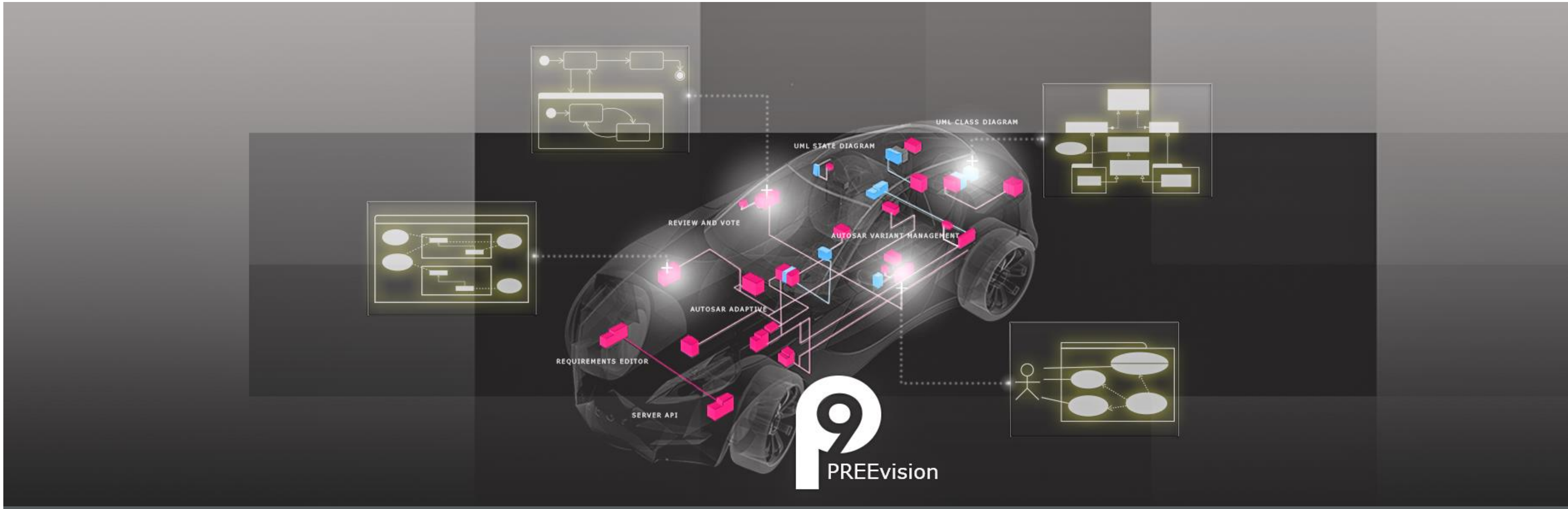


Development of Functional Safe Systems using PREEvision

Webinar, 2020-03-03

V1.2 | 2020-03-03

Agenda

- ▶ **PREEvision at a Glance**
- Introduction Functional Safety
- Item definition, HAZOP and HARA
- Functional and Technical Safety Concept
- Safety Analysis
- Verification and Validation
- Safety Plan, Safety Case
- Functional Safety Perspectives
- Summary

Basic idea and benefits to our customers

PREEvision is in the market to …

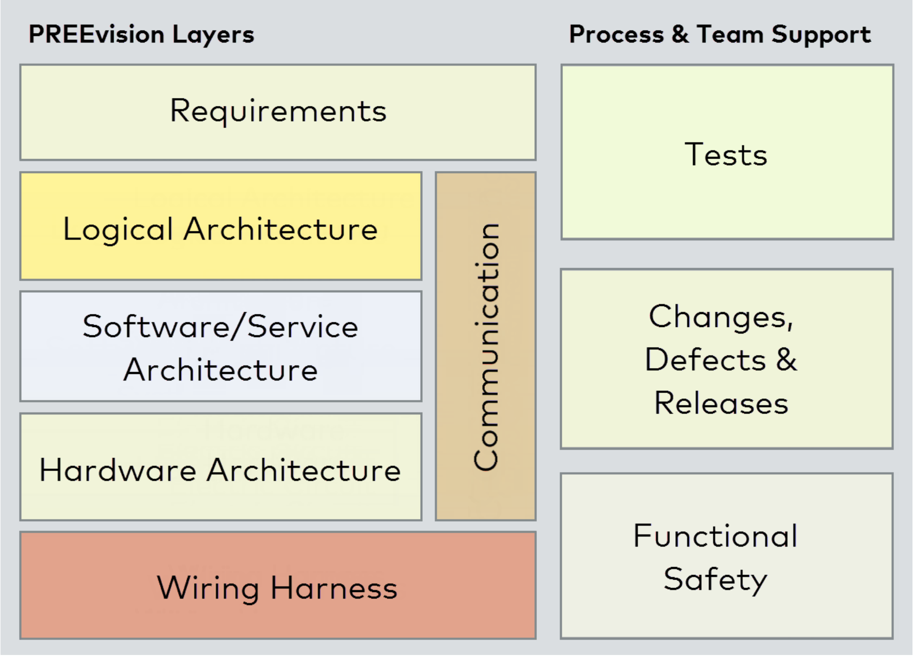
- Perform and control E/E development
- Support the related processes
- Ensure quality of work products
- Improve efficiency
- Reduce costs and time to market

PREEvision = Model Based E/E Systems Engineering

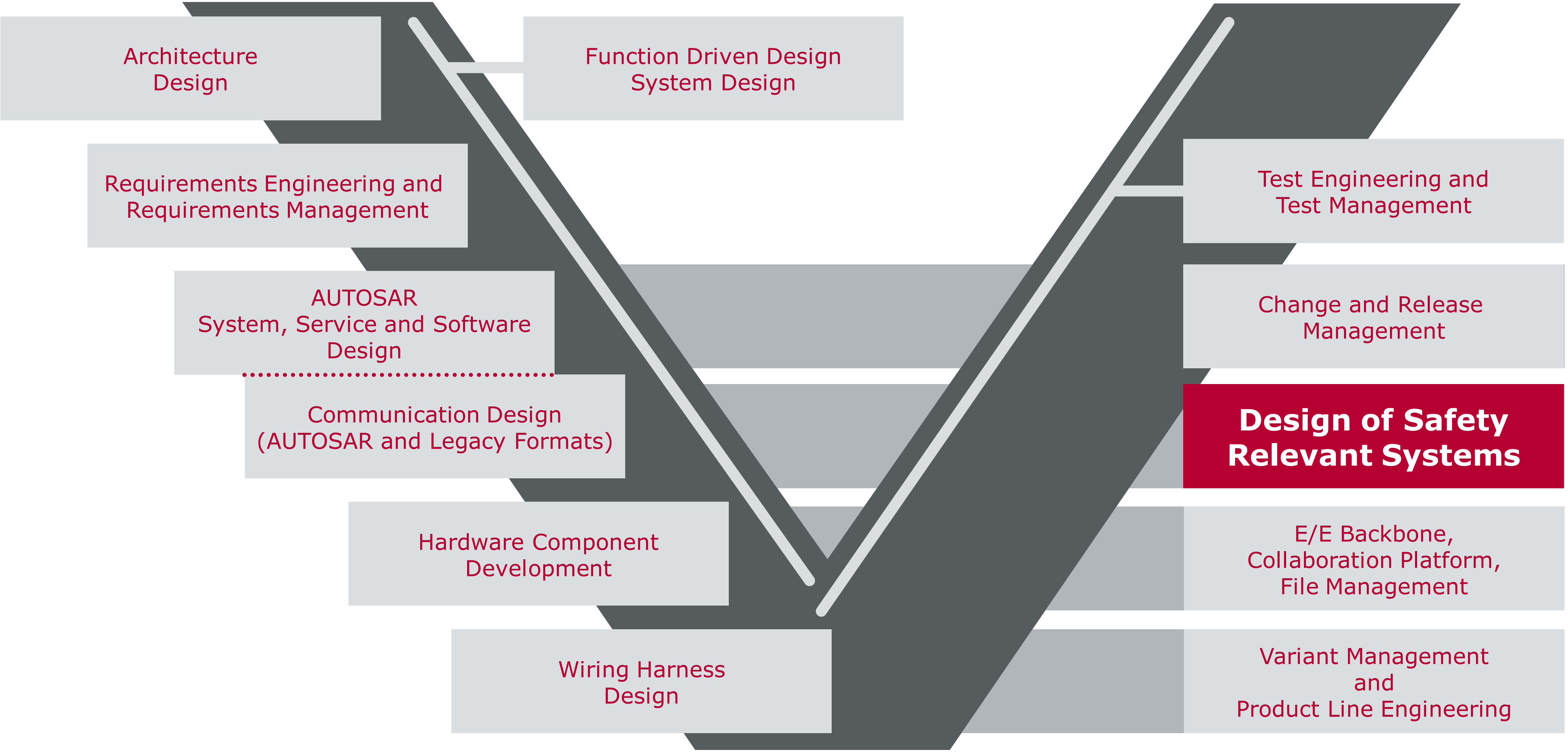
- Integrated business logic and one comprehensive data model for the entire E/E development process.

PREEvision stands for …

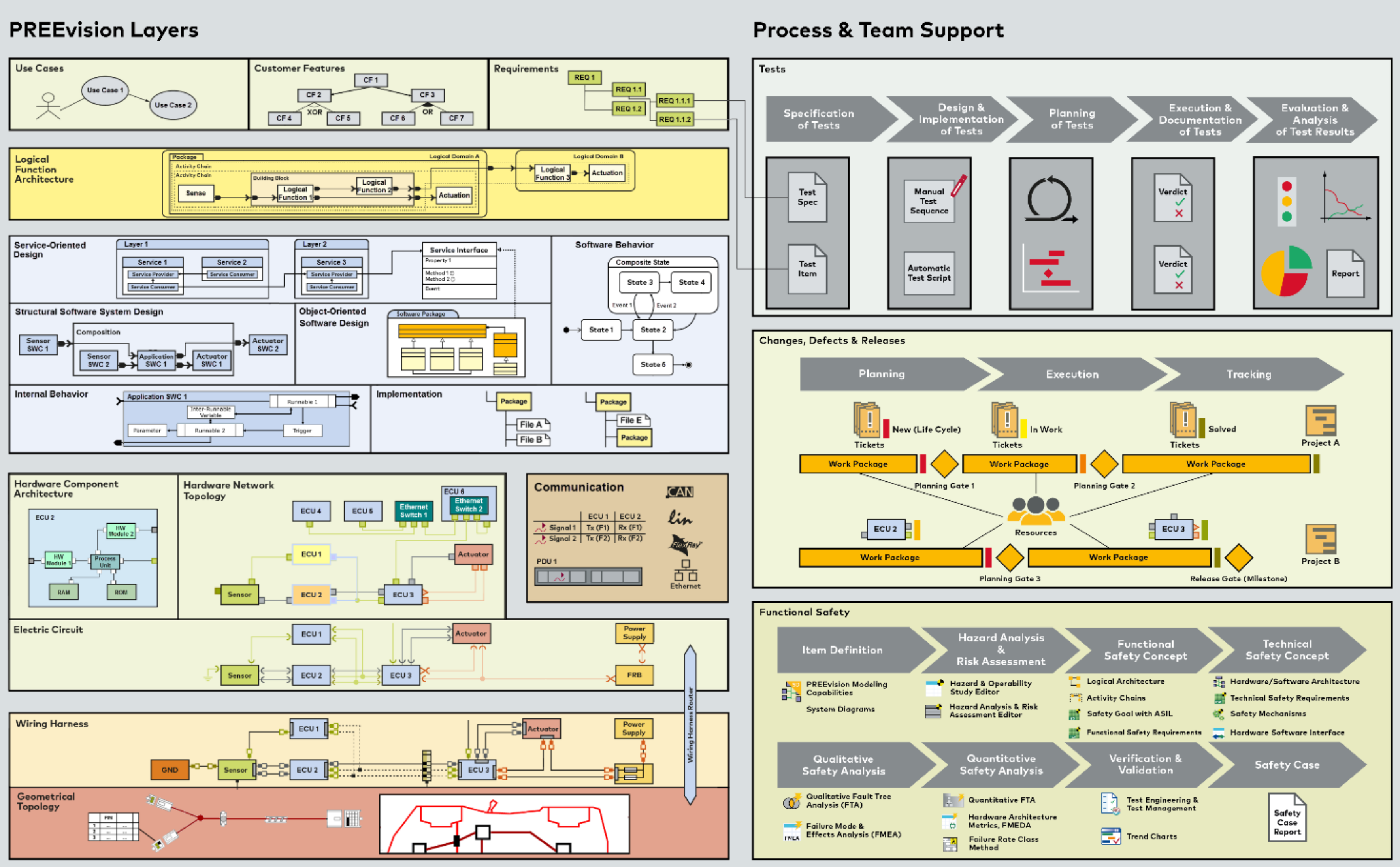
- One Data Model. One GUI.
- Many Users. Multiple Sites. One Data Source.
- One Process. Full traceability. Full Transparency.
- Environment for function and software driven Automotive E/E development



Supported Use Cases


Architecture Design
Function Driven Design System Design
Requirements Engineering and Requirements Management
AUTOSAR System, Service and Software Design
Communication Design (AUTOSAR and Legacy Formats)
Hardware Component Development
Wiring Harness Design
Test Engineering and Test Management
Change and Release Management
Design of Safety Relevant Systems
E/E Backbone, Collaboration Platform, File Management
Variant Management and Product Line Engineering

PREEvision Layer Model



Agenda

PREEvision at a Glance

▶ **Introduction Functional Safety**

Item definition, HAZOP and HARA

Functional and Technical Safety Concept

Safety Analysis

Verification and Validation

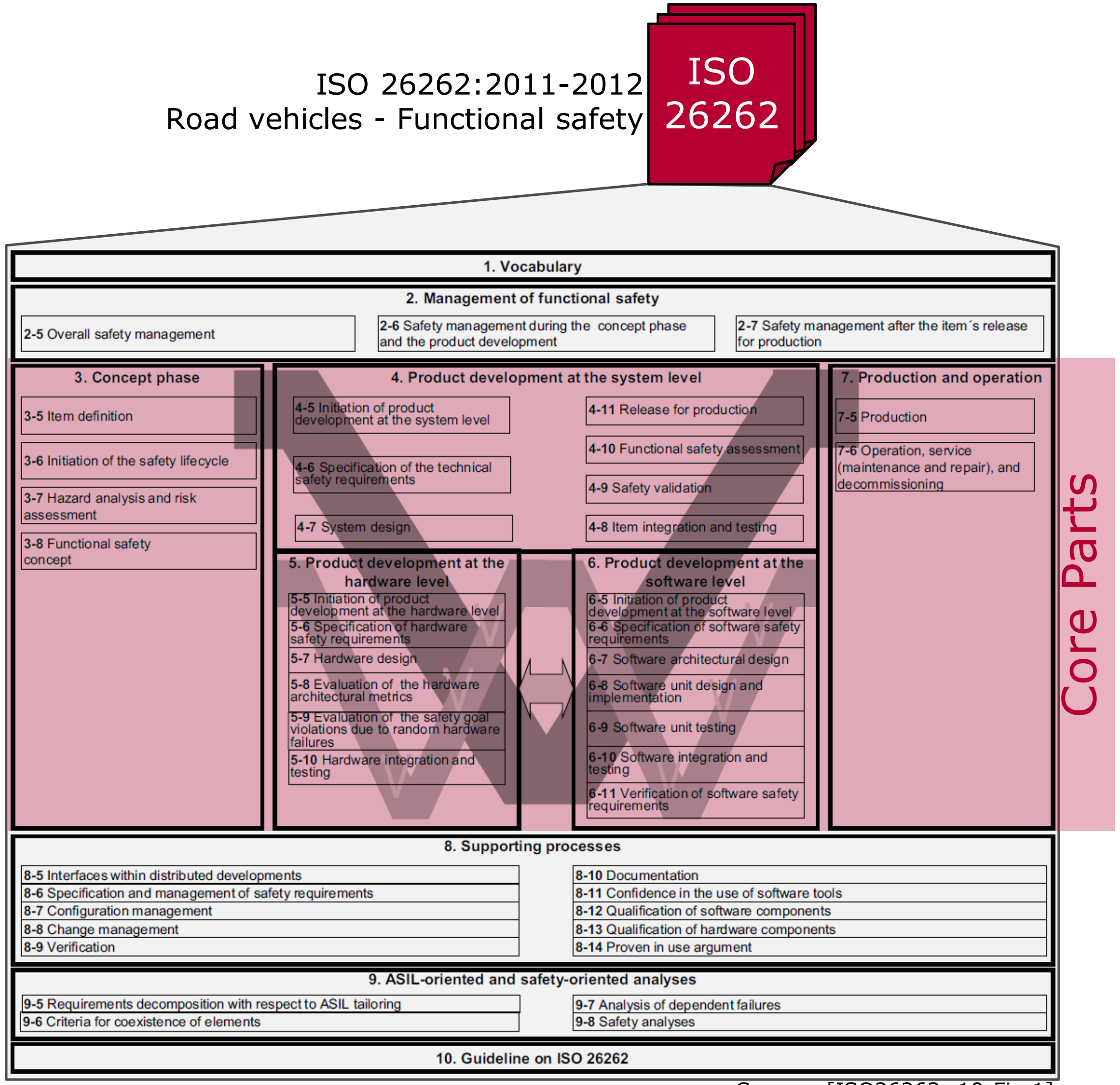
Safety Plan, Safety Case

Functional Safety Perspectives

Summary

Challenges

- ▶ 10 Parts
- ▶ 43 Chapters
- ▶ 100 Work products
- ▶ 180 Engineering methods
- ▶ 500 Pages
- ▶ 600 Requirements



ISO 26262:2011-2012
Road vehicles - Functional safety

ISO 26262

1. Vocabulary

2. Management of functional safety
- 2-5 Overall safety management
- 2-6 Safety management during the concept phase and the product development
- 2-7 Safety management after the item´s release for production

3. Concept phase
- 3-5 Item definition
- 3-6 Initiation of the safety lifecycle
- 3-7 Hazard analysis and risk assessment
- 3-8 Functional safety concept

4. Product development at the system level
- 4-5 Initiation of product development at the system level
- 4-6 Specification of the technical safety requirements
- 4-7 System design
- 4-8 Item integration and testing
- 4-9 Safety validation
- 4-10 Functional safety assessment
- 4-11 Release for production

5. Product development at the hardware level
- 5-5 Initiation of product development at the hardware level
- 5-6 Specification of hardware safety requirements
- 5-7 Hardware design
- 5-8 Evaluation of the hardware architectural metrics
- 5-9 Evaluation of the safety goal violations due to random hardware failures
- 5-10 Hardware integration and testing

6. Product development at the software level
- 6-5 Initiation of product development at the software level
- 6-6 Specification of software safety requirements
- 6-7 Software architectural design
- 6-8 Software unit design and implementation
- 6-9 Software unit testing
- 6-10 Software integration and testing
- 6-11 Verification of software safety requirements

7. Production and operation
- 7-5 Production
- 7-6 Operation, service (maintenance and repair), and decommissioning

Core Parts

8. Supporting processes
- 8-5 Interfaces within distributed developments
- 8-6 Specification and management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the use of software tools
- 8-12 Qualification of software components
- 8-13 Qualification of hardware components
- 8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analyses

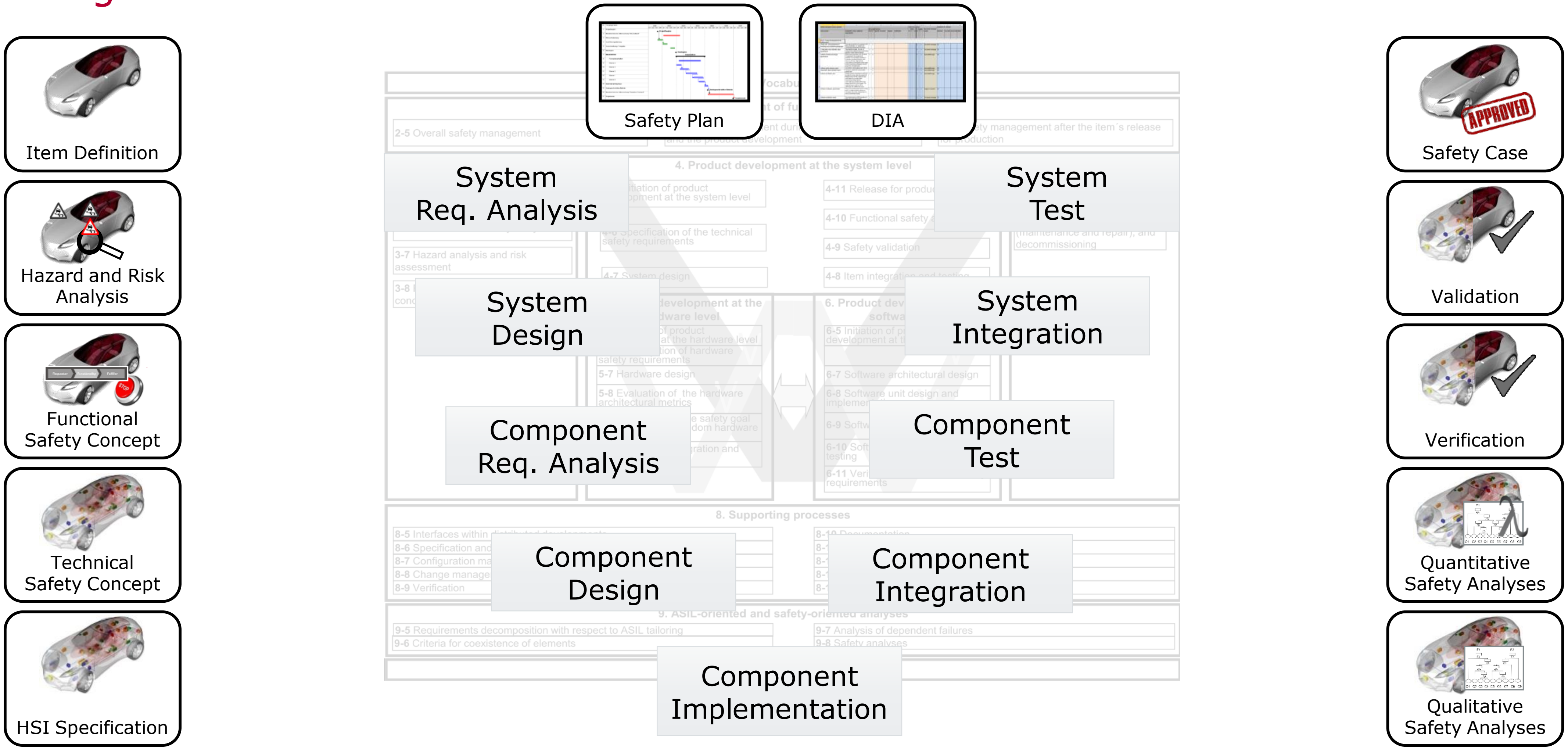
10. Guideline on ISO 26262

Source: [ISO26262, 10-Fig.1]

▶▶ Complex standard → Risk of overheads and costs if applied ad hoc

VECTOR

Challenges



Item Definition

Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

HSI Specification

Safety Plan

DIA

System Req. Analysis

System Design

Component Req. Analysis

Component Design

Component Implementation

Component Integration

Component Test

System Integration

System Test

Safety Case

Validation

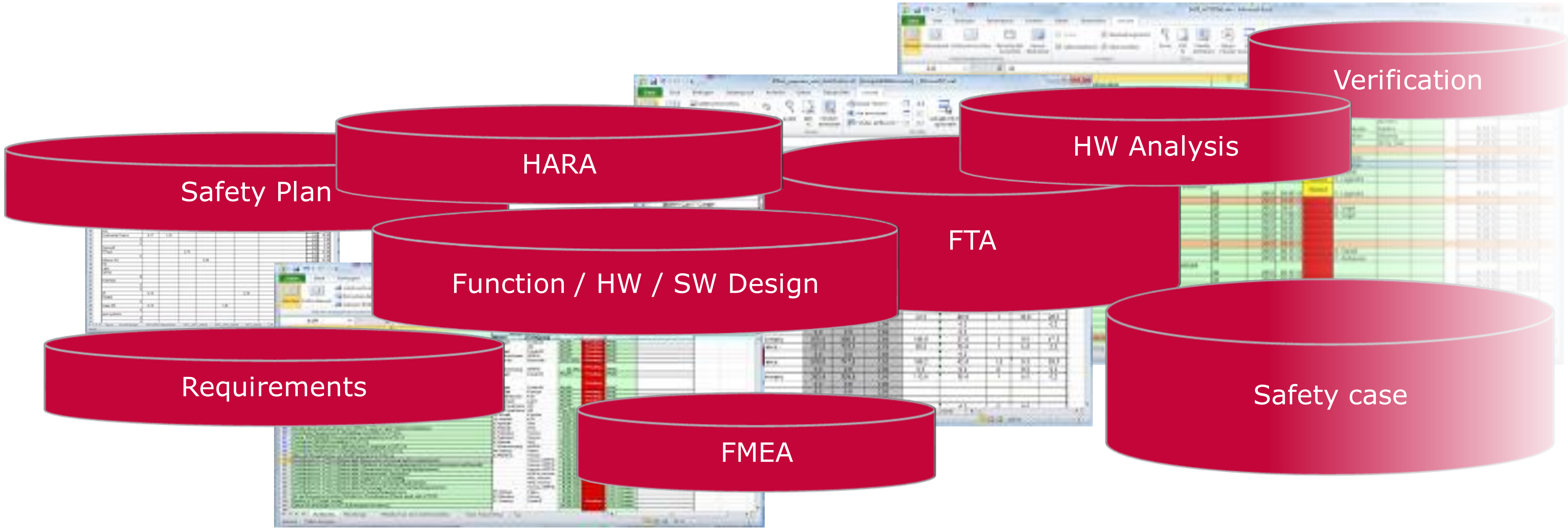
Verification

Quantitative Safety Analyses

Qualitative Safety Analyses

►► ISO 26262 key deliverables have impact on all process areas

Challenges

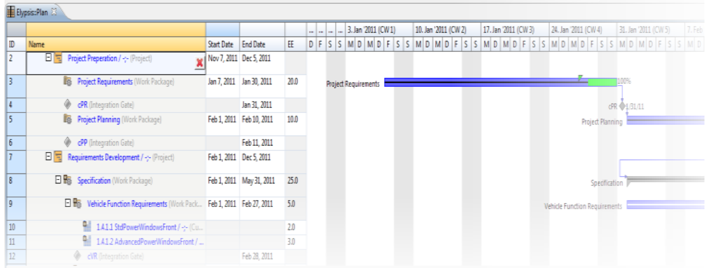


- Data for work products fragmented across legacy tools and documents
- System responsible, safety managers and engineers have to struggle with multiple mostly inconsistent sources for producing the work products
- Maintaining traceability and consistency is inefficient, error prone and a source for quality and compliance problems

►► High cost for ISO 26262 compliant work products

Integrated Model Based System Engineering Platform

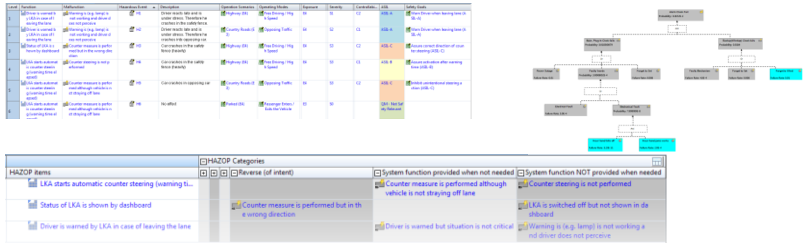
Safety Plan



Elypsis::Plan

ID	Name	Start Date	End Date	EE
2	Project Preperation / -;- (Project)	Nov 7, 2011	Dec 5, 2011	
3	Project Requirements (Work Package)	Jan 7, 2011	Jan 30, 2011	20.0
4	cPR (Integration Gate)		Jan 31, 2011	
5	Project Planning (Work Package)	Feb 1, 2011	Feb 10, 2011	10.0
6	cPP (Integration Gate)		Feb 11, 2011	
7	Requirements Development / -;- (Project)	Feb 1, 2011	Dec 5, 2011	
8	Specification (Work Package)	Feb 1, 2011	May 31, 2011	25.0
9	Vehicle Function Requirements (Work Pack...	Feb 1, 2011	Feb 27, 2011	5.0
10	1.4.1.1 StdPowerWindowsFront / -;- (Cu...			2.0
11	1.4.1.2 AdvancedPowerWindowsFront / ...			3.0
12	cVR (Integration Gate)		Feb 28, 2011	

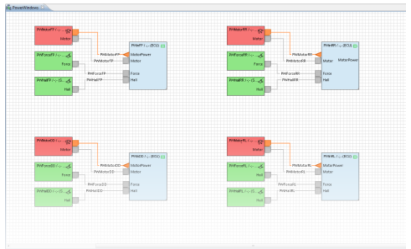
Safety Analysis Methods



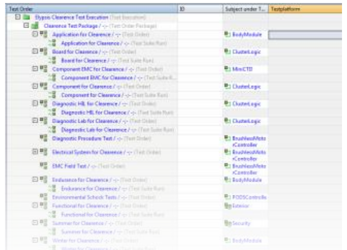
HAZOP items	Reverse (of intent)	System function provided when not needed	System function NOT provided when needed
LKA starts automatic counter steering (warning ti...		Counter measure is performed although vehicle is not straying off lane	Counter steering is not performed
Status of LKA is shown by dashboard	Counter measure is performed but in th e wrong direction		LKA is switched off but not shown in da shboard
Driver is warned by LKA in case of leaving the lane		Driver is warned but situation is not critical	Warning is (e.g. lamp) is not working a nd driver does not perceive

Cost efficient consistency and traceability

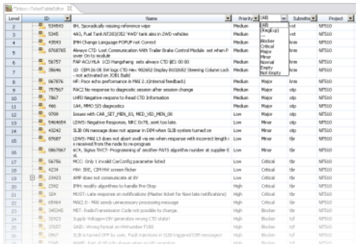
Requirements Management



System / Function / HW / SW Design



Test Management



Change Management

ISO 26262 key areas supported by PREEvision

Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

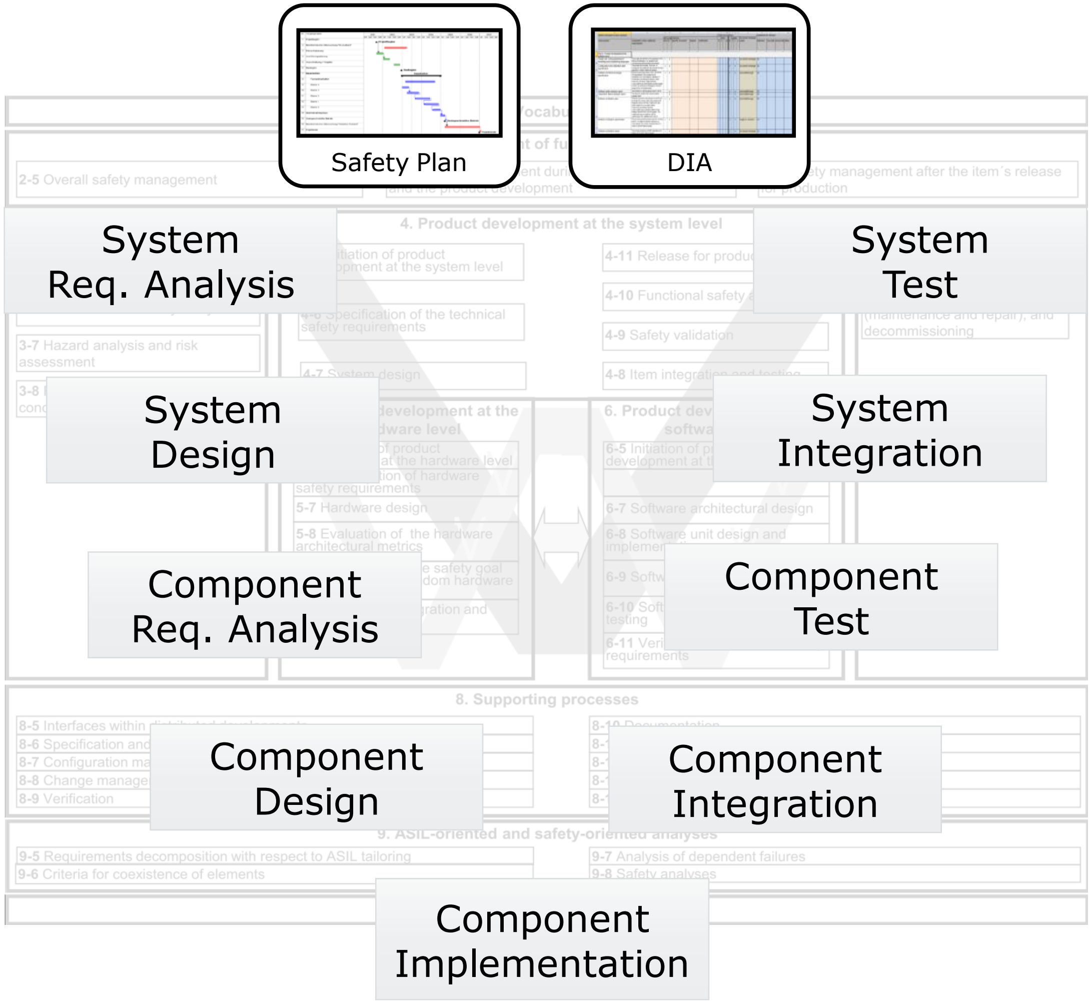
Item Definition

Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

HSI Specification

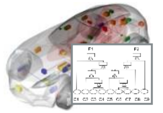

Safety Plan
DIA
2-5 Overall safety management
4. Product development at the system level
System Req. Analysis
System Test
3-7 Hazard analysis and risk assessment
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
4-7 System design
System Design
System Integration
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
6-7 Software architectural design
6-8 Software unit design and implementation
Component Req. Analysis
Component Test
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
Component Design
Component Integration
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
Component Implementation

Safety Case

Validation

Verification

Quantitative Safety Analyses



Qualitative Safety Analyses

Safety Case

Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

Agenda

PREEvision at a Glance

Introduction Functional Safety

▶ **Item definition, HAZOP and HARA**

Functional and Technical Safety Concept

Safety Analysis

Verification and Validation

Safety Plan, Safety Case

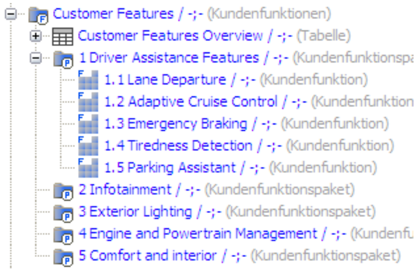
Functional Safety Perspectives

Summary

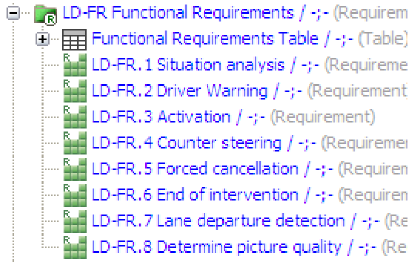
VECTOR

Item Definition

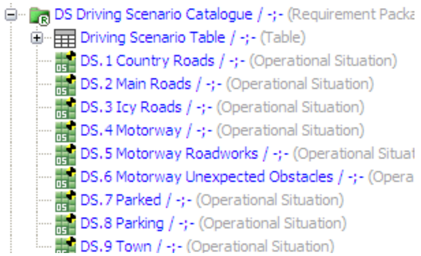
Item Definition



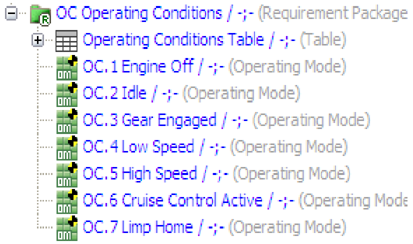
- Customer Features / -;- (Kundenfunktionen)
  - Customer Features Overview / -;- (Tabelle)
  - 1 Driver Assistance Features / -;- (Kundenfunktionspa
    - 1.1 Lane Departure / -;- (Kundenfunktion)
    - 1.2 Adaptive Cruise Control / -;- (Kundenfunktion
    - 1.3 Emergency Braking / -;- (Kundenfunktion)
    - 1.4 Tiredness Detection / -;- (Kundenfunktion)
    - 1.5 Parking Assistant / -;- (Kundenfunktion)
  - 2 Infotainment / -;- (Kundenfunktionspaket)
  - 3 Exterior Lighting / -;- (Kundenfunktionspaket)
  - 4 Engine and Powertrain Management / -;- (Kundenfu
  - 5 Comfort and interior / -;- (Kundenfunktionspaket)



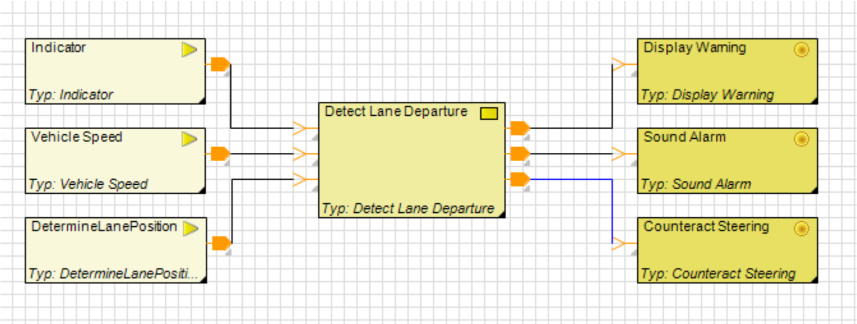
- LD-FR Functional Requirements / -;- (Requirem
  - Functional Requirements Table / -;- (Table)
  - LD-FR.1 Situation analysis / -;- (Requireme
  - LD-FR.2 Driver Warning / -;- (Requirement
  - LD-FR.3 Activation / -;- (Requirement)
  - LD-FR.4 Counter steering / -;- (Requireme
  - LD-FR.5 Forced cancellation / -;- (Requiren
  - LD-FR.6 End of intervention / -;- (Requiren
  - LD-FR.7 Lane departure detection / -;- (Re
  - LD-FR.8 Determine picture quality / -;- (Re

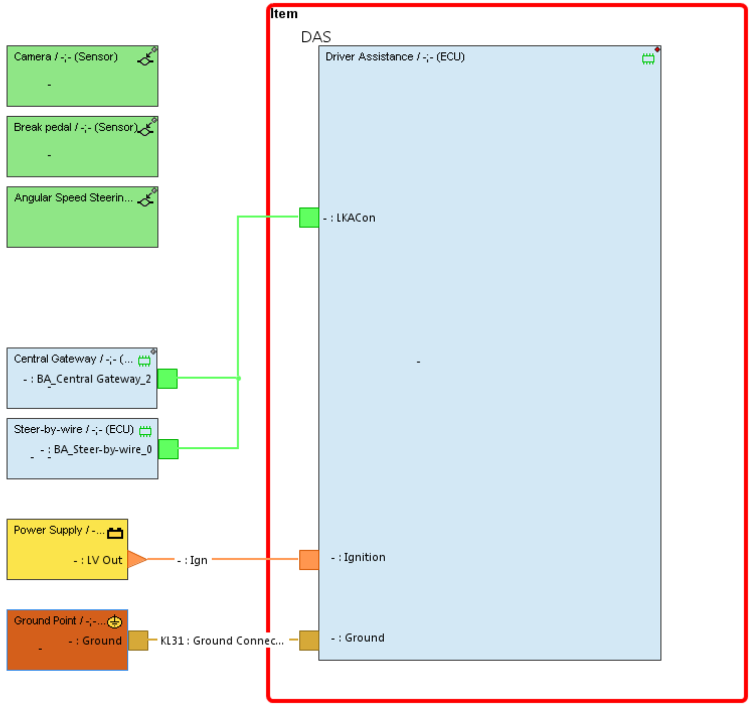


- DS Driving Scenario Catalogue / -;- (Requirement Packa
  - Driving Scenario Table / -;- (Table)
  - DS.1 Country Roads / -;- (Operational Situation)
  - DS.2 Main Roads / -;- (Operational Situation)
  - DS.3 Icy Roads / -;- (Operational Situation)
  - DS.4 Motorway / -;- (Operational Situation)
  - DS.5 Motorway Roadworks / -;- (Operational Situat
  - DS.6 Motorway Unexpected Obstacles / -;- (Opera
  - DS.7 Parked / -;- (Operational Situation)
  - DS.8 Parking / -;- (Operational Situation)
  - DS.9 Town / -;- (Operational Situation)



- OC Operating Conditions / -;- (Requirement Package
  - Operating Conditions Table / -;- (Table)
  - OC.1 Engine Off / -;- (Operating Mode)
  - OC.2 Idle / -;- (Operating Mode)
  - OC.3 Gear Engaged / -;- (Operating Mode)
  - OC.4 Low Speed / -;- (Operating Mode)
  - OC.5 High Speed / -;- (Operating Mode)
  - OC.6 Cruise Control Active / -;- (Operating Mode
  - OC.7 Limp Home / -;- (Operating Mode)





Artifacts modeled in PREEvision:

- Feature specifications, functional and non-functional requirements
- Operating scenarios and operating modes
- Logical and topological system architecture including allocation of functions
- Dependencies with other systems

ISO 26262 key areas supported by PREEvision

Item Definition

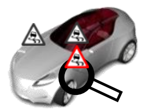
Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

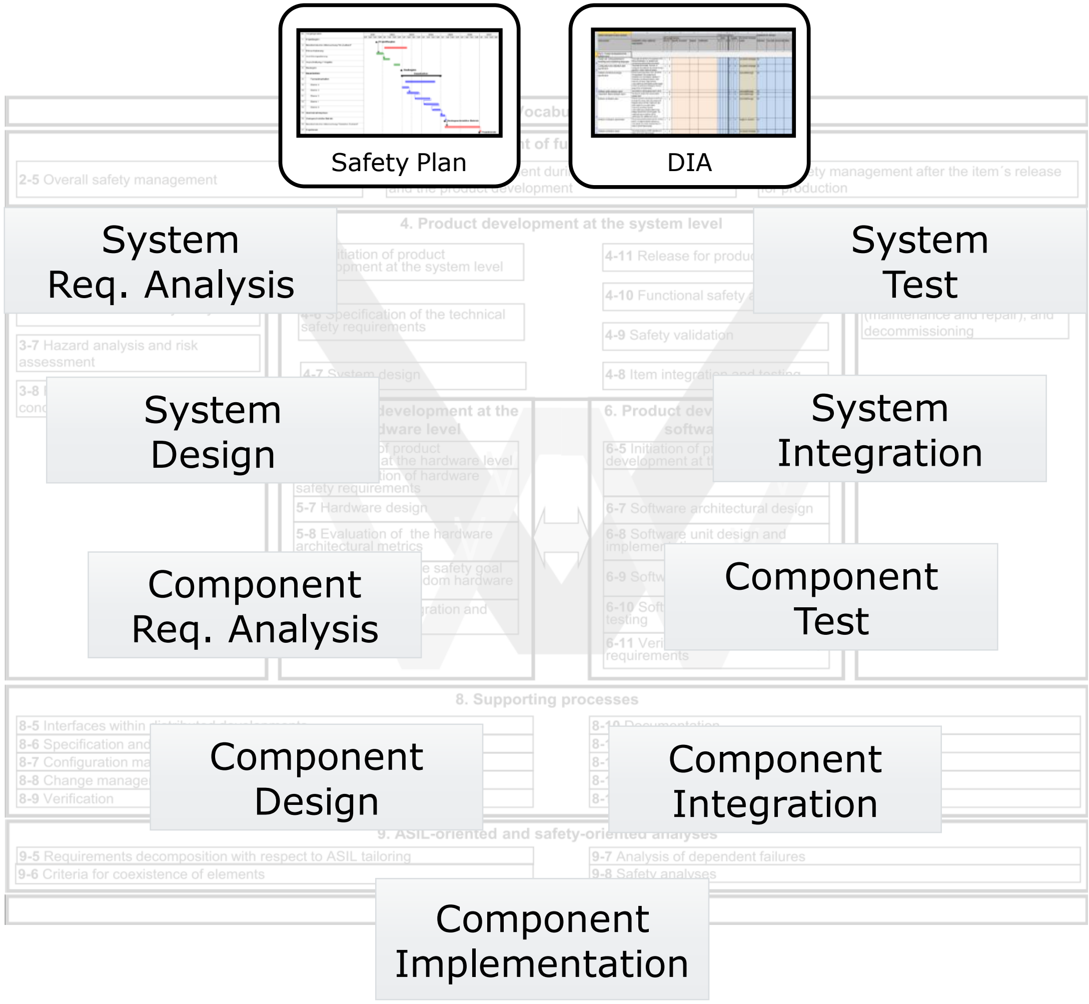
Item Definition


Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

HSI Specification

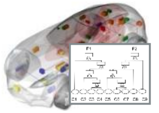

Safety Plan
DIA
System Req. Analysis
System Test
System Design
System Integration
Component Req. Analysis
Component Test
Component Design
Component Integration
Component Implementation
2-5 Overall safety management
4. Product development at the system level
3-7 Hazard analysis and risk assessment
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
4-7 System design
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
6-7 Software architectural design
6-8 Software unit design and implementation
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and
8-7 Configuration ma
8-8 Change manage
8-9 Verification
8-10 Documentation
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses

Safety Case

Validation

Verification

Quantitative Safety Analyses


Qualitative Safety Analyses

Safety Case

Validation

Verification

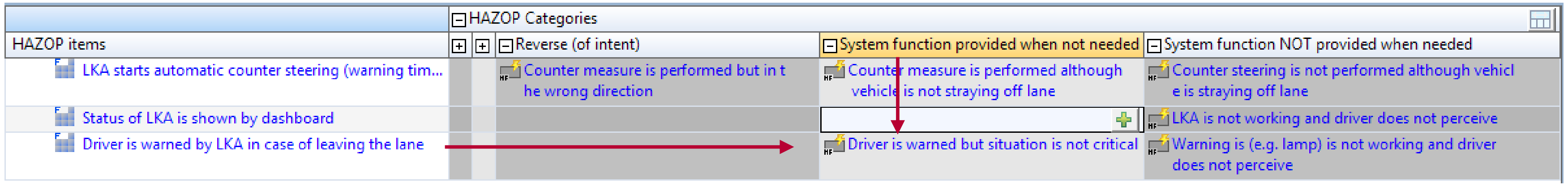
Quantitative Safety Analysis

Qualitative Safety Analysis

HAZard and OPerability Study (HAZOP) Editor

Hazard and Risk Analysis

- HAZOP is a qualitative analysis method to **systematically identify malfunctions** for a system
- The malfunctions can be used in a following Hazard and Risk Analysis (HARA) to derive and classify hazardous events
- The malfunctions are identified based on **defined guide words**
- PREEvision supports HAZOPs with the **HAZOP editor**
- The following artifacts can be used as HAZOP items: logical functions, customer features, requirements

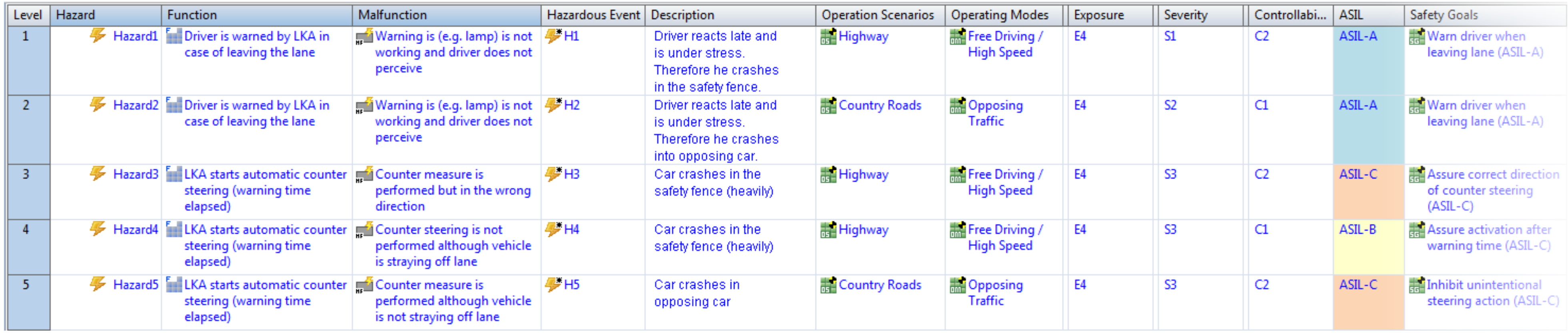


	⊟ HAZOP Categories				
HAZOP items	⊞	⊞	⊟ Reverse (of intent)	⊟ System function provided when not needed	⊟ System function NOT provided when needed
LKA starts automatic counter steering (warning tim...			Counter measure is performed but in t he wrong direction	Counter measure is performed although vehicle is not straying off lane	Counter steering is not performed although vehicl e is straying off lane
Status of LKA is shown by dashboard					LKA is not working and driver does not perceive
Driver is warned by LKA in case of leaving the lane				Driver is warned but situation is not critical	Warning is (e.g. lamp) is not working and driver does not perceive

Hazard Analysis and Risk Assessment (HARA) Editor

Hazard and Risk Analysis

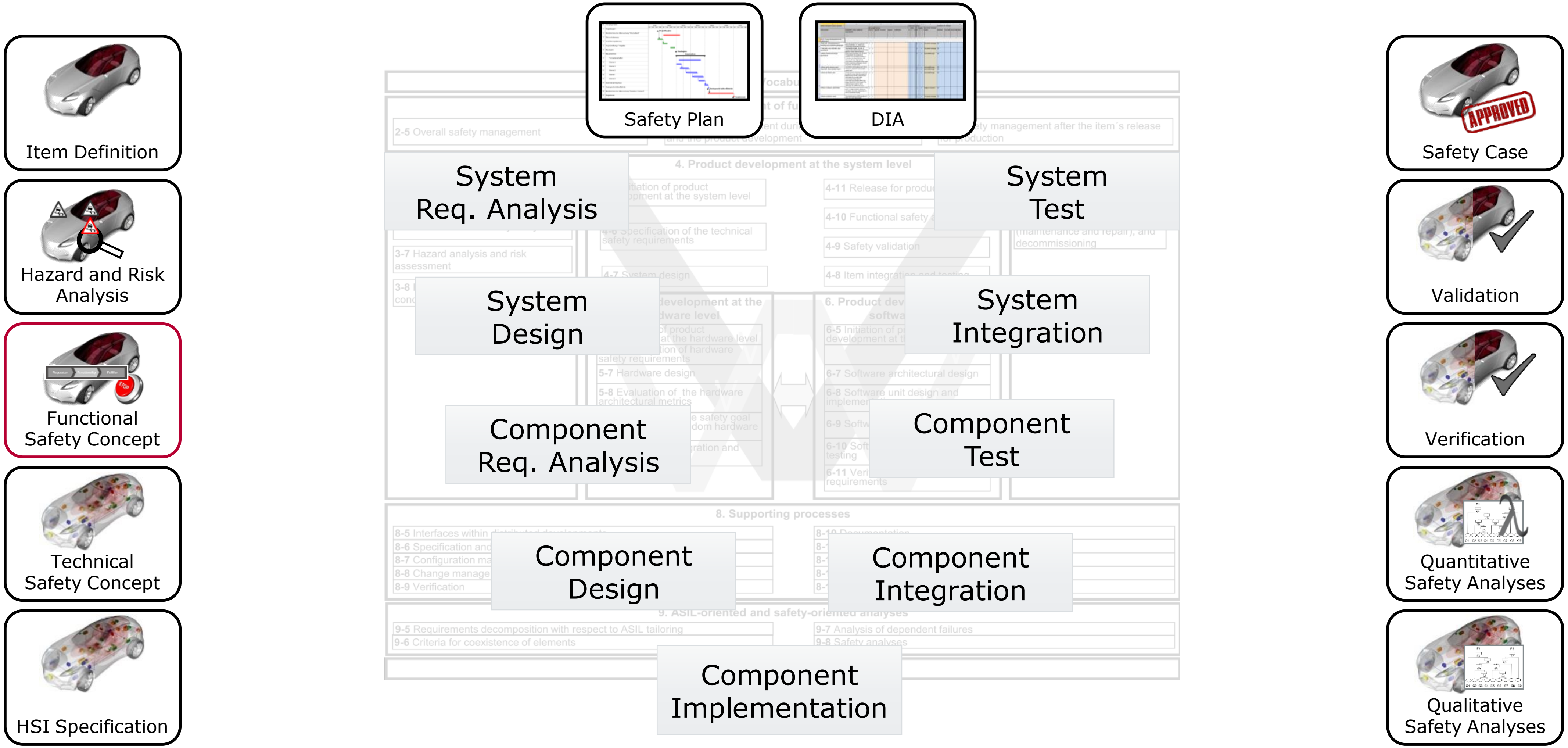
- Pick functions and malfunctions from catalogues
- Pick operating scenarios and operating modes from catalogues
- Automatic calculation of Automotive Safety Integrity Level (ASIL) of hazardous events and derived safety goals
- Highlighting based on ASIL classification
- Create and link safety goals directly in table
- Set Safe State of Safety Goal
- Consistency checks and highlighting
  e.g. check ASIL classification of Hazardous Event against Safety Goal



Level	Hazard	Function	Malfunction	Hazardous Event	Description	Operation Scenarios	Operating Modes	Exposure	Severity	Controllabi...	ASIL	Safety Goals
1	Hazard1	Driver is warned by LKA in case of leaving the lane	Warning is (e.g. lamp) is not working and driver does not perceive	H1	Driver reacts late and is under stress. Therefore he crashes in the safety fence.	Highway	Free Driving / High Speed	E4	S1	C2	ASIL-A	Warn driver when leaving lane (ASIL-A)
2	Hazard2	Driver is warned by LKA in case of leaving the lane	Warning is (e.g. lamp) is not working and driver does not perceive	H2	Driver reacts late and is under stress. Therefore he crashes into opposing car.	Country Roads	Opposing Traffic	E4	S2	C1	ASIL-A	Warn driver when leaving lane (ASIL-A)
3	Hazard3	LKA starts automatic counter steering (warning time elapsed)	Counter measure is performed but in the wrong direction	H3	Car crashes in the safety fence (heavily)	Highway	Free Driving / High Speed	E4	S3	C2	ASIL-C	Assure correct direction of counter steering (ASIL-C)
4	Hazard4	LKA starts automatic counter steering (warning time elapsed)	Counter steering is not performed although vehicle is straying off lane	H4	Car crashes in the safety fence (heavily)	Highway	Free Driving / High Speed	E4	S3	C1	ASIL-B	Assure activation after warning time (ASIL-C)
5	Hazard5	LKA starts automatic counter steering (warning time elapsed)	Counter measure is performed although vehicle is not straying off lane	H5	Car crashes in opposing car	Country Roads	Opposing Traffic	E4	S3	C2	ASIL-C	Inhibit unintentional steering action (ASIL-C)

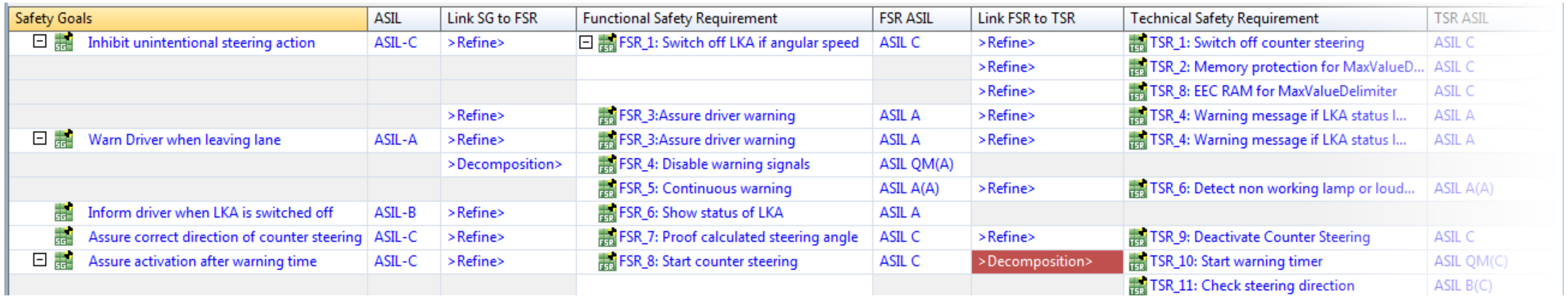
ISO 26262 key areas supported by PREEvision

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)

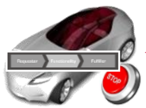


Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis

Functional Safety Concept (FSC) - Requirements



Safety Goals	ASIL	Link SG to FSR	Functional Safety Requirement	FSR ASIL	Link FSR to TSR	Technical Safety Requirement	TSR ASIL
⊟ Inhibit unintentional steering action	ASIL-C	>Refine>	⊟ FSR_1: Switch off LKA if angular speed	ASIL C	>Refine>	TSR_1: Switch off counter steering	ASIL C
					>Refine>	TSR_2: Memory protection for MaxValueD...	ASIL C
					>Refine>	TSR_8: EEC RAM for MaxValueDelimiter	ASIL C
		>Refine>	FSR_3:Assure driver warning	ASIL A	>Refine>	TSR_4: Warning message if LKA status l...	ASIL A
⊟ Warn Driver when leaving lane	ASIL-A	>Refine>	FSR_3:Assure driver warning	ASIL A	>Refine>	TSR_4: Warning message if LKA status l...	ASIL A
		>Decomposition>	FSR_4: Disable warning signals	ASIL QM(A)			
			FSR_5: Continuous warning	ASIL A(A)	>Refine>	TSR_6: Detect non working lamp or loud...	ASIL A(A)
Inform driver when LKA is switched off	ASIL-B	>Refine>	FSR_6: Show status of LKA	ASIL A			
Assure correct direction of counter steering	ASIL-C	>Refine>	FSR_7: Proof calculated steering angle	ASIL C	>Refine>	TSR_9: Deactivate Counter Steering	ASIL C
⊟ Assure activation after warning time	ASIL-C	>Refine>	FSR_8: Start counter steering	ASIL C	>Decomposition>	TSR_10: Start warning timer	ASIL QM(C)
						TSR_11: Check steering direction	ASIL B(C)

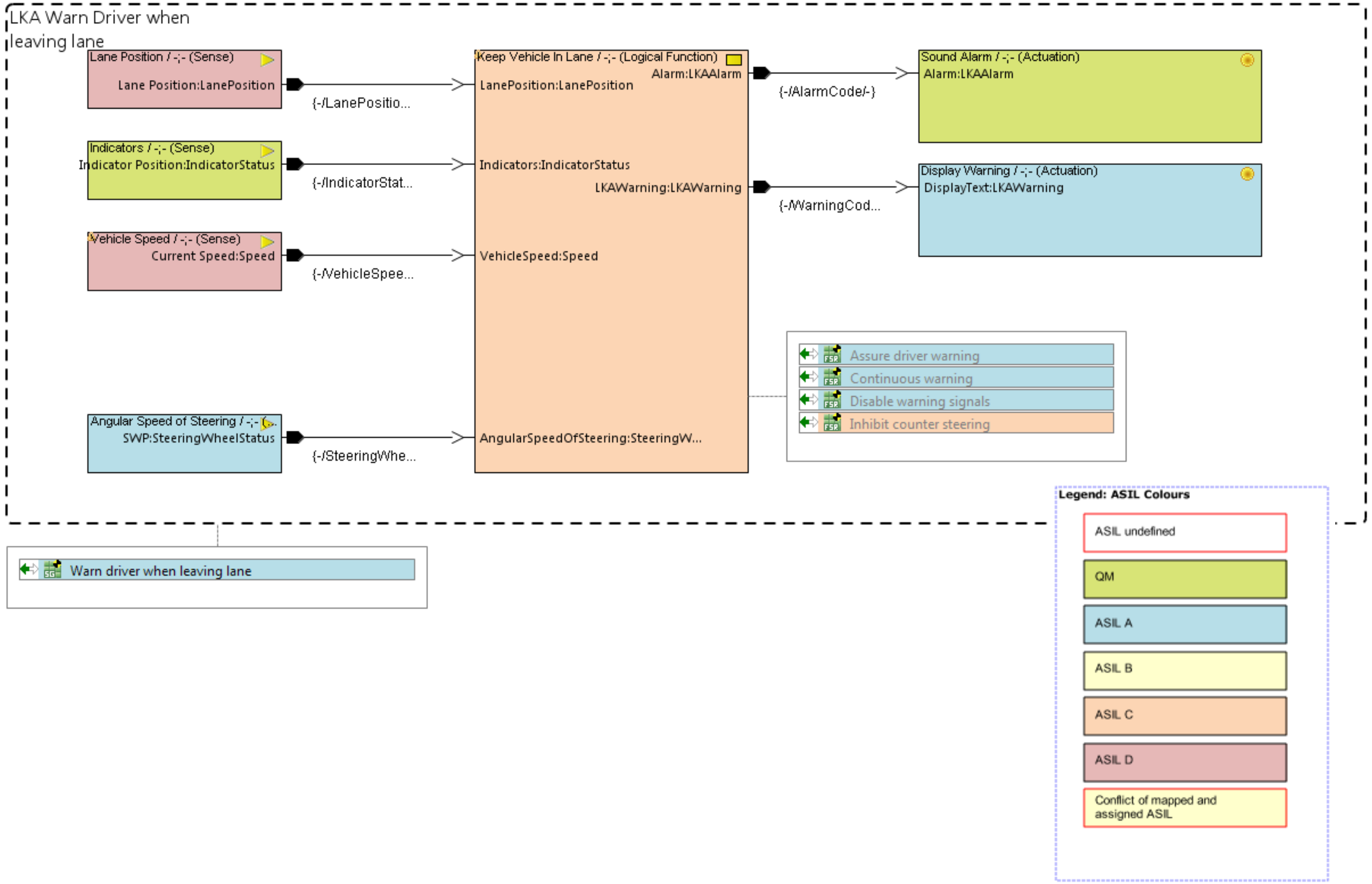


Functional Safety Concept

- Support detailing safety goals via
  - Refinement
  - Decomposition
- Prevent errors and inconsistencies
  - Trace tables with **automatic validation** of ASIL decomposition
- Increase efficiency and reduce manual efforts
  - Automatically **create valid decompositions** of Safety Goals, Functional Safety Requirements and Technical Safety Requirements via metrics

Functional Safety Concept (FSC) - High Level

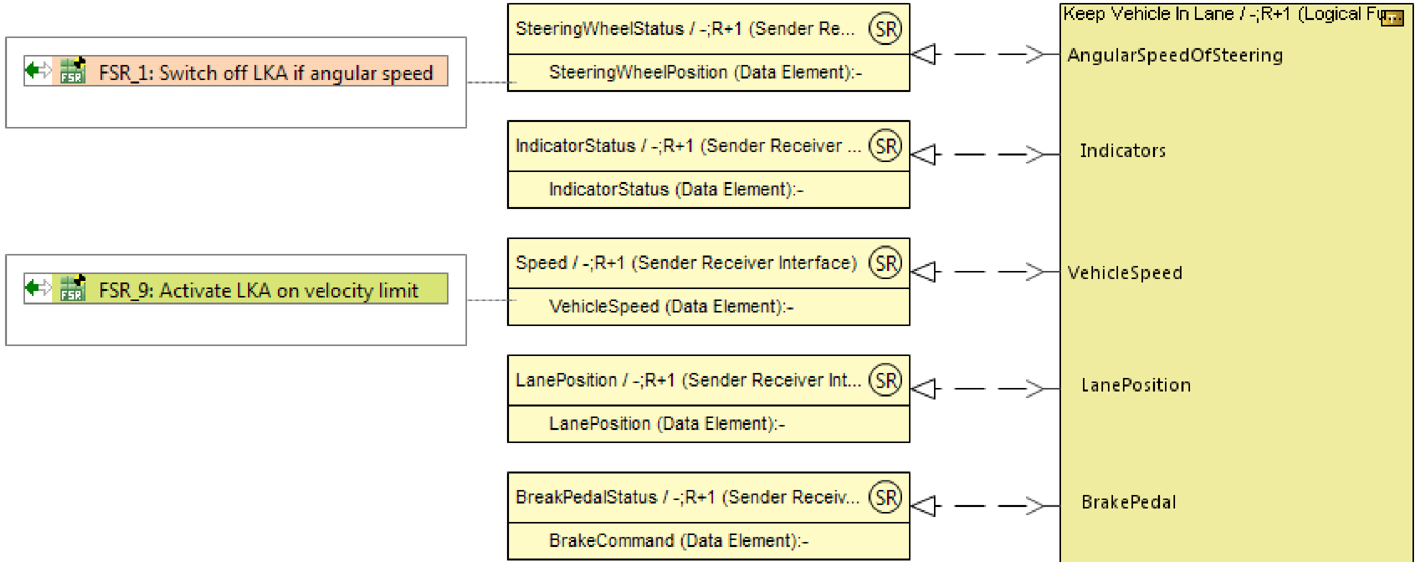
Functional Safety Concept


LKA Warn Driver when leaving lane
Lane Position / -;- (Sense)
Lane Position:LanePosition
{-/LanePositio...
Indicators / -;- (Sense)
Indicator Position:IndicatorStatus
{-/IndicatorStat...
Vehicle Speed / -;- (Sense)
Current Speed:Speed
{-/VehicleSpee...
Angular Speed of Steering / -;- (...
SWP:SteeringWheelStatus
{-/SteeringWhe...
Keep Vehicle In Lane / -;- (Logical Function)
Alarm:LKAAlarm
LanePosition:LanePosition
Indicators:IndicatorStatus
LKAWarning:LKAWarning
VehicleSpeed:Speed
AngularSpeedOfSteering:SteeringW...
{-/AlarmCode/-}
{-/WarningCod...
Sound Alarm / -;- (Actuation)
Alarm:LKAAlarm
Display Warning / -;- (Actuation)
DisplayText:LKAWarning
FSR Assure driver warning
FSR Continuous warning
FSR Disable warning signals
FSR Inhibit counter steering
SG Warn driver when leaving lane
Legend: ASIL Colours
ASIL undefined
QM
ASIL A
ASIL B
ASIL C
ASIL D
Conflict of mapped and assigned ASIL

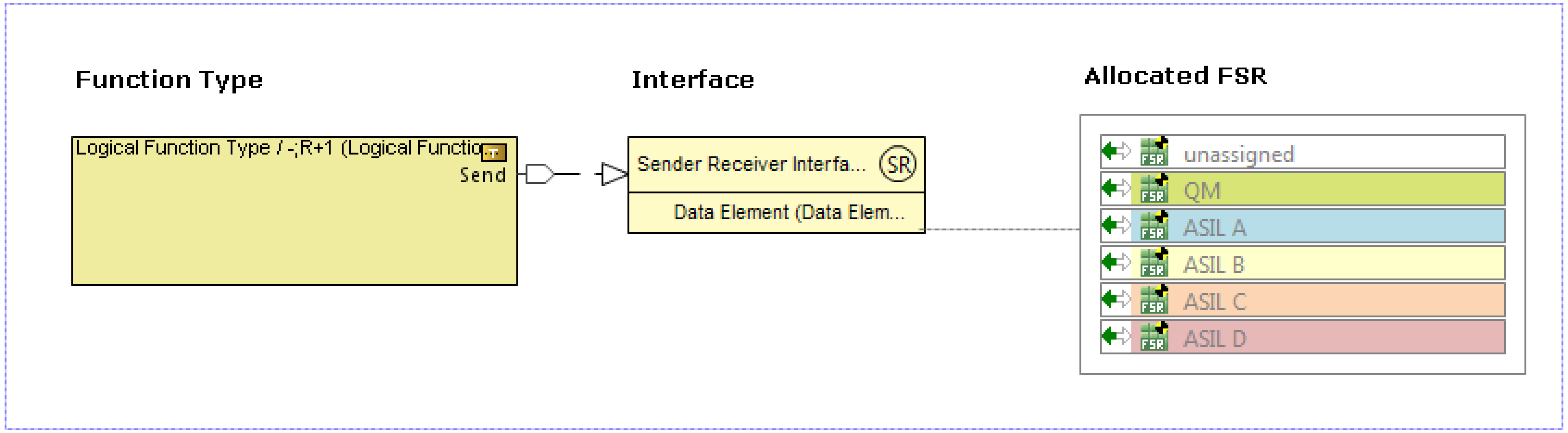
Functional Safety Concept (FSC) – Detailed Level

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)

Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis

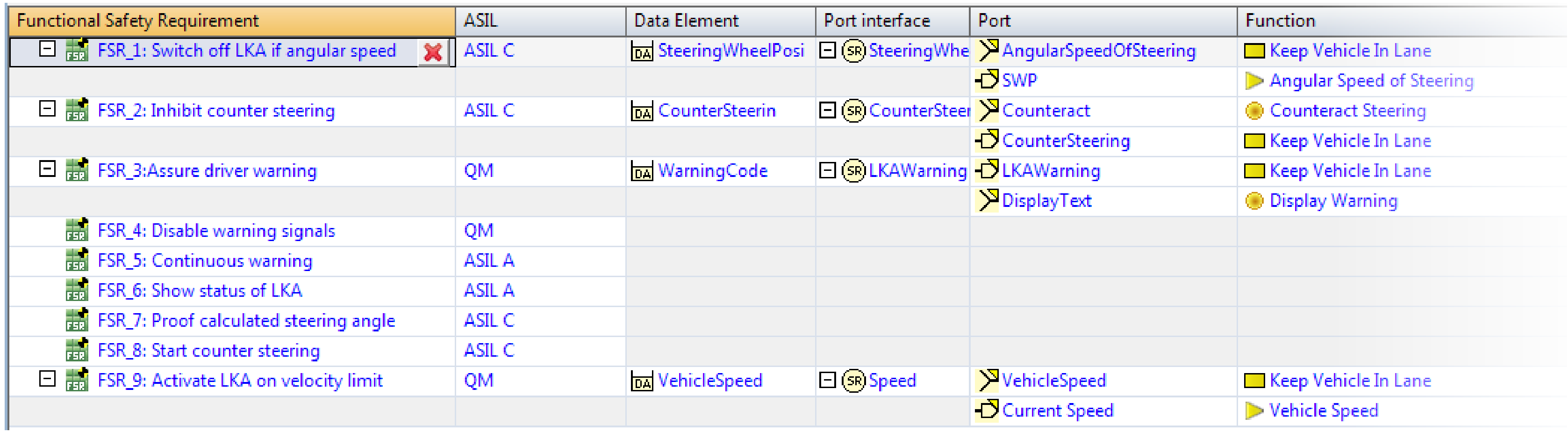

FSR_1: Switch off LKA if angular speed
FSR_9: Activate LKA on velocity limit
SteeringWheelStatus / -;R+1 (Sender Re... SR
SteeringWheelPosition (Data Element):-
IndicatorStatus / -;R+1 (Sender Receiver ... SR
IndicatorStatus (Data Element):-
Speed / -;R+1 (Sender Receiver Interface) SR
VehicleSpeed (Data Element):-
LanePosition / -;R+1 (Sender Receiver Int... SR
LanePosition (Data Element):-
BreakPedalStatus / -;R+1 (Sender Receiv... SR
BrakeCommand (Data Element):-
Keep Vehicle In Lane / -;R+1 (Logical Fu...
AngularSpeedOfSteering
Indicators
VehicleSpeed
LanePosition
BrakePedal

Functional Safety Concept


Function Type
Interface
Allocated FSR
Logical Function Type / -;R+1 (Logical Functio...
Send
Sender Receiver Interfa... SR
Data Element (Data Elem...
unassigned
QM
ASIL A
ASIL B
ASIL C
ASIL D

Functional Safety Concept (FSC) - Requirements Allocation

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)
Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis

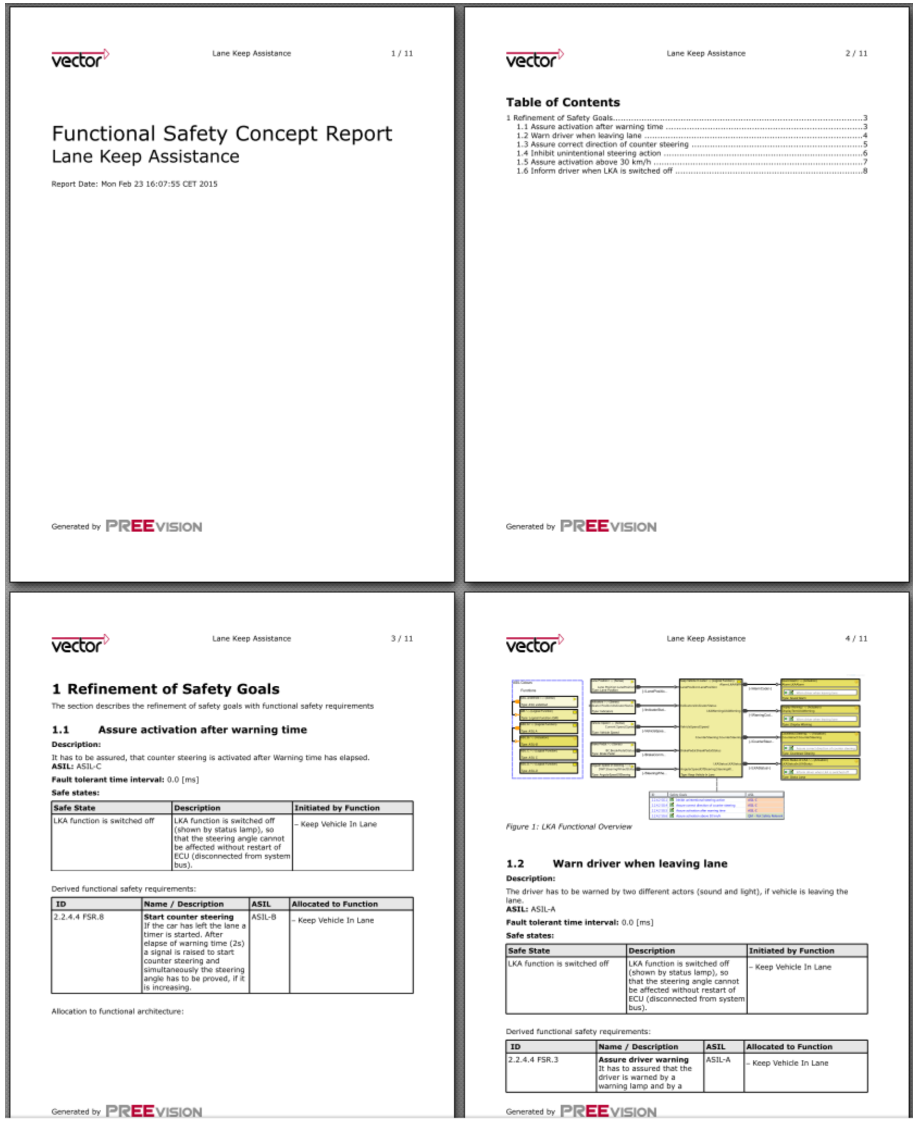


Functional Safety Requirement	ASIL	Data Element	Port interface	Port	Function
FSR_1: Switch off LKA if angular speed	ASIL C	SteeringWheelPosi	SteeringWhe	AngularSpeedOfSteering	Keep Vehicle In Lane
				SWP	Angular Speed of Steering
FSR_2: Inhibit counter steering	ASIL C	CounterSteerin	CounterSteer	Counteract	Counteract Steering
				CounterSteering	Keep Vehicle In Lane
FSR_3:Assure driver warning	QM	WarningCode	LKAWarning	LKAWarning	Keep Vehicle In Lane
				DisplayText	Display Warning
FSR_4: Disable warning signals	QM				
FSR_5: Continuous warning	ASIL A				
FSR_6: Show status of LKA	ASIL A				
FSR_7: Proof calculated steering angle	ASIL C				
FSR_8: Start counter steering	ASIL C				
FSR_9: Activate LKA on velocity limit	QM	VehicleSpeed	Speed	VehicleSpeed	Keep Vehicle In Lane
				Current Speed	Vehicle Speed

Functional Safety Concept

- Tabular trace views visualize the **allocation** of functional safety requirements to the preliminary architecture elements

Functional Safety Concept (FSC) - Report



Lane Keep Assistance 1 / 11

Functional Safety Concept Report
Lane Keep Assistance

Report Date: Mon Feb 23 16:07:55 CET 2015

Generated by PREEVISION

Lane Keep Assistance 2 / 11

Table of Contents

Generated by PREEVISION

Lane Keep Assistance 3 / 11

1 Refinement of Safety Goals

The section describes the refinement of safety goals with functional safety requirements

1.1 Assure activation after warning time

Description:

It has to be assured, that counter steering is activated after Warning time has elapsed.
ASIL: ASIL-C

Fault tolerant time interval: 0.0 [ms]

Safe states:

Safe State	Description	Initiated by Function
LKA function is switched off	LKA function is switched off (shown by status lamp), so that the steering angle cannot be affected without restart of ECU (disconnected from system bus).	– Keep Vehicle In Lane

Derived functional safety requirements:

ID	Name / Description	ASIL	Allocated to Function
2.2.4.4 FSR.8	**Start counter steering** If the car has left the lane a timer is started. After elapse of warning time (2s) a signal is raised to start counter steering and simultaneously the steering angle has to be proved, if it is increasing.	ASIL-B	– Keep Vehicle In Lane

Allocation to functional architecture:

Generated by PREEVISION

Lane Keep Assistance 4 / 11

Figure 1: LKA Functional Overview

1.2 Warn driver when leaving lane

Description:

The driver has to be warned by two different actors (sound and light), if vehicle is leaving the lane.
ASIL: ASIL-A

Fault tolerant time interval: 0.0 [ms]

Safe states:

Safe State	Description	Initiated by Function
LKA function is switched off	LKA function is switched off (shown by status lamp), so that the steering angle cannot be affected without restart of ECU (disconnected from system bus).	– Keep Vehicle In Lane

Derived functional safety requirements:

ID	Name / Description	ASIL	Allocated to Function
2.2.4.4 FSR.3	**Assure driver warning** It has to assured that the driver is warned by a warning lamp and by a	ASIL-A	– Keep Vehicle In Lane

Generated by PREEVISION

- ISO 26262 compliant report for Functional Safety Concept (FSC)
- Automatically generated from model data
- Report template can be adapted to fit to company specific requirements

ISO 26262 key areas supported by PREEvision

Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

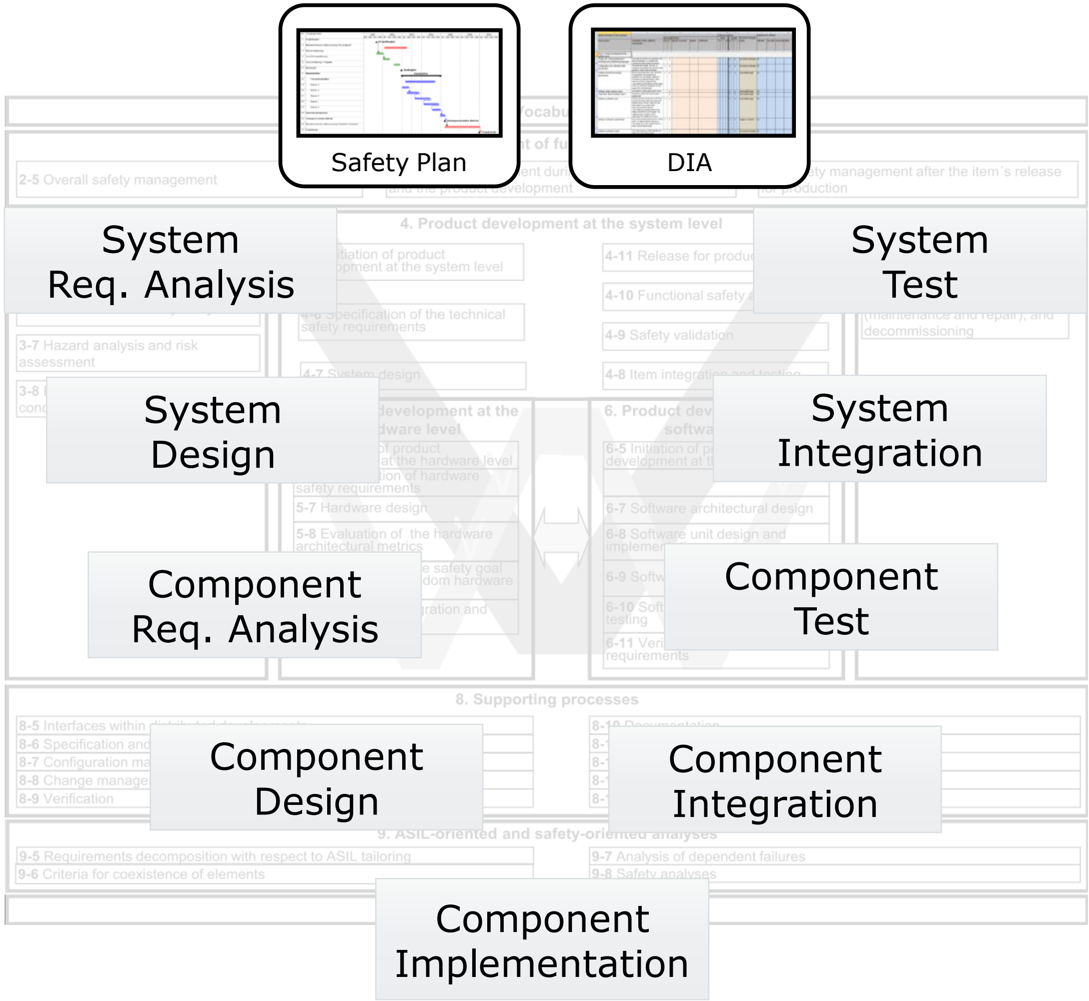
Item Definition

Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

HSI Specification



Safety Plan

DIA

System Req. Analysis

System Test

System Design

System Integration

Component Req. Analysis

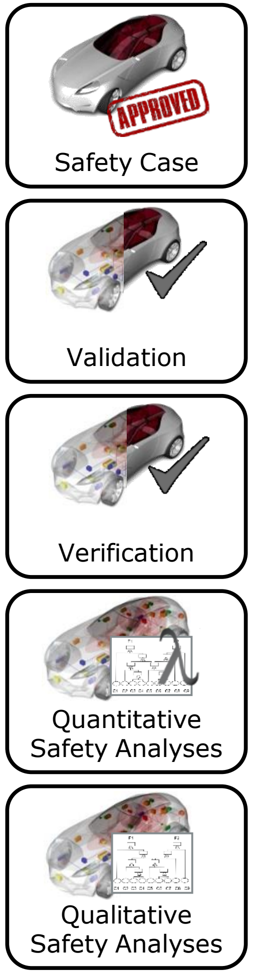
Component Test

Component Design

Component Integration

Component Implementation

2-5 Overall safety management
safety management after the item´s release for production
4. Product development at the system level
4-11 Release for production
4-10 Functional safety
4-9 Safety validation
4-8 Item integration and testing
4-7 System design
3-7 Hazard analysis and risk assessment
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
6-7 Software architectural design
6-8 Software unit design and implementation
6-11 Verification of software requirements
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and
8-7 Configuration ma
8-8 Change manage
8-9 Verification
8-10 Documentation
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses



Safety Case

Validation

Verification

Quantitative Safety Analyses

Qualitative Safety Analyses

Safety Case

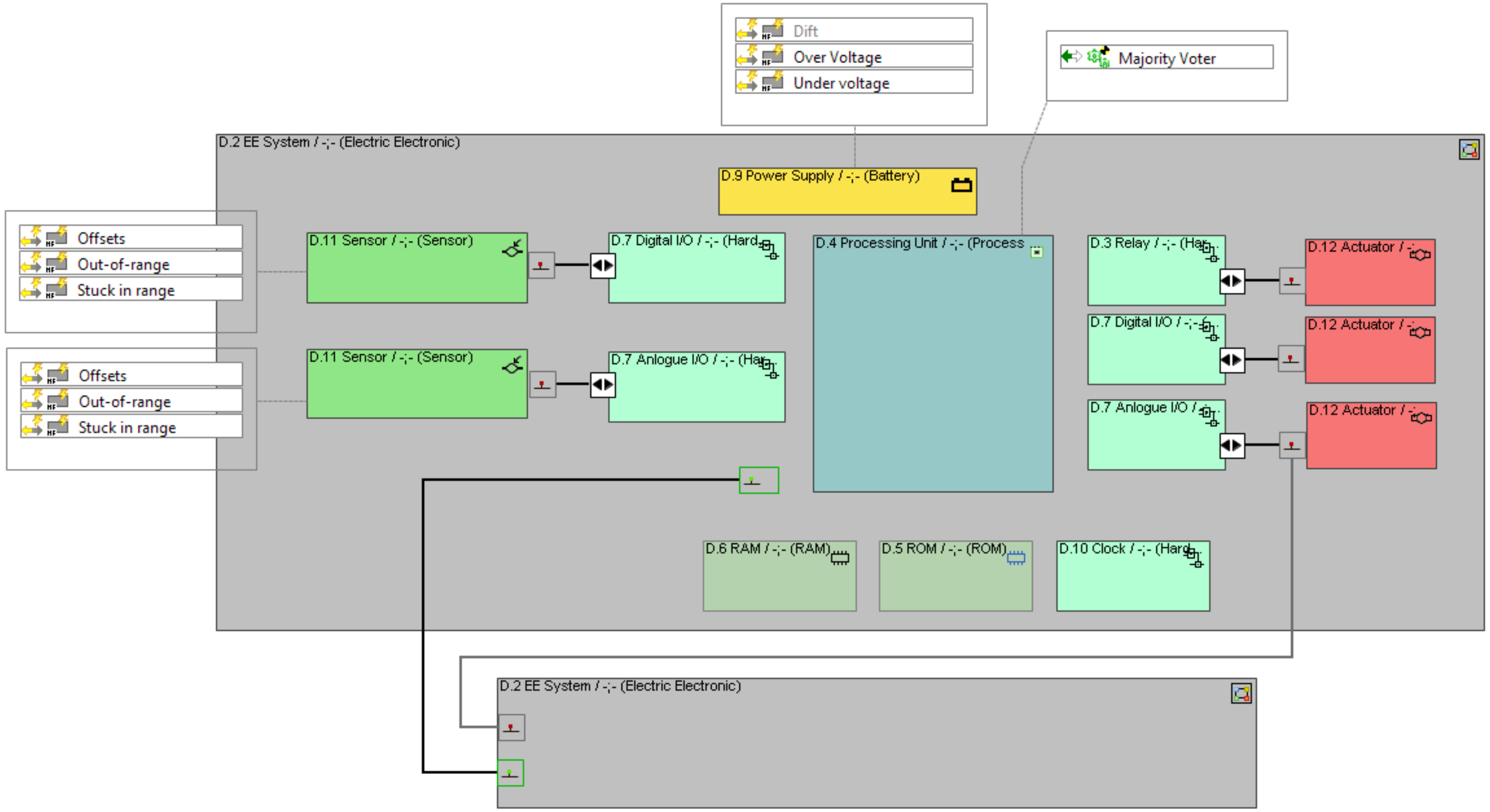
Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

Technical Safety Concept (TSC) – Hardware – High Level



Technical Safety Concept

- HW elements can be modeled and associated with technical safety requirements, faults and safety mechanisms
- Powerful library concept for faults and safety mechanisms

1) Example Based on ISO 26262 – 5, Annex D.1

Technical Safety Concept (TSC) – Hardware – Detailed Level

Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

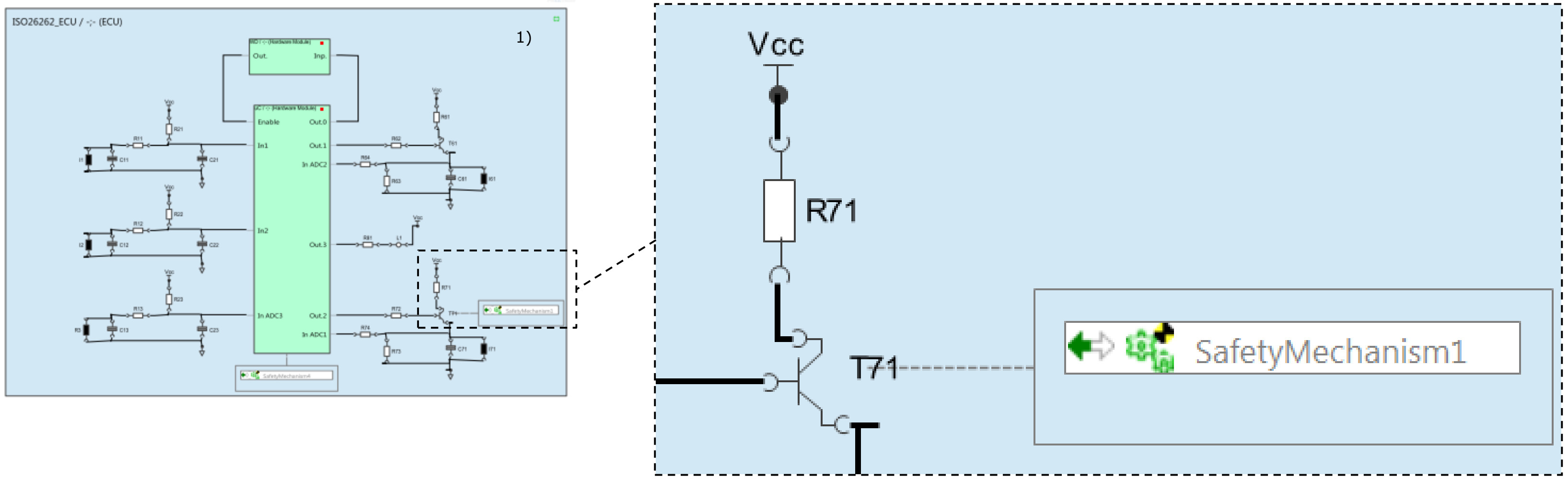
Safety Case

Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

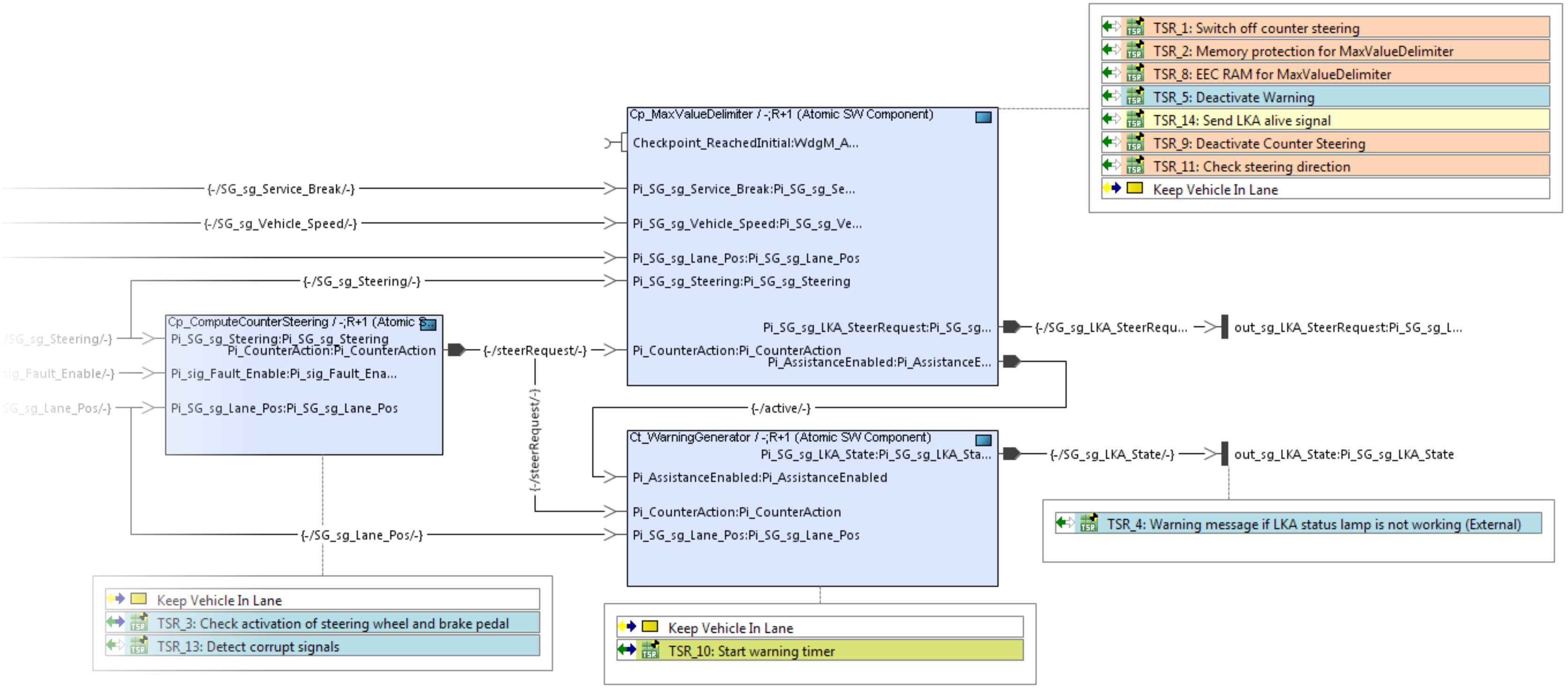


Technical Safety Concept

- HW elements can be modeled and associated with technical safety requirements, faults and safety mechanisms
- Powerful library concept for faults and safety mechanisms
- HW safety design can be detailed down to the device level

1) Example Based on ISO 26262 – 5, Annex E.1

Technical Safety Concept (TSC) – Software – Detailed Level


TSR_1: Switch off counter steering
TSR_2: Memory protection for MaxValueDelimiter
TSR_8: EEC RAM for MaxValueDelimiter
TSR_5: Deactivate Warning
TSR_14: Send LKA alive signal
TSR_9: Deactivate Counter Steering
TSR_11: Check steering direction
Keep Vehicle In Lane
Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
Checkpoint_ReachedInitial:WdgM_A...
{-/SG_sg_Service_Break/-}
Pi_SG_sg_Service_Break:Pi_SG_sg_Se...
{-/SG_sg_Vehicle_Speed/-}
Pi_SG_sg_Vehicle_Speed:Pi_SG_sg_Ve...
Pi_SG_sg_Lane_Pos:Pi_SG_sg_Lane_Pos
{-/SG_sg_Steering/-}
Pi_SG_sg_Steering:Pi_SG_sg_Steering
Pi_SG_sg_LKA_SteerRequest:Pi_SG_sg...
{-/SG_sg_LKA_SteerRequ...
out_sg_LKA_SteerRequest:Pi_SG_sg_L...
Pi_CounterAction:Pi_CounterAction
Pi_AssistanceEnabled:Pi_AssistanceE...
Cp_ComputeCounterSteering / -;R+1 (Atomic S...
SG_sg_Steering/-}
Pi_SG_sg_Steering:Pi_SG_sg_Steering
Pi_CounterAction:Pi_CounterAction
{-/steerRequest/-}
sig_Fault_Enable/-}
Pi_sig_Fault_Enable:Pi_sig_Fault_Ena...
SG_sg_Lane_Pos/-}
Pi_SG_sg_Lane_Pos:Pi_SG_sg_Lane_Pos
{-/active/-}
{-/steerRequest/-}
Ct_WarningGenerator / -;R+1 (Atomic SW Component)
Pi_SG_sg_LKA_State:Pi_SG_sg_LKA_Sta...
{-/SG_sg_LKA_State/-}
out_sg_LKA_State:Pi_SG_sg_LKA_State
Pi_AssistanceEnabled:Pi_AssistanceEnabled
Pi_CounterAction:Pi_CounterAction
{-/SG_sg_Lane_Pos/-}
Pi_SG_sg_Lane_Pos:Pi_SG_sg_Lane_Pos
TSR_4: Warning message if LKA status lamp is not working (External)
Keep Vehicle In Lane
TSR_3: Check activation of steering wheel and brake pedal
TSR_13: Detect corrupt signals
Keep Vehicle In Lane
TSR_10: Start warning timer

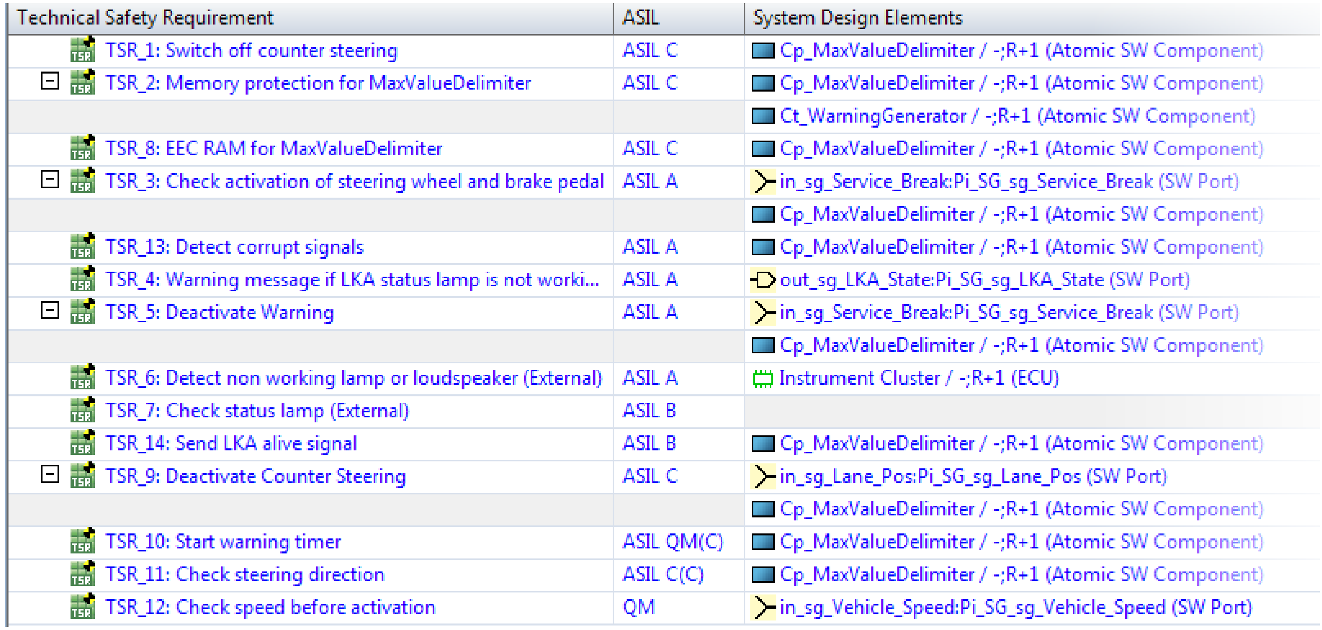
Technical Safety Concept

- SW safety design, technical safety requirements (TSR), faults and safety mechanisms (SM) can be detailed down to ports, interfaces and data elements

- AUTOSAR Import / Export of SW Architecture

Technical Safety Concept (TSC) – Trace Editor

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)
Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis



Technical Safety Requirement	ASIL	System Design Elements
TSR_1: Switch off counter steering	ASIL C	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_2: Memory protection for MaxValueDelimiter	ASIL C	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
		Ct_WarningGenerator / -;R+1 (Atomic SW Component)
TSR_8: EEC RAM for MaxValueDelimiter	ASIL C	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_3: Check activation of steering wheel and brake pedal	ASIL A	in_sg_Service_Break:Pi_SG_sg_Service_Break (SW Port)
		Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_13: Detect corrupt signals	ASIL A	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_4: Warning message if LKA status lamp is not worki...	ASIL A	out_sg_LKA_State:Pi_SG_sg_LKA_State (SW Port)
TSR_5: Deactivate Warning	ASIL A	in_sg_Service_Break:Pi_SG_sg_Service_Break (SW Port)
		Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_6: Detect non working lamp or loudspeaker (External)	ASIL A	Instrument Cluster / -;R+1 (ECU)
TSR_7: Check status lamp (External)	ASIL B	
TSR_14: Send LKA alive signal	ASIL B	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_9: Deactivate Counter Steering	ASIL C	in_sg_Lane_Pos:Pi_SG_sg_Lane_Pos (SW Port)
		Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_10: Start warning timer	ASIL QM(C)	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_11: Check steering direction	ASIL C(C)	Cp_MaxValueDelimiter / -;R+1 (Atomic SW Component)
TSR_12: Check speed before activation	QM	in_sg_Vehicle_Speed:Pi_SG_sg_Vehicle_Speed (SW Port)

- Tabular trace views visualize the allocation of Technical Safety Requirements (TSR) to the technical architecture elements

Technical Safety Concept

ISO 26262 key areas supported by PREEvision

Item Definition

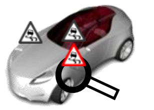
Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

Item Definition

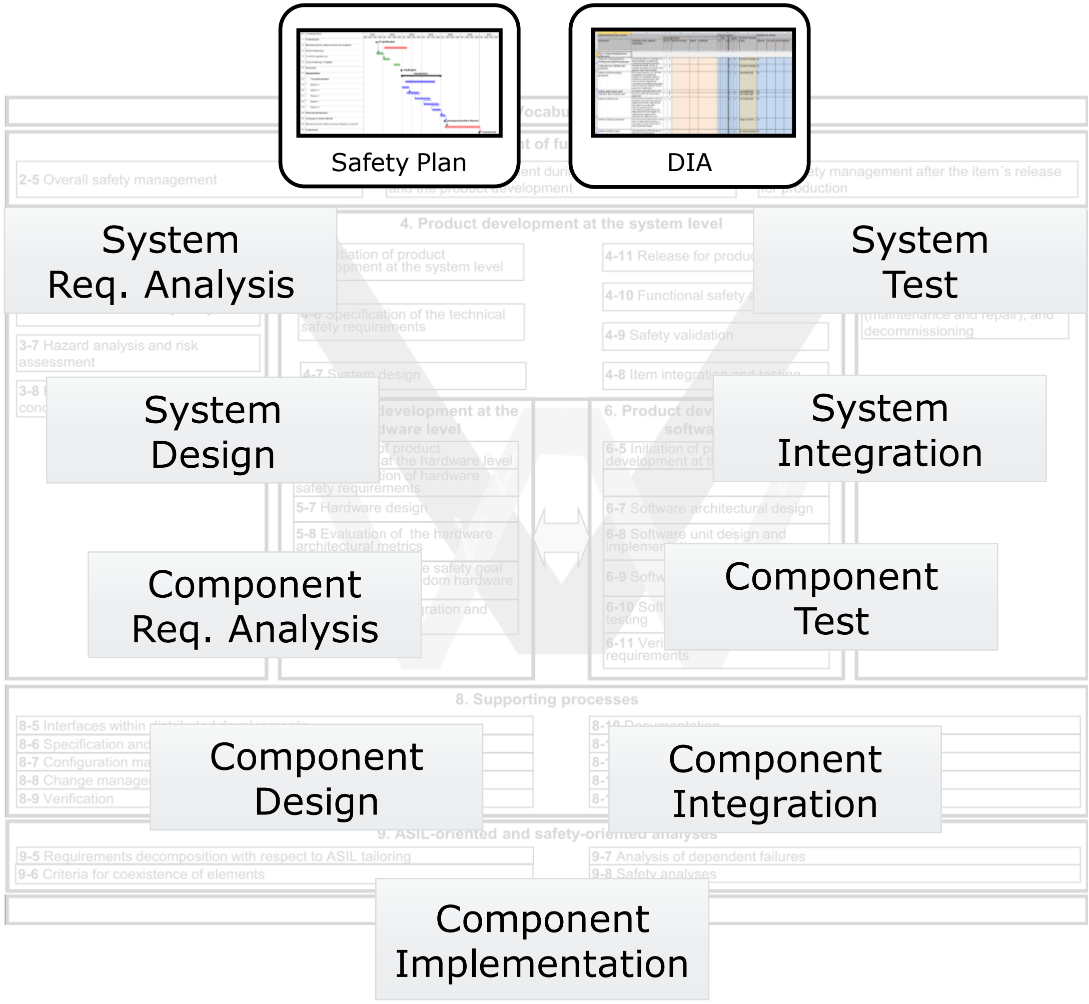


Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

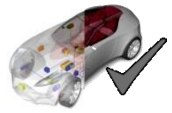
HSI Specification



Safety Plan
DIA
System Req. Analysis
System Test
System Design
System Integration
Component Req. Analysis
Component Test
Component Design
Component Integration
Component Implementation
2-5 Overall safety management
4. Product development at the system level
3-7 Hazard analysis and risk assessment
4-7 System design
4-9 Safety validation
4-10 Functional safety
4-11 Release for production
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
6-7 Software architectural design
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and
8-7 Configuration ma
8-8 Change manage
8-9 Verification
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses

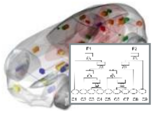
Safety Case

Validation



Verification

Quantitative Safety Analyses



Qualitative Safety Analyses

Safety Case

Validation

Verification

Quantitative Safety Analysis

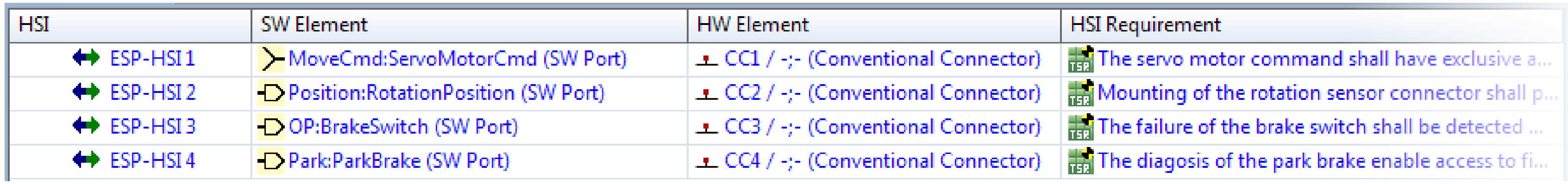
Qualitative Safety Analysis

Hardware-Software Interface (HSI) Specification

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)

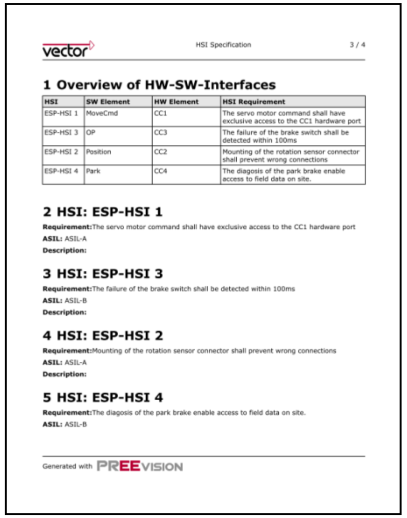
Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis

- Efficiently specify HSI via HSI Editor
  - Create HSI-Requirements directly in Editor
  - Pick HW/SW Elements in Editor from existing Architecture



HSI	SW Element	HW Element	HSI Requirement
ESP-HSI 1	MoveCmd:ServoMotorCmd (SW Port)	CC1 / -;- (Conventional Connector)	The servo motor command shall have exclusive a...
ESP-HSI 2	Position:RotationPosition (SW Port)	CC2 / -;- (Conventional Connector)	Mounting of the rotation sensor connector shall p...
ESP-HSI 3	OP:BrakeSwitch (SW Port)	CC3 / -;- (Conventional Connector)	The failure of the brake switch shall be detected ...
ESP-HSI 4	Park:ParkBrake (SW Port)	CC4 / -;- (Conventional Connector)	The diagosis of the park brake enable access to fi...

- Efficiently generate HSI Specification
  - Work Product required by ISO 26262-4/5/6



vector HSI Specification 3 / 4

1 Overview of HW-SW-Interfaces

HSI	SW Element	HW Element	HSI Requirement
ESP-HSI 1	MoveCmd	CC1	The servo motor command shall have exclusive access to the CC1 hardware port
ESP-HSI 3	OP	CC3	The failure of the brake switch shall be detected within 100ms
ESP-HSI 2	Position	CC2	Mounting of the rotation sensor connector shall prevent wrong connections
ESP-HSI 4	Park	CC4	The diagosis of the park brake enable access to field data on site.

2 HSI: ESP-HSI 1

Requirement: The servo motor command shall have exclusive access to the CC1 hardware port

ASIL: ASIL-A

Description:

3 HSI: ESP-HSI 3

Requirement: The failure of the brake switch shall be detected within 100ms

ASIL: ASIL-B

Description:

4 HSI: ESP-HSI 2

Requirement: Mounting of the rotation sensor connector shall prevent wrong connections

ASIL: ASIL-A

Description:

5 HSI: ESP-HSI 4

Requirement: The diagosis of the park brake enable access to field data on site.

ASIL: ASIL-B

Generated with PREEVISION

HSI Specification

See ISO 26262 – 4, Annex B

ISO 26262 key areas supported by PREEvision

Item Definition

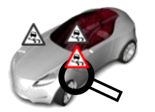
Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

Item Definition

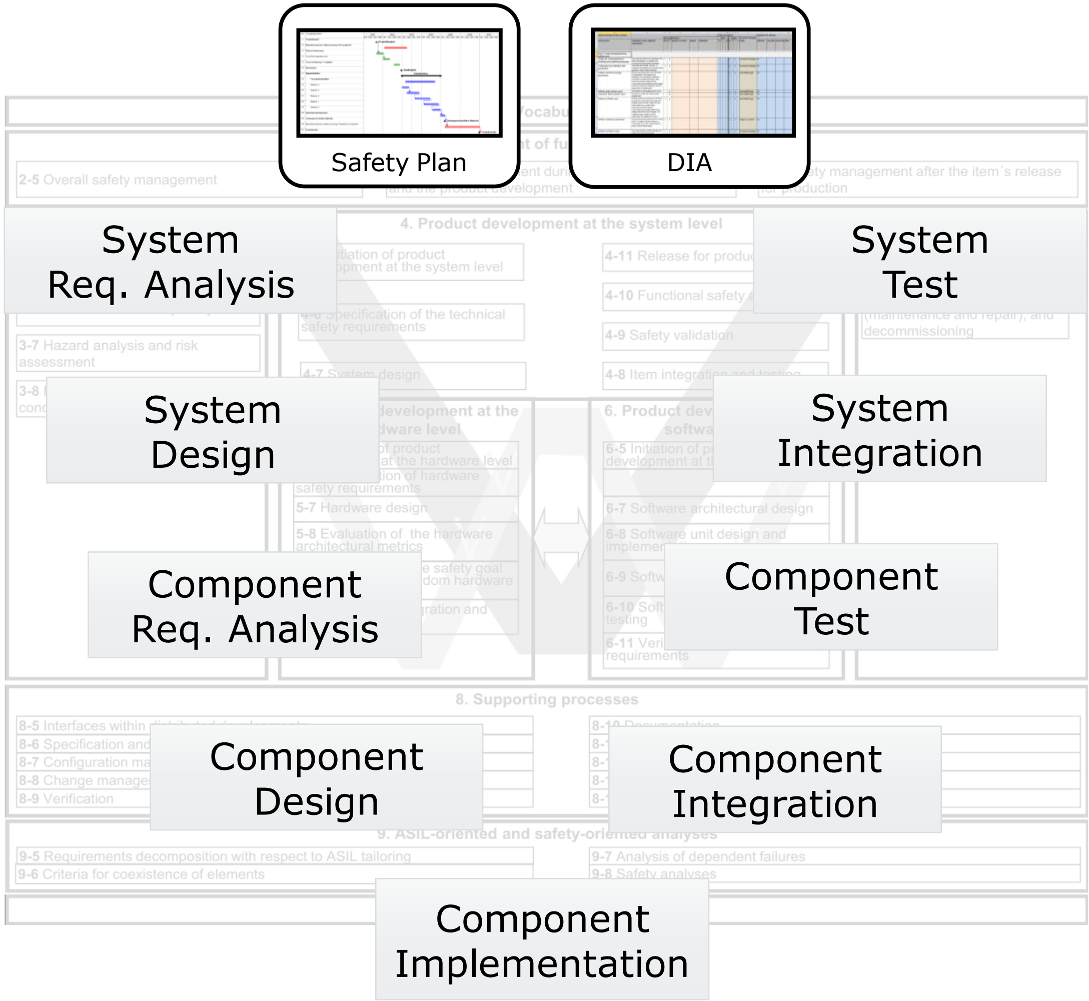


Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

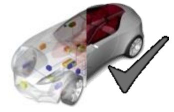
HSI Specification



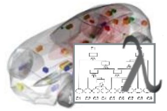
Safety Plan
DIA
2-5 Overall safety management
4. Product development at the system level
System Req. Analysis
System Test
3-7 Hazard analysis and risk assessment
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
4-7 System design
System Design
System Integration
6. Product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
Component Req. Analysis
Component Test
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
Component Design
Component Integration
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
Component Implementation

Safety Case

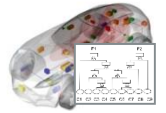
Validation



Verification



Quantitative Safety Analyses



Qualitative Safety Analyses

Safety Case

Validation

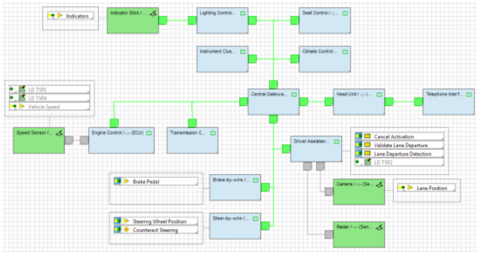
Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

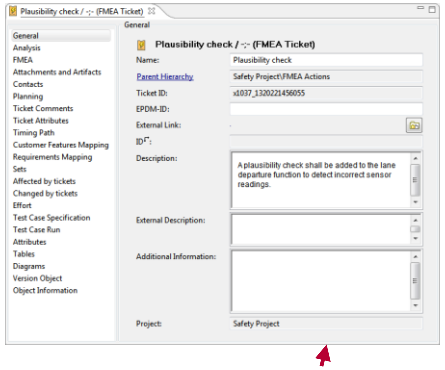
Failure Mode and Effects Analysis (FMEA)

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)
Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis



- Use technical architecture to derive FMEA Parts

- Analysis leads to FMEA issues which can lead to new requirements or solutions



Plausibility check / -;- (FMEA Ticket)

General

Plausibility check / -;- (FMEA Ticket)

Name: Plausibility check

Parent Hierarchy: Safety Project\FMEA Actions

Ticket ID: x1037_1320221456055

EPDM-ID:

External Link:

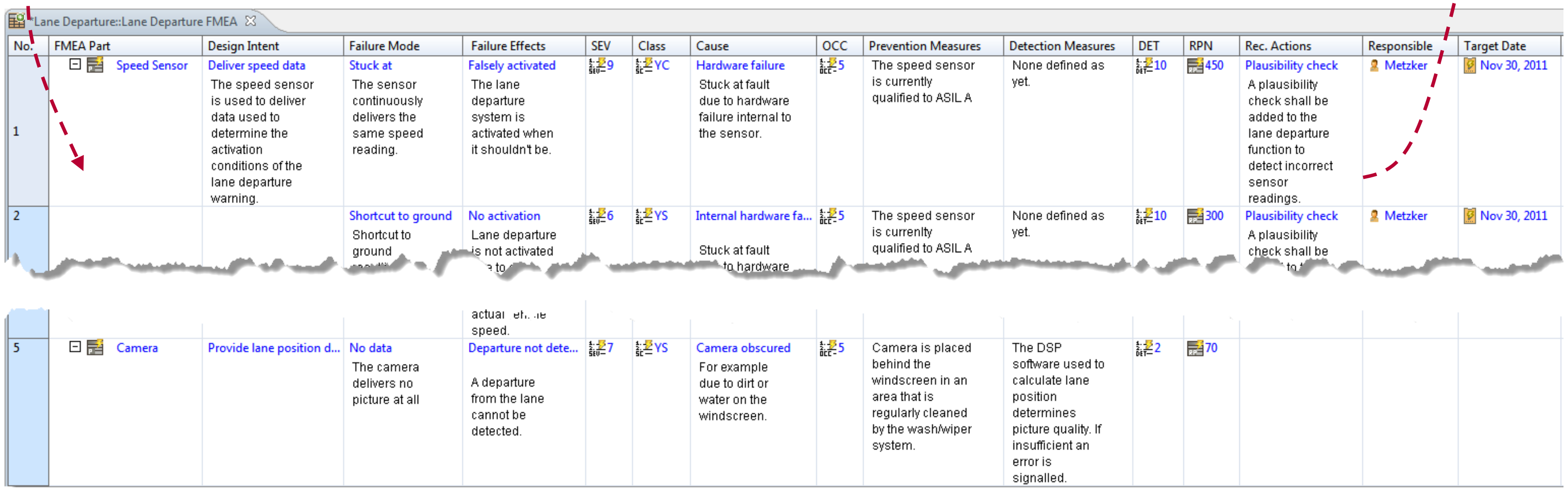
ID:

Description: A plausibility check shall be added to the lane departure function to detect incorrect sensor readings.

External Description:

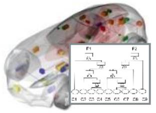
Additional Information:

Project: Safety Project



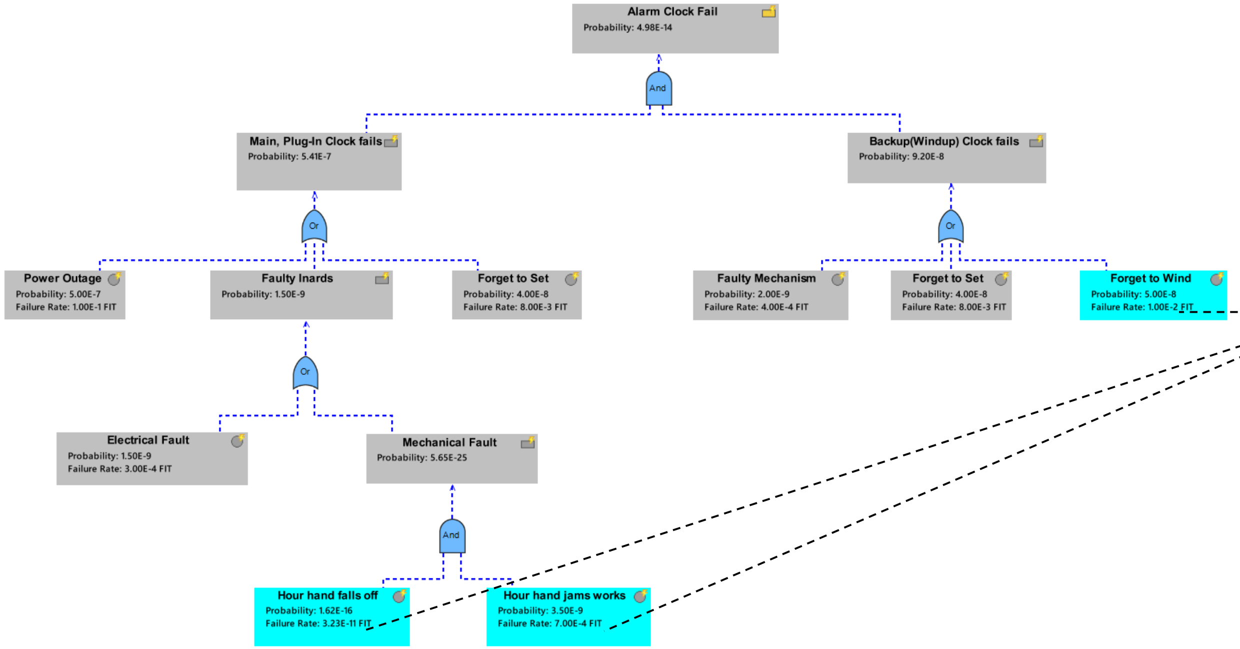
*Lane Departure::Lane Departure FMEA

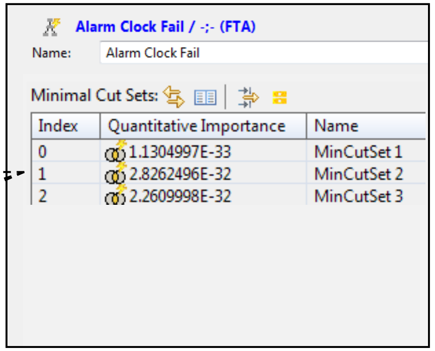
No.	FMEA Part	Design Intent	Failure Mode	Failure Effects	SEV	Class	Cause	OCC	Prevention Measures	Detection Measures	DET	RPN	Rec. Actions	Responsible	Target Date
1	Speed Sensor	Deliver speed data The speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning.	Stuck at The sensor continuously delivers the same speed reading.	Falsely activated The lane departure system is activated when it shouldn't be.	9	YC	Hardware failure Stuck at fault due to hardware failure internal to the sensor.	5	The speed sensor is currently qualified to ASIL A	None defined as yet.	10	450	Plausibility check A plausibility check shall be added to the lane departure function to detect incorrect sensor readings.	Metzker	Nov 30, 2011
2			Shortcut to ground Shortcut to ground	No activation Lane departure is not activated	6	YS	Internal hardware fa... Stuck at fault to hardware	5	The speed sensor is currenlty qualified to ASIL A	None defined as yet.	10	300	Plausibility check A plausibility check shall be	Metzker	Nov 30, 2011
				actual [illegible] speed.											
5	Camera	Provide lane position d...	No data The camera delivers no picture at all	Departure not dete... A departure from the lane cannot be detected.	7	YS	Camera obscured For example due to dirt or water on the windscreen.	5	Camera is placed behind the windscreen in an area that is regularly cleaned by the wash/wiper system.	The DSP software used to calculate lane position determines picture quality. If insufficient an error is signalled.	2	70			



Qualitative Safety Analyses

Qualitative Fault Tree Analysis (FTA)





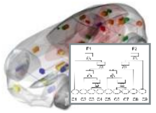
Alarm Clock Fail / -;- (FTA)

Name: Alarm Clock Fail

Minimal Cut Sets:

Index	Quantitative Importance	Name
0	1.1304997E-33	MinCutSet 1
1	2.8262496E-32	MinCutSet 2
2	2.2609998E-32	MinCutSet 3

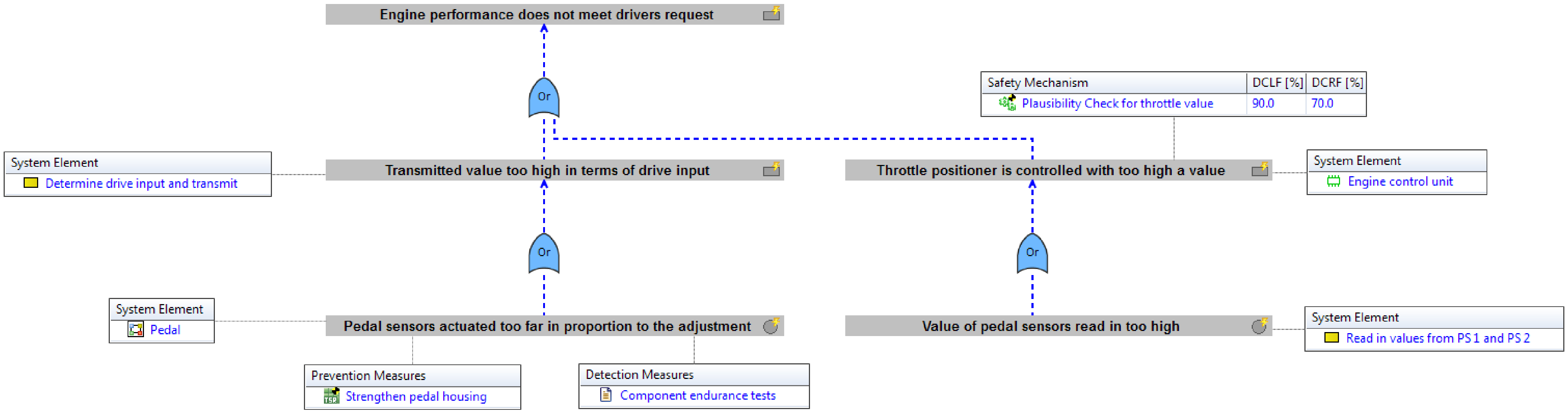
- Modeling of fault trees in malfunction diagrams
- Calculation of minimal cut sets



Qualitative Safety Analyses

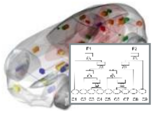
Qualitative Fault Tree Analysis (FTA)

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)
Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis


Engine performance does not meet drivers request
Or
System Element
Determine drive input and transmit
Transmitted value too high in terms of drive input
Throttle positioner is controlled with too high a value
System Element
Engine control unit
Or
Or
System Element
Pedal
Pedal sensors actuated too far in proportion to the adjustment
Value of pedal sensors read in too high
System Element
Read in values from PS 1 and PS 2
Prevention Measures
Strengthen pedal housing
Detection Measures
Component endurance tests

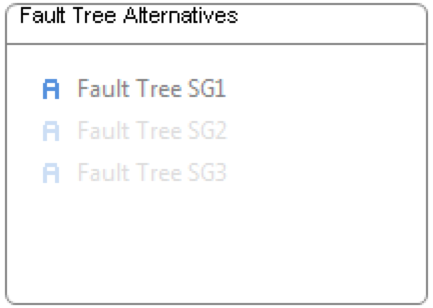
Safety Mechanism	DCLF [%]	DCRF [%]
Plausibility Check for throttle value	90.0	70.0

- Typical relevant information for analysis can be easily added to fault trees via diagram tables
- Visibility can be controlled via diagram filters



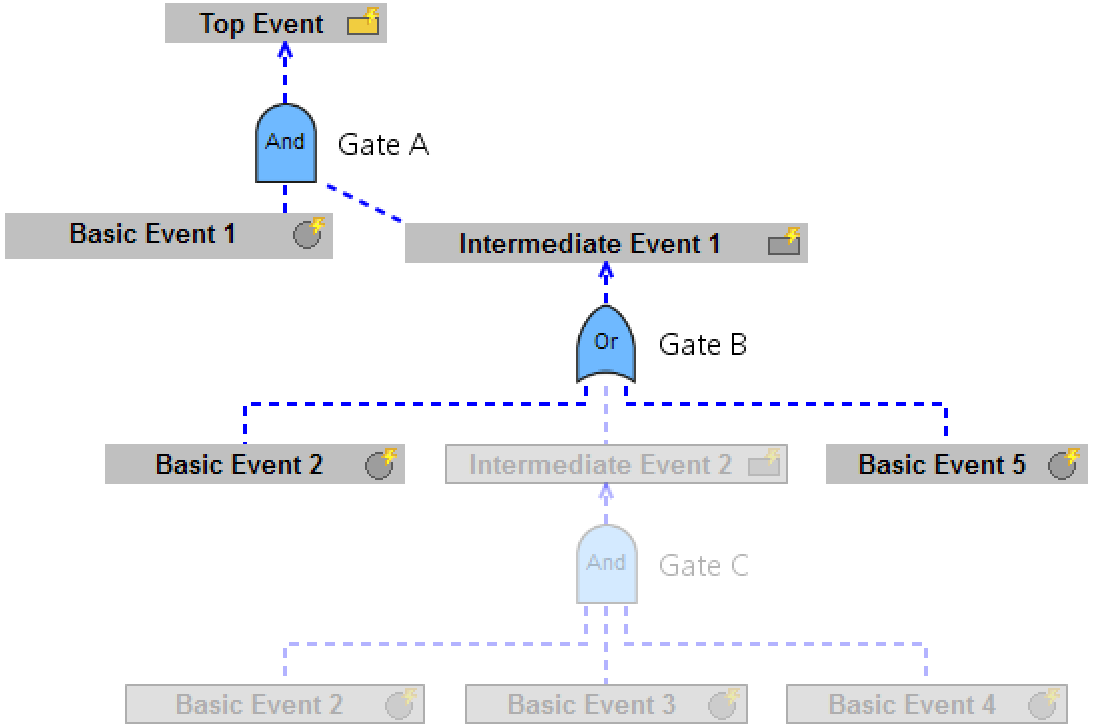
Qualitative Safety Analyses

Qualitative Fault Tree Analysis (FTA)

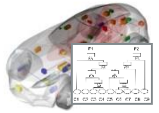


Fault Tree Alternatives

- Fault Tree SG1
- Fault Tree SG2
- Fault Tree SG3



- Efficient, redundancy free modelling of fault tree alternatives
- Alternatives of fault trees can be easily switched and visualized
- The only tool which supports analysis on alternatives of fault trees



Qualitative Safety Analyses

VECTOR

ISO 26262 key areas supported by PREEvision

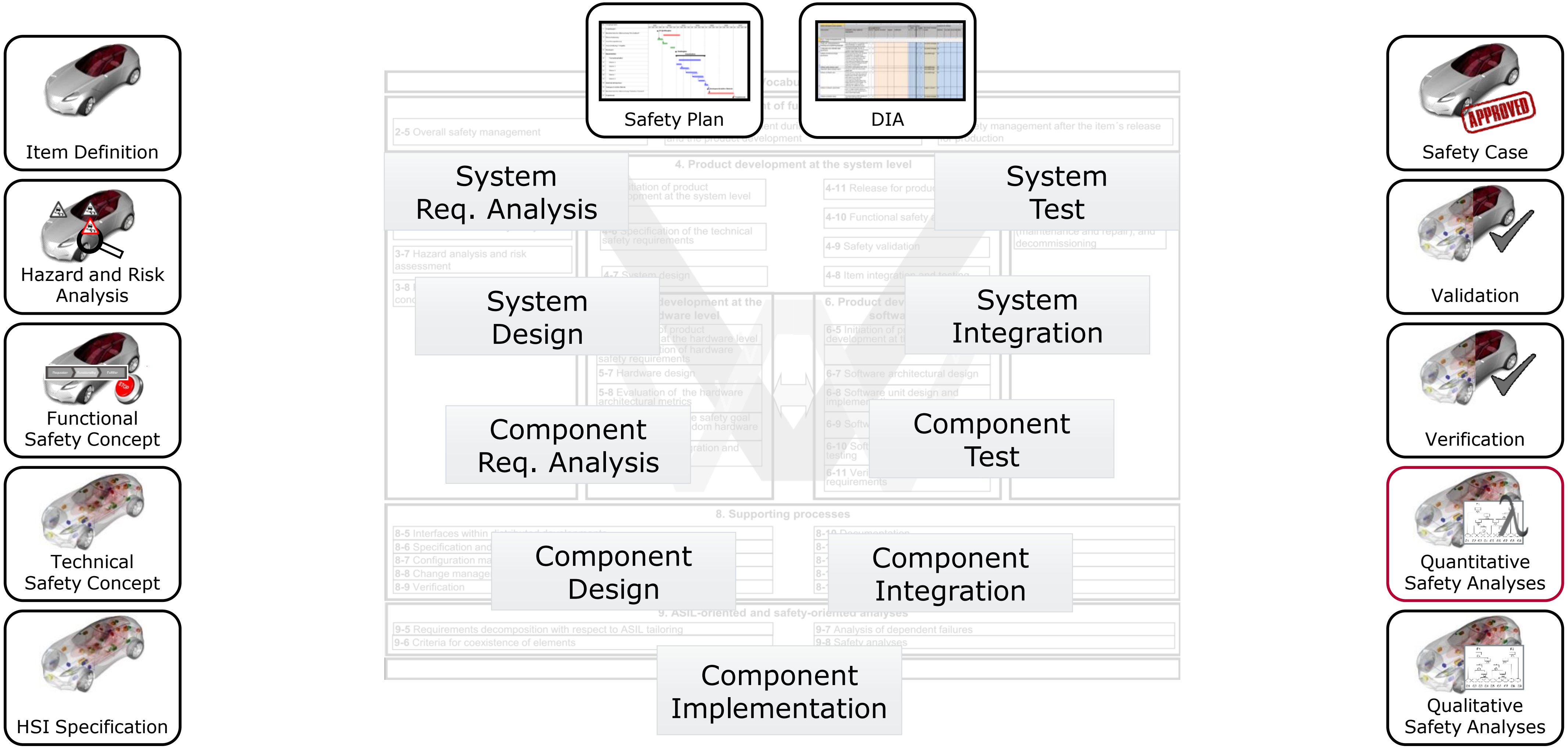
Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)


Item Definition
Hazard and Risk Analysis
Functional Safety Concept
Technical Safety Concept
HSI Specification
Safety Plan
DIA
System Req. Analysis
System Test
System Design
System Integration
Component Req. Analysis
Component Test
Component Design
Component Integration
Component Implementation
Safety Case
APPROVED
Validation
Verification
Quantitative Safety Analyses
Qualitative Safety Analyses
2-5 Overall safety management
4. Product development at the system level
4-11 Release for production
4-10 Functional safety
4-9 Safety validation
4-8 Item integration and testing
4-7 System design
3-7 Hazard analysis and risk assessment
6. Product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and
8-7 Configuration ma
8-8 Change manage
8-9 Verification
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses

Safety Case

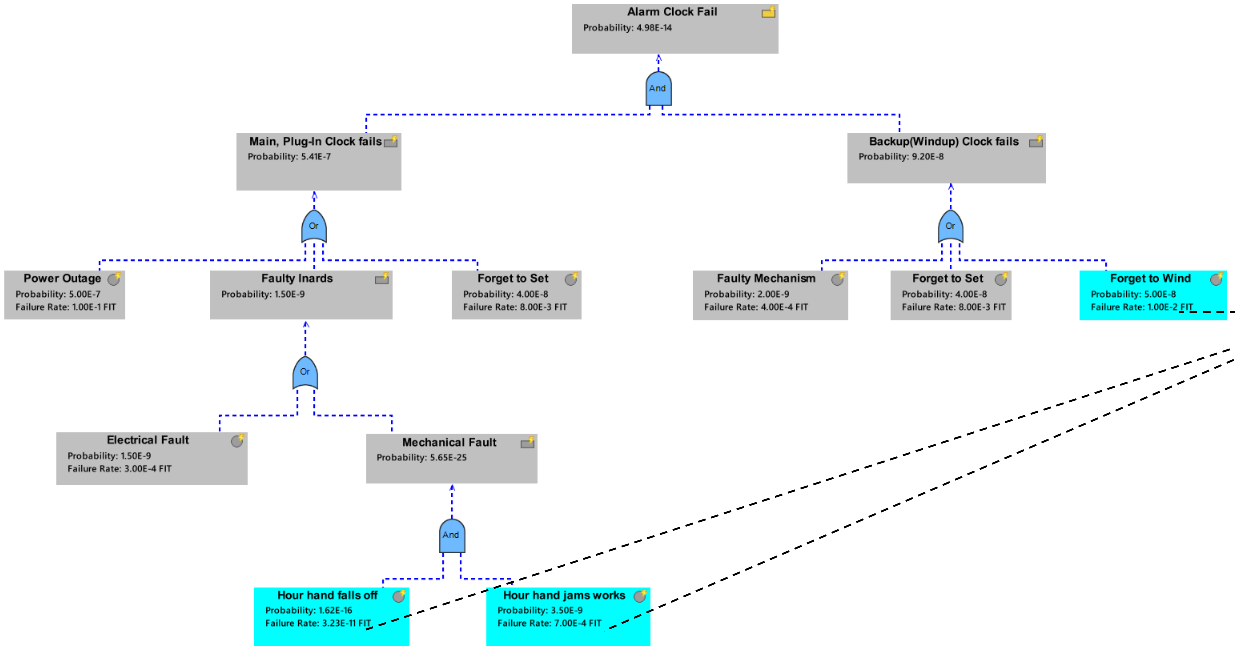
Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

Quantitative Fault Tree Analysis (FTA)



Alarm Clock Fail
Probability: 4.98E-14

And

Main, Plug-In Clock fails
Probability: 5.41E-7

Or

Power Outage
Probability: 5.00E-7
Failure Rate: 1.00E-1 FIT

Faulty Inards
Probability: 1.50E-9

Forget to Set
Probability: 4.00E-8
Failure Rate: 8.00E-3 FIT

Or

Electrical Fault
Probability: 1.50E-9
Failure Rate: 3.00E-4 FIT

Mechanical Fault
Probability: 5.65E-25

And

Hour hand falls off
Probability: 1.62E-16
Failure Rate: 3.23E-11 FIT

Hour hand jams works
Probability: 3.50E-9
Failure Rate: 7.00E-4 FIT

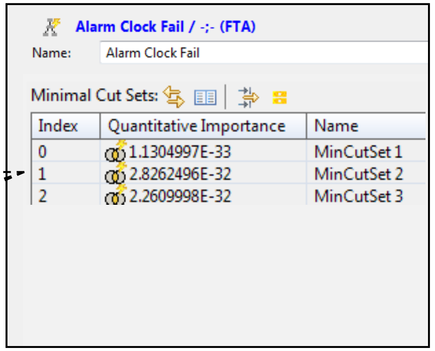
Backup(Windup) Clock fails
Probability: 9.20E-8

Or

Faulty Mechanism
Probability: 2.00E-9
Failure Rate: 4.00E-4 FIT

Forget to Set
Probability: 4.00E-8
Failure Rate: 8.00E-3 FIT

Forget to Wind
Probability: 5.00E-8
Failure Rate: 1.00E-2 FIT



Alarm Clock Fail / -;- (FTA)

Name: Alarm Clock Fail

Minimal Cut Sets:

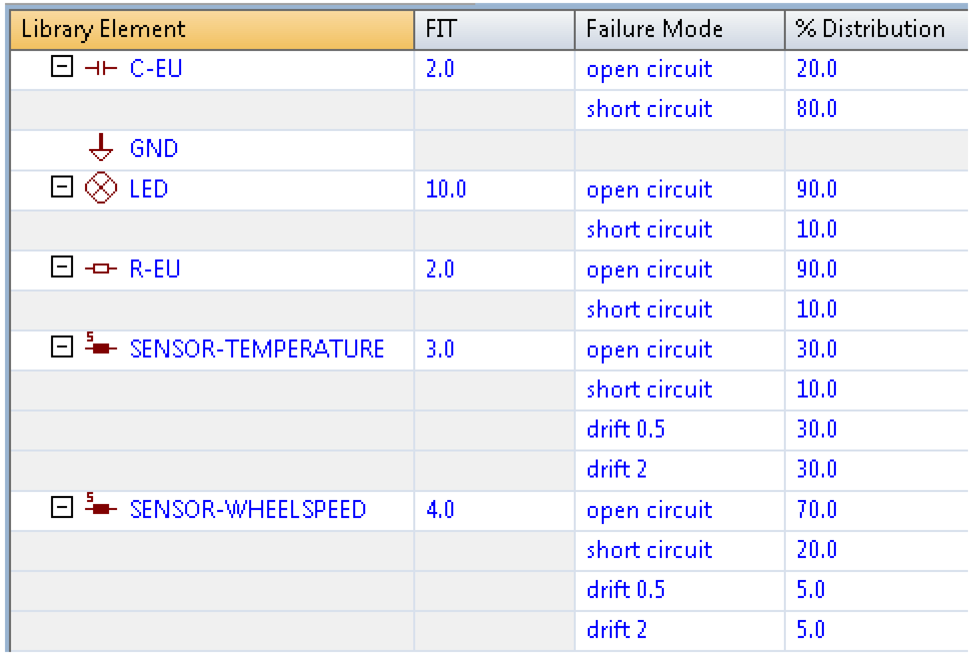
Index	Quantitative Importance	Name
0	1.1304997E-33	MinCutSet 1
1	2.8262496E-32	MinCutSet 2
2	2.2609998E-32	MinCutSet 3

- Modeling of fault trees in malfunction diagrams
- Calculation of minimal cut sets (with order and quantitative importance)
- Calculation of probabilities

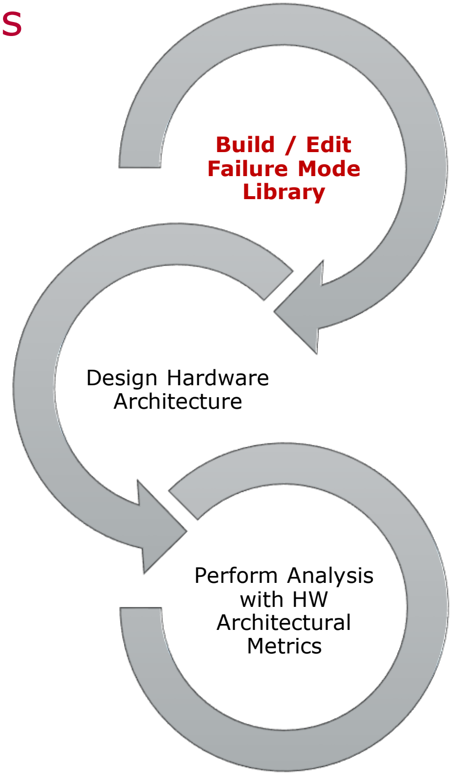
Quantitative Safety Analyses

Hardware Architectural Metrics: Failure Mode Library

- Build failure mode library by convenient annotation of all HW library elements
- Dedicated Failure Mode Library Editor for high usability and efficiency



Library Element	FIT	Failure Mode	% Distribution
⊟ C-EU	2.0	open circuit	20.0
		short circuit	80.0
GND			
⊟ LED	10.0	open circuit	90.0
		short circuit	10.0
⊟ R-EU	2.0	open circuit	90.0
		short circuit	10.0
⊟ SENSOR-TEMPERATURE	3.0	open circuit	30.0
		short circuit	10.0
		drift 0.5	30.0
		drift 2	30.0
⊟ SENSOR-WHEELSPEED	4.0	open circuit	70.0
		short circuit	20.0
		drift 0.5	5.0
		drift 2	5.0



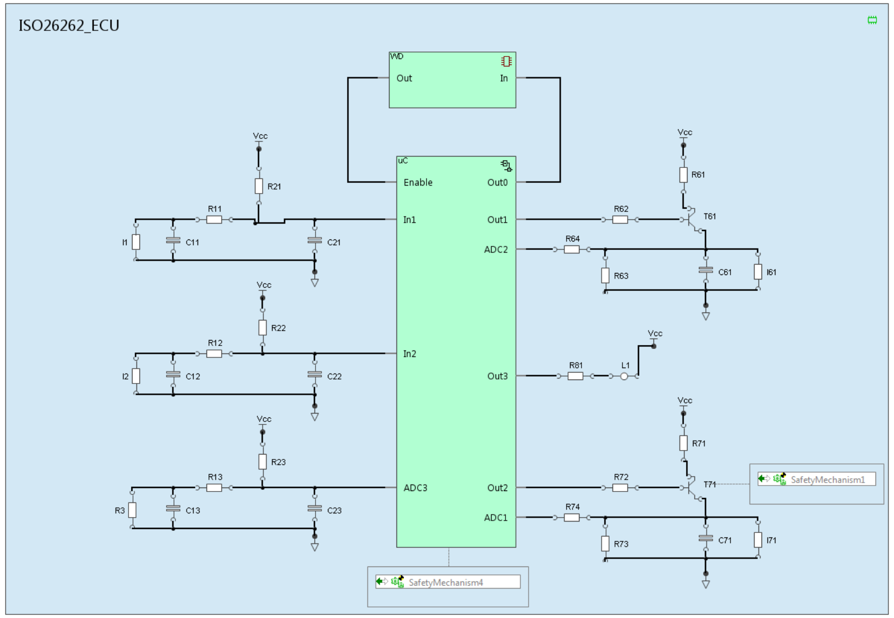
Build / Edit Failure Mode Library

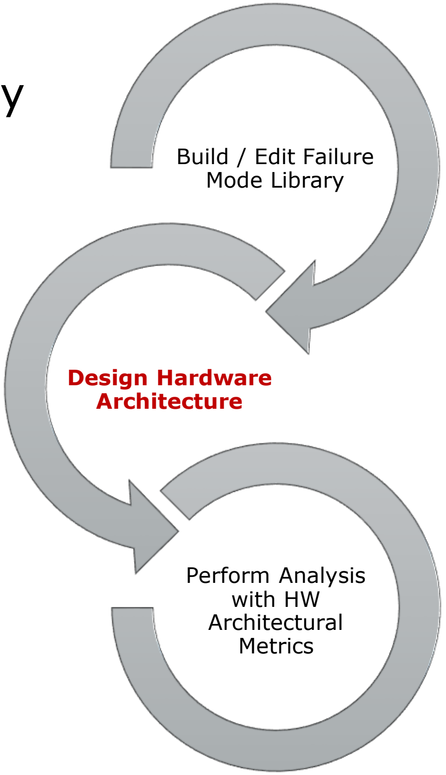
Design Hardware Architecture

Perform Analysis with HW Architectural Metrics

Hardware Architectural Metrics: Using library elements

- Use library elements during HW design as usual
- Increased efficiency by reusing failure mode definitions for design from library




Build / Edit Failure Mode Library

Design Hardware Architecture

Perform Analysis with HW Architectural Metrics

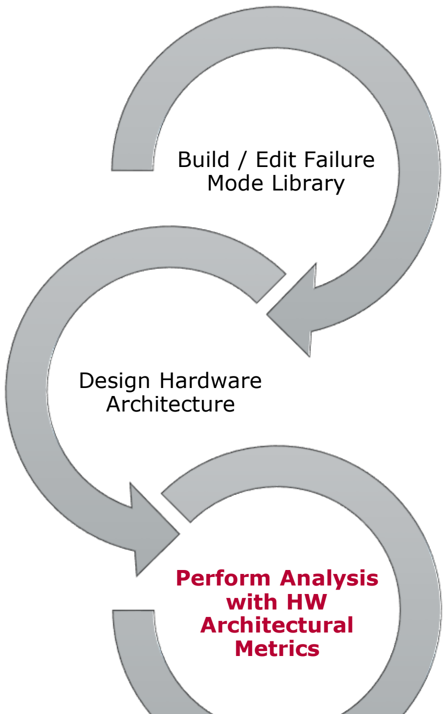
1) Example Based on ISO 26262 – 5, Annex E.1

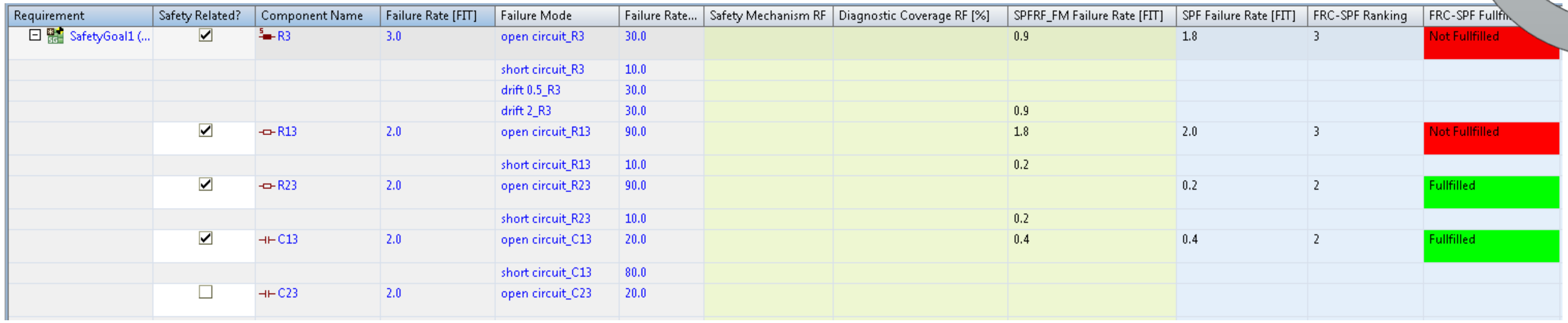
VECTOR

Hardware Architectural Metrics

Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Hardware Software Interface (HIS)

- Allocate target values via D&D
- Assign safety mechanisms via D&D
- Convenient HW architectural metrics calculator
- Instant highlighting of fulfillments and violations


Build / Edit Failure Mode Library
Design Hardware Architecture
Perform Analysis with HW Architectural Metrics



Requirement	Safety Related?	Component Name	Failure Rate [FIT]	Failure Mode	Failure Rate...	Safety Mechanism RF	Diagnostic Coverage RF [%]	SPFRF_FM Failure Rate [FIT]	SPF Failure Rate [FIT]	FRC-SPF Ranking	FRC-SPF Fullfi
⊟ SafetyGoal1 (...	☑	R3	3.0	open circuit_R3	30.0			0.9	1.8	3	Not Fullfilled
				short circuit_R3	10.0						
				drift 0.5_R3	30.0						
				drift 2_R3	30.0			0.9			
	☑	R13	2.0	open circuit_R13	90.0			1.8	2.0	3	Not Fullfilled
				short circuit_R13	10.0			0.2			
	☑	R23	2.0	open circuit_R23	90.0				0.2	2	Fullfilled
				short circuit_R23	10.0			0.2			
	☑	C13	2.0	open circuit_C13	20.0			0.4	0.4	2	Fullfilled
				short circuit_C13	80.0						
	☐	C23	2.0	open circuit_C23	20.0						

Safety Case
Validation
Verification
Quantitative Safety Analysis
Qualitative Safety Analysis

ISO 26262 key areas supported by PREEvision

Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)

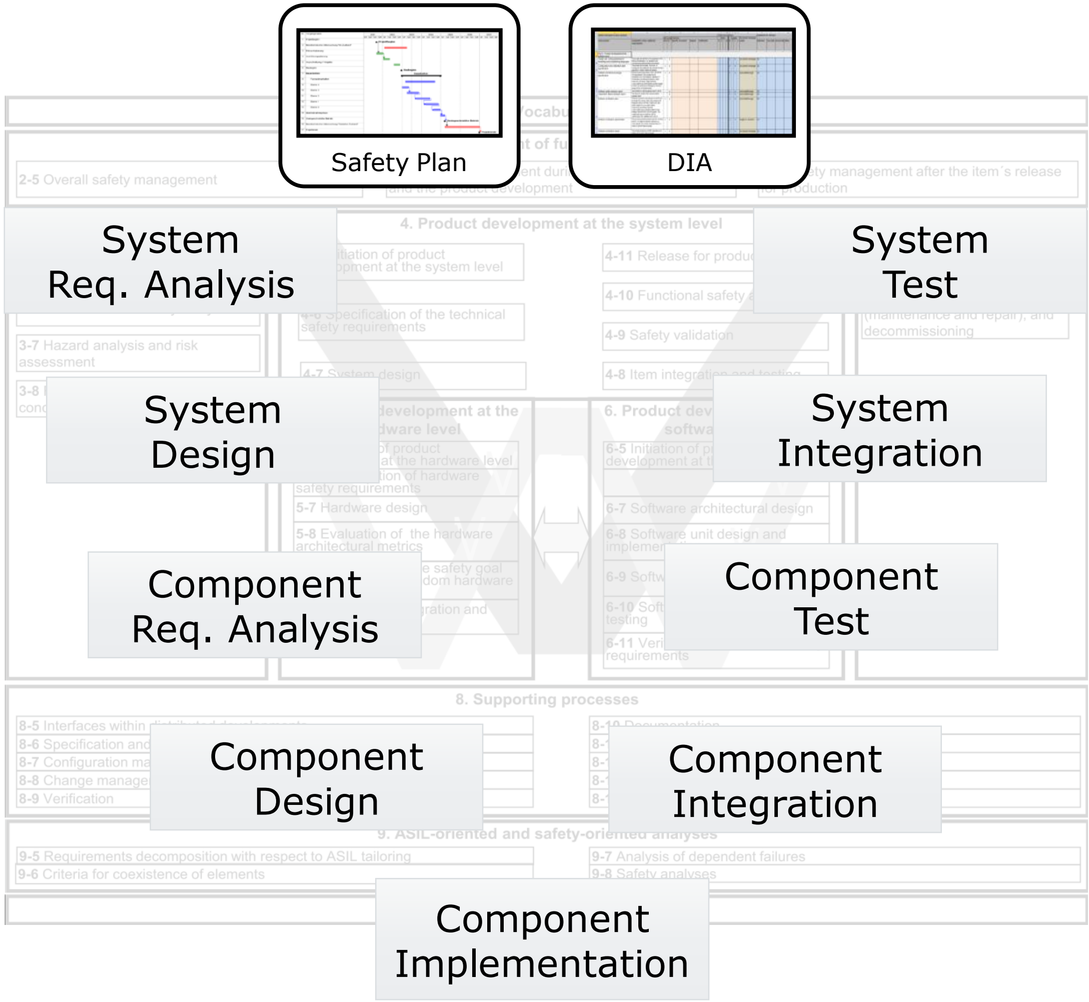
Item Definition

Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

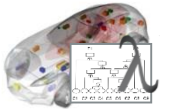
HSI Specification

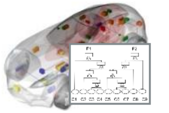


Safety Case

Validation

Verification


Quantitative Safety Analyses


Qualitative Safety Analyses

Safety Case

Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

VECTOR

PREEvision Test Engineering und Test Management: Information Flow

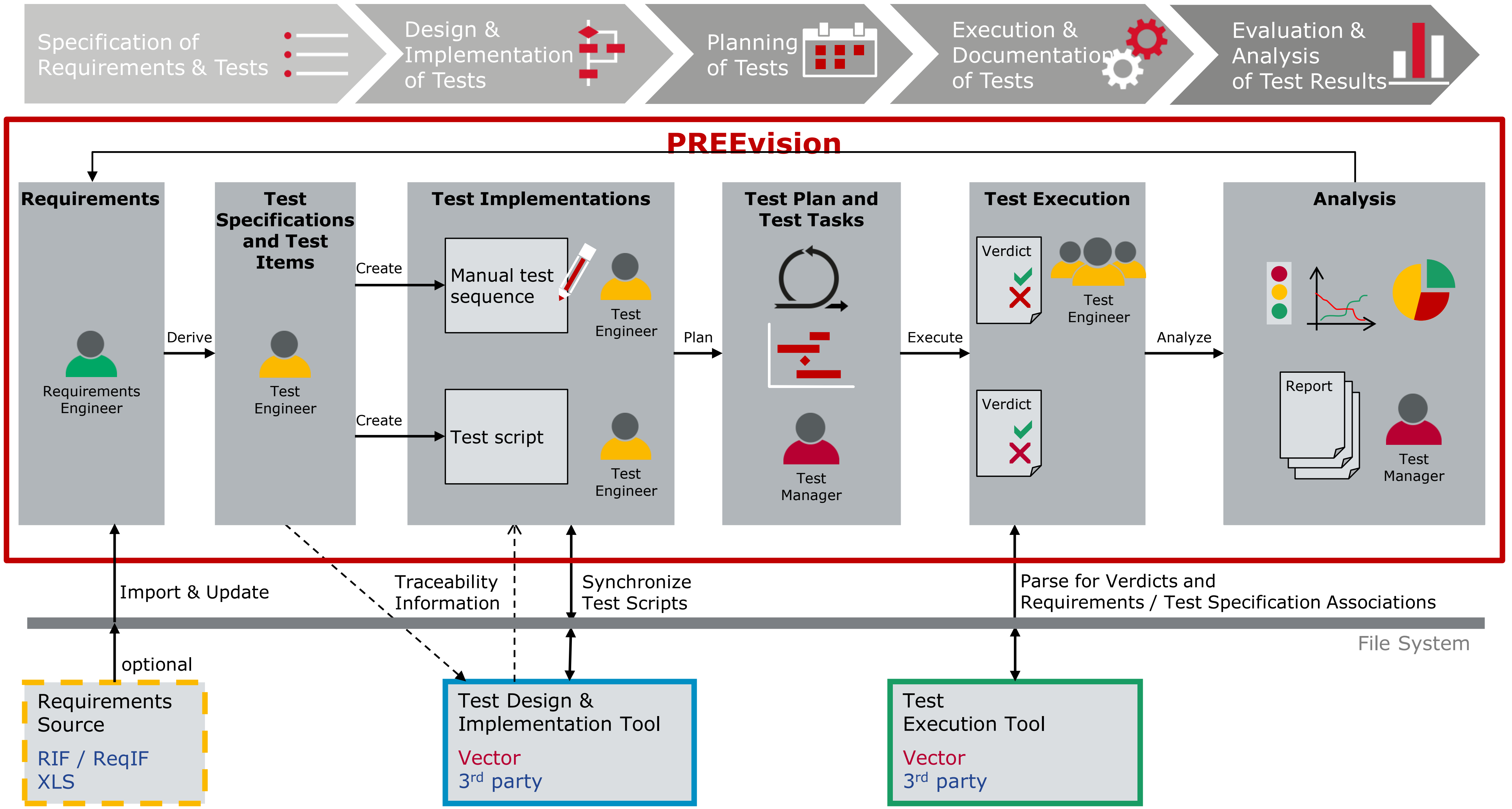
Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)



Specification of Requirements & Tests

Design & Implementation of Tests

Planning of Tests

Execution & Documentation of Tests

Evaluation & Analysis of Test Results

PREEvision

Requirements

Requirements Engineer

Derive

Test Specifications and Test Items

Test Engineer

Create

Create

Test Implementations

Manual test sequence

Test script

Test Engineer

Test Engineer

Plan

Test Plan and Test Tasks

Test Manager

Execute

Test Execution

Verdict

Verdict

Test Engineer

Analyze

Analysis

Report

Test Manager

Import & Update

Traceability Information

Synchronize Test Scripts

Parse for Verdicts and Requirements / Test Specification Associations

File System

optional

Requirements Source

RIF / ReqIF

XLS

Test Design & Implementation Tool

Vector

3rd party

Test Execution Tool

Vector

3rd party

Safety Case

Validation

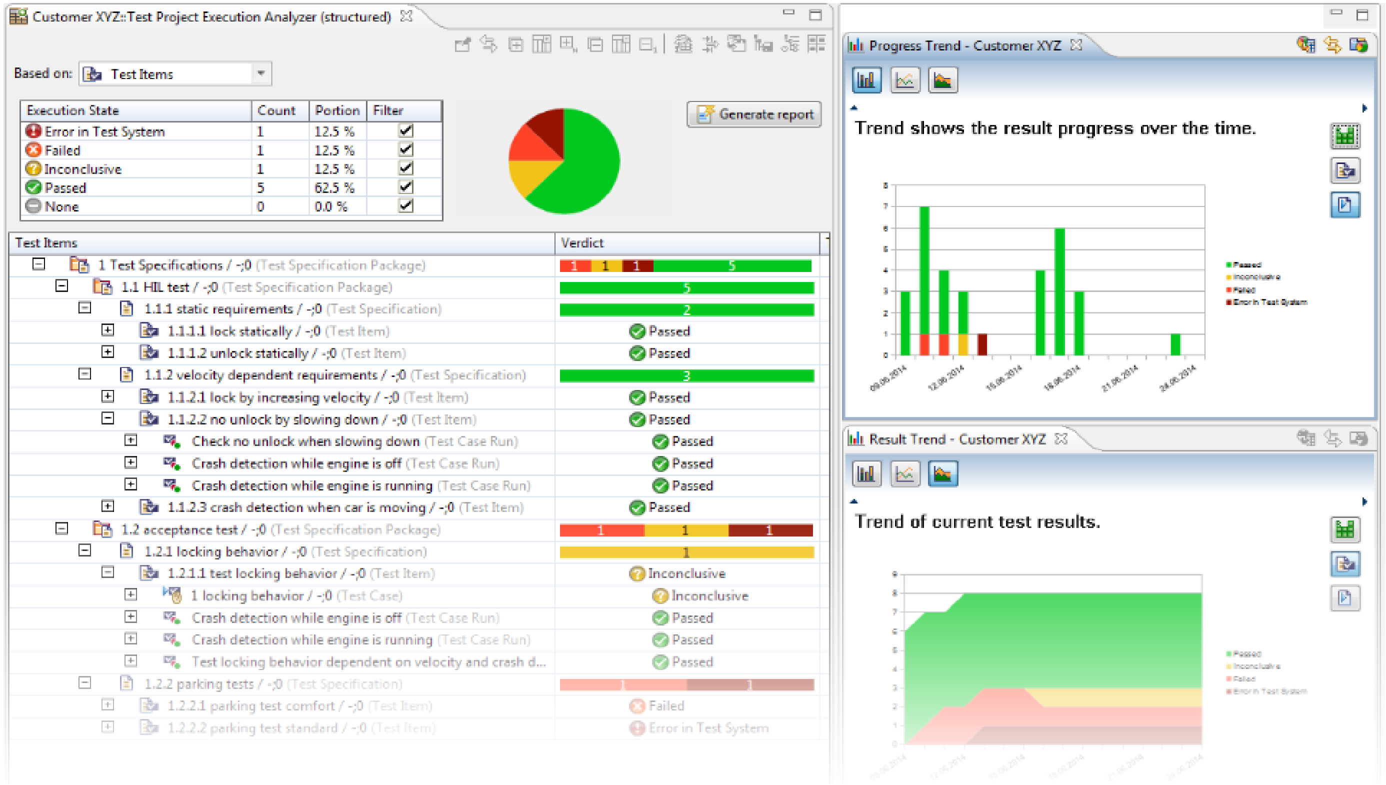
Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

VECTOR

Verification and Validation



Customer XYZ::Test Project Execution Analyzer (structured)

Based on: Test Items

Execution State	Count	Portion	Filter
Error in Test System	1	12.5 %	☑
Failed	1	12.5 %	☑
Inconclusive	1	12.5 %	☑
Passed	5	62.5 %	☑
None	0	0.0 %	☑

Generate report

Test Items	Verdict
1 Test Specifications / -;0 (Test Specification Package)	1 1 1 5
1.1 HIL test / -;0 (Test Specification Package)	5
1.1.1 static requirements / -;0 (Test Specification)	2
1.1.1.1 lock statically / -;0 (Test Item)	Passed
1.1.1.2 unlock statically / -;0 (Test Item)	Passed
1.1.2 velocity dependent requirements / -;0 (Test Specification)	3
1.1.2.1 lock by increasing velocity / -;0 (Test Item)	Passed
1.1.2.2 no unlock by slowing down / -;0 (Test Item)	Passed
Check no unlock when slowing down (Test Case Run)	Passed
Crash detection while engine is off (Test Case Run)	Passed
Crash detection while engine is running (Test Case Run)	Passed
1.1.2.3 crash detection when car is moving / -;0 (Test Item)	Passed
1.2 acceptance test / -;0 (Test Specification Package)	1 1 1
1.2.1 locking behavior / -;0 (Test Specification)	1
1.2.1.1 test locking behavior / -;0 (Test Item)	Inconclusive
1 locking behavior / -;0 (Test Case)	Inconclusive
Crash detection while engine is off (Test Case Run)	Passed
Crash detection while engine is running (Test Case Run)	Passed
Test locking behavior dependent on velocity and crash d...	Passed
1.2.2 parking tests / -;0 (Test Specification)	1 1
1.2.2.1 parking test comfort / -;0 (Test Item)	Failed
1.2.2.2 parking test standard / -;0 (Test Item)	Error in Test System

Progress Trend - Customer XYZ

Trend shows the result progress over the time.

Result Trend - Customer XYZ

Trend of current test results.

ISO 26262 key areas supported by PREEvision

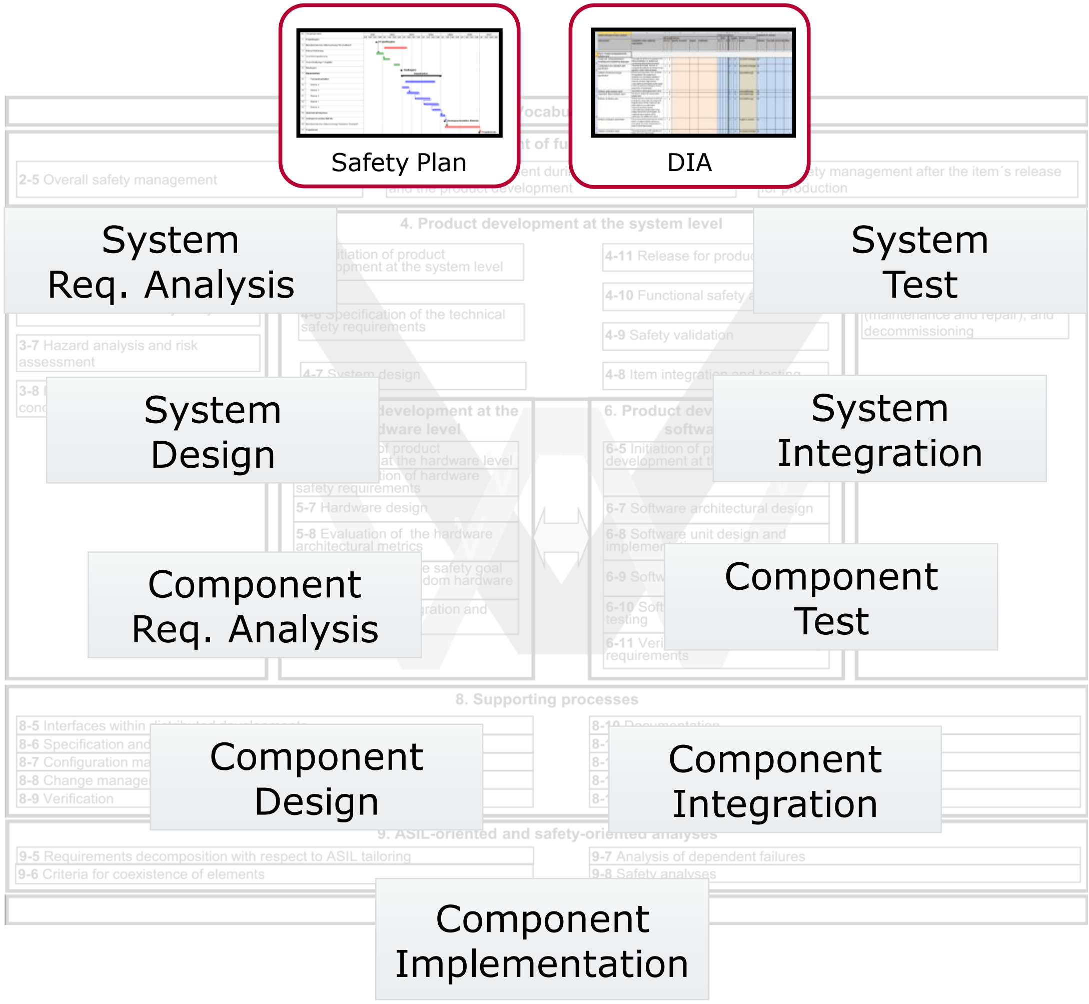
Item Definition

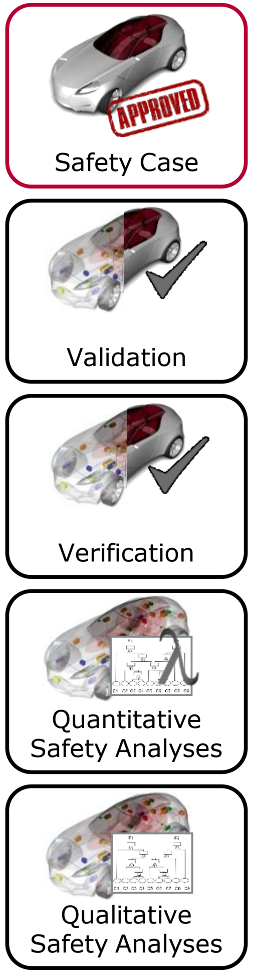
Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)





Safety Case

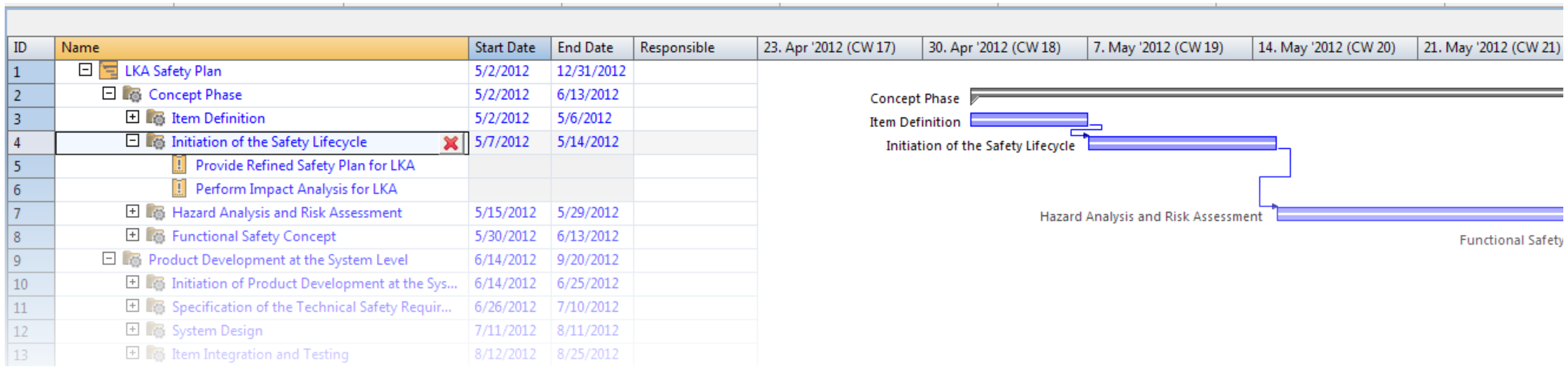
Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

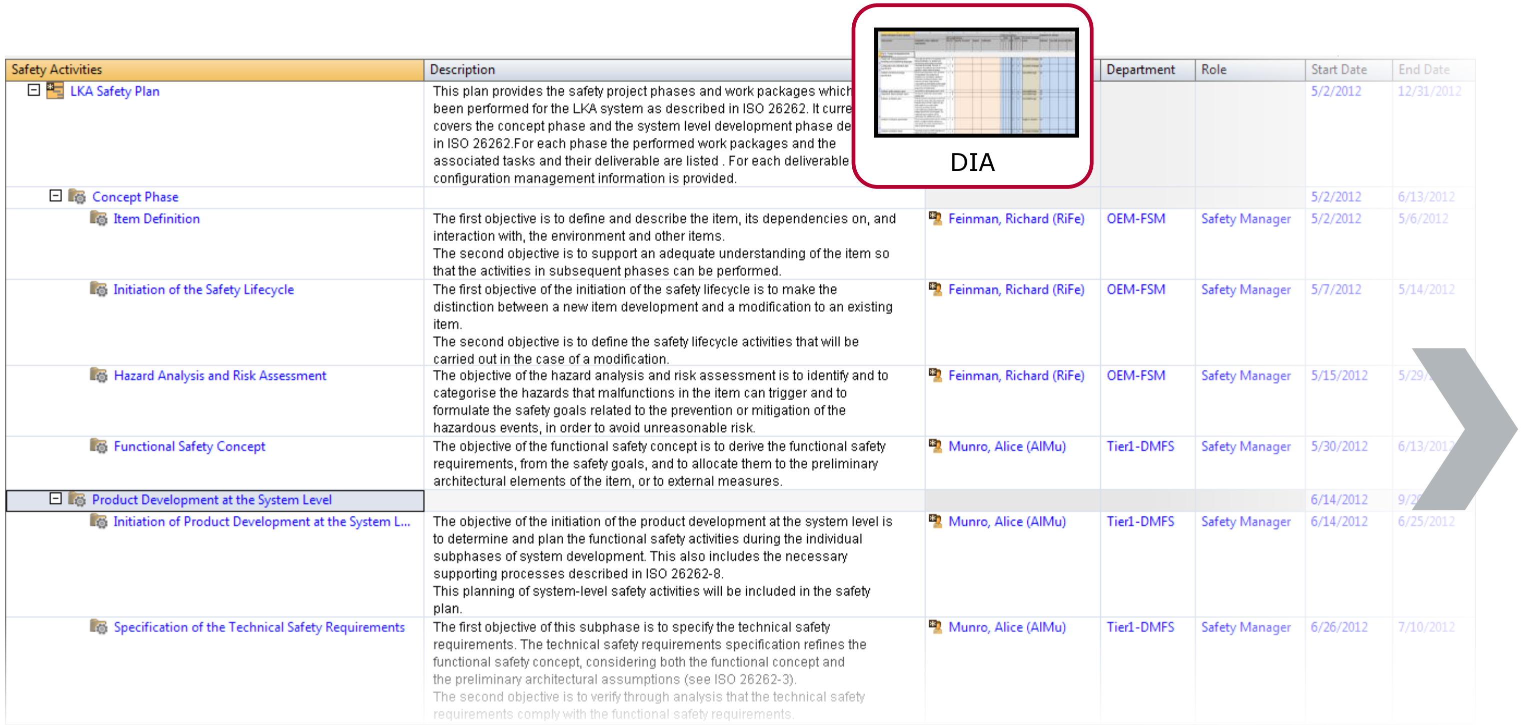
Safety Plan



ID	Name	Start Date	End Date	Responsible
1	⊟ LKA Safety Plan	5/2/2012	12/31/2012	
2	⊟ Concept Phase	5/2/2012	6/13/2012	
3	⊞ Item Definition	5/2/2012	5/6/2012	
4	⊟ Initiation of the Safety Lifecycle	5/7/2012	5/14/2012	
5	Provide Refined Safety Plan for LKA			
6	Perform Impact Analysis for LKA			
7	⊞ Hazard Analysis and Risk Assessment	5/15/2012	5/29/2012	
8	⊞ Functional Safety Concept	5/30/2012	6/13/2012	
9	⊟ Product Development at the System Level	6/14/2012	9/20/2012	
10	⊞ Initiation of Product Development at the Sys...	6/14/2012	6/25/2012	
11	⊞ Specification of the Technical Safety Requir...	6/26/2012	7/10/2012	
12	⊞ System Design	7/11/2012	8/11/2012	
13	⊞ Item Integration and Testing	8/12/2012	8/25/2012	

- Predefined safety plan template according to ISO 26262
  - Can be adapted to match organizational needs
  - Serves as process justification argument for safety case
  - Can be used to generate DIA

Development Interface Agreement (DIA)



DIA

Safety Activities	Description		Department	Role	Start Date	End Date
LKA Safety Plan	This plan provides the safety project phases and work packages which been performed for the LKA system as described in ISO 26262. It curre covers the concept phase and the system level development phase de in ISO 26262.For each phase the performed work packages and the associated tasks and their deliverable are listed . For each deliverable configuration management information is provided.				5/2/2012	12/31/2012
Concept Phase					5/2/2012	6/13/2012
Item Definition	The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items. The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed.	Feinman, Richard (RiFe)	OEM-FSM	Safety Manager	5/2/2012	5/6/2012
Initiation of the Safety Lifecycle	The first objective of the initiation of the safety lifecycle is to make the distinction between a new item development and a modification to an existing item. The second objective is to define the safety lifecycle activities that will be carried out in the case of a modification.	Feinman, Richard (RiFe)	OEM-FSM	Safety Manager	5/7/2012	5/14/2012
Hazard Analysis and Risk Assessment	The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.	Feinman, Richard (RiFe)	OEM-FSM	Safety Manager	5/15/2012	5/29/
Functional Safety Concept	The objective of the functional safety concept is to derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements of the item, or to external measures.	Munro, Alice (AlMu)	Tier1-DMFS	Safety Manager	5/30/2012	6/13/201
Product Development at the System Level					6/14/2012	9/2
Initiation of Product Development at the System L...	The objective of the initiation of the product development at the system level is to determine and plan the functional safety activities during the individual subphases of system development. This also includes the necessary supporting processes described in ISO 26262-8. This planning of system-level safety activities will be included in the safety plan.	Munro, Alice (AlMu)	Tier1-DMFS	Safety Manager	6/14/2012	6/25/2012
Specification of the Technical Safety Requirements	The first objective of this subphase is to specify the technical safety requirements. The technical safety requirements specification refines the functional safety concept, considering both the functional concept and the preliminary architectural assumptions (see ISO 26262-3). The second objective is to verify through analysis that the technical safety requirements comply with the functional safety requirements.	Munro, Alice (AlMu)	Tier1-DMFS	Safety Manager	6/26/2012	7/10/2012

- MS Excel

- Predefined template for development interface agreement according to ISO 26262, including
  - Distribution of safety activities between customer and supplier
  - Responsible for each activity
  - Data to be exchanged

ISO 26262 key areas supported by PREEvision

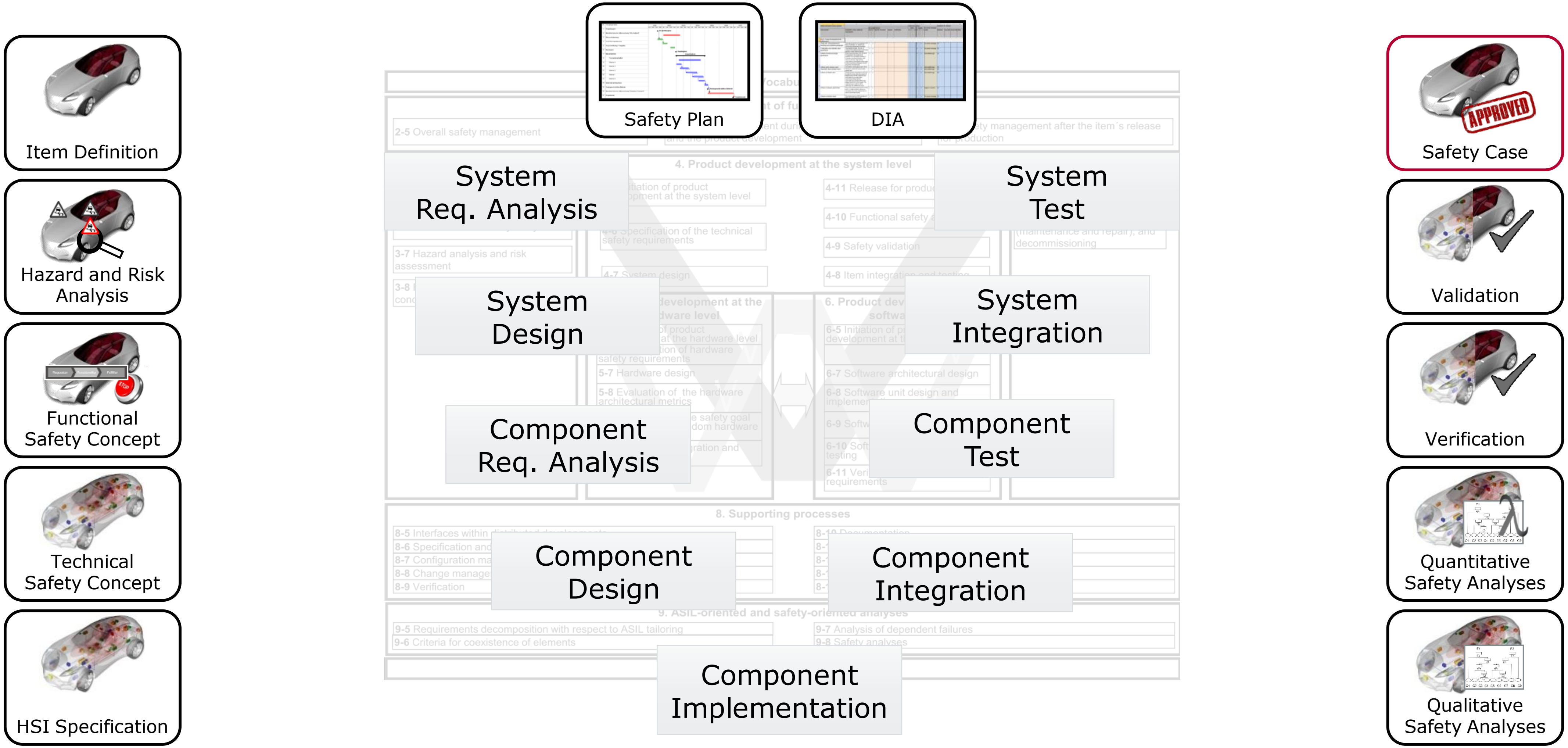
Item Definition

Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Hardware Software Interface (HIS)



Item Definition

Hazard and Risk Analysis

Functional Safety Concept

Technical Safety Concept

HSI Specification

Safety Plan

DIA

System Req. Analysis

System Design

Component Req. Analysis

Component Design

Component Implementation

Component Integration

Component Test

System Integration

System Test

Safety Case

Validation

Verification

Quantitative Safety Analyses

Qualitative Safety Analyses

Safety Case

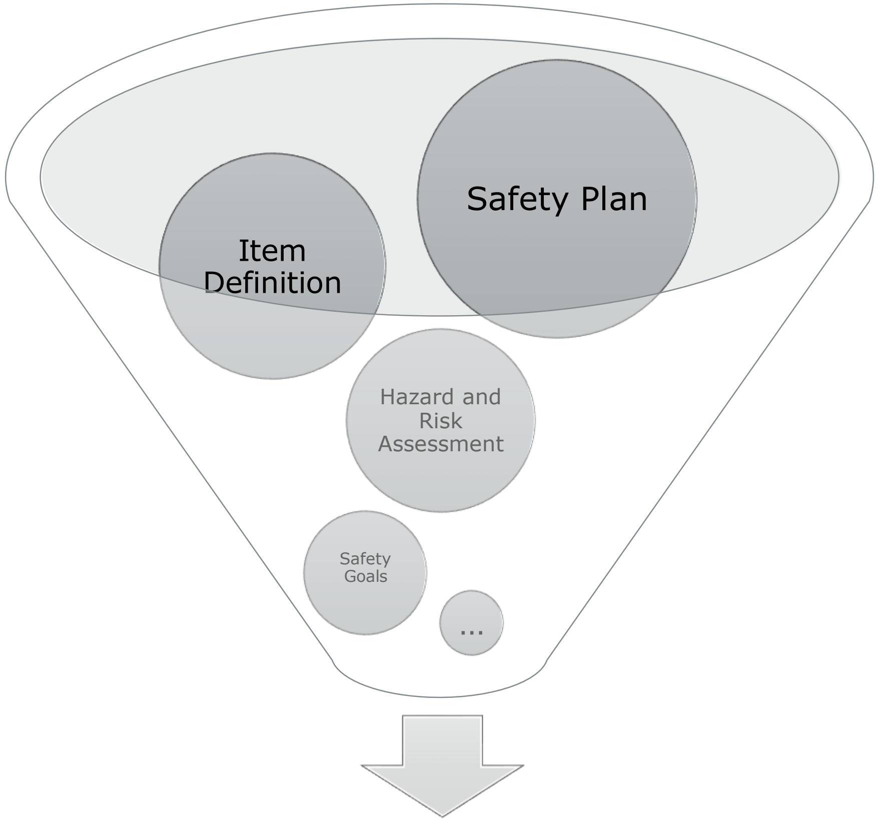
Validation

Verification

Quantitative Safety Analysis

Qualitative Safety Analysis

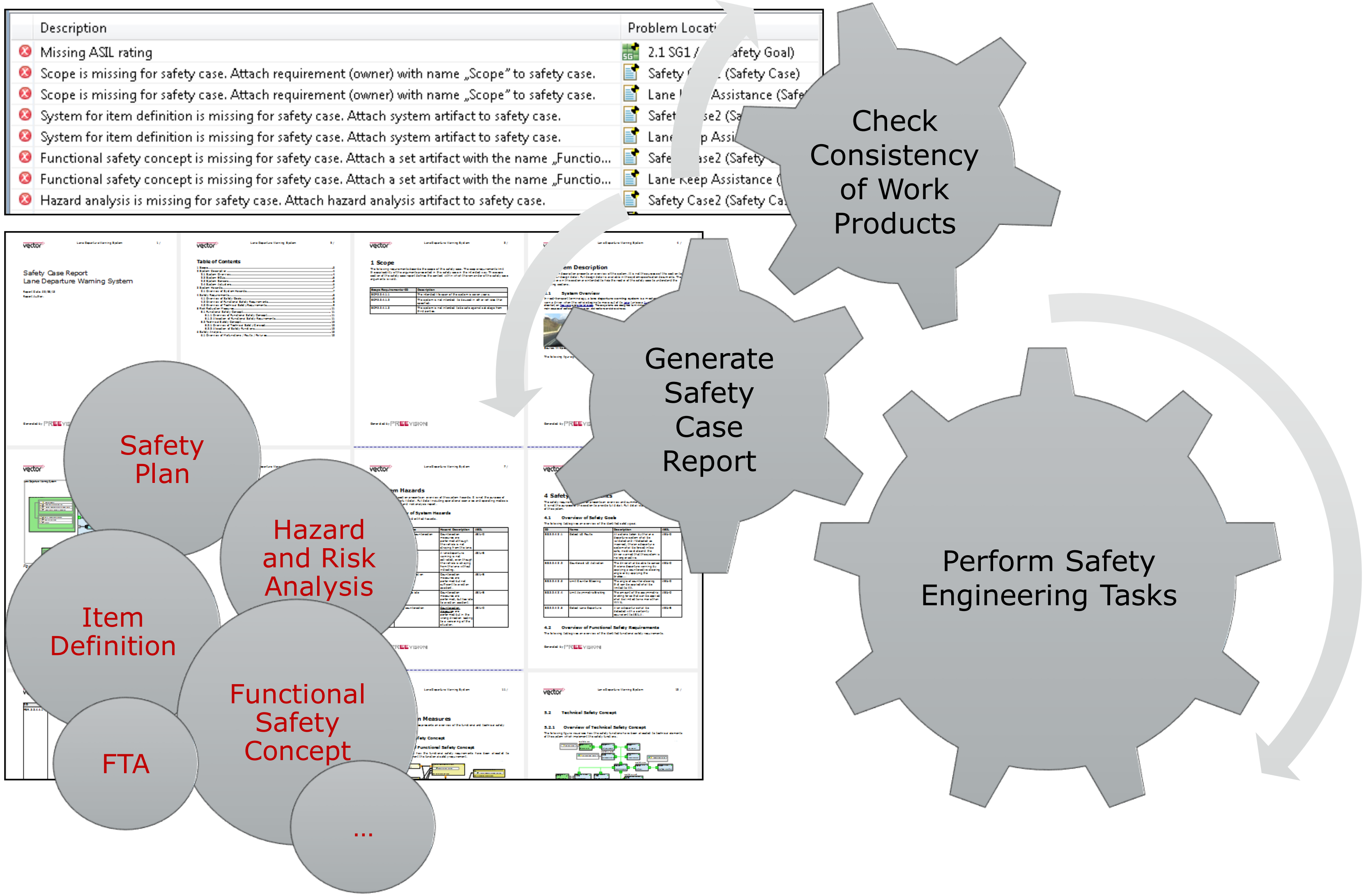
Concept of safety case



Safety Case Report

- Based on work products and safety plan
- Always consistent, can be generated at any time
- Covers technical safety argument and process justification argument

Workflow for generating safety case reports

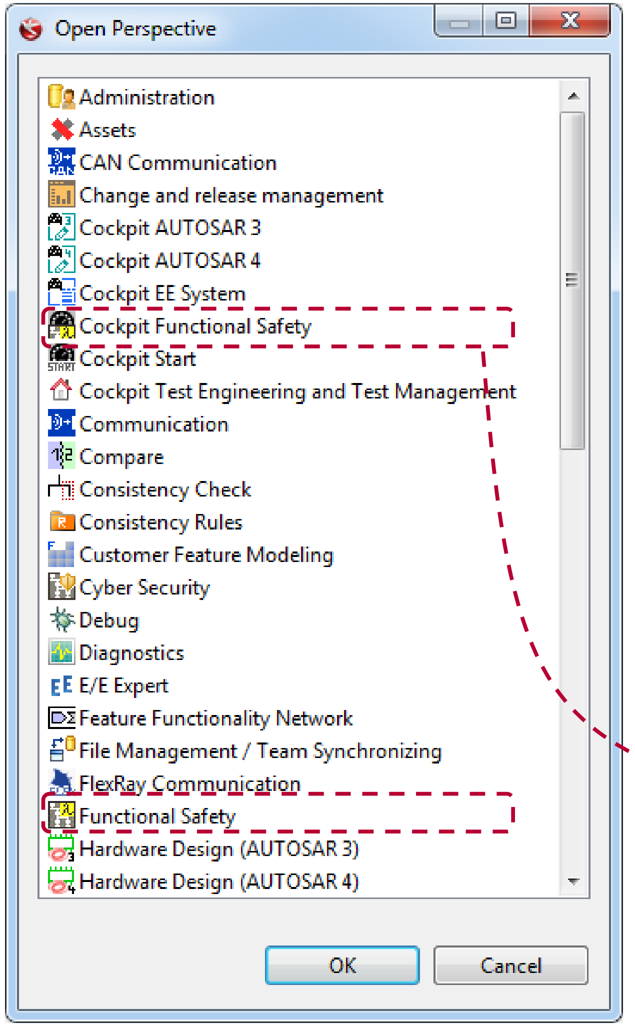


	Description	Problem Locati
⊗	Missing ASIL rating	2.1 SG1 / afety Goal)
⊗	Scope is missing for safety case. Attach requirement (owner) with name „Scope" to safety case.	Safety . (Safety Case)
⊗	Scope is missing for safety case. Attach requirement (owner) with name „Scope" to safety case.	Lane Assistance (Safe
⊗	System for item definition is missing for safety case. Attach system artifact to safety case.	Safet se2 (Sa
⊗	System for item definition is missing for safety case. Attach system artifact to safety case.	Lane p Assi
⊗	Functional safety concept is missing for safety case. Attach a set artifact with the name „Functio...	Safe ase2 (Safety
⊗	Functional safety concept is missing for safety case. Attach a set artifact with the name „Functio...	Lane Keep Assistance (
⊗	Hazard analysis is missing for safety case. Attach hazard analysis artifact to safety case.	Safety Case2 (Safety Ca

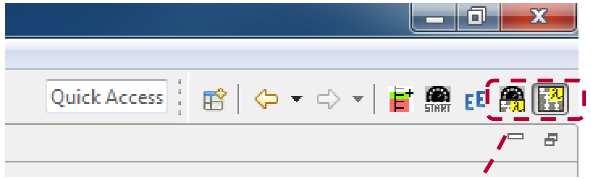
Safety Case Report
Lane Departure Warning System
Table of Contents
1 Scope
Check Consistency of Work Products
Generate Safety Case Report
Perform Safety Engineering Tasks
Safety Plan
Hazard and Risk Analysis
Item Definition
Functional Safety Concept
FTA
...

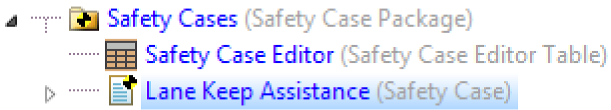
Safety assessment support

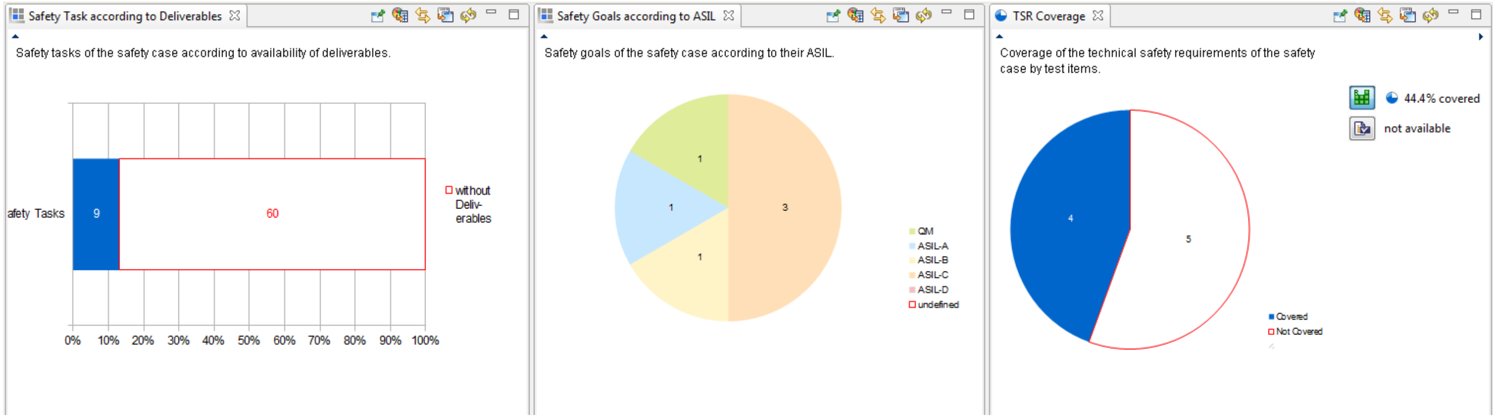
- Automatic support for review of safety deliverables via online checks
- Support for (safety) managers via safety cockpit


Open Perspective

- Administration
- Assets
- CAN Communication
- Change and release management
- Cockpit AUTOSAR 3
- Cockpit AUTOSAR 4
- Cockpit EE System
- Cockpit Functional Safety
- Cockpit Start
- Cockpit Test Engineering and Test Management
- Communication
- Compare
- Consistency Check
- Consistency Rules
- Customer Feature Modeling
- Cyber Security
- Debug
- Diagnostics
- E/E Expert
- Feature Functionality Network
- File Management / Team Synchronizing
- FlexRay Communication
- Functional Safety
- Hardware Design (AUTOSAR 3)
- Hardware Design (AUTOSAR 4)




- Safety Cases (Safety Case Package)
  - Safety Case Editor (Safety Case Editor Table)
  - Lane Keep Assistance (Safety Case)


Safety Task according to Deliverables

Safety tasks of the safety case according to availability of deliverables.

Safety Goals according to ASIL

Safety goals of the safety case according to their ASIL.

TSR Coverage

Coverage of the technical safety requirements of the safety case by test items.

Agenda

PREEvision at a Glance

Introduction Functional Safety

Item definition, HAZOP and HARA

Functional and Technical Safety Concept

Safety Analysis

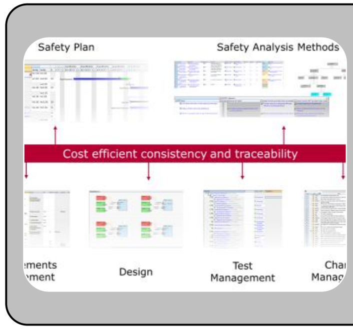
Verification and Validation

Safety Plan, Safety Case

Functional Safety Perspectives

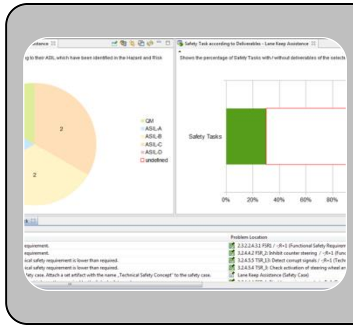
▶ **Summary**

Advantages



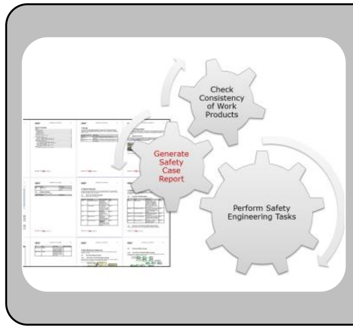
Integrated approach

- Full traceability can be easily established and maintained
- Consistent work products
- Reduce cost for tool interfaces



Automated consistency checking of deliverables

- Relieve engineers from error prone and tedious tasks
- Provide safety managers with insight in status and progress
- Reduce effort for manual reviews and progress reports


Check Consistency of Work Products
Generate Safety Case Report
Perform Safety Engineering Tasks

Engineer safe products – generate compliant deliverables

- Deliverables can be generated from engineering data
- Reduced effort for compliant deliverables

For more information about Vector
and our products please visit

www.vector.com

Author:
Nico Adler
Vector Germany