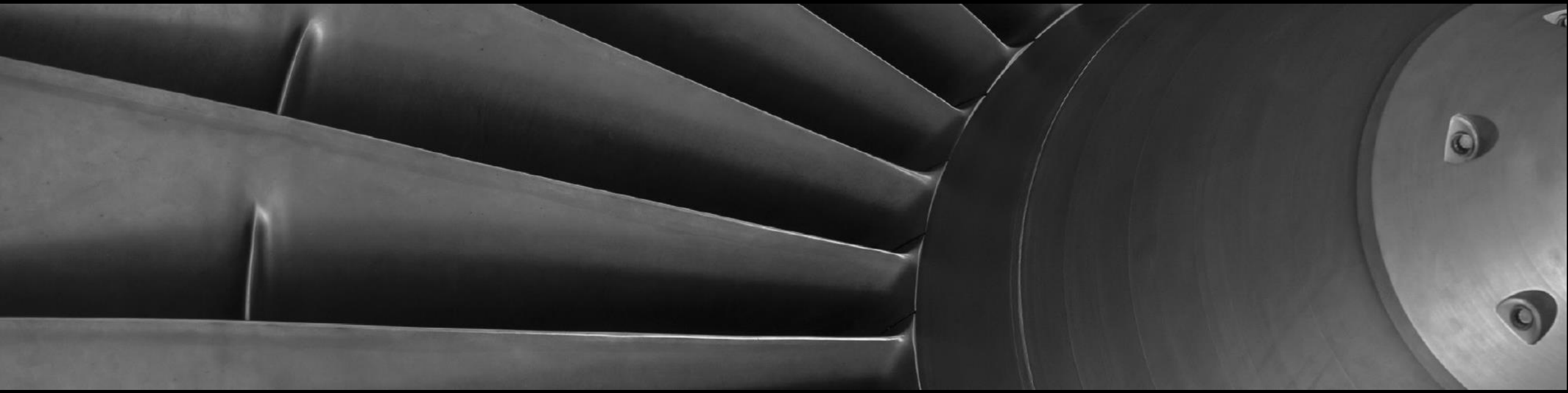


EnCo Software – Project C-SOX

Outline

1. Introduction EnCo & SOX2

2. Project C-SOX

Introduction EnCo & SOX2

EnCo Software GmbH

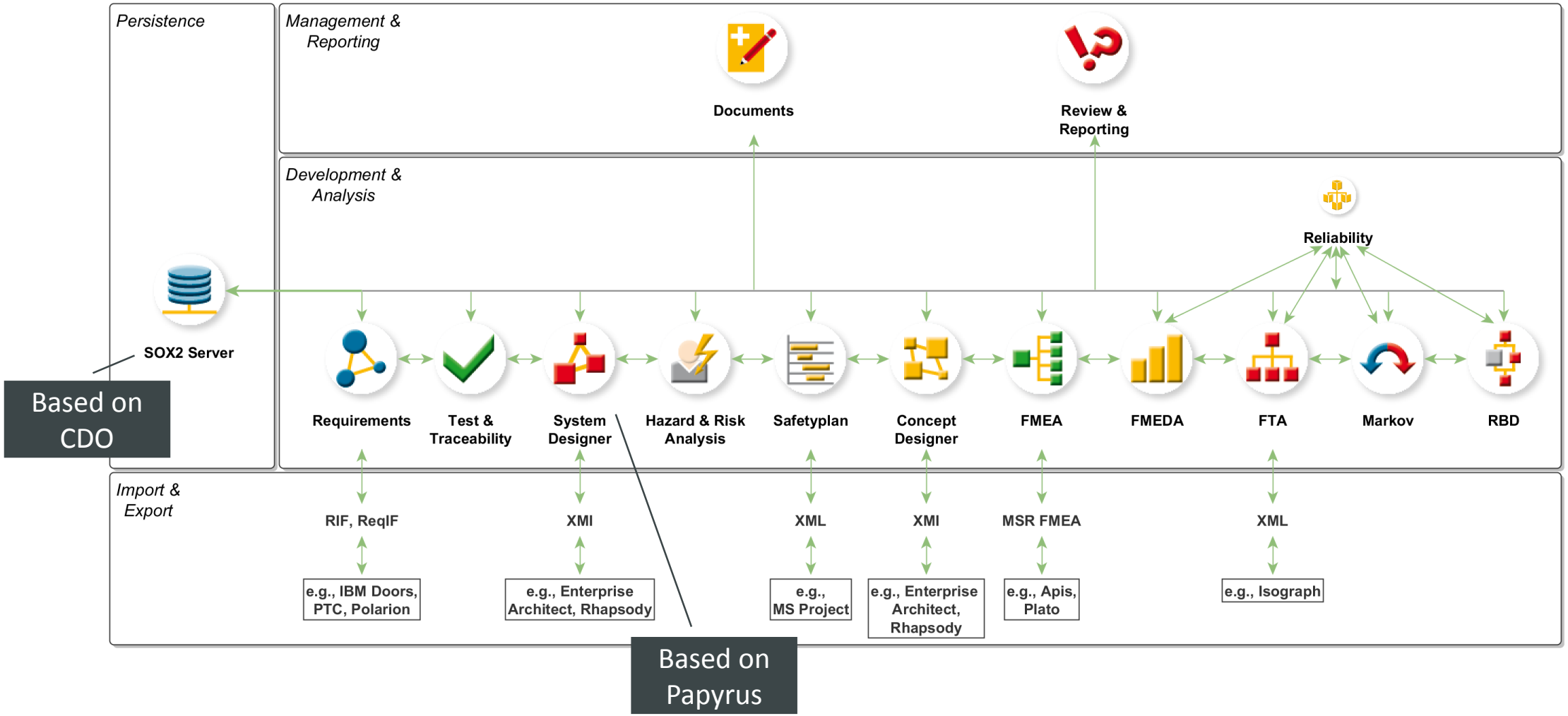
- Founded in 2007; now based in Munich, Germany
- Training, consulting and operational support in functional safety (ISO 26262)
- Since 2009: Focus on development of tool suite *Safety Office X2* (*SOX2*) for functional safety
- Resellers: China, Japan, Korea
- Research projects:
  - *InTelekt*: Safety & reliability of power electronics in electric vehicles, national funding (BMBF)

    Fraunhofer, BOSCH, Continental, SCHAEFFLER, BERNER & MATTNER AN ASSYSTEM COMPANY, ZF, RWTH RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
  - *qSafe*: Semi-automated generation of safety analyses, national funding (BMWi)

    TUM TECHNISCHE UNIVERSITÄT MÜNCHEN, INVENSITY CONSULTING·ACADEMY·INNOVATION
- Customers & partnerships:

  BOSCH, SIEMENS, KNORR-BREMSE, AUTOMOTIVE LIGHTING, MAGNA MAGNA POWERTRAIN, Continental, Honeywell, ifm electronic, VW, LG, HARMAN, 北汽新能源 BAIC BJEV, ZF Lenksysteme, ZF, Deutsche ACCUmotive

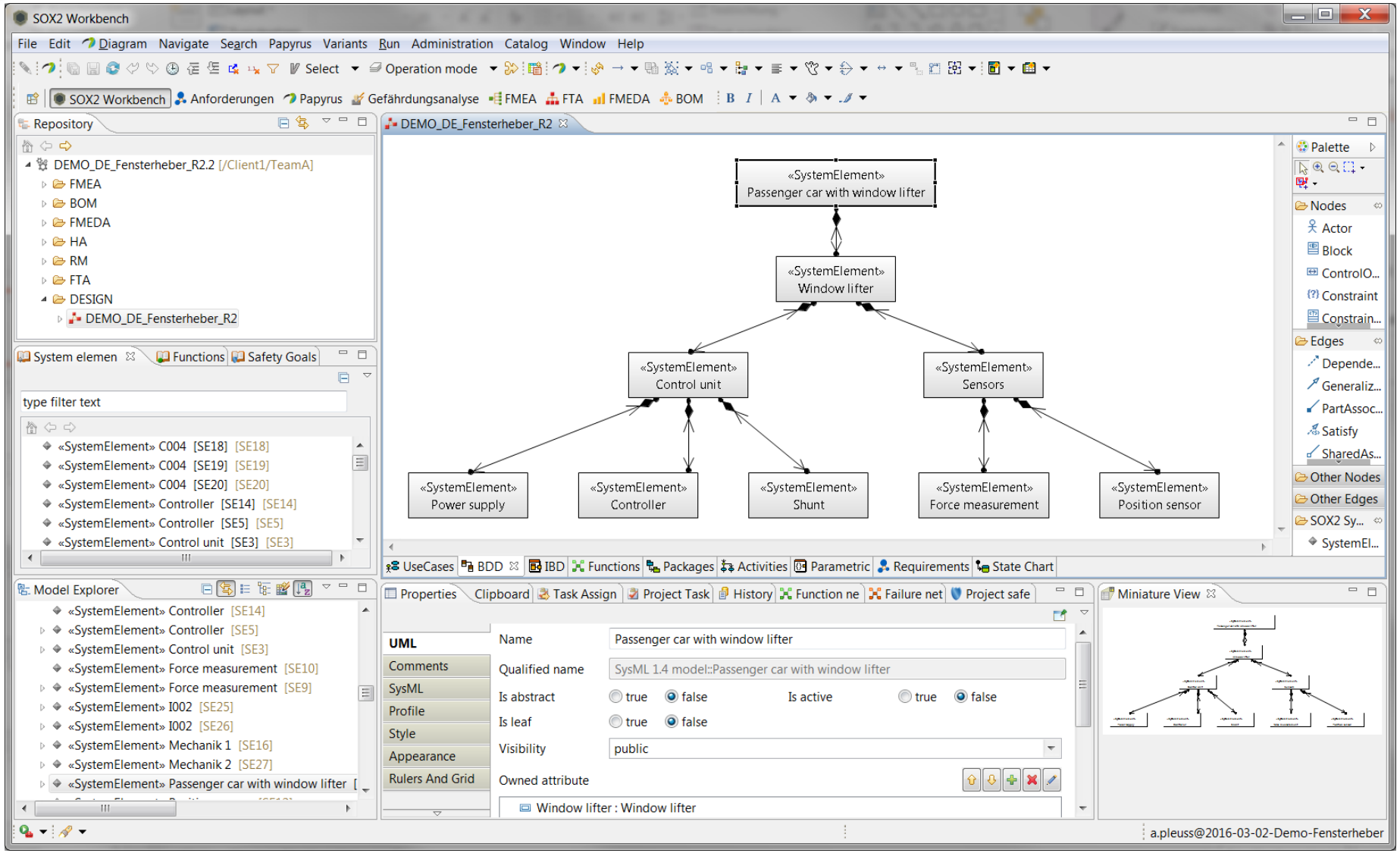
SOX2 - Modules



SOX2: Initial Workbench

Open multiple perspectives, customize them & switch between them

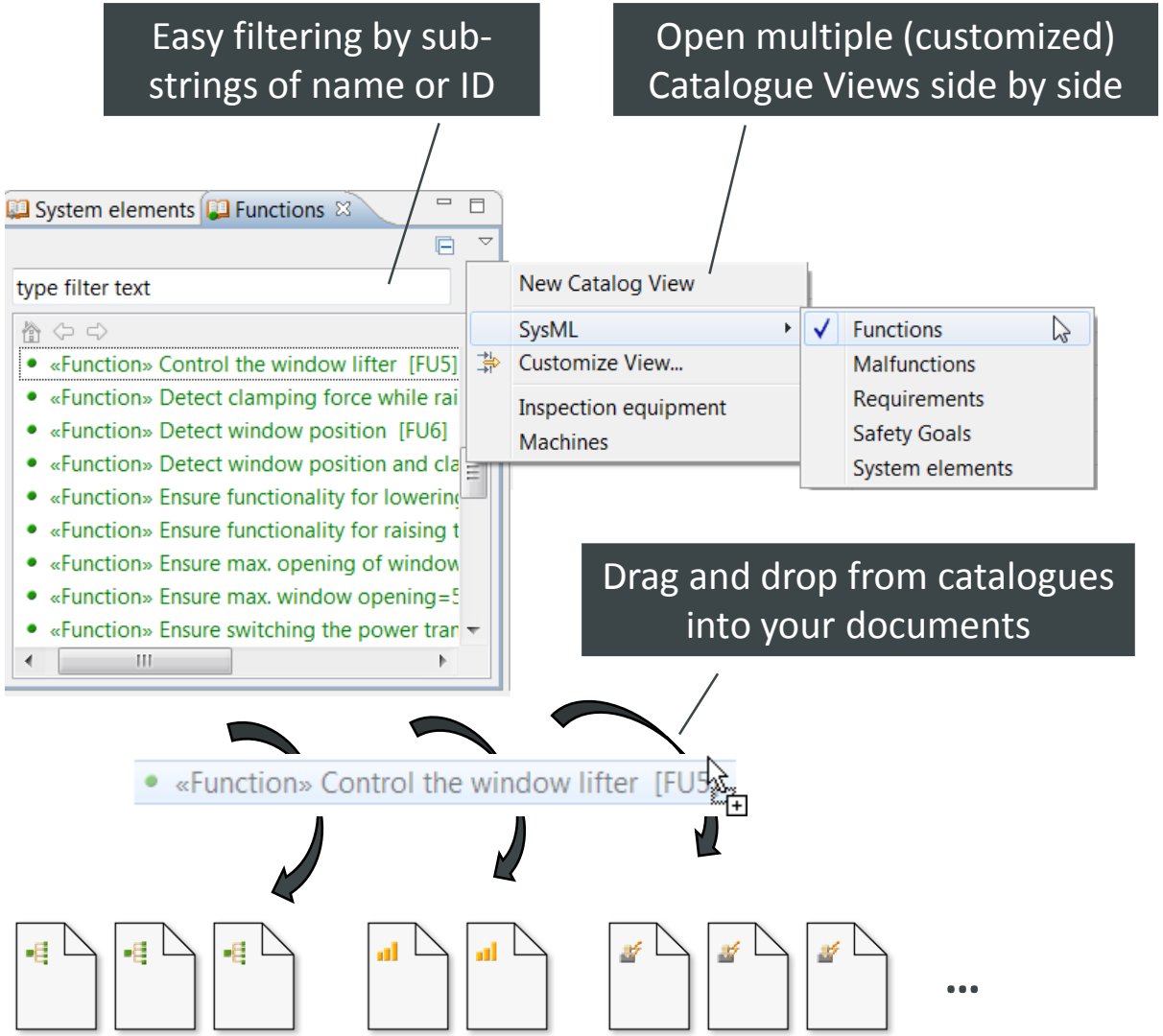
System Designer (SD) – Overview



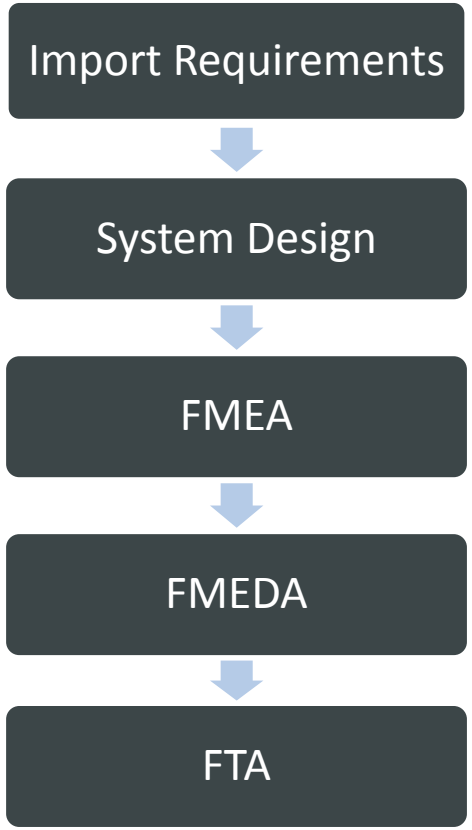
Module Integration: Catalogues

- Elements relevant in multiple modules can be re-used project-wide
- Re-use „by reference“, i.e., changes at one place are reflected project-wide (tool-supported consistency)
- Catalogue View provides list of all available elements of a certain type

- Catalogue View available for:
  - System Elements
  - Functions (and subtypes such as Diagnoses)
  - Malfunctions
  - Safety Goals
  - Requirements
  - Inspection equipment, Machines (for Process FMEAs)
  - Project Tasks and Team Members (displayed in specific views)



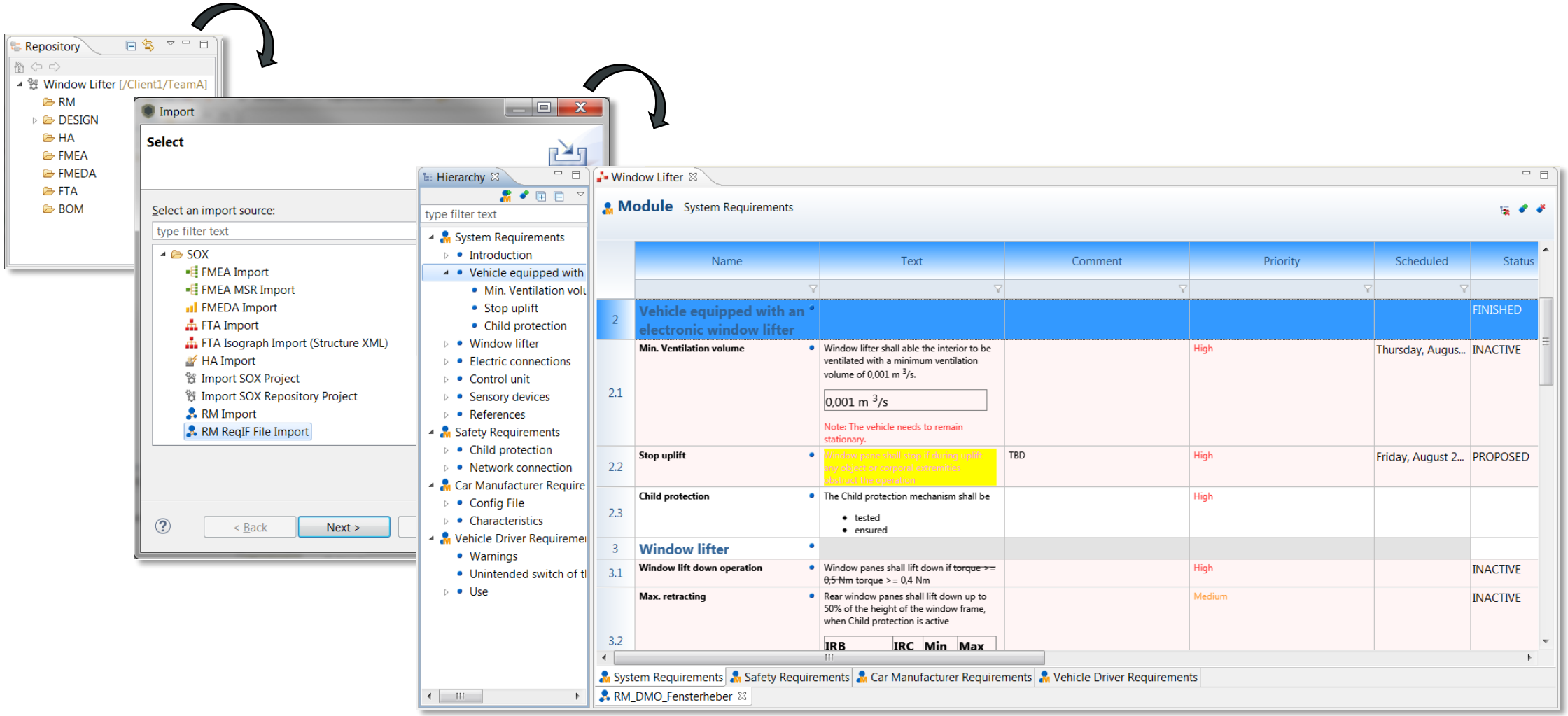
Example Case with SOX2



[1] except BOM and FMEDA

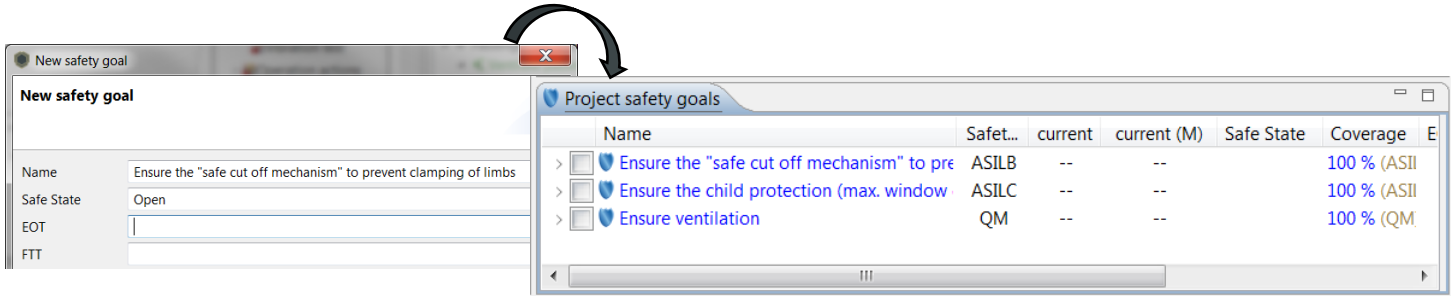
Requirements: Create or Import Requirements

- Create an empty project and import existing requirements, e.g. in ReqIF or Excel format

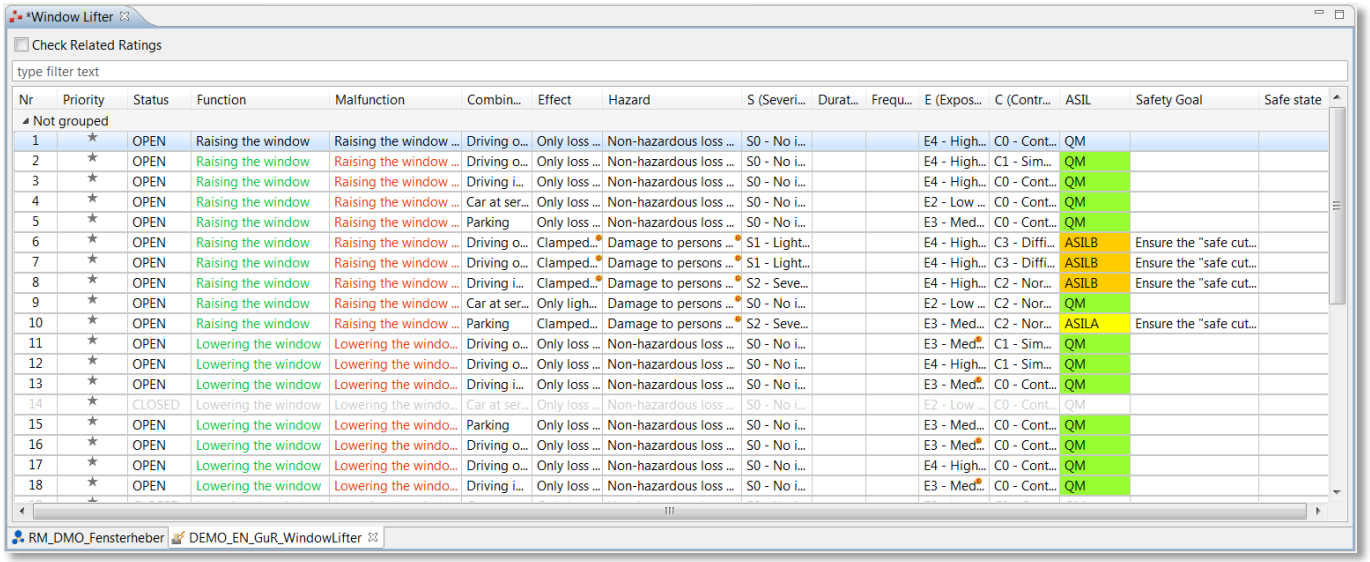


Requirements: Safety Goals

- Define Safety Goals



- Optionally, a Hazard and Risk Analysis can be performed to derive the safety goals

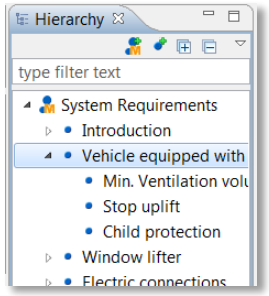


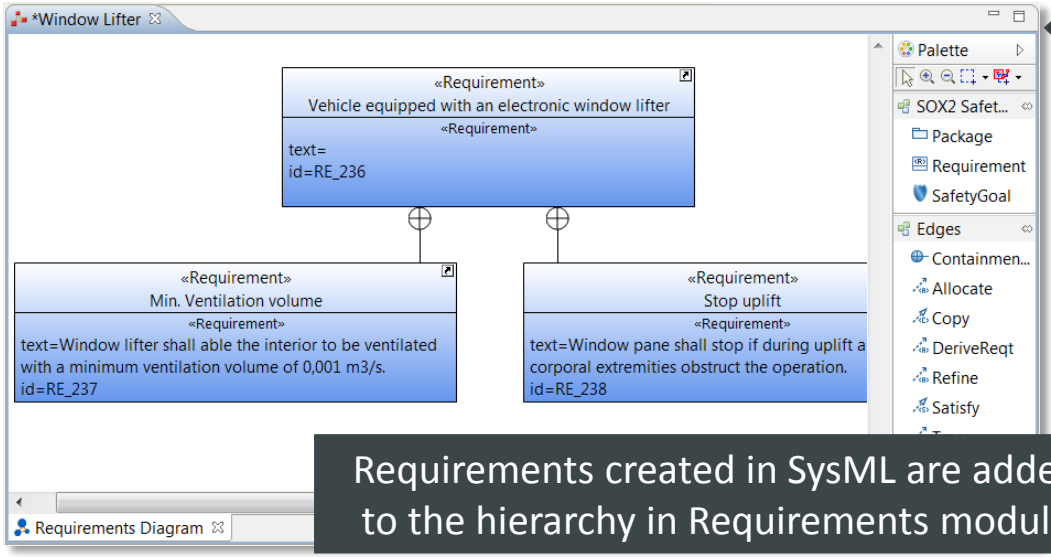
System Design: Requirements

- Requirements in Requirements module can be directly used in SysML via drag and drop
- Vice versa, changes and newly created Requirements from SysML are reflected in Requirements module

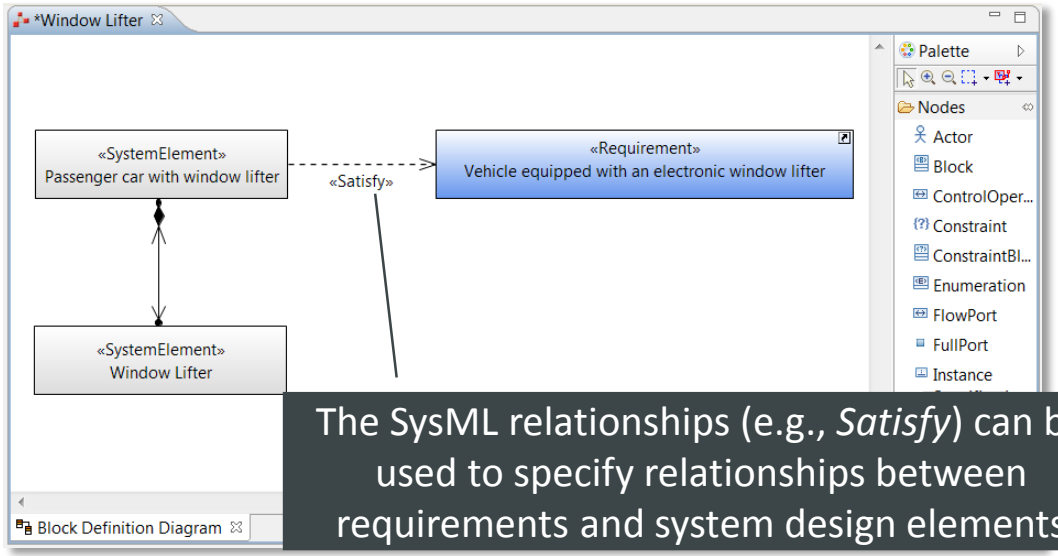
Optionally, derive SysML Requirements Diagram

Alternatively, use them directly in other SysML diagrams where needed





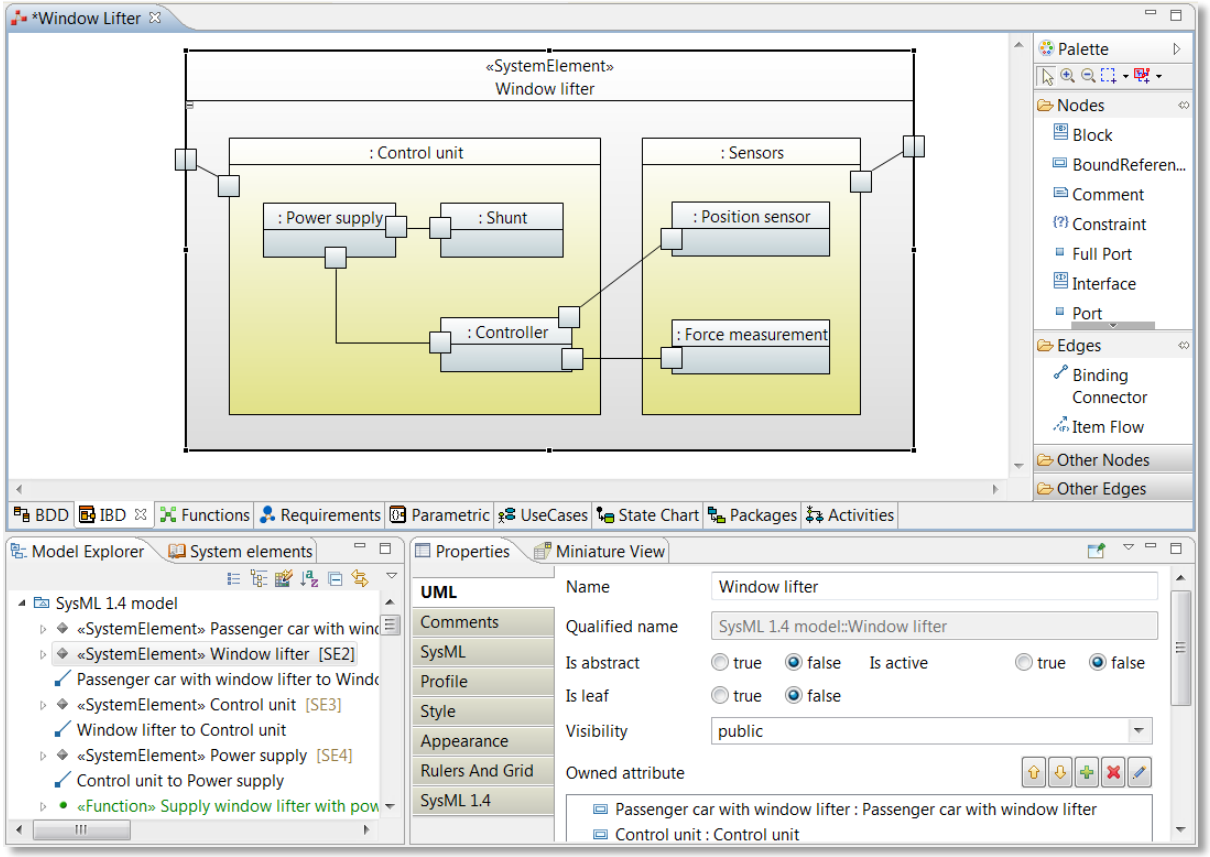
Requirements created in SysML are added to the hierarchy in Requirements module



The SysML relationships (e.g., *Satisfy*) can be used to specify relationships between requirements and system design elements

System Design: SysML diagrams

- Create your system design with SysML according to the needs of your project
- Comprehensive support of the SysML and UML standard



System Design: Stereotypes

- Use specific stereotypes to mark elements to be considered for safety analysis:
  - *System element*: Extension of a SysML block

    «SystemElement»
    Passenger car with window lifter

  - *Function*: Extension of a SysML block

    «Function»
    Ventilate Passenger Car

  - *Malfunction*: Extension of a SysML block

    «Malfunction»
    Passenger car not ventilated

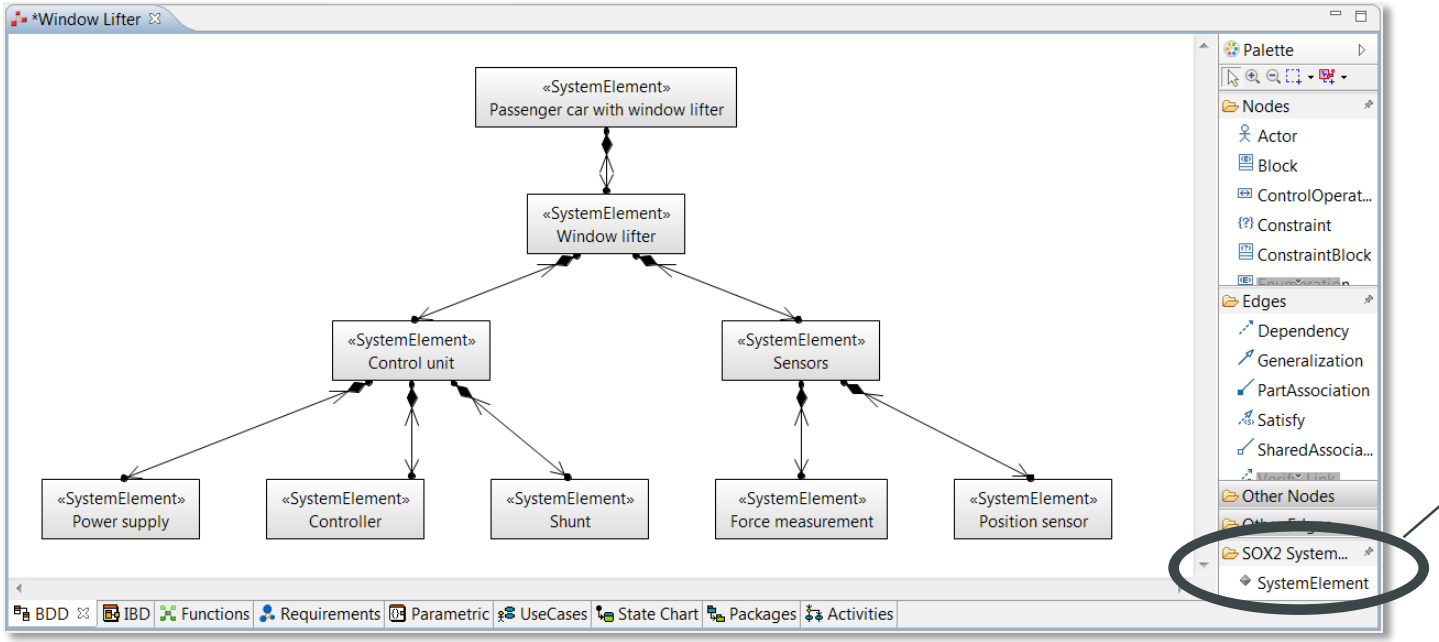
  - *Safety Goal*: Extension of a SysML Requirement

    «SafetyGoal» ASILC
    Ensure the child protection (max. window opening=50%)
    «SafetyGoal»
    safetyNorm=ISO26262_ASIL
    safetyLevel=ASILC

  - Additional stereotypes for specific sub-types of functions:
    Diagnosis, *Safety Function*, *Process Characteristics*, *Product Characteristics*

System Design: Hierarchy of System Elements

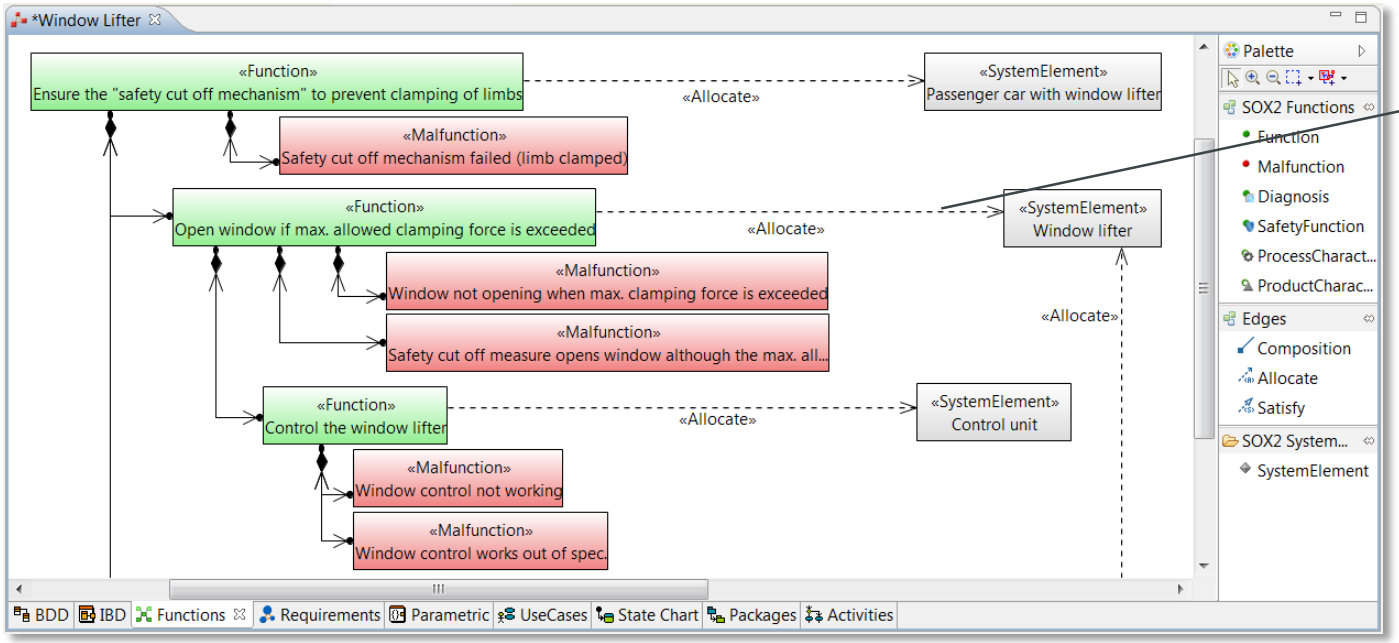
- SysML blocks that should be considered for the safety analysis as system elements are marked with the stereotype *SystemElement*
- The hierarchy of system elements is defined in a Block Definition Diagram (BDD) as usual in SysML



Create System Elements from the palette or add/remove stereotype *System Element* from/to blocks later

System Design: Hierarchy of Functions

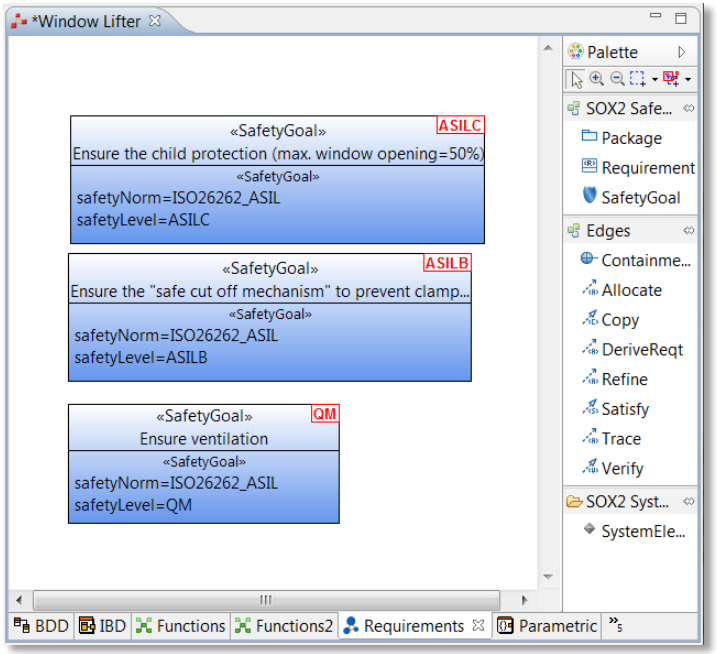
- Functions are marked with stereotype *Function*
- Hierarchy of functions is specified as a functions tree in a SysML Block Definition Diagram
- Possibility to specify and assign malfunctions directly in the system design

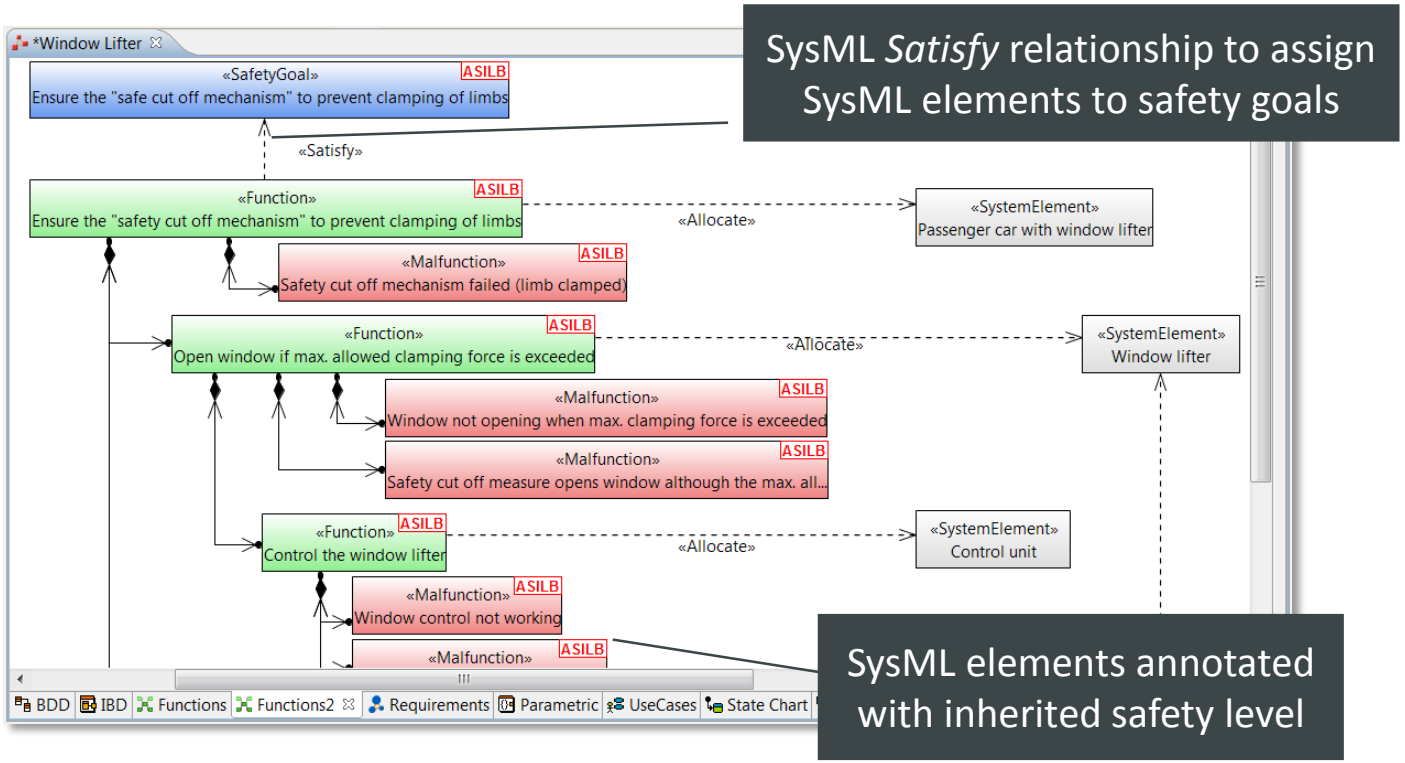


SysML *Allocate* relationship to allocate functions to system elements

System Design: Safety Goals

- All Safety Goals are available in the system design and can also be edited, created and assigned to system elements within the system design
- Assignment of Safety Goals to Malfunctions is represented in SysML via SysML *Satisfy* relationship
- Safety Classifications are calculated for all elements directly or indirectly related to a safety goal and can be displayed within SysML diagrams



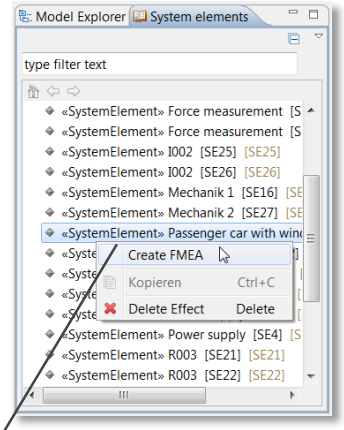


SysML *Satisfy* relationship to assign SysML elements to safety goals

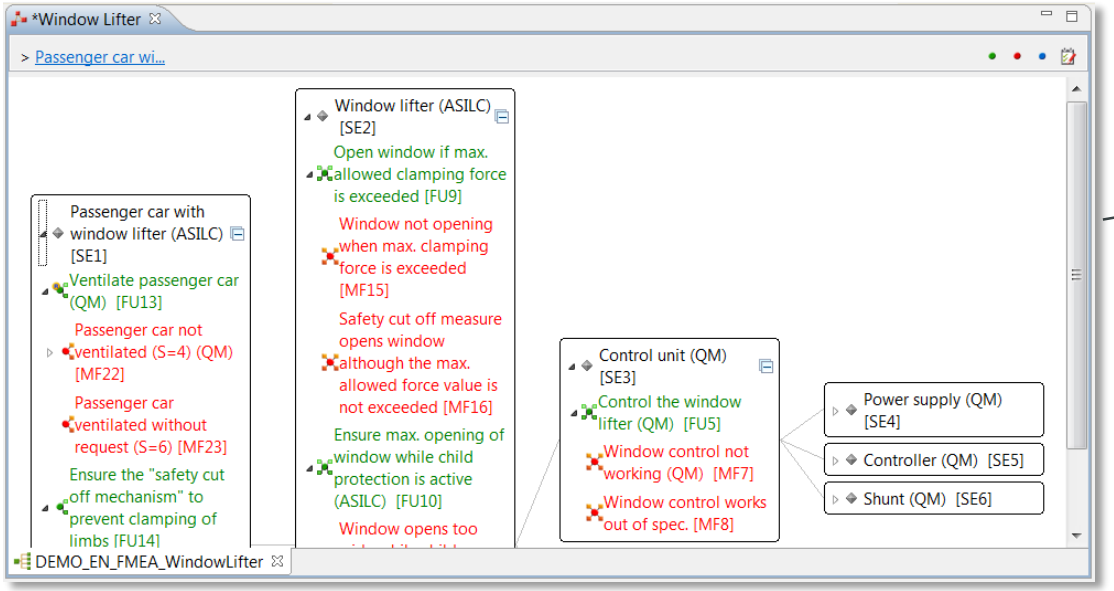
SysML elements annotated with inherited safety level

FMEA: Derive FMEA from System Design

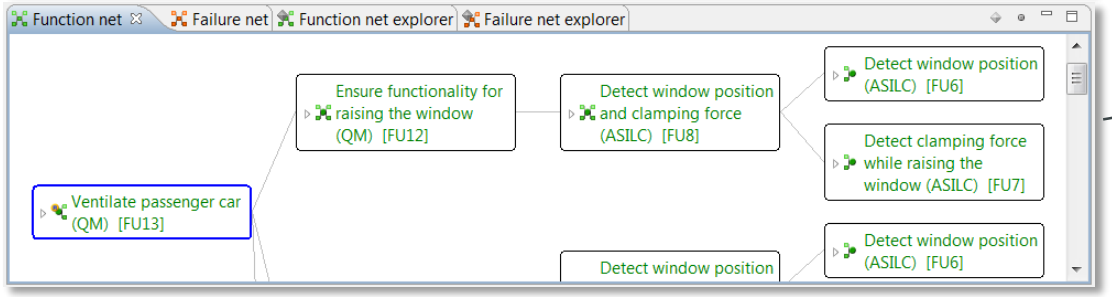
- The structure of an FMEA can be automatically derived from system design
- Irrelevant elements from system design can be omitted



Select root system element in catalogue and select *Create FMEA*



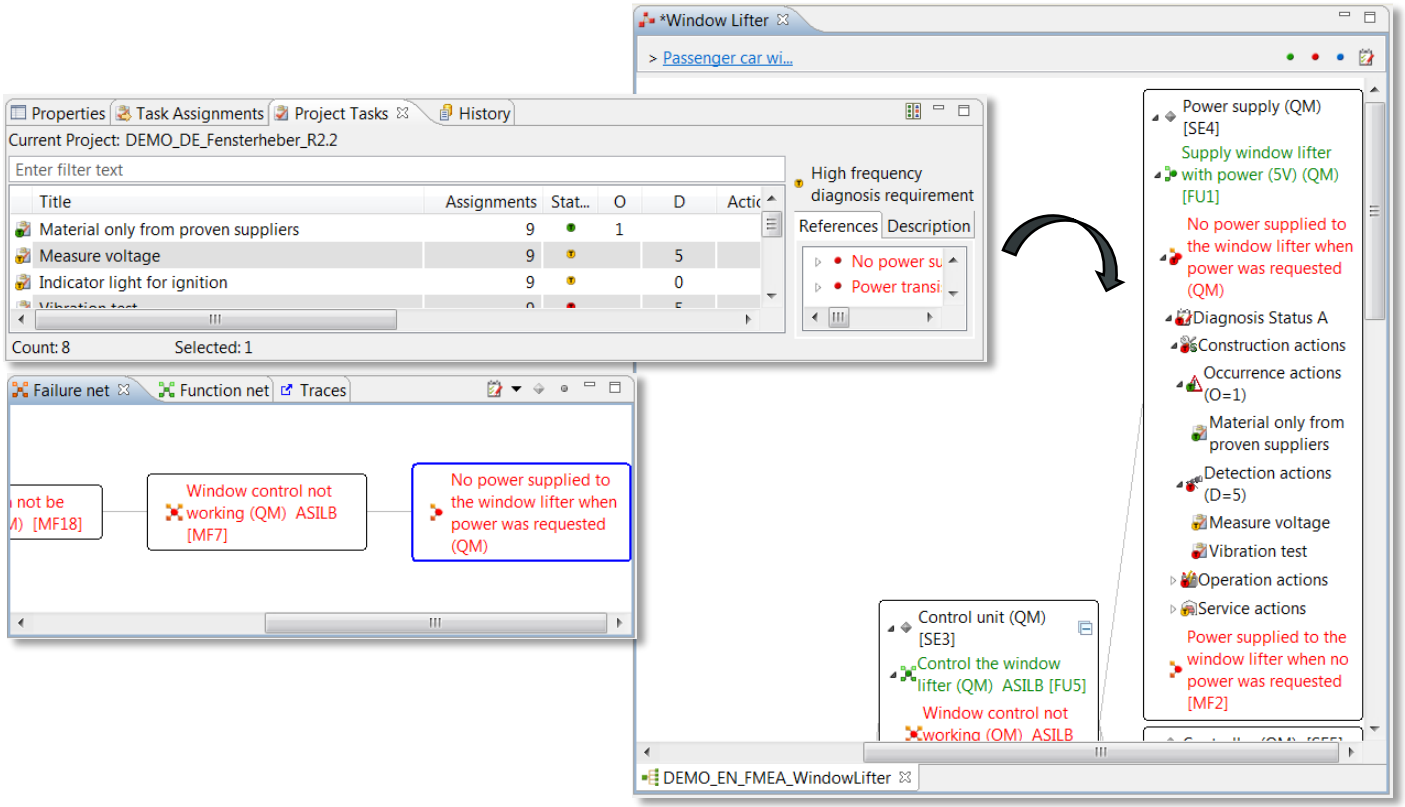
Corresponds to system design



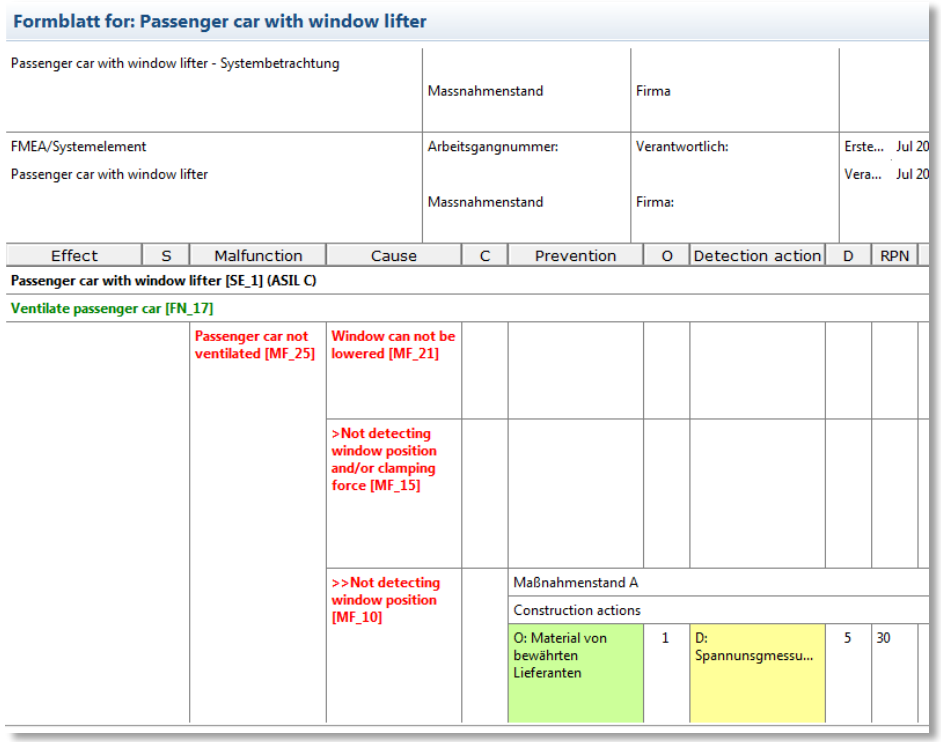
Corresponds to system design

FMEA: Finalize FMEA

- Complete the FMEA (define failure net, define actions, etc.)
- Changes/additions to system elements, functions, malfunctions can be specified directly within the FMEA and are propagated back to system design

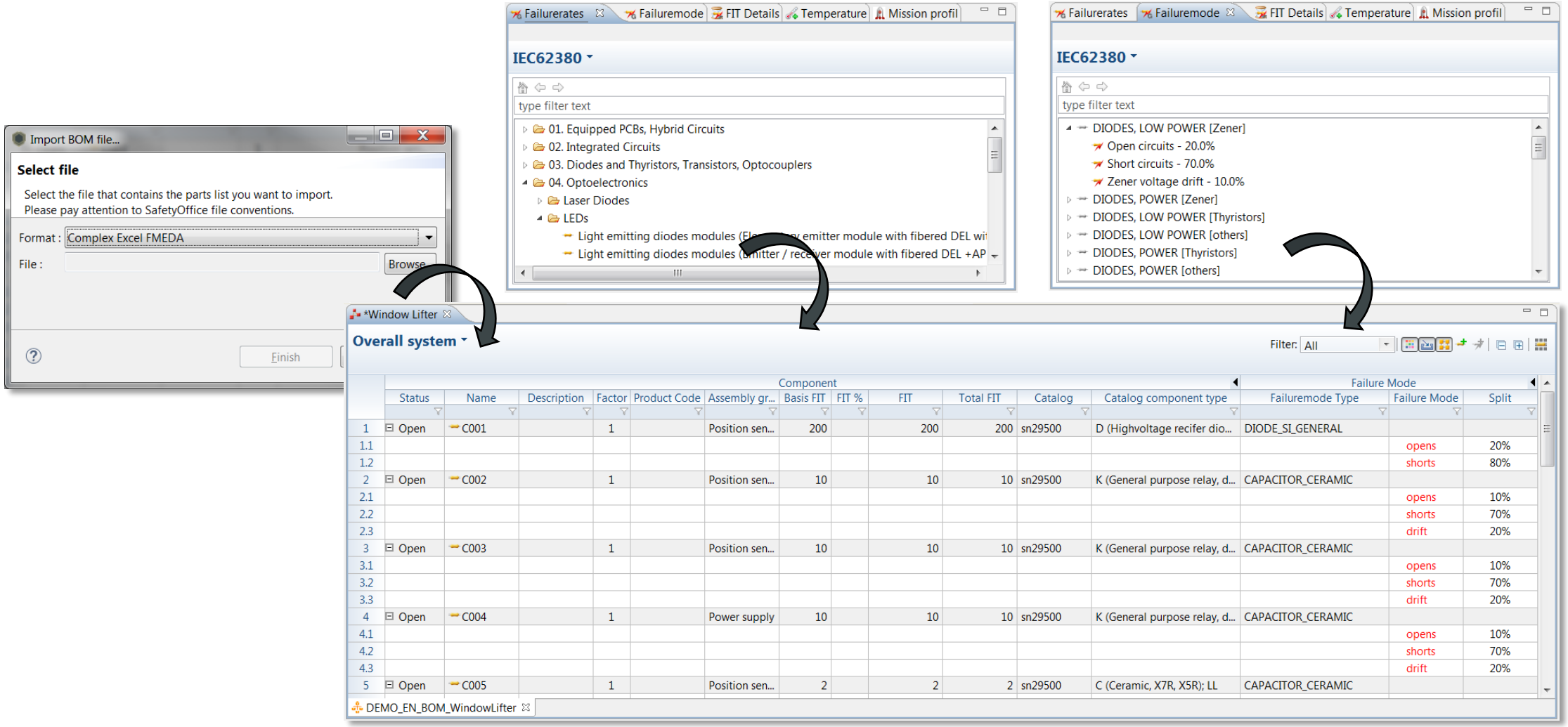


Generation of reports



BOM: Create or Import BOM

- Import a BOM or create one using the built-in failure rate catalogues and failure mode catalogues



	Component												Failure Mode		
	Status	Name	Description	Factor	Product Code	Assembly gr...	Basis FIT	FIT %	FIT	Total FIT	Catalog	Catalog component type	Failuremode Type	Failure Mode	Split
1	Open	C001		1		Position sen...	200		200	200	sn29500	D (Highvoltage recifer dio...	DIODE_SI_GENERAL		
1.1														opens	20%
1.2														shorts	80%
2	Open	C002		1		Position sen...	10		10	10	sn29500	K (General purpose relay, d...	CAPACITOR_CERAMIC		
2.1														opens	10%
2.2														shorts	70%
2.3														drift	20%
3	Open	C003		1		Position sen...	10		10	10	sn29500	K (General purpose relay, d...	CAPACITOR_CERAMIC		
3.1														opens	10%
3.2														shorts	70%
3.3														drift	20%
4	Open	C004		1		Power supply	10		10	10	sn29500	K (General purpose relay, d...	CAPACITOR_CERAMIC		
4.1														opens	10%
4.2														shorts	70%
4.3														drift	20%
5	Open	C005		1		Position sen...	2		2	2	sn29500	C (Ceramic, X7R, X5R); LL	CAPACITOR_CERAMIC		

FMEDA: Create FMEDA from BOM

- Safety goals can be taken from the project safety goals / system design
- Diagnoses are considered as specific functions and, hence
  - Can be taken from catalogue
  - Newly added diagnoses are added to the system design and the catalogue

Project safety goals

Name	Safet...	current	current (M)	Safe State	Coverage	E
Ensure the "safe cut off mechanism" to pre	ASILB	--	--		100 % (ASII	
Ensure the child protection (max. window	ASILC	--	--		100 % (ASII	
Ensure ventilation	QM	--	--		100 % (QM	

Diagnoses

type filter text

Name	Code	FMC Single	FMC Mult...	Thres
SM-Controller				
Startup Test	SM_Rege_01	50%	50%	
SM-Force measurement				
Plausibilisation	SM_KrSe_02	90%	99%	
internal self-test	SM_KrSe_01	99%	90%	
SM-Position sensor				
Plausibilisation	SM_PoSe_01	90%	90%	
internal self-test	SM_PoSe_02	99%	99%	
SM-Power supply				
Power test	SM_SpVe_01	99%	90%	

*Window Lifter

Overall system

Filter: All

BOM: DEMO_EN_BOM_WindowLifter

	Component		Failure Mode		Ensure the "safe cut off mechanism" to prevent clamping of limbs											SR (SP)	Relevance (SP)	Diagnosis (S
	Status	Name	Failure Mode	Split	SR (SP)	Relevance (SP)	Diagnosis (SP)	FMC (SP)	λ (SP)	SR (MP)	Relevance (M...	Diagnosis (M...	FMC (MP)	λ (MP)	CCF			
1	Open	C001																
1.1			opens	20%		100%		0%	0		100%		0%	40			100%	
1.2			shorts	80%		100%		0%	0		100%		0%	160			100%	
2	Open	C002																
2.1			opens	10%	✕	100%	SM_PoSe_02	99%	0		100%	SM_PoSe_02	99%	0.01		✕	100%	SM_PoSe_0
2.2			shorts	70%	✕	100%	SM_PoSe_02	99%	0	✕	100%	SM_PoSe_02	99%	0.07		✕	100%	SM_PoSe_0
2.3			drift	20%		100%	SM_PoSe_01	90%	0	✕	100%	SM_PoSe_01	90%	0.2			100%	SM_PoSe_0
3	Open	C003																
3.1			opens	10%	✕	100%	SM_PoSe_02	99%	0		100%	SM_PoSe_02	99%	0.01		✕	100%	SM_PoSe_0
3.2			shorts	70%	✕	100%	SM_PoSe_02	99%	0	✕	100%	SM_PoSe_02	99%	0.07		✕	100%	SM_PoSe_0
3.3			drift	20%		100%	SM_PoSe_01	90%	0	✕	100%	SM_PoSe_01	90%	0.2			100%	SM_PoSe_0
4	Open	C004																
4.1			opens	10%	✕	100%	SM_SpVe_01	99%	0	✕	100%	SM_SpVe_01	90%	0.1		✕	100%	SM_SpVe_0

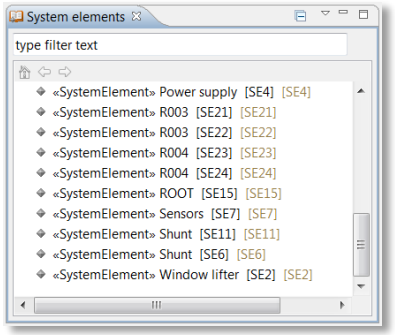
DEMO_EN_BOM_WindowLifter | DEMO_EN_FMEDA_WindowLifter

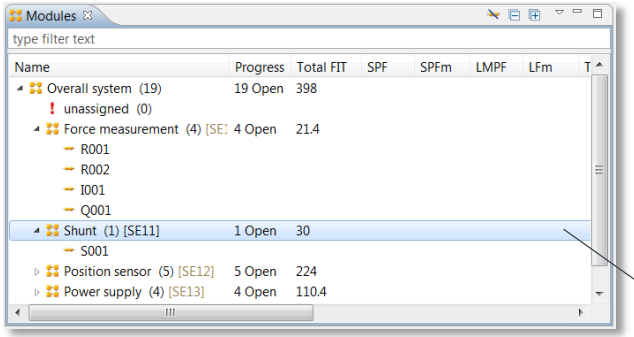
FMEDA: Modules

- Assign components to modules
- A module corresponds to a system element from system design

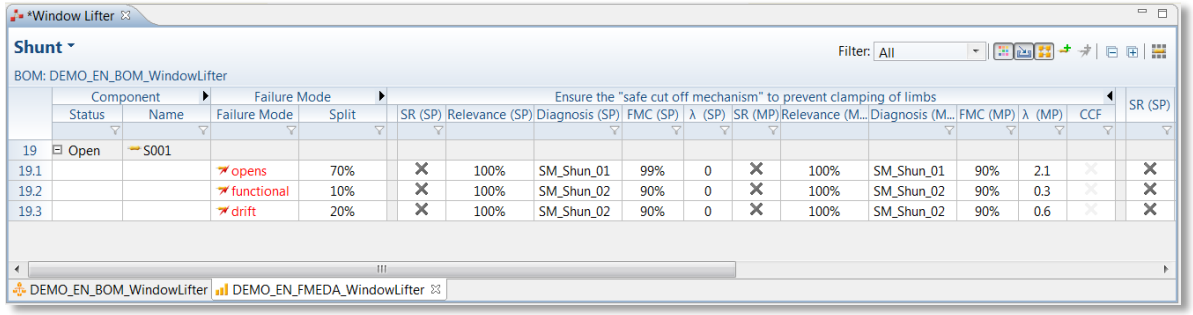
Use system elements from system design as modules

New modules are added to system design



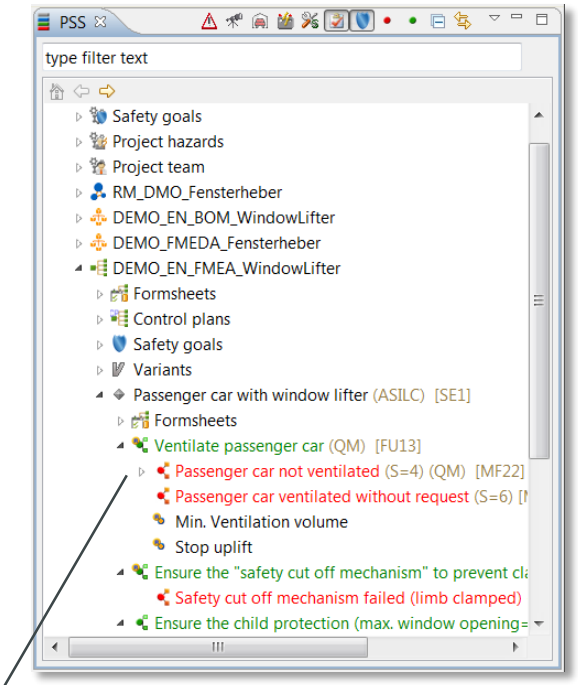


Filtering according to selected module



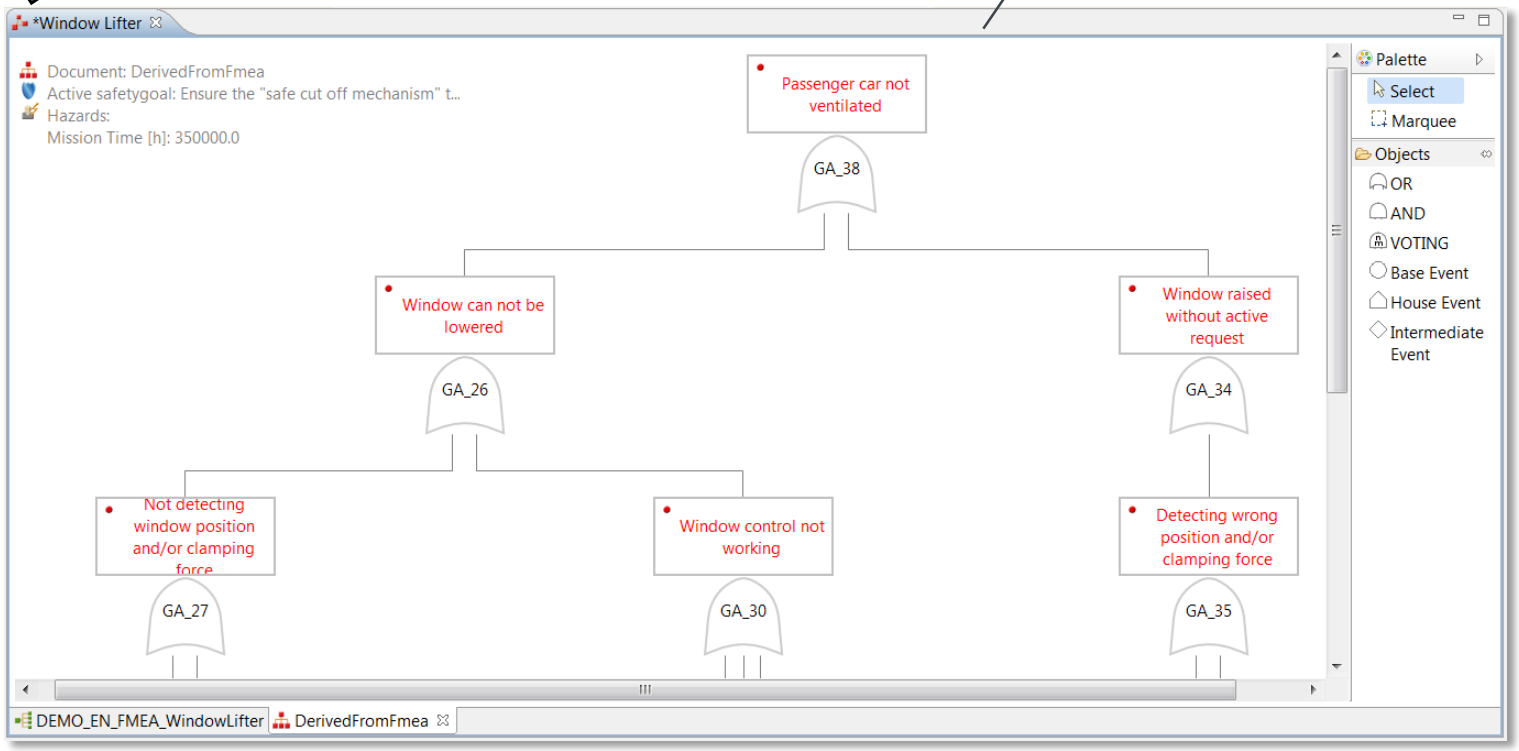
FTA: Derive FTA from FMEA

- An FTA can be automatically derived from the FMEA



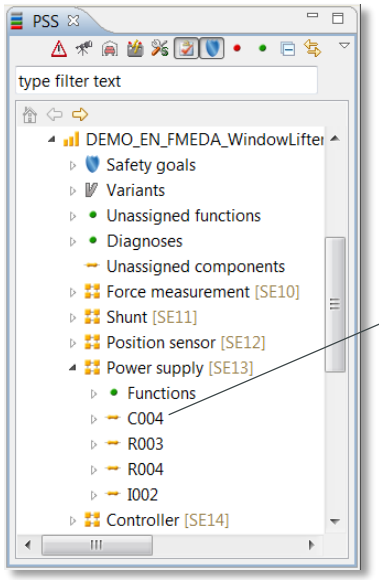
Drag Malfunction from FMEA as root node into FTA document

Generated FTA corresponds to the failure net

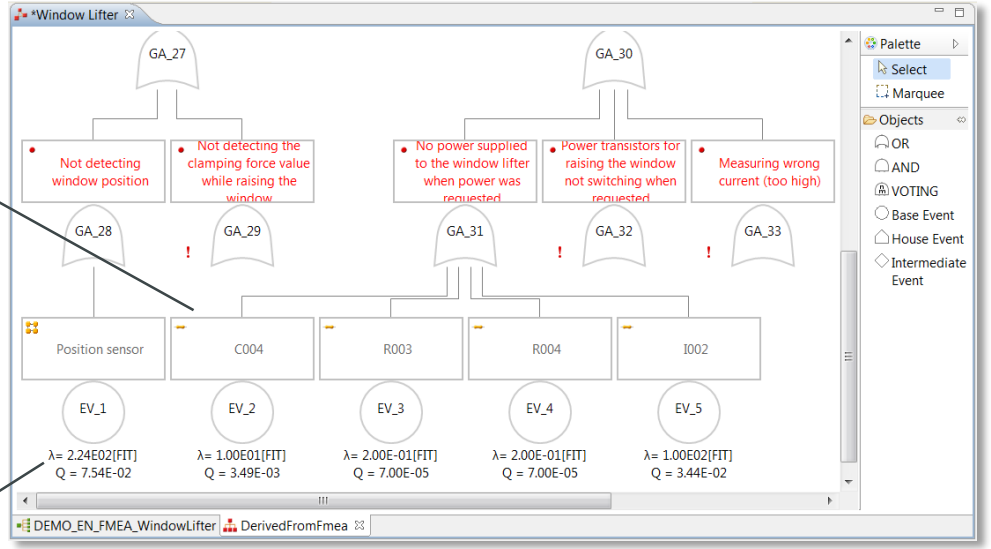


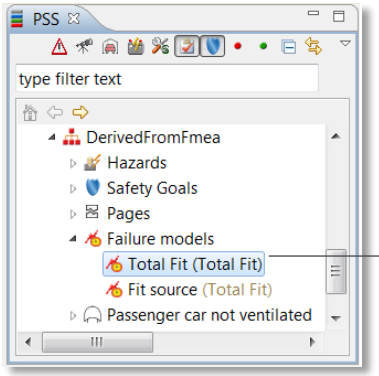
FTA: Finalize FTA

- Create base events, select failure models and calculate minimal cut sets and probabilities



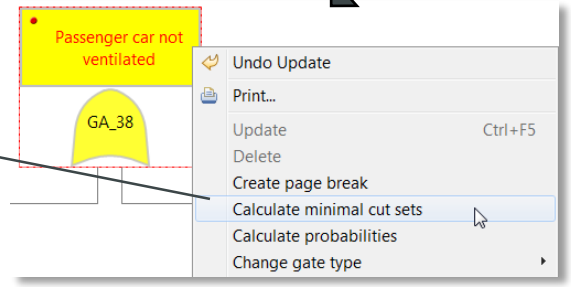
Drag and drop, e.g., Components from FMEDA as base events





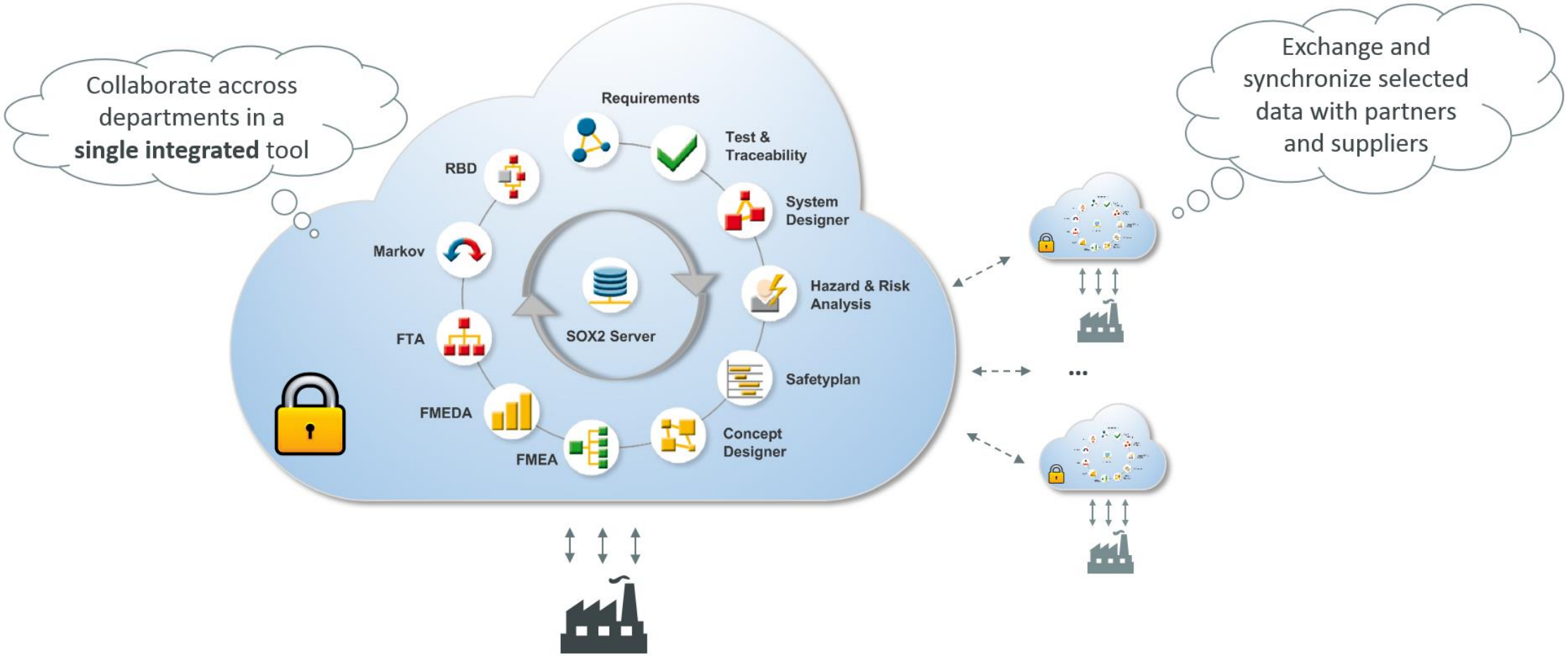
Drag and drop a failure model (e.g. total fit) to define source of probabilities

Calculate minimal cut sets and probabilities of root and intermediate events



Project C-SOX

Project *C-SOX*: SOX2 in the Cloud



Goals

- Multi-user collaboration based on a cloud server
- Cloud server: private cloud (hosted by customers)
  - Might be extended later on by public cloud server to provide easier access e.g., for academic use
- Support for very large models
- Web-based User Interface accessible via web browser
  - Still provide option to run HTML-based UIs in Eclipse RCP applications

- **Requires: Framework for graphical modelling (UML, SysML) supporting HTML-based UIs**
- Collaboration with CEA

Research Programme *SME Instruments*

- EU funding scheme for small- and medium sized enterprises (SMEs)
- Purpose: Boost single SMEs to bring innovations to market
- Very market-oriented, no research
- Phase 1: Feasibility study (optional)
  - Analysis of technical and commercial feasibility
  - Detailed planning for phase 2 (Business Plan)
  - Duration: 6 months
  - Funding: Fixed amount (50.000 Euro)
- Phase 2: Innovation project
  - Commercialize project
  - Duration: Typically 2 years
  - Funding: Up to 2.5 Mio Euro EU contribution
- Phase 3: Commercialization
  - Commercial exploitation

Current Status

HORIZON 2020

[PROJECT] **SOX2-Cloud** - Integrated Safety Engineering Platform for electrical and electronic systems for transportation
ID: 743519
Start date: 2016-11-01, **End date:** 2017-04-30
Electrical and electronic systems (Electrical/Electronic/Programmable Electronic Safety-related Systems – E/E/PE) play an important role in our lives and take over important decisions and safety-related functions. Accidents and hazards may arise due to technical defects in...
Programme: H2020-EU.3.4.
Record Number: 207103
Last updated on: 2016-11-29

- In Phase 1
- Report on Phase 1 to submit end of April
- Proposal for Phase 2 to submit beginning of June
- Supported by consulting company with strong success rate in this programme (EuraConsult)

Intended Project on “Cloud-based Graphical Modelling”

- Eclipse OSS project
- Four intended building blocks of contributions:
  1. Contributions from EnCo
  2. Allocate funding to CEA to contribute
  3. Contributions from other interested partners, e.g., from Polarsys IC
  4. OSS community

- Additional partners wanted
- LOI by interested parties (e.g., Polarsys IC) would help to secure funding

Contact

EnCo Software GmbH

Balanstr. 55
81541 München
Germany

Phone: +49 (89) 716 775 890
Fax: +49 (89) 716 775 899
Email: info@enco-software.com
www.enco-software.com