

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:

- *InTelegt*: Safety & reliability of power electronics in electric vehicles, national funding (BMBF)



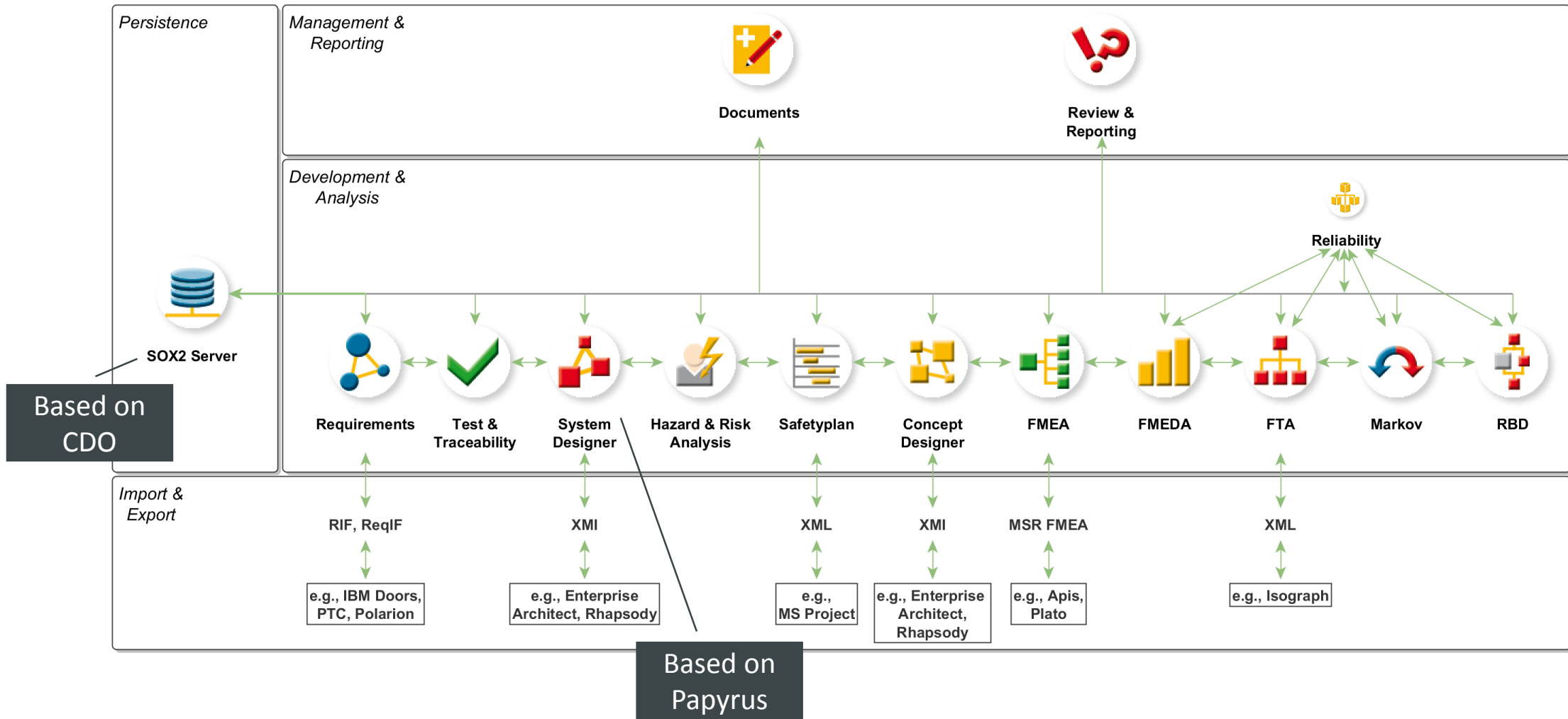
- *qSafe*: Semi-automated generation of safety analyses, national funding (BMW i)



- Customers & partnerships:

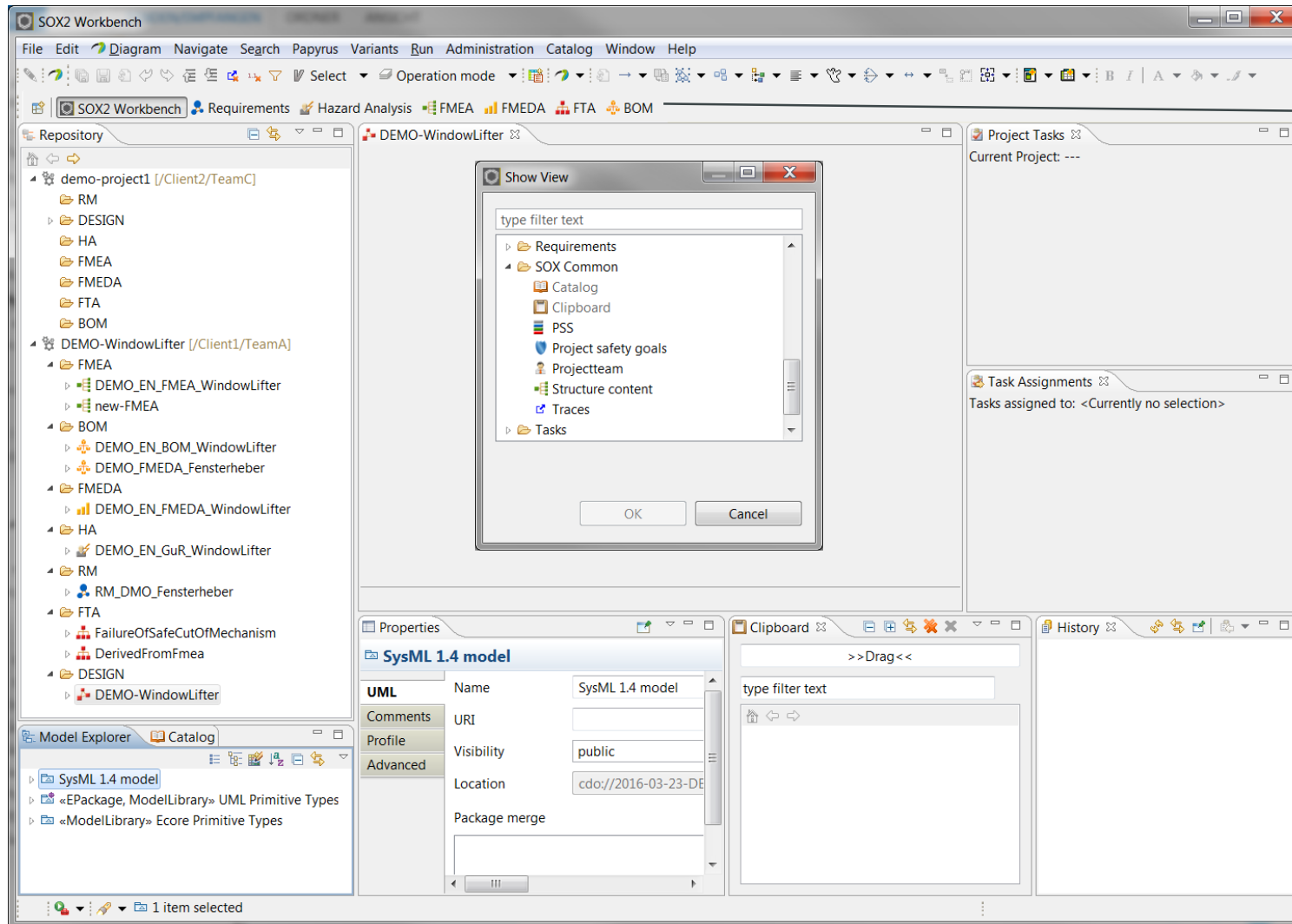


SOX2 - Modules

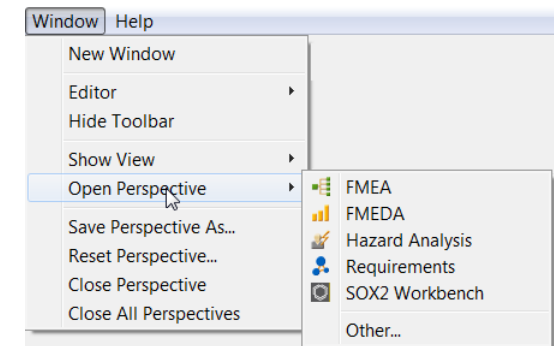




SOX2: Initial Workbench



Open multiple perspectives,
customize them & switch
between them





System Designer (SD) – Overview



The screenshot displays the SOX2 Workbench interface with a SysML diagram titled "DEMO_DE_Fensterheber_R2". The diagram shows a hierarchical structure of system elements:

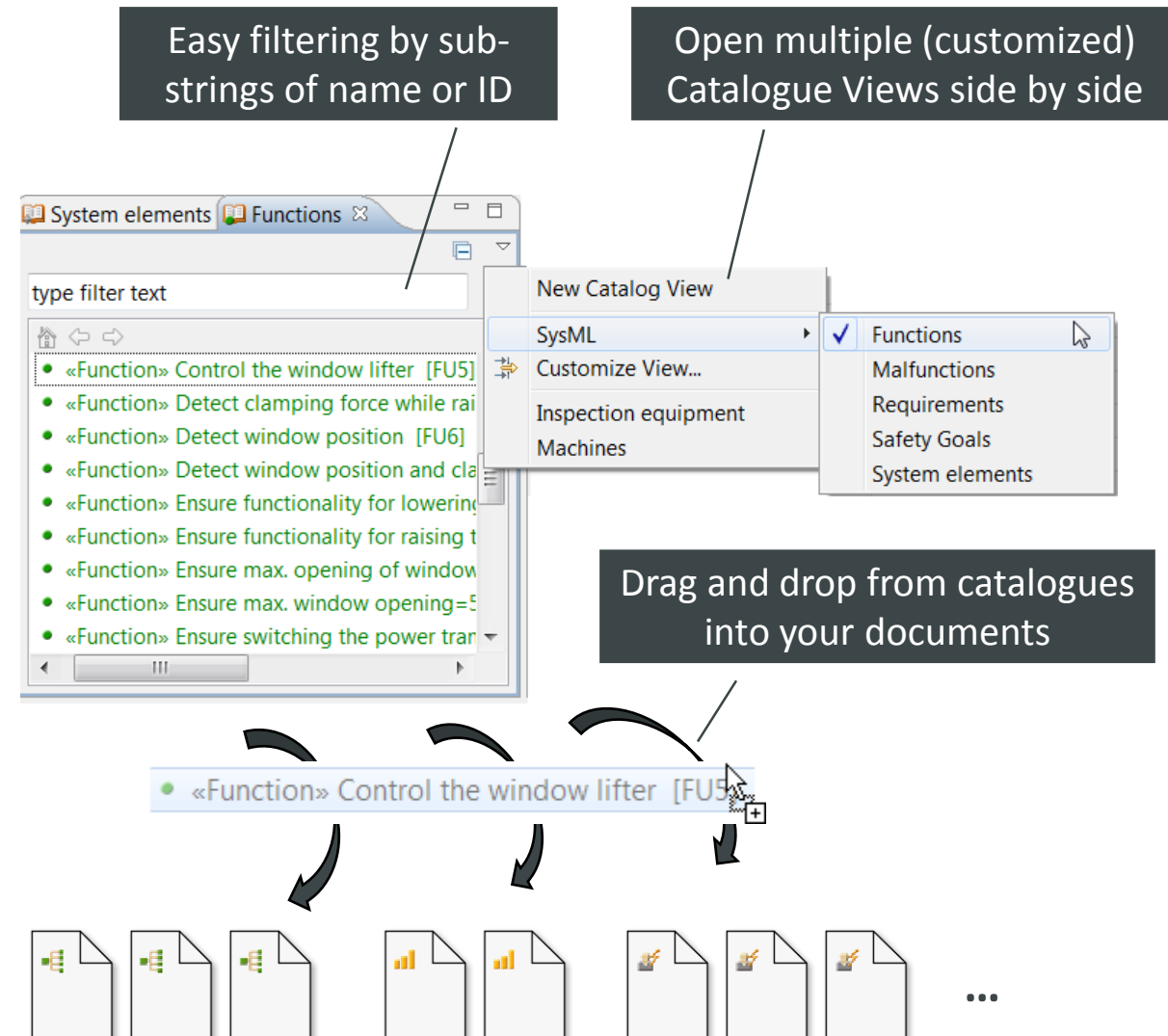
- «SystemElement» Passenger car with window lifter (Root)
 - «SystemElement» Window lifter
 - «SystemElement» Control unit
 - «SystemElement» Power supply
 - «SystemElement» Controller
 - «SystemElement» Shunt
 - «SystemElement» Sensors
 - «SystemElement» Force measurement
 - «SystemElement» Position sensor

The interface includes a Repository on the left showing the project structure, a Model Explorer at the bottom left listing system elements, a Properties window at the bottom center for the selected element, and a Miniature View at the bottom right.



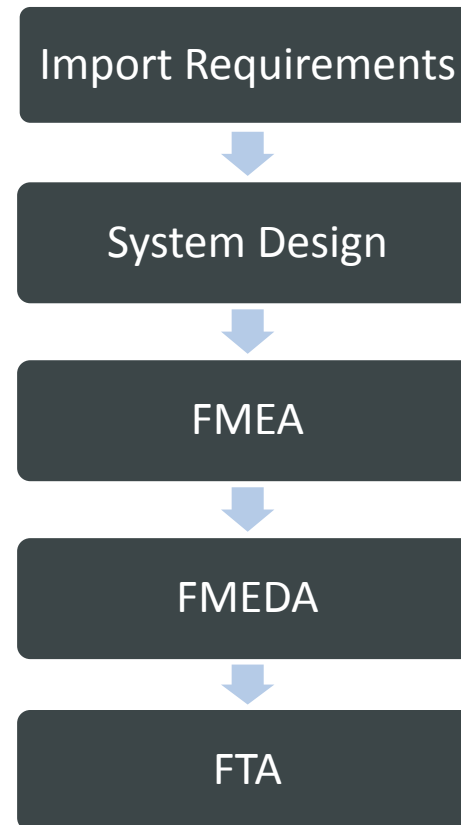
Module Integration: Catalogues

- 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

The screenshot illustrates the workflow for importing requirements into the C-SOX system. It shows three main components:

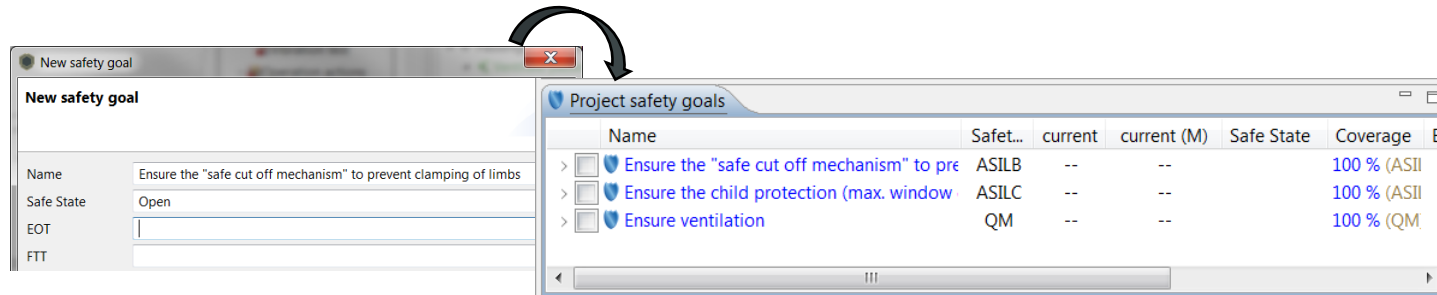
- Repository:** A tree view on the left showing a project named 'Window Lifter [Client1/TeamA]' with sub-projects like RM, DESIGN, HA, FMEA, FMEDA, FTA, and BOM.
- Import Wizard:** A dialog box titled 'Import' with a 'Select' tab. It prompts the user to 'Select an import source:' and lists various options, with 'RM ReqIF File Import' selected. Navigation buttons '< Back' and 'Next >' are visible.
- Hierarchy:** A tree view showing the project structure, with 'Vehicle equipped with an electronic window lifter' selected.
- Requirements Table:** A table titled 'Module System Requirements' displaying the imported requirements. The table has columns for Name, Text, Comment, Priority, Scheduled, and Status.

	Name	Text	Comment	Priority	Scheduled	Status
2	Vehicle equipped with an electronic window lifter					FINISHED
2.1	Min. Ventilation volume	Window lifter shall able the interior to be ventilated with a minimum ventilation volume of 0,001 m ³ /s. <input type="text" value="0,001 m<sup>3</sup>/s"/>	Note: The vehicle needs to remain stationary.	High	Thursday, August...	INACTIVE
2.2	Stop uplift	Window pane shall stop if during uplift any object or corporal extremities obstruct the operation	TBD	High	Friday, August 2...	PROPOSED
2.3	Child protection	The Child protection mechanism shall be <ul style="list-style-type: none">• tested• ensured		High		
3	Window lifter					
3.1	Window lift down operation	Window panes shall lift down if torque >= 0,5 Nm torque >= 0,4 Nm		High		INACTIVE
3.2	Max. retracting	Rear window panes shall lift down up to 50% of the height of the window frame, when Child protection is active		Medium		INACTIVE



Requirements: Safety Goals

- Define Safety Goals



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

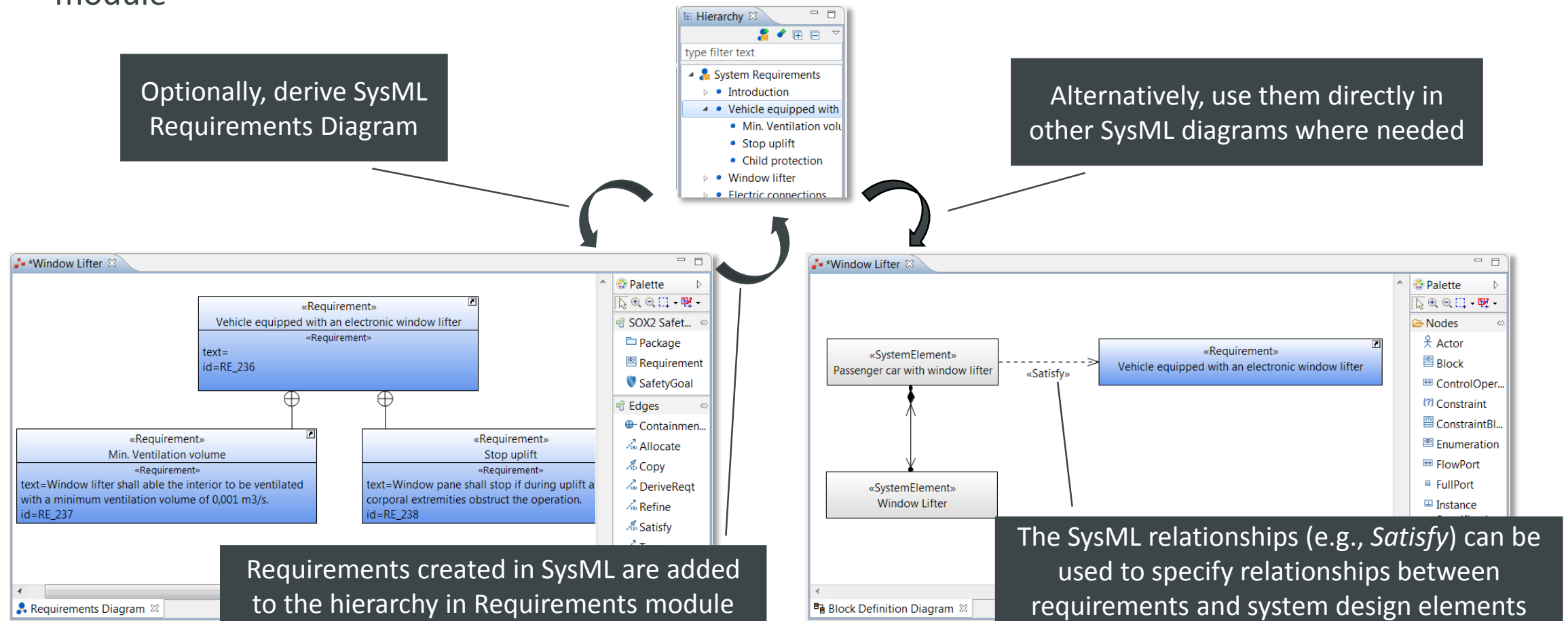
The image shows a screenshot of a 'Window Lifter' HAZOP table. The table has columns for Nr, Priority, Status, Function, Malfunction, Combin..., Effect, Hazard, S (Severi..., Durat..., Frequ..., E (Expos..., C (Contr..., ASIL, Safety Goal, and Safe state. The table contains 18 rows of data, with some cells highlighted in green or yellow. The table is filtered by 'type filter text'.

Nr	Priority	Status	Function	Malfunction	Combin...	Effect	Hazard	S (Severi...	Durat...	Frequ...	E (Expos...	C (Contr...	ASIL	Safety Goal	Safe state
1	★	OPEN	Raising the window	Raising the window ...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E4 - High...	C0 - Cont...	QM		
2	★	OPEN	Raising the window	Raising the window ...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E4 - High...	C1 - Sim...	QM		
3	★	OPEN	Raising the window	Raising the window ...	Driving i...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E4 - High...	C0 - Cont...	QM		
4	★	OPEN	Raising the window	Raising the window ...	Car at ser...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E2 - Low ...	C0 - Cont...	QM		
5	★	OPEN	Raising the window	Raising the window ...	Parking	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C0 - Cont...	QM		
6	★	OPEN	Raising the window	Raising the window ...	Driving o...	Clamped...	Damage to persons ...	S1 - Light...			E4 - High...	C3 - Diffi...	ASILB	Ensure the "safe cut...	
7	★	OPEN	Raising the window	Raising the window ...	Driving o...	Clamped...	Damage to persons ...	S1 - Light...			E4 - High...	C3 - Diffi...	ASILB	Ensure the "safe cut...	
8	★	OPEN	Raising the window	Raising the window ...	Driving i...	Clamped...	Damage to persons ...	S2 - Seve...			E4 - High...	C2 - Nor...	ASILB	Ensure the "safe cut...	
9	★	OPEN	Raising the window	Raising the window ...	Car at ser...	Only ligh...	Damage to persons ...	S0 - No i...			E2 - Low ...	C2 - Nor...	QM		
10	★	OPEN	Raising the window	Raising the window ...	Parking	Clamped...	Damage to persons ...	S2 - Seve...			E3 - Med...	C2 - Nor...	ASILA	Ensure the "safe cut...	
11	★	OPEN	Lowering the window	Lowering the windo...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C1 - Sim...	QM		
12	★	OPEN	Lowering the window	Lowering the windo...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E4 - High...	C1 - Sim...	QM		
13	★	OPEN	Lowering the window	Lowering the windo...	Driving i...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C0 - Cont...	QM		
14	★	CLOSED	Lowering the window	Lowering the windo...	Car at ser...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E2 - Low ...	C0 - Cont...	QM		
15	★	OPEN	Lowering the window	Lowering the windo...	Parking	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C0 - Cont...	QM		
16	★	OPEN	Lowering the window	Lowering the windo...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C0 - Cont...	QM		
17	★	OPEN	Lowering the window	Lowering the windo...	Driving o...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E4 - High...	C0 - Cont...	QM		
18	★	OPEN	Lowering the window	Lowering the windo...	Driving i...	Only loss ...	Non-hazardous loss ...	S0 - No i...			E3 - Med...	C0 - Cont...	QM		



System Design: Requirements

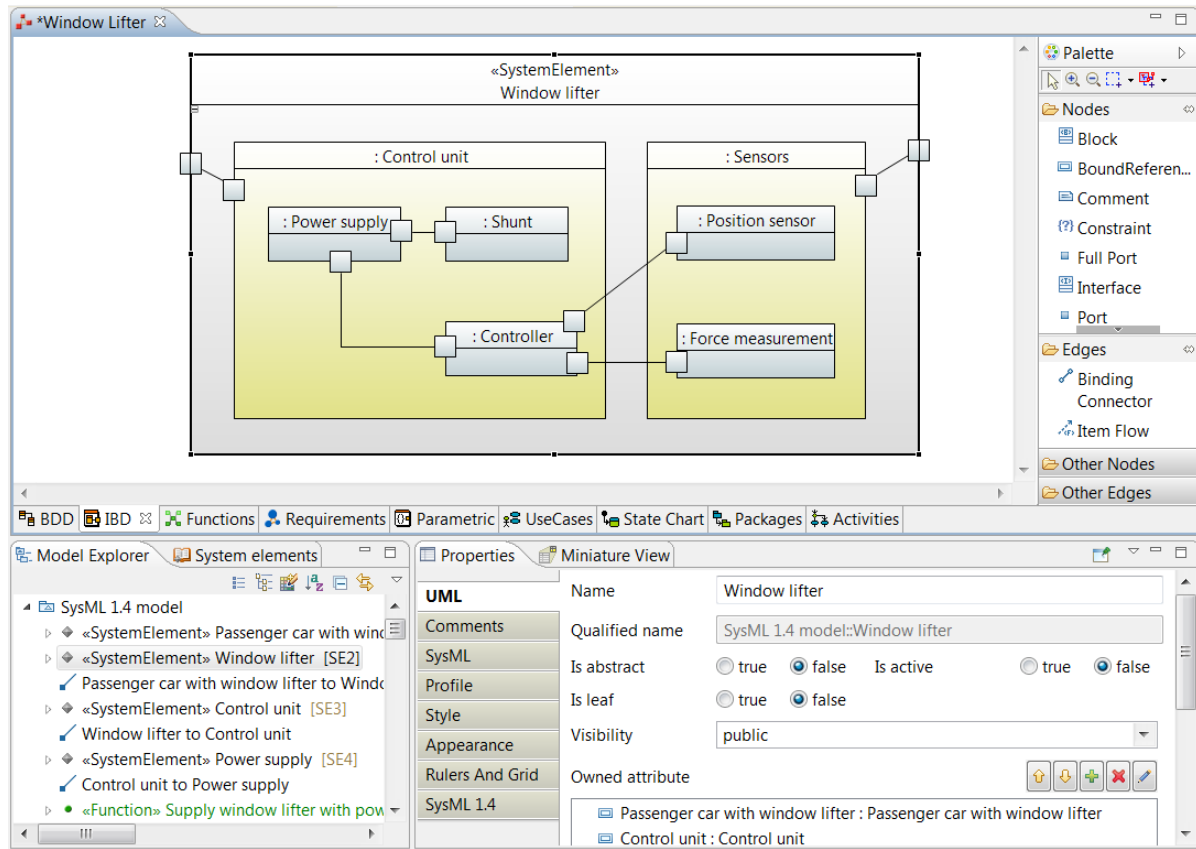
- Requirements in Requirements module can be directly used in SysML via drag and drop
- Vice versa, changes and newly created Requirements from SysML are reflected in Requirements module





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

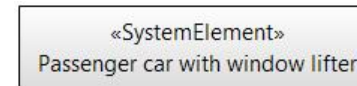




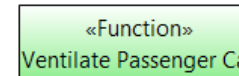
System Design: Stereotypes

- Use specific stereotypes to mark elements to be considered for safety analysis:

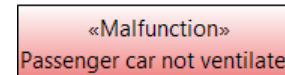
- System element*: Extension of a SysML block



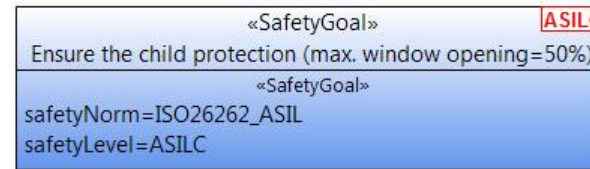
- Function*: Extension of a SysML block



- Malfunction*: Extension of a SysML block



- Safety Goal*: Extension of a SysML Requirement



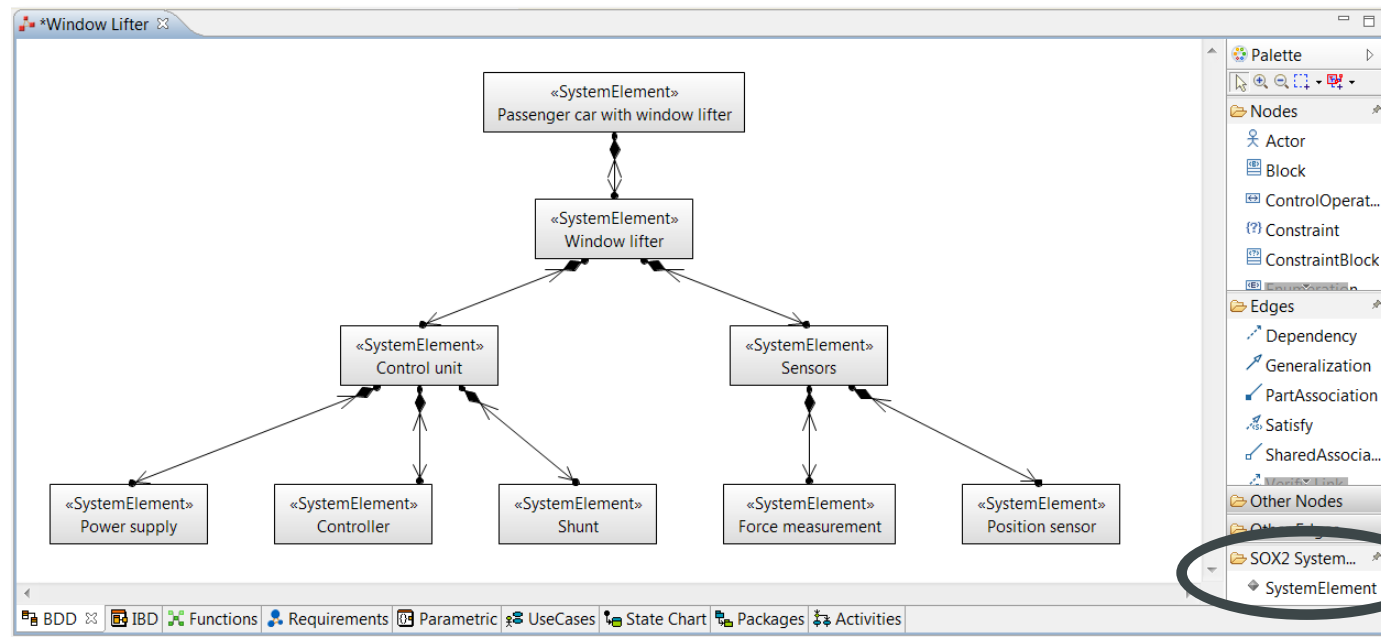
- Additional stereotypes for specific sub-types of functions:

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

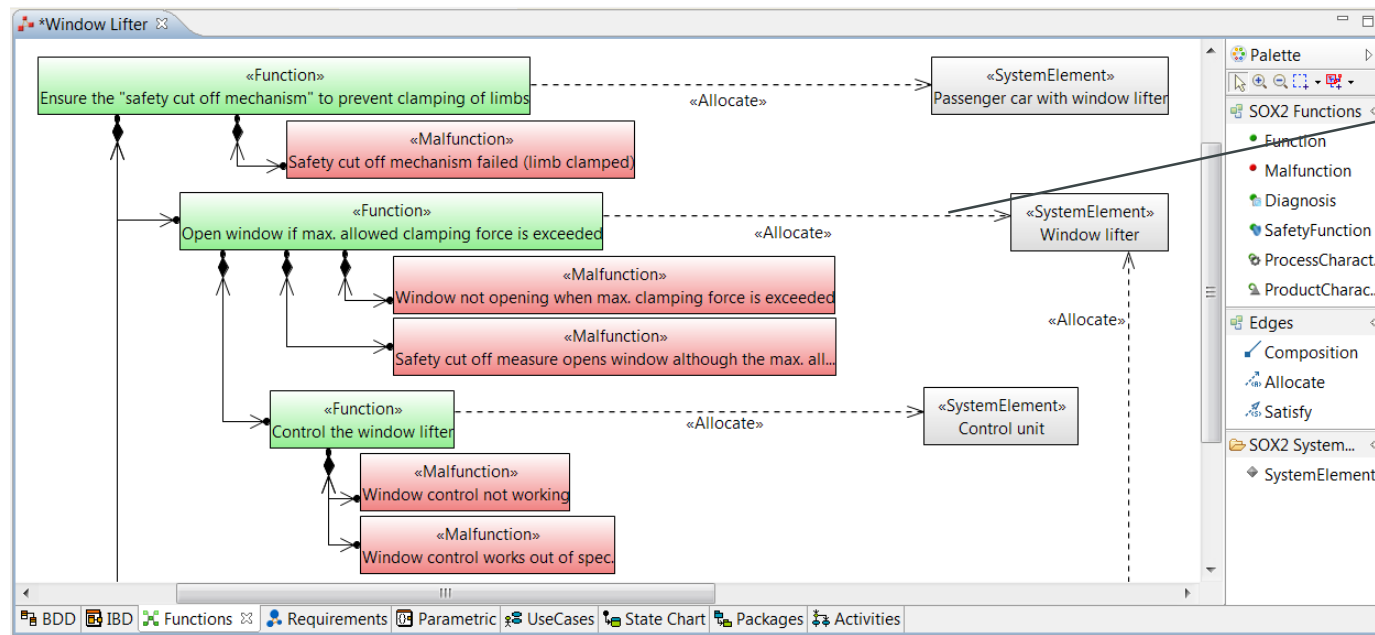


Create System Elements from the palette or add/remove stereotype *System Element* from/to blocks later



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

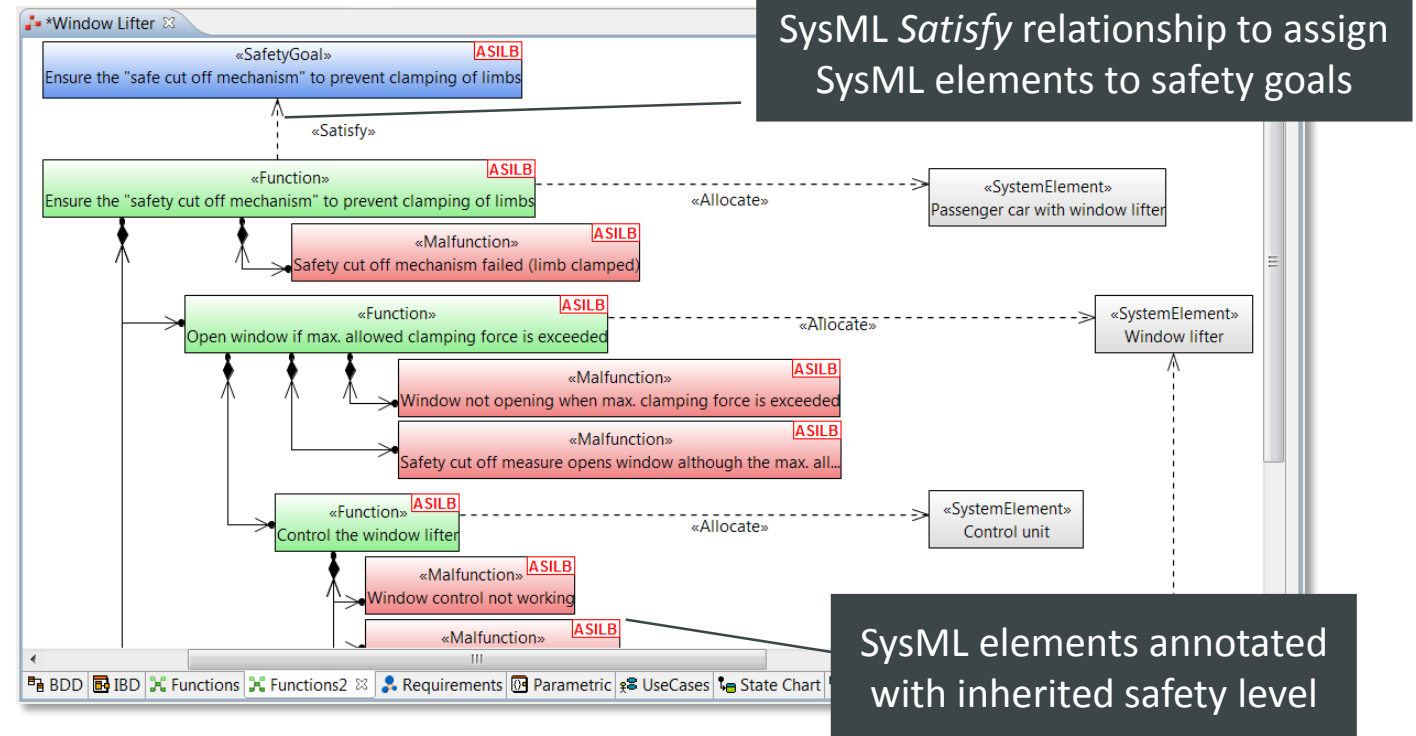
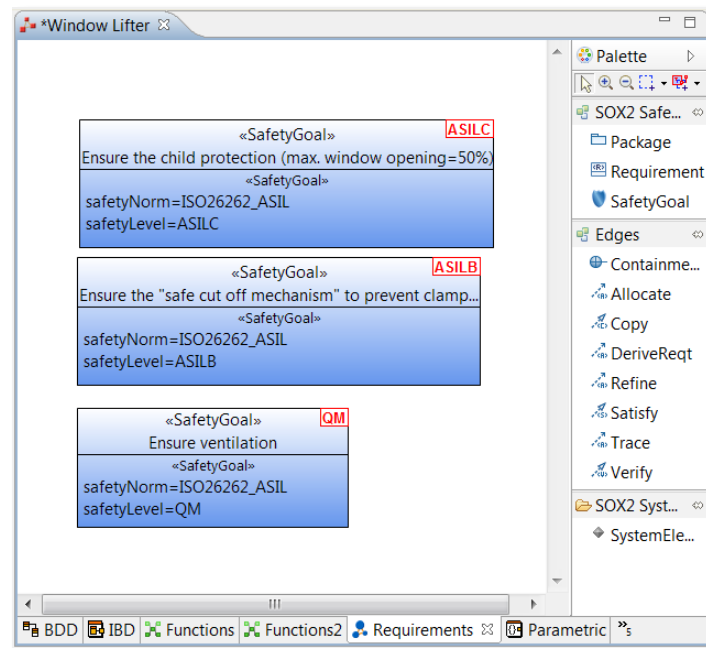


SysML *Allocate* relationship to allocate functions to system elements



System Design: Safety Goals

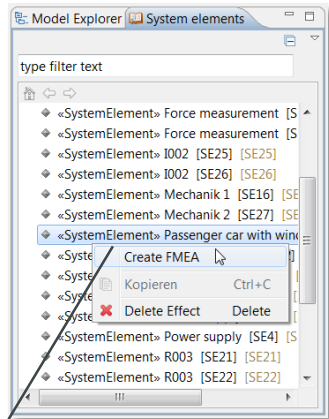
- All Safety Goals are available in the system design and can also be edited, created and assigned to system elements within the system design
- Assignment of Safety Goals to Malfunctions is represented in SysML via SysML *Satisfy* relationship
- Safety Classifications are calculated for all elements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



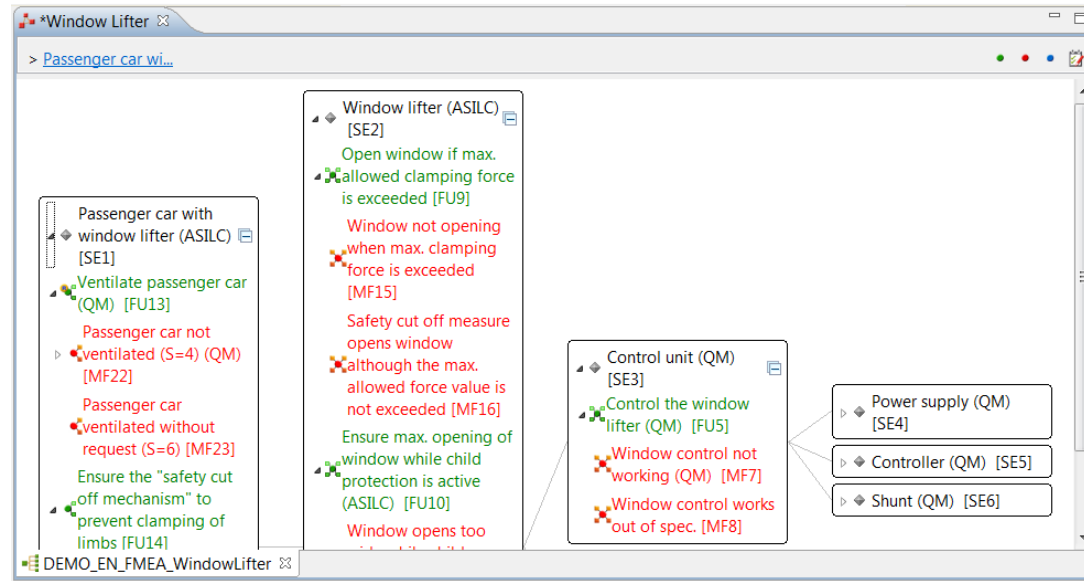


FMEA: Derive FMEA from System Design

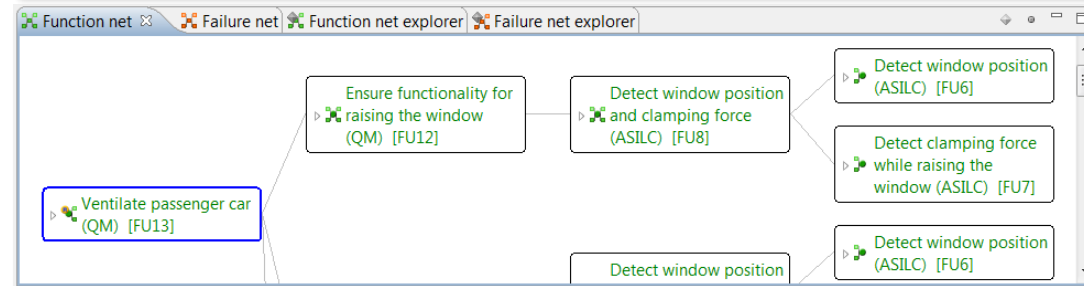
- The structure of an FMEA can be automatically derived from system design
- Irrelevant elements from system design can be omitted



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

The screenshot shows the FMEA software interface for a 'Window Lifter' project. It includes a 'Failure net' diagram with nodes like 'Window control not working (QM) ASILB [MF7]' and 'No power supplied to the window lifter when power was requested (QM)'. A list of actions is visible, such as 'Power supply (QM) [SE4]', 'Supply window lifter with power (5V) (QM) [FU1]', and 'Diagnosis Status A'. A filter table is also present with columns for Title, Assignments, Status, and Detection (D).

Title	Assignments	Stat...	O	D	Acti...
Material only from proven suppliers	9	●	1		
Measure voltage	9	●	5		
Indicator light for ignition	9	●	0		
Vibration test	9	●	5		



Generation of reports

Formblatt for: Passenger car with window lifter

Passenger car with window lifter - Systembetrachtung		Massnahmenstand	Firma		
FMEA/Systemelement	Arbeitsgangnummer:	Verantwortlich:	Erste...	Jul 20	
Passenger car with window lifter	Massnahmenstand	Firma:	Ver...	Jul 20	

Effect	S	Malfunction	Cause	C	Prevention	O	Detection action	D	RPN
Passenger car with window lifter [SE_1] (ASIL C)									
Ventilate passenger car [FN_17]									
		Passenger car not ventilated [MF_25]	Window can not be lowered [MF_21]						
			>Not detecting window position and/or clamping force [MF_15]						
			>>Not detecting window position [MF_10]						
Maßnahmenstand A									
Construction actions									
		O: Material von bewährten Lieferanten		1			D: Spannungsmessu...	5	30



BOM: Create or Import BOM

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

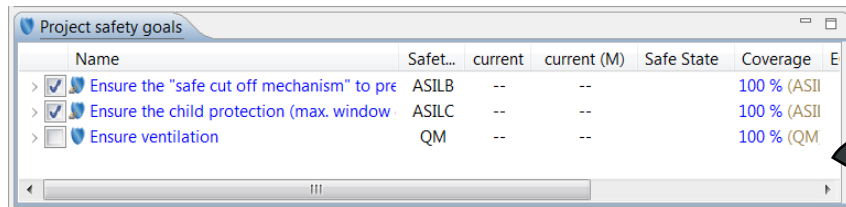
The screenshot illustrates the workflow for importing a BOM and viewing failure mode catalogues. On the left, the 'Import BOM file...' dialog is shown with 'Complex Excel FMEDA' selected as the format. In the center, the 'IEC62380' catalogue is expanded to show categories like '01. Equipped PCBs, Hybrid Circuits' and '04. Optoelectronics'. On the right, another 'IEC62380' window shows specific failure modes for diodes, such as 'Open circuits - 20.0%' and 'Short circuits - 70.0%'. At the bottom, the 'Overall system' window displays a detailed table of components and their failure modes.

	Status	Name	Description	Factor	Product Code	Assembly gr...	Component				Failure Mode				
							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_SL_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		

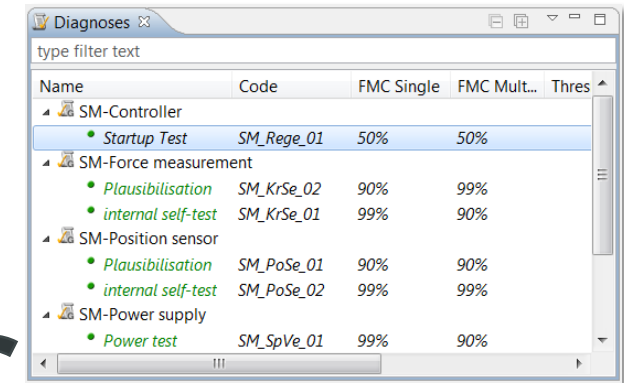


FMEDA: Create FMEDA from BOM

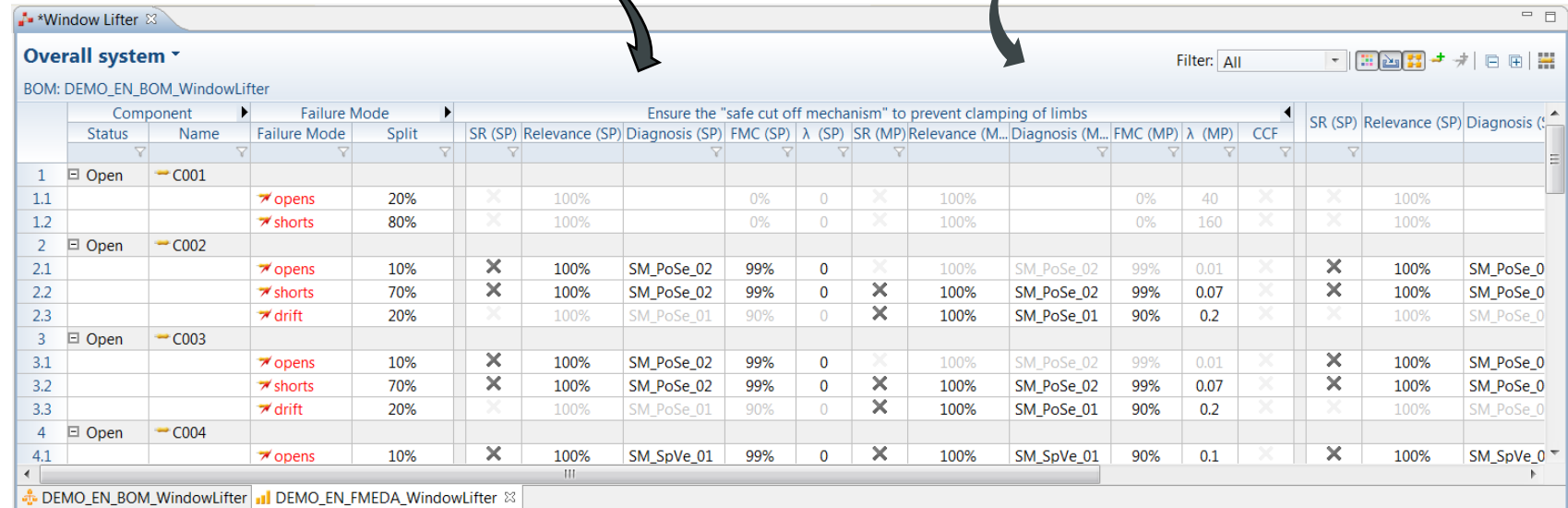
- Safety goals can be taken from the project safety goals / system design
- Diagnoses are considered as specific functions and, hence
 - Can be taken from catalogue
 - Newly added diagnoses are added to the system design and the catalogue



Name	Safet...	current	current (M)	Safe State	Coverage
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)



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%	



Component		Failure Mode		Ensure the "safe cut off mechanism" to prevent clamping of limbs													
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	SR (SP)	Relevance (SP)	Diagnosis (SP)
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

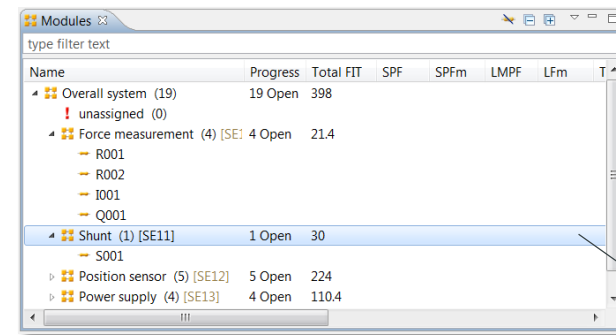
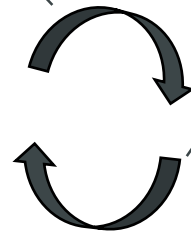
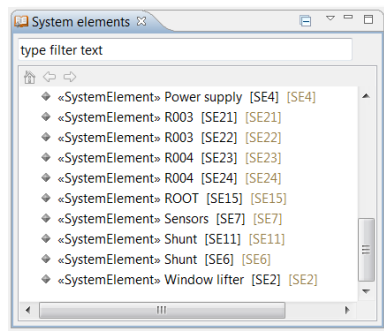


FMEDA: Modules

- 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



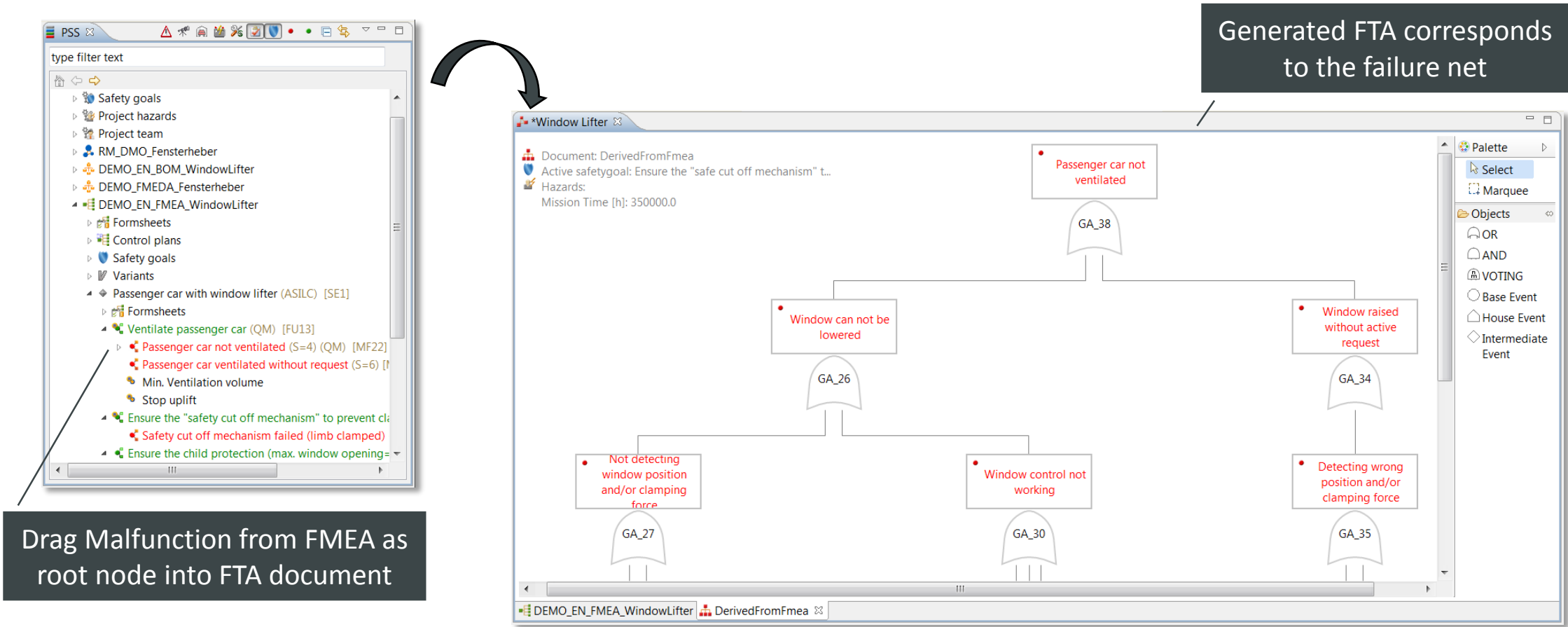
Filtering according to selected module

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	SR (SP)
Open	S001														
19.1		opens	70%	×	100%	SM_Shun_01	99%	0	×	100%	SM_Shun_01	90%	2.1	×	×
19.2		functional	10%	×	100%	SM_Shun_02	90%	0	×	100%	SM_Shun_02	90%	0.3	×	×
19.3		drift	20%	×	100%	SM_Shun_02	90%	0	×	100%	SM_Shun_02	90%	0.6	×	×



FTA: Derive FTA from FMEA

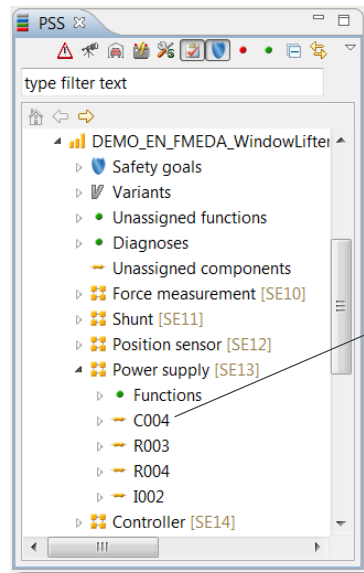
- An FTA can be automatically derived from the FMEA



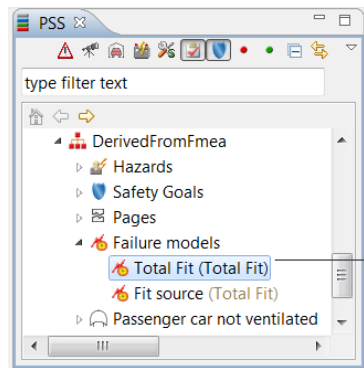
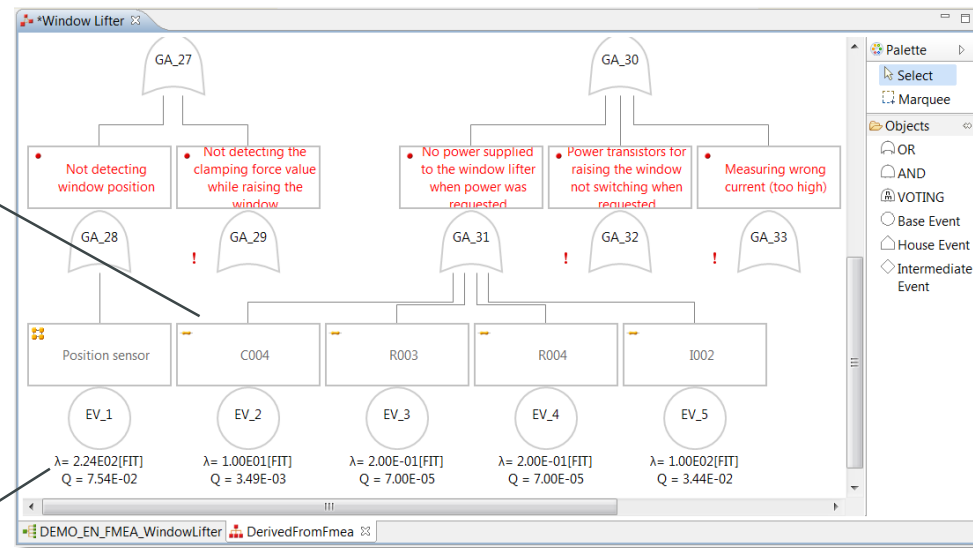


FTA: Finalize FTA

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

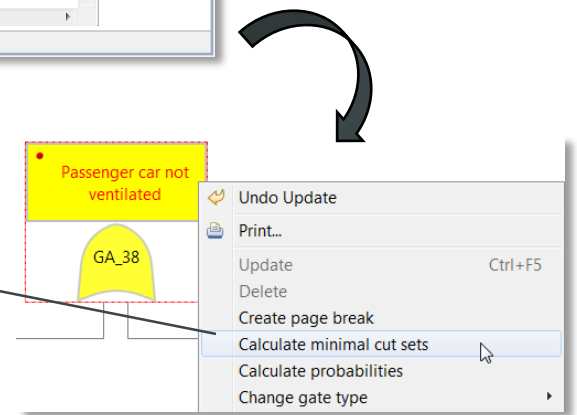


Drag and drop, e.g.,
Components from
FMEDA as base events



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



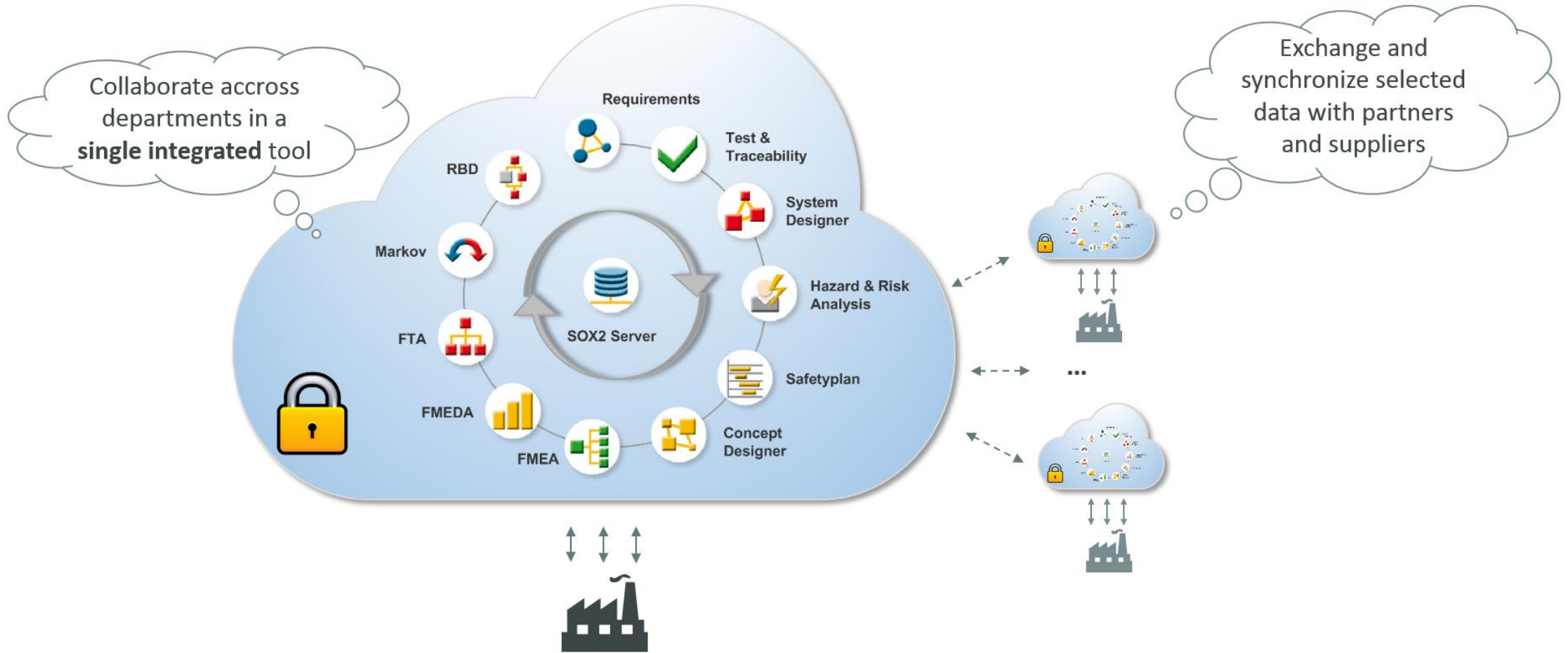


Project C-SOX





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