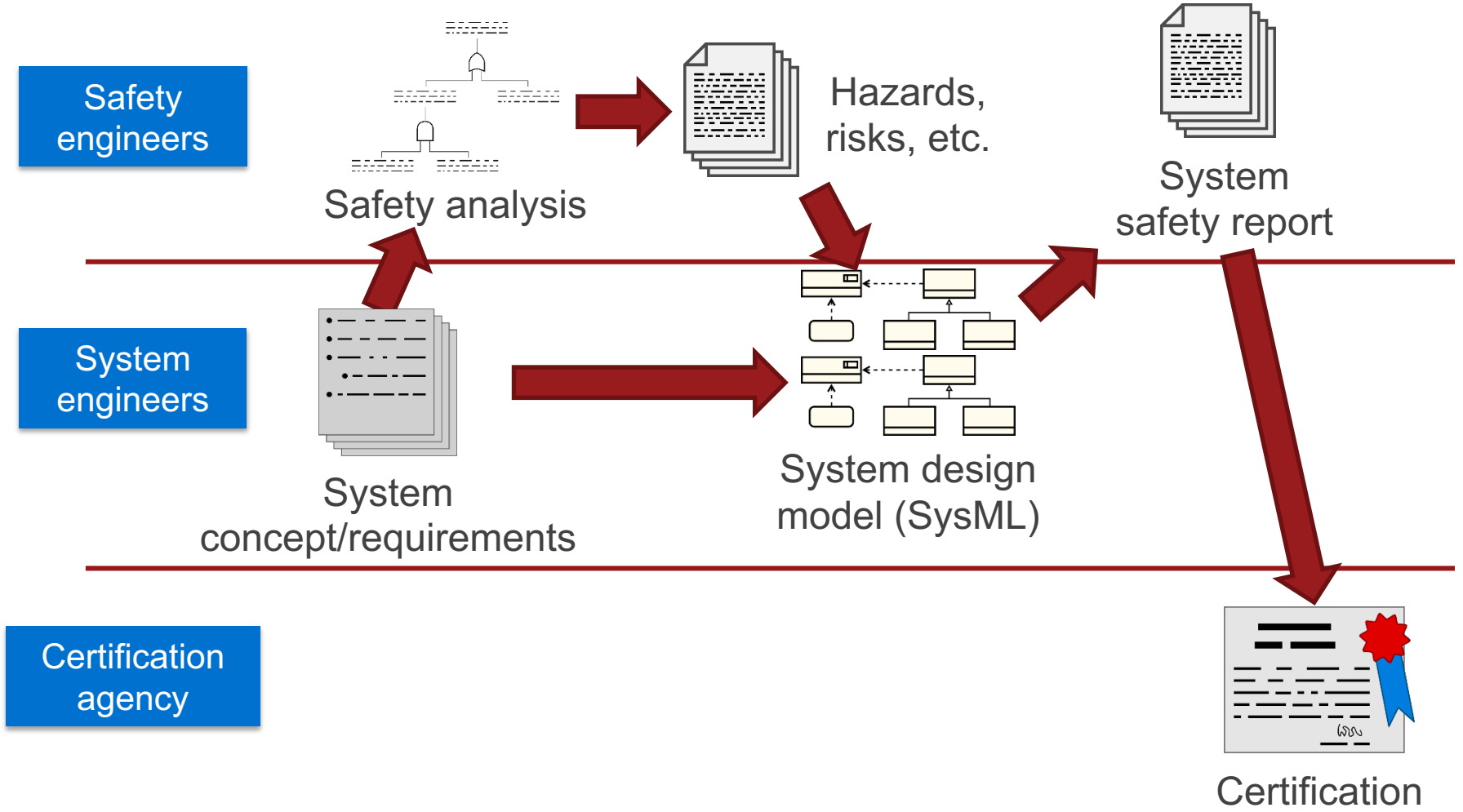
- Each industry has developed domain specific ISO standards, derived from IEC 61508 that reflect more accurately the needs and challenges within their domain.



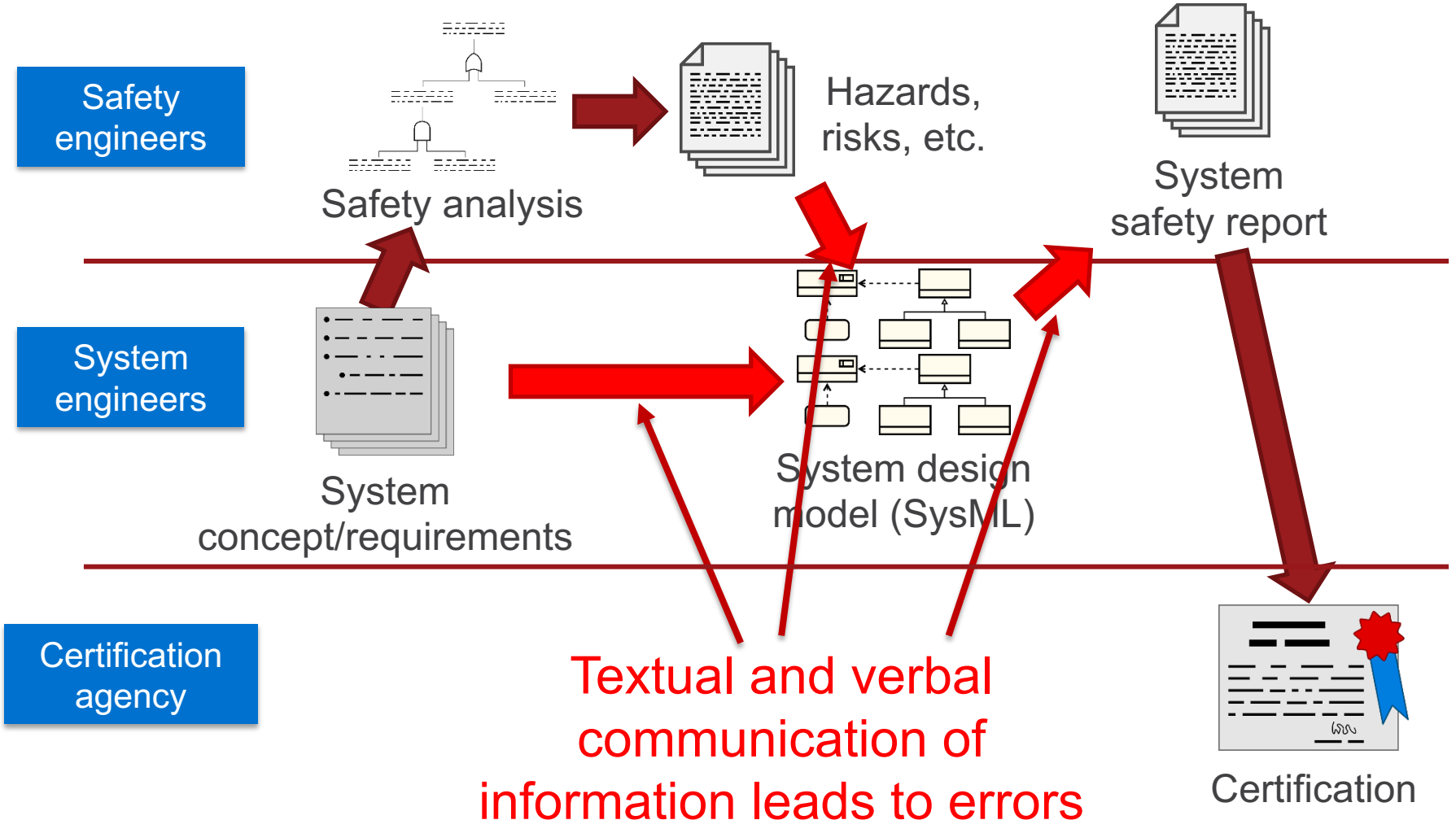
Why do model-based Safety and Reliability?

- Current methods have been in use for decades.
- They seem to work…

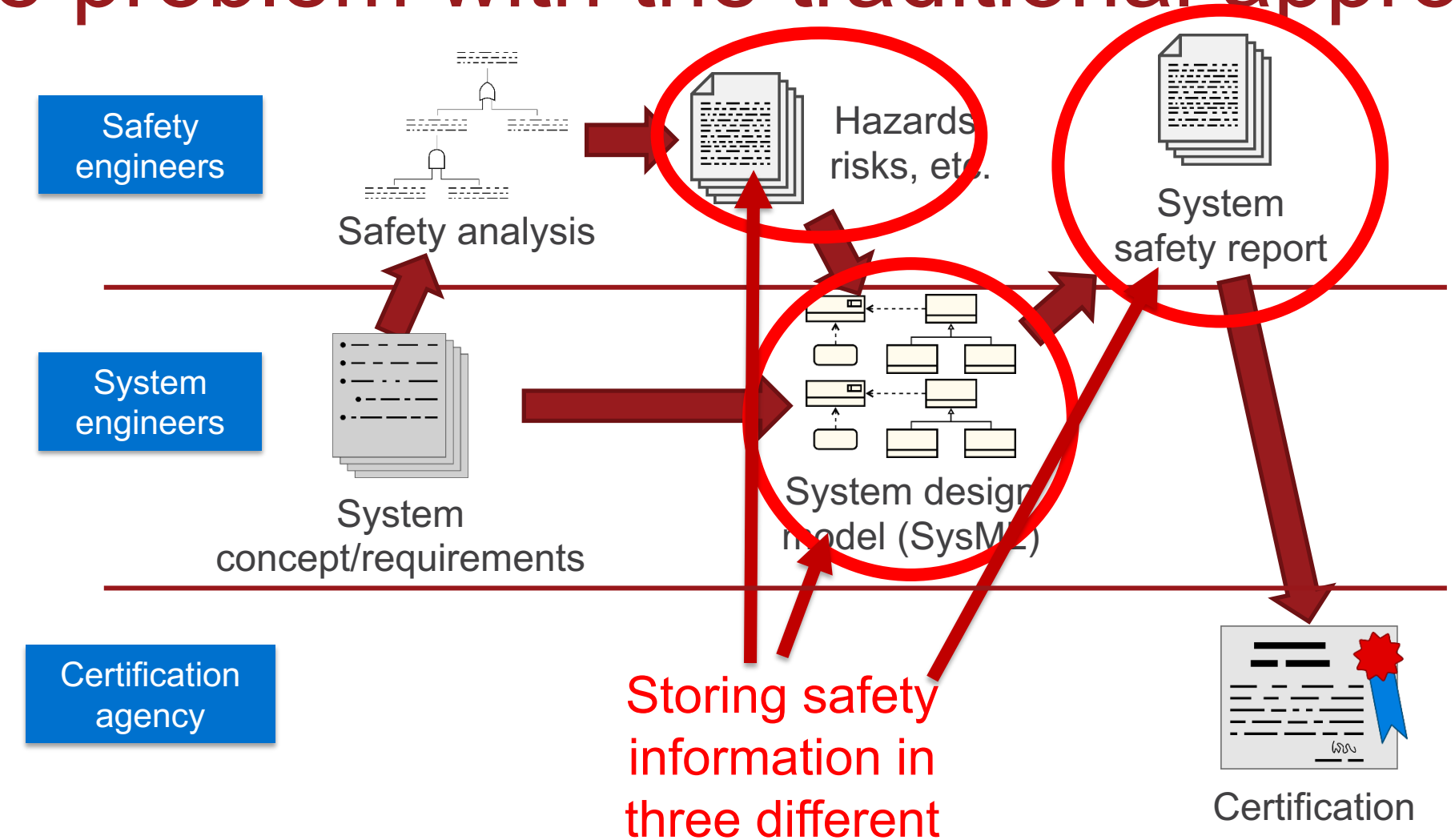
The problem with the traditional approach



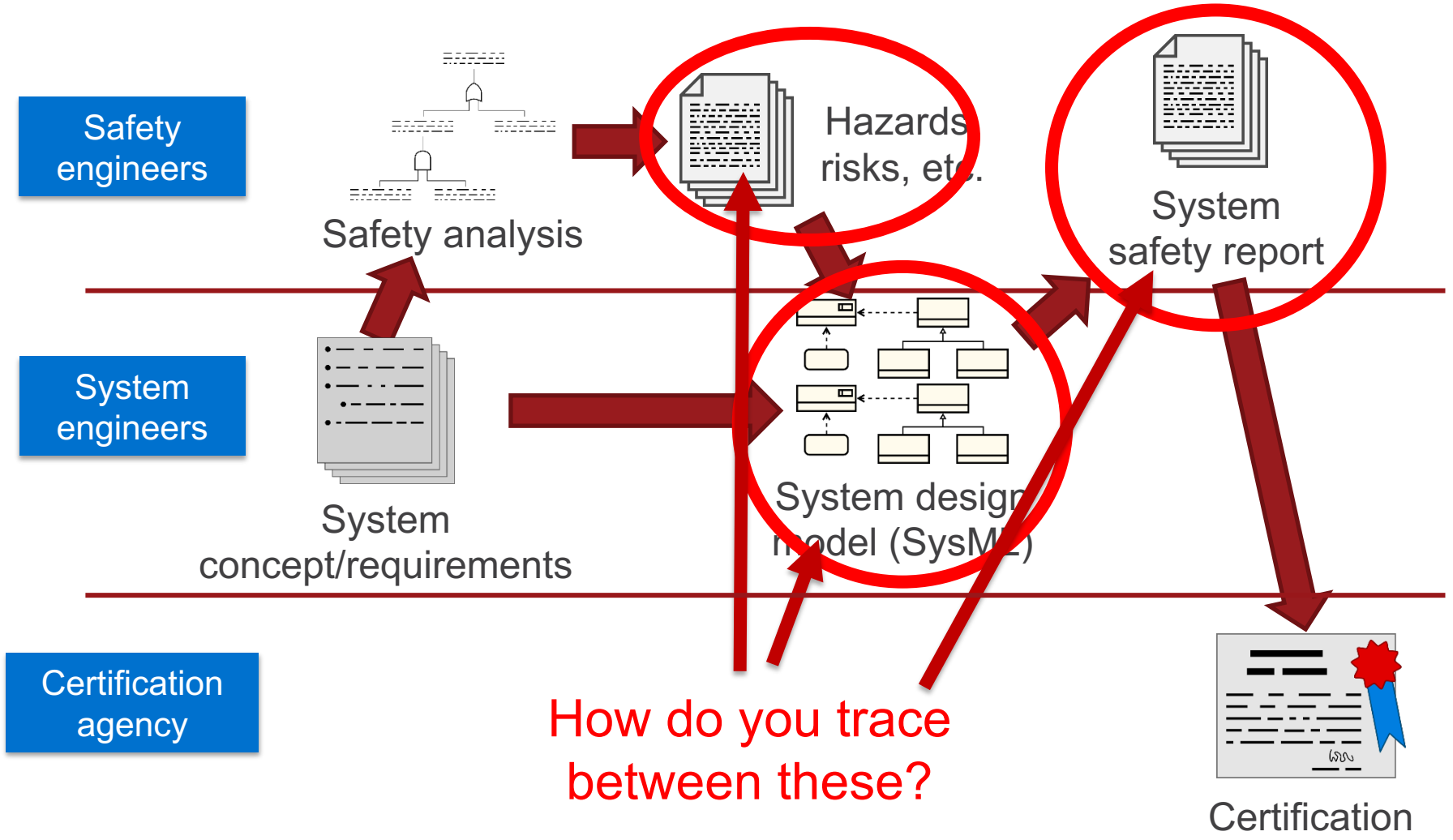
The problem with the traditional approach



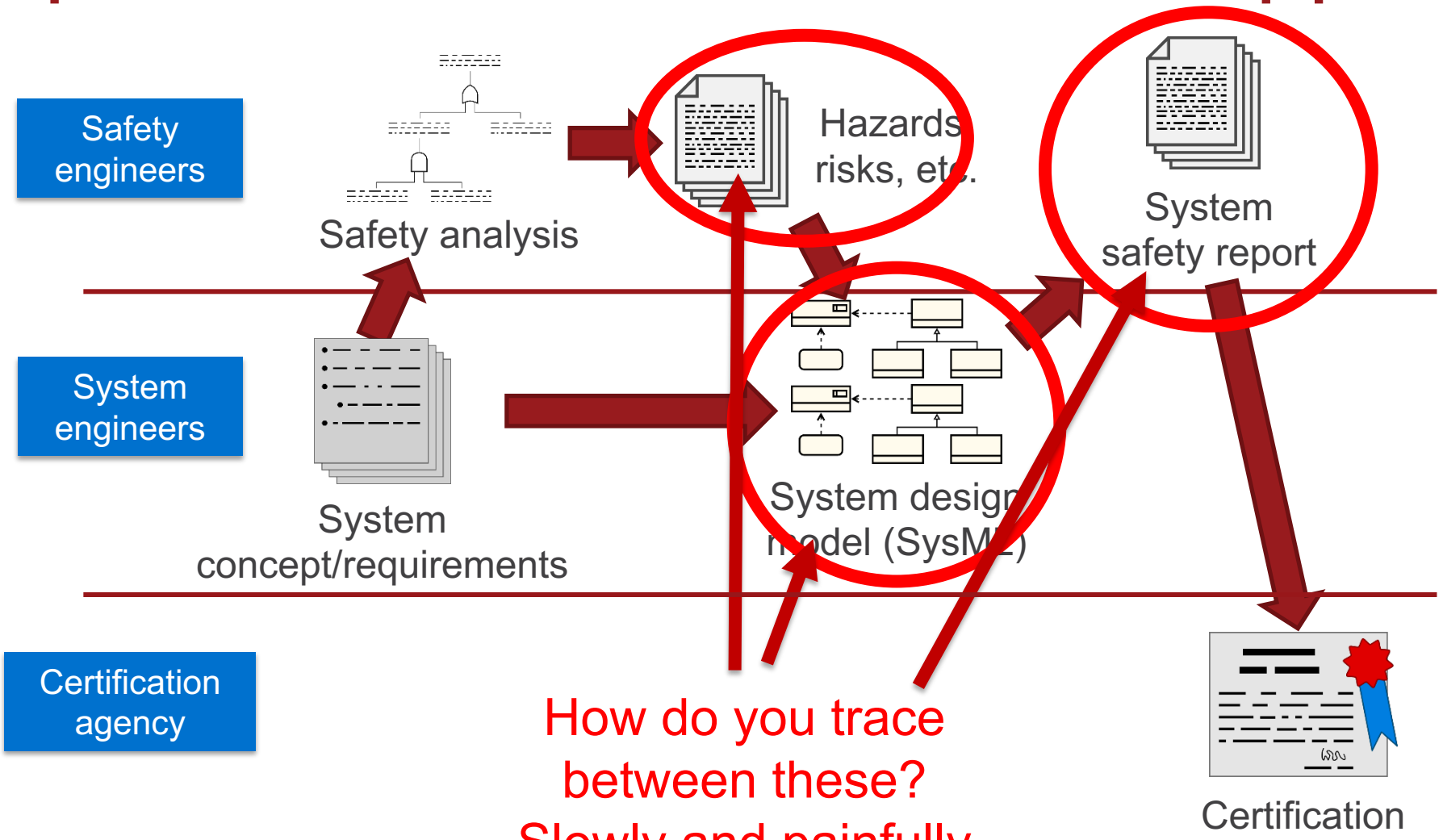
The problem with the traditional approach



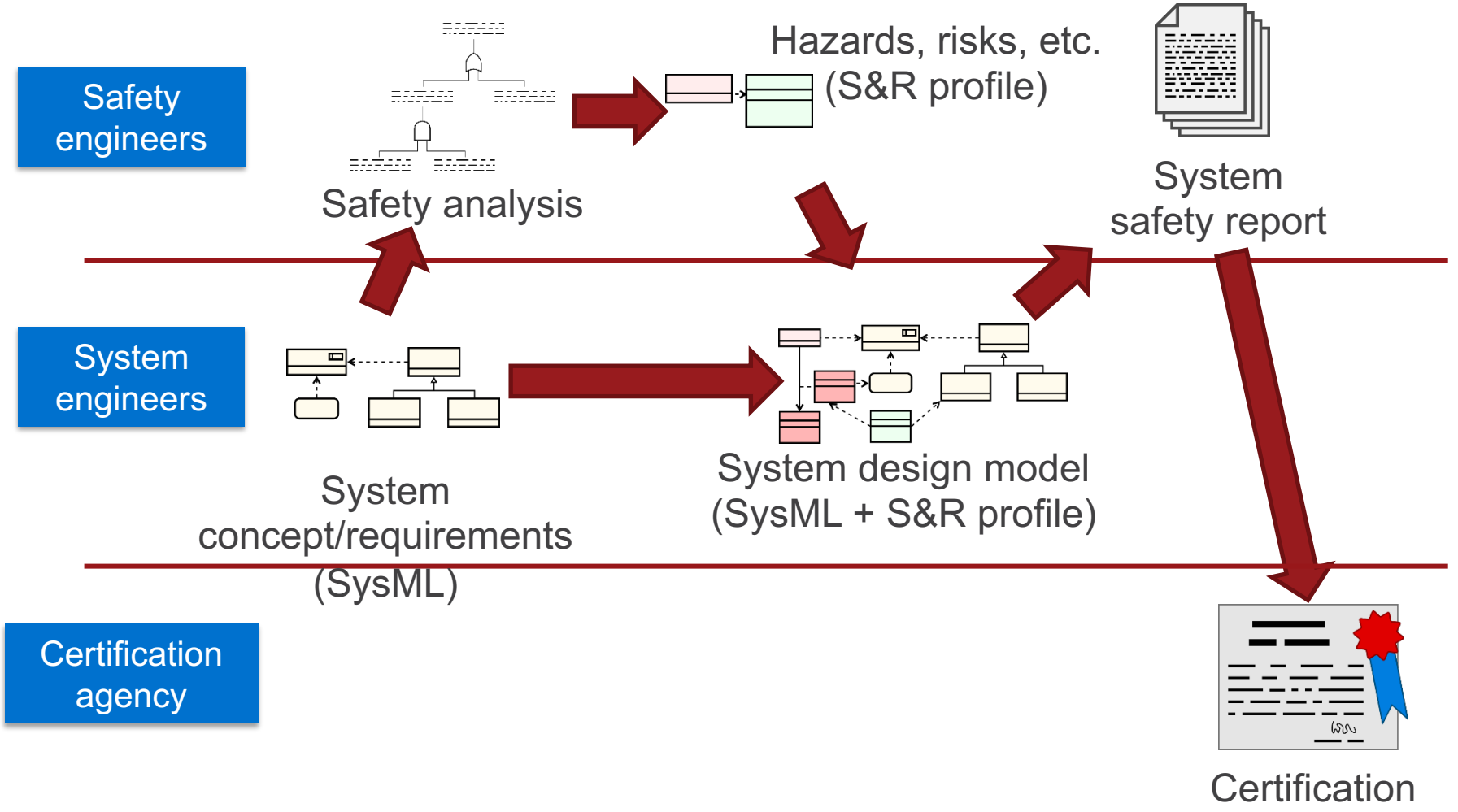
The problem with the traditional approach



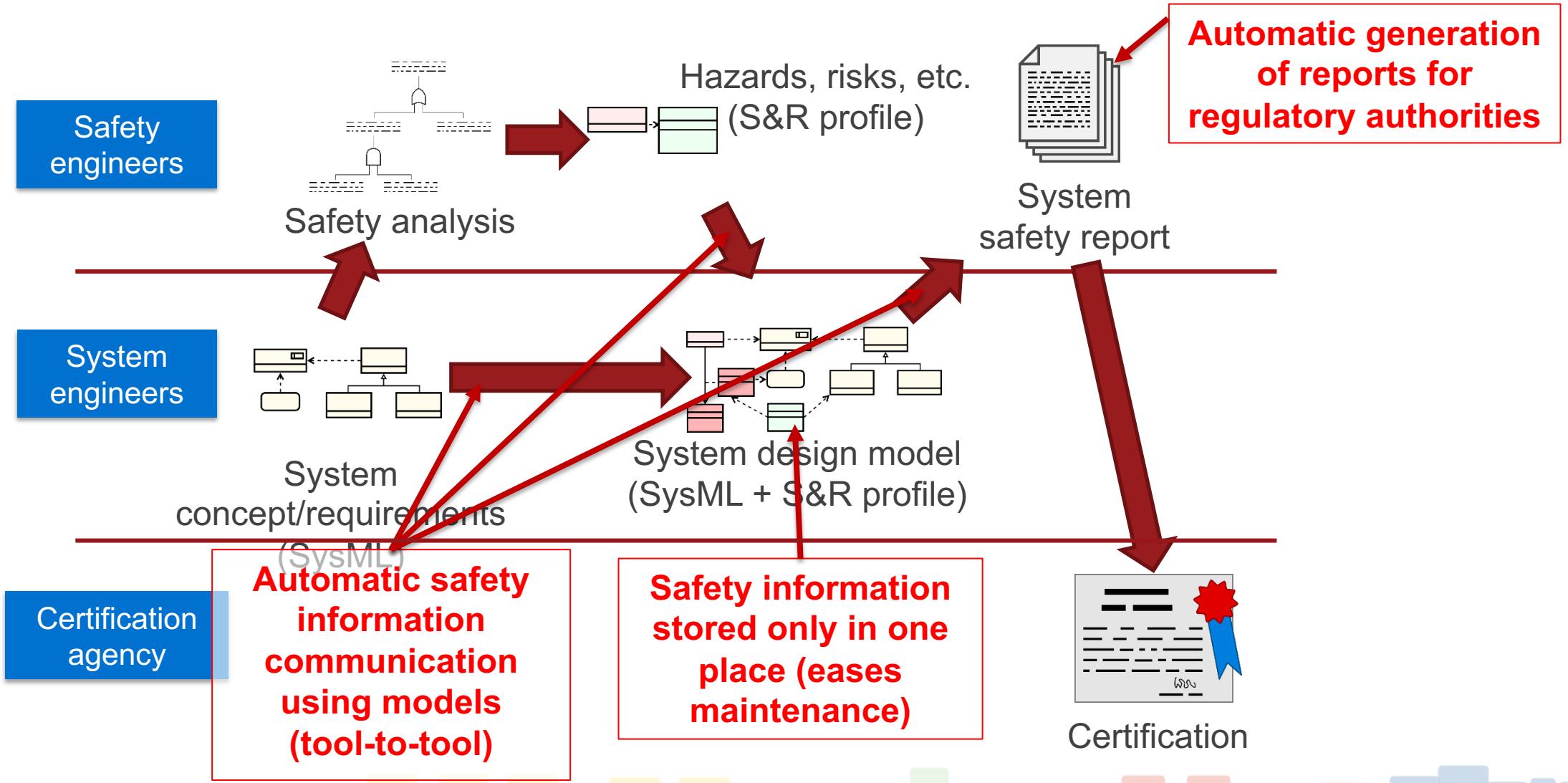
The problem with the traditional approach



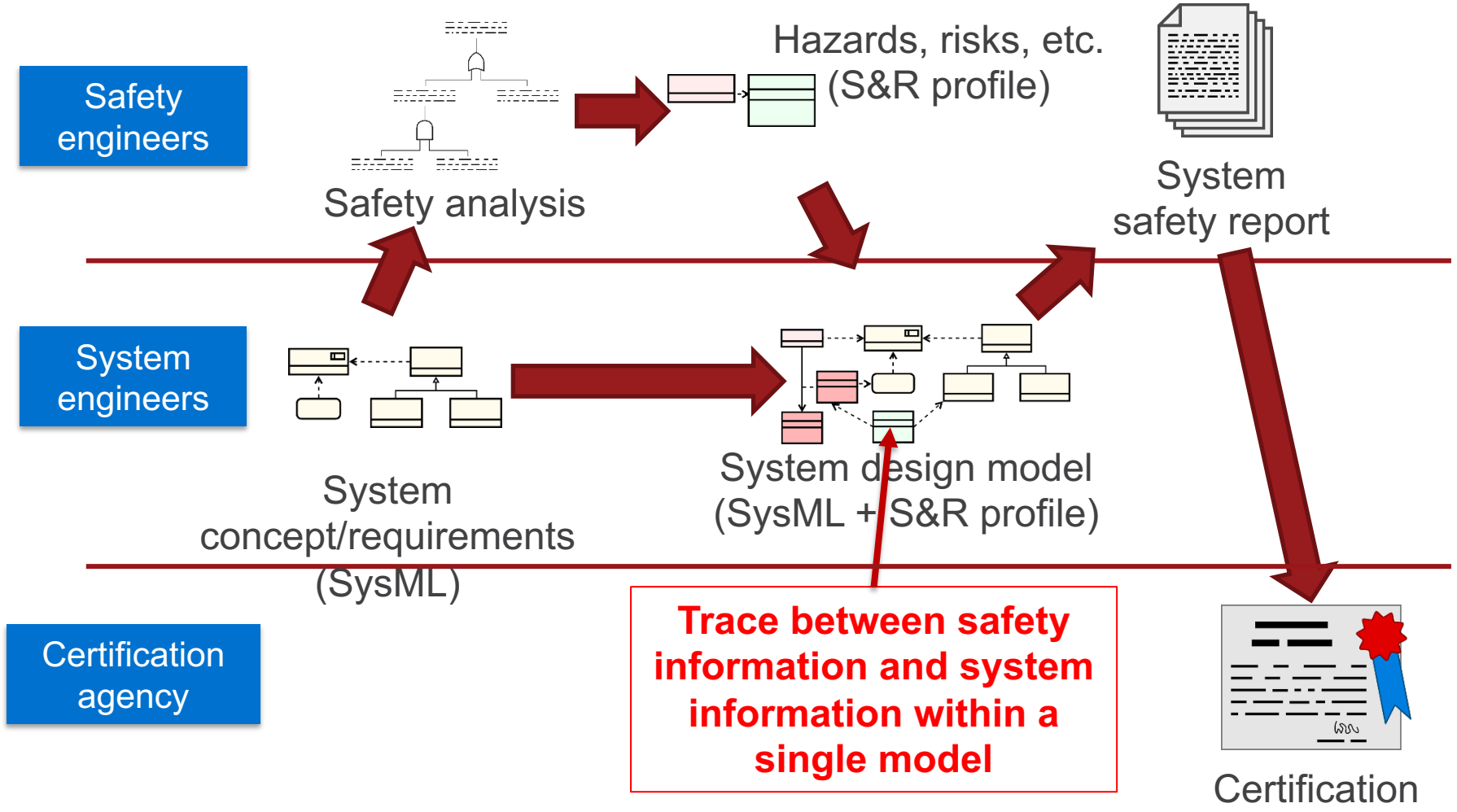
Benefits of a model-based approach



Benefits of a model-based approach



Benefits of a model-based approach



OMG Safety and Reliability profile working group

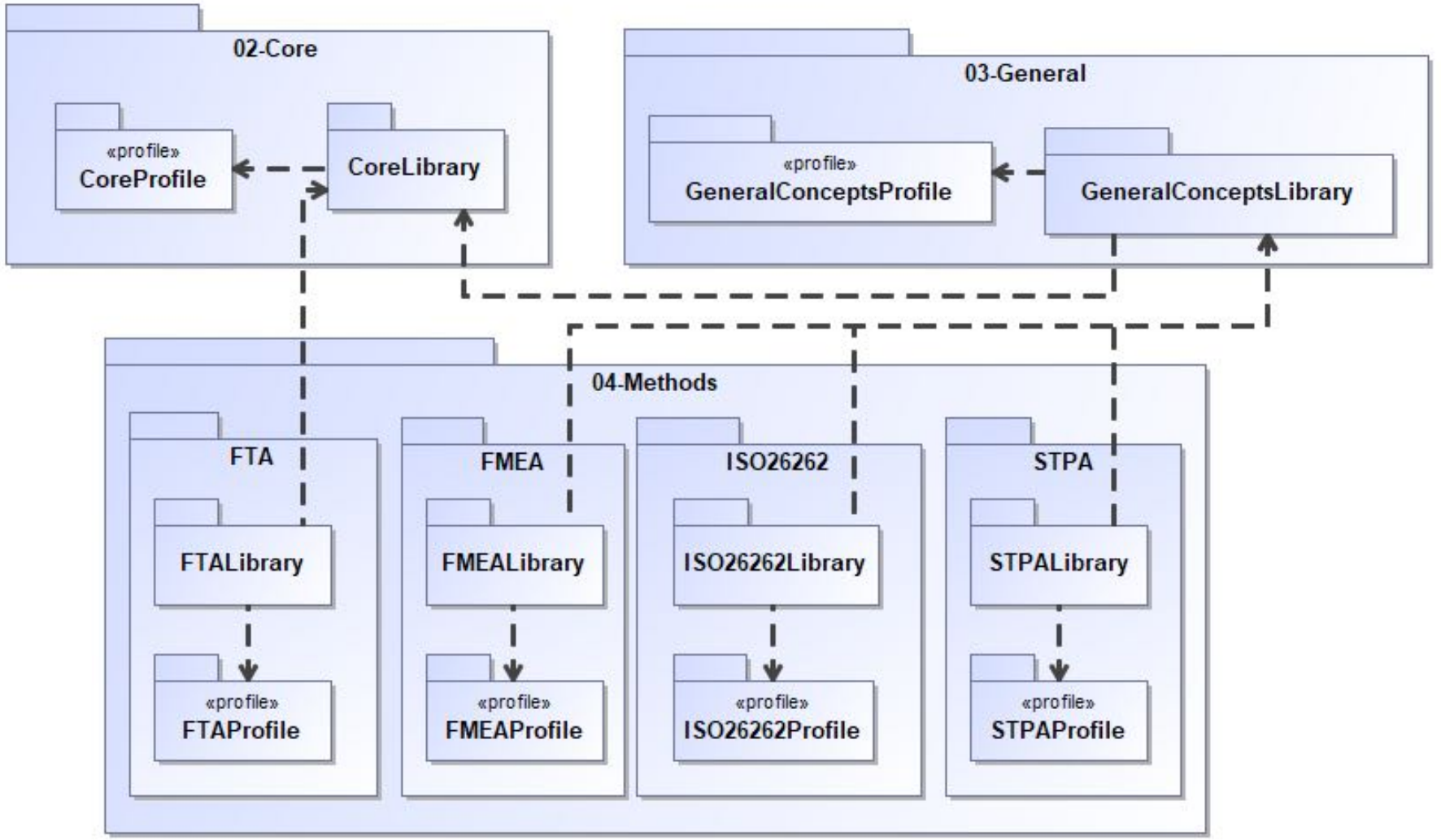
- RFP published by OMG in March, 2017
- Initial version submitted to OMG on Aug 28, 2017
- Current status: revising the specification (until Aug 2019)
- Main contributors of content:
  - Japan's National Institute of Advanced Industrial Science and Technology
  - NASA Jet Propulsion Laboratory
  - France's Alternative Energies and Atomic Energy Commission (CEA)
  - No Magic, Inc. / Dassault Systemes
  - Ford Motor Company
  - GfSE e.V. (the German chapter for systems engineering, Gesellschaft für Systems Engineering)
  - The Aerospace Corporation
- Plus comments from many others

Standards-based

- Based on established international standards as much as possible
- Reliability: IEC 60812 for FMEA and IEC 61025 for FTA
- Safety: IEC 61508 and its offspring
  - Medical software safety: IEC 62304
  - Medical equipment safety: ISO 14971
  - Automotive safety: ISO 26262
  - Other fields welcome, of course!

The library & profile

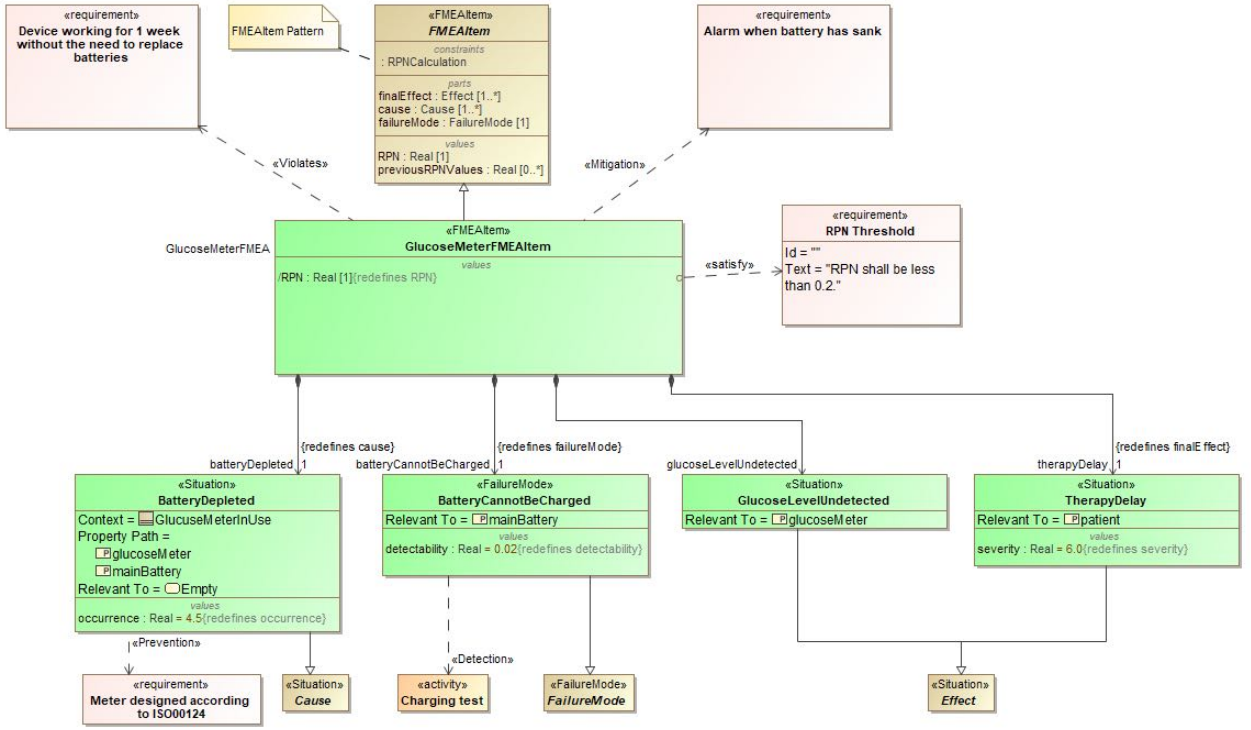
Profile and library structure



Supported Methods

FMEA

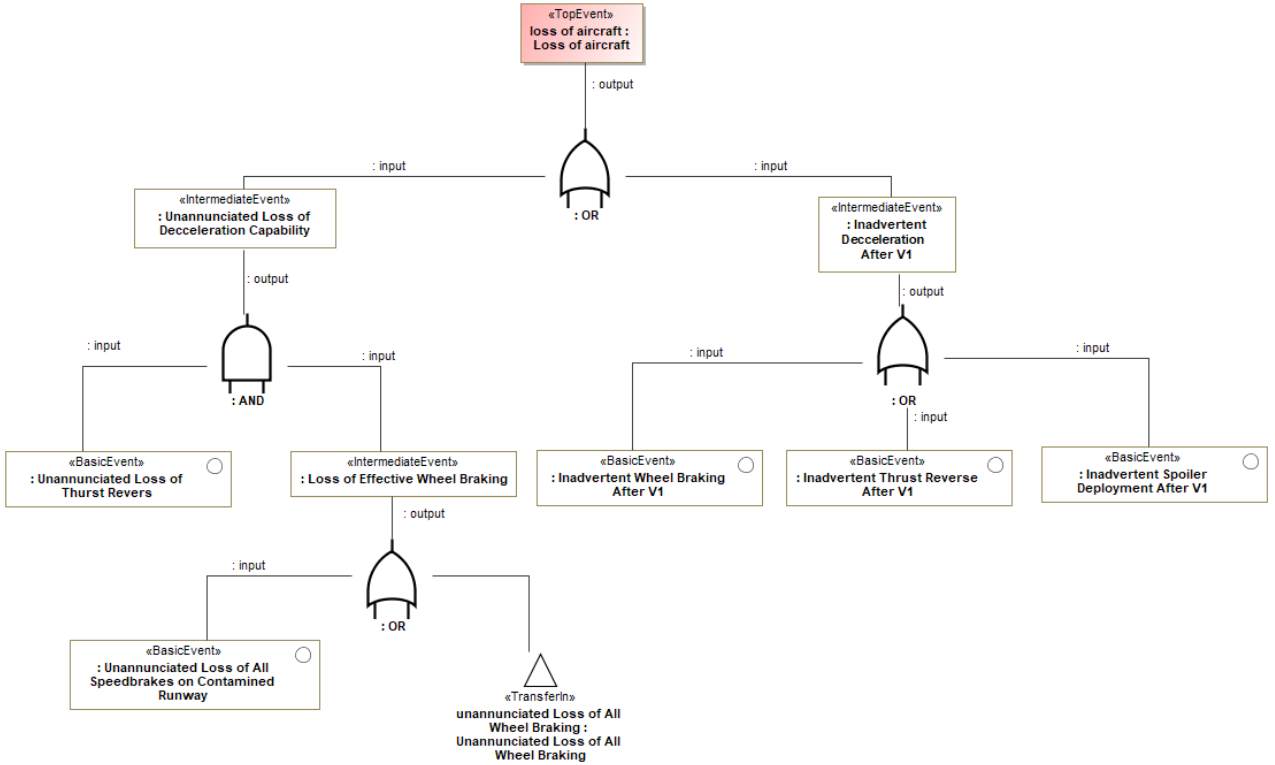
- FMEA (Failure Mode and Effect Analysis) is a bottom-up (or can performed functionally for top-down) methodology designed:
  - to identify potential failure modes for a product, part or process,
  - to assess the risk associated with those failure modes,
  - to rank the issues in terms of importance, and
  - to identify and carry out corrective actions to address the most serious concerns.



IEC 61025

FTA

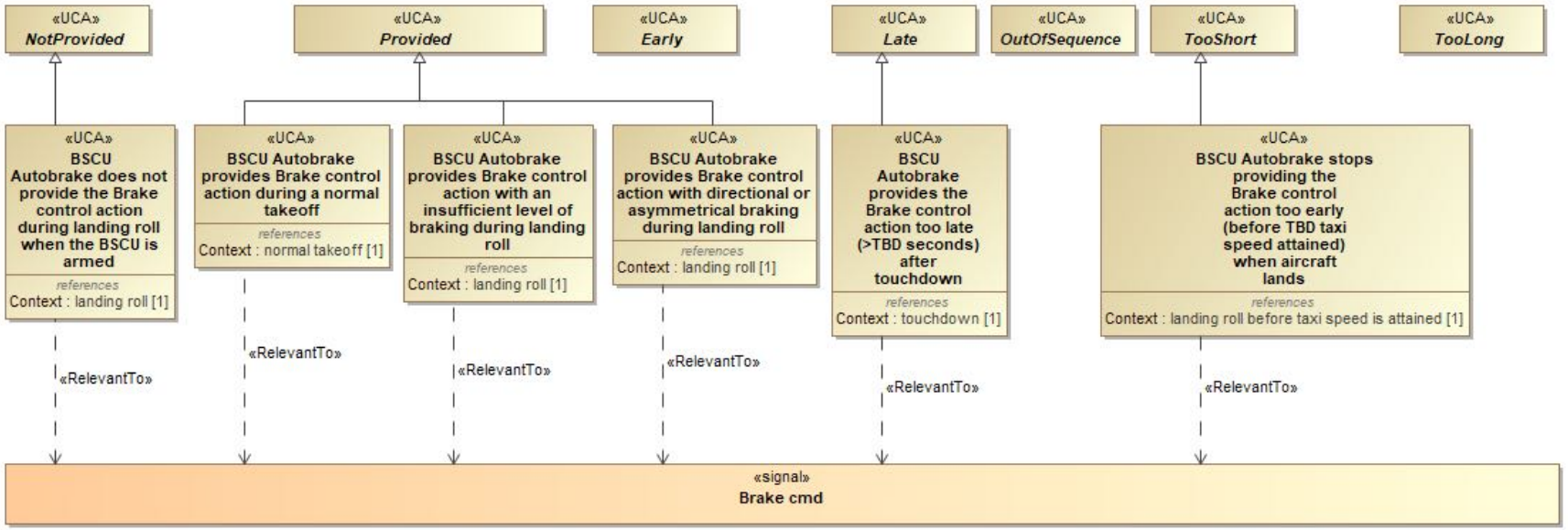
- FTA (Fault Tree Analysis) is a top-down methodology designed:
  - to identify the contributing events to an undesired event across a whole system,
  - to identify how those events combine to enable the undesired event, and
  - to identify the most likely combinations of contributing events for design of preventative actions.



IEC 60812

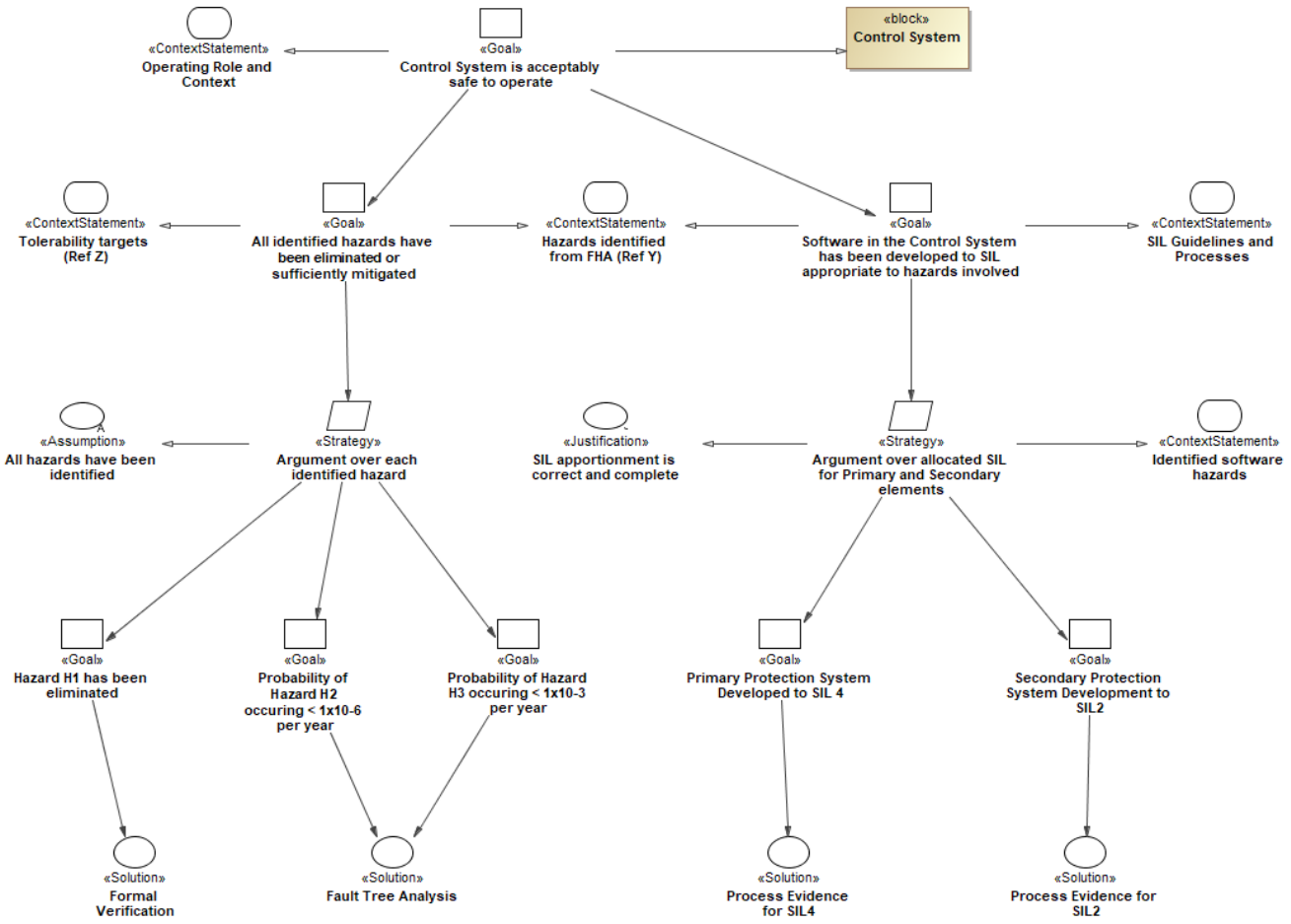
STPA

- STPA (Systems-Theoretic Process Analysis) is a systems and controls theory based exploratory methodology designed:
  - to identify system losses to avoid and the contributing hazards
  - to identify control actions which could lead to a hazard and their causes
  - to identify constraints (requirements) on the system to prevent or mitigate hazards
  - can be applied to cyber-physical systems



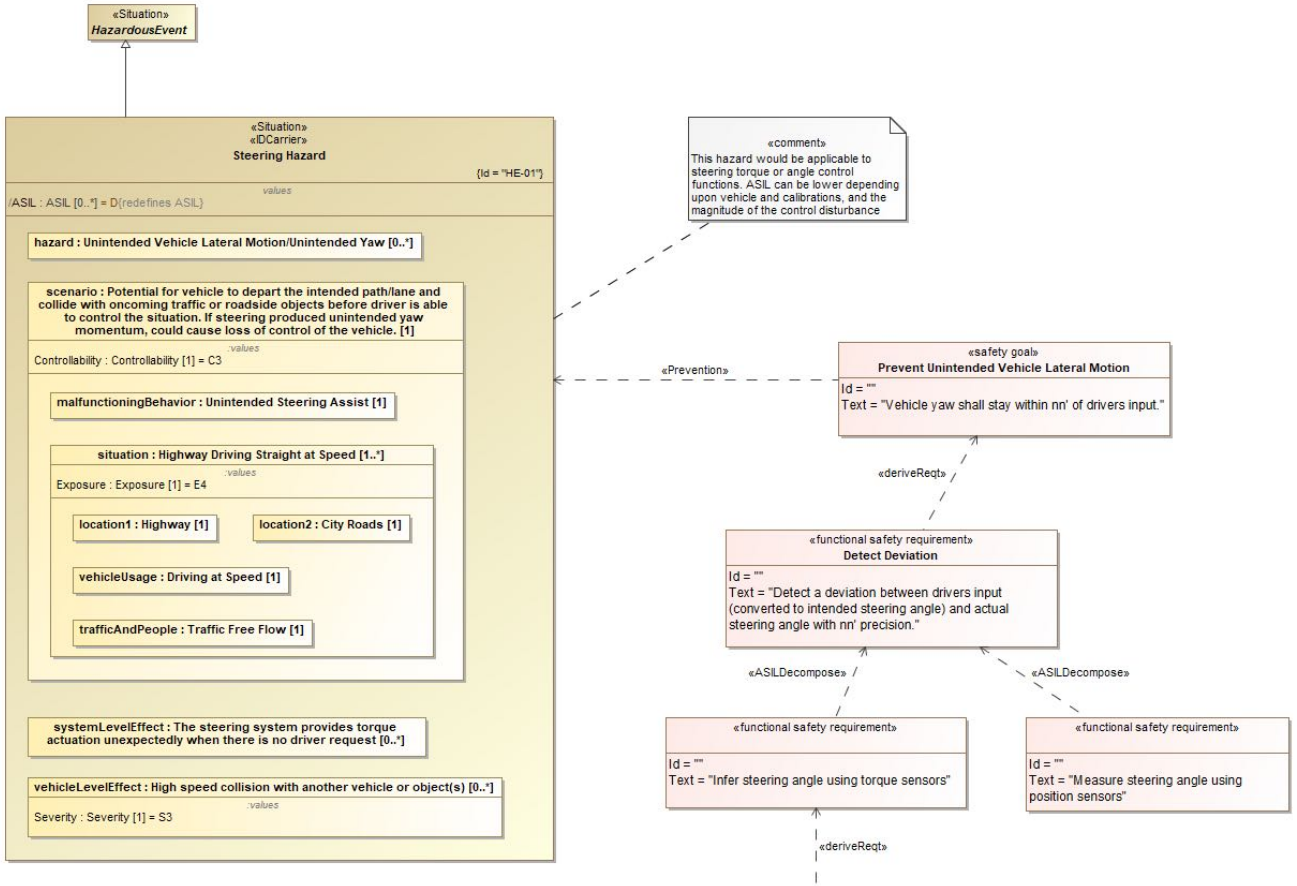
GSN

- GSN (Goal Structured Notation) is a argumentation notation:
  - used to graphically present the proof that that a goal is fulfilled
  - can be used to argue a system's safety case.



ISO 26262

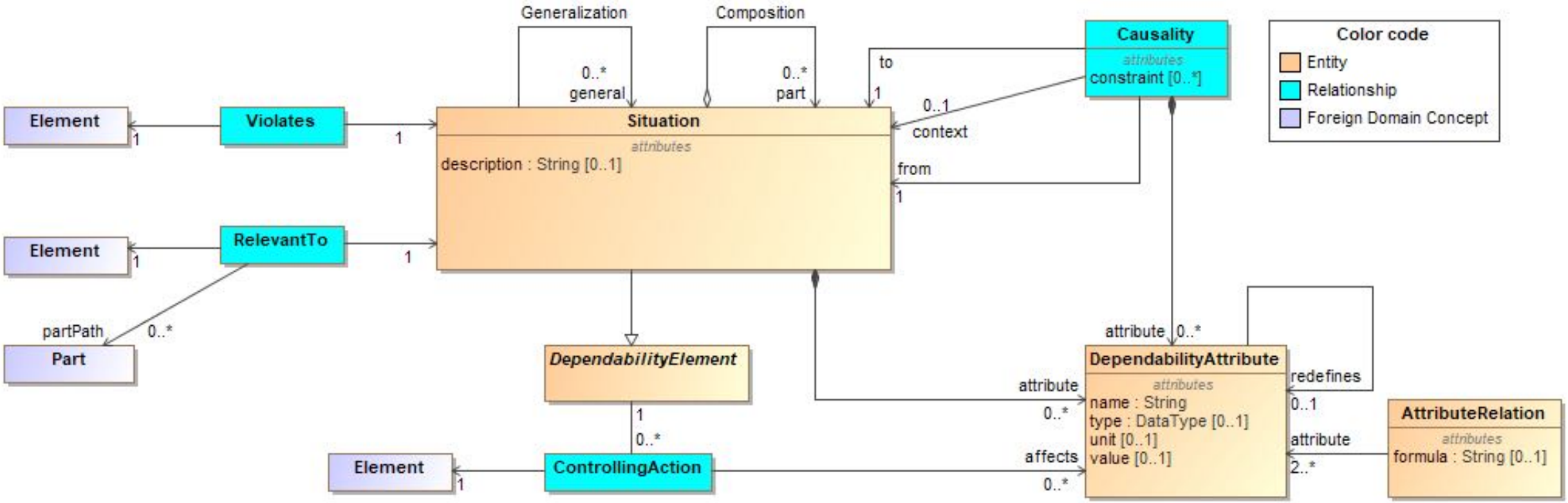
- ISO 26262 (Functional Safety) is a automotive specific functional safety standard:
  - Provides an automotive safety lifecycle
  - Defines a risk-based approach to determine Automotive Safety Integrity Levels



Key concepts

- A core foundation on which to build model-based S&R tools
- Representative profiles for specific domains and methodologies
- Easy to extend to additional domains and methodologies
  - In particular, without needing a long standardization cycle

Core Concepts



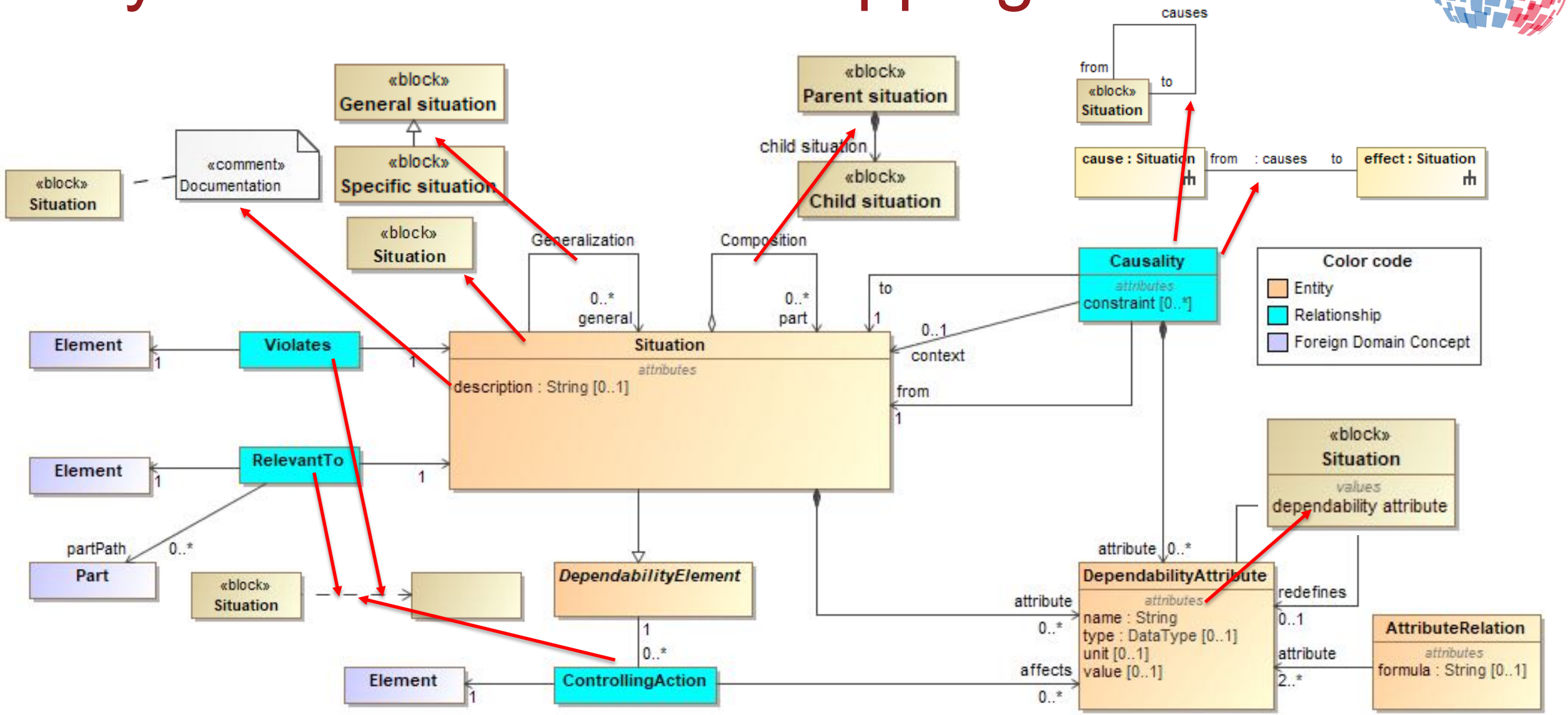
Implementation Approach

- UML Structure-description mechanisms are used
  - Block Definition Diagram/Internal Block Diagram (aka Class diagrams, Composite Structure diagrams for non-SysML people)

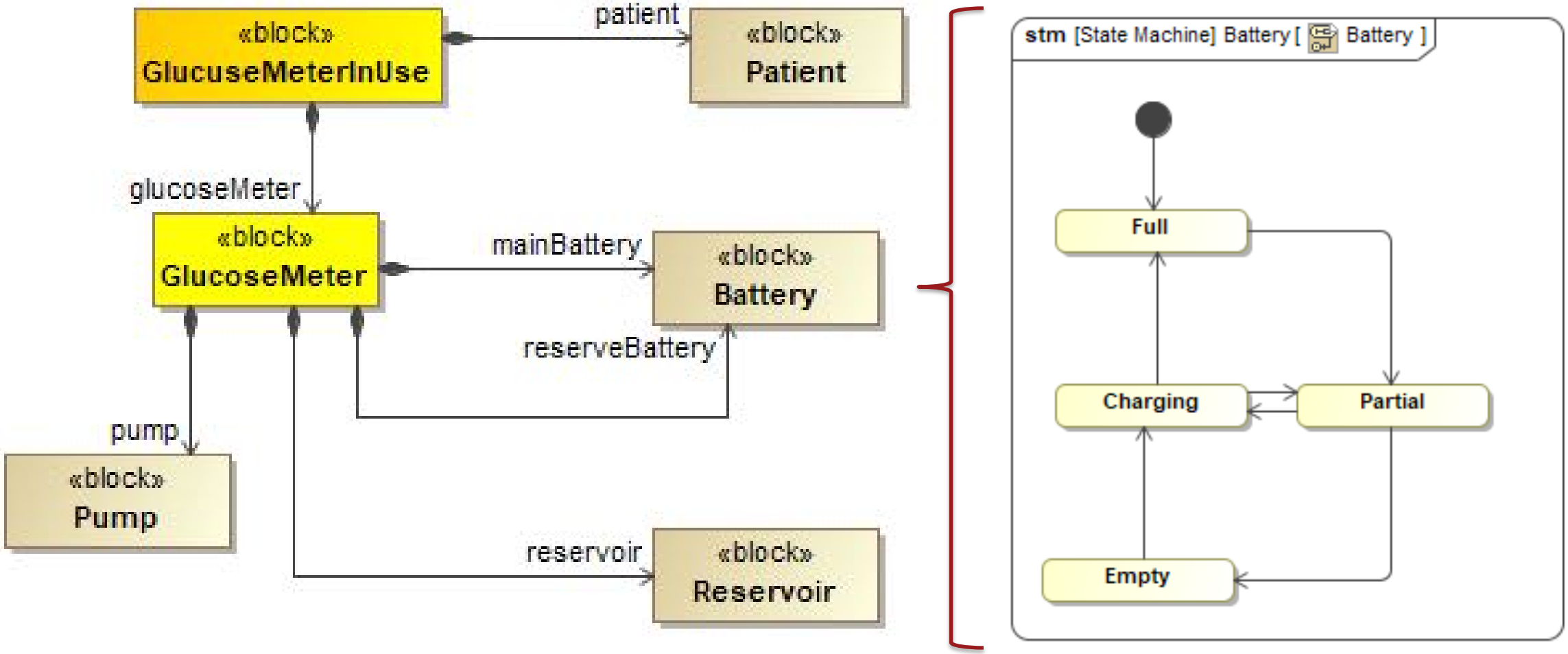
- Effort to reduce the usage of Profiling mechanisms (Stereotypes, Tags) in favor of using more Model Library Approach

- Seems to “rhyme” well with the SysML v2 group efforts!

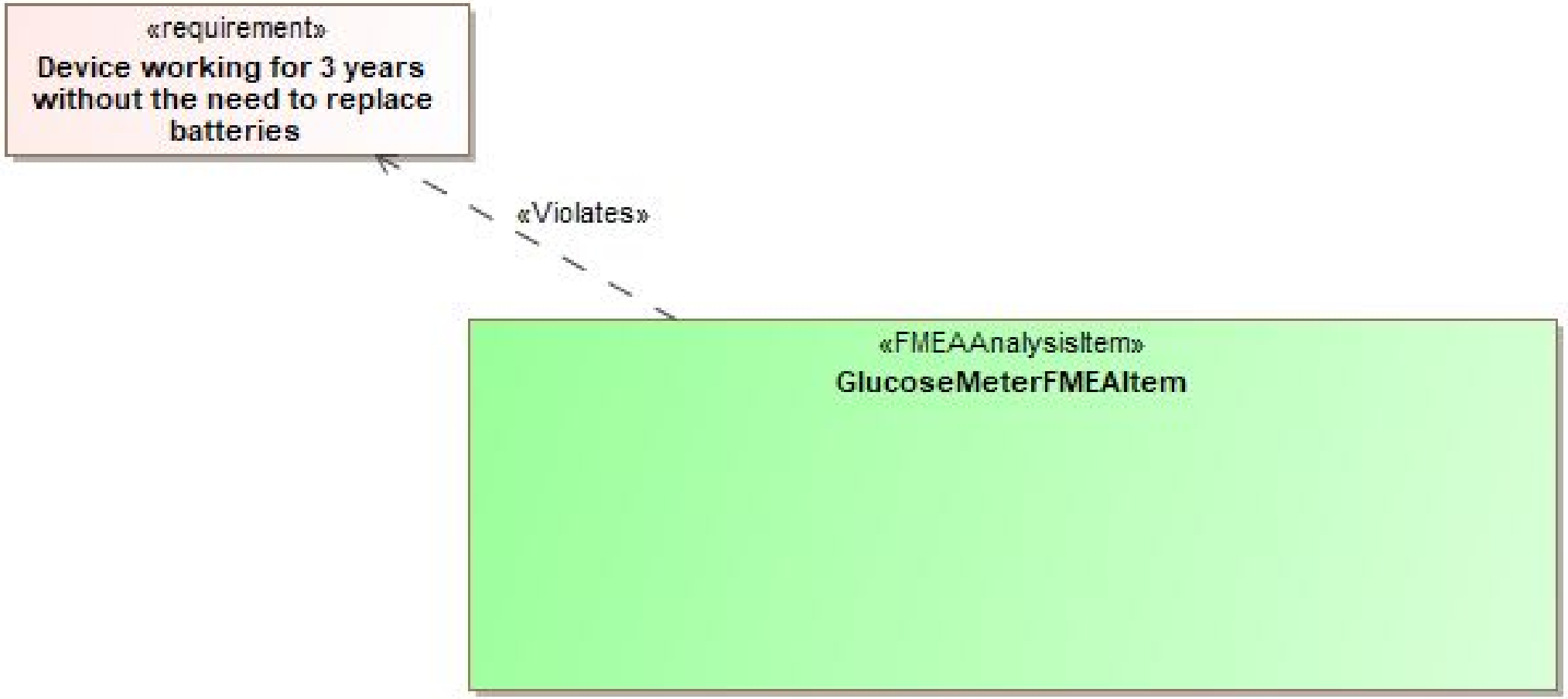
SysML/UML-to-S&R mapping



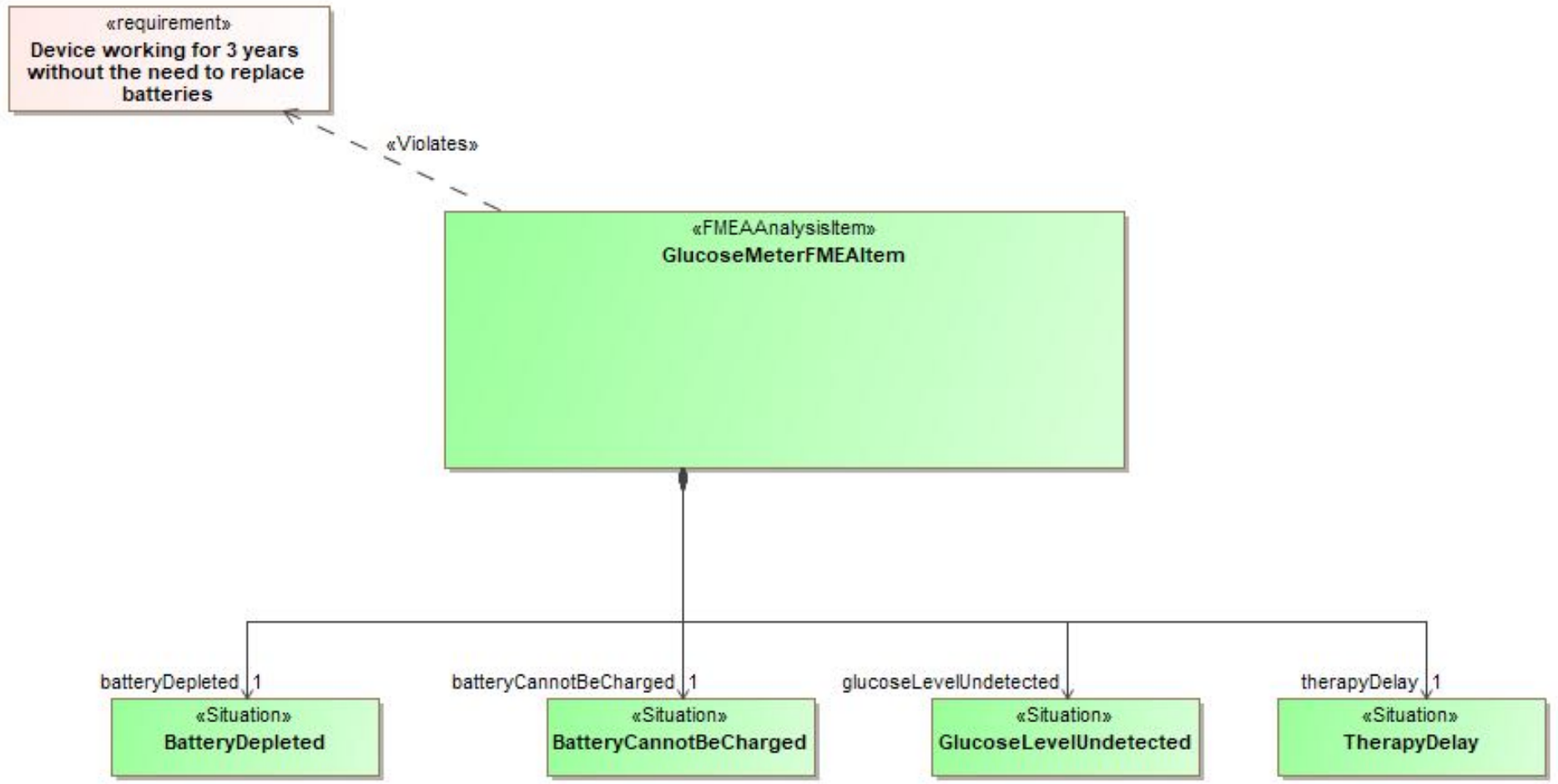
FMEA example: system model



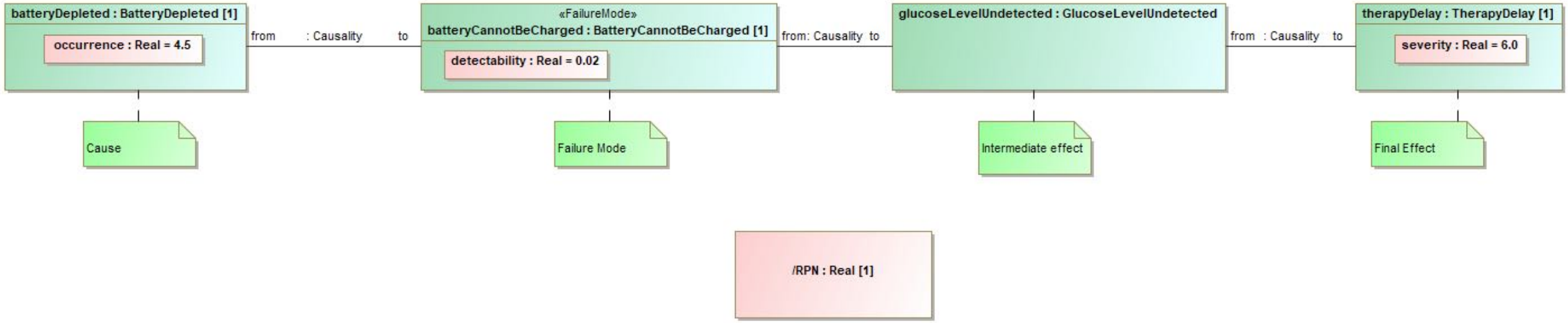
FMEA example: requirements violation



FMEA example: identification of situations



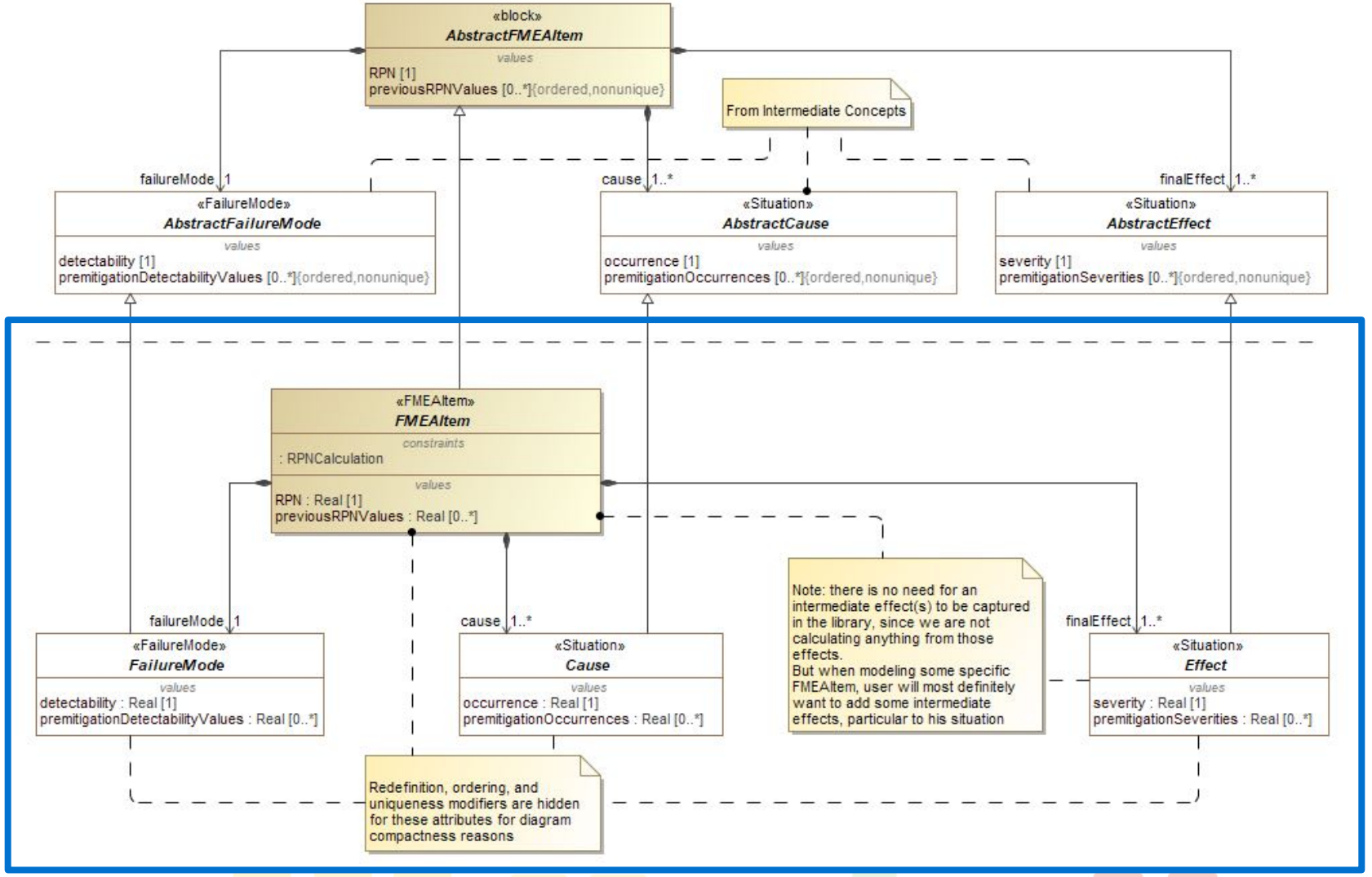
FMEA example: chaining and rating situations



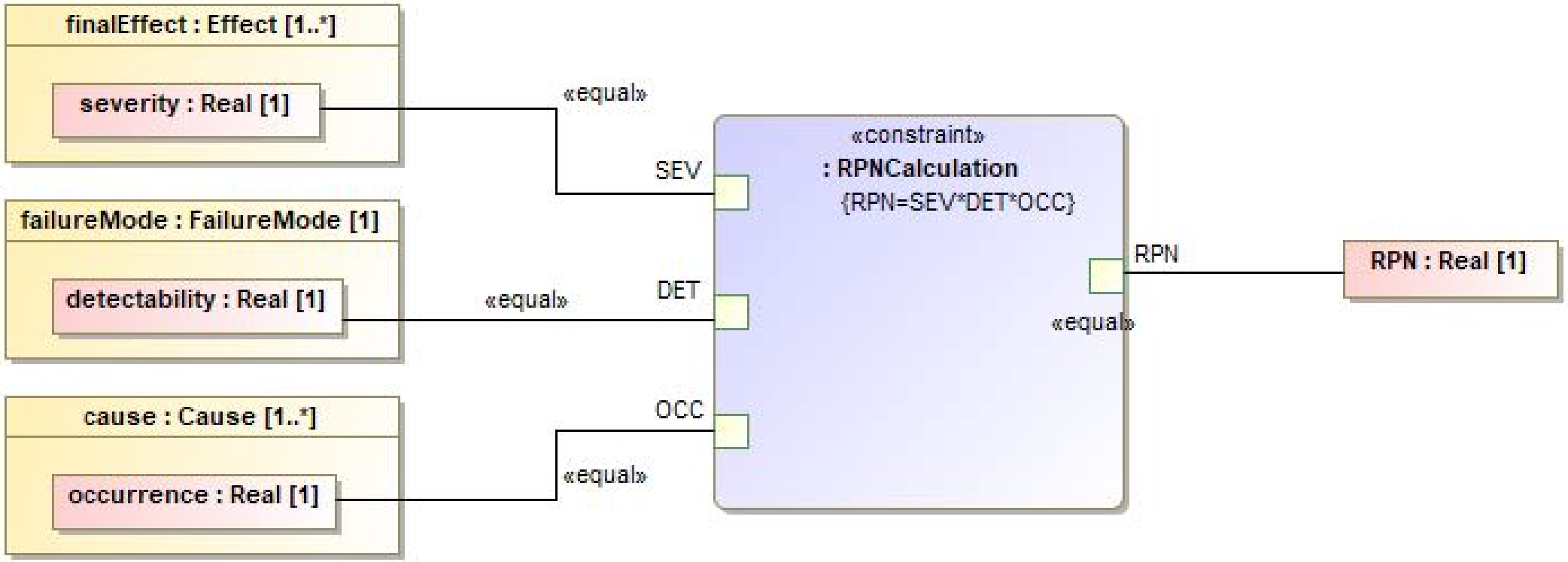
FMEA example: tabular view

#	Name	Item	Failure Mode	Local Effect Of Failure	Final Effect Of Failure	SEV	Cause Of Failure	OCC	Prevention Control	Detection Control	DET	OxD	RPN	Recomm
1	F1	airbag : Airbag	Bag does not open on impact		Injure Passenger	4.0	Sensor is not functioning properly Broken wire Controller is not functioning prope	4.0	Designed per material standard MS-XX123	Environmental stress test 03-000	4.0	16.0	64.0	Add reduno monitor imp Light to not
2	F2	light : Light	Light does not turn on	Car inoperable at night Car inoperable under ba		3.0	Battery dead	2.0			3.0	6.0	18.0	
3	F3	light : Light	Light does not turn on	Car inoperable at night Car inoperable under ba		3.0	Broken wire	2.0			3.0	6.0	18.0	
4	F4	light : Light	Light does not turn off	Car won't start		3.0	Short circuit in switch	2.0			3.0	6.0	18.0	Redesign: A indicator wl driver's doo while lights
5	F5	light : Light	Light does not turn on	Car inoperable at night Car inoperable under ba		3.0	Headlight out	2.0			1.0	2.0	6.0	Redesign: a lights-on di in console;
6	F6	light : Light	Light does not turn off	Car won't start		2.0	Operator error (left on)	2.0			2.0	4.0	8.0	Redesign: A indicator wl driver's doo while lights visual lights
7	F7	light : Light	Light does not turn on	Car inoperable at night Car inoperable under ba		2.0	Switch broken	2.0			1.0	2.0	4.0	
8	F8	light : Light	Light does not turn on	Car inoperable at night Car inoperable under ba		2.0	Switch corroded	2.0	Designed per material standard MS-XXX1		3.0	6.0	12.0	

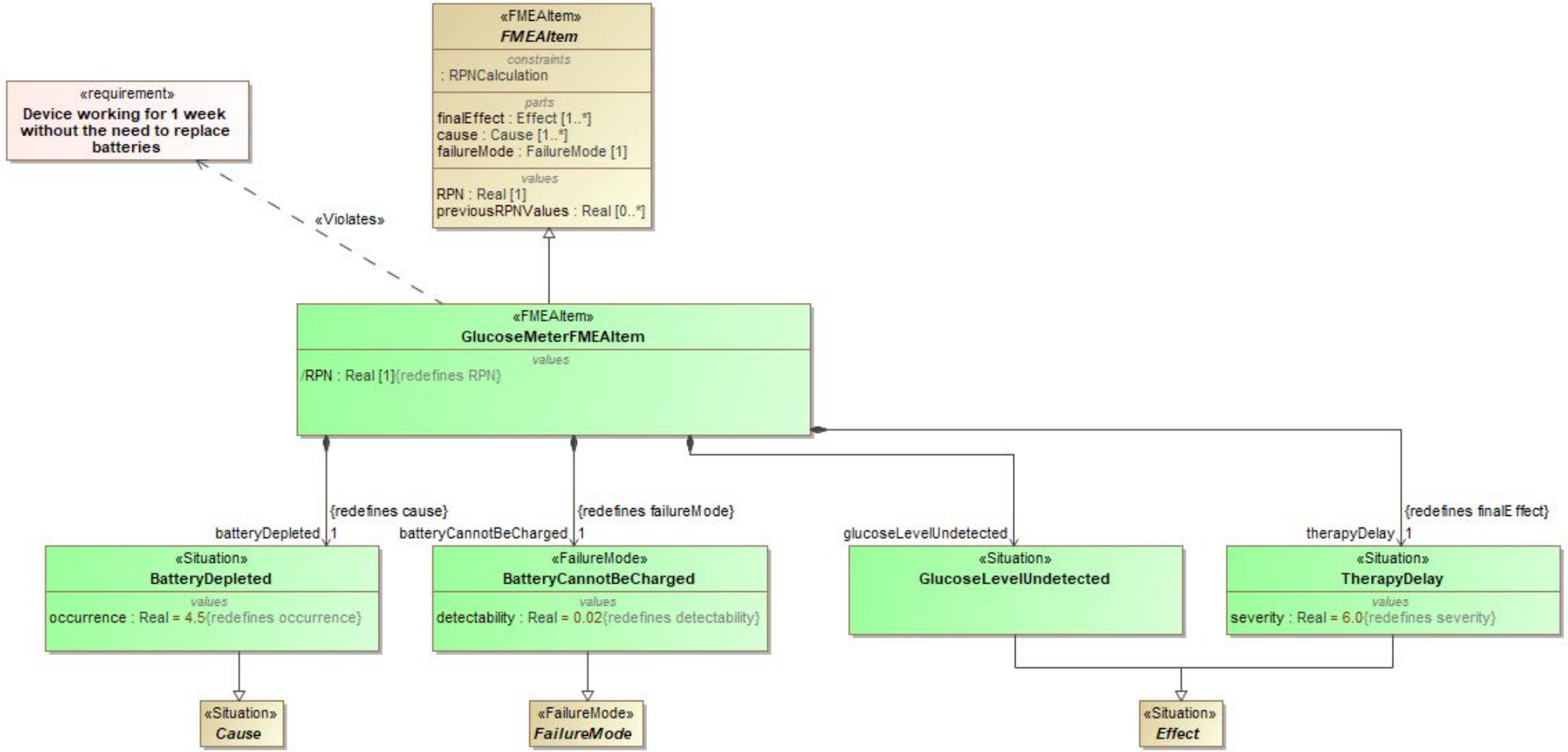
FMEA example: FMEA pattern



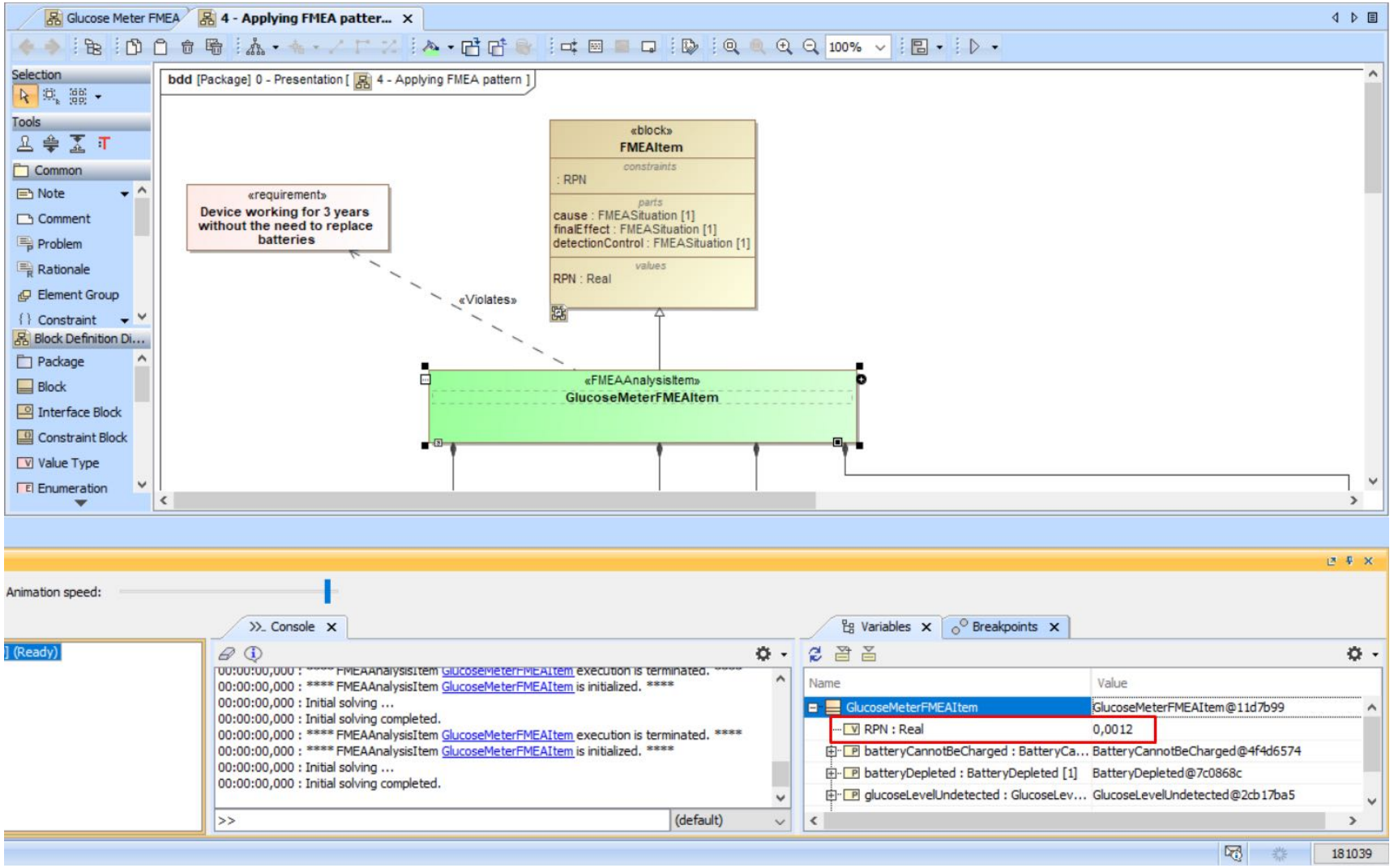
FMEA example: FMEA pattern parametrics



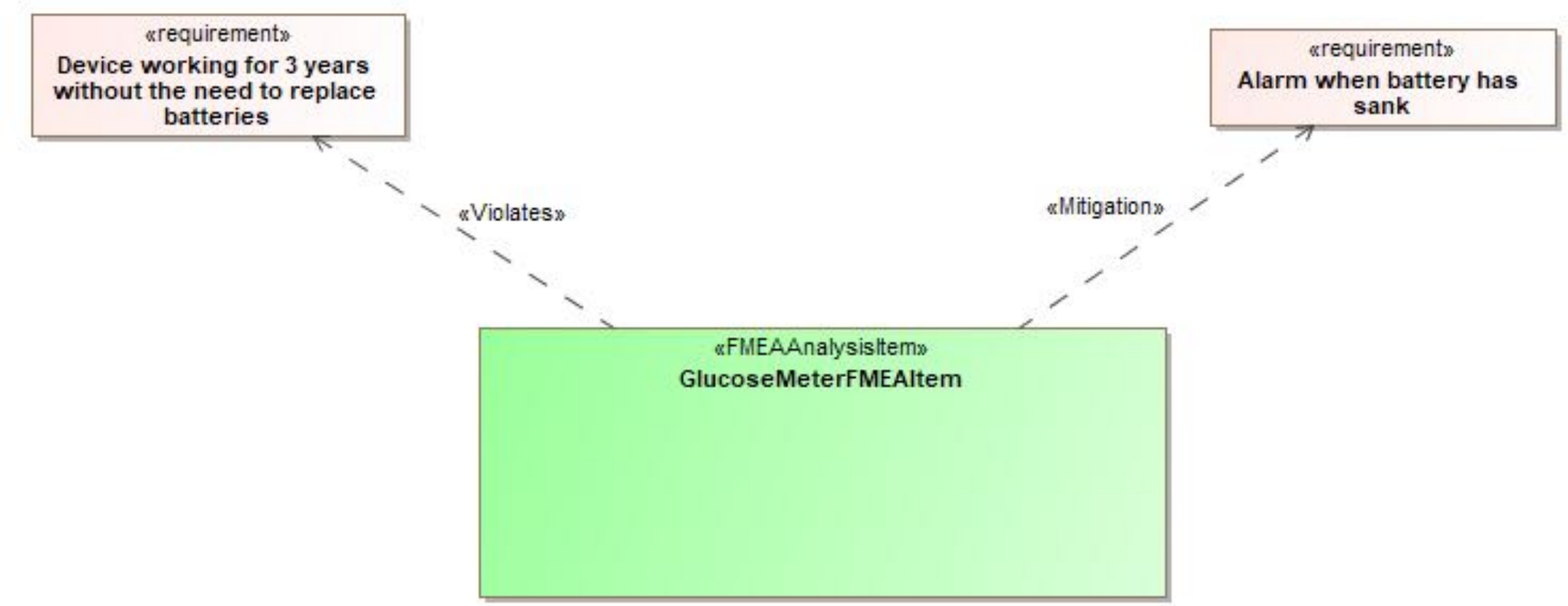
FMEA example: applying FMEA analysis pattern



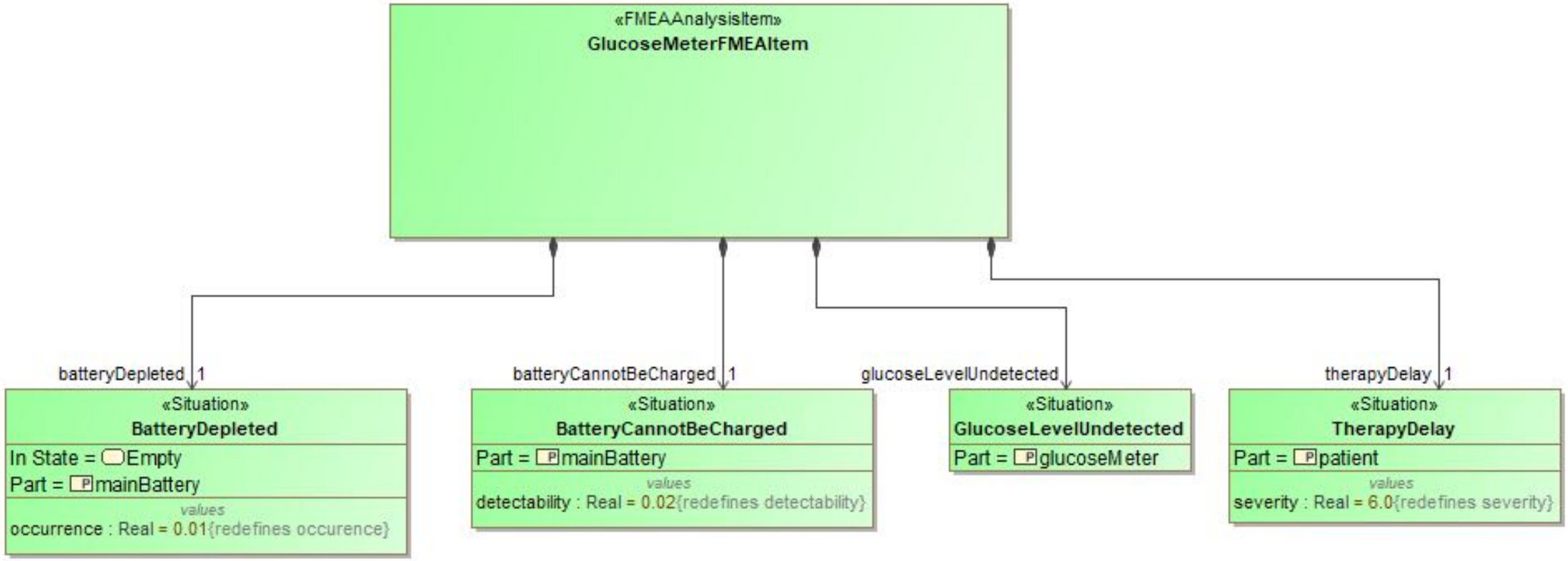
FMEA example: RPN calculation



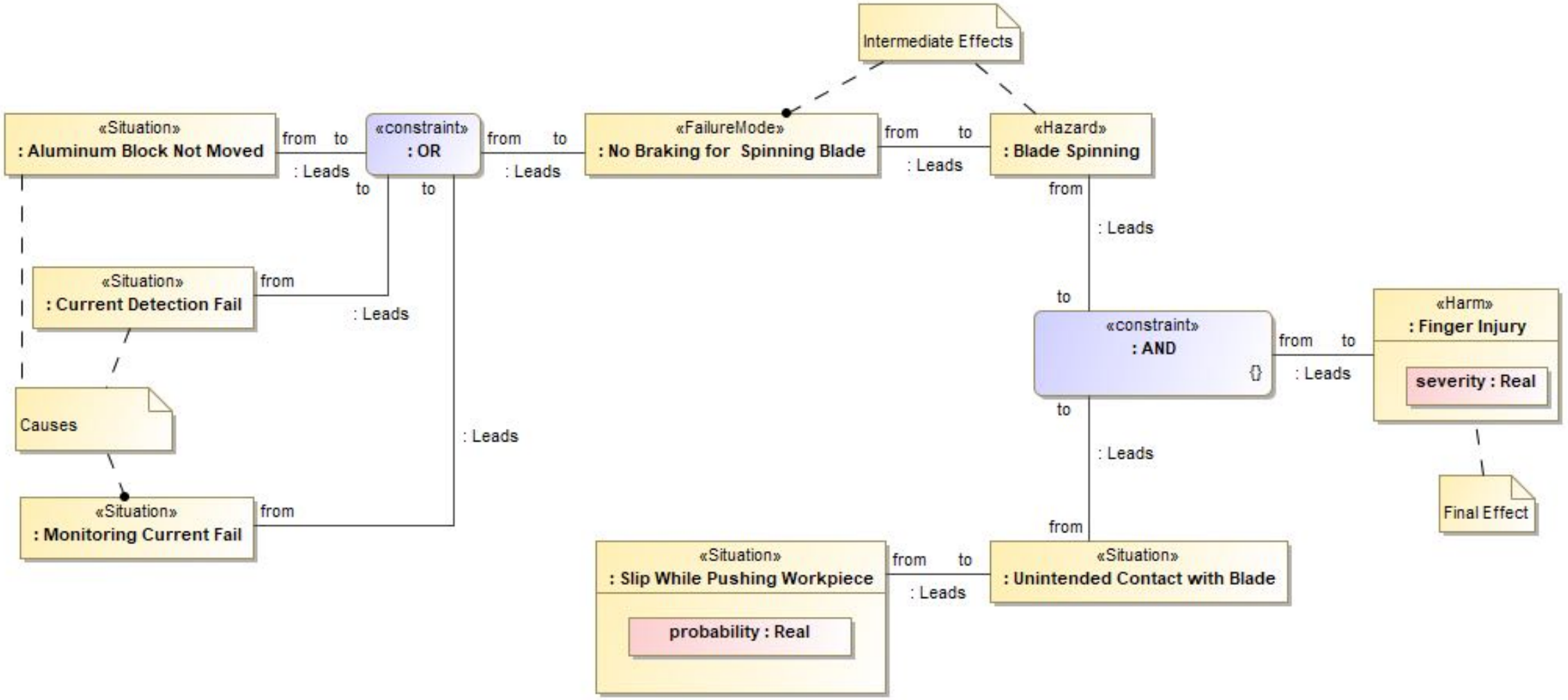
FMEA example: mitigation



FMEA example: tying situations to states and parts



FTA integrated with FMEA: example



Let’s keep in touch!

Geoffrey Biggs <gbiggs@ieee.org>

Andrius Armonas
<andrius.armonas@3ds.com>

29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

www.incose.org/symp2019