Challenges in Automotive Software Development ---

Running on Big Software

BSR 2016

Mark van den Brand
Software Engineering and Technology
Eindhoven University of Technology

TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Introduction

- **Joint work with:**
  - **Yanja Dajsuren**
  - **Arash Khabbaz Saberi**
  - **Yaping Luo**

Automotive Software Engineering

Paradigm shift in automotive industry
HW-centric to SW-centric

↓

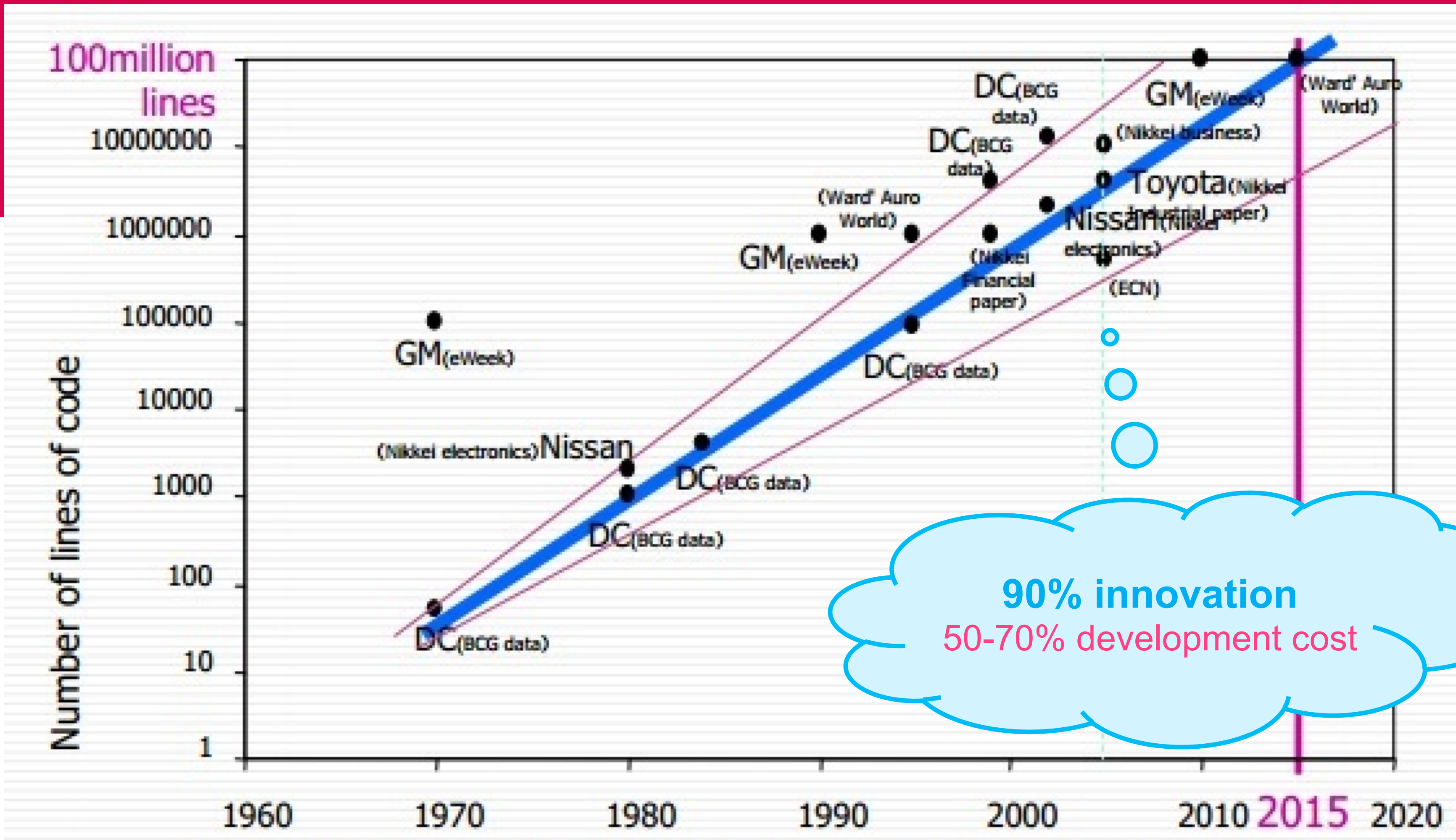
Rapid increase of SW causes challenges in all areas
Organization, key competencies, processes, models, methods, tools, maintenance, and strategies etc.

↓

Automotive SW engineering
Adopting SW engineering disciplines from other domains

Automotive Software Engineering

- 100 million lines of code in a vehicle is no exception!
- How many lines of code does the F-35 fighter jet (JSF) contain?
- Why does a vehicle contains such a huge amount of code?



Electronic Spark Timing (EST) System (1 ECU)

2000 functions enabled by software (70-100 ECUs)

Technische Universiteit
Eindhoven
University of Technology

Automotive Software Engineering

- Innovations lead to more software
  - Adaptive Cruise Control
  - Parking assistance
  - Lane detection
  - Connected cars
  - Eventually: autonomous driving

Automotive Software Engineering

- Automotive industry is changing wrt software:
  - Randy Mott, CIO GM: "You're not creative and fast enough when IT is outsourced."
  - General Motors has started the recruitment of 500 IT professionals for an innovation center in Austin. This is the first installment of the estimated 10,000 IT professionals GM will attract in the next three years

Automotive Software Engineering

Software problem that could cause

- the cars to <u>stop suddenly</u>
- accelerate <u>without warning</u>
- <u>overheats/damages</u> power electronics
- …

YEAR	TOTAL RECALLS ISSUED	TOTAL NO. OF VEHICLES AND EQUIPMENT RECALLED IN MILLIONS
1990	269	18.5
1991	282	14.4
1992	217	13.6
1993	264	11
1994	290	9.9
1995	348	19
1996	341	19.5
1997	312	16.7
1998	408	19.2
1999	440	55.6
2000	626	44.6
2001	527	22.4
2002	506	25.3
2003	600	22.9
2004	698	33
2005	645	20.4
2006	613	14.1
2007	713	20.6
2008	781	22.6
2009	571	18
2010	723	23
2011	657	17.5
2012	657	18.1
2013	714	27
2014 YTD	*500	**56

Source: National Highway Traffic Safety Administration

Automotive Software Engineering

- **Quality is essential:**
  - **Vehicle OEMs spend millions on warranty and recall costs each year, with over 50% of recalls attributed to software glitches and electronics defects** [http://www.arynga.com/]
  - **Software now to blame for 15% of car recalls**
  - **September 2016: GM recalled 4.3 million vehicles for software-related airbag defect**

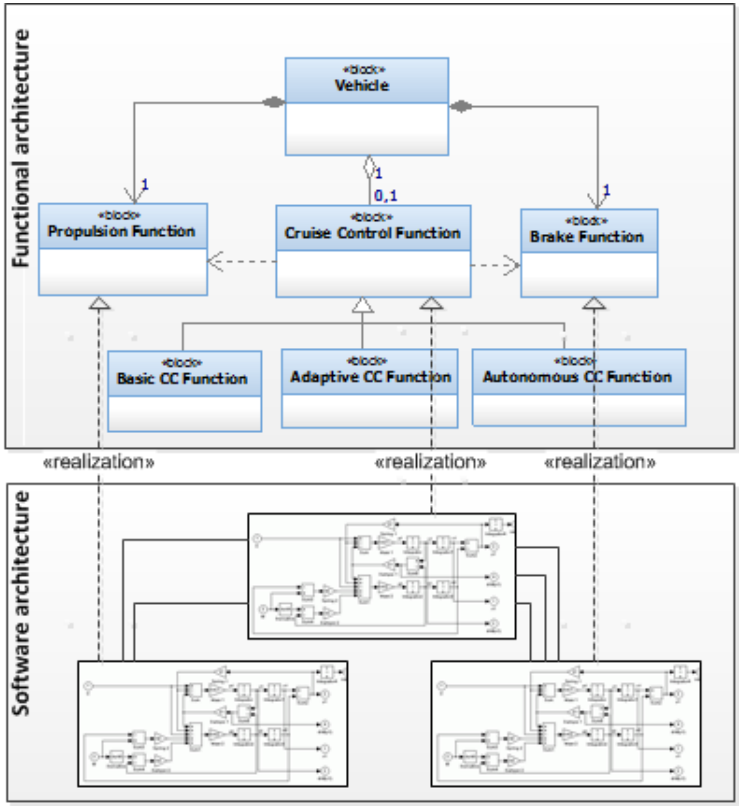
Car	Airbag spiral cable	Engine starter	Seat rails	Steering Bracket
Auris		X		
Belta			X	
Camry	X			
Corolla	X			
Corolla Axio		X		
Corolla Fielder		X		
Fortuner	X			
Highlander	X			
Hilux	X			
Innova	X			
Ist			X	X
Land Cruiser Prado	X			
Mark X	X			
Matrix	X			
Porte		X		
*Ractis		X	X	X
Rav 4	X			
Reiz	X			
Scion xD			X	
Spade		X		
Tacoma	X			
Urban Cruiser			X	
Vanguard	X			
Vitz			X	
Yaris and Yaris Sedan	X		X	X
GM Pontiac Vibe	X			
Subaru Trezia		X		

Source: Toyota

Quality of Simulink models

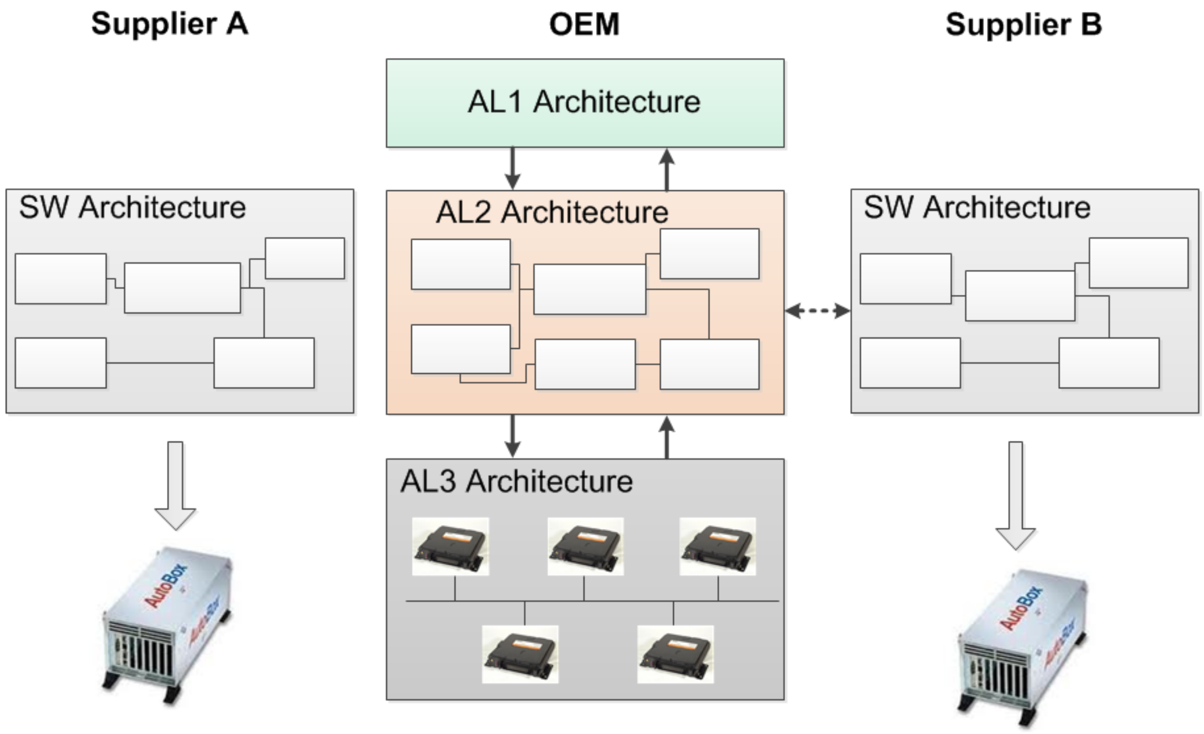
More electronics and software systems in vehicles:

- **to enable innovation**
- **to decrease costs**
- **to fulfill legal needs (e.g. CO2 emission) etc.**



More and more complex architectural and design models

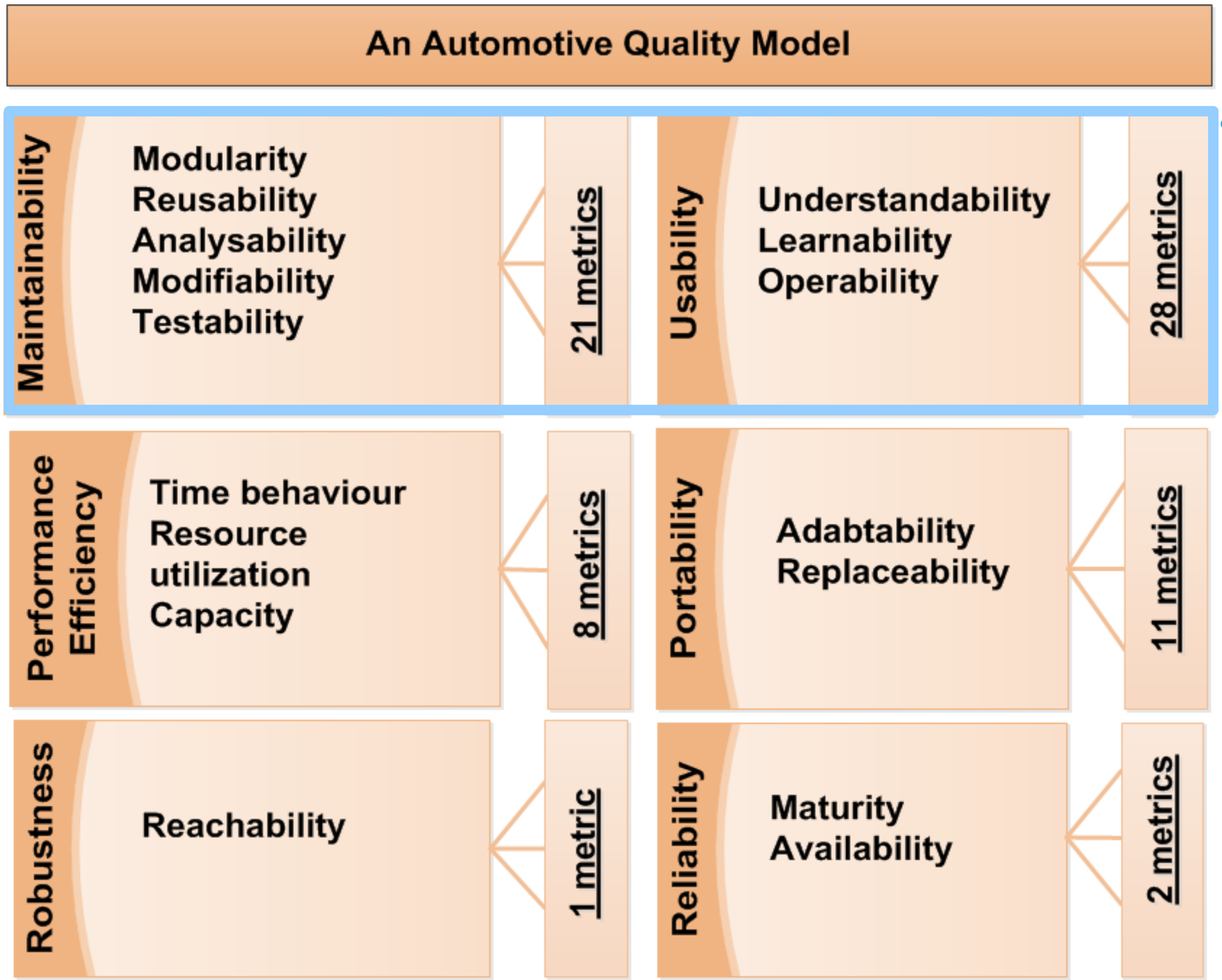
Quality of Simulink models



Large automotive MATLAB Simulink can consist of:
- ~15,000 building blocks
- 700 subsystems
- 16 hierarchical levels

How to ensure its quality?

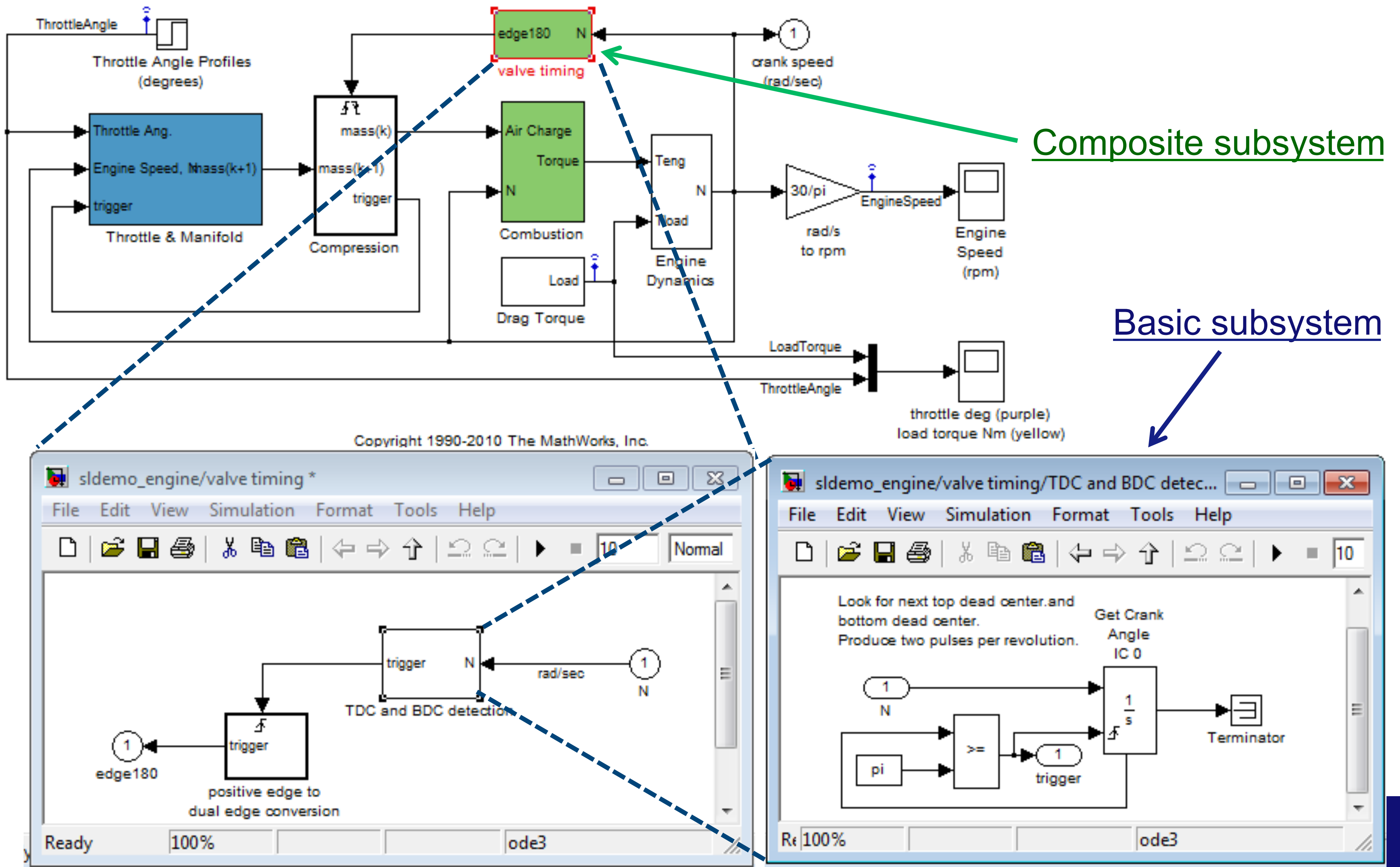
Quality of Simulink models



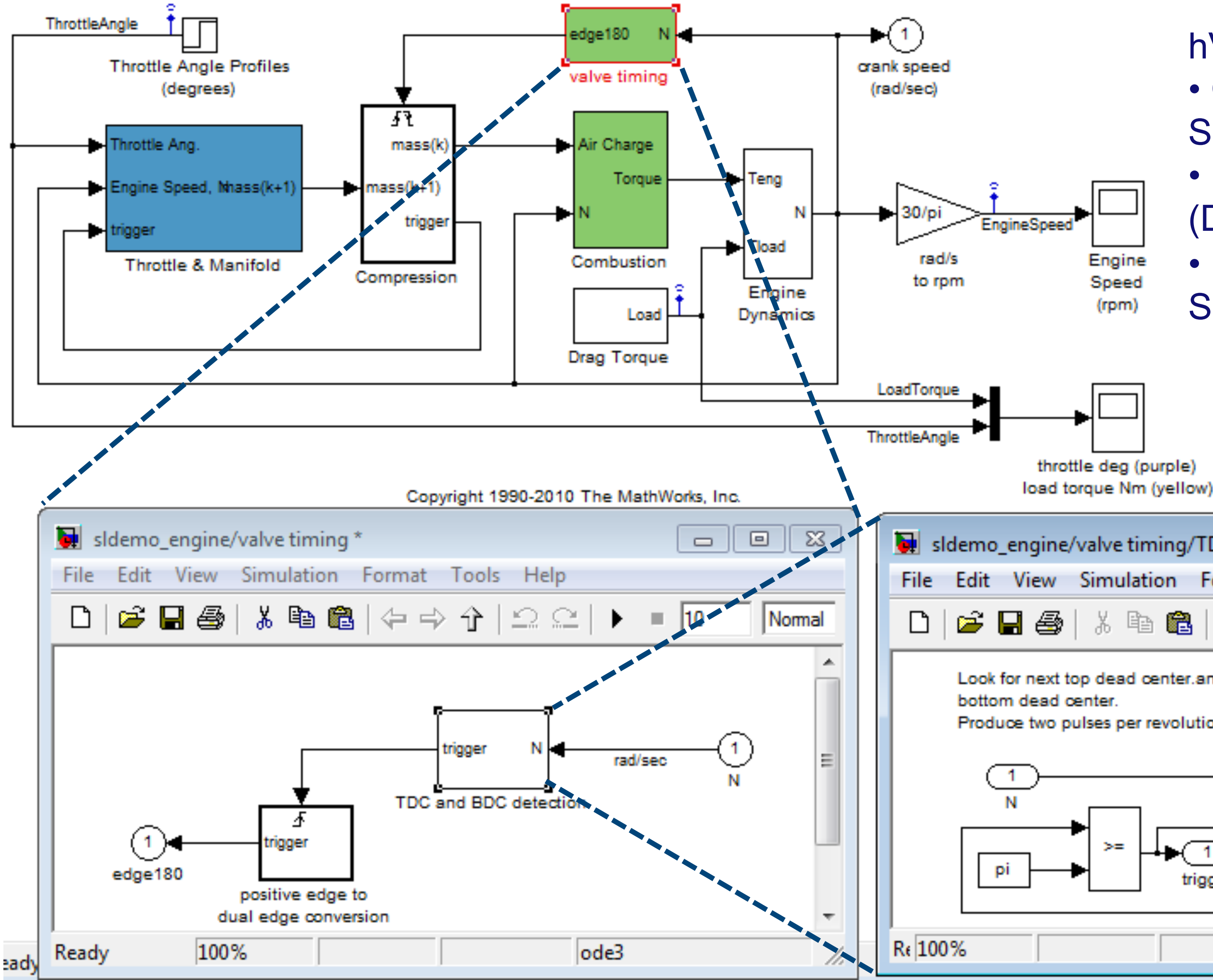
- **<u>Objective</u>: maintainable and usable software**

Are all these metrics useful?

Quality of Simulink models



Quality of Simulink models

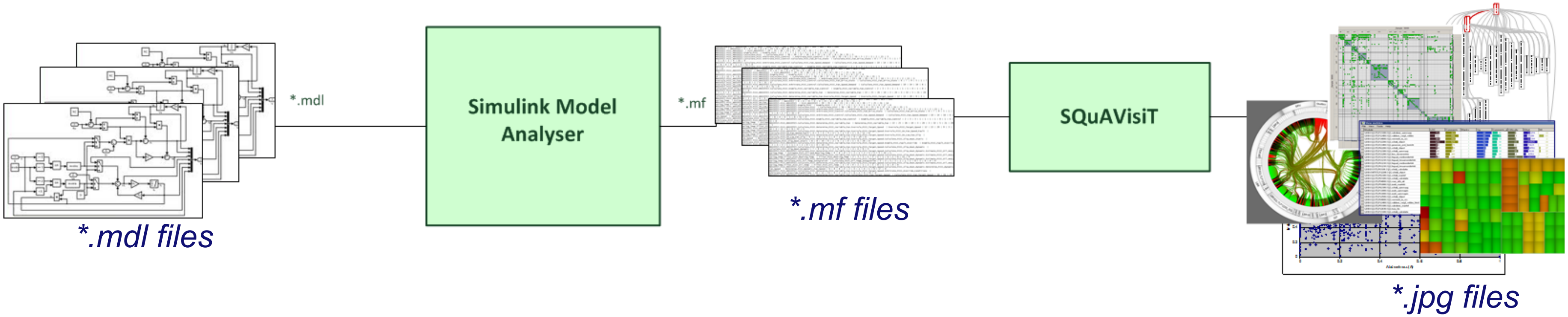


hValve timing:

- Coupling Between Subsystems (CBS) = 2;
- Depth of a Subsystem (DoS) = 2;
- Number Of Subsystems (NOS) = 2

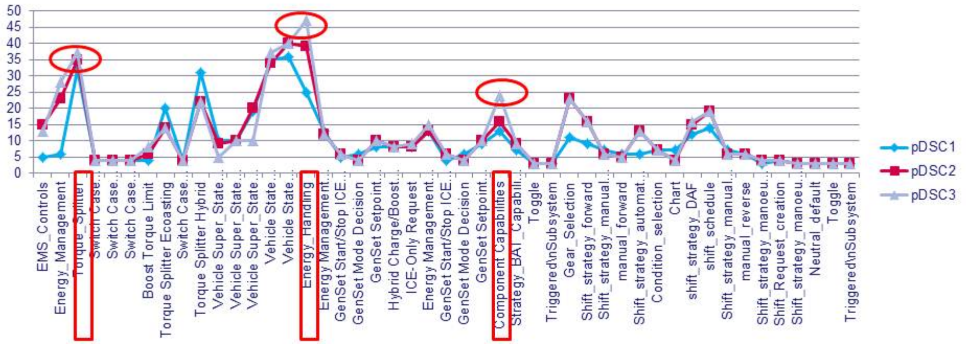
Quality of Simulink models

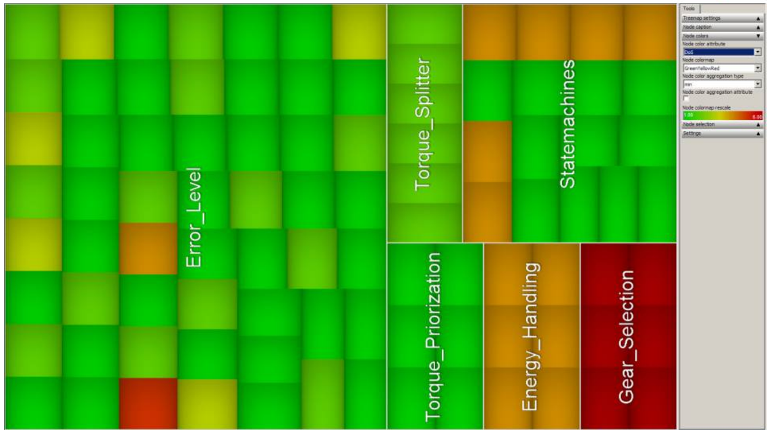
- **Measurement and visualization tool chain**

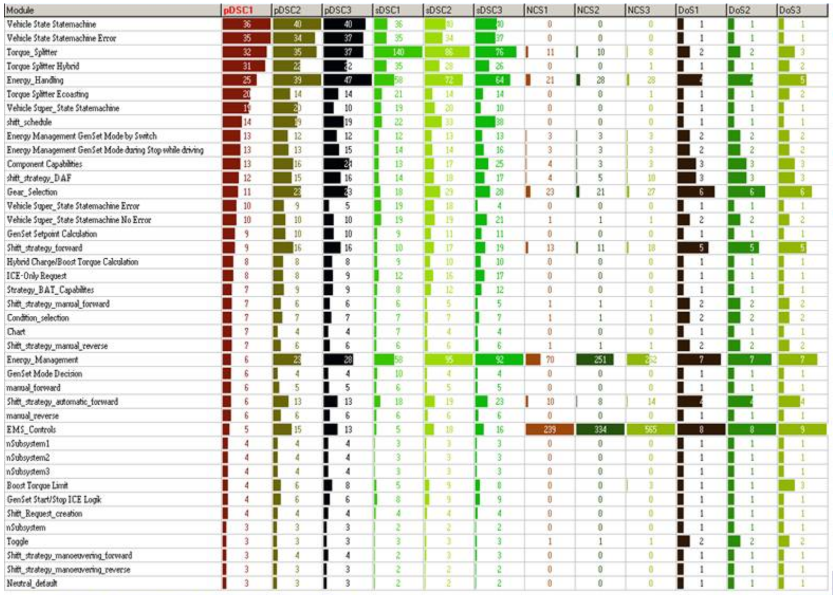


- **Measurement tool for Simulink model developed**
  - **Based on ConQAT Simulink Parser**
- **Interface with SQuAVisit Visualization tool**
  - **Extended with Simulink input**

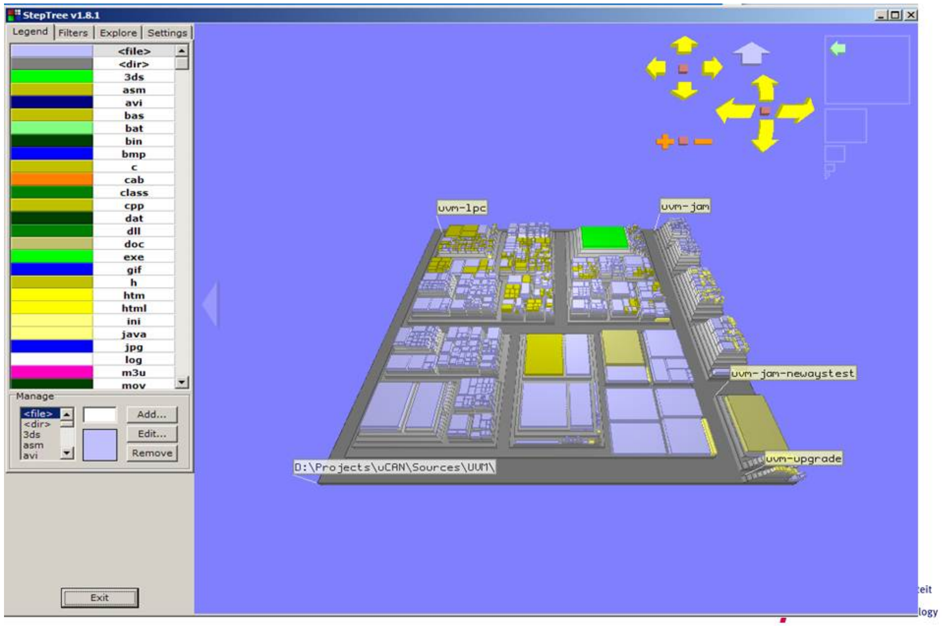
Quality of Simulink models







Module	pDSC1	pDSC2	pDSC3	sDSC1	sDSC2	sDSC3	NCS1	NCS2	NCS3	DoS1	DoS2	DoS3
Vehicle State Statemachine	36	40	40	36	30	30	0	0	0	1	1	1
Vehicle State Statemachine Error	35	34	37	35	34	37	0	0	0	1	1	1
Torque_Splitter	32	35	37	140	86	76	11	10	8	2	2	3
Torque Splitter Hybrid	31	22	22	35	28	26	0	0	1	1	1	2
Energy_Handling	25	39	47	58	72	64	21	28	28	4	4	5
Torque Splitter Ecoasting	20	14	14	21	14	14	0	0	1	1	1	2
Vehicle Super_State Statemachine	19	20	10	19	20	10	0	0	0	1	1	1
shift_schedule	14	19	19	22	33	38	0	0	0	1	1	1
Energy Management GenSet Mode by Switch	13	12	12	12	13	13	3	3	3	2	2	2
Energy Management GenSet Mode during Stop while driving	13	13	15	14	14	16	3	3	3	2	2	2
Component Capabilities	13	16	24	13	17	25	4	3	3	3	3	3
shift_strategy_DAF	12	15	16	14	18	17	4	5	10	3	3	3
Gear_Selection	11	23	23	18	29	28	23	21	27	6	6	6
Vehicle Super_State Statemachine Error	10	9	5	19	18	4	0	0	0	1	1	1
Vehicle Super_State Statemachine No Error	10	10	10	19	19	21	1	1	1	2	2	2
GenSet Setpoint Calculation	9	10	10	9	11	11	0	0	0	1	1	1
Shift_strategy_forward	9	16	16	10	17	19	13	11	18	5	5	5
Hybrid Charge/Boost Torque Calculation	8	8	8	9	10	10	0	0	0	1	1	1
ICE-Only Request	8	8	9	12	16	17	0	0	0	1	1	1
Strategy_BAT_Capabilites	7	9	9	8	12	12	0	0	0	1	1	1
Shift_strategy_manual_forward	7	6	6	6	5	5	1	1	1	2	2	2
Condition_selection	7	7	7	7	7	7	1	1	1	2	2	2
Chart	7	4	4	7	4	4	0	0	0	1	1	1
Shift_strategy_manual_reverse	7	6	6	6	6	6	1	1	1	2	2	2
Energy_Management	6	23	28	58	95	92	70	251	262	7	7	7
GenSet Mode Decision	6	4	4	10	4	4	0	0	0	1	1	1
manual_forward	6	5	5	6	5	5	0	0	0	1	1	1
Shift_strategy_automatic_forward	6	13	13	18	19	23	10	8	14	4	4	4
manual_reverse	6	6	6	6	6	6	0	0	0	1	1	1
EMS_Controls	5	15	13	5	18	16	239	334	565	8	8	9
nSubsystem1	4	4	4	3	3	3	0	0	0	1	1	1
nSubsystem2	4	4	4	3	3	3	0	0	0	1	1	1
nSubsystem3	4	4	4	3	3	3	0	0	0	1	1	1
Boost Torque Limit	4	6	8	5	9	8	0	0	3	1	1	3
GenSet Start/Stop ICE Logik	4	6	6	8	9	9	0	0	0	1	1	1
Shift_Request_creation	4	4	4	4	4	4	0	0	0	1	1	1
nSubsystem	3	3	3	2	2	2	0	0	0	1	1	1
Toggle	3	3	3	3	3	3	1	1	1	2	2	2
Shift_strategy_manoeuvering_forward	3	4	4	2	3	3	0	0	0	1	1	1
Shift_strategy_manoeuvering_reverse	3	3	3	2	2	2	0	0	0	1	1	1
Neutral_default	3	3	3	2	2	2	0	0	0	1	1	1



Model Driven Engineering

- Model Driven Engineering (MDE) is a (software) development methodology focusing on creating and using (domain) models

- Functional safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes

Modeling of functional safety

- **Standards and functional safety assurance**

- **Most important requirement in automotive:**
  - ***A vehicle should not harm its passengers or (people in) its environment when being used***

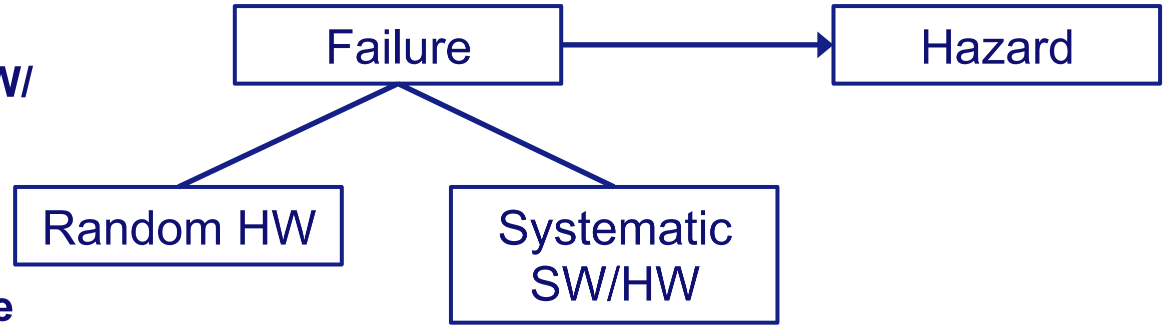
- **Safety related standards for automotive:**
  - **IEC 61508: the general functional safety standard**
  - **ISO 26262: the automotive specific functional safety standard**

Modeling of functional safety

- **Functional safety: operating correctly with fail-(safe/ operational) strategies**

Goals:

1) **Prevent systematic SW/ HW failures**
2) **Mitigate random HW failures**
3) **Show/assess how safe the designed product is**



Modeling of functional safety

- **People's lives**
  - **Toyota Camry case in 2010: Guilty by software defect! [1]**
- **Legislation**
  - **Most probably legislations for automated driving are based on ISO26262**
- **Cost**
  - **Toyota recalled 6M cars due to safety defect in 2014, estimated cost > $6B [2]**

[1] http://en.wikipedia.org/wiki/Michael_Barr_%28software_engineer%29

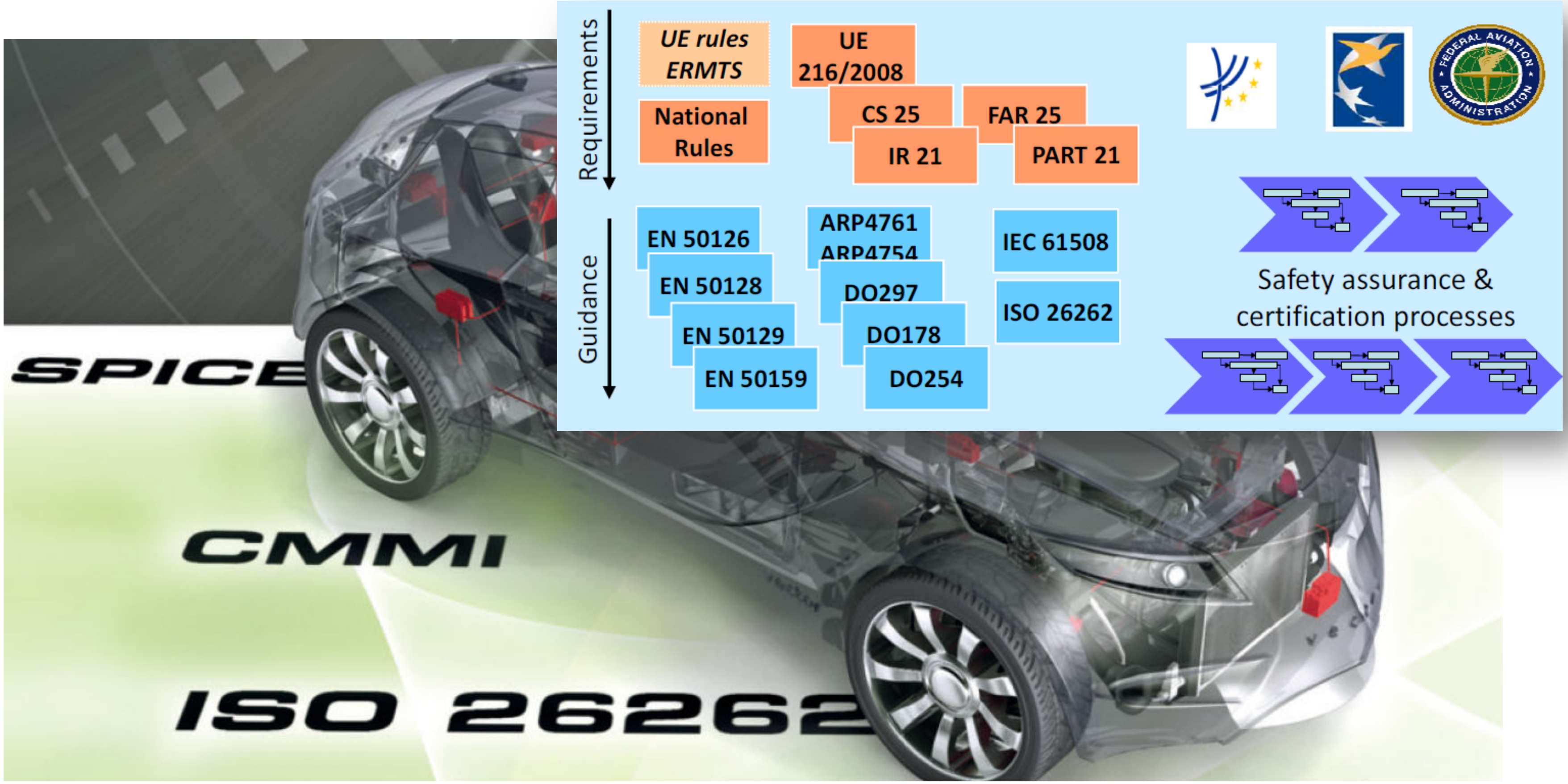
[2] http://www.bloomberg.com/news/articles/2014-04-09/toyota-recalls-6-76-million-vehicles-worldwide-including-rav4

Modeling of functional safety

- Testing a pedestrian detection system
- Failure happens
- Even when you are sure it will not!

Modeling of functional safety

- **Standards**



Modeling of functional safety

- **Certification**

Standards

Compliance argument

5 Item definition

5.1 Objectives

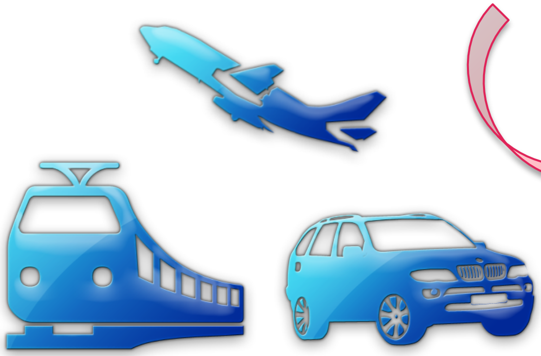
The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed.

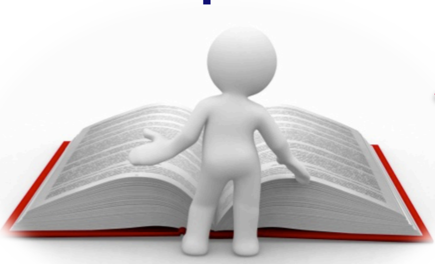
5.2 General

This clause lists the requirements and recommendations for establishing the definition of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, hazards, etc. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent subphases: “Initiation of safety lifecycle” (see Clause 6), “Hazard analysis and risk assessment” (see Clause 7) and “Functional safety concept” (see Clause 8).

NOTE Table A.1 provides an overview of objectives, prerequisites and work products of the concept phase.



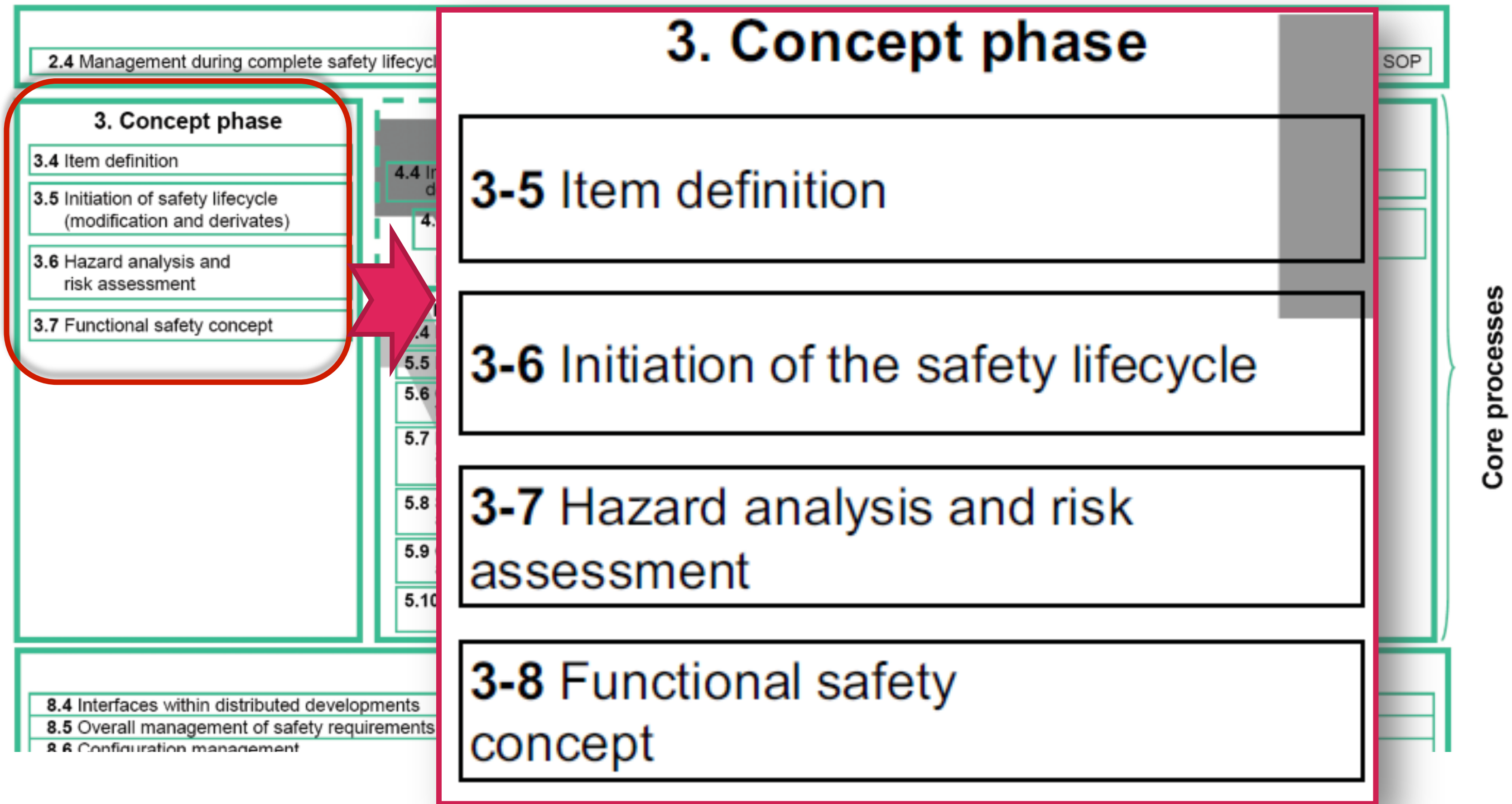
Experts



Modeling of functional safety

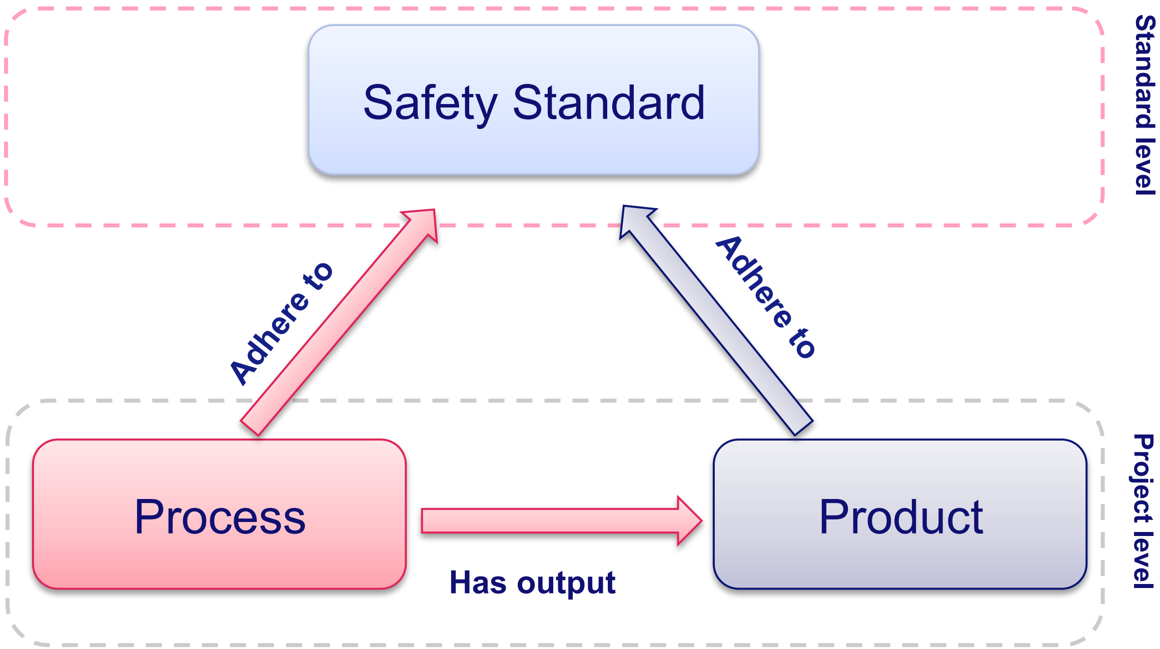
- ISO 26262 standard is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles:
  - Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
  - Provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).
  - V-model based.

Modeling of functional safety



Modeling of functional safety

- **Relationships between standard and project**
  - **From process to product**



Modeling of functional safety

Generic MetaModel

Domain Concepts from Standard (ISO 26262) or Project

Specific MM

SM Editor

Add domain concepts

Automatic generated

Technische Universiteit **Eindhoven** University of Technology

Modeling of functional safety

- Generic Meta Model (GMM) is
  - designed for multiple domains
  - suited for certification data re-use
- Why Specific Meta Models (SMM)?
  - Different ways of addressing safety:
    - per domain
    - per company
    - per project
  - For each domain, the safety engineer needs to adapt the current way of working to conform to the GMM

Modeling of functional safety

Generic MM

Meta Model Transformation

Specific MM

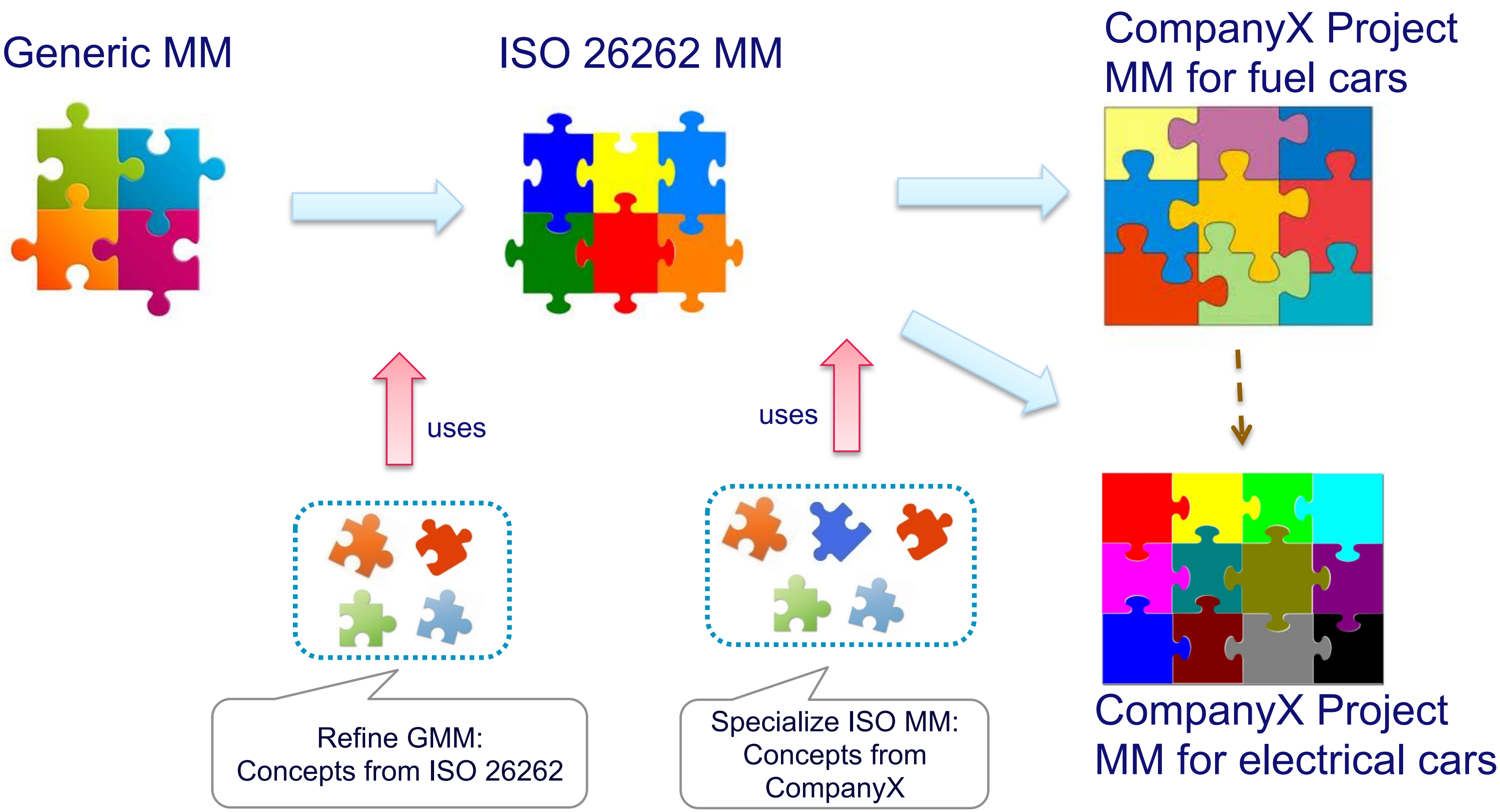
uses

Operators
----MM Refine Language

DSL containing Domain Concepts
(External Element etc.)
expressed in MMRL

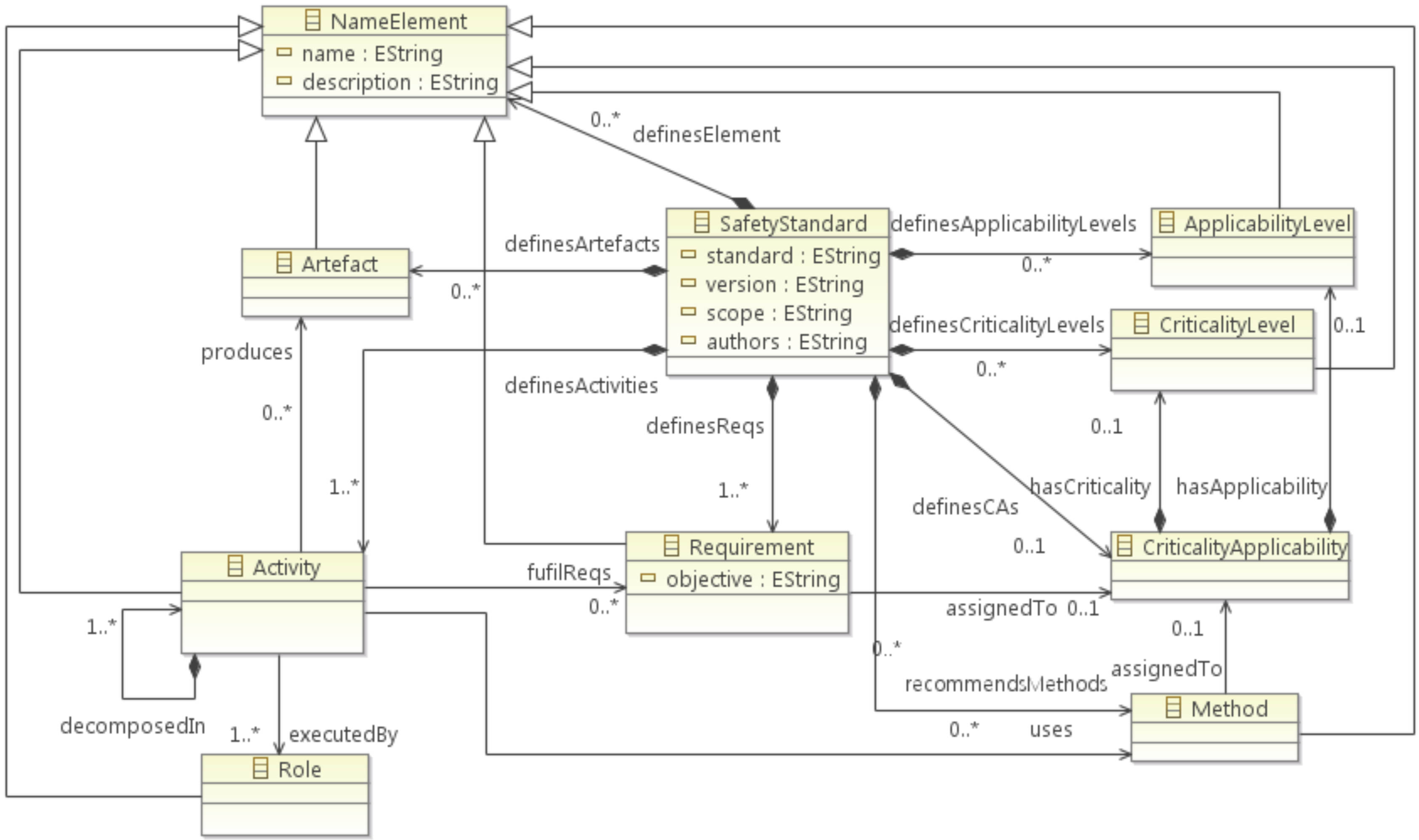
Specific Model Editor

Modeling of functional safety

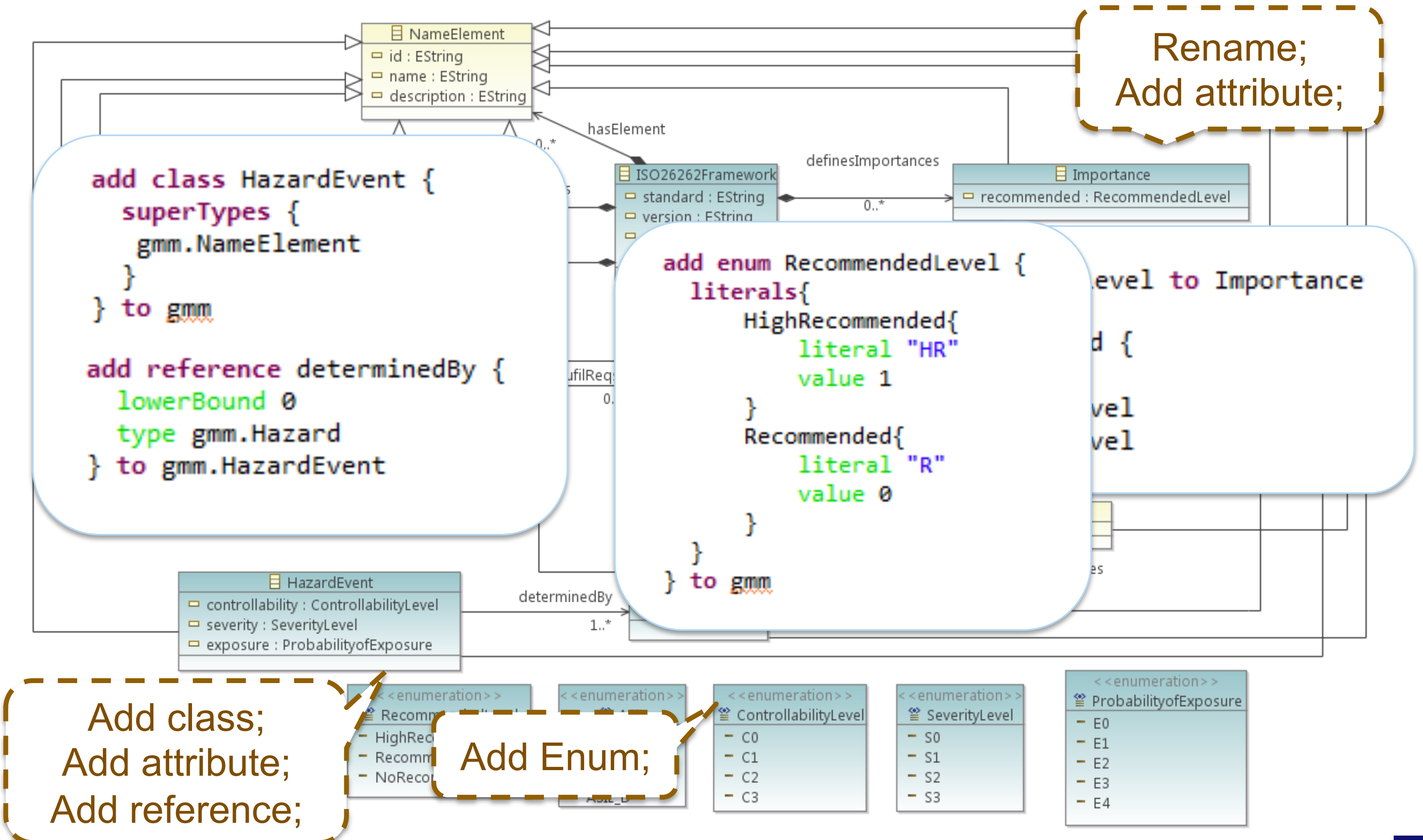


Modeling of functional safety

- **Case study: refining the Generic MM**

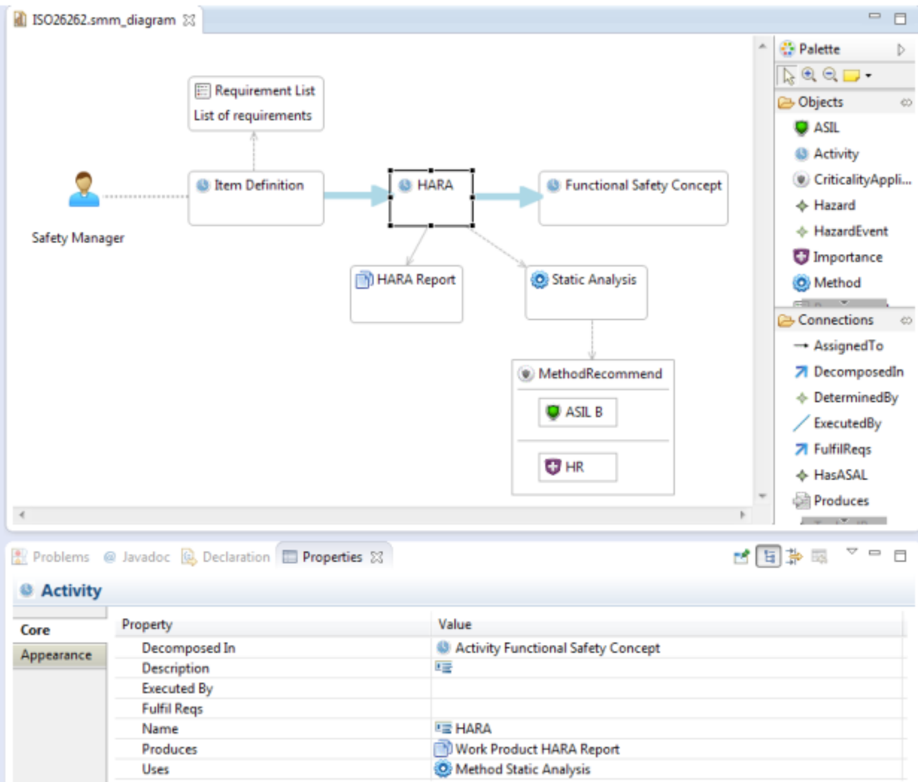


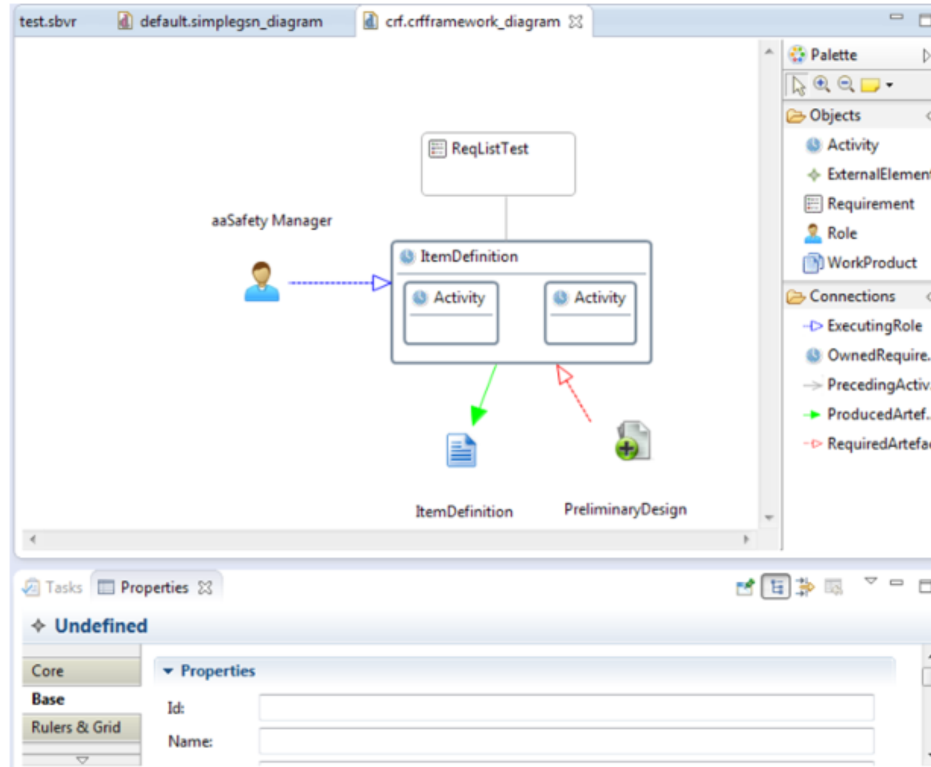
Modeling of functional safety



Modeling of functional safety

- **Editor for ISO 26262 models**





- **Editor for company specific models**

TU/e Technische Universiteit Eindhoven University of Technology

Modeling of functional safety

Generic MetaModel

Specific MM

SM Editor

Safety Case

Domain Concepts from Standard (ISO 26262) or Project

Add domain concepts

Automatic generated

Link to

Technische Universiteit **Eindhoven** University of Technology

Modeling of functional safety

- **Safety cases**
  - **ISO 26262, Safety case: "argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development."**
  - **The guidelines in Part10 provides some ideas about formal approaches to arguing safety from the evidence compiled in the safety case.**

Modeling of functional safety

- **Story of a safety case**

Claim 1: Dependable System
System X meets its

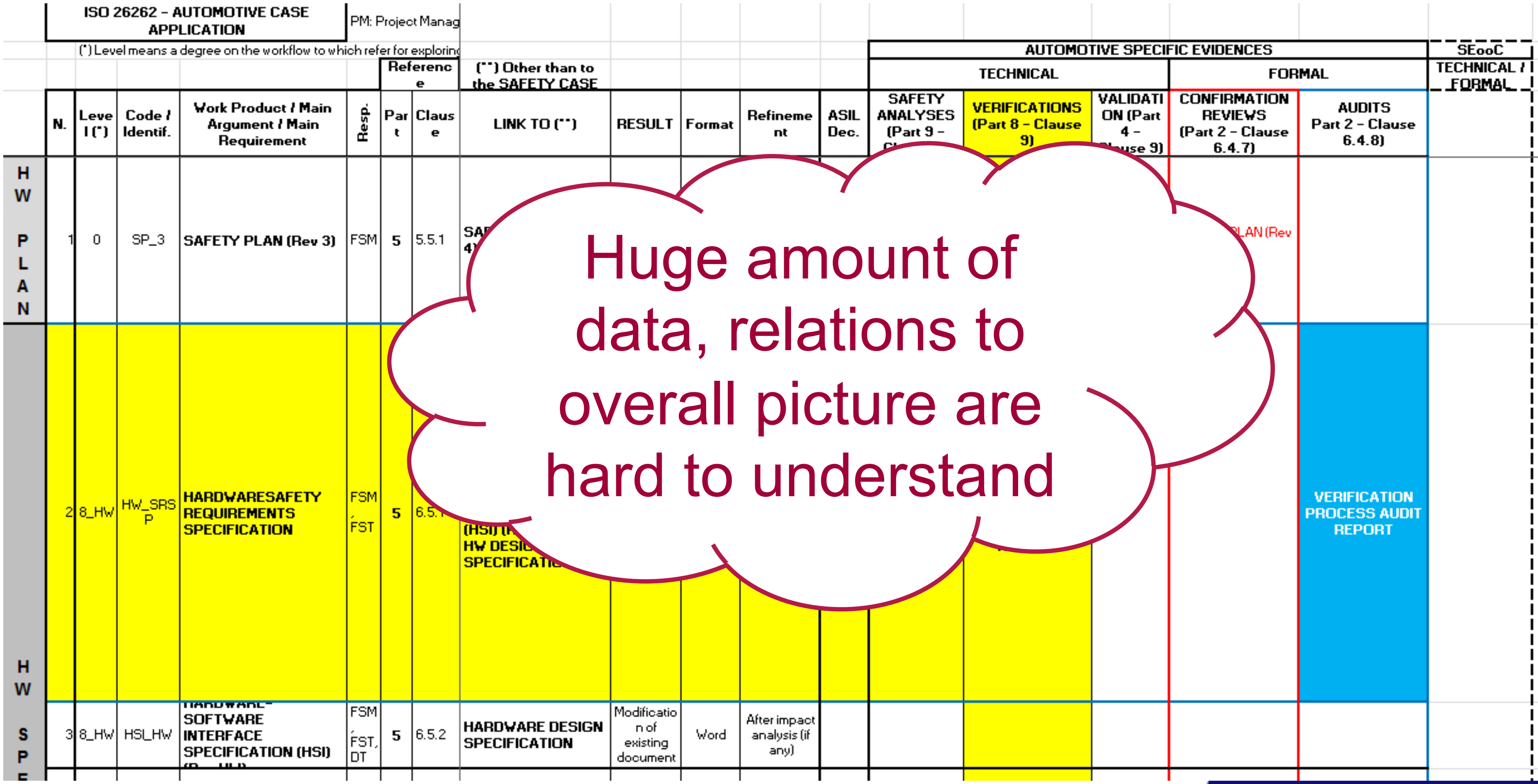
Context 1: Depend
Top level assuran
Derived requiremen

Strategy 1.1: argue over ... s.
Claim 1.1: Reliability: the releva... ity requirements are satisfied.
Claim 1.2: Availability: the relevant availability requirements are satisfied.
Claim 1.3: Security: the relevant security requirements are satisfied.

Clearness is a problem!

Modeling of functional safety

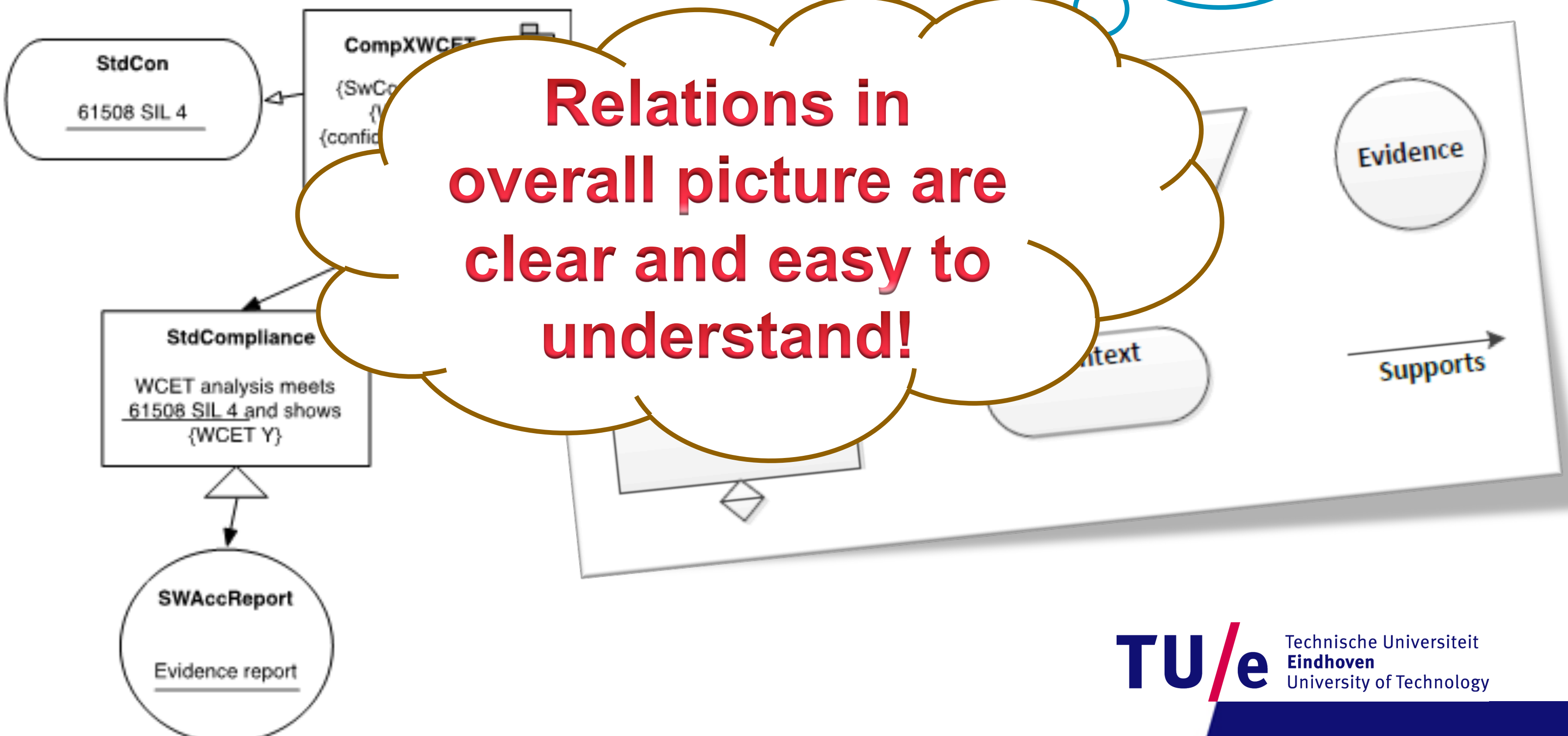
- **Story of a safety case**



Modeling of functional safety

- **Story of a safety case**

Goal Structuring Notation (GSN): mentioned explicitly in ISO 26262



Relations in overall picture are clear and easy to understand!

Modeling of functional safety

Any definition?

Link safety cases to conceptual models; use structured language

!?

Any relation?

Modeling of functional safety

- **Semantics of Business Vocabulary and Business Rules (SBVR) in GSN**

Base Business Definitions & Rules on Verb Concepts

↑

Associate Concepts to define Verb Concepts

↑

Define Noun Concepts

Definitions & Rules
Verb Concepts (Fact Types)
Noun Concepts

→ **Vocabulary**

Develop Vocabularies and Rules Sets to represent them (starting with terms for the concepts)

It is obligatory that each driver *of* a rental *is qualified*.

rental *has* driver

driver *is qualified*

The noun concept ‘driver’ *is* a facet *of* the noun concept ‘person.’

Structured English

Modeling of functional safety

Extraction (Model Transformation)

Existing Conceptual Model

SBVR Model (vocabulary)

Safety Case

Domain Concepts from Standard (ISO 26262) or Project

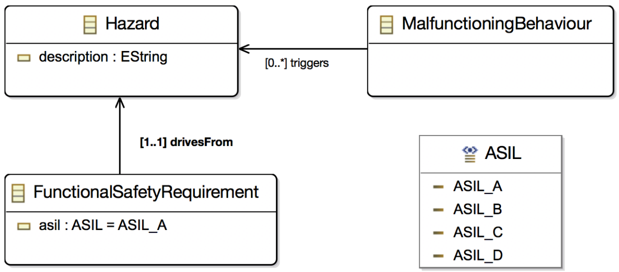
SBVR editor integrated in argument editor

TU/e Technische Universiteit Eindhoven University of Technology

Modeling of functional safety

```
Noun Concepts  :
⊖ MalfunctioningBehaviour
      Source : "From Eclass MalfunctioningBehaviour"
      Concept Type : general concept
⊖ Hazard
      Source : "From Eclass Hazard"
      Concept Type : general concept
      Necessity : Each Hazard has exactly one description .
⊖ FunctionalSafetyRequirement
      Source : "From Eclass FunctionalSafetyRequirement"
      Concept Type : general concept
      Necessity : Each FunctionalSafetyRequirement has exactly one ASIL .
⊖ ASIL
      Concept Type : categorization
⊖ description
      Source : "From Attribute : description in Eclass Hazard"
      Concept Type : role
⊖ ASIL_A
      General Concept : ASIL
      Concept Type : individual concept
```

Noun Concepts



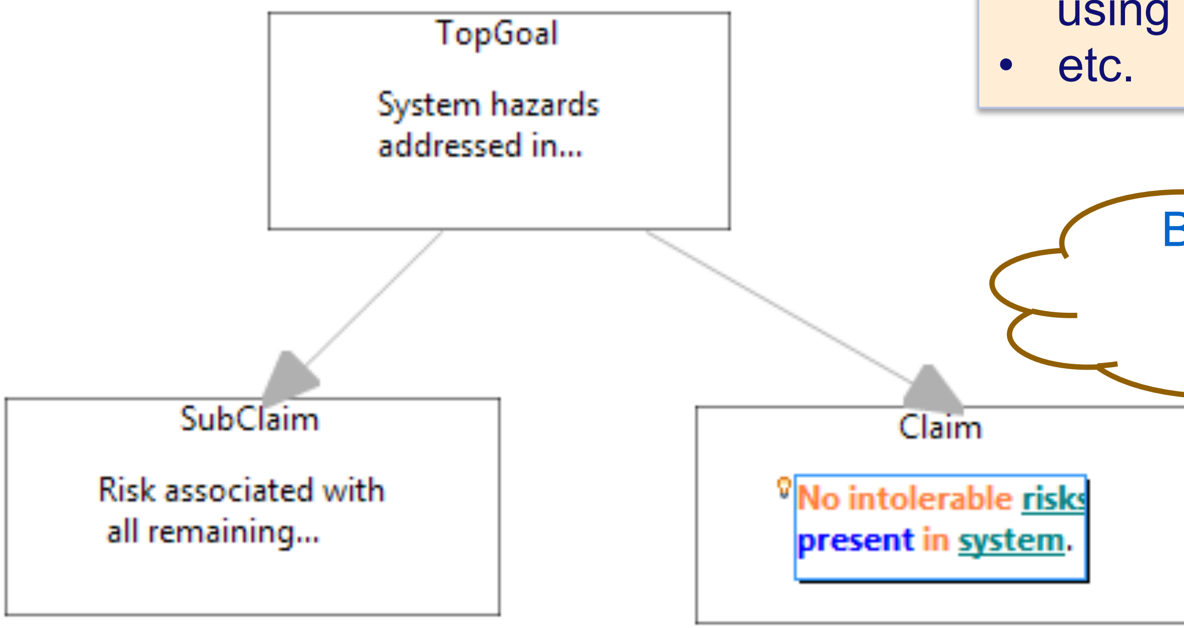

```
Verb Concepts :
⊖ MalfunctioningBehaviour triggers Hazard
      Concept Type : association
⊖ FunctionalSafetyRequirement is_derived_from Hazard
      Concept Type : association
⊖     Necessity : Each FunctionalSafetyRequirement is_derived_from at least one
      Hazard .
;
```

Verb Concepts

Modeling of functional safety

- **Safety claims and goals can now be parsed**

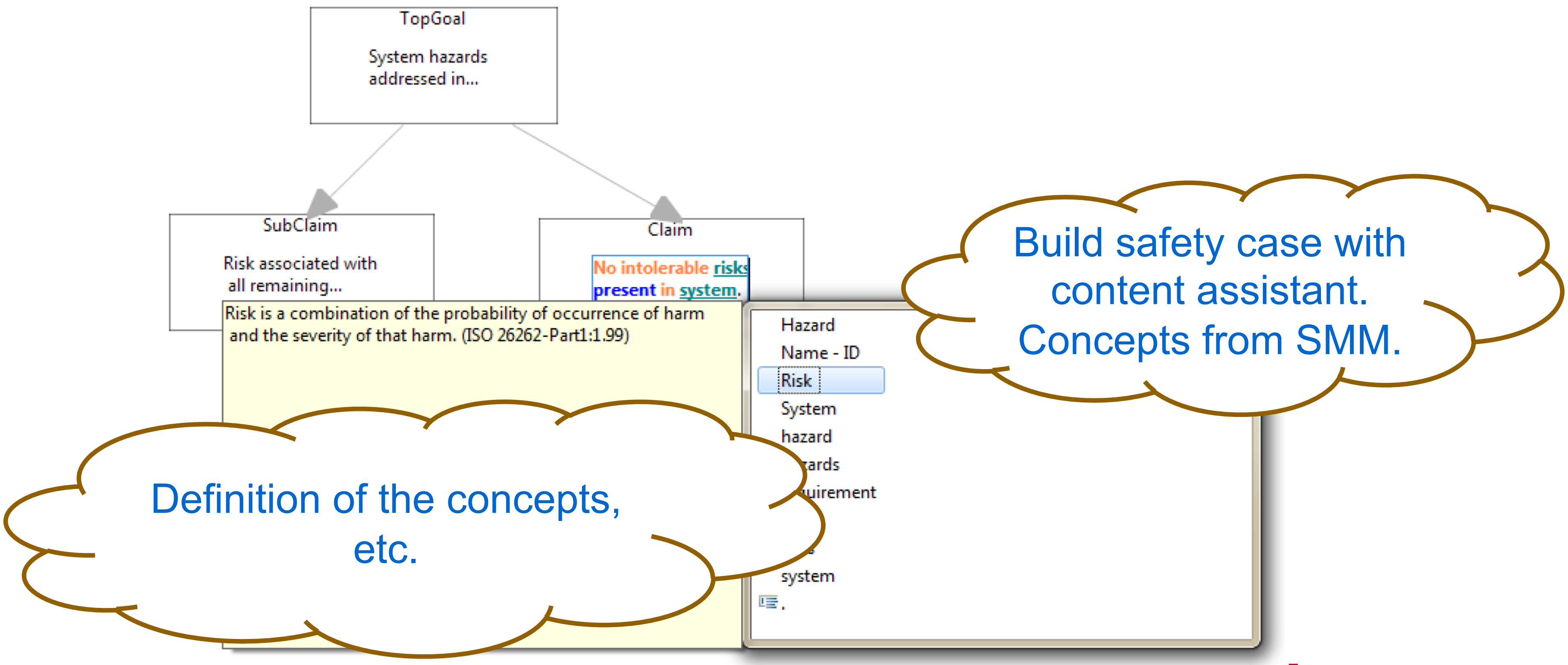
Language can be controlled:
- By restricting to a concise vocabulary;
- Limiting the size of sentences;
- Reducing the complexity of sentences;
- By restricting the verbal syntax; using of smaller set of tenses;
- etc.



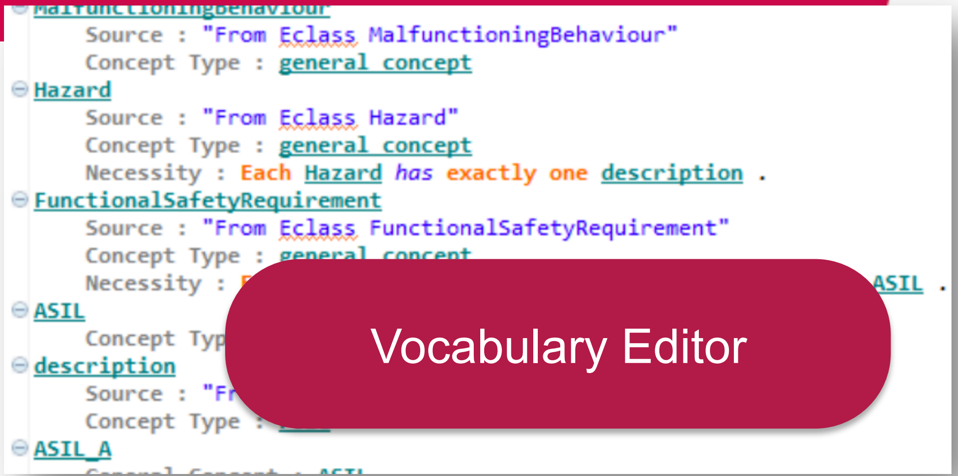
Build safety cases with structured language

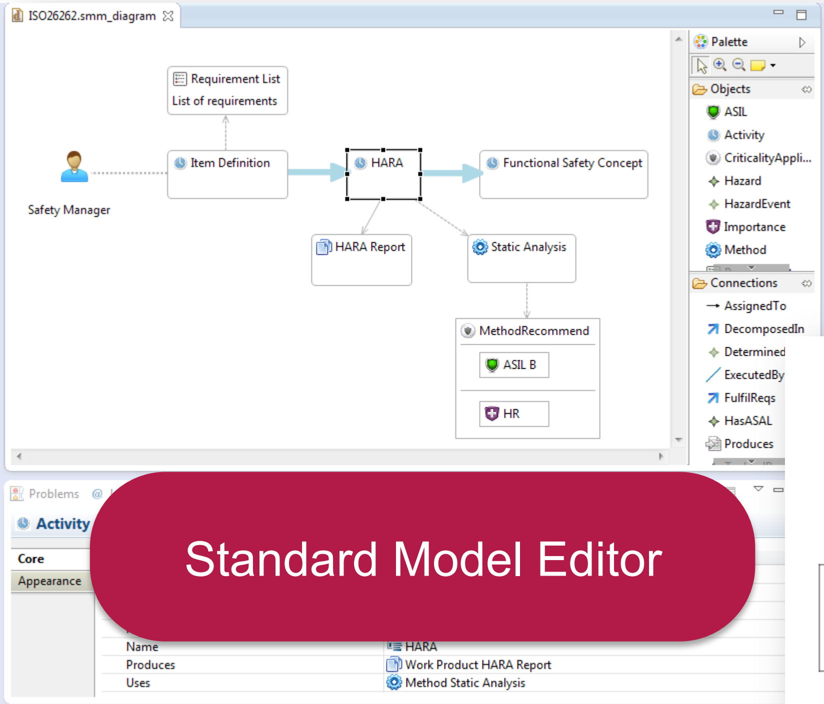
Modeling of functional safety

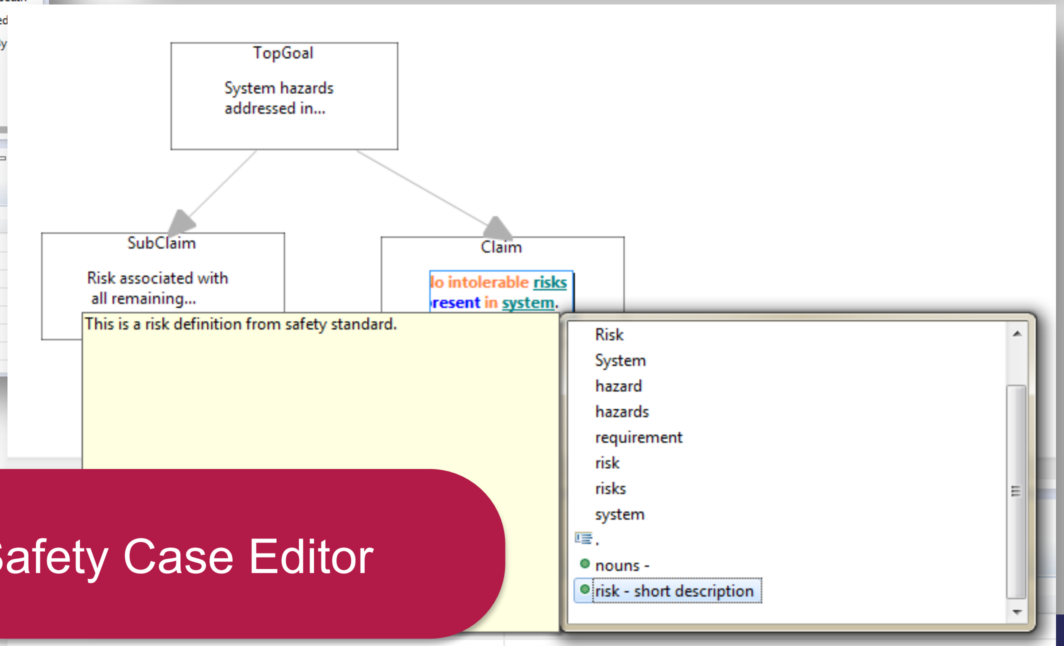
- **SBVR in action**



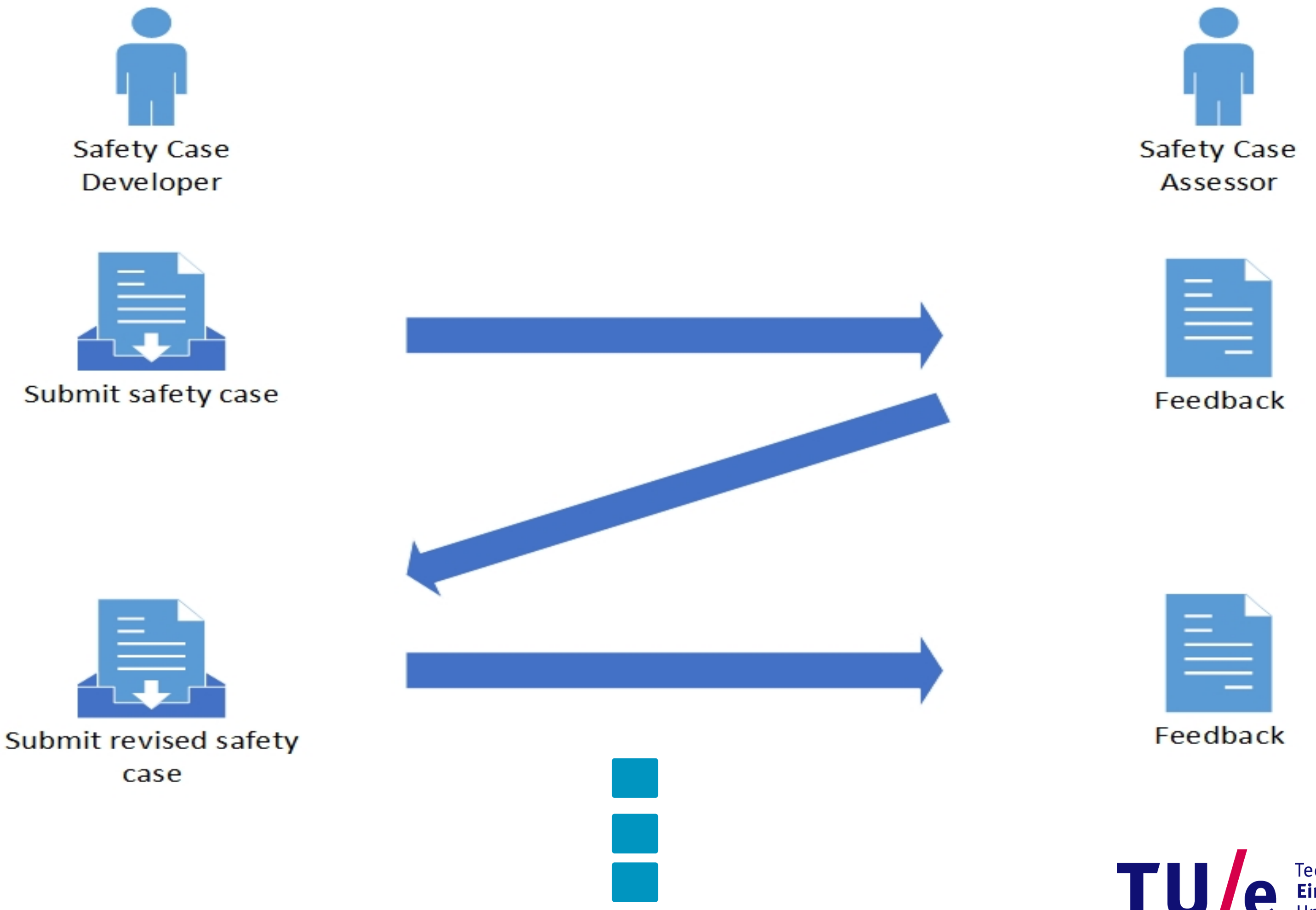
Modeling of functional safety







Safety Case Assessment



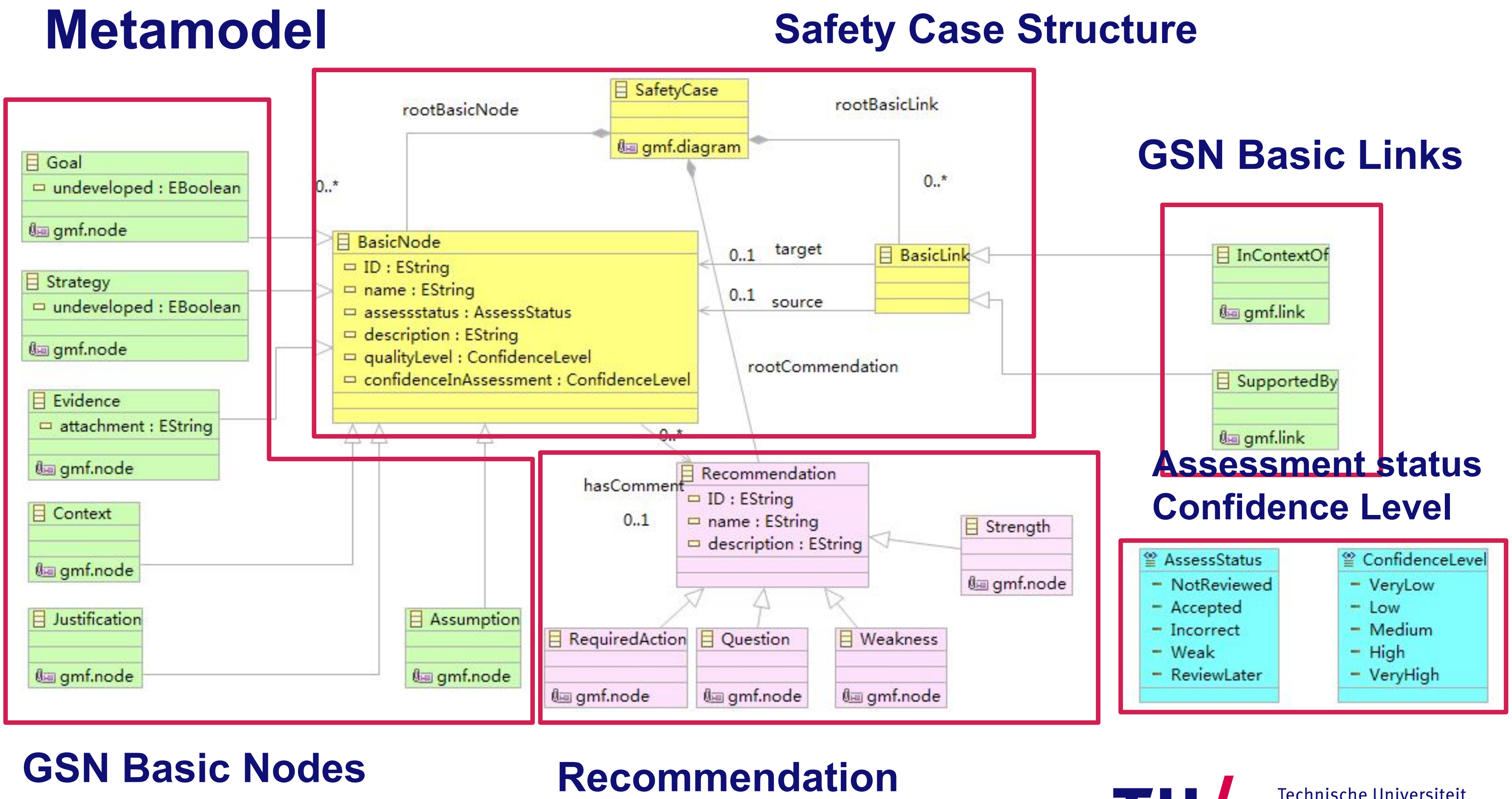
Safety Case Assessment

- Objectives
  - To evaluate whether the reasoning about the (functional) safety of the product is valid
  - To get an independent statement that the claim about the (functional) safety of the product is reasonable
- Outcome
  - Strengths and weaknesses are identified
  - Recommendation (for acceptance or rejection) based on judgment of the provided claims and evidence
  - Required corrective actions are presented, if any

Technische Universiteit **Eindhoven** University of Technology

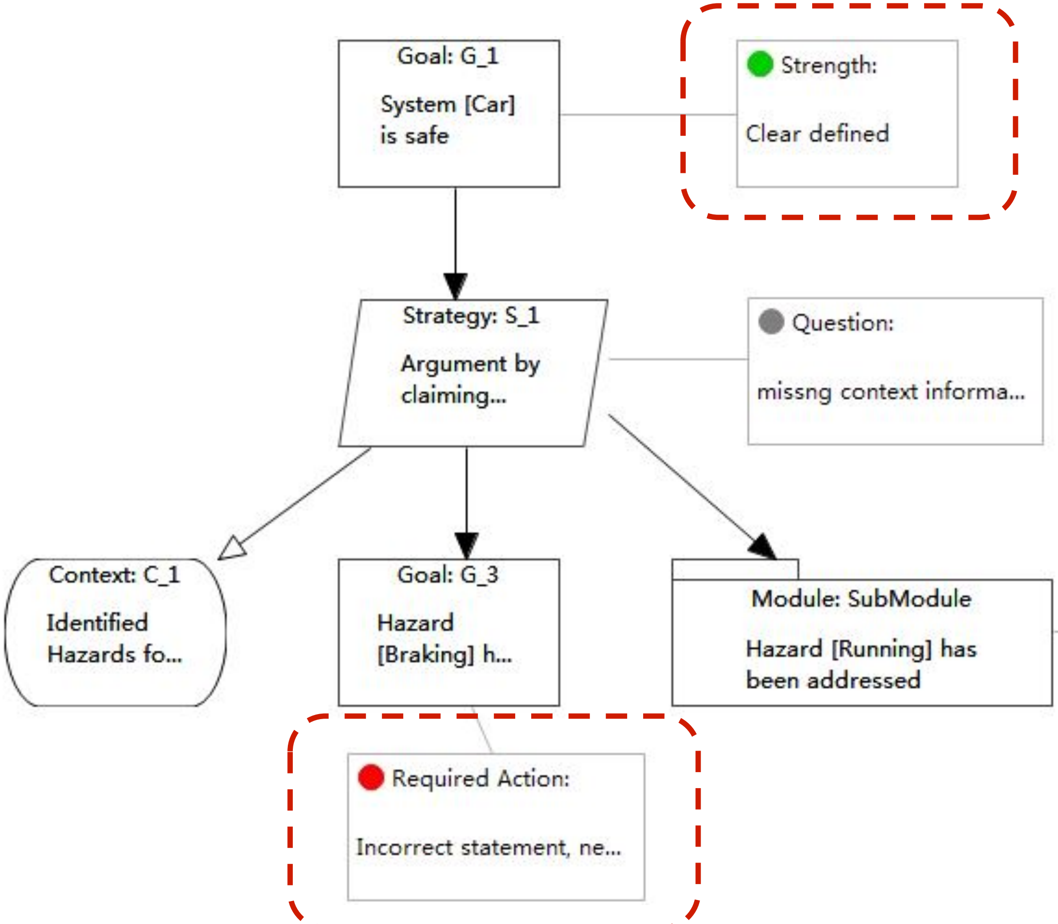
Safety Case Assessment

Metamodel



Safety Case Assessment

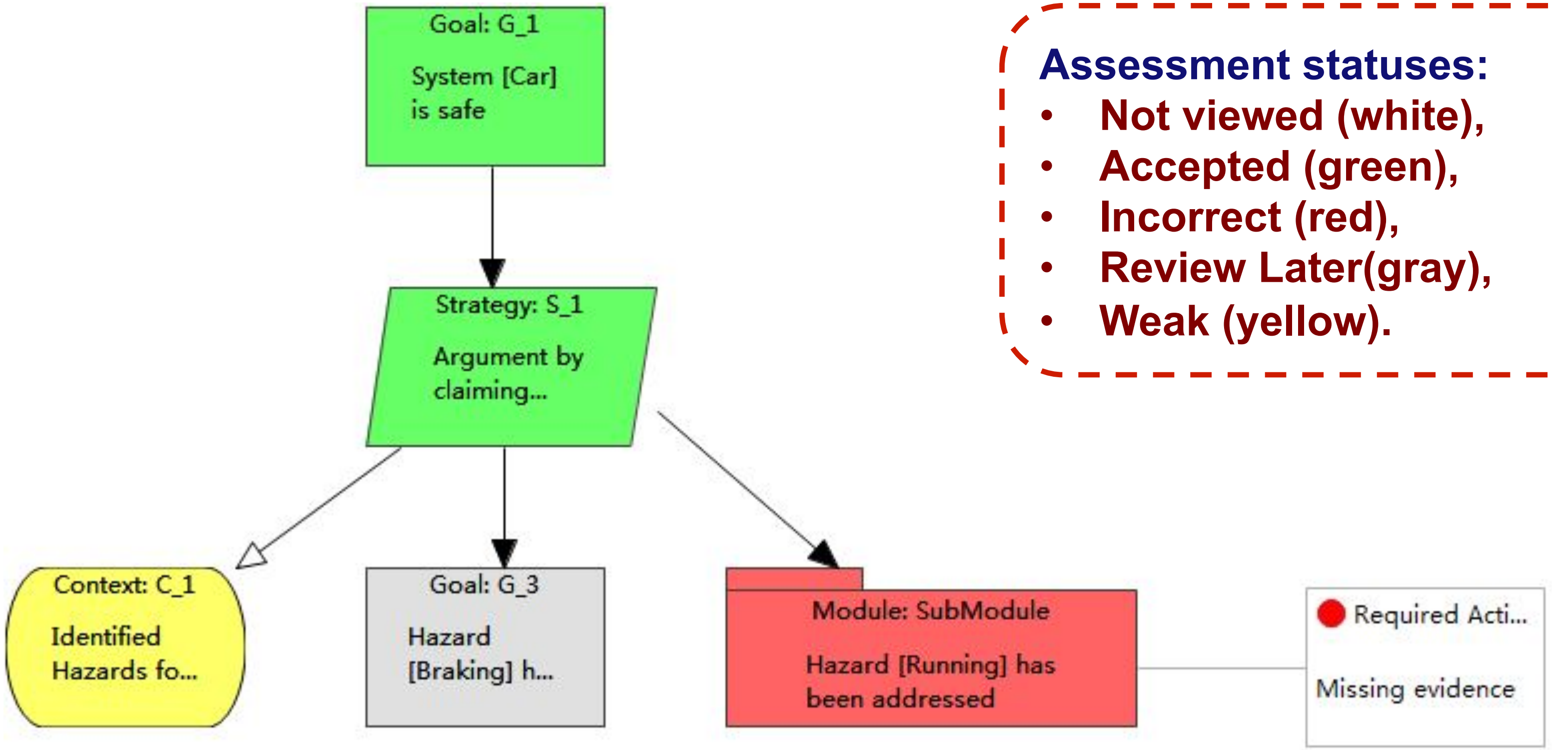
- **Use Case 1: add annotations to GSN elements**



Comment types:
- **Strength,**
- **Question,**
- **Weakness,**
- **Required repair Action.**

Safety Case Assessment

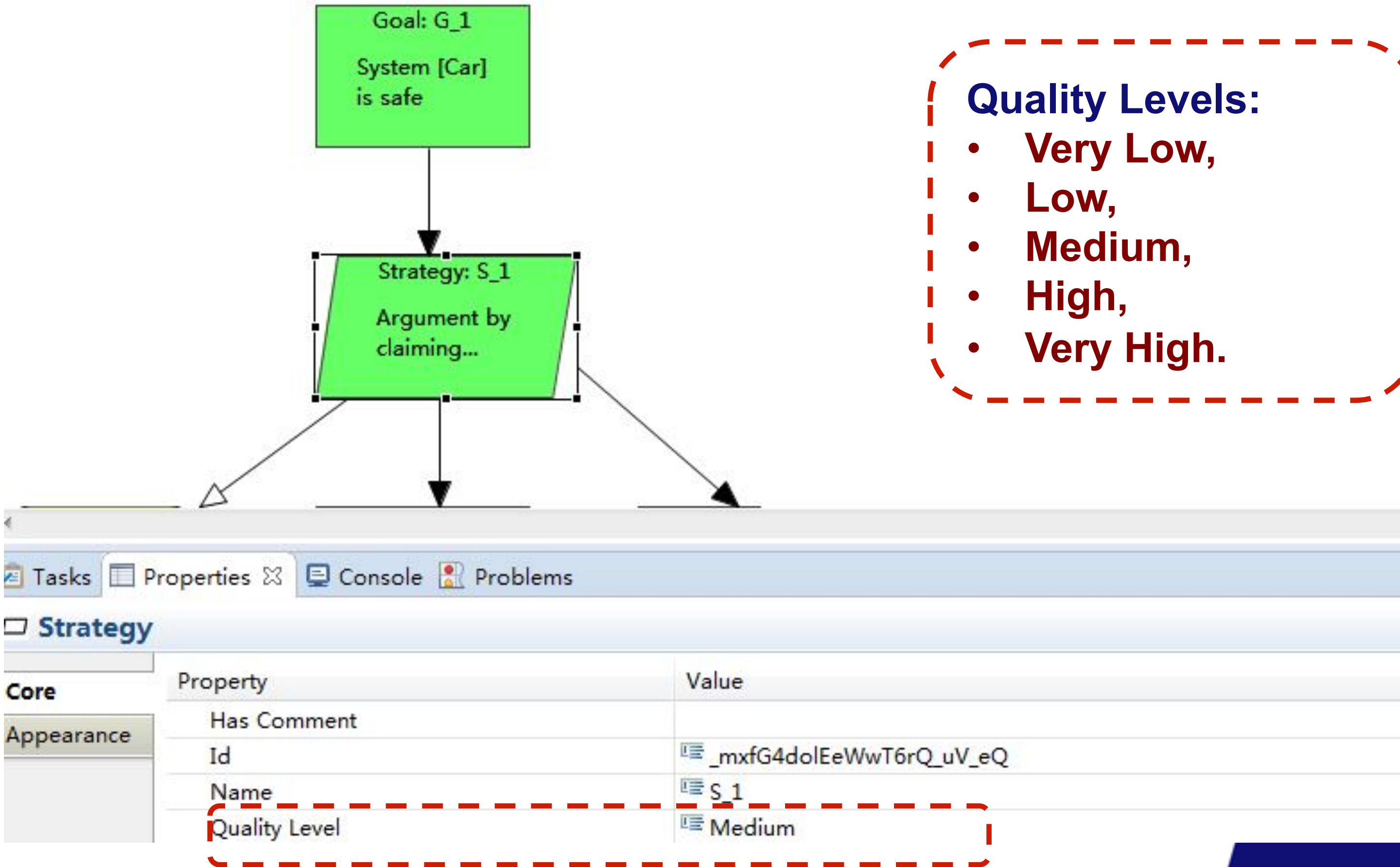
- **Use Case 2: change status of GSN elements**



Assessment statuses:
- **Not viewed (white),**
- **Accepted (green),**
- **Incorrect (red),**
- **Review Later(gray),**
- **Weak (yellow).**

Safety Case Assessment

- **Use Case 3: evaluate quality of GSN elements**



Quality Levels:
- **Very Low,**
- **Low,**
- **Medium,**
- **High,**
- **Very High.**

Future work

- Deriving metrics for safety case assessment to give an overall quality score of safety case and evidence
- Integration of functional safety standard into architectural modeling (in cooperation with TNO Automotive)
- Application to autonomous driving (i-CAVE project)

Conclusions

- Metrics are a means to establish the quality of automotive software

- Meta modeling is a powerful way of modeling safety standards
  - A meta model transformation approach is proposed to facilitate safety assurance
  - SMM in combination with SBVR allows a better way of developing safety cases
  - Meta-modeling of GSN creates better ways of safety case assessment

Observations

- Automotive industry is becoming more software intensive but still lack of proper software engineering disciplines
- Automotive software should be more open for inspection, maybe completely Open Source

Questions