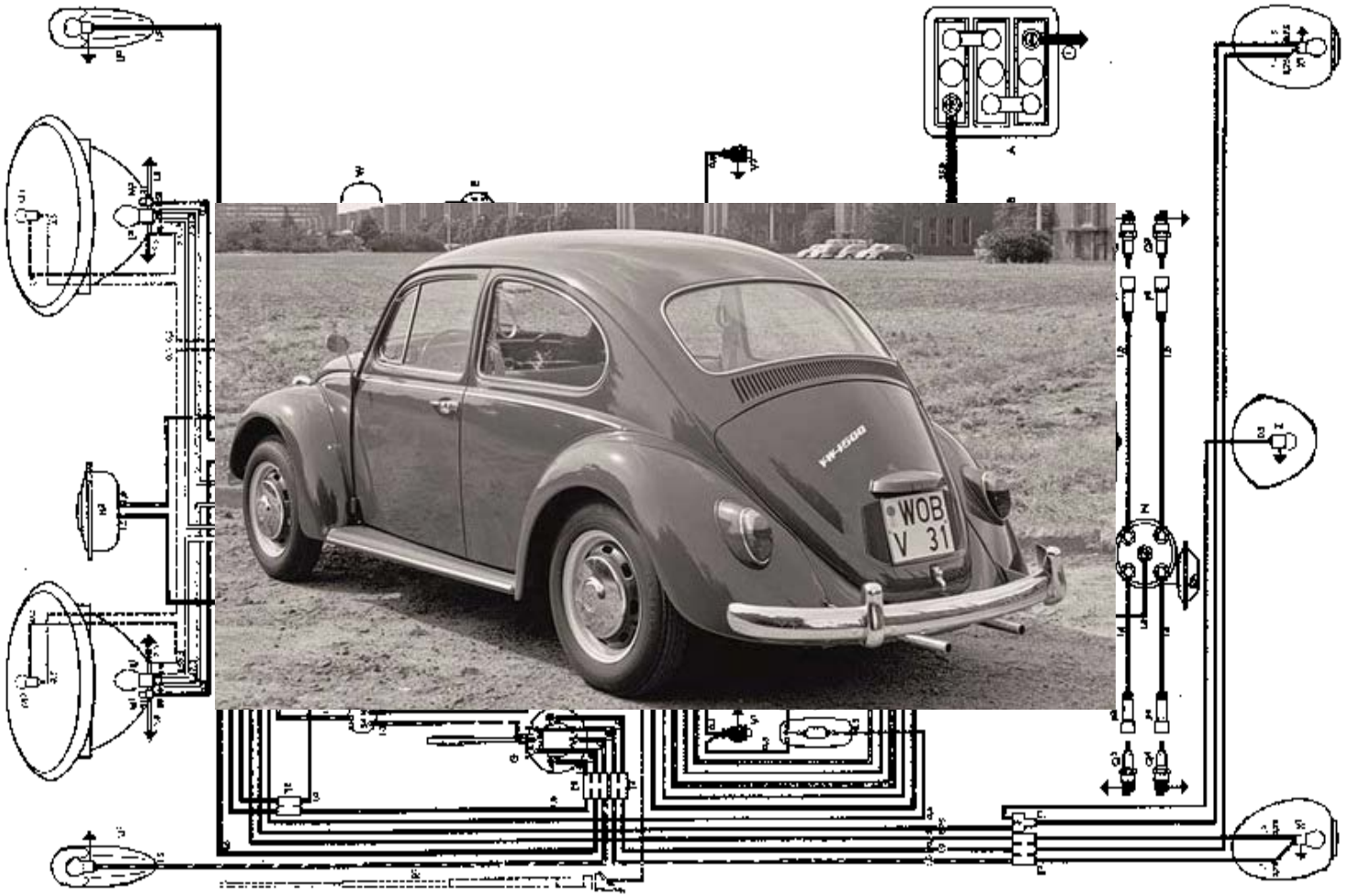
3.5. Elektrik-/ Elektronik-Konzeptbewertung

Dr.-Ing. Clemens Reichmann

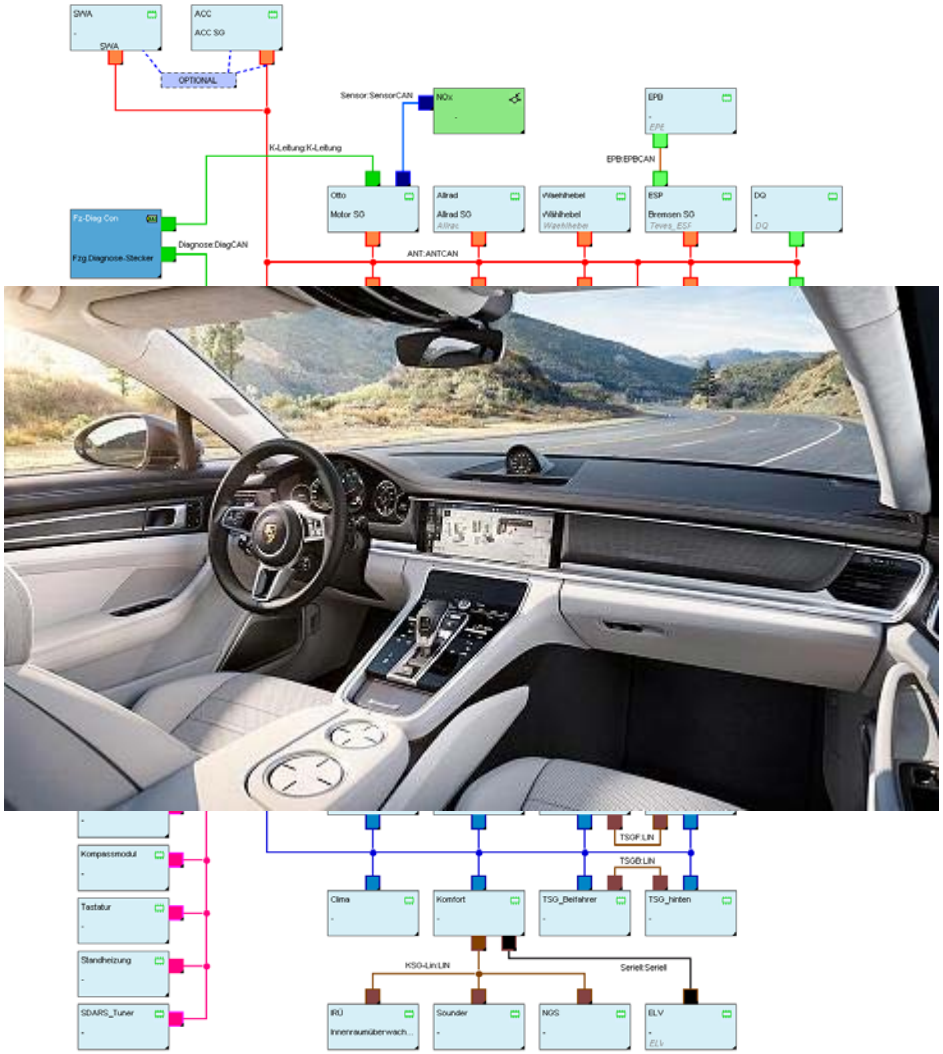
Clemens.Reichmann@vector.com,
Tel. 0721 / 91430-200

Institut für Technik der Informationsverarbeitung
Fakultät für Elektrotechnik & Informationstechnik
Universität Karlsruhe (KIT)

Overall E/E Complexity Increasing over Years now…



Overall E/E Complexity Increasing over Years now…



Overall E/E Complexity Increasing over Years now…

- Active Management of System Complexity is necessary
  - Economical cost targets
  - Technical targets: weight, fuel consumption, …
  - Installation space is restricted, deeper integration
  - Upcoming technologies have to be considered and integrated
  - …

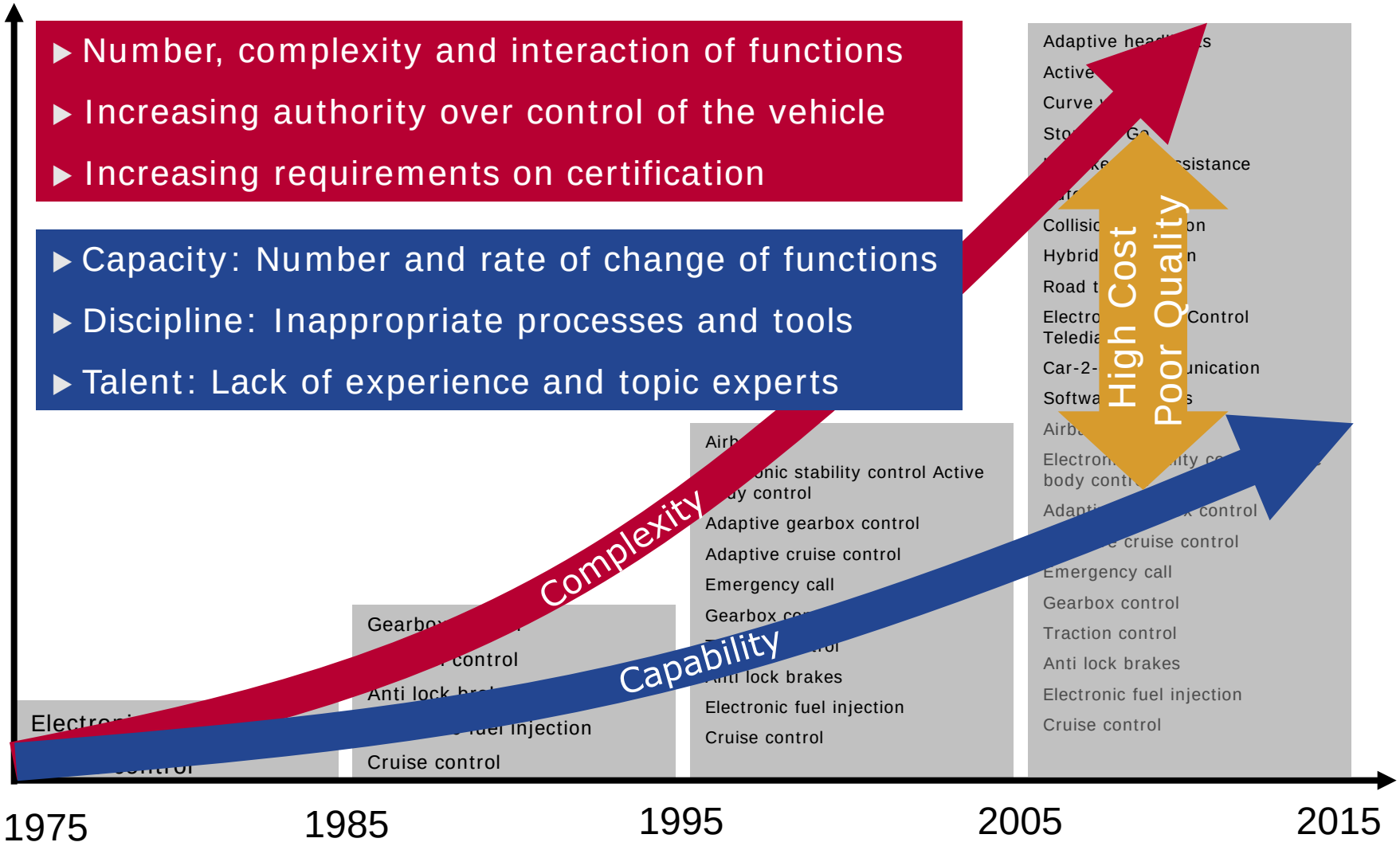
Mehr als 25% (zukünftig bis zu 40%) der Produktionskosten eines Personenkraftwagens für Elektrik/Elektronik

90 % aller Innovationen basieren auf Elektronik

Software Anteil schnell wachsend

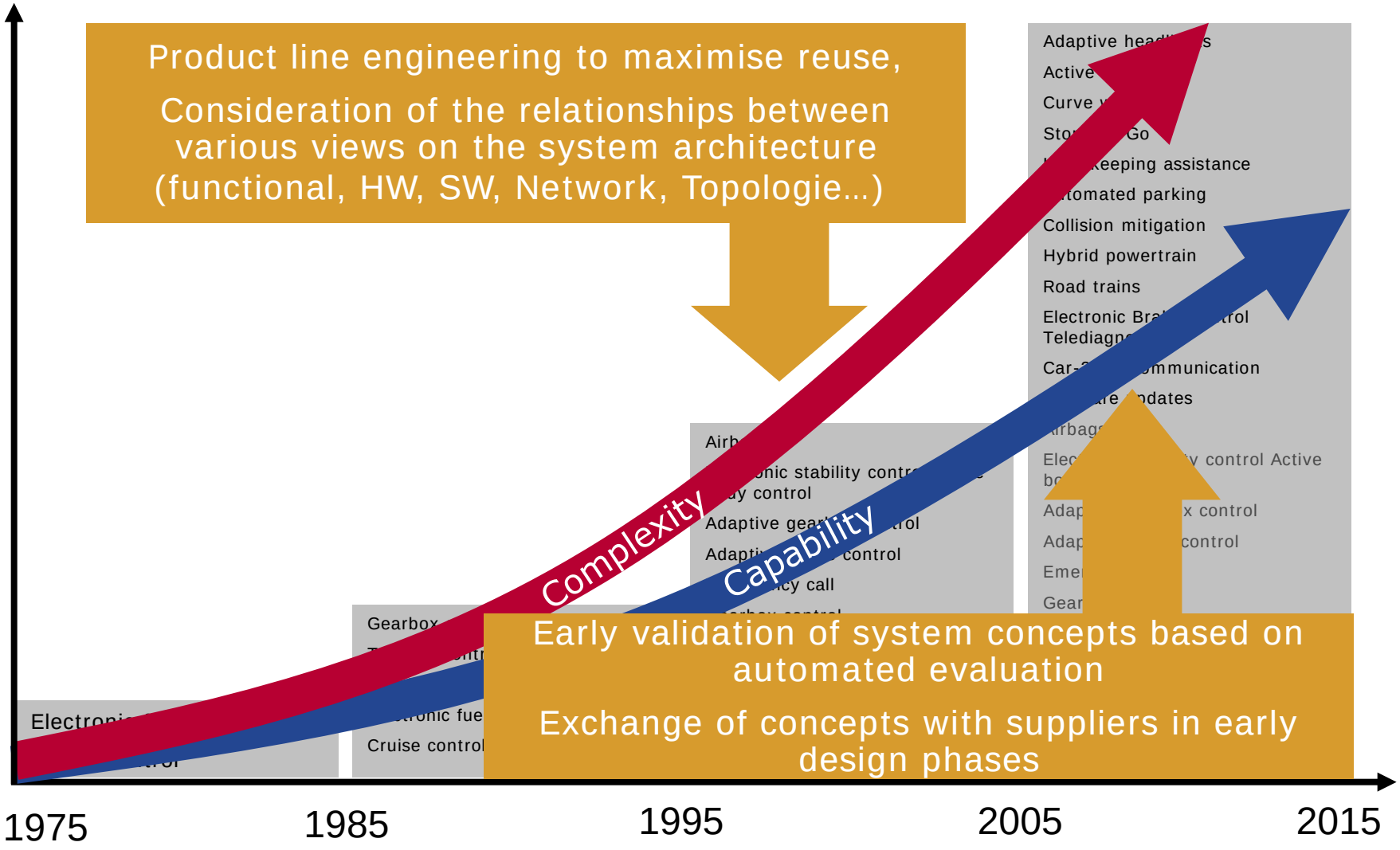
Challenges in E/E Development

The Complexity/Capability Gap

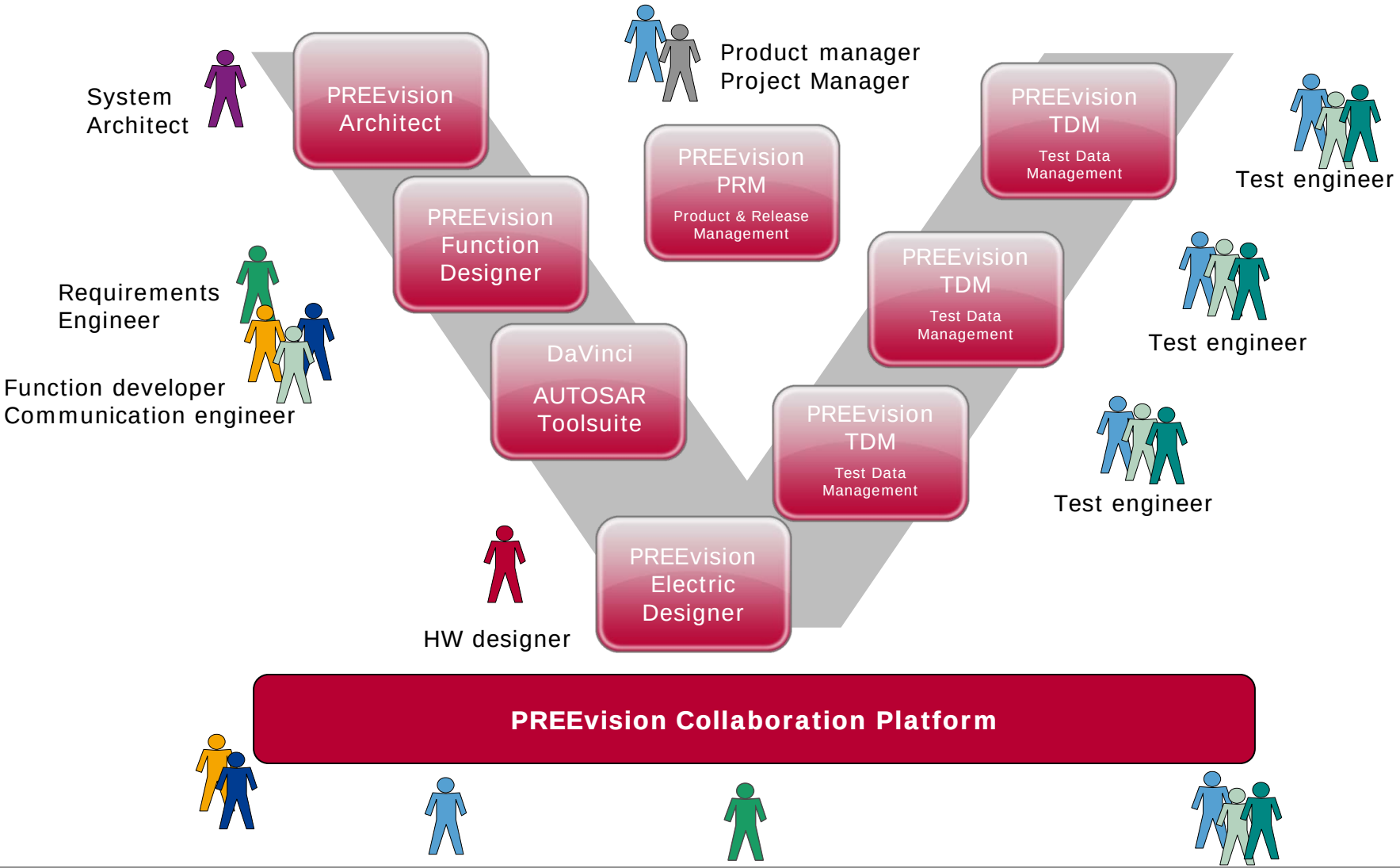


Challenges in E/E Development

Closing the Complexity/Capability Gap



Roles



Challenges in E/E Development

Current Situation – Document Based Development Process

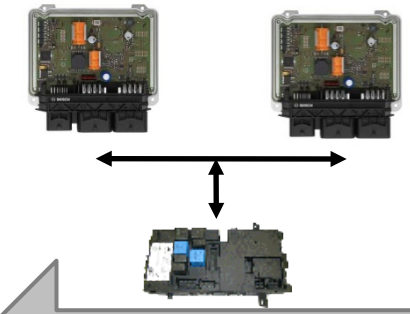
Function & Network Design Process

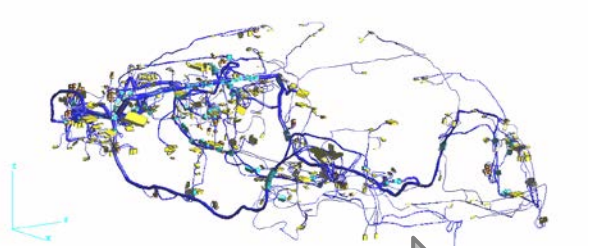
Electric Design Process

1000s of Inconsistent Documents

-Components
-Functions
-Networks
-Signals
...

-Harness
-Topology
-Fusing
-PowerSupply
...

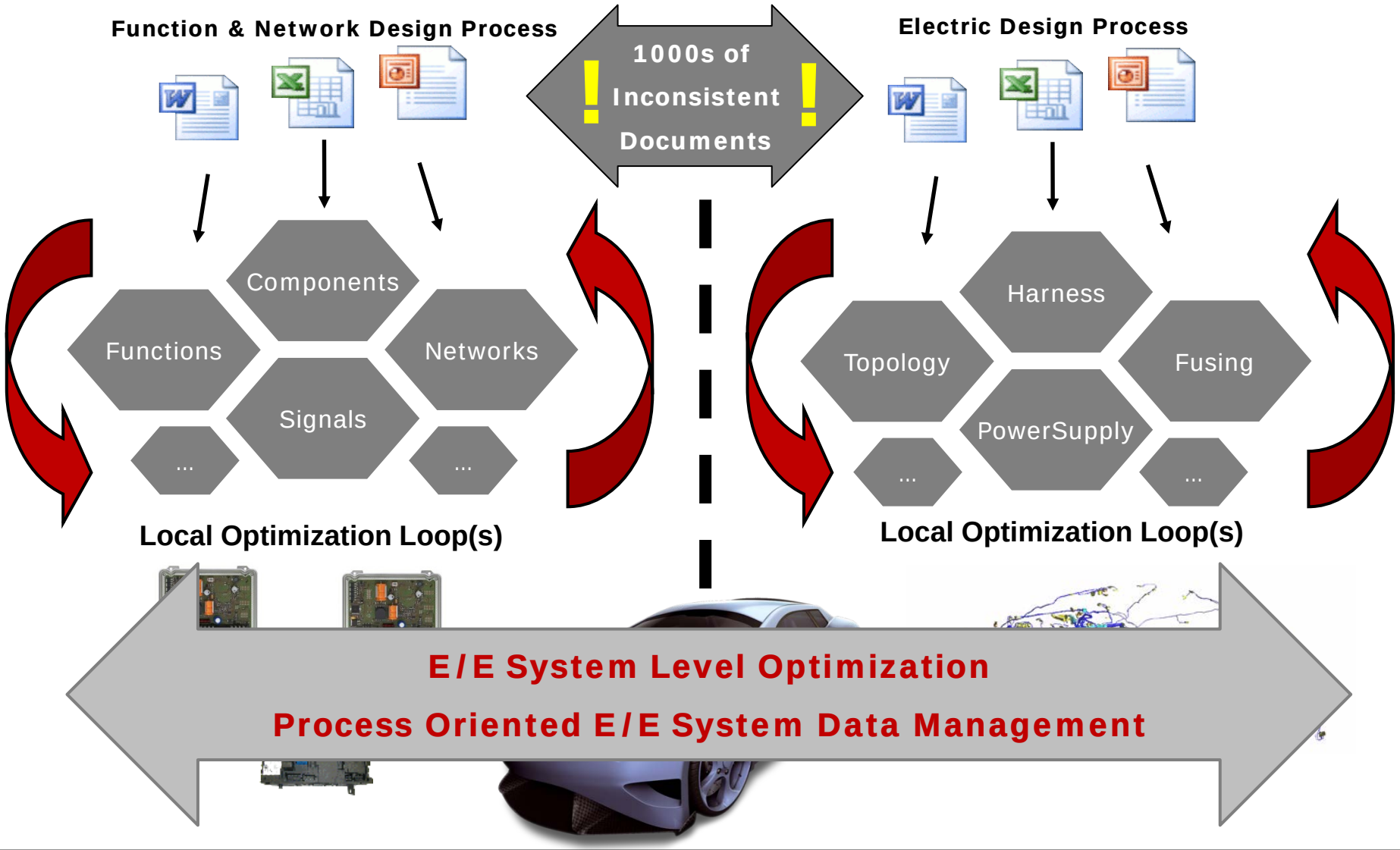




E/E Systems Level Optimization

Process Oriented E/E System Data Management

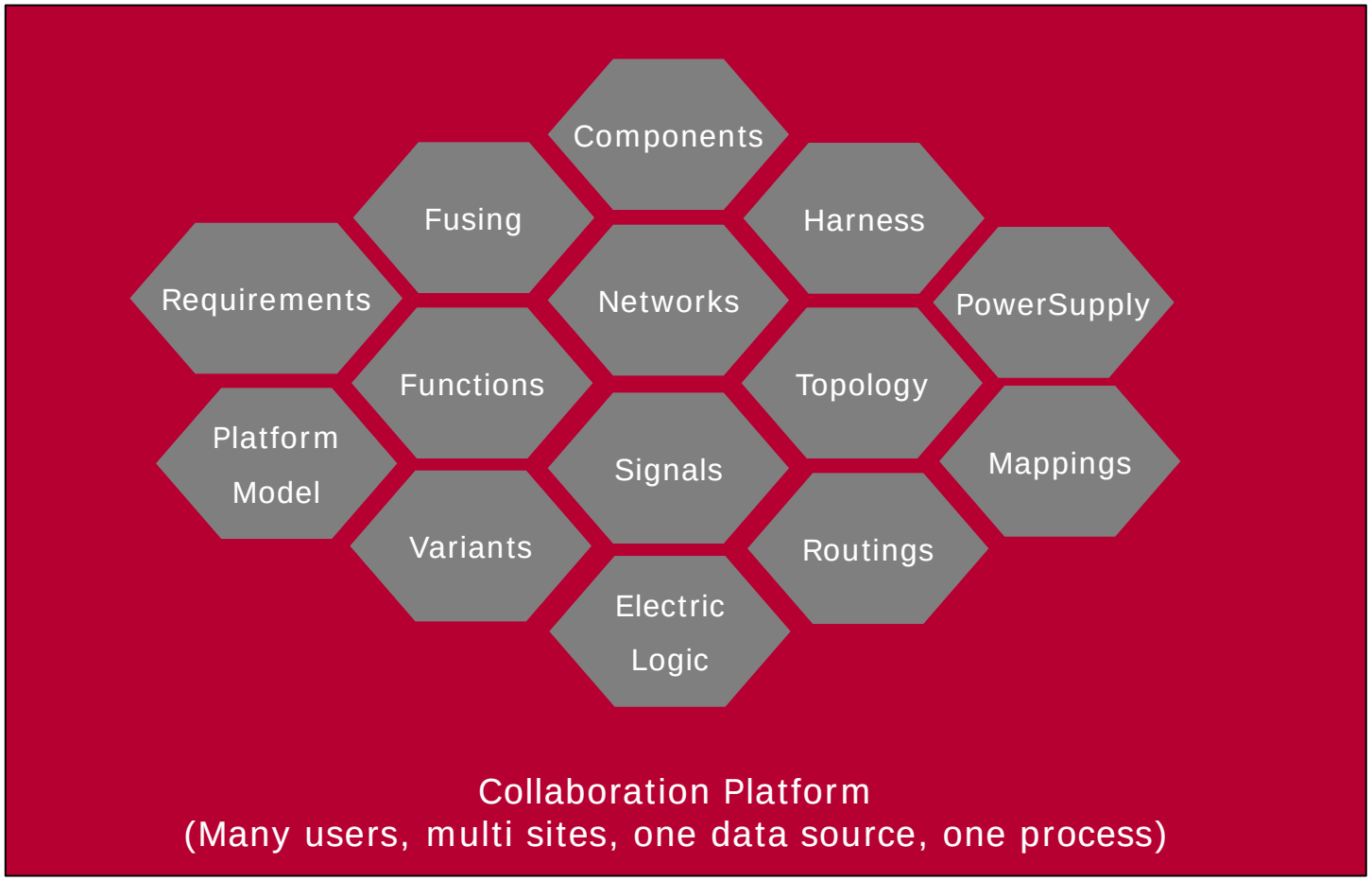
E/E Backbone – Central Team Server



Integrated E/E Development with PREEvision

Data Oriented E/E Development Process

PREEVISION® One data model, one GUI, full traceability



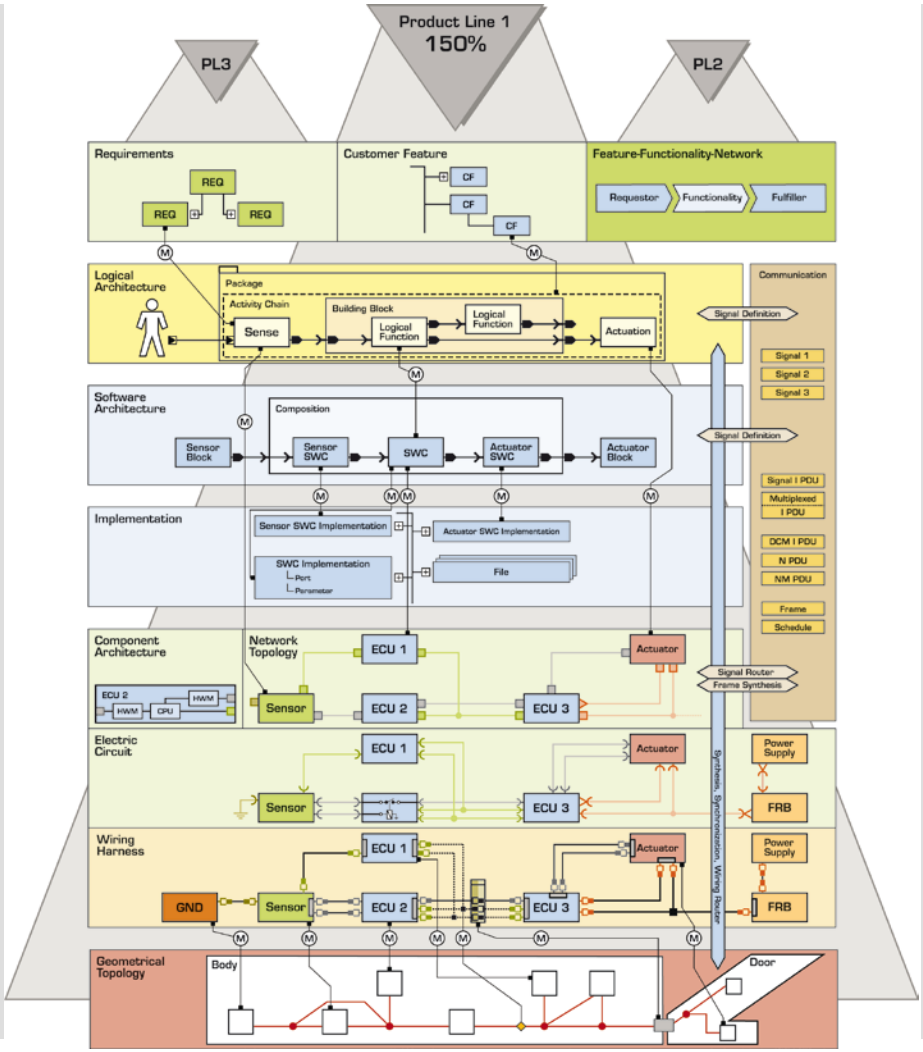
vector

Integrated E/E Development with PREEvision

Architecture Layers

Engineering Aid

- Model Queries
- Consistency checks
- Metrics
- Report generation
- Synthesis
- Routing



Interfaces

- Excel
- RIF
- Simulink
- ASCET
- ARXML
- FIBEX
- DBC
- ELOG
- KBL
- Catia

PREEvision Layers – Requirement to Function

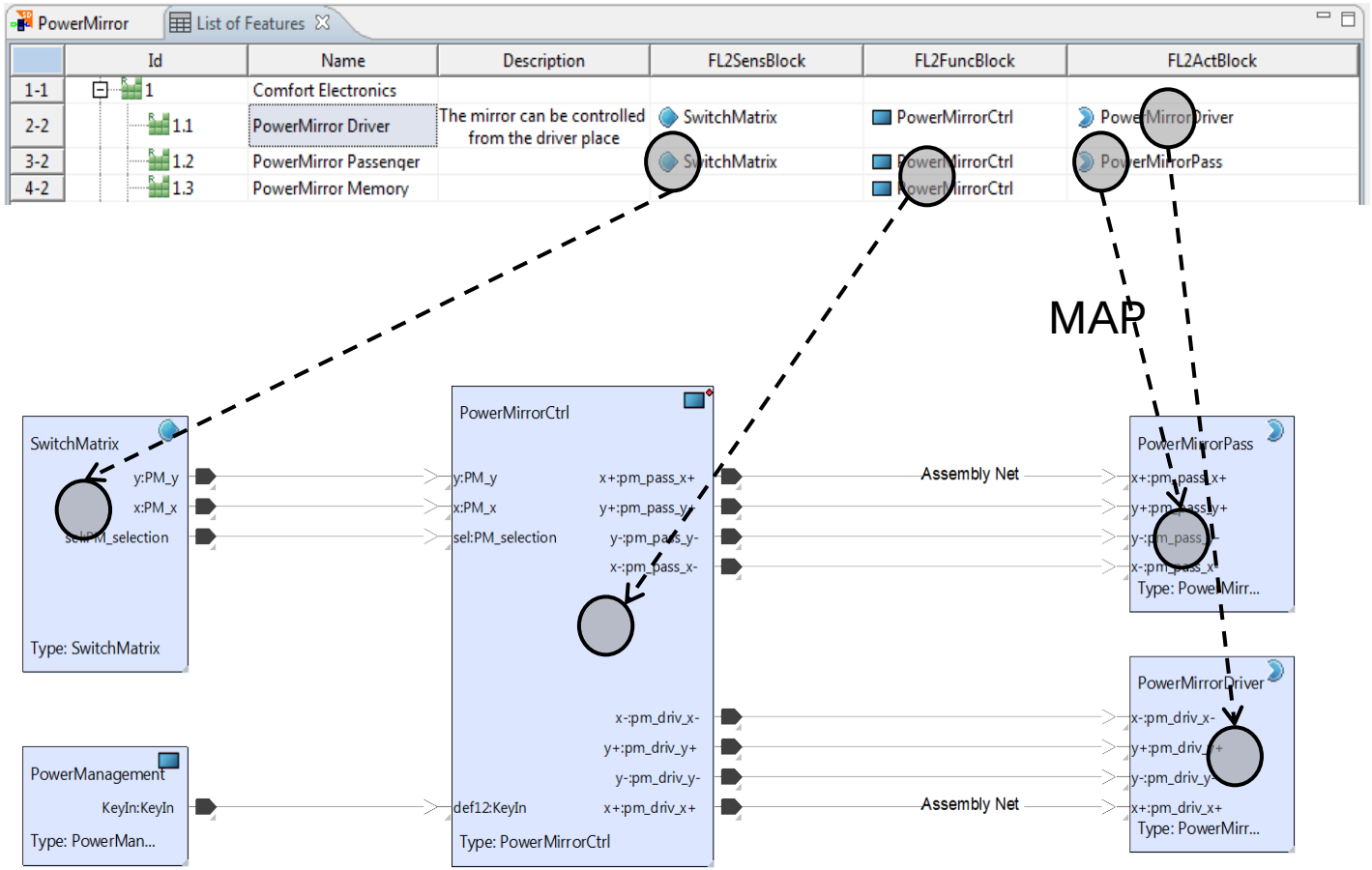
Requirements

Feature List

MAP

Function

Network



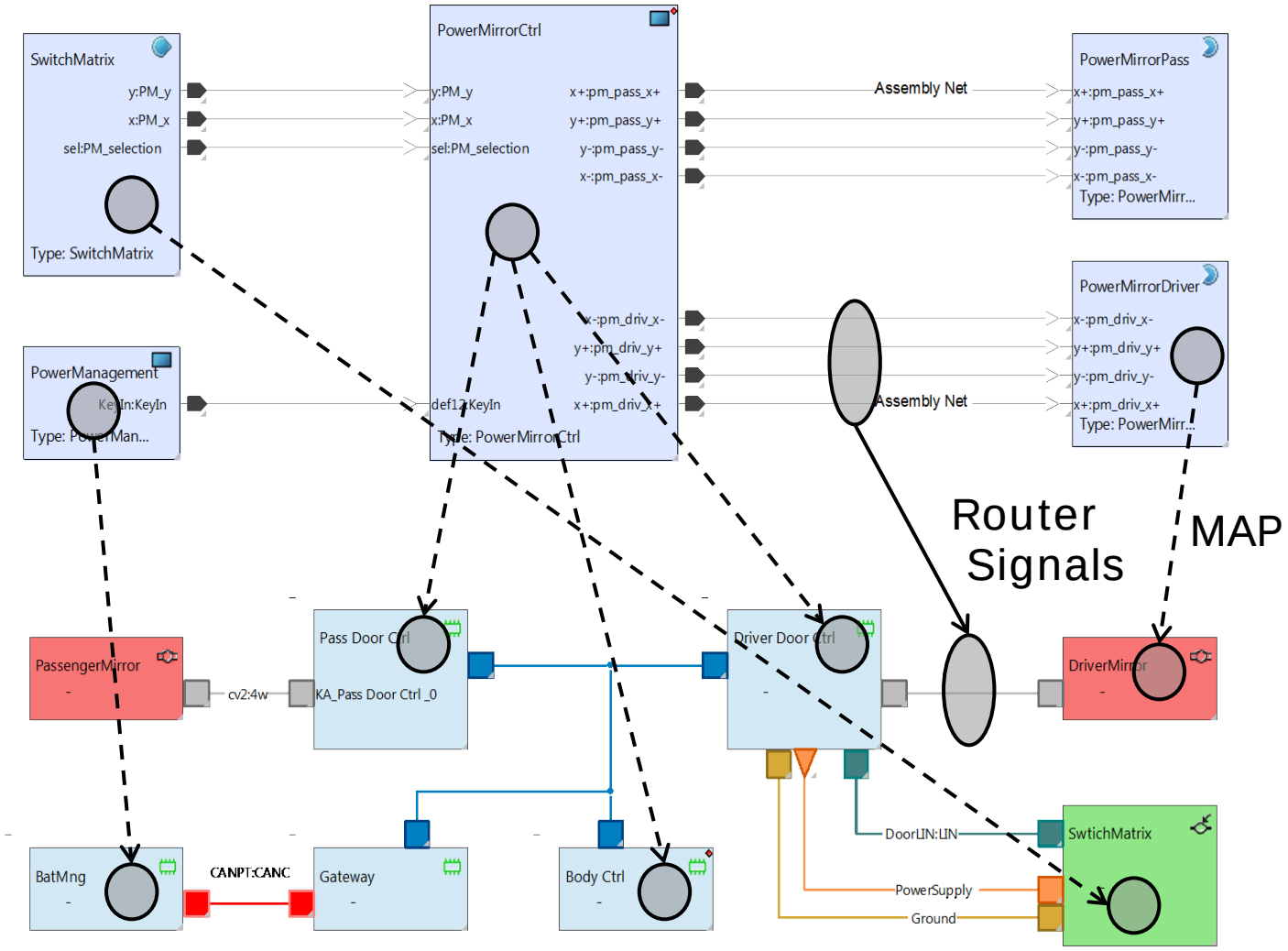
PREEvision Layers – Function Net to Components

Function Network

ROUTE

MAP

Component Network

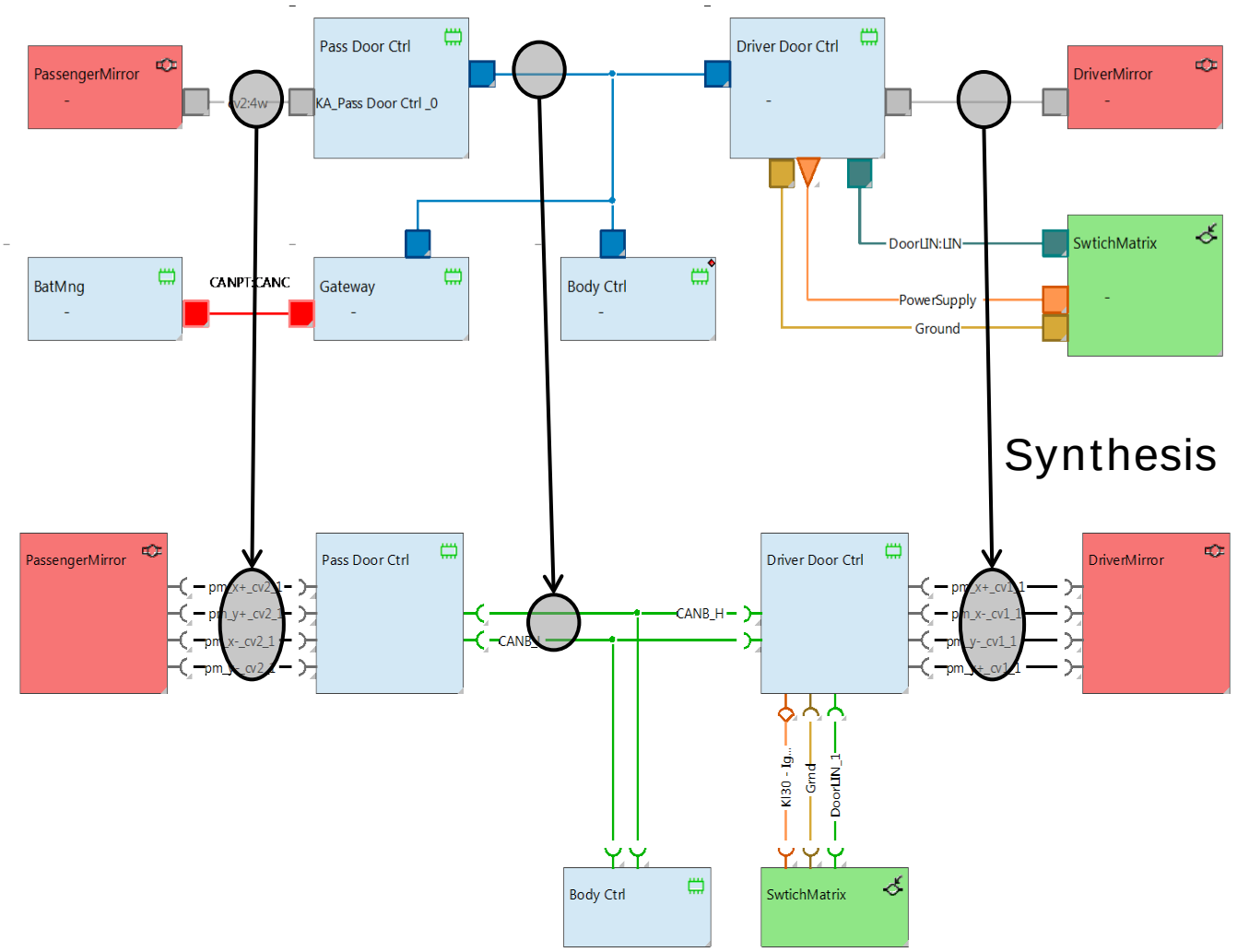


PREEvision Layers – Components & Circuits

Component Network

Synthesis

Circuits

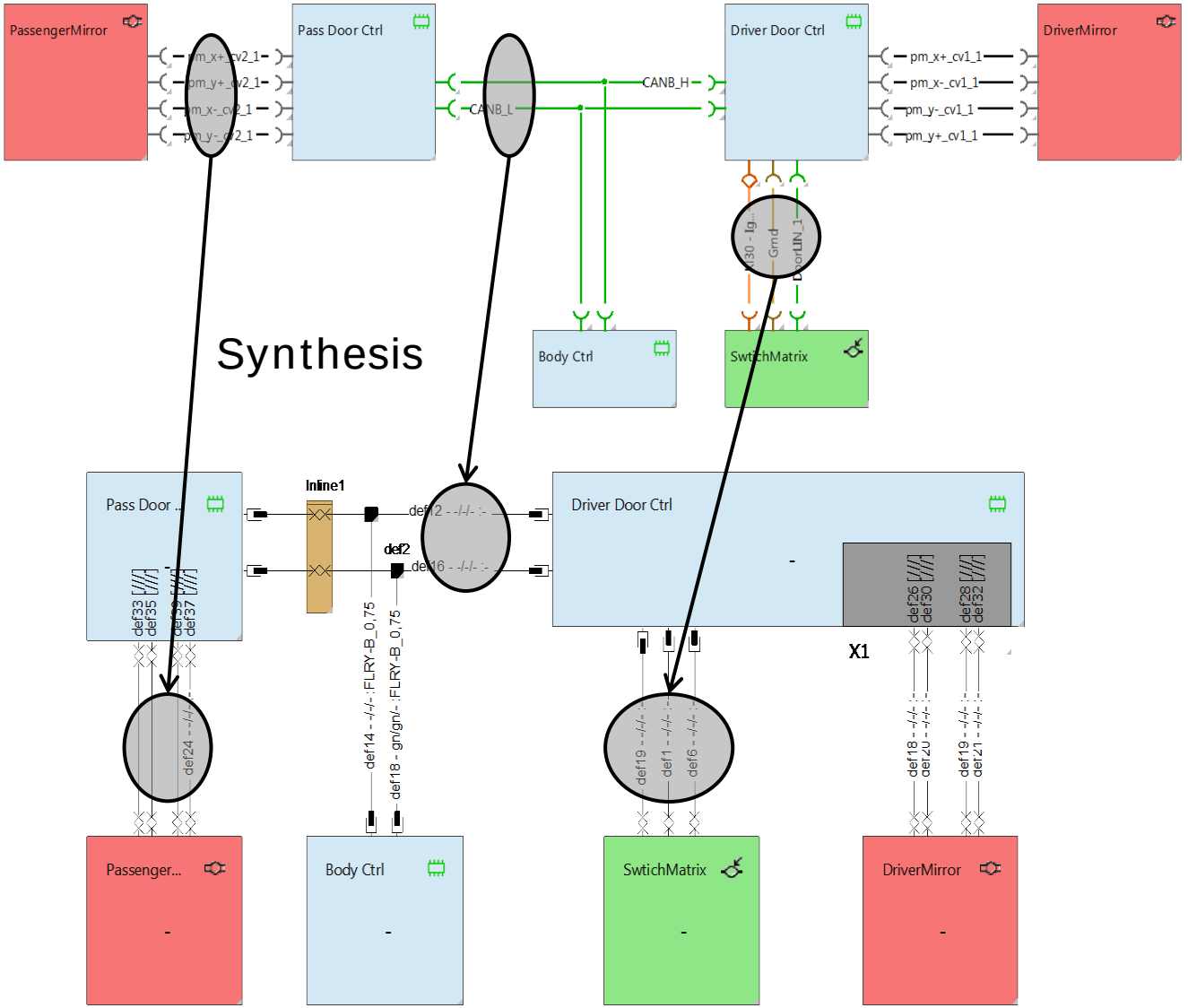


PREEvision Layers – Components & Wiring Harness

Circuits

Synthesis

Wiring Harness



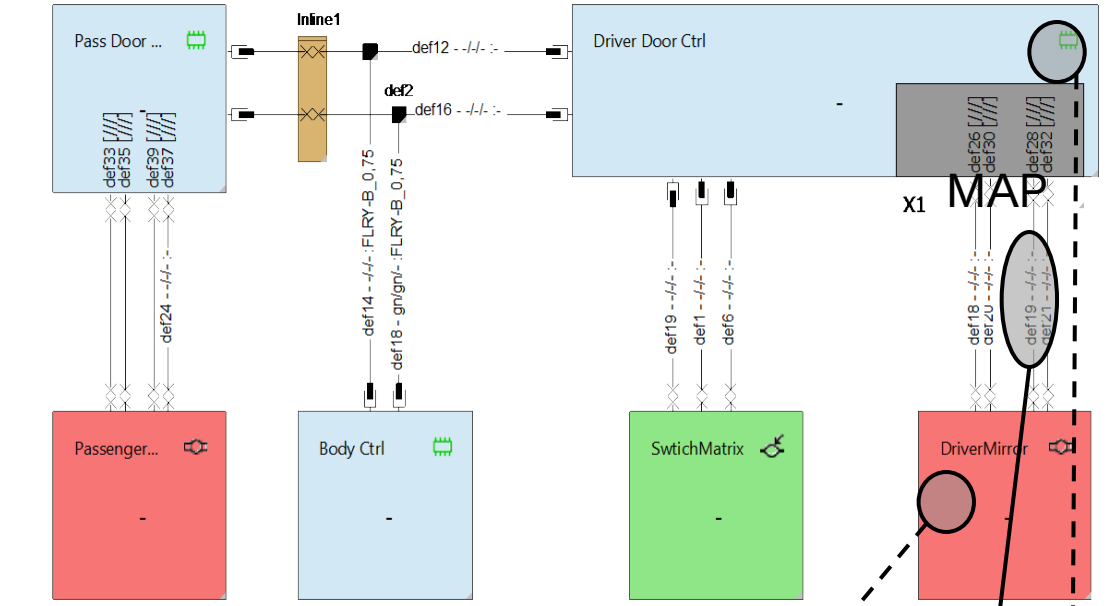
PREEvision Layers – Harness + Components to Topology

Wiring Harness

ROUTE

MAP

Topology



Integrated E/E Development with PREEvision

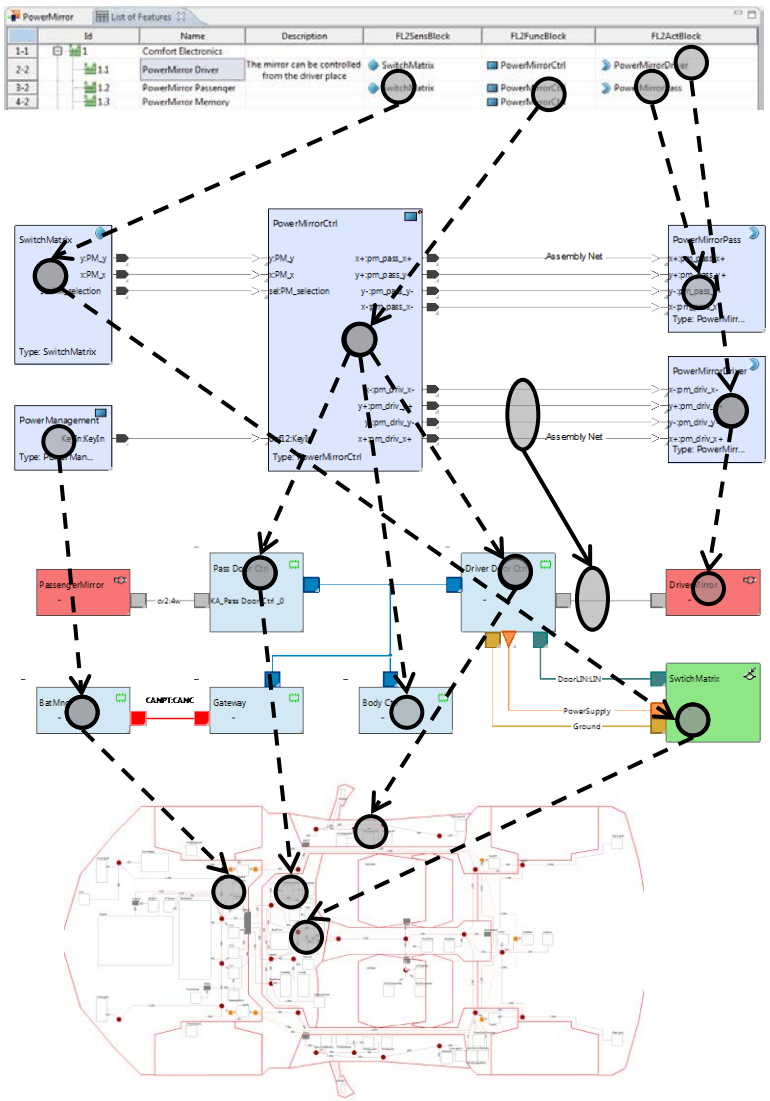
Model Based Systems Engineering

Requirements

Logical/SW Architecture

Network/HW Architecture

Wiring/ Geometry



- **Domain specific** language and data model.
- **Single source model** across all development levels and disciplines.
- Support for reuse and **product line engineering**.
- Automated **report generation** and **consistency checks**.
- **Metrics** for Benchmarking
- **Automated algorithms** for scheduling, signal routing, etc.
- **Import and export** of industry exchange formats (e.g. AUTOSAR, KBL, FIBEX...)

Improvements in Handling of Complex Systems

Strategic Focus Areas

Variants / Reuse,

E/E Domain Modeling,

Many People

Productline Support

Extended Vehicle-Variant-Management (brands, construction types)

- Definition of Productline structure
- Reuse of ReuseUnits
- Adaption of ReuseUnits
- Integration of ReuseUnit

Seamless E/E Data Model

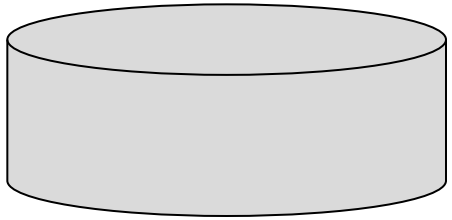
- Integrated Requirements and Test Management
- E/E & SW/Impl.
  - E/E-Modeling
  - Data-/Filemanagement
  - Metadata of Impl. Artifacts
  - Traceability

Feasibility & Efficiency

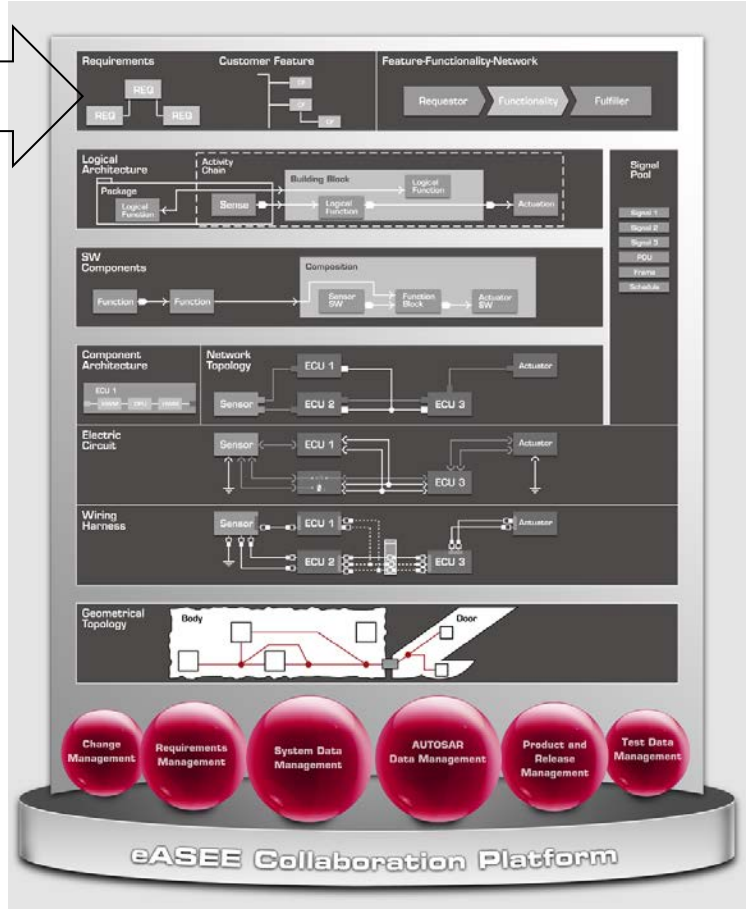
- Cost, Optimizations
- Synthesis
- Evaluation / Benchmarking

Multiuser Environment

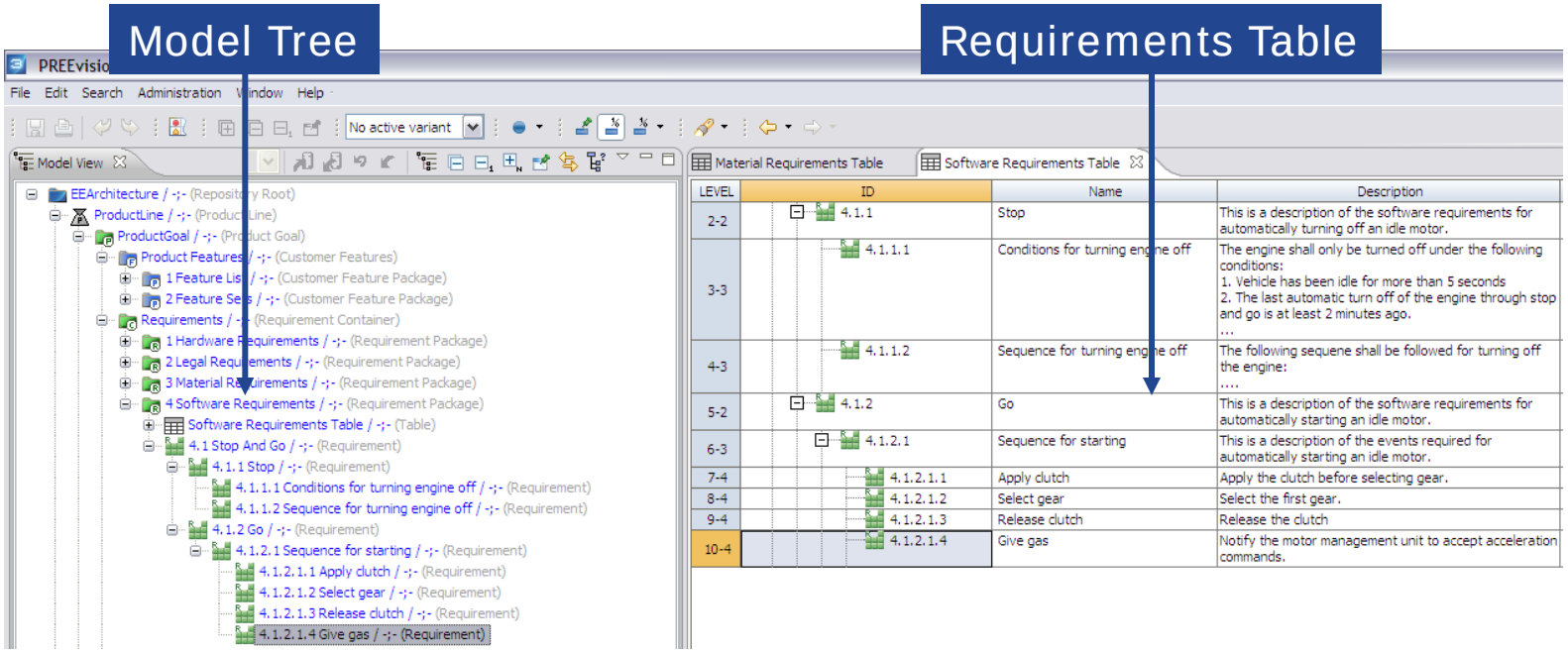
- Team Collaboration
- High Performance Cache
- E/E Data Backbone
  - With corporate wide PDM (preferred Teamcenter)
  - Standalone



Requirements Management

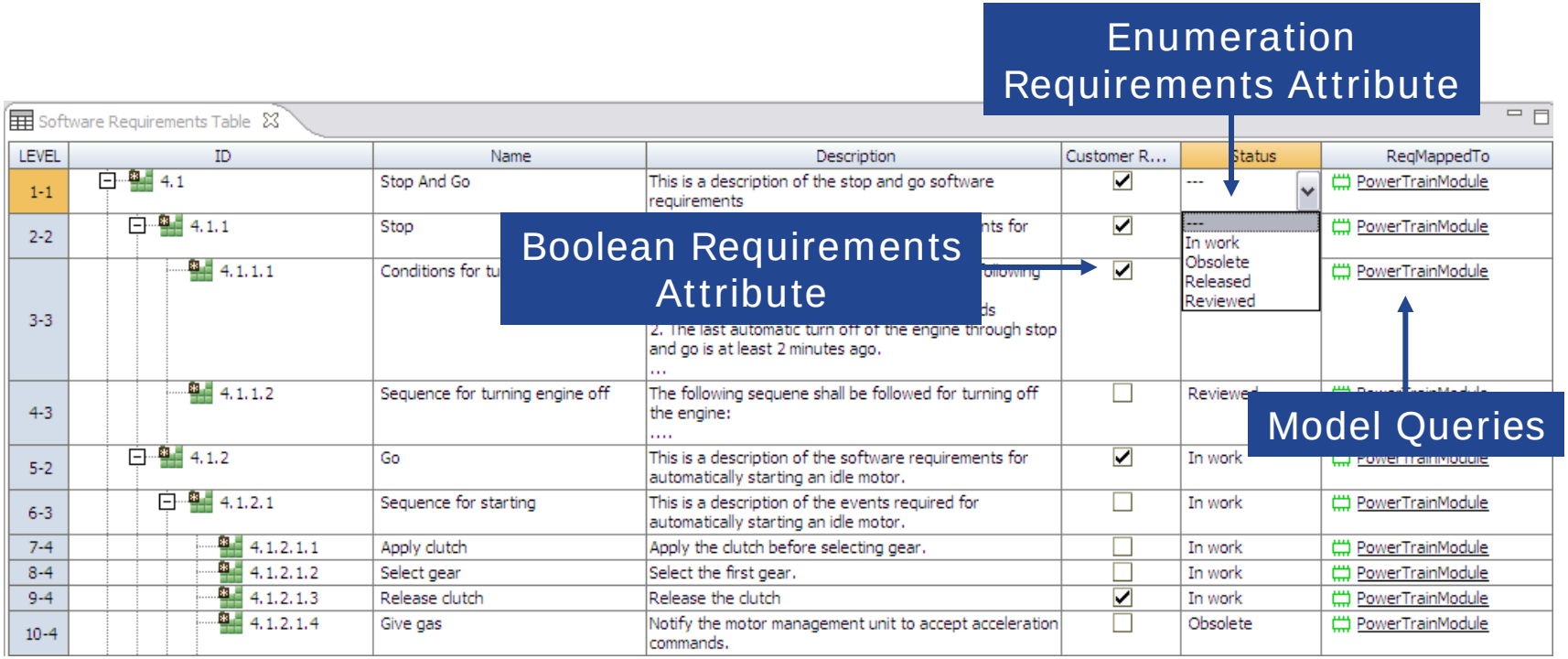


Structuring and Editing Requirements



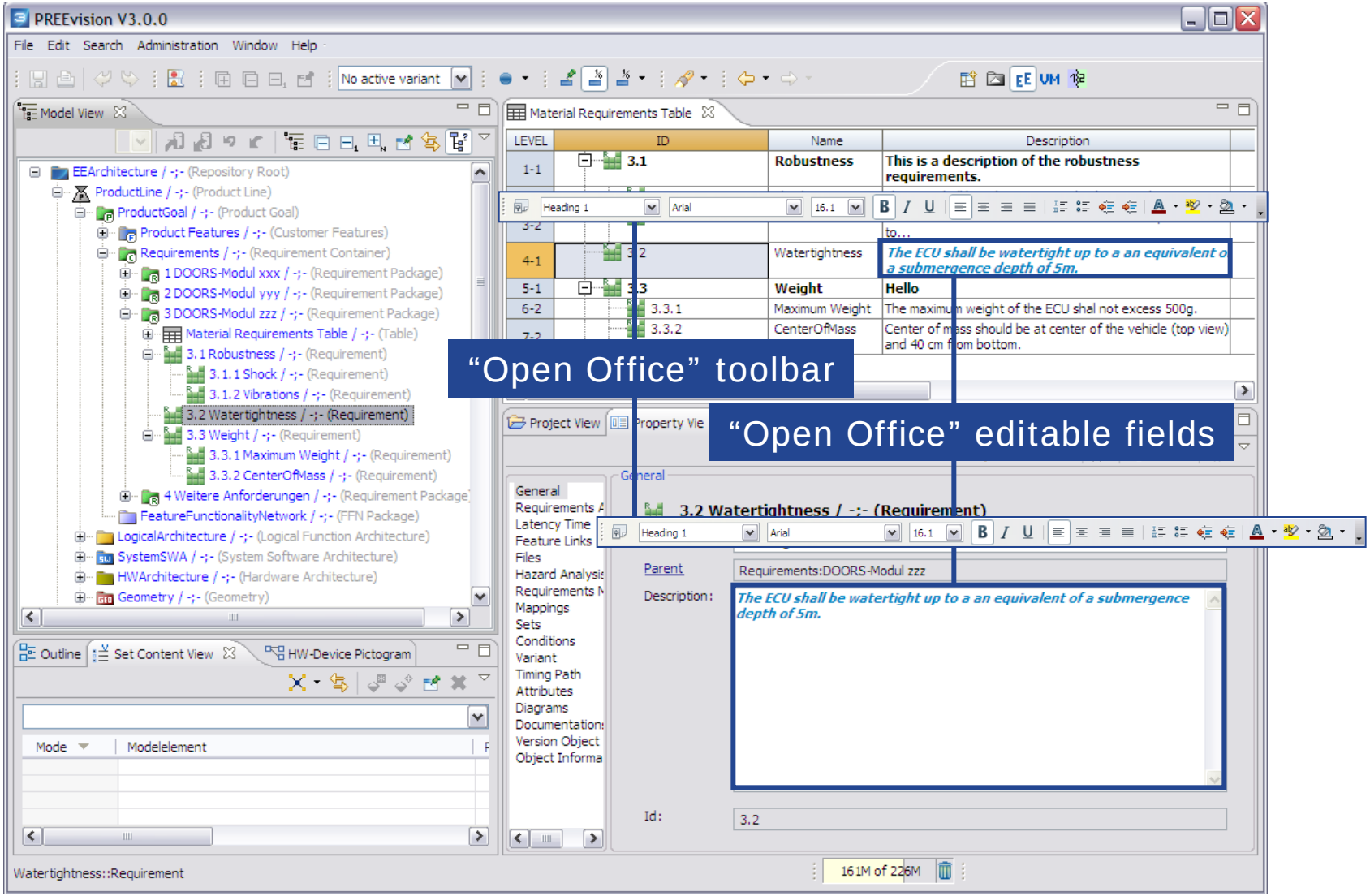
- Requirements can be grouped into requirements packages and structured hierarchically.
- Tables provide an efficient overview and editing capability.

Requirements Attributes and tables

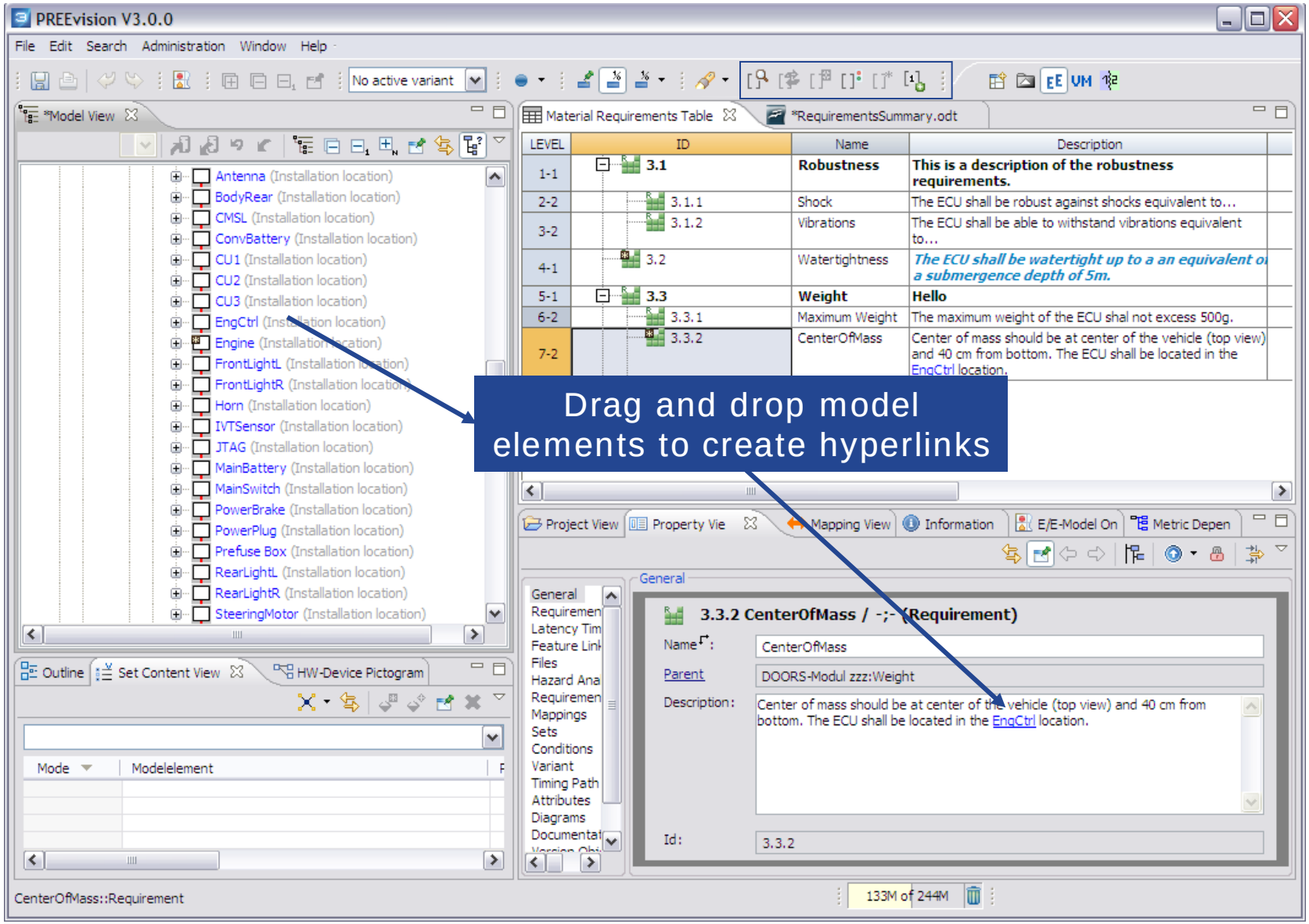


- Requirements can be extended with user-defined attributes that can be directly edited in the requirements tables.
- Attributes can be typed, e.g. Boolean, Enumeration, Integers with valid value ranges,..., and are handled accordingly in tables.
- Requirements tables can display the results of model queries. E.g. ECUs to which the requirements are mapped.

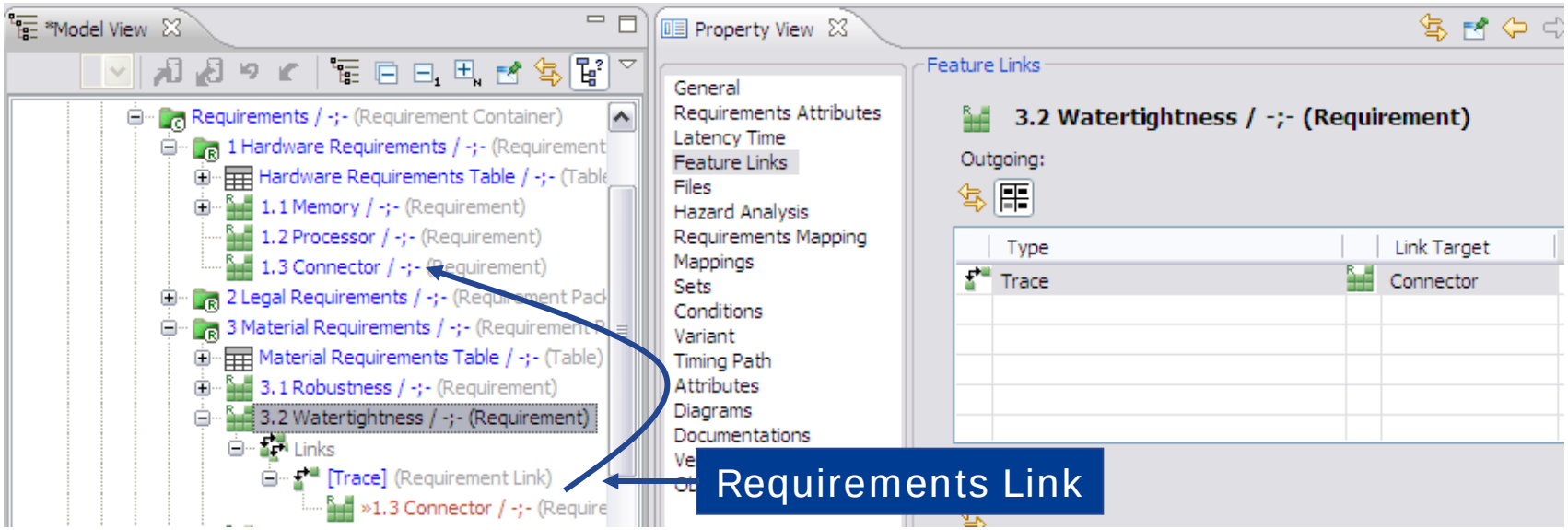
Open Office Integration – Editable Fields



Open Office Integration – Hyperlinks

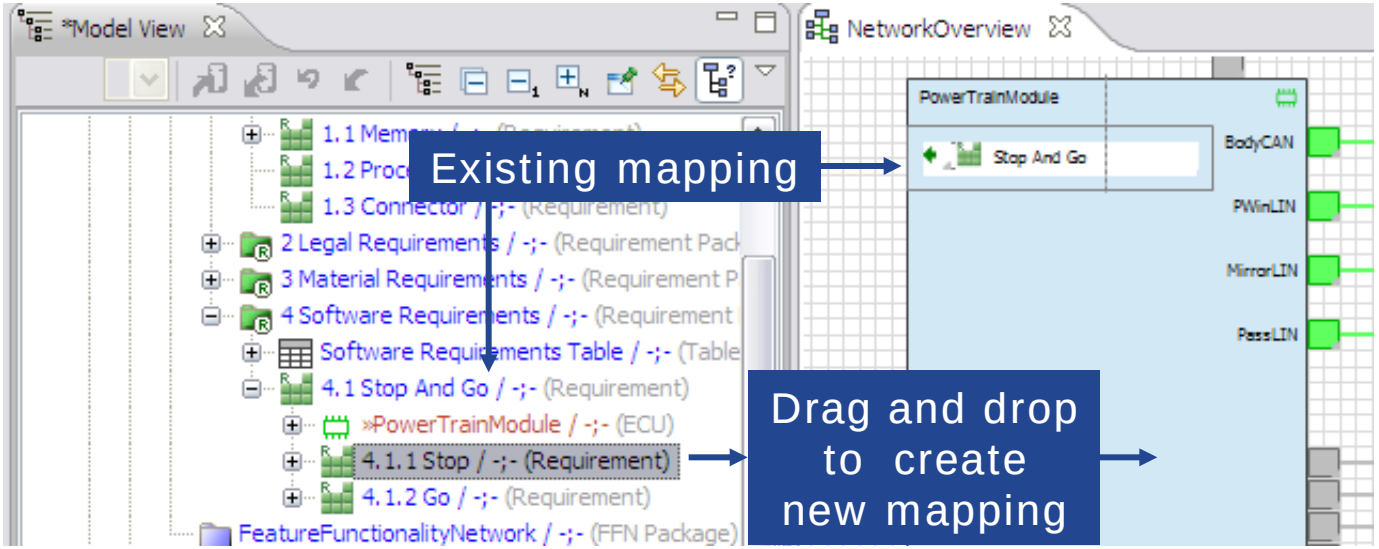


Linking Requirements



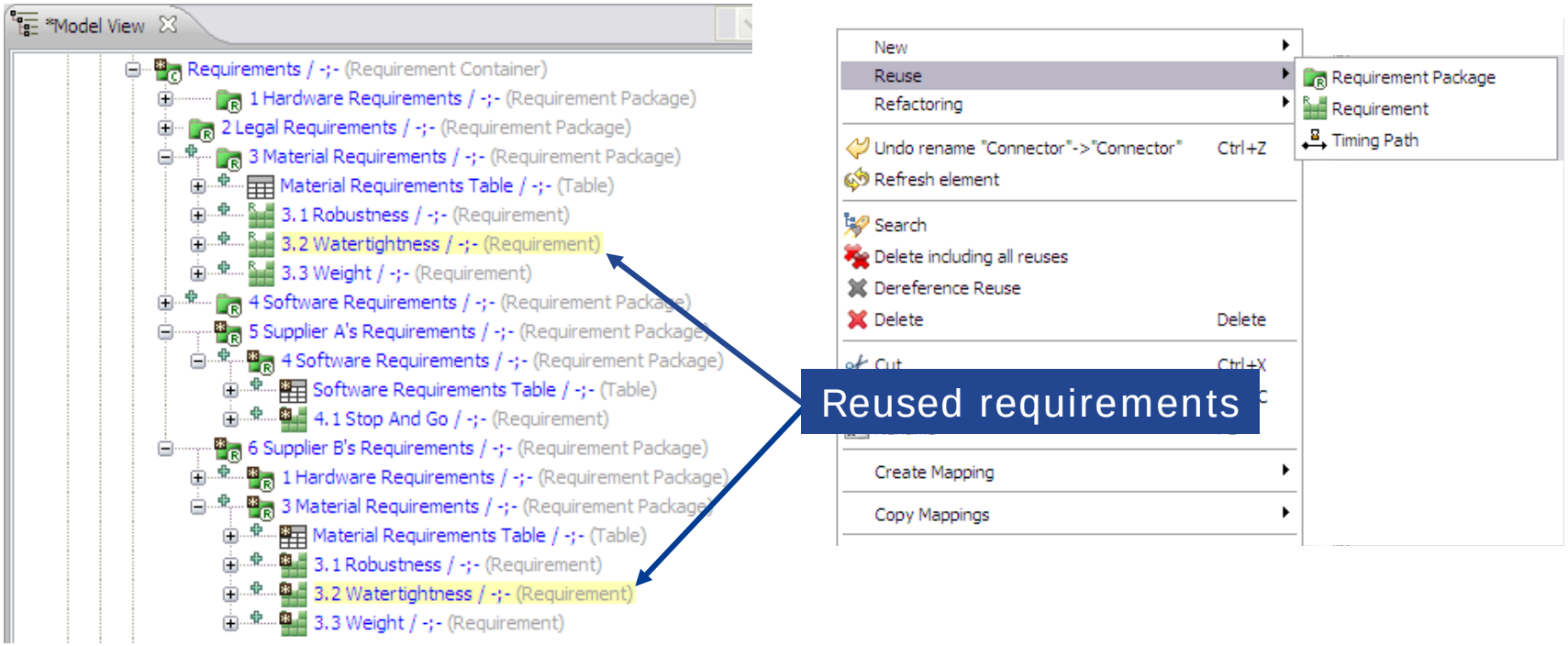
- Requirements can be linked to other requirements to maintain traceability.
- Linked requirements are shown in the model tree and property view.
- User can directly navigate to linked requirements by pressing the space bar.

Mapping Requirements



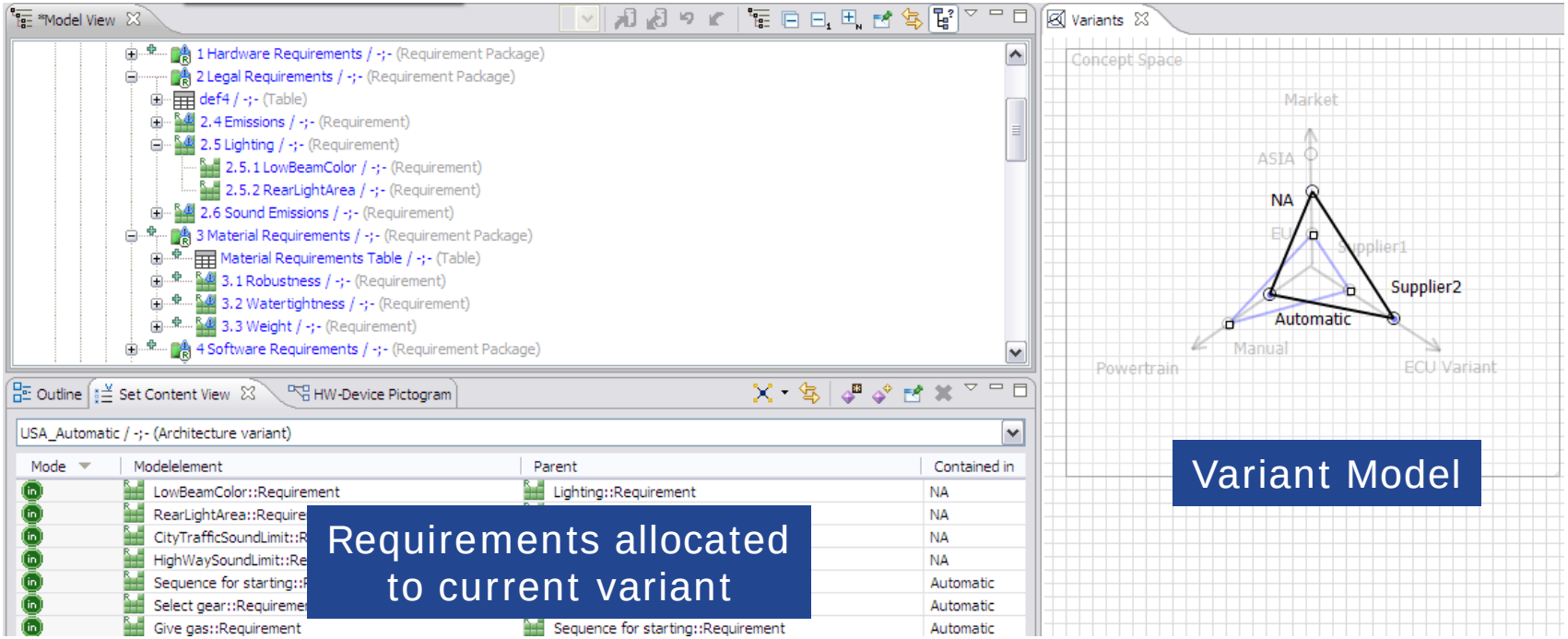
- Requirements can be directly mapped to architecture artefacts E.g. Logical functions, SW Functions, ECUs, Hardware modules,…
- Mappings can be created by dragging and dropping between requirements in the model tree and graphical elements.
- The results of the mappings can be displayed in the diagrams and model tree.

Reuse of Requirements



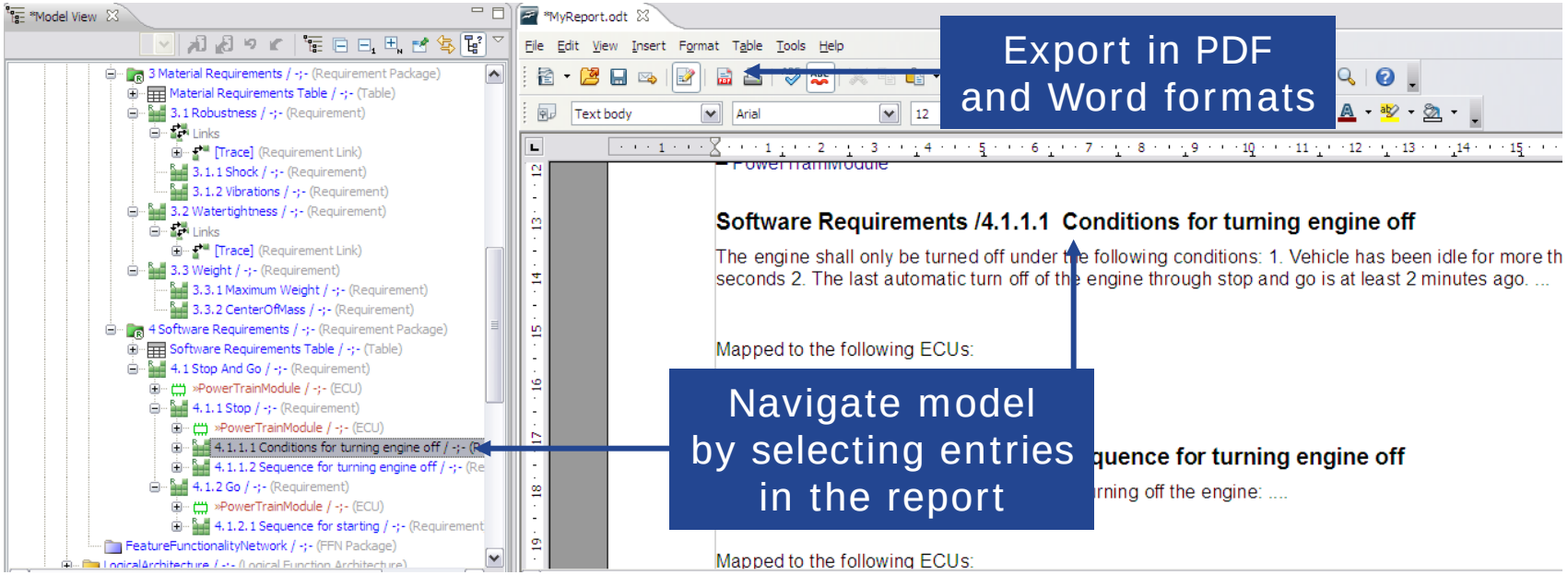
- Requirements, Requirements Packages and Timings can be reused in a number of contexts.
- Changes in the description are copied across all reuses.
- Reuse can be used to efficiently manage different groupings of the same requirements, e.g. for different suppliers.

Requirements and Variant Management



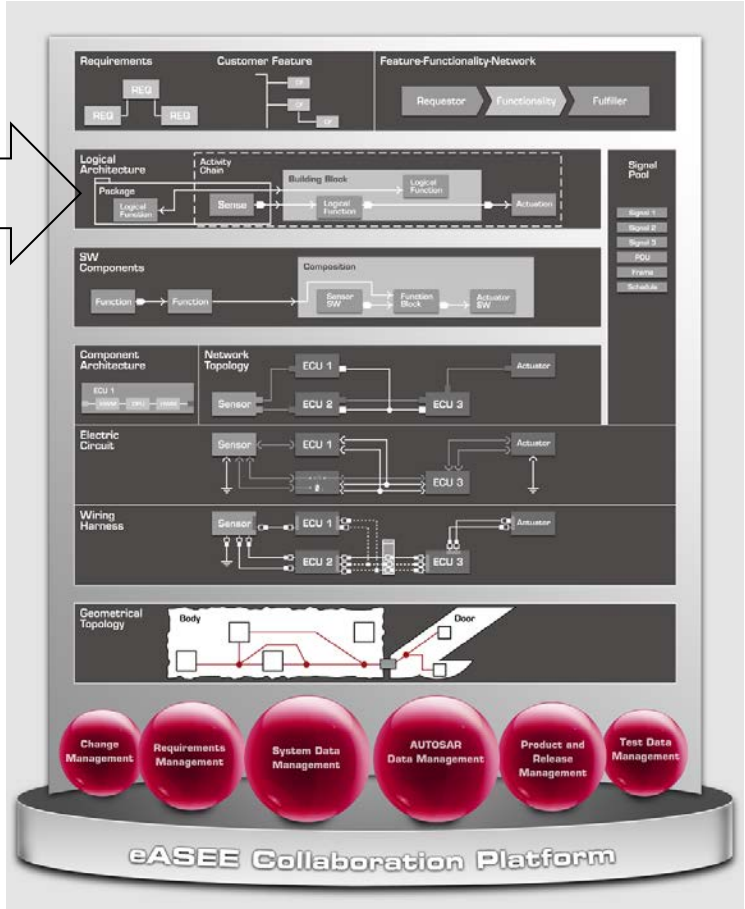
- Requirements can be allocated to sets and alternatives defined in the variant model.
- Requirements not allocated to the current selected variant are indicated in the model tree ( )
- Can be used to manage variant-specific requirements.

Report Generation



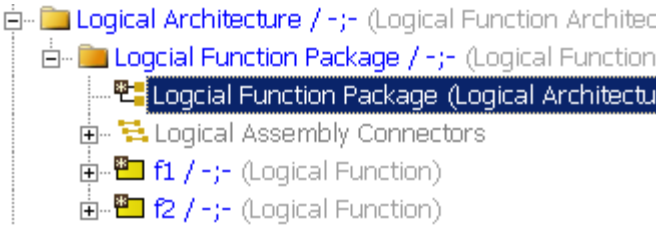
- Reports can be generated based on user defined templates.
- High level of flexibility in the report format including the use of tables, diagrams and complex model queries.
- Generation of variant-specific reports possible (e.g. to create supplier specific specifications in PDF).

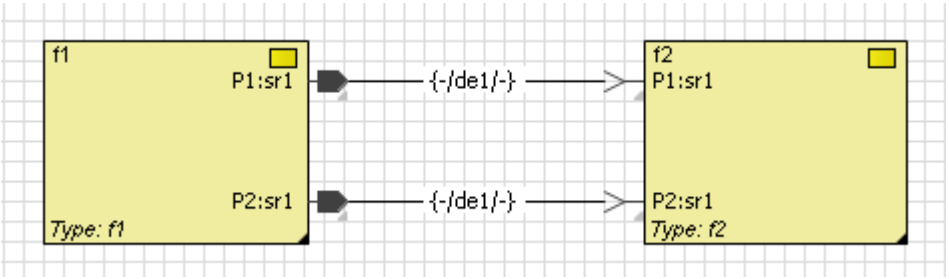
Logische Architektur
SW Architektur



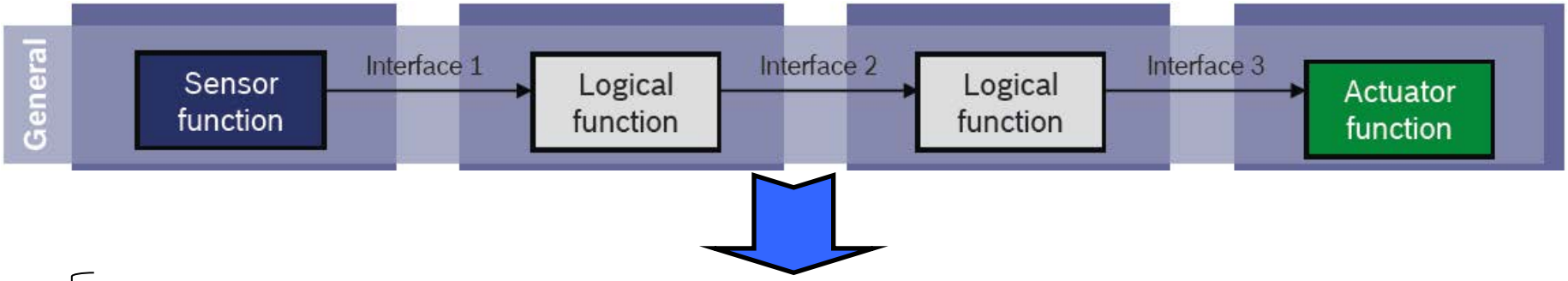
Logical Architecture

- The network communication specification for distributed systems is typically driven by the Logical Architecture and its mapping to the Hardware Architecture
- The Logical Architecture specification is supported by graphical block diagrams
- The communication between logical functions in the Logical Architecture is specified by ports and connections (in a similar way as AUTOSAR)



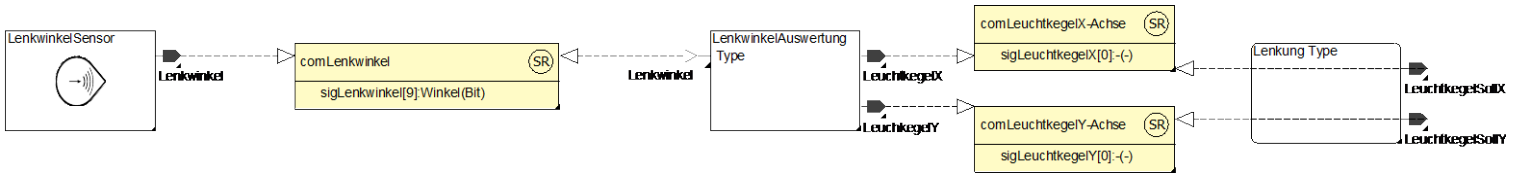


Funktionsmodellierung → SW Architektur

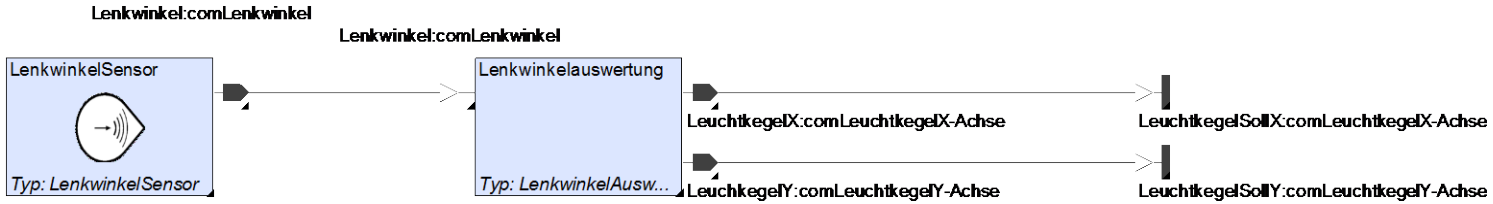


SW

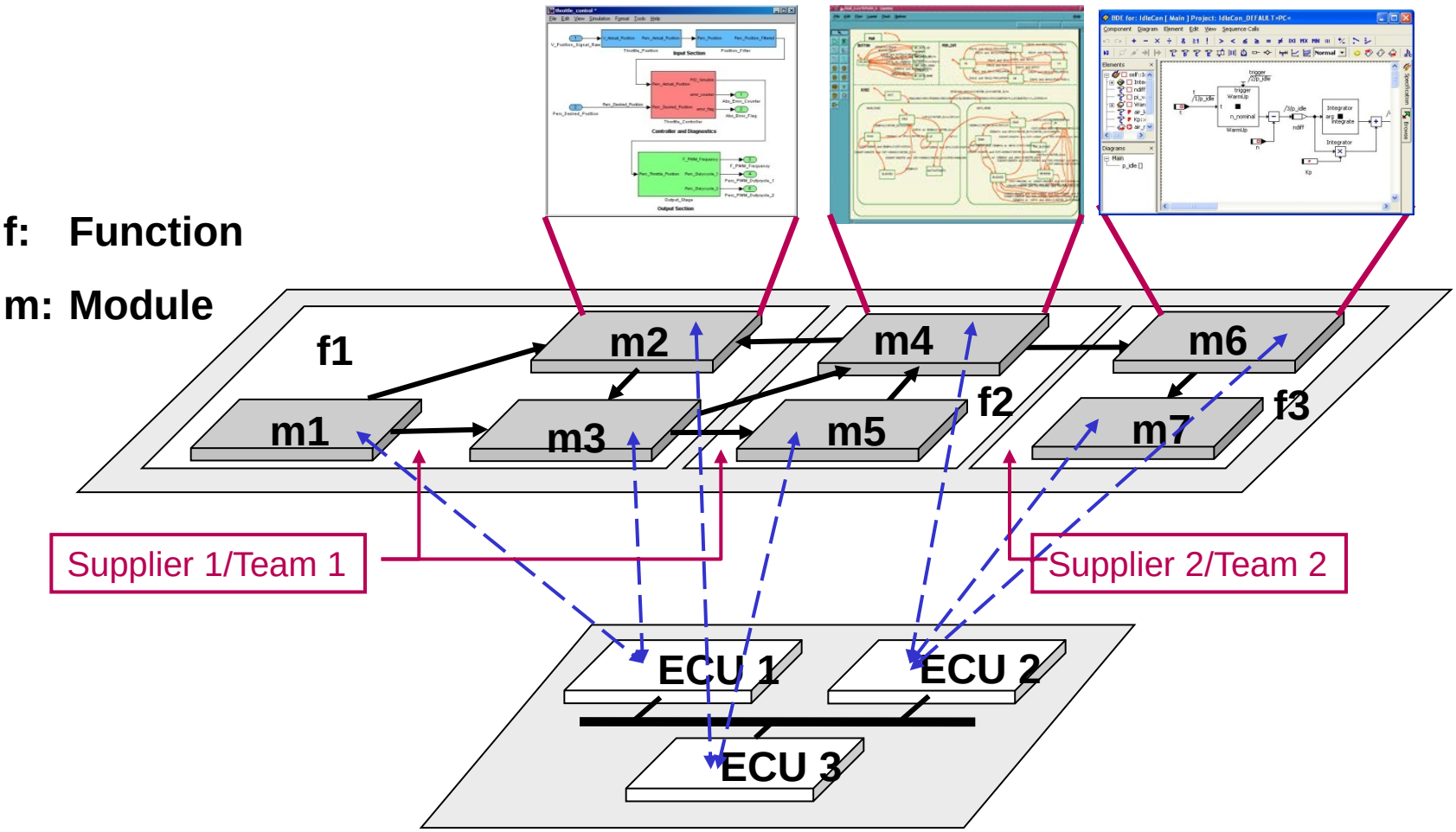
Funktionstyp, Schnittstelle, Datenbeschreibung



Hierarchische SW Architektur, Signale



Function Oriented System Development



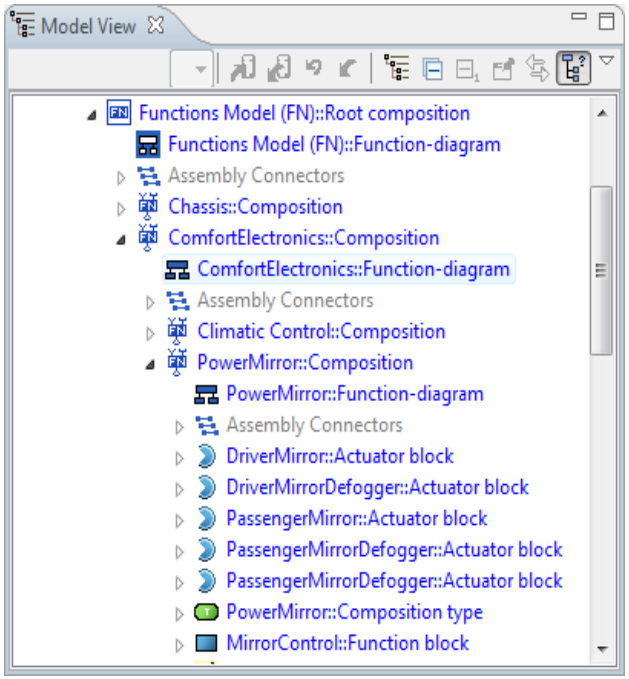
Function / Function Network Layer (1)

Function Layer / Function Network Layer (FN)

- Defines the Software Architecture
- Function Blocks as Software Component
- Logical Sensors & Logical Actuators
- Compositional Hierarchy
- All Elements have corresponding types
- Graphical Busses, Model Refactorings

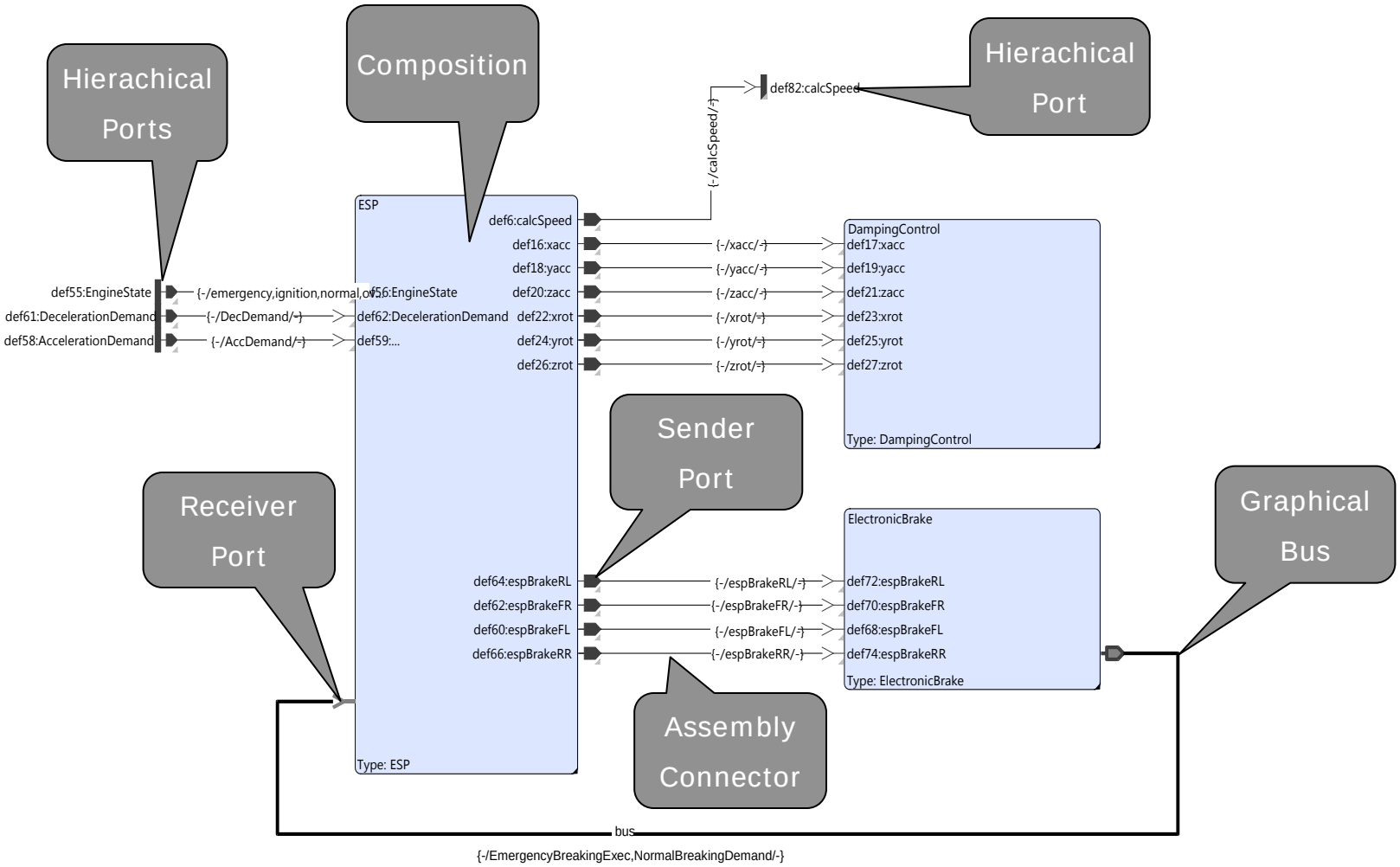
Function Types

- Specify the structure of FN Components
- Ports with different communication styles
  - Send/Receive, Client/Server, Slave/Controller
- Ports are assigned to Interfaces
- Interface specify the the communication protocol
  - Interface contain data elements

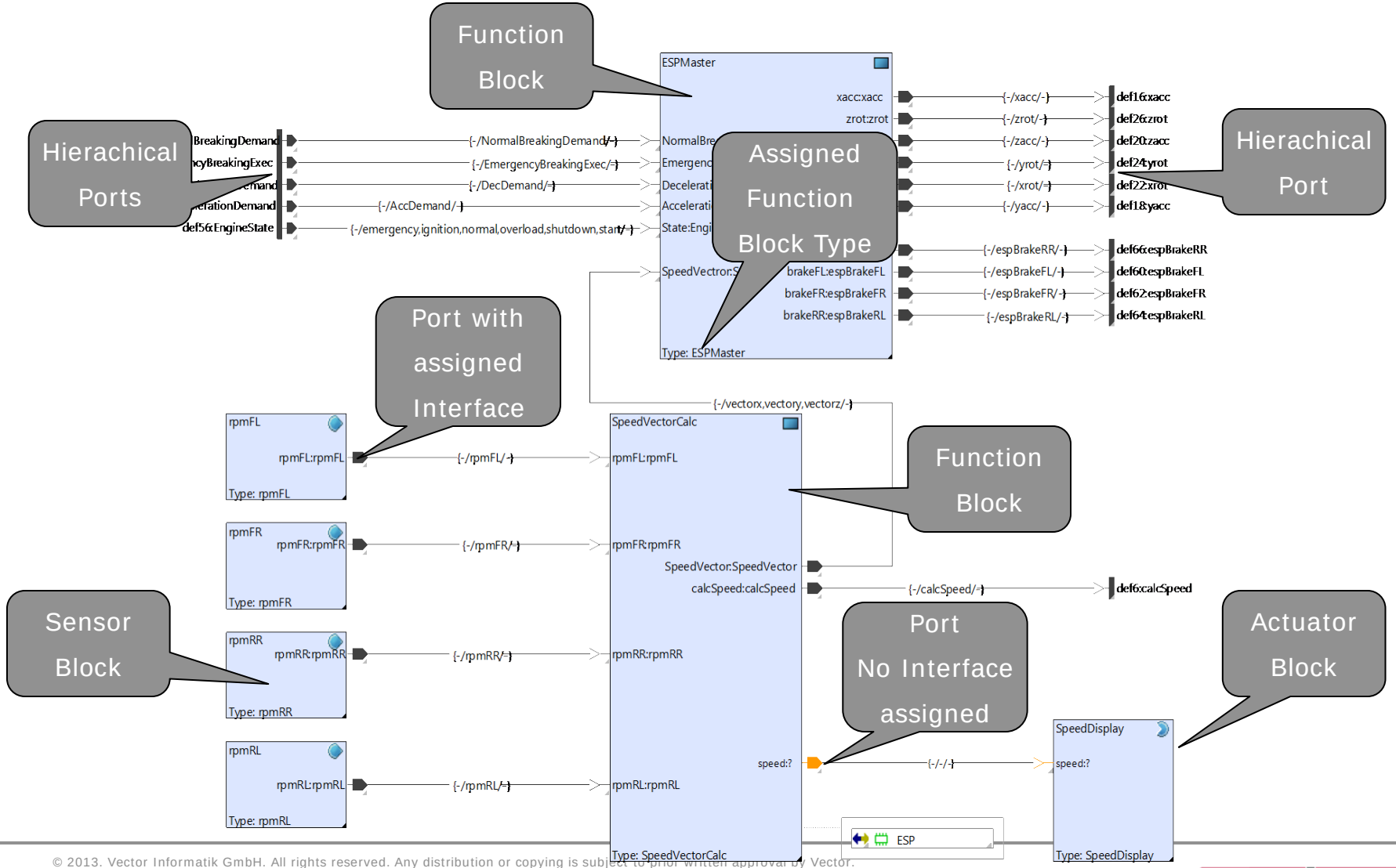


Modelview Hierachy / Block Level

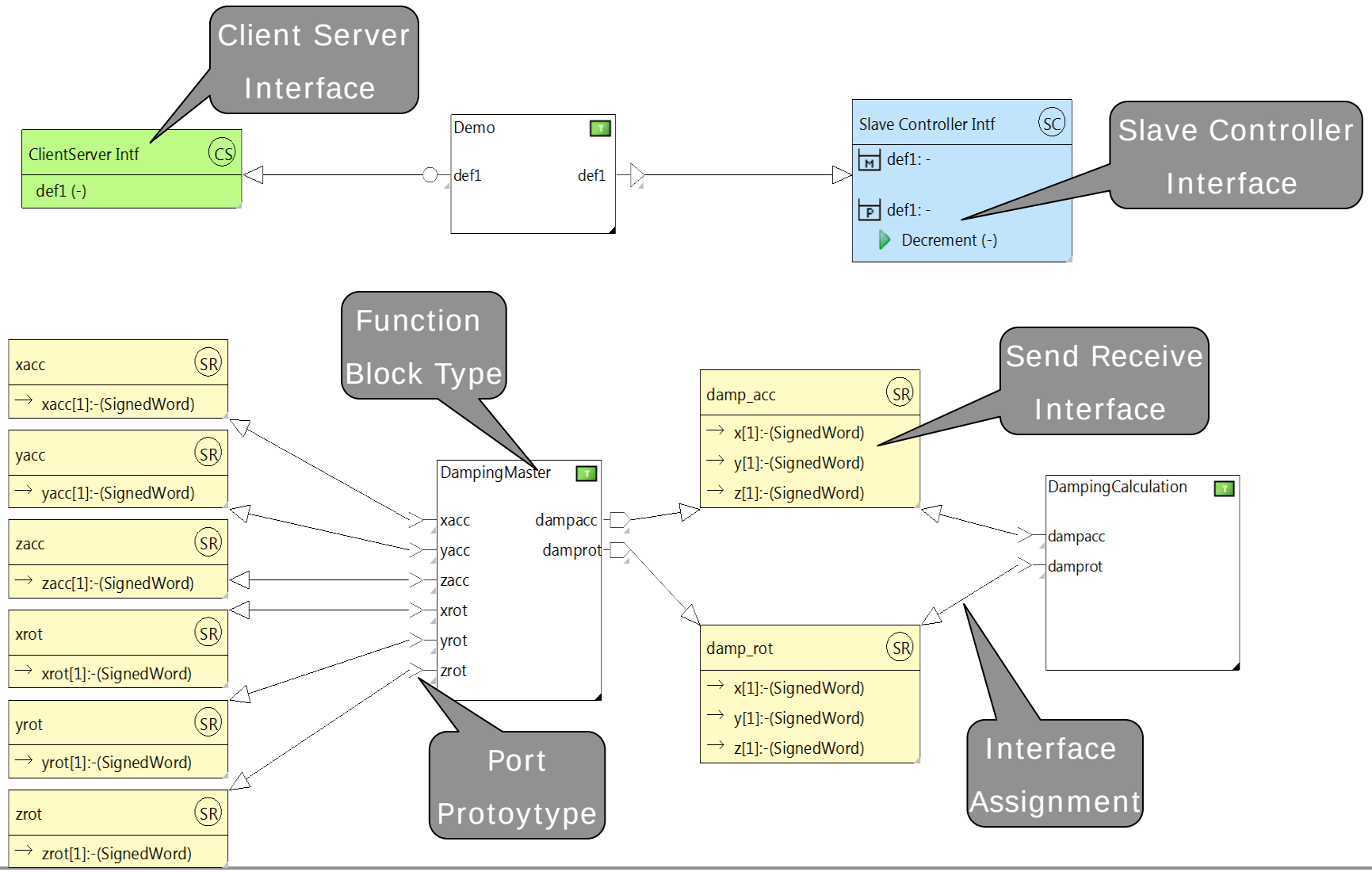
Function / Function Network Layer (2)



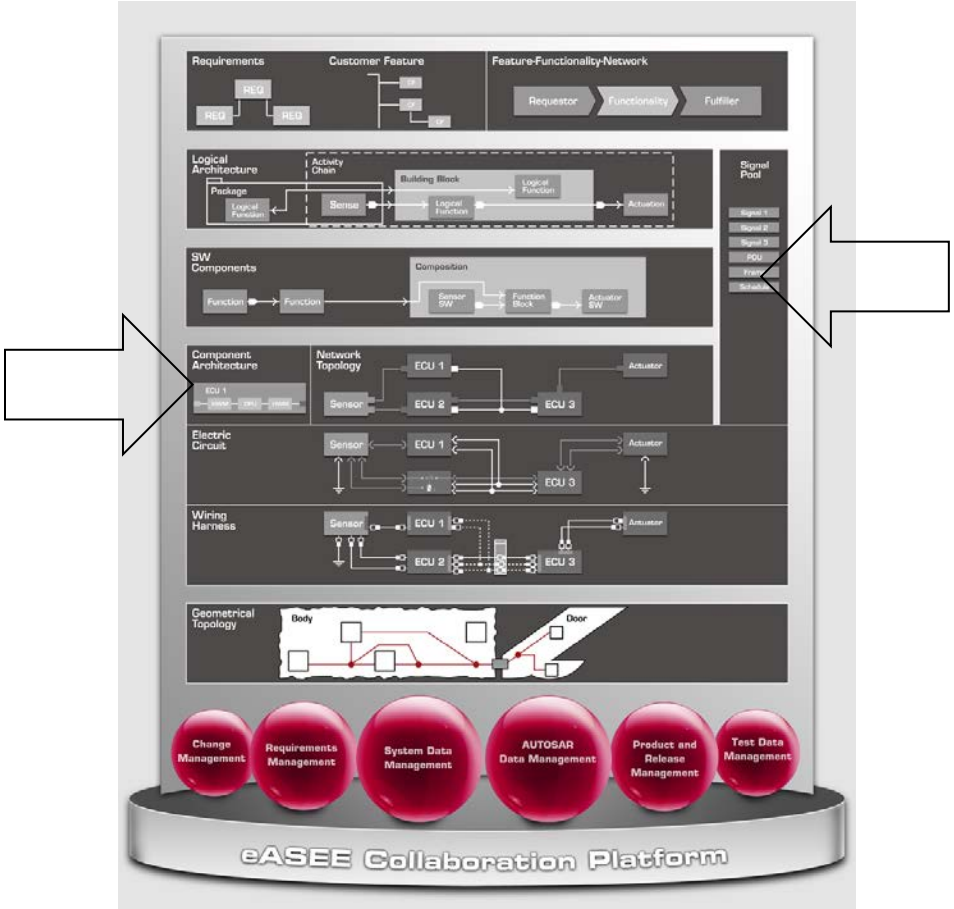
Function / Function Network Layer (3)



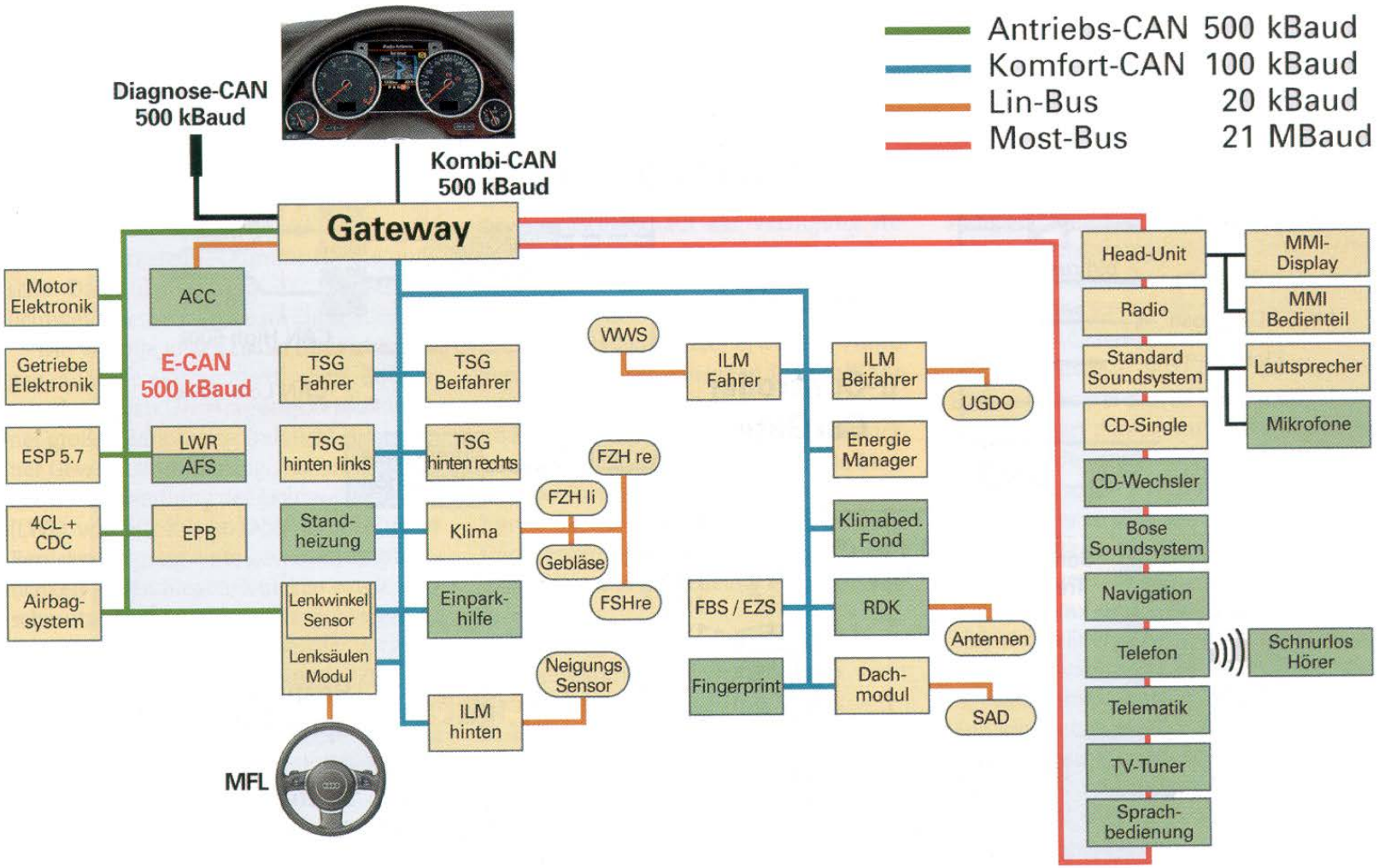
Function / Function Network Layer (4)



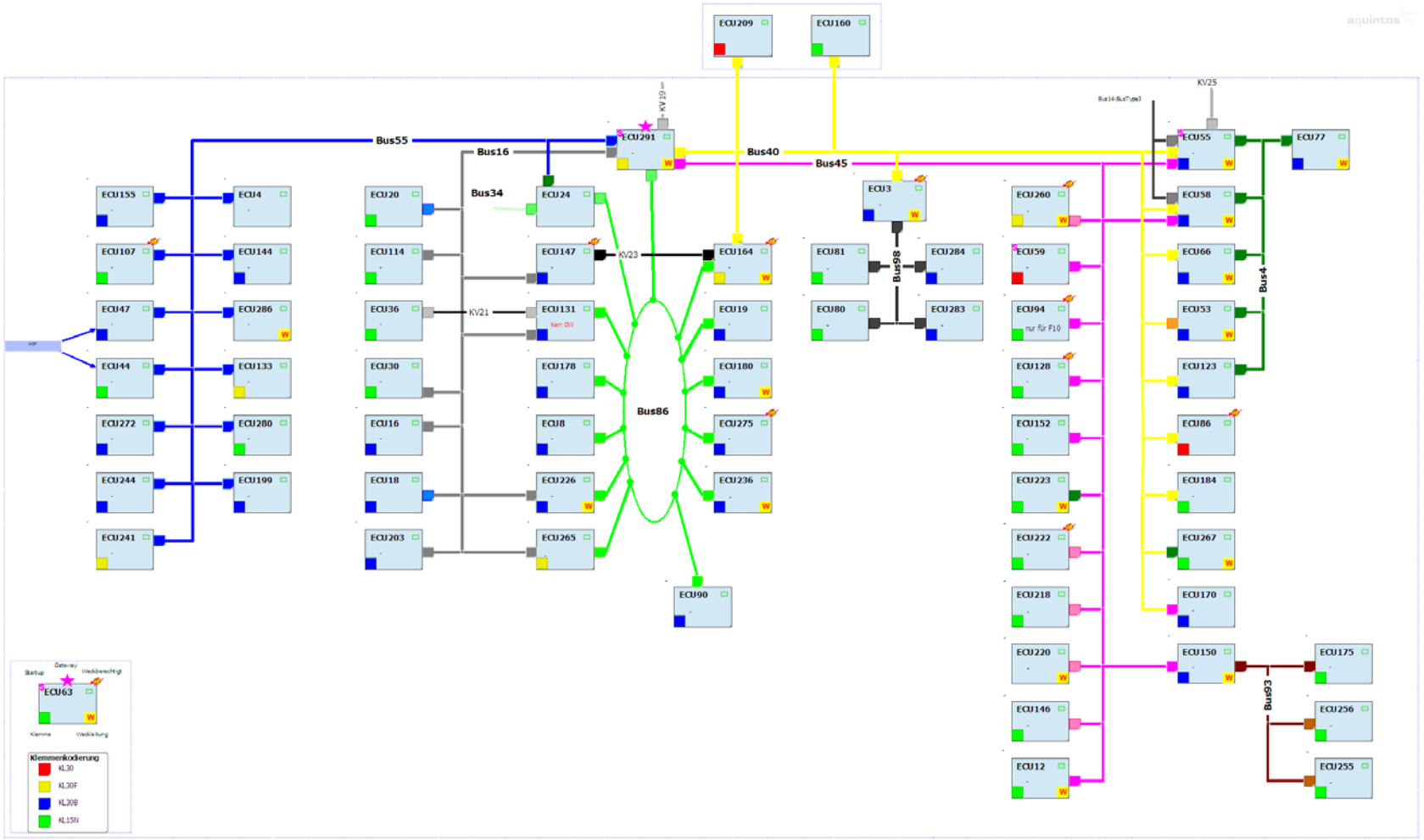
Vernetzungs-Architektur



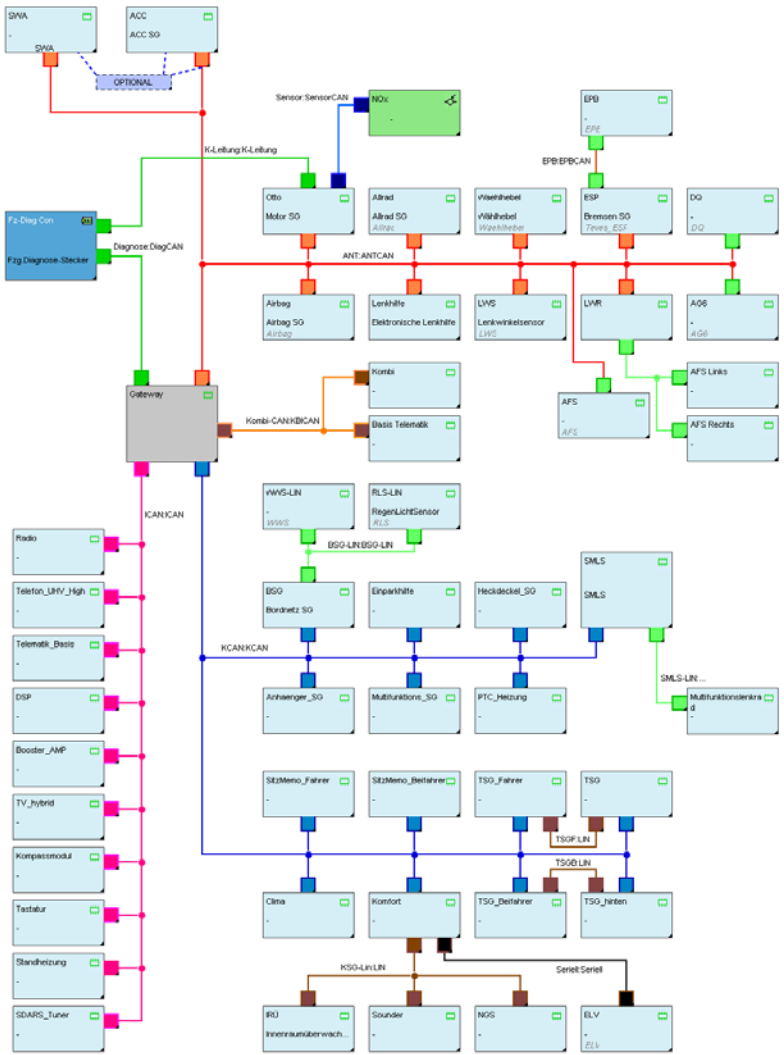
Kommunikationsarchitektur Audi A8



Network Overview



Typisches Vernetzungskonzept PKW



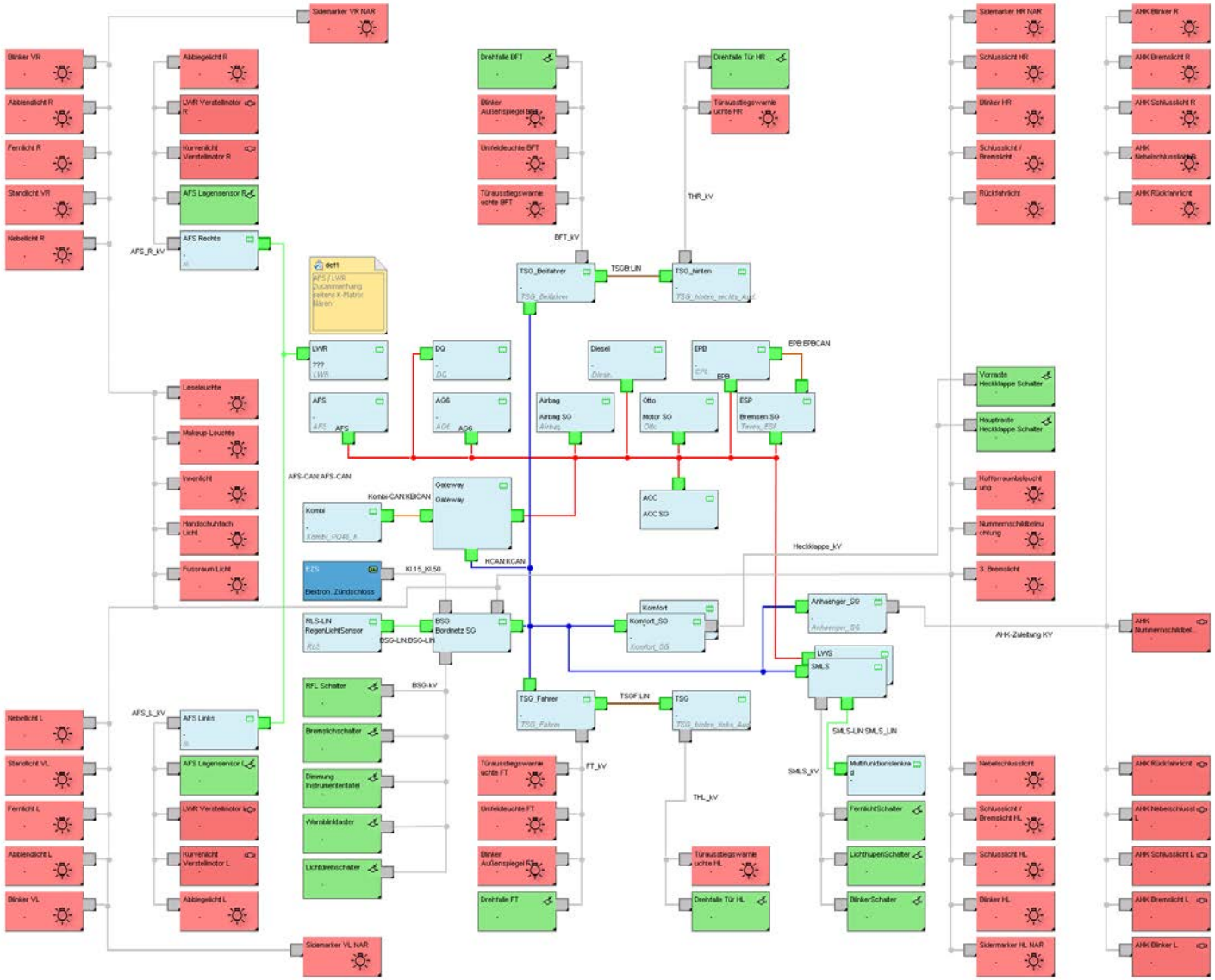
E/E-Architekturen im Kfz werden meistens in die folgenden Domänen unterteilt:

- Antriebsstrang
- Komfort (Innenraum)
- Chassis
- Telematik oder Infotainment

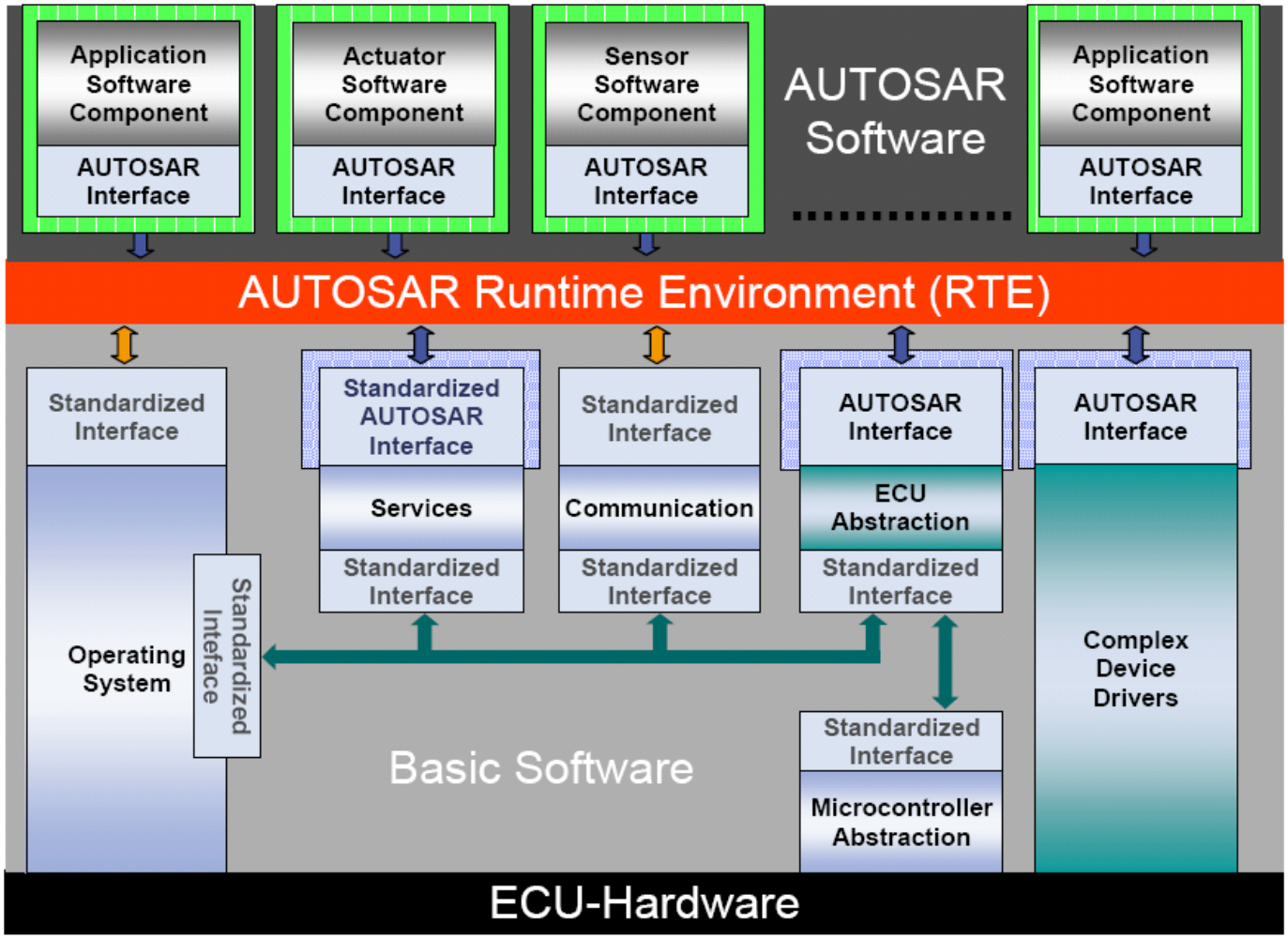
Das E/E-System eines Fahrzeugs ist stark verteilt. Die Kommunikation der Systeme erfolgt über standardisierte Bussysteme (CAN, LIN, MOST, FlexRay).

Der modellbasierte Architekturentwurf unterstützt den Entwurfsprozess stark verteilter Elektroniksysteme und erlaubt eine Optimierung z.B. nach Kosten, Gewicht, Bauraumbedarf etc.

Typischer Aufbau eines Lichtsystems im PKW



AUTOSAR (ECU and Software)



The software component template describes these components completely

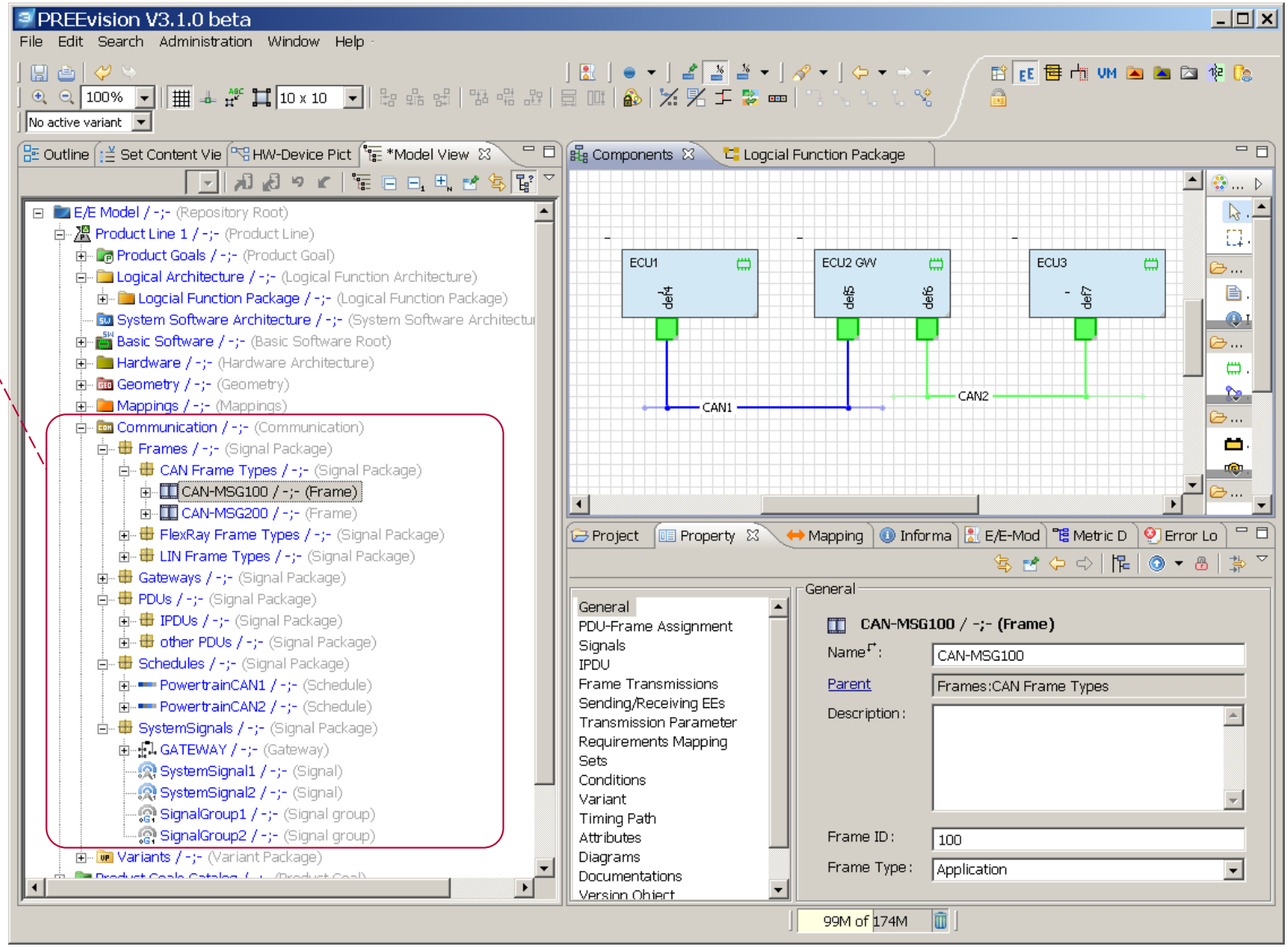
Of these software components only the AUTOSAR Interface side can be fully described in the software component template

Figure 3: Scope of this document in the ECU SW Architecture

Communication Layer in PREEvision

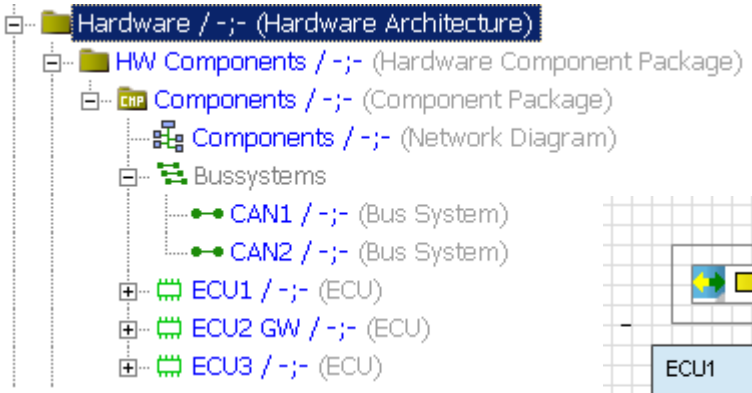
Communication Layer to specify

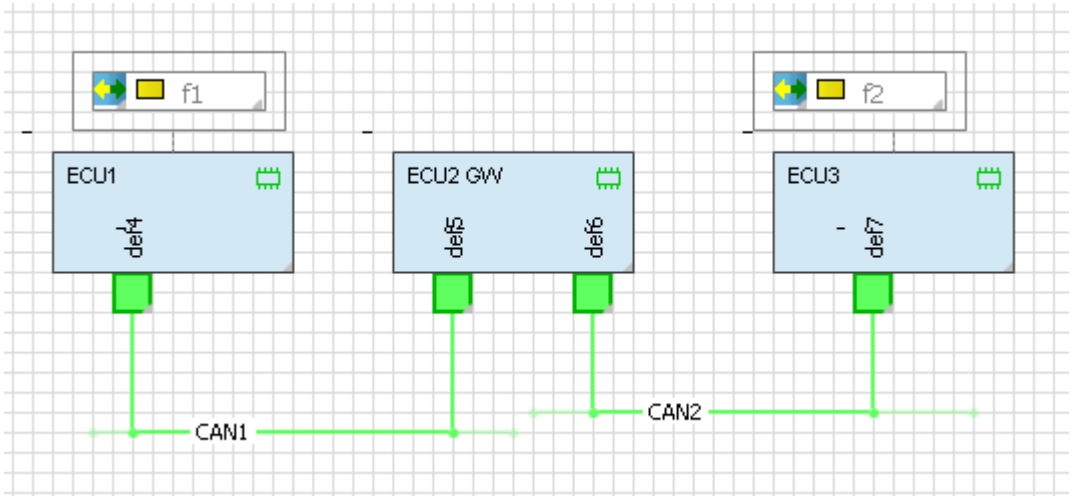
- Signals,
- PDUs,
- Frames, and
- Schedules.



Hardware Architecture

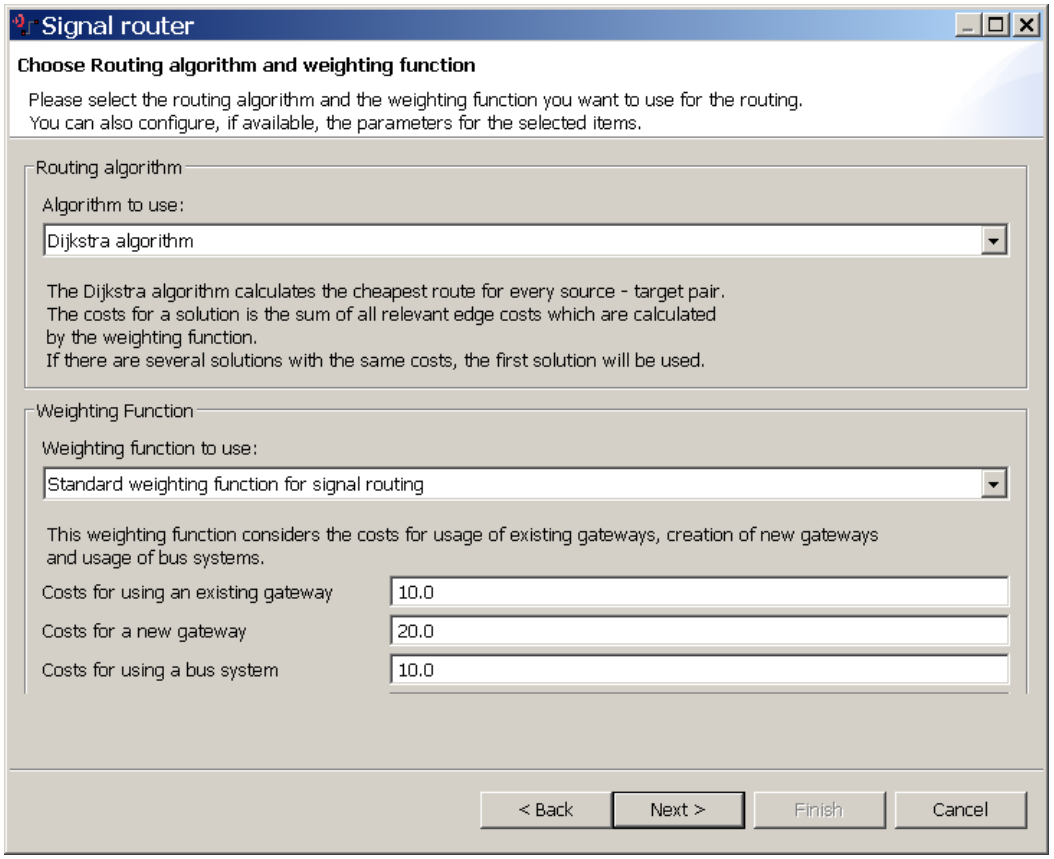
- The Hardware Architecture specification is also supported by graphical block diagrams.
- The mapping of logical functions can be displayed directly in the graphics, shown over the ECU block





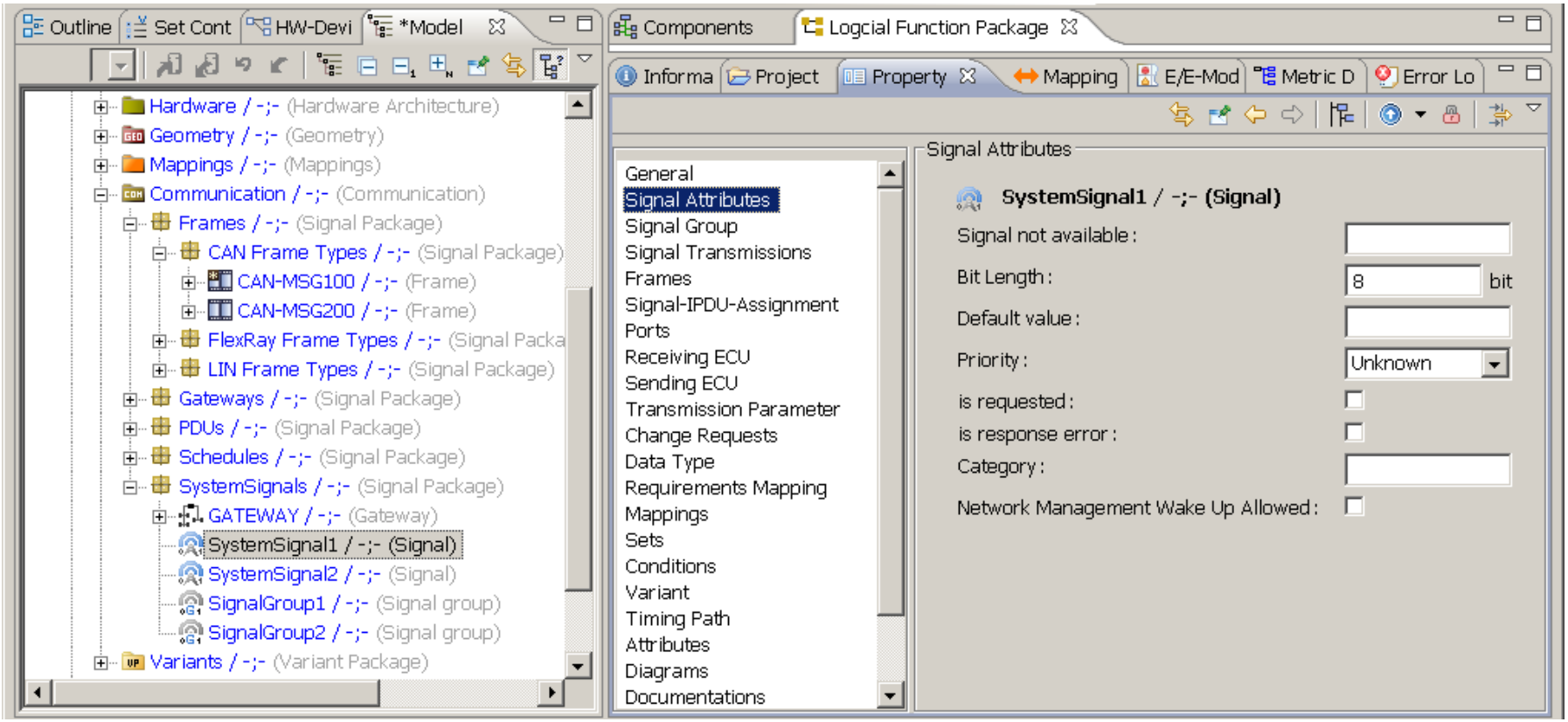
Signal Routing

- Based on these information the integrated PREEvision Signal Router calculates for the sender-receiver communication
  - System signals
  - System signal mappings
  - Signal routings for all signals, which need to be communicated in the network



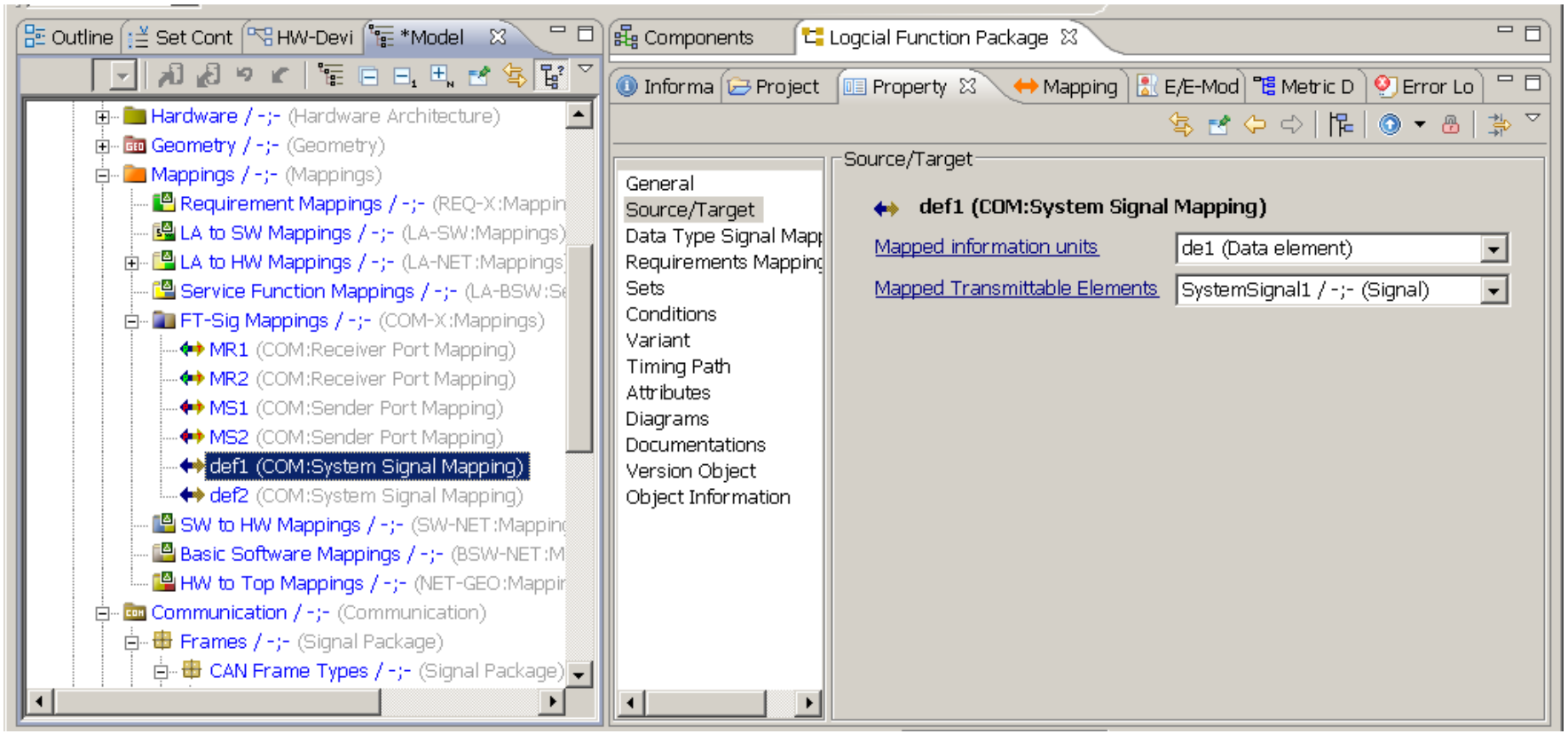
System Signal Specification

The specification of System Signals can be done by the Property Editor...



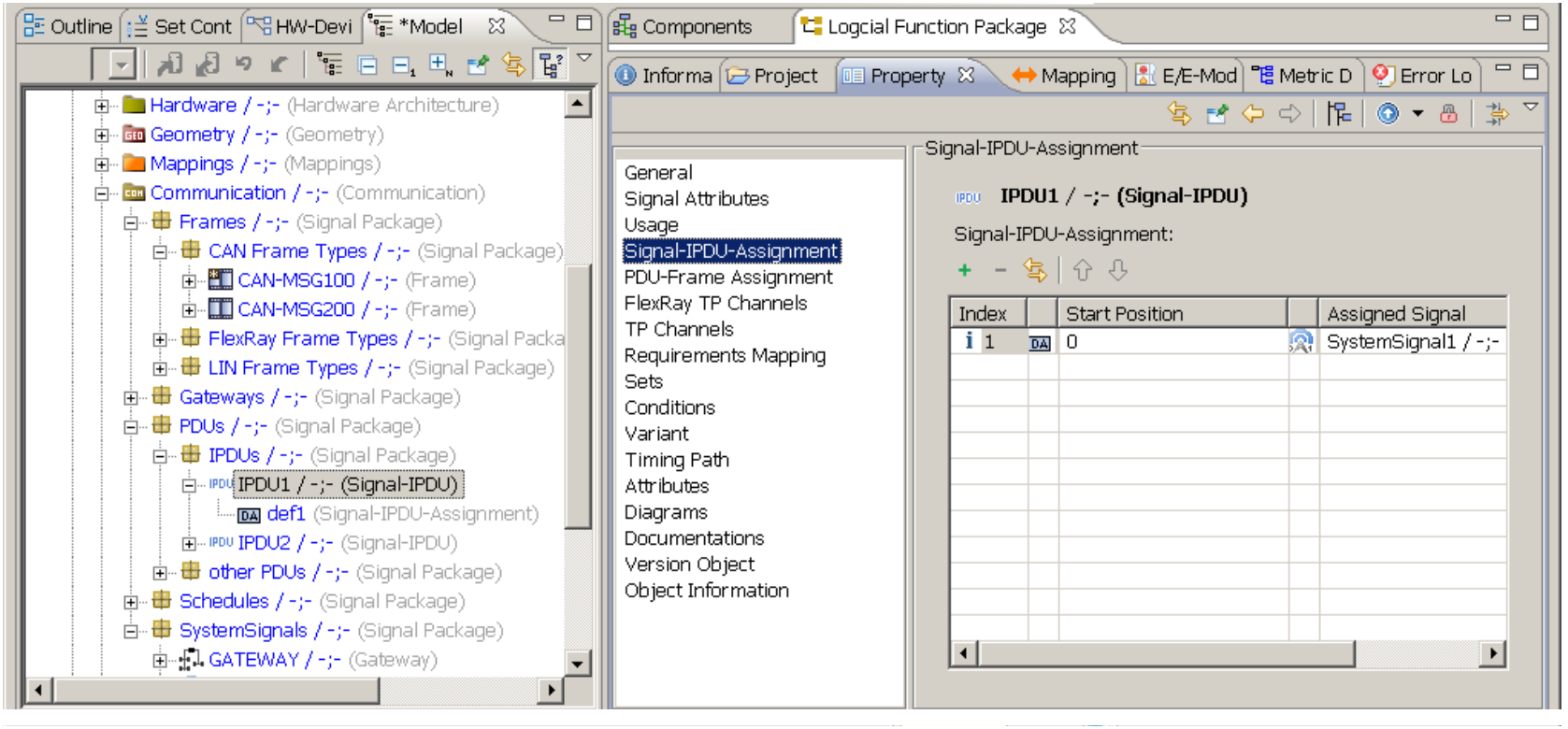
System Signal Mapping

... as well as for the System Signal Mapping



PDU Specification

PDUs are specified interactively based on System Signals

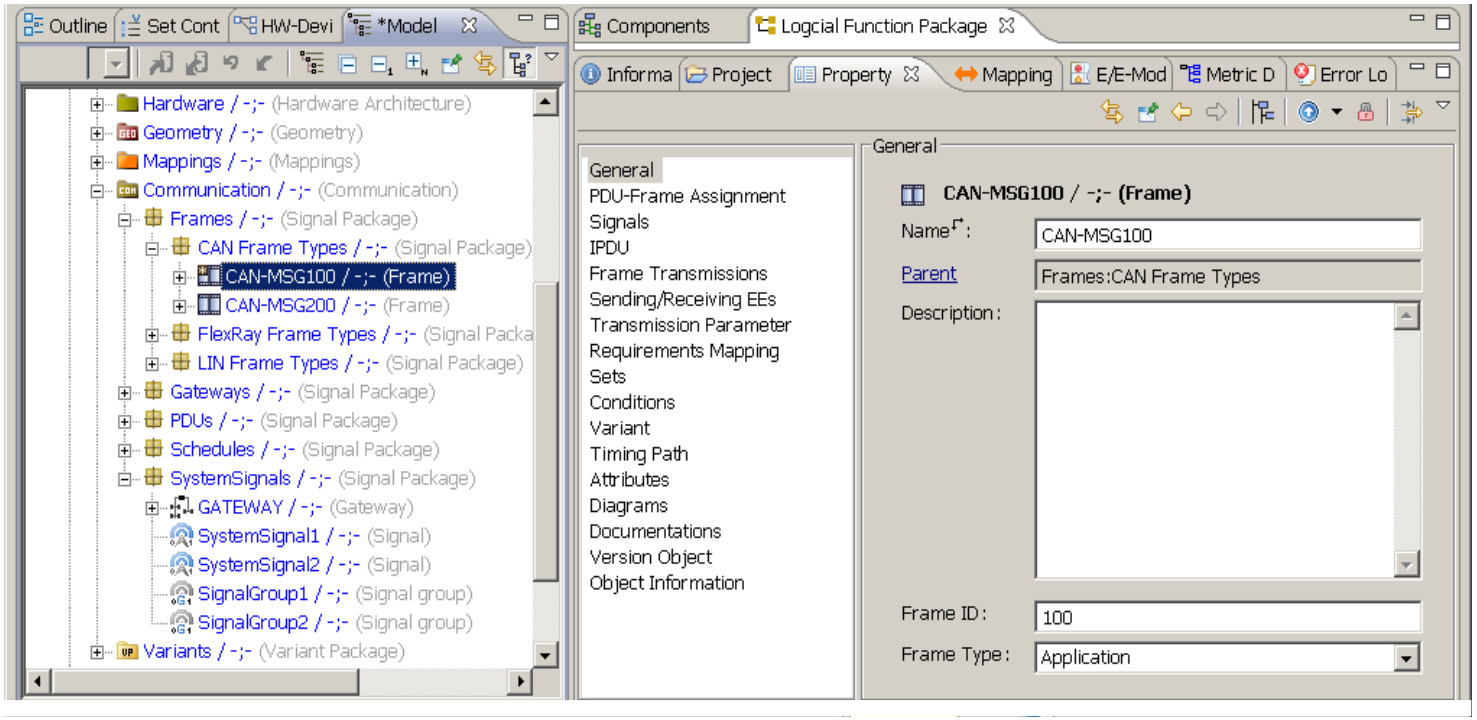


PDU: Protocol-Data-Unit

Frame Specification

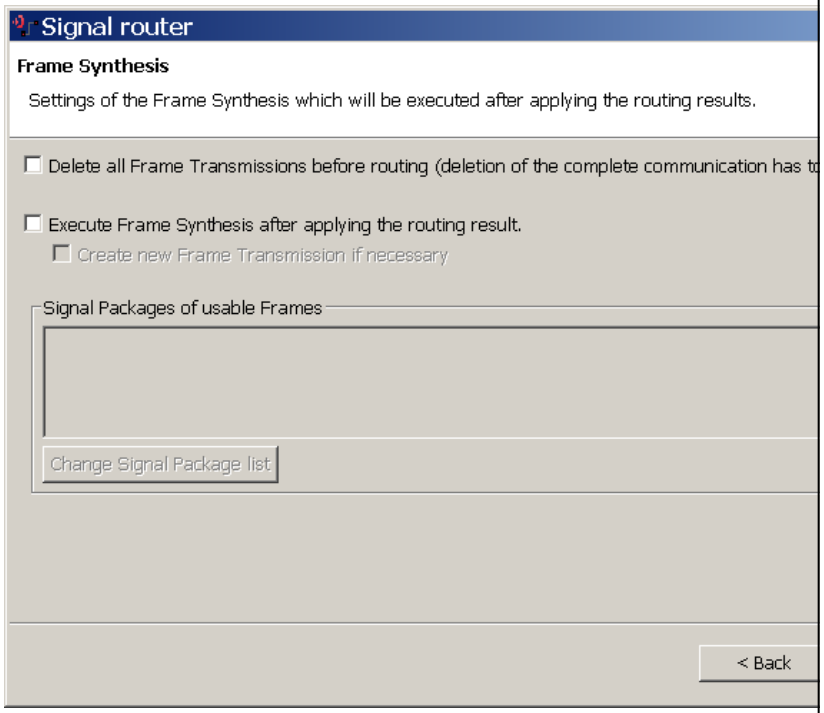
Frames are specified interactively based on PDUs and are available for

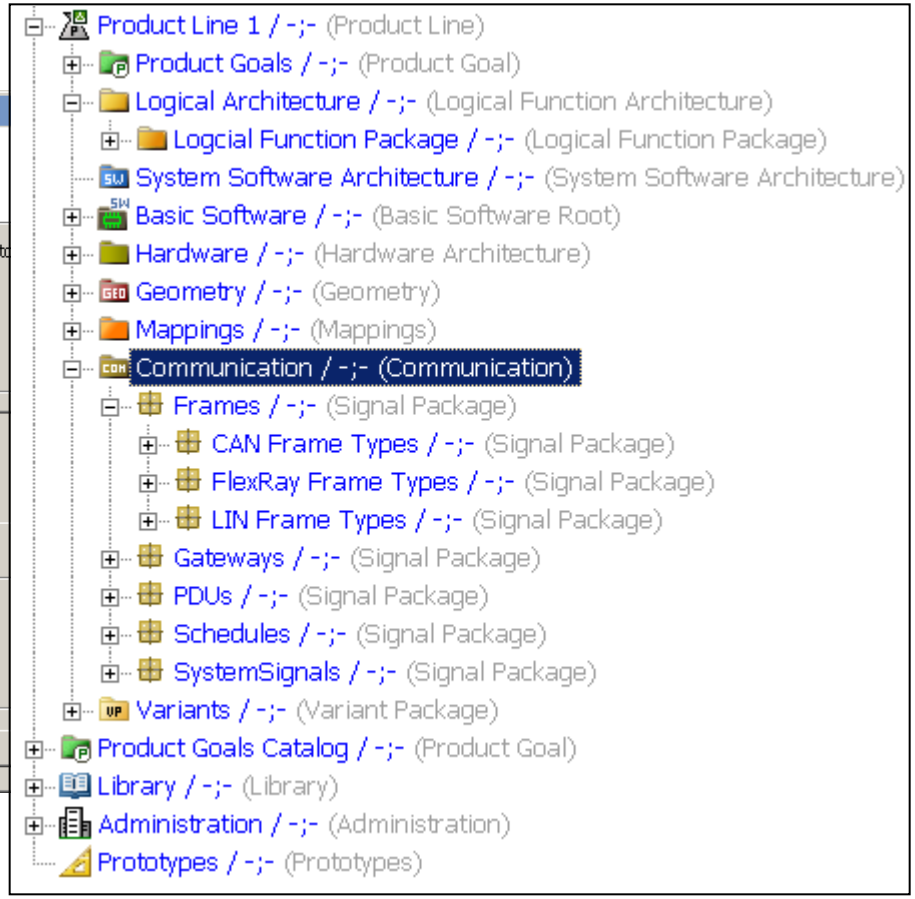
- CAN
- LIN
- FlexRay



Frame Synthesis

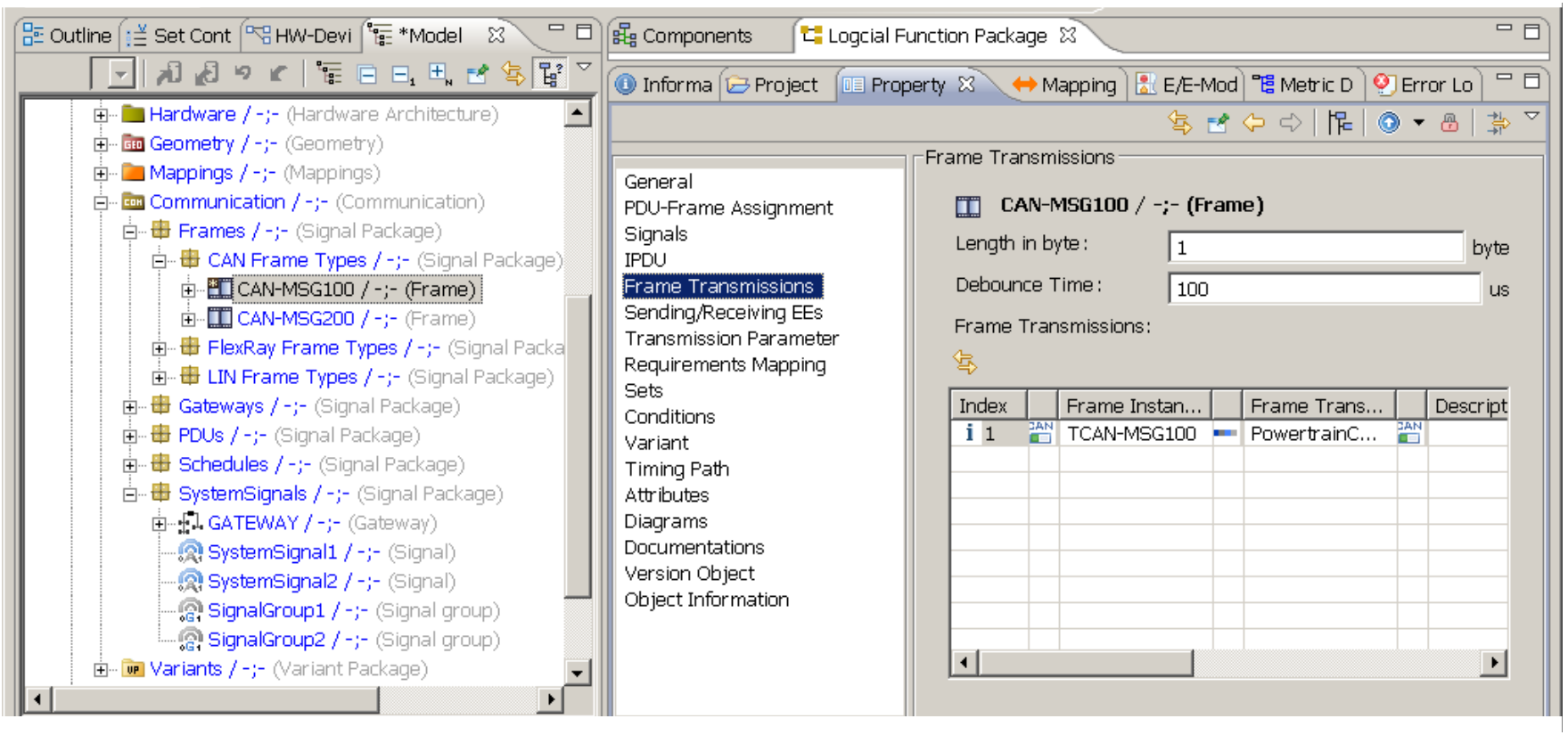
The Frame Synthesis generates a schedule for FlexRay or frame transmissions for CAN and LIN using predefined frames





Communication Layer in PREEvision

Schedule Specification - Frame Transmissions



Generated routing results of the frame transmissions

Aufbau eines Steuergerätes (Komponenteneditor)

Aufbau einer ECU

- CPU, FPGA, RAM, etc.
- Gatewaystruktur

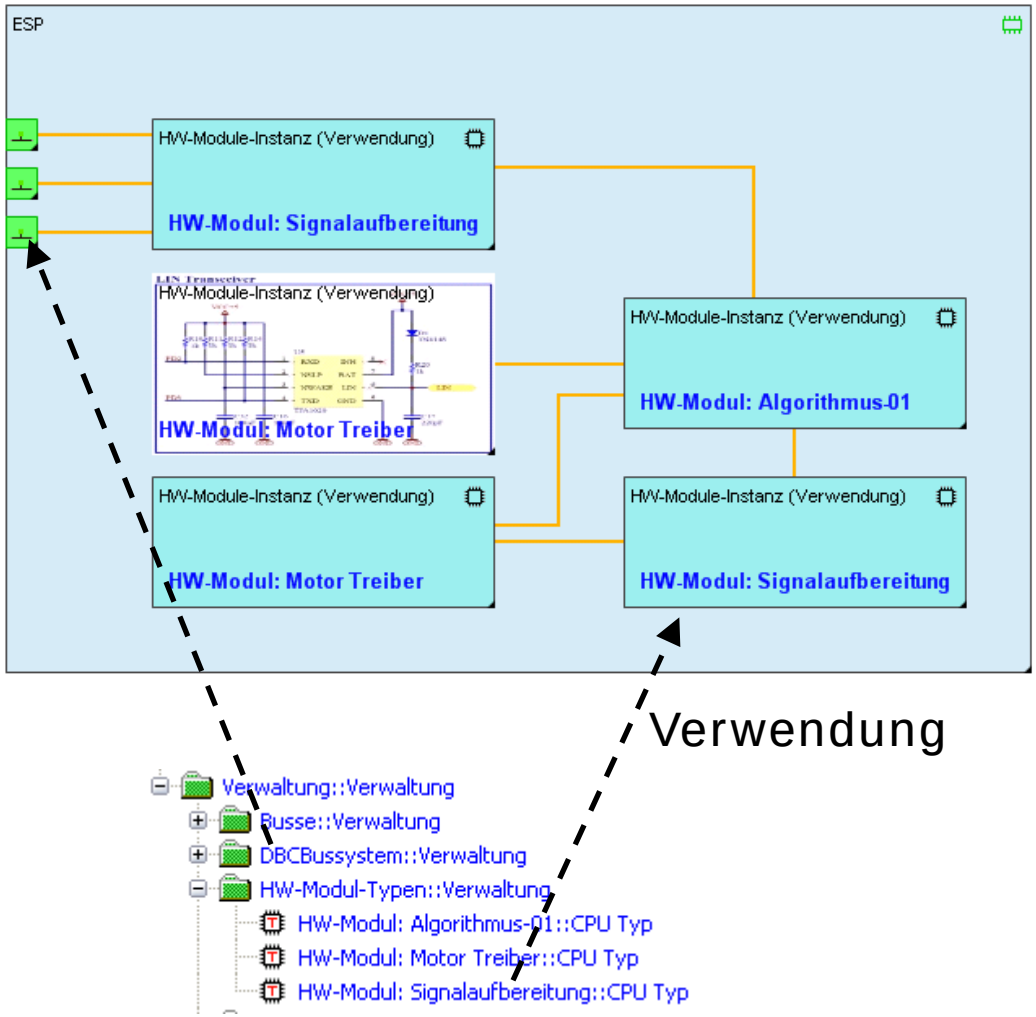
Kommunikation zwischen Busanbindung und CPU

HW-Modulmodellierung: Aus Zulieferer Sicht

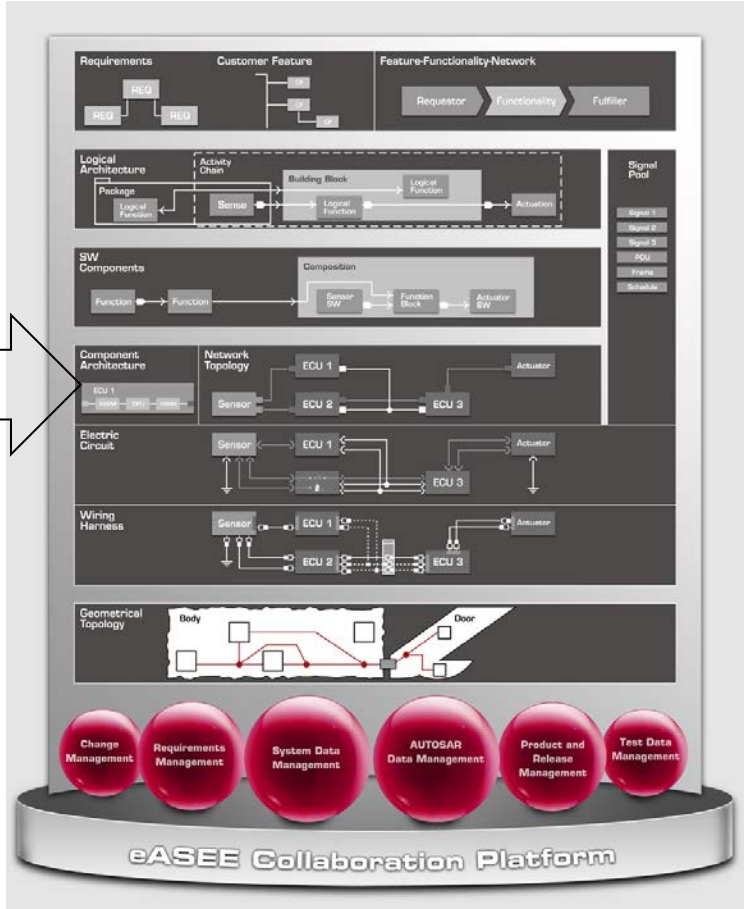
HW Modul zur Verwendung
HW Modul als Bibliothek
Attribute eines HW Moduls:

- Stückliste
  - Bauteilbezeichner
  - Teilenummer
  - Gehäuse
  - Fläche
  - Anzahl
  - Einzelkosten (aus DB) Import
  - Bild
- Kommulierte Attribute
  - Kosten
  - Fläche (aus Bauform, Overhead Anteil, offset)
  - Gewicht

Finden von HW-Modulen (#300-500)



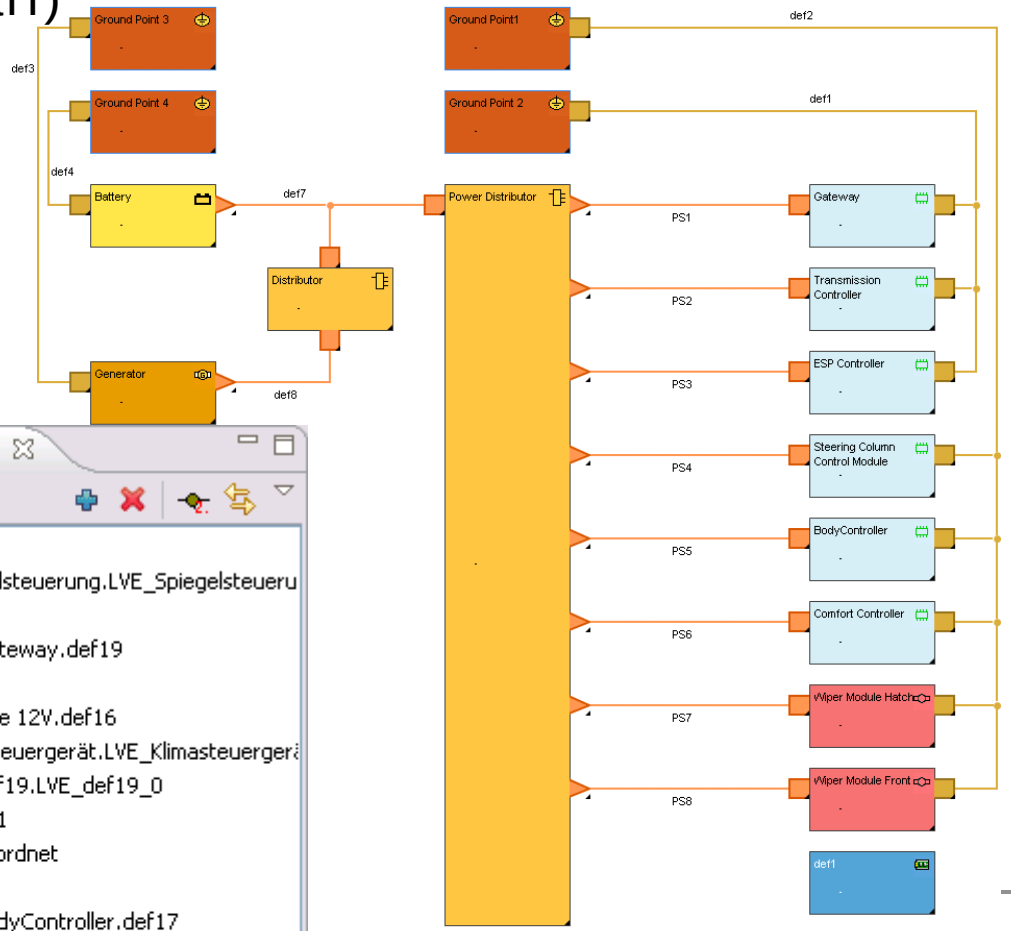
Leitstungsversorgungs-Architektur

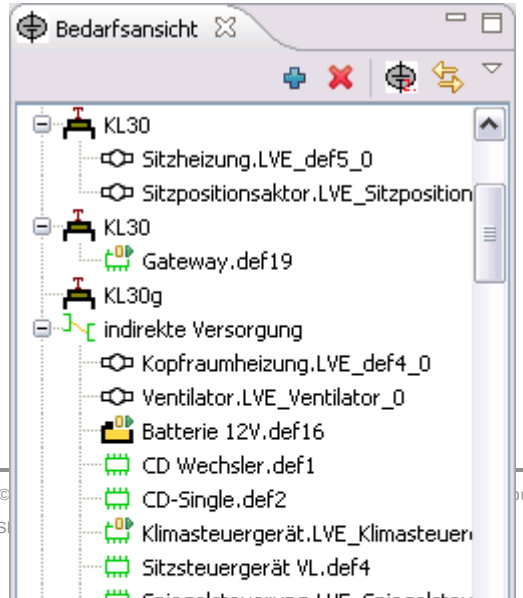


Stromversorgung

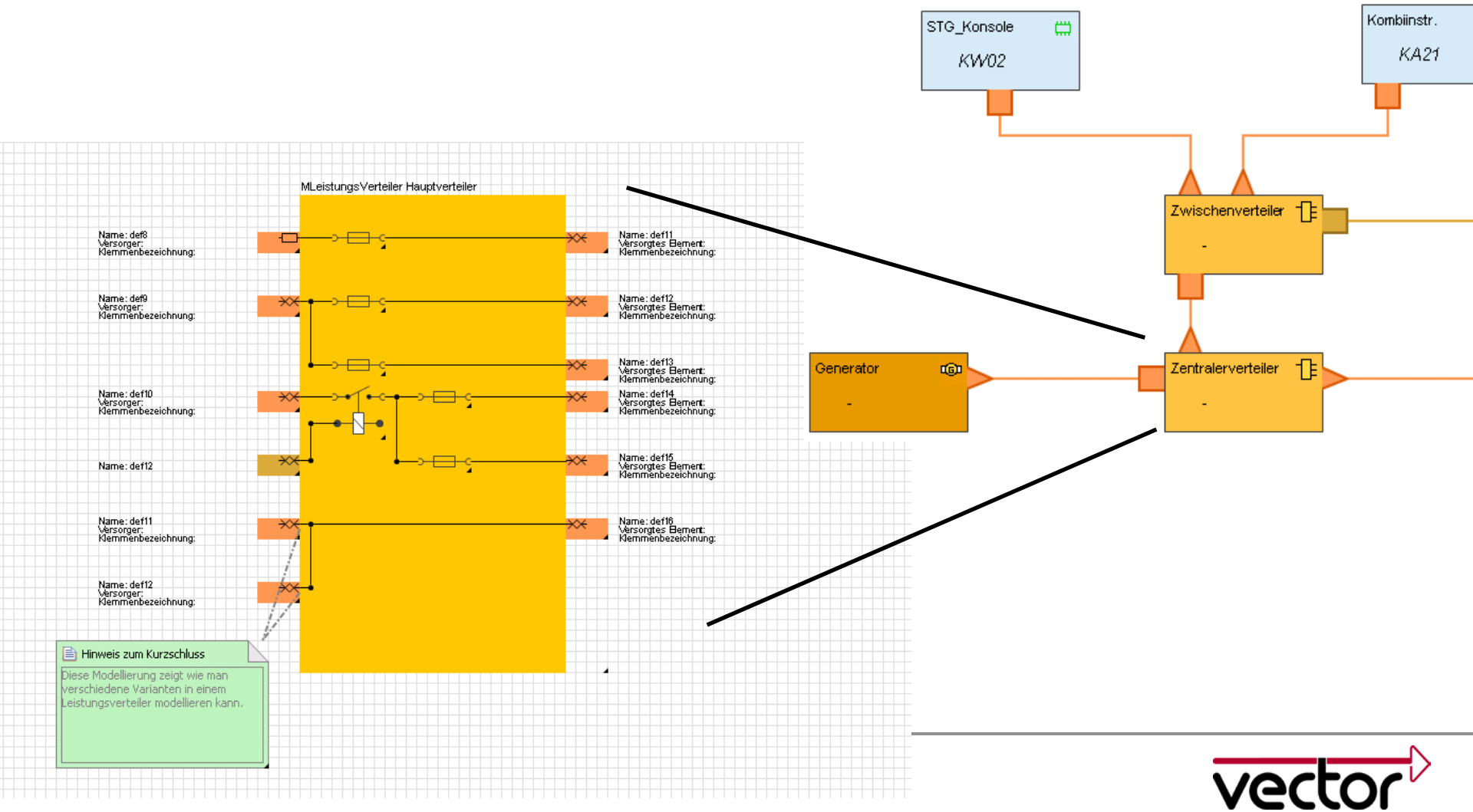
Schnelle Erstellung der Stomverteilungsmodellierung durch 2 Ansichten:

- Bedarfsansicht (Klemmenbedarf)
- Verteilungsansicht

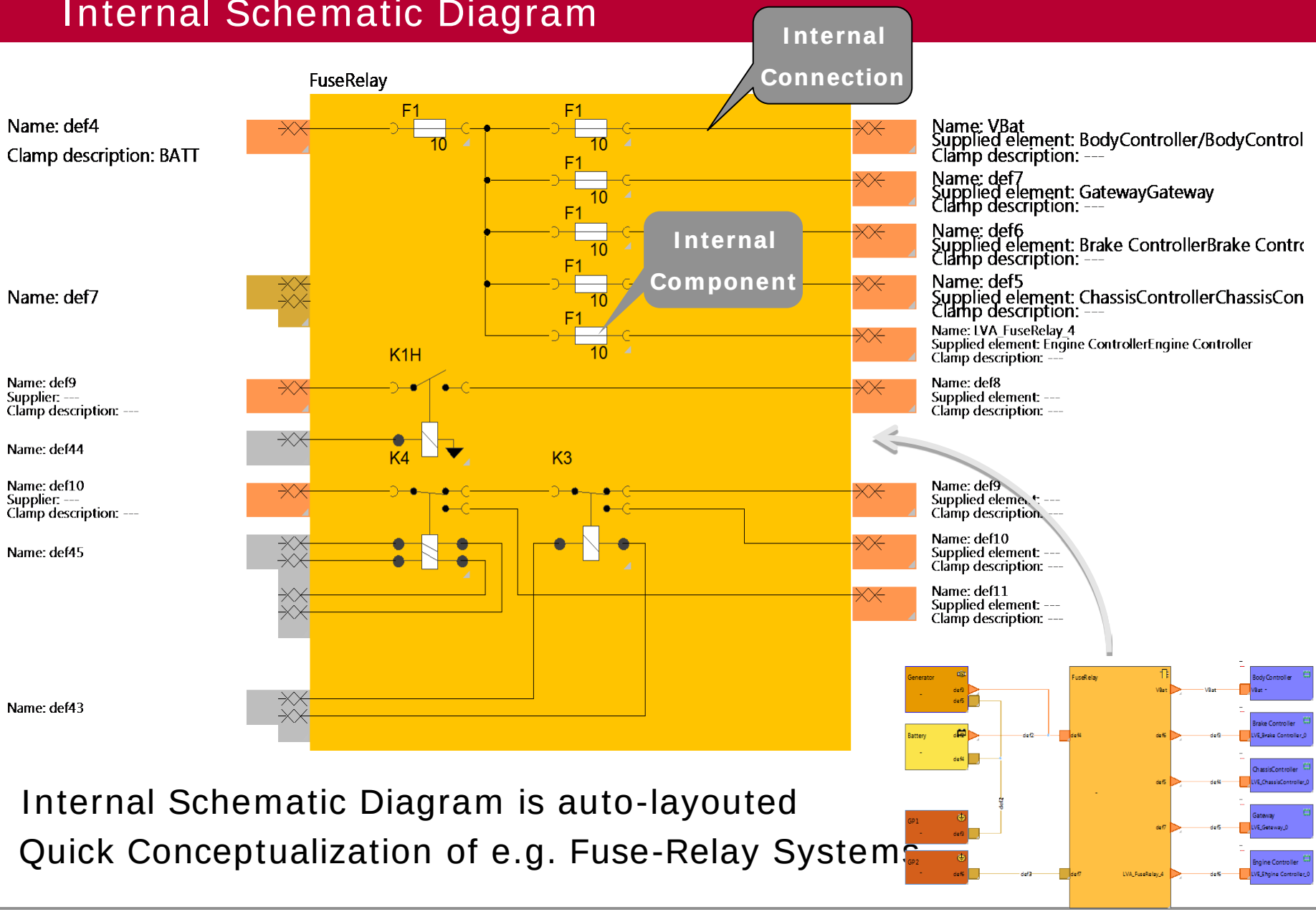




- Spezifikation von Sicherungen und Relais



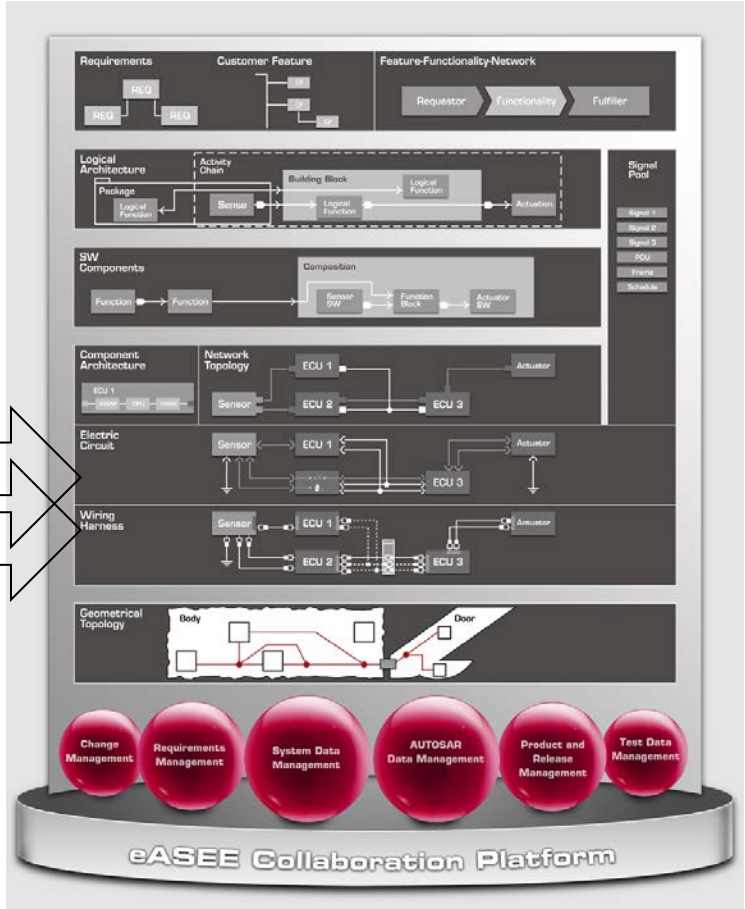
Internal Schematic Diagram



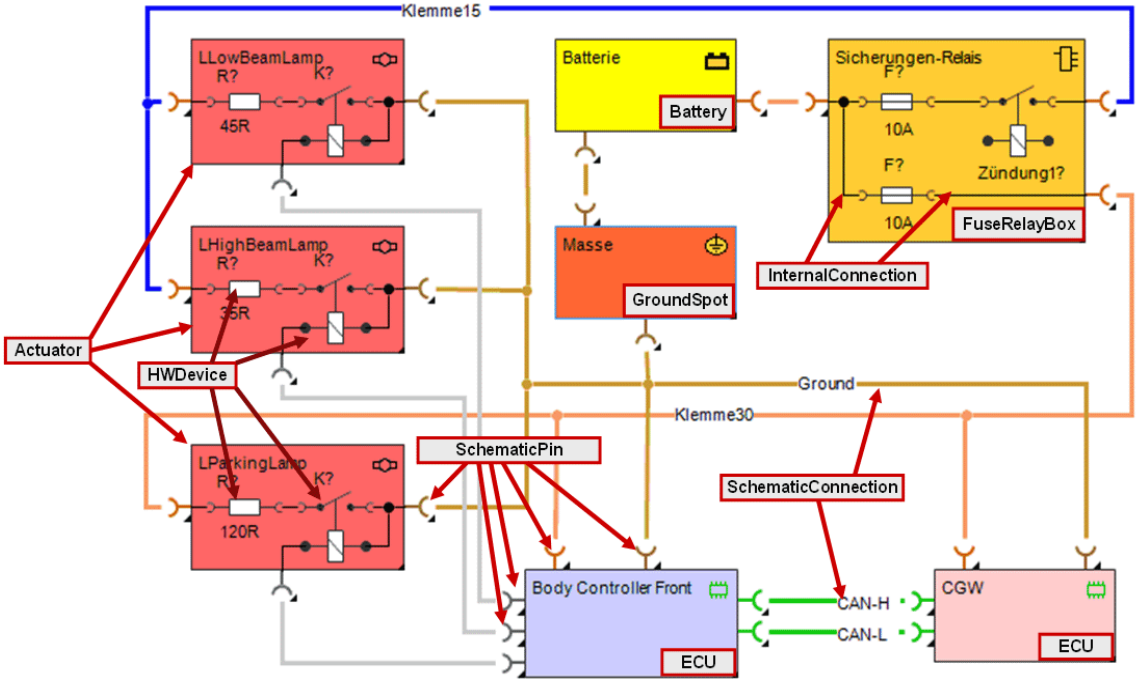
Internal Schematic Diagram is auto-layouted

Quick Conceptualization of e.g. Fuse-Relay Systems

Stromlaufplan Leitungssatz (Elektrik)



Stromlaufplan



Darstellung der elektrischen Verbindungen zwischen Komponenten

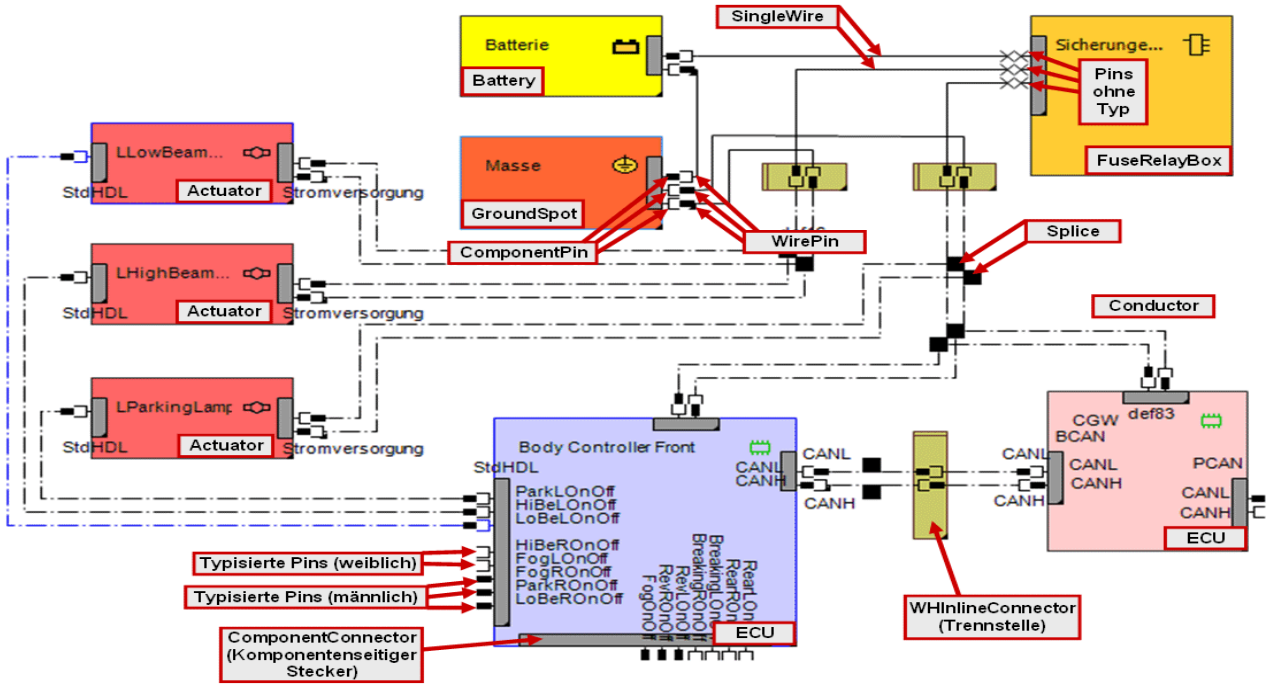
- Keine Trennstellen
- Keine Splices
- Keine Stecker
- Vereinfachte Darstellung von Pins

Komponenten können mit „Ersatzschaltbild“ hinterlegt werden

> Leichteres Verständnis der elektrischen Zusammenhänge

> Automatisierte Generierung von Werkstattmaterial

Leitungssatz-Editor

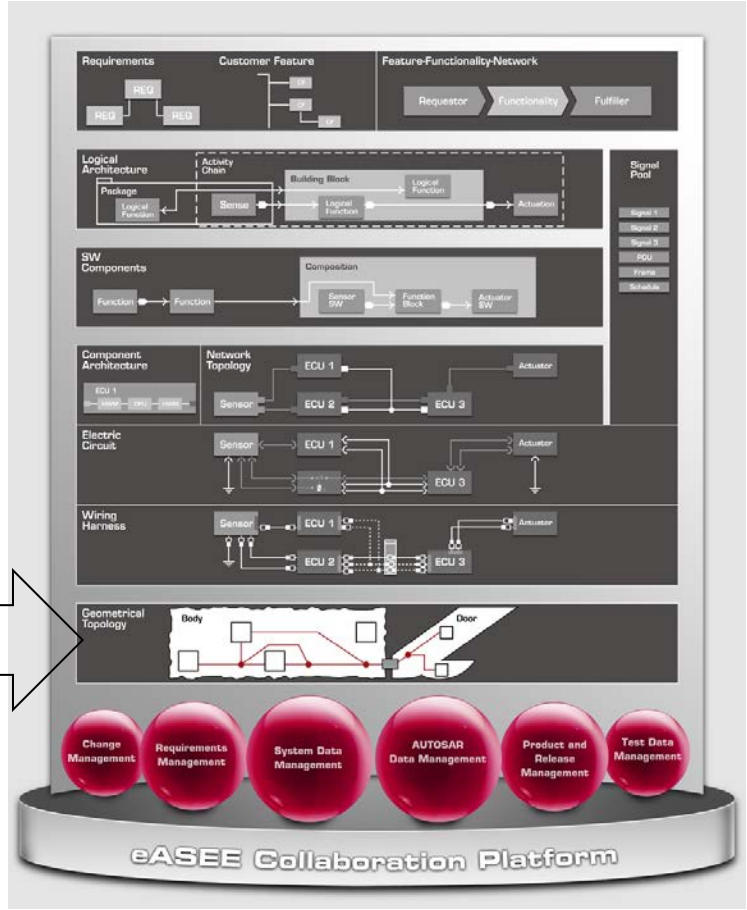


Darstellung aller Leitungssatzelemente

- Trennstellen
- Splices
- Detaillierte Pins
- Steckerpartitionierung

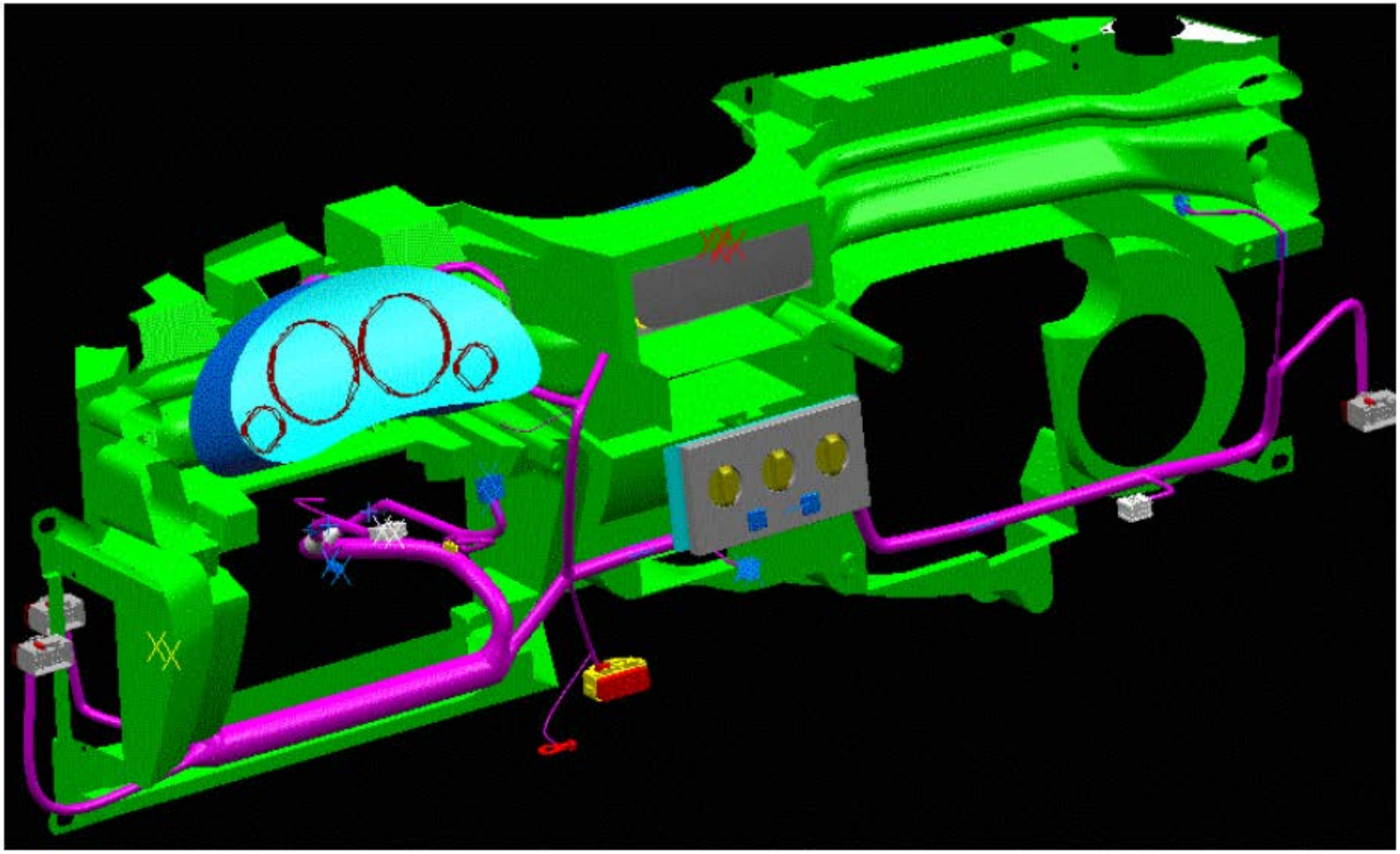
> Dokumentation des Leitungssatzes

Geometrie

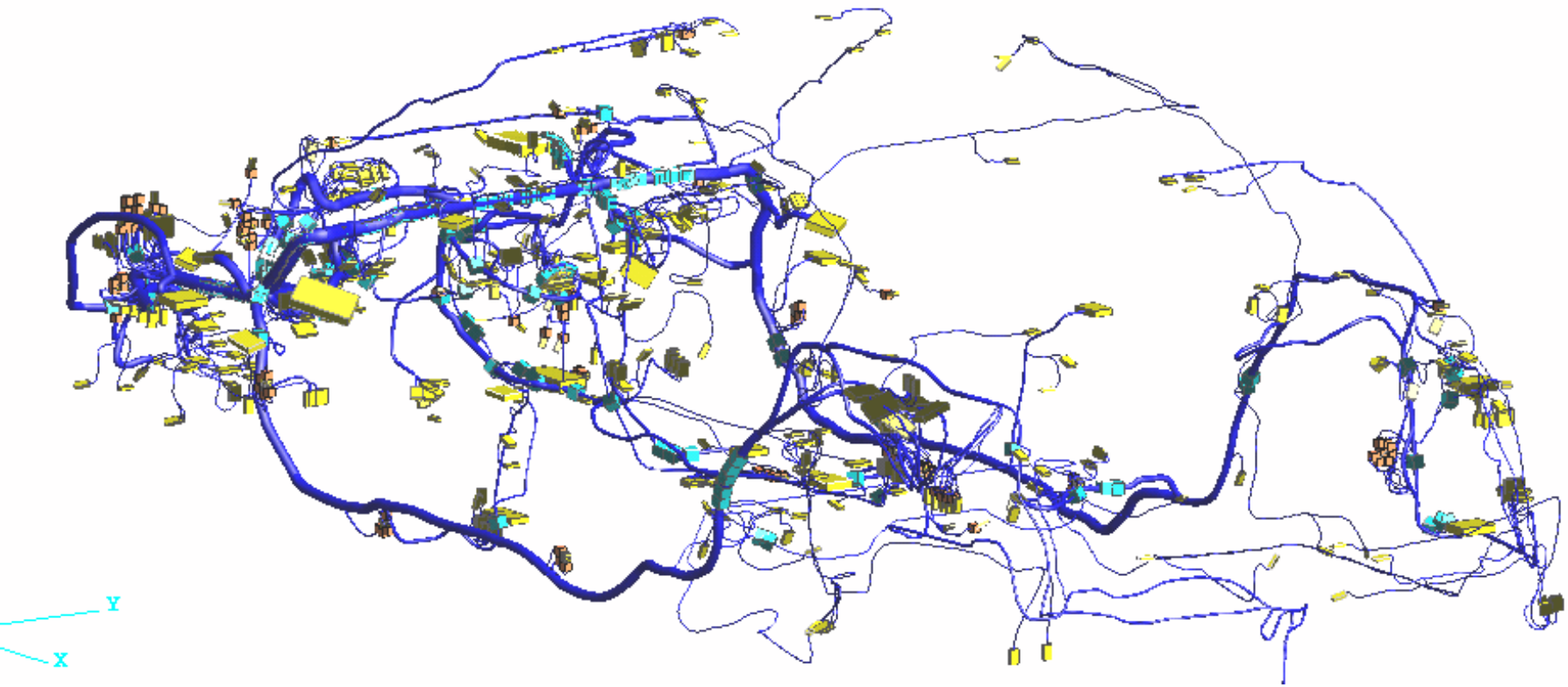


Leitungssatz im 3D-Modell

Der Leitungssatz verbindet die Steuergeräte und ist an die Fahrzeugstruktur angepasst.

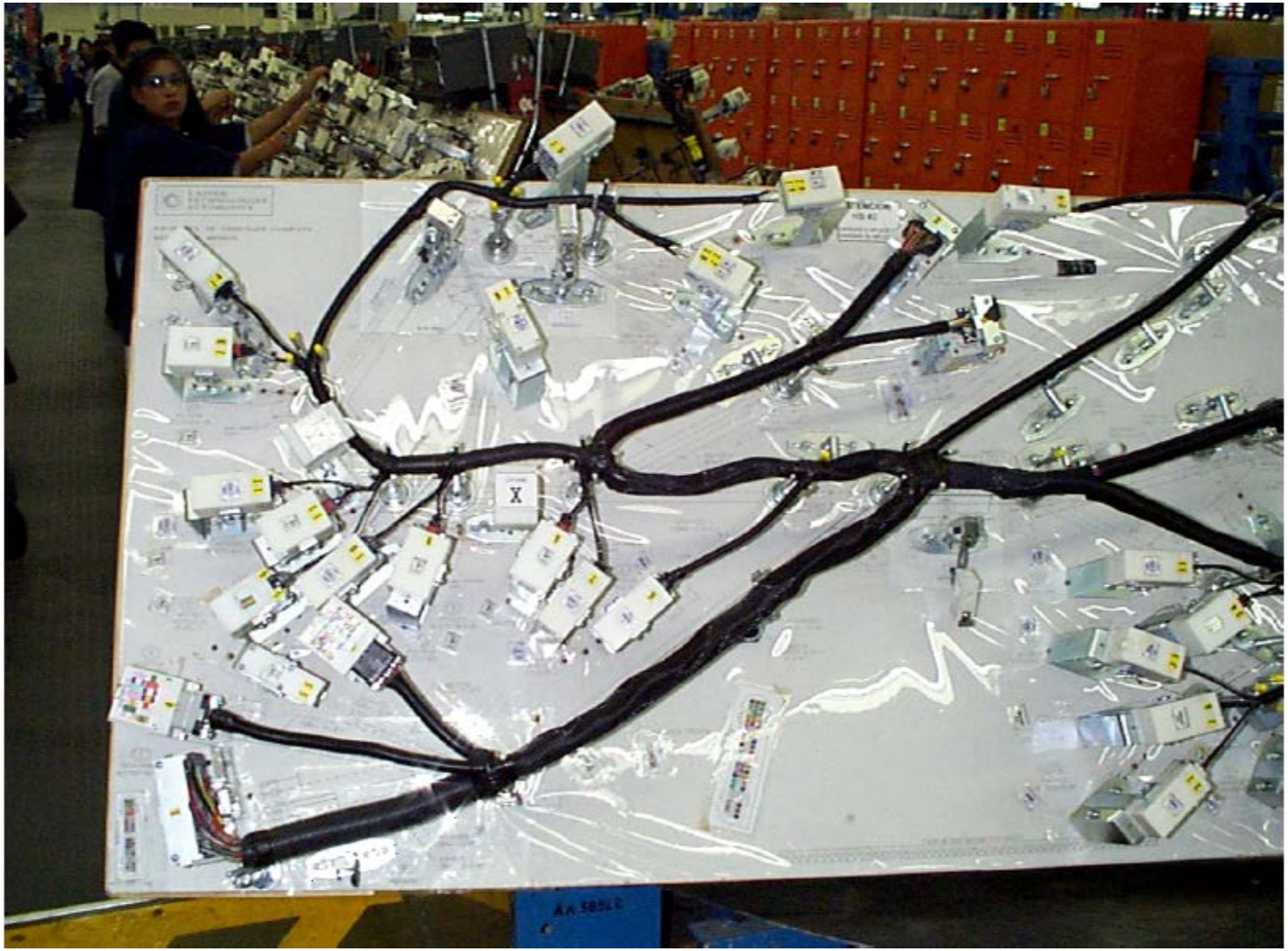


Zentralleitungssatz eines PKWs

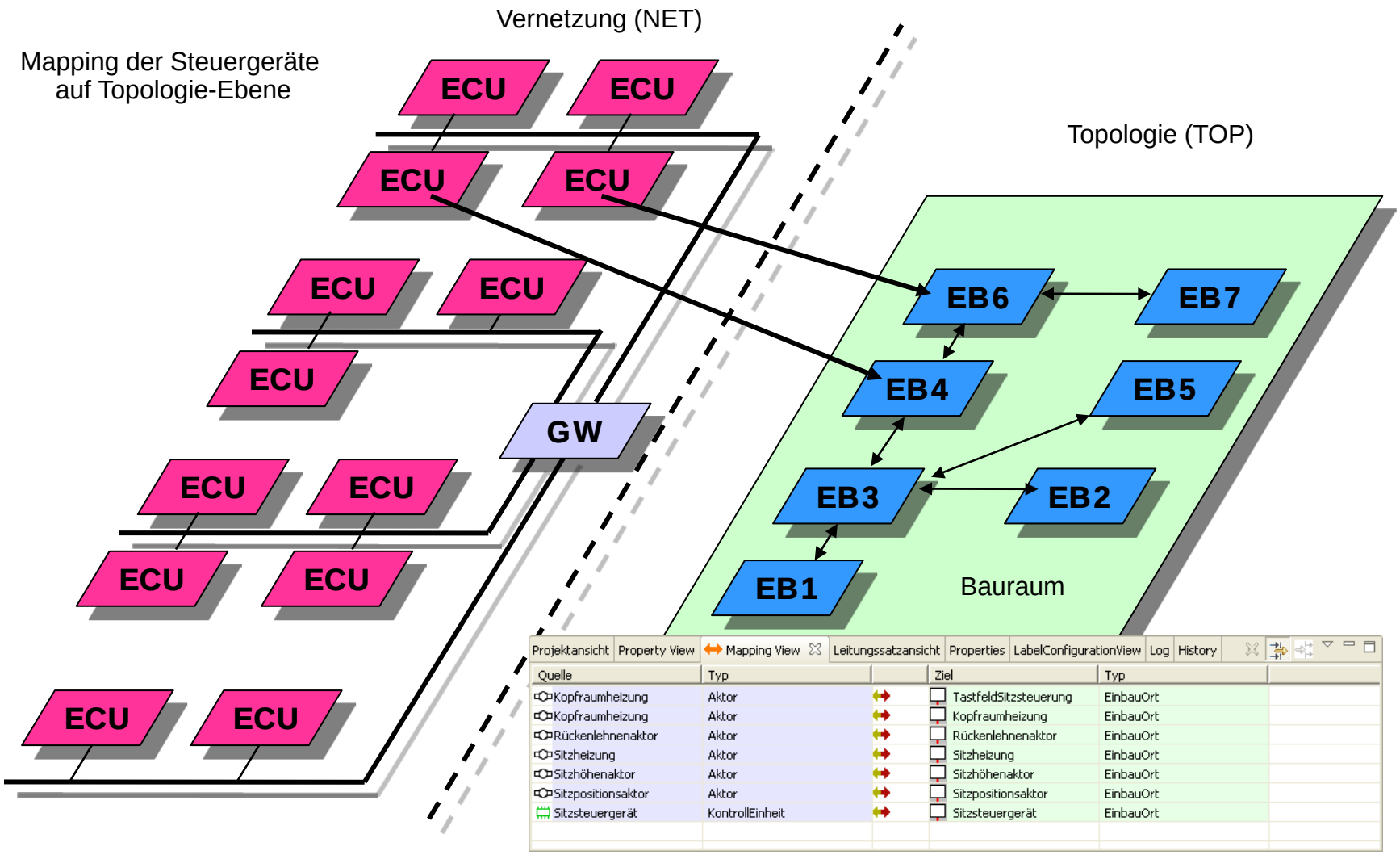


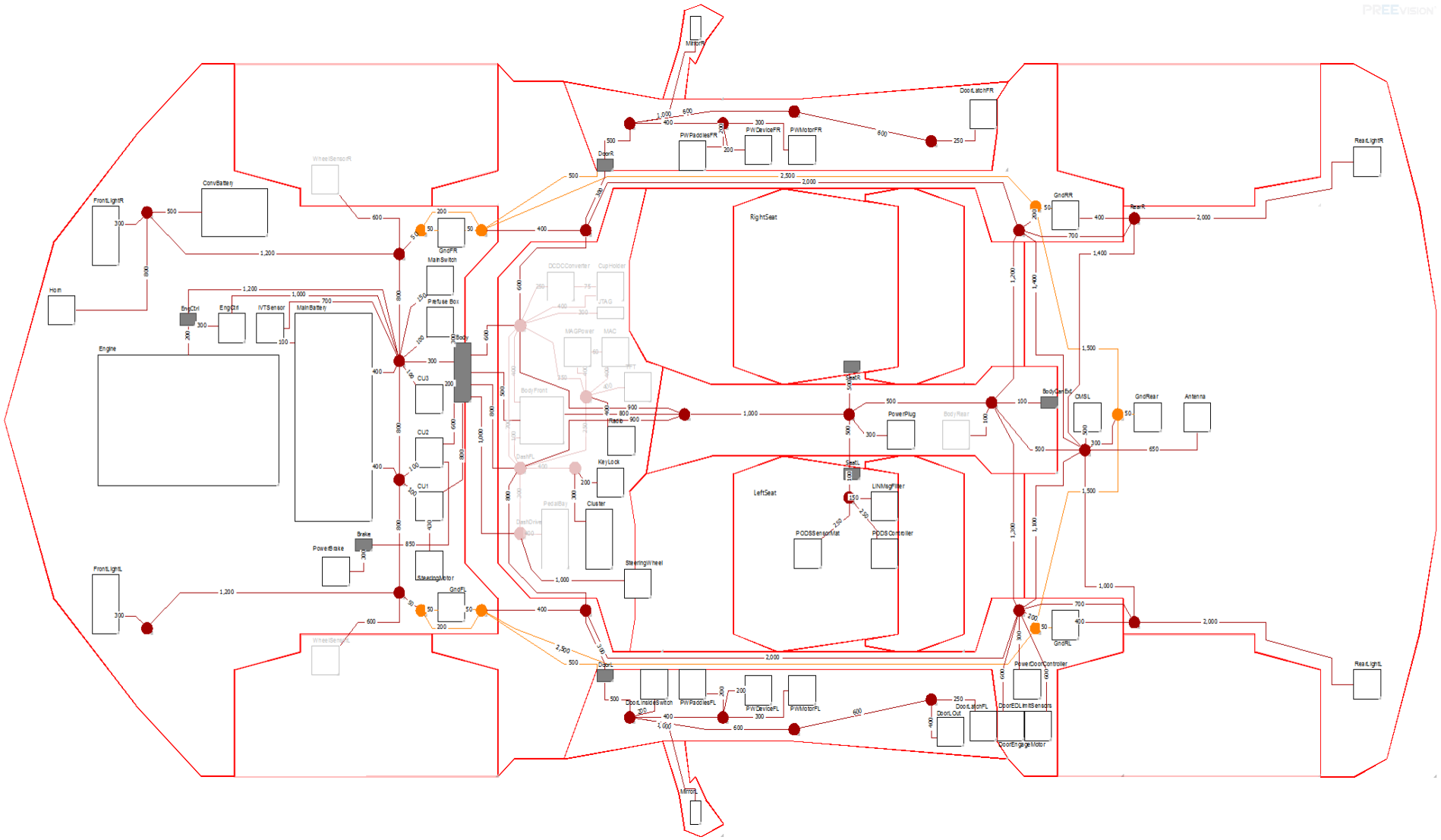
Ca. 2500 verlegte Leitungen mit Querschnitten zwischen 1qmm und 16qmm Kupfer

Realer Leitungssatz

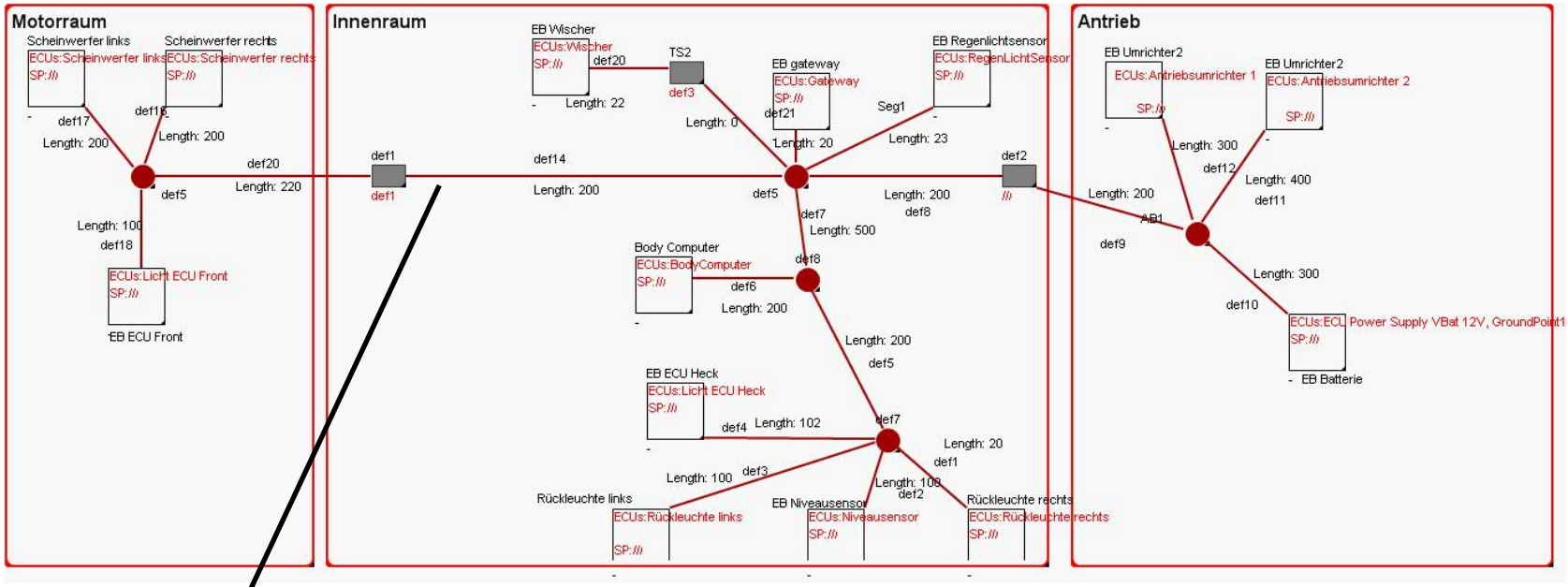


Verknüpfung NET → GEO durch Mappings

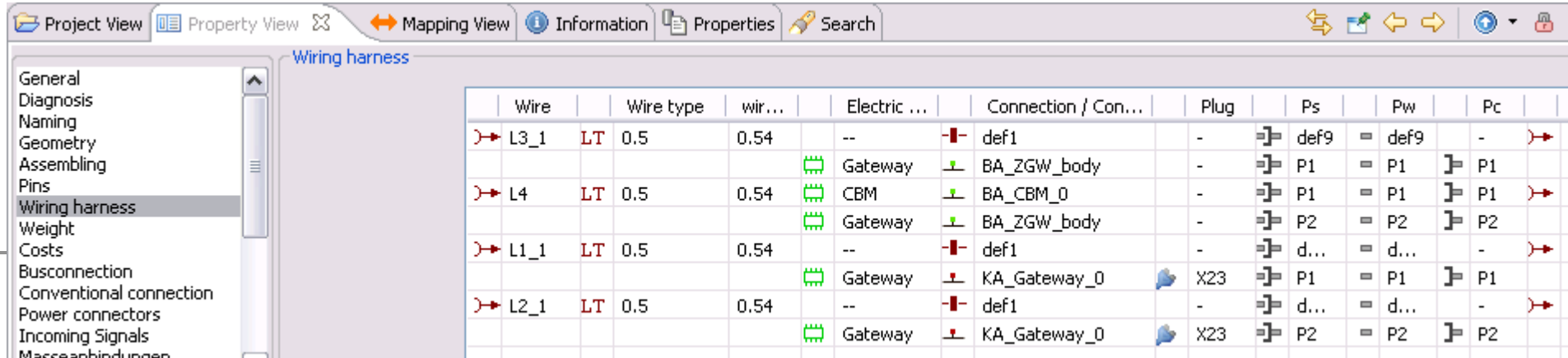




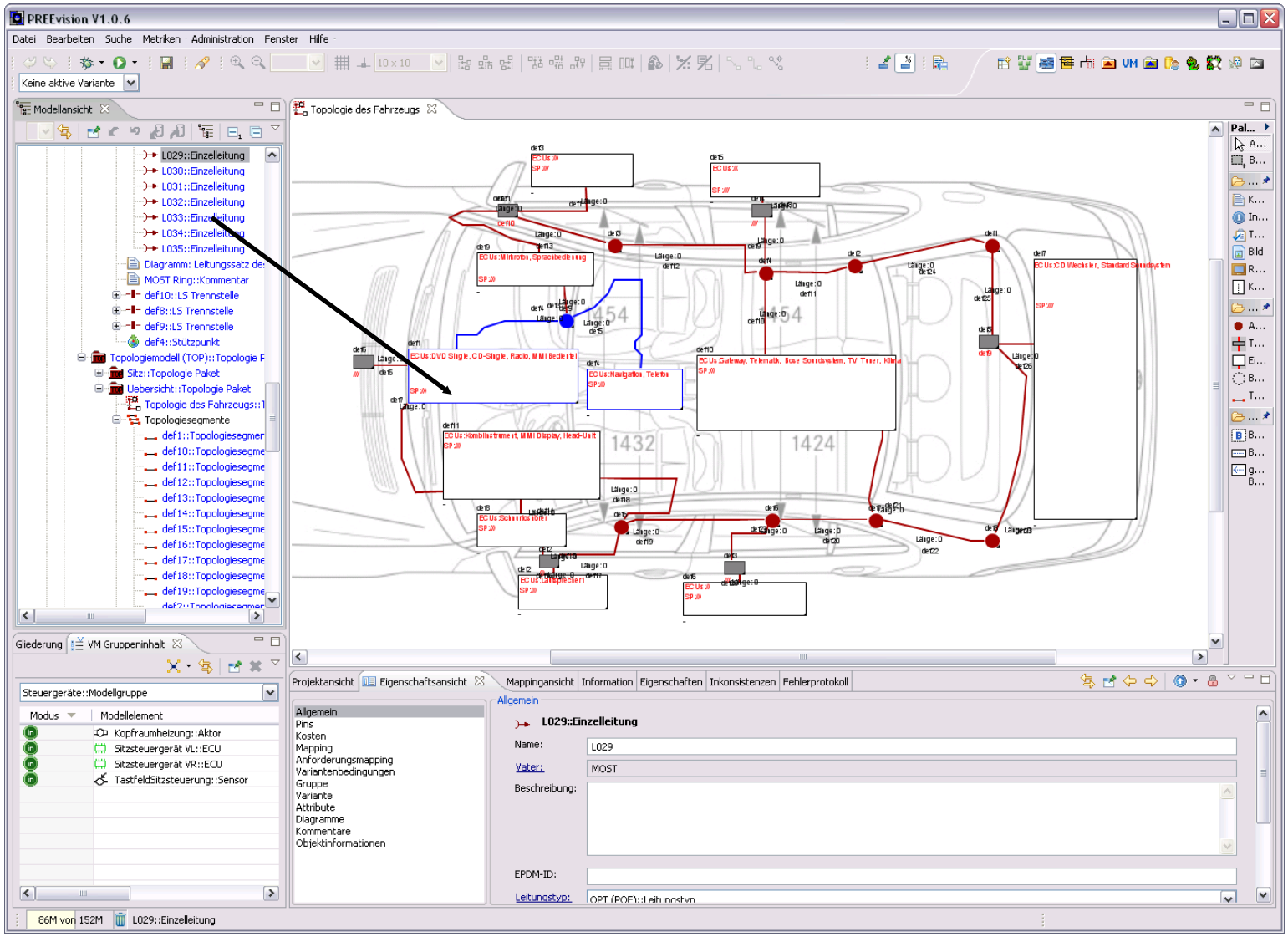
Topologie Sitzmodul



Leitungssatz

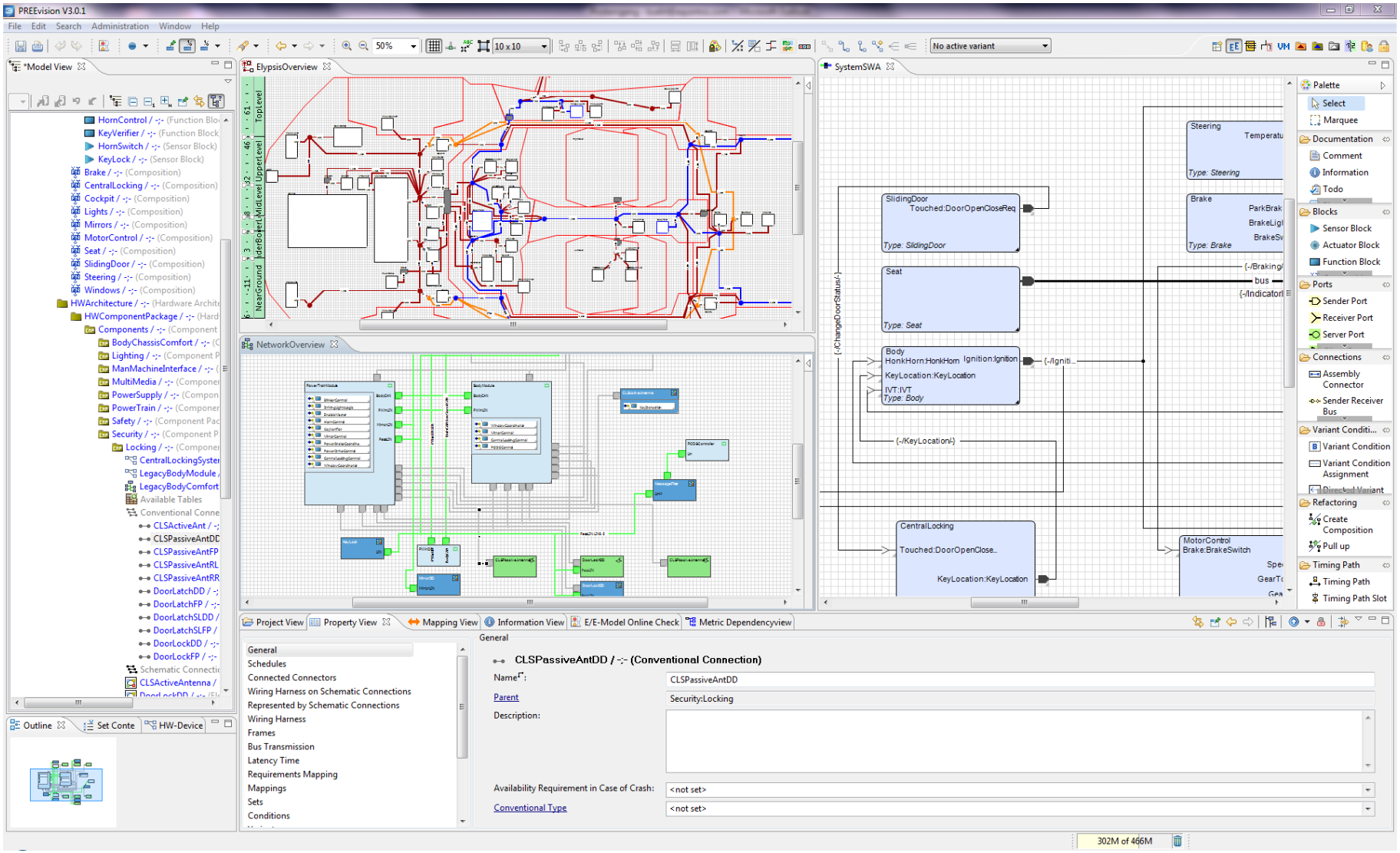


2D Topologie in PREEvision

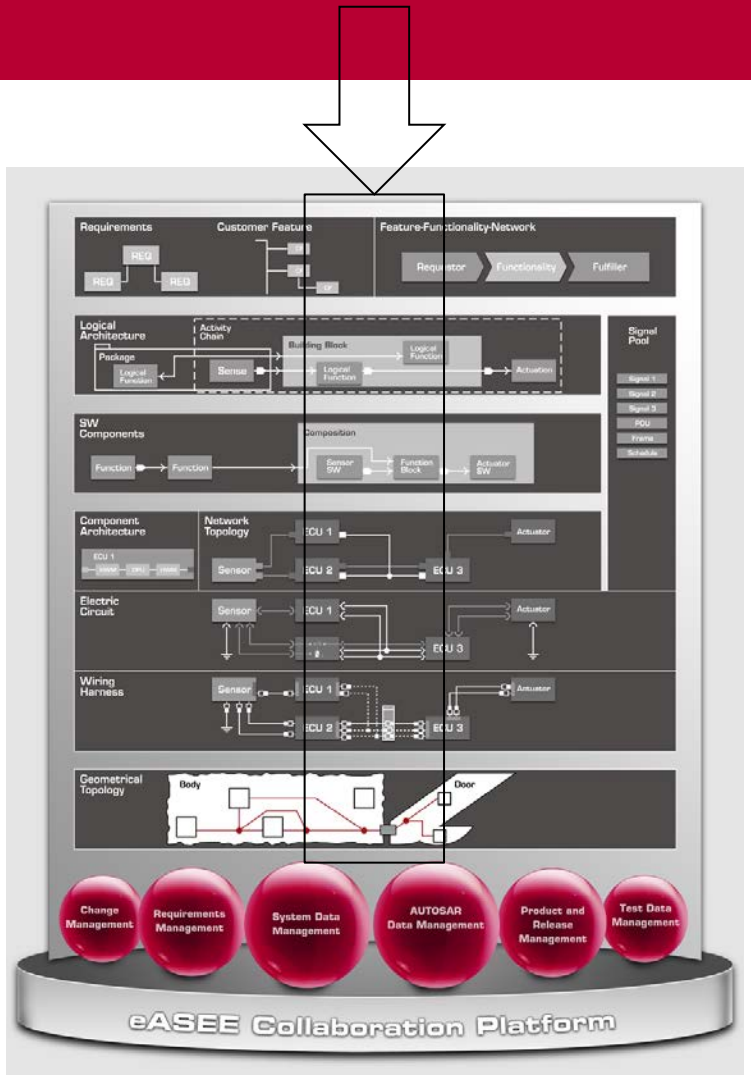


PREEvision

Customer Benefits: GUI concept



Varianten



Use Case: Variant Management

Solution Space in Product Lines

Explicit vs. Implicit Definition

Explicit – Variants as Representatives

- Concept Selection by Variant
- Set and System Content
  On all Modeling Layers
  And in between

Implicit

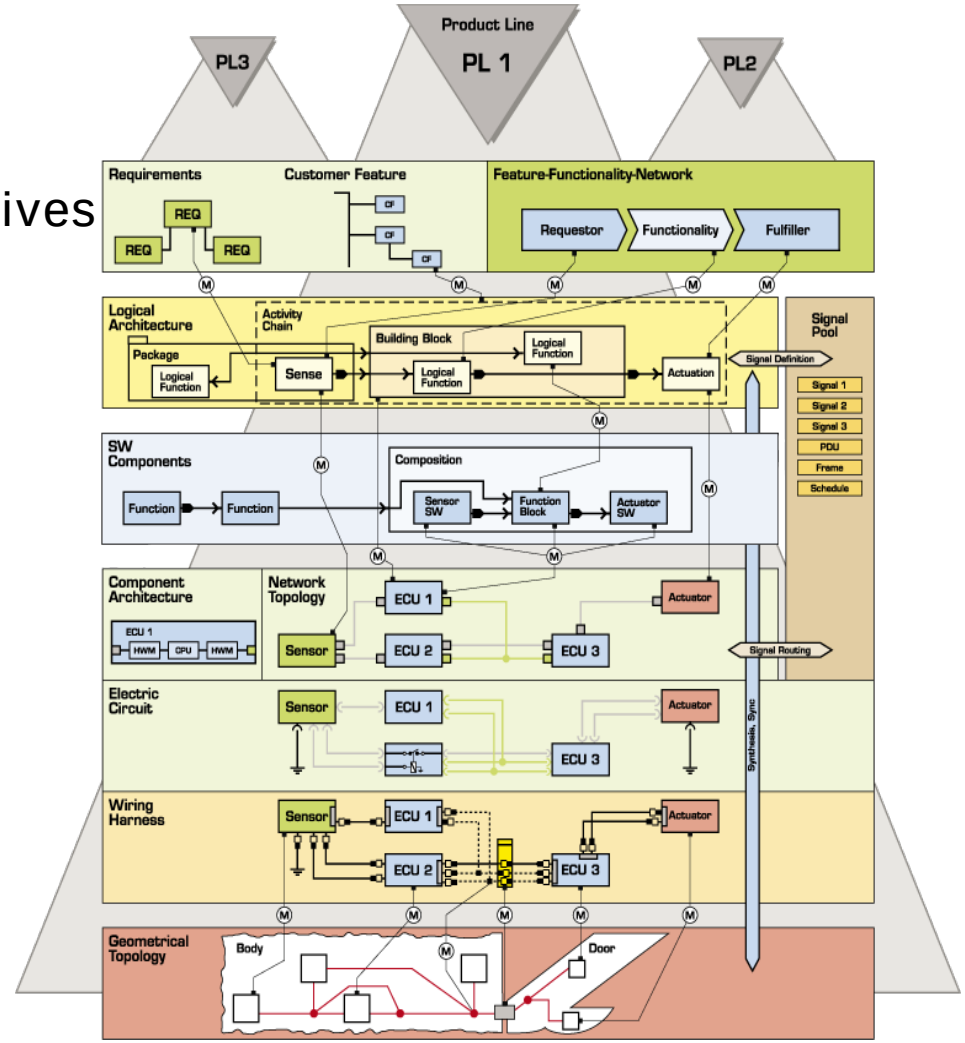
- Variant Structure
  - (Hierarchy)
- Propagation Rules
- Variant Conditions

xor

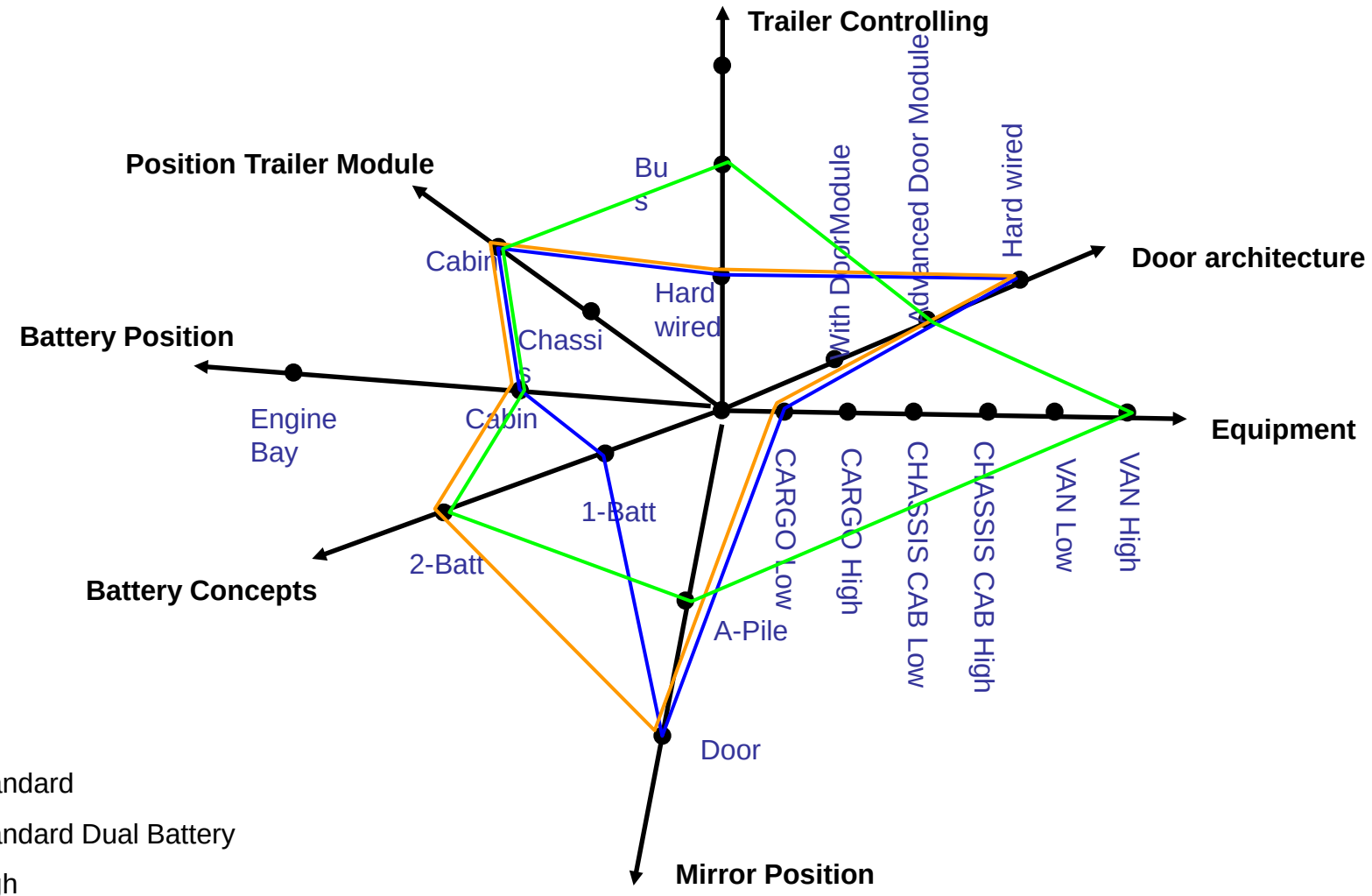
or

optional

req



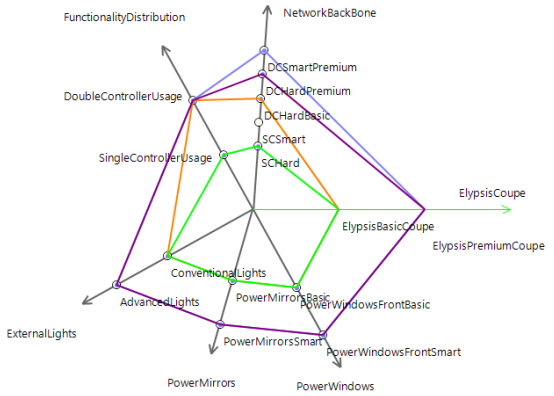
Beispiel: Architekturvarianten



Use Case: Variant Management

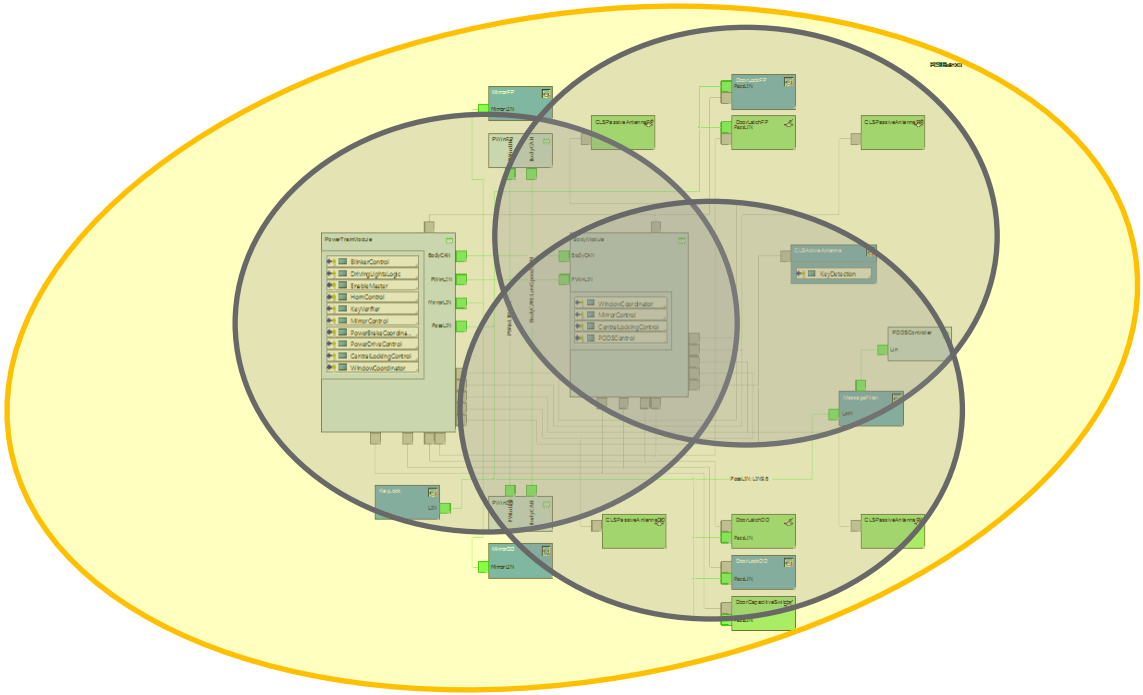
Super-Set Modeling

‘150% Modeling’ of Product Lines and Libraries

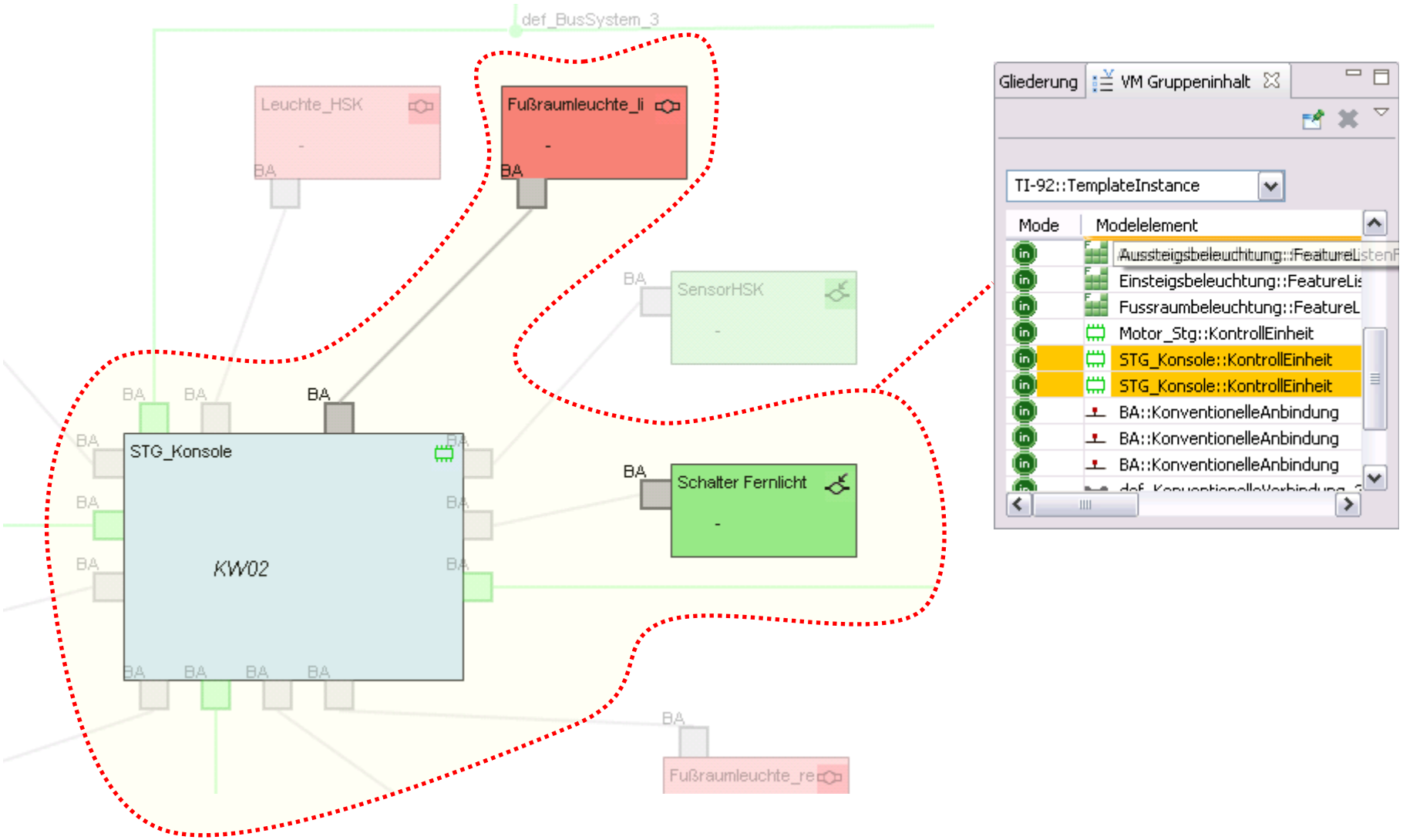


- Technical Concepts: Definition and Selection
- Equipment: Defining Configurations of Features
- Building Representative Architecture Variants

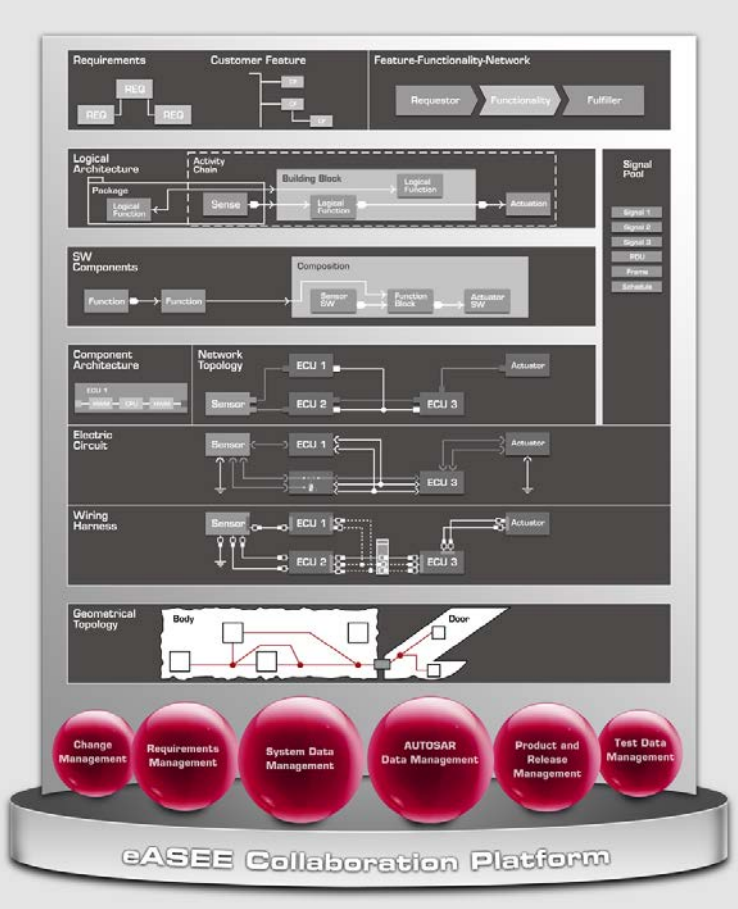
- Set-based Structuring
- System Integration



Bilden von Varianten



Metrics



Bewertungskriterien einer E/E-Architektur

Qualität

- Wiederverwendbarkeit
- Robustheit
- EMV-Klassifikation
- Erweiterbarkeit
- Testbarkeit von Feature / Funktionen
- Unabhängigkeit der Teilfunktionen
- Kompatibilität
- Abhängigkeit zu einzelnen Zulieferern
- Einsatz bewährter Technologie (Anteil)
- Wiederverwendung bestehender Komponente
- Redundanz (SIL)

Kosten

- Gesamtsystem
  - Entwicklungskosten
    - Steuergeräte
    - Leitungssatz
    - Einsparungen Wiederverwendung
  - Materialkosten
    - Leitungssatz
    - Komponenten
  - Zeitaufwand Montage
    - # Teile
    - # Baugruppen
- Min-, Max-, Ecktypen
- Feature
  - Systemkosten
  - Garantie / Wartung
- Life Cycle

Mech. Eigenschaften

- Gewichte
  - Steuergeräte
  - Aktoren
  - Sensoren
  - Leitungssatz
  - Gewichtsverteilung
- Dimensionen
  - Leitungslängen
  - Komponentengrößen
  - Befüllung Segmente

E / E

- Bordnetz
  - Netzmanagementereigniss
  - Nachlauf
  - Ruhestrom
  - Versorgung Komponenten
  - Sicherung Komponenten
- Informationsaustausch
  - Anzahl Bussysteme
  - Buslasten
  - Anzahl konv. Verb.
- Diagnoseeigenschaften
- Beiträge zu Fehlerspeicher-einträgen
- Gateways

Dokumentation

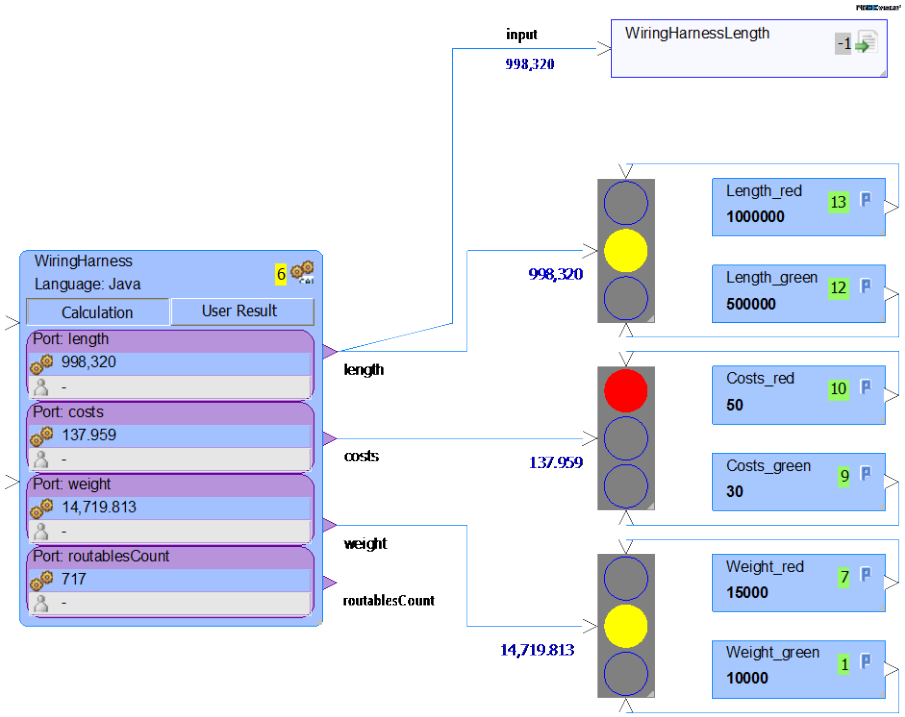
- Entwicklungsstand
  - Funktionsbeschreibung
  - SG- / Systemsteckbriefe
- Versionsverwaltung
- Dokumentationsunterlagen
  - Präsentationen
  - Topologieschaltbild
  - Architekturbewertungen
  - Architekturvergleiche
- Lastenheft
- Unterlagen für Audits

Machbarkeit

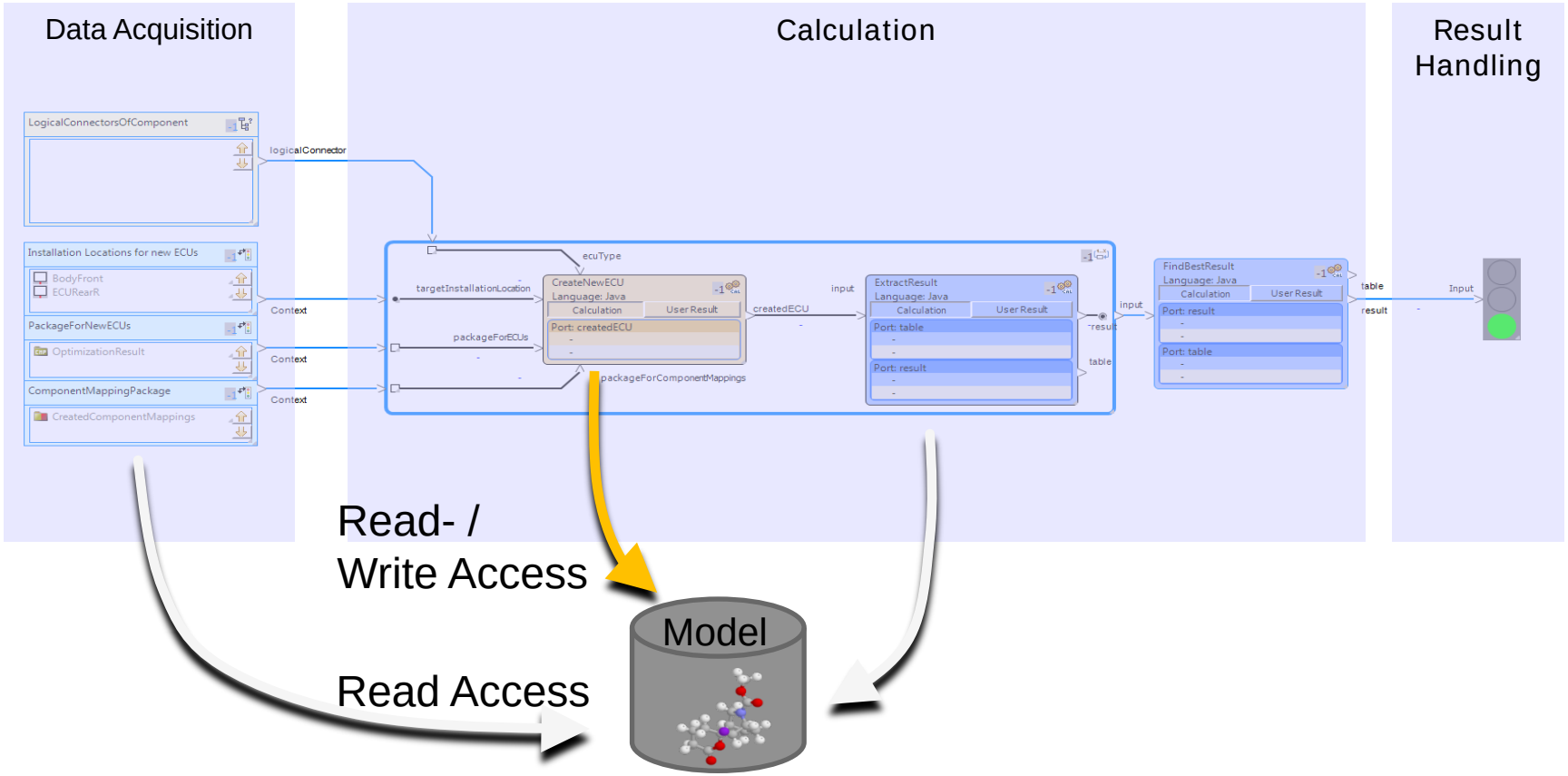
- Physikalische Baubarkeit, logisches Vernetzungskonzept
  - Steuergeräte
  - Bauräume, Verkabelung, Komponenten
- Gesetzliche Vorschriften
- Stückliste
- Reifegrad der Funktionen

Metrics

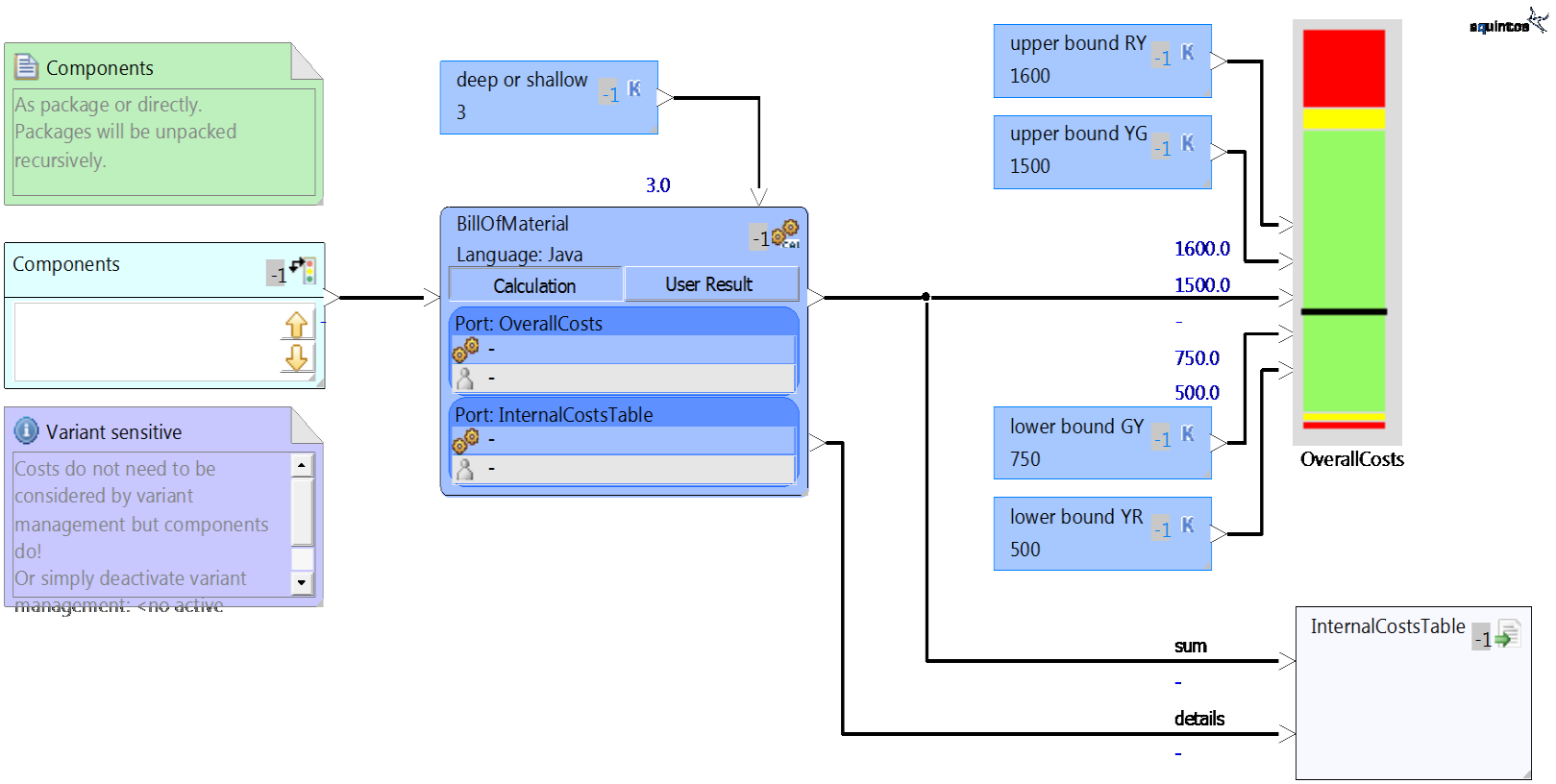
- Are used to perform **calculations** on the data model for analysis and optimization.
- Can be widely used to enrich tool with customer **individual IP**
- Always run on the full model – the result is up to date.
- Output of metrics is streamed into **Reports** or into **GUI** as lights, scales or values.



- Are based on a **graphical notation** and can be expanded by Java- code



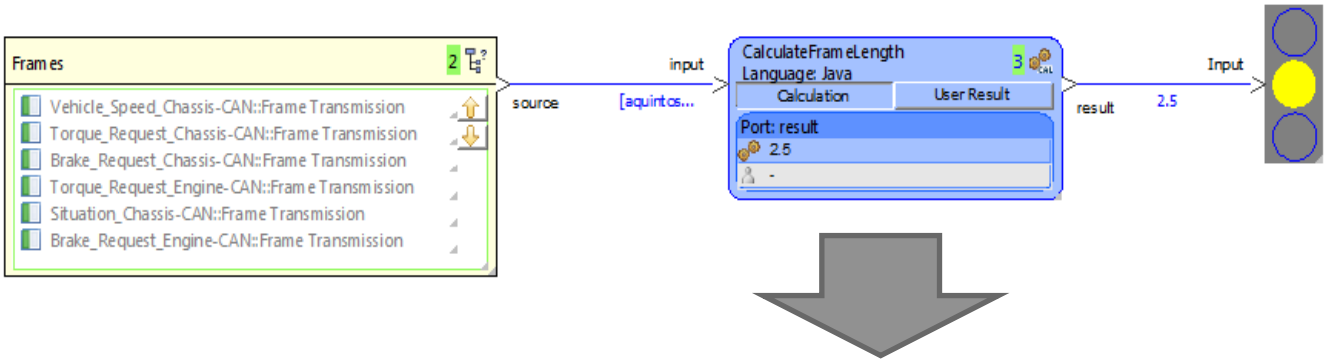
Metrics (1) – Graphical Data-Flow Oriented Language

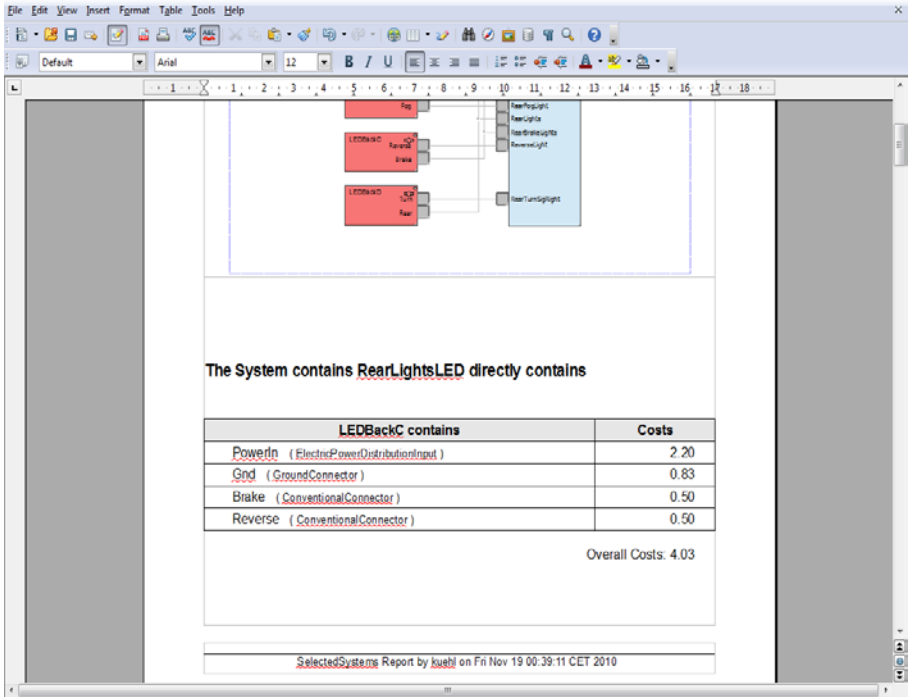


Metrics are used to compute different evaluation criteria

Output of metrics is streamed into Reports or into GUI

Use Case: Report Generator





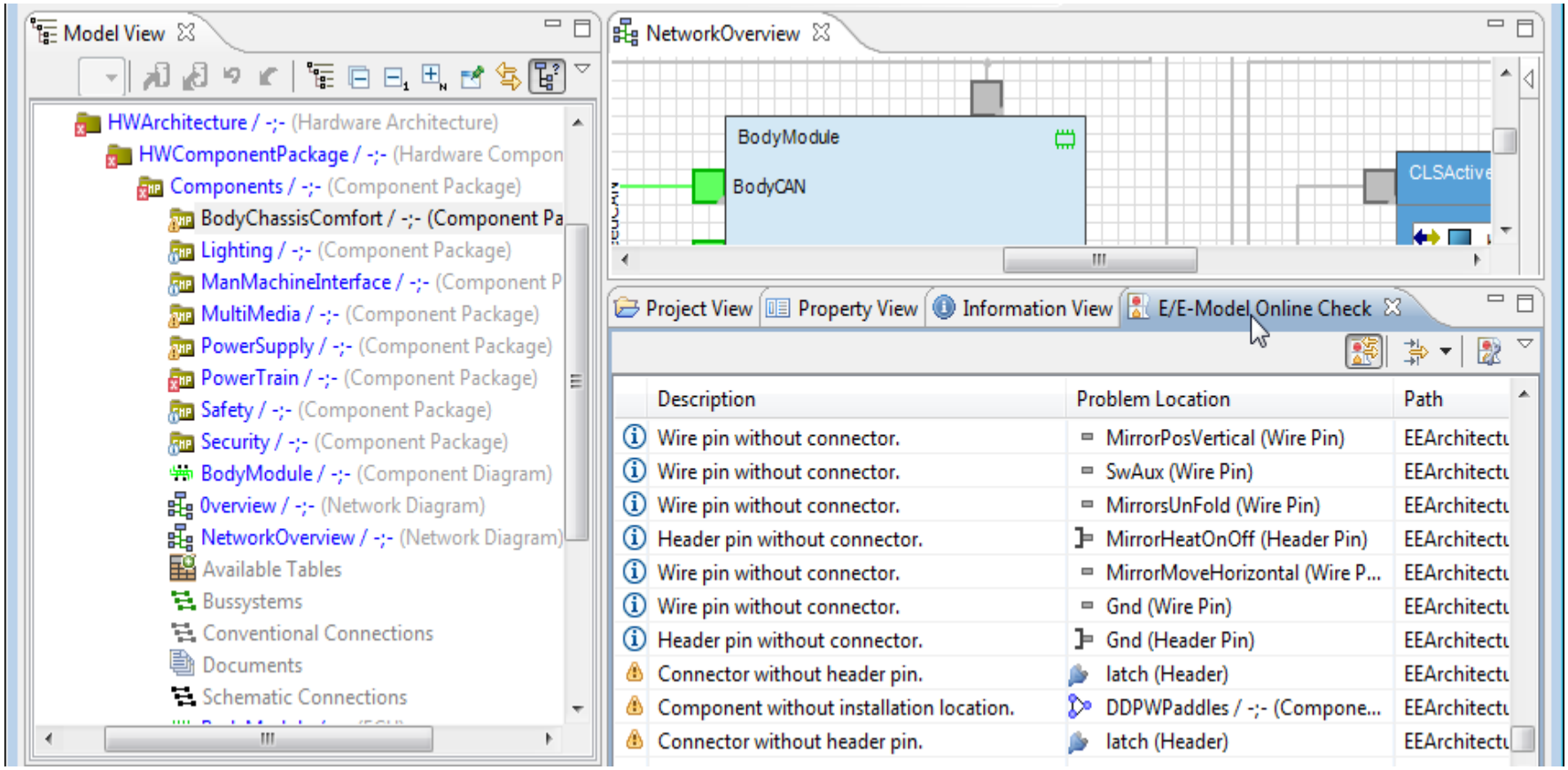
The System contains RearLightsLED directly contains

LEDBackC contains	Costs
PowerIn (ElectricPowerDistributionInput)	2.20
Gnd (GroundConnector)	0.83
Brake (ConventionalConnector)	0.50
Reverse (ConventionalConnector)	0.50

Overall Costs: 4.03

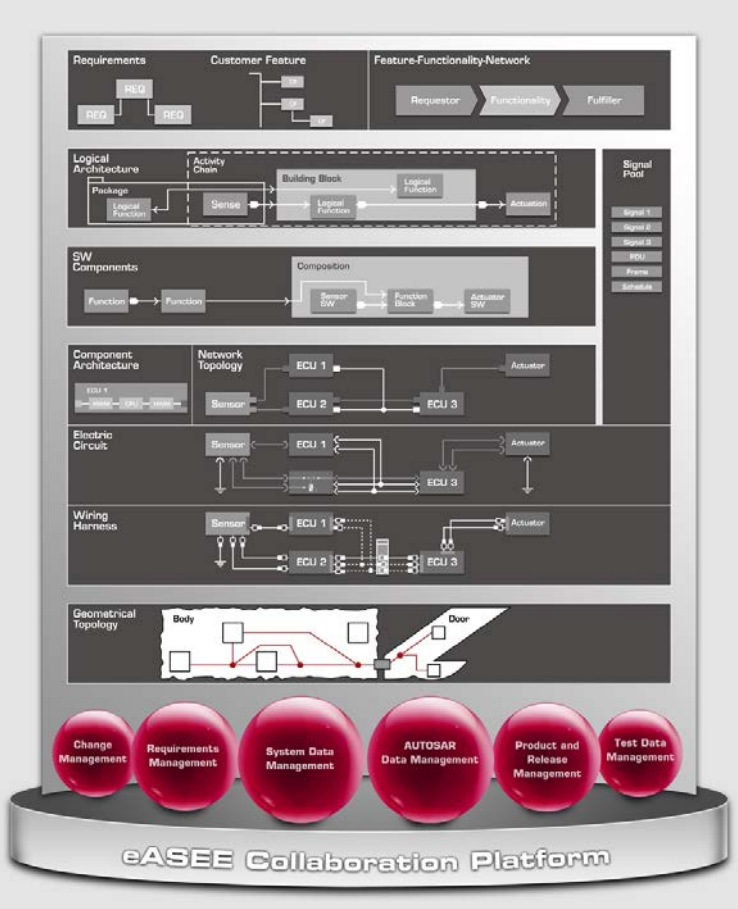
SelectedSystems Report by kuehl on Fri Nov 19 00:39:11 CET 2010

Consistency Checker

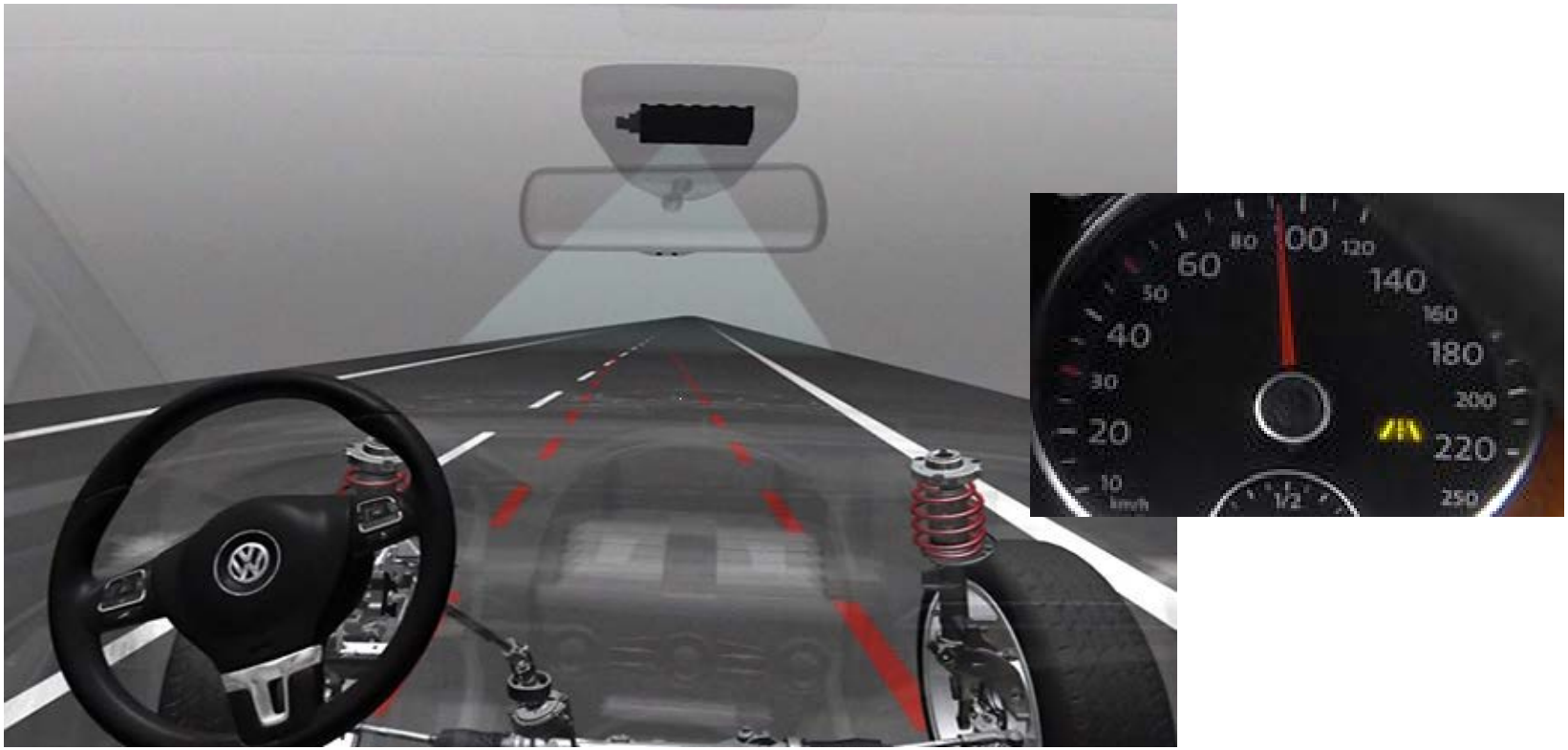


- Errors, Warnings, Information on Architecture or selected Parts
- Relevant Consistency Checks to be selected/extended
- Interactive ToDo List

Safety



Safety Critical System: Lane Departure Warning

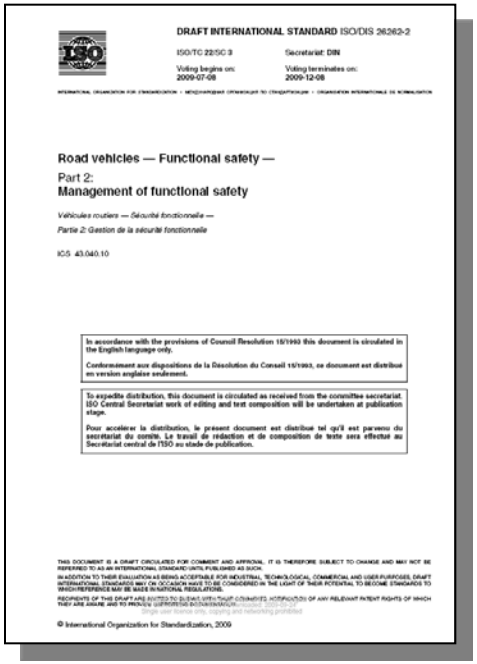


Source: www.volkswagen.de

- Warns the driver in the event of an unintentional lane departure
- Corrects the direction via the steering column and braking

Current status

- Increased awareness for functional safety since the publication of ISO DIS 26262.
- Helped to improve understanding of the necessary processes and methods.
- Nevertheless there is uncertainty in the implementation of requirements that are not described clearly enough in the standard.



DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-2

ISO/TC 22/SC 3 Secretariat: DIN

Voting begins on: 2009-07-08 Voting terminates on: 2009-12-08

Road vehicles — Functional safety —

Part 2:
Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

ICS 43.040.10

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2009

1. Structure, content and presentation of the safety case

2. Type and scope of the necessary tests

The safety lifecycle according to ISO 26262

1

Item Definition

Definition of features and their interactions, operating modes, vehicle states, etc.

2

Hazard and Risk Analysis

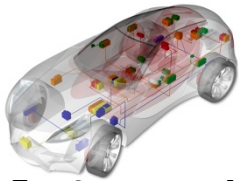
Identification and classification of hazardous scenarios and derivation of appropriate system safety goals.

3

System safety concept

Design of a system concept for implementing the safety goals, for example on the basis of diagnostic or redundancy measures.

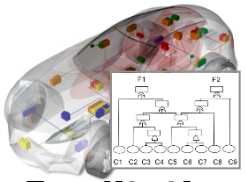
4



System and component design

Design of technical system and component concepts including the derivation and implementation of technical safety requirements accordingly.

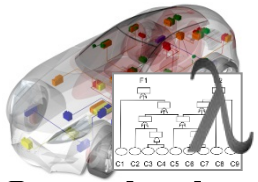
5



Qualitative Safety Analyses

Application of deductive and inductive safety analysis techniques (e.g. FTA, FMEA) to validate the ability of the design to meet the system safety goals.

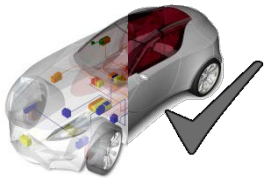
6



Quantitative Safety Analyses

Calculation of the probability of the system failing to meet the safety goals and confirmation that the failure rate and diagnostic coverage targets are met.

7



Verification and Validation

Confirmation through review, analysis and test that all safety requirements are correctly implemented in the delivered system and that all assumptions made in the safety concept are valid.

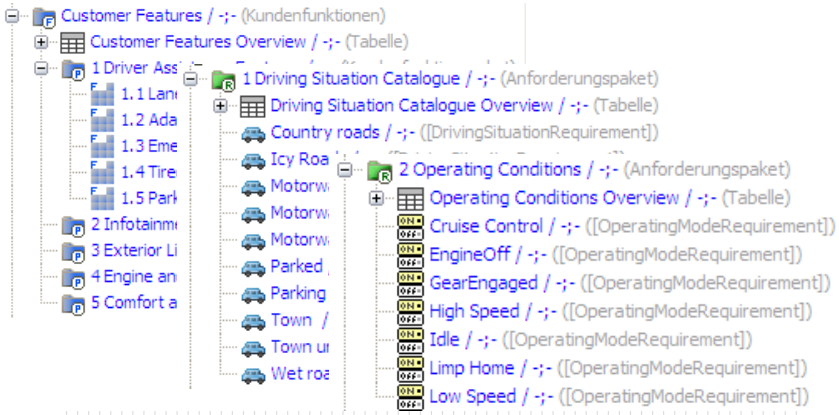
8

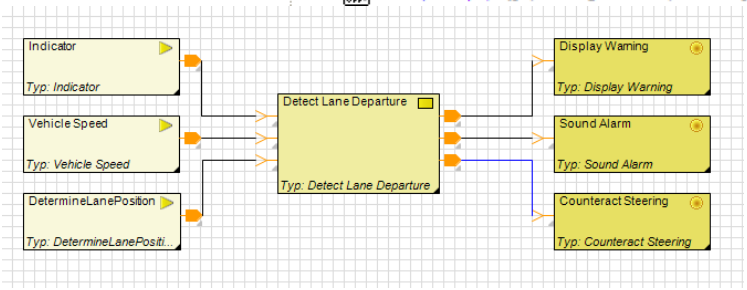
Safety Case

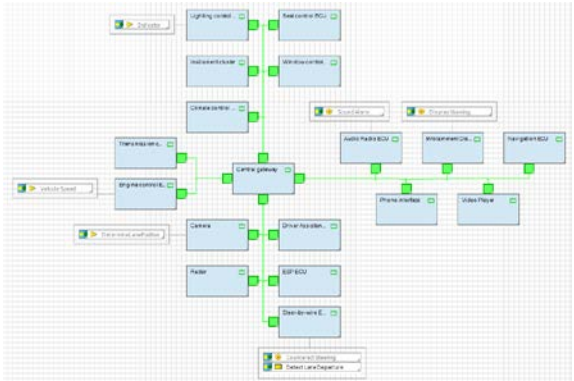
Construction of a structured, coherent, complete and convincing argument that the system meets all its safety goals and appropriate regulations.

vector

Item definition





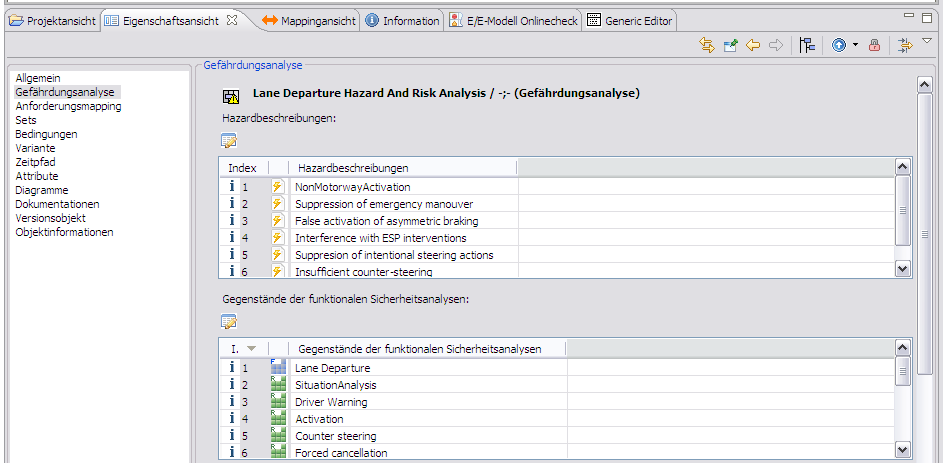


Item Definition:

- Feature specifications
- Product-line variant model
- Functional and non-functional requirements
- Operating scenarios and operating modes
- Pre-existing safety requirements and concepts
- Logical and topological system architecture including allocation of functions
- Dependencies with other systems

Hazard and risk analysis

HazardDescriptions	DrivingSituations	OperatingMode	Severity	Exposure	Controllabilty	ASIL	SafetyGoals
The lane departure function activates whilst not driving on the motorway. This leads to the suppression of intentional manouvers, e.g. to avoid unexpected obstructions in town traffic.	Icy Roads	Idle	S2	E3	C3	ASIL B	The lane departure function shall only be activated after the vehicle has been travelling at a speed > 100km/h and has not changed lane in the last 2 minutes.
	Town unexpected...	GearEngaged					
The lane departure system suppresses an intentional and necessary avoidance manouver required to avoid hitting an unexpected obstacle such as animals leaping into the road ahead.	Motorway	GearEngaged	S3	E3	C3	ASIL C	The lane departure function shall be deactivated by the application of sudden steering actions of a steering angle > 15 degrees within a time period of < 1 second.
The lane depature function applies too much asymmetric braking force when intervening causing the vehicle to lose control.	Motorway	GearEngaged	S3	E3	C3	ASIL C	The asymmetric braking force applied to counteract an unintended lane departure shall not exceed 0. 1g.
The lane departure system applies steering resistance and asymmetric braking while the ESP system is intervening to maintain control of the vehicle. Control of the vehicle cannot be maintained.	Icy Roads	GearEngaged	S3	E2	C3	ASIL B	The lane departure function shall not intervence while the ESP system is applying commands to the braking system.
	Wet roads						
The lane departure suppresses an intented and necessary steering action resulting in a collision.	Town unexpected...	GearEngaged	S3	E2	C3	ASIL B	The lane departure function shall identify the driving lane with an accuracy adequate to ASIL B.
	Motorway unexpe...						The lane departure function shall be able to differentiate between permanent and non-permanent markings on the road (e.g. to denote diversions due to temporary roadworks.). If an accurate identification of the required driving lane is not possible, the lane departure function shall be
	Motorway roadwo...						
The lane departure does not apply sufficient counter steering to avoid an accident.	Motorway	Cruise Control	S3	E3	C2	ASIL B	The lane departure function shall ensure that sufficient counter steering force is applied to prevent the vehicle crossing into the oncoming or overtaking stream of
	Motorway roadwo...	High Speed					

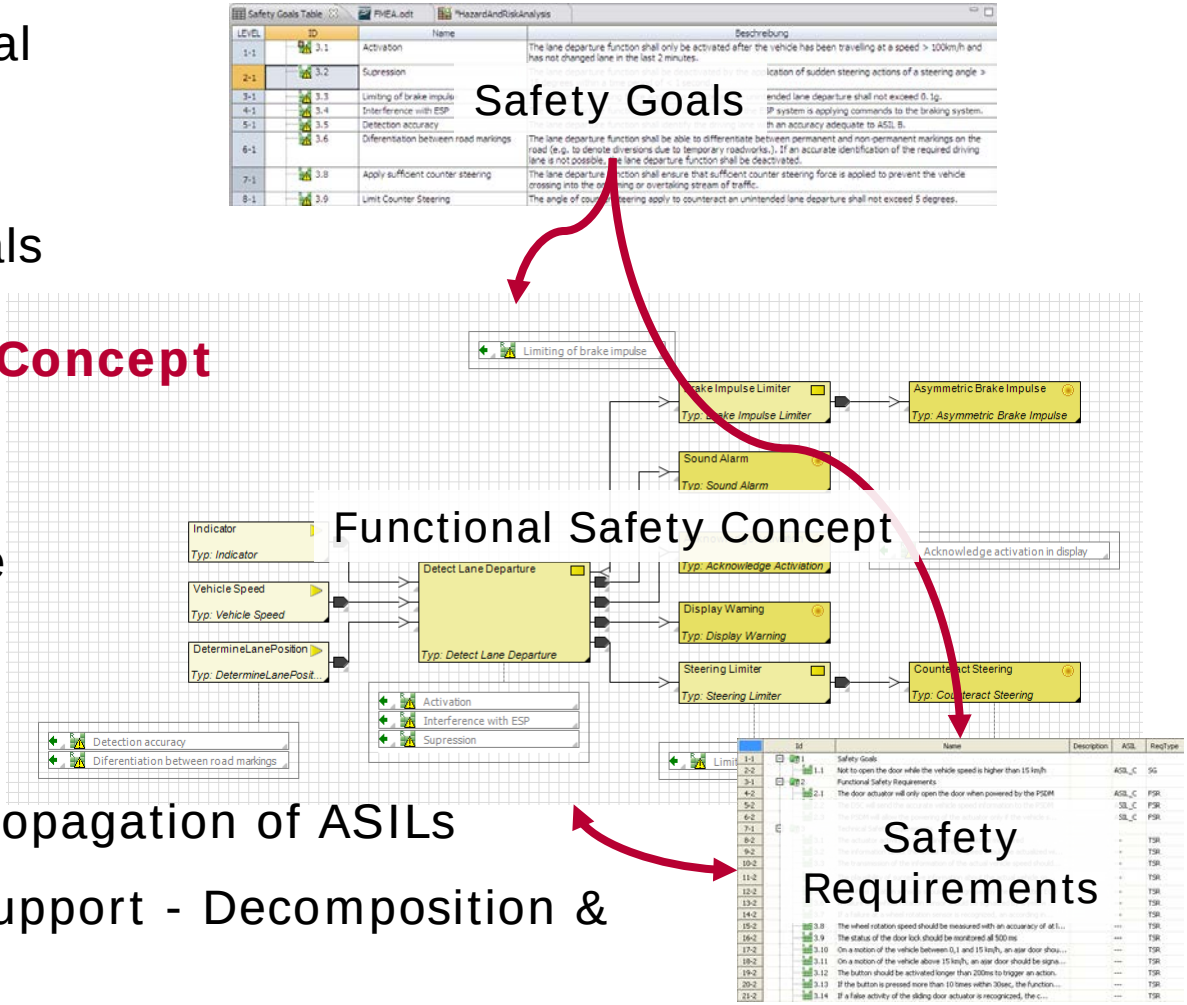


Hazard and Risk Analysis:

- Conform to ISO/DIS 26262-3
- Bi-directional traceability to the item definition and derived safety goals
- Automated calculation of ASIL
- Automated consistency checks
  - At least 1 safety goal for each hazard, consistency of safety goal ASILs,...
- Full configuration management support for distributed development and verification of analyses
- Fully configurable report generator

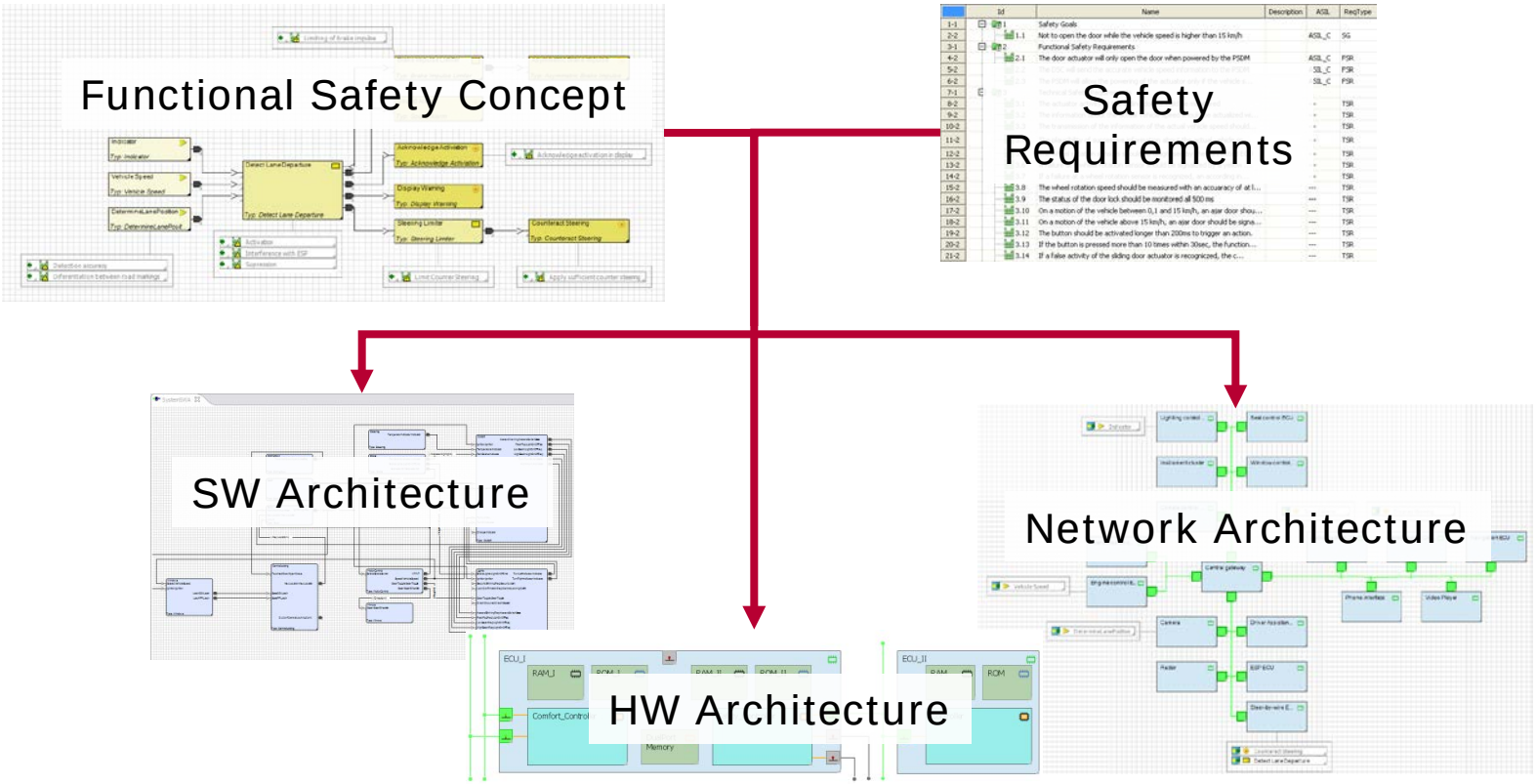
System safety concept

- Refinement of functional structure of item (**logical architecture**)
- Allocation of safety goals to logical components
  ➔ Functional Safety Concept
- Refinement of safety goals according to the functional structure
  ➔ Functional Safety Requirements



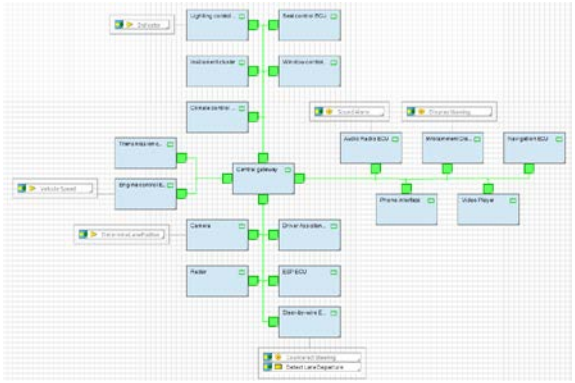
- Planned: Automated propagation of ASILs
- Planned: Refinement support - Decomposition & Coexistence

System and component design



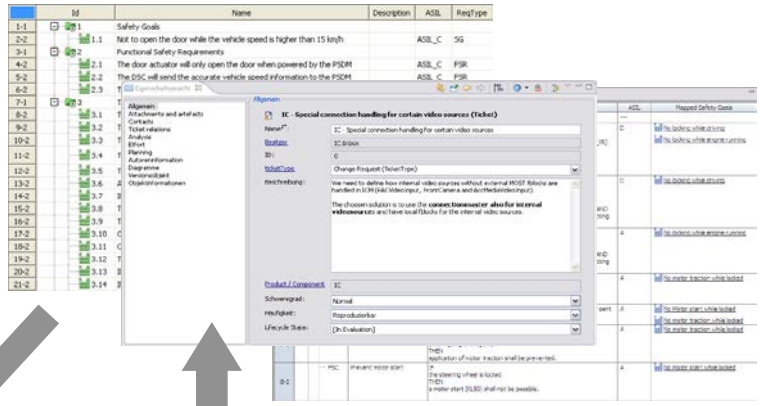
- **Allocation** of safety goals and safety functions to technical components
- **Refinement** of safety requirements based on the technical system, SW and HW architecture

Model-based FMEA



1. Structure of FMEA derived from EE Architecture

2. Existing requirements and tests used to analyse failure effects, prevention and detection measures.



3. FMEA Measures followed up as change requests and newly created requirements and tests.

Failure Modes

The lane departure function is not activated although selected by the driver.
(25 %/ ...)

Potential Effect(s) of Failure	Sev
Driver is not warned that he is straying from the lane although he is depending on this action	5

Class	Potential Cause(s)/ Mechanisms of Failure	Occ	Current Design Controls Prevention	Current Design Controls Detection	Det	RPN
YS	The button to activate lane departure has not transmitted the signal to the driver assistance ECU.	2	None defined as yet See measures: Shielded Wire For Activation Button	Presence of activation signal in off or on state is validated. See measures: Acknowledge activation in display Validate activation signal	6	60

Actions

Recommended Actions	Responsibility/ Target Date	Actions Taken	Sev	Occ	Det	RPN
Ensure that the command to activate or deactivate lane departure is continually verified. See tickets: ...	Burton / 31.01.2011	None as yet See measures:				

Bi-directional traceability is ensured between the Architecture, FMEA, Requirements, Change Requests and Tests

Automated qualitative and quantitative safety analyses

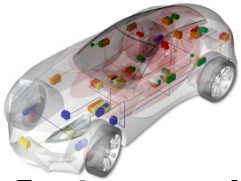
Subject of ongoing research

Hazard and Risk Analysis

- Determine Safety Goals and ASIL Targets.

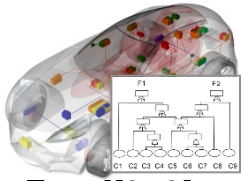
System safety concept

- Mapping of safety goals and safety requirements to components.
- **Enhancement of the E/E architecture model with failure modeling logic.***



System and component design

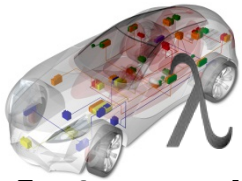
How can safety goals be violated by faults in the system?



Qualitative Safety Analyses

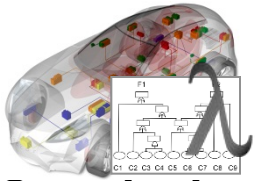
- **Automatically determine the effect of faults within the system or at its interfaces.***
- **Automatically determine the minimal cut sets that can lead to a violation of the safety goals.***

- Determine reliability of system components.
- Define fault prevention and detection measures.
- Determine diagnostic coverage.



System and component design

Is the probability of violating a safety goal acceptably low?



Quantitative Safety Analyses

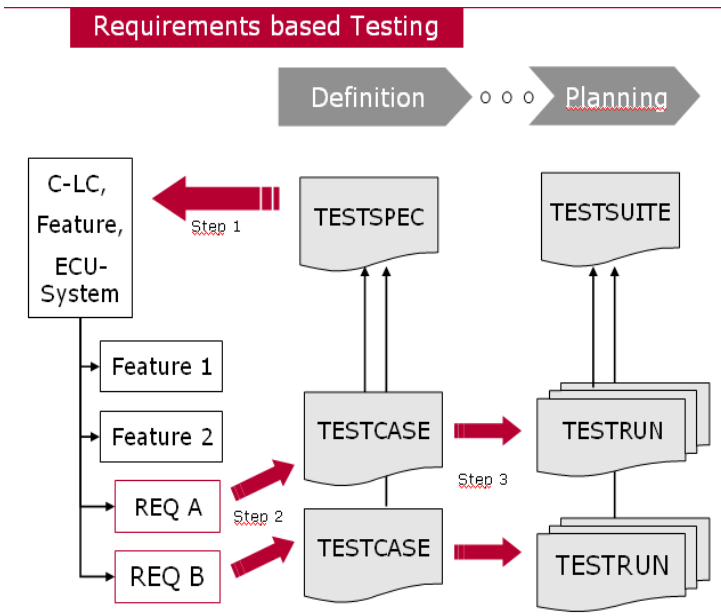
- **Automatically determine probability of faults leading to a violation of a safety goal.***

***extensions of the safety lifecycle**

vector

Test data management

- Test cases are derived directly from the (safety) requirements and linked appropriately.
- Information from the architecture model can be used to design the tests (e.g. input/output signals).
- Automatic report generation to track coverage and maturity of requirements.
- The variant model can be used to create test plans for specific product configurations.

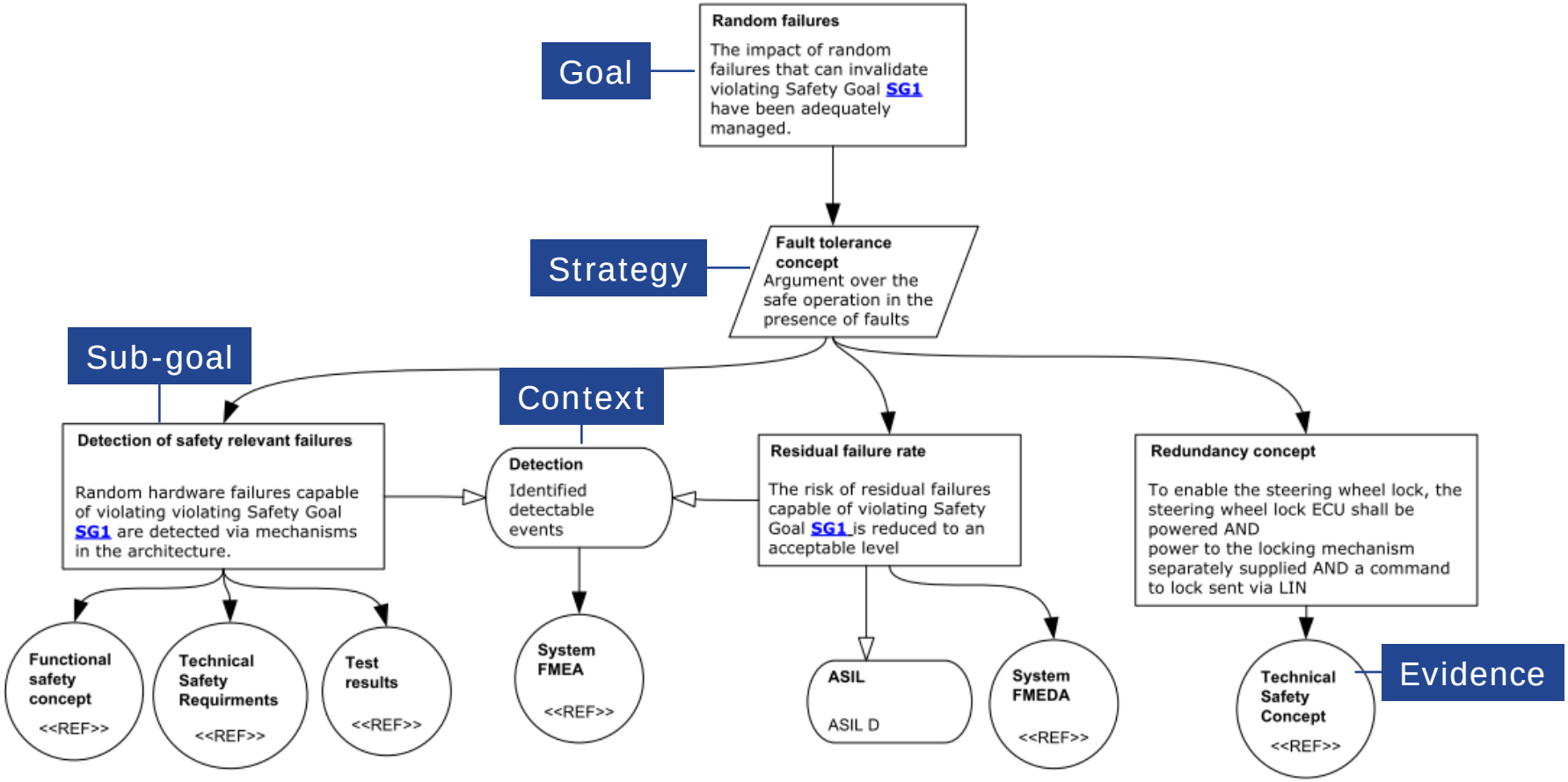


- Step 1: Map TESTSPEC with Architecture, Identify relevant requirements
- Step 2: Generate TESTCASES for each requirement
- Step 3: Plan TESTSUITE for execution

Safety management

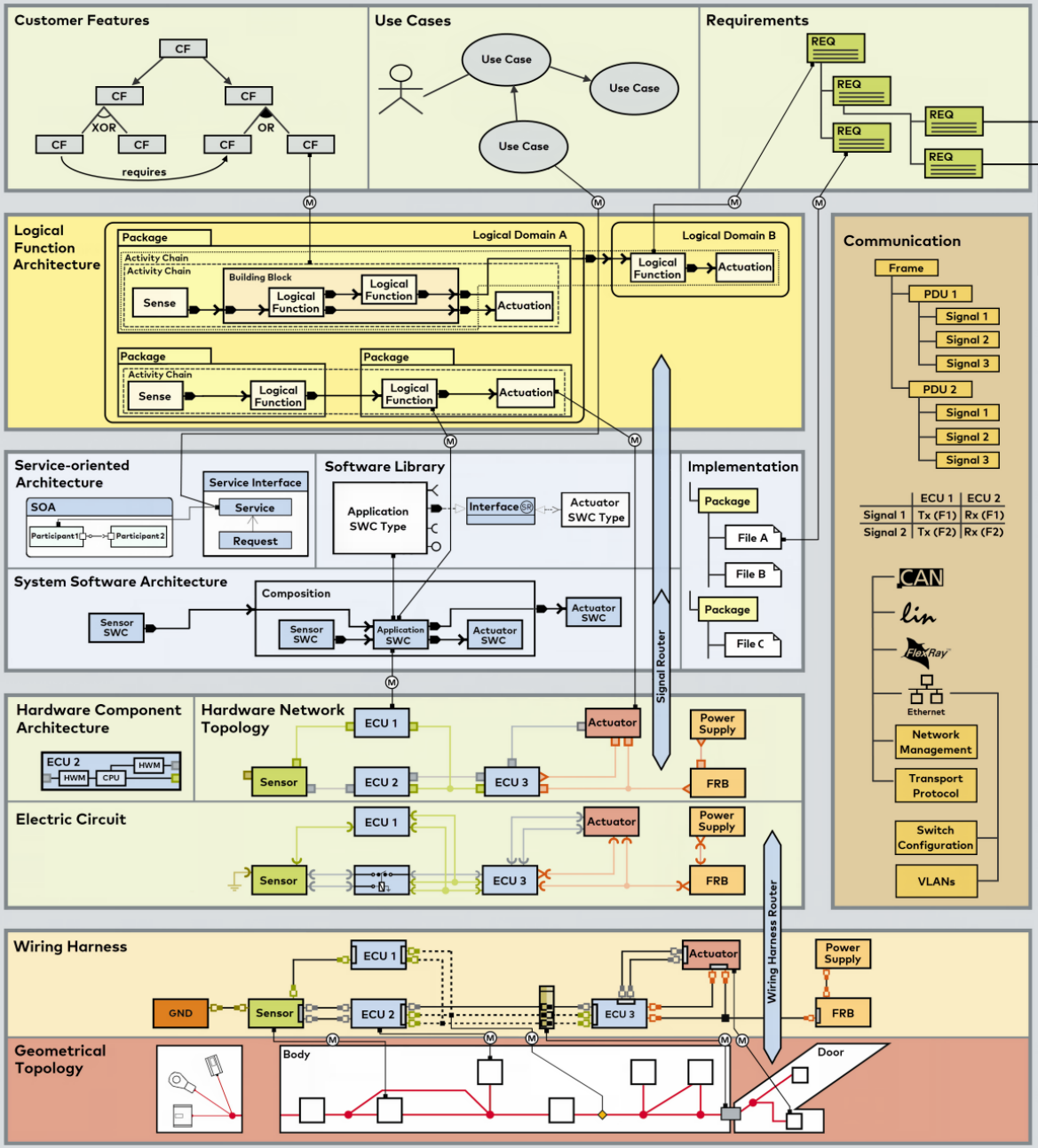
- **ISO 26262 conform** planning and tracking of safety activities.
- **ISO 26262 conform** approach to requirements, change, configuration and test management is ensured.
- **Bi-directional traceability** of safety goals and safety requirements throughout the entire development process.
- The **impact of safety-relevant changes** across all development artifacts is automatically analysed to ensure all appropriate actions are taken.
- ISO 26262 conform **safety cases** as an integral part of project configuration management:
  - Safety case is developed and maintained in parallel with the product development.
  - Dependencies between development artifacts ensure consistency of the safety case.

Safety case: Goal Structuring Notation (GSN)

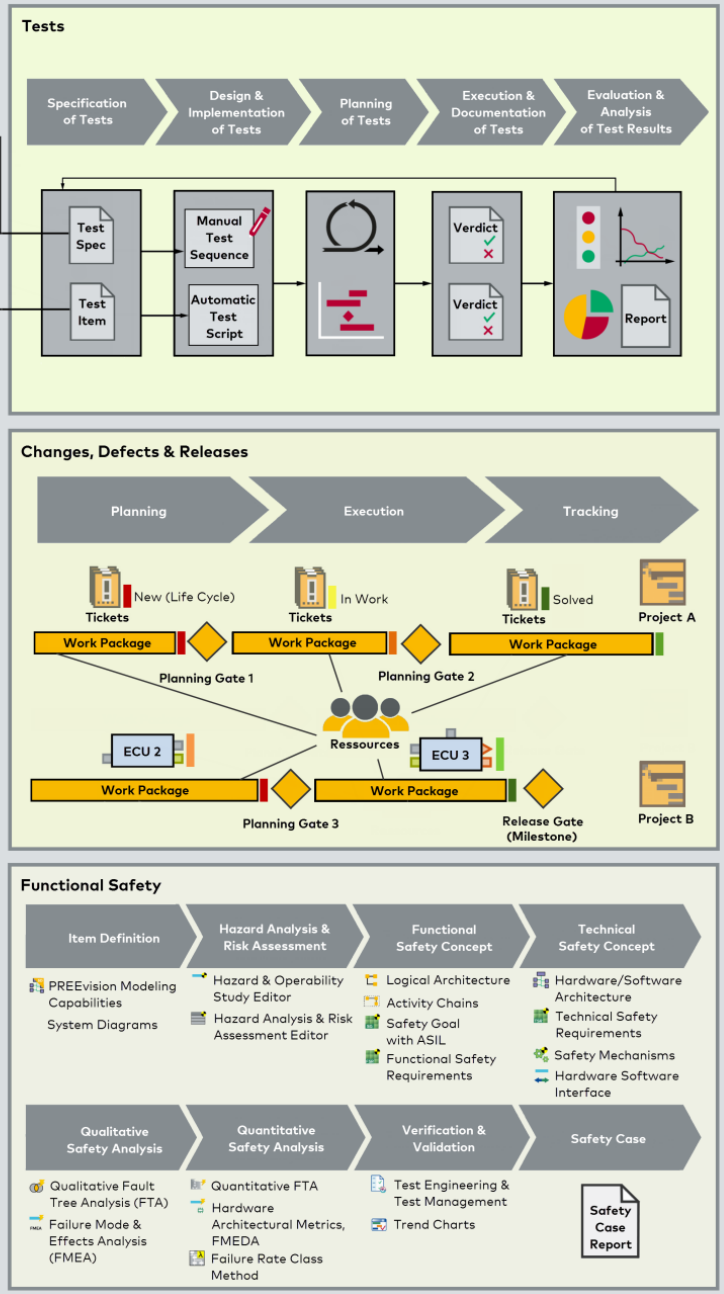


Evidence in the safety case directly references versioned artefacts in the underlying configuration management databank. The impact of changes to these artefacts can be directly traced in the safety case.

PREEvision Layers



Process & Team Support



Thank you for your attention.

For detailed information about Vector
and our products please have a look at:
www.vector.com

Authors:
Dr. Clemens Reichmann
Productline Process Tools
Vector Informatik GmbH, Stuttgart
aquintos GmbH, Karlsruhe