
# The model-based approach to ISO 26262 compliant development in PREEvision 7.0

Dr. Eduard Metzker
May 2014

# Agenda

> **Introduction to PREEvision**

Introduction to ISO 26262

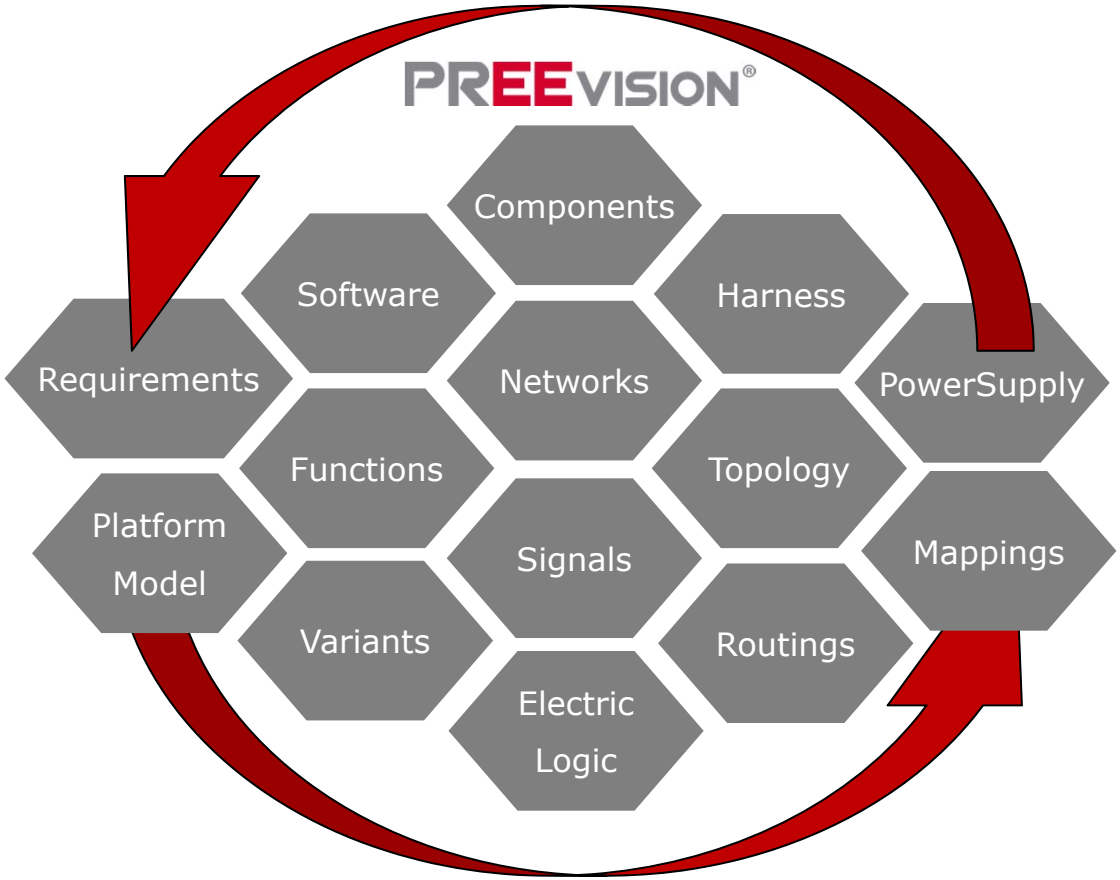
ISO 26262 Compliant Development in PREEvision

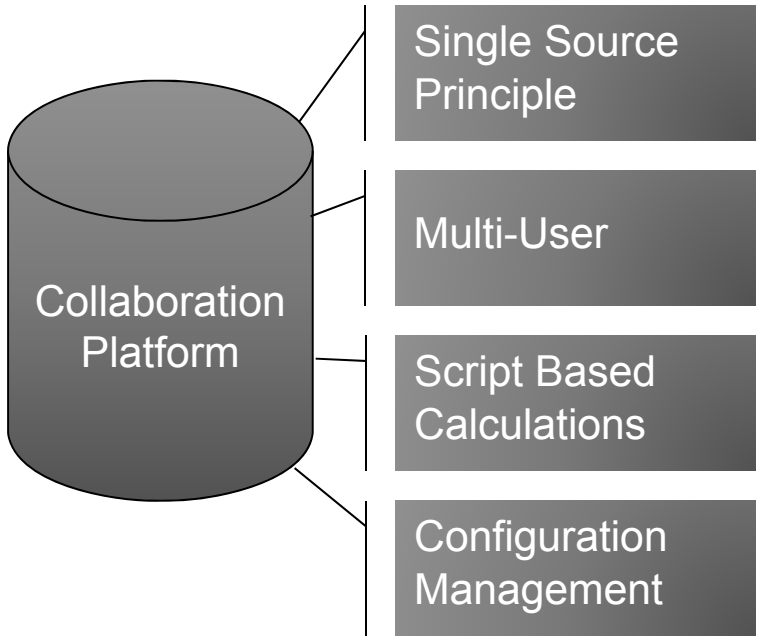
1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

# Introduction to PREEvision

## Model-Based E/E-System Engineering (1/2)

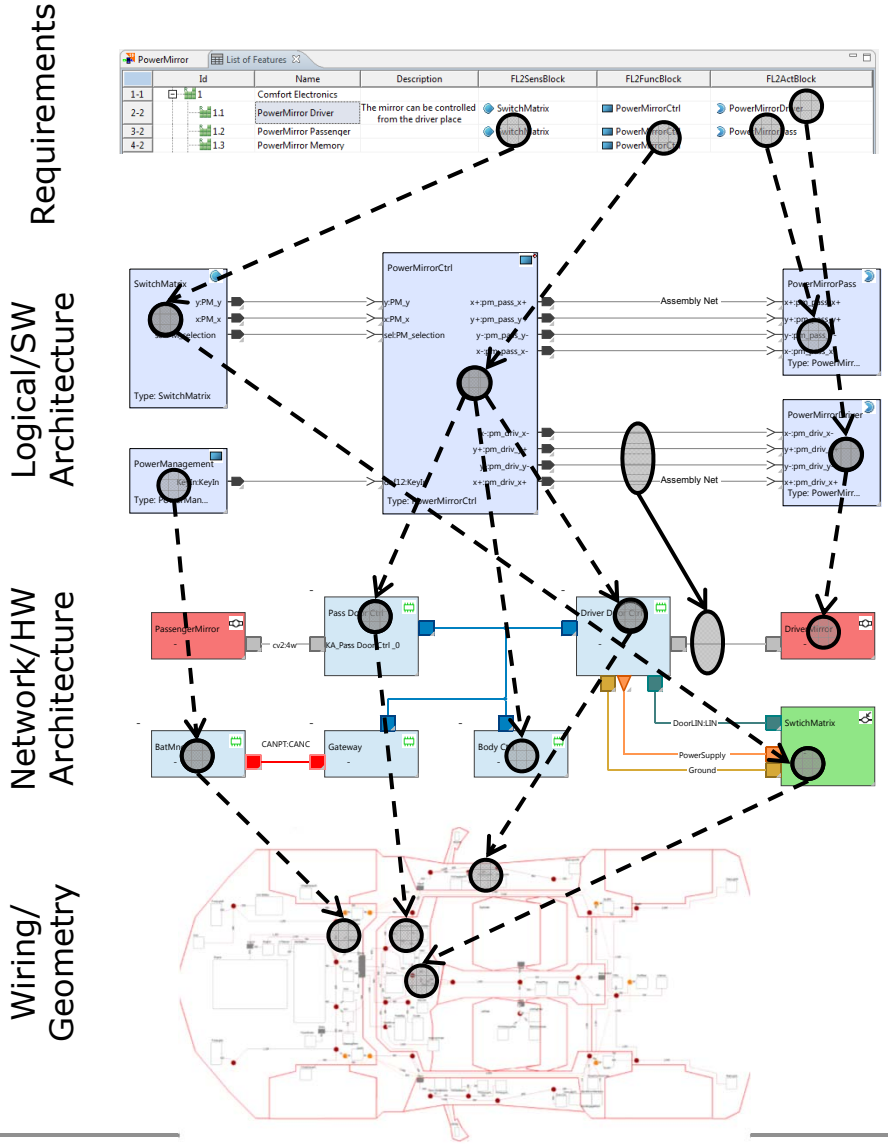



System Level Optimization → Smarter E/E Architecture → Lowered System Costs → Better Expandability → Market Success

# Introduction to PREEvision

## Model-Based E/E-System Engineering (2/2)




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

# Agenda

Introduction to PREEvision

> **Introduction to ISO 26262**

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

# Introduction to ISO 26262

Achieving functional safety effectively means applying best practice to **systems engineering**, **project management** and **quality assurance**

- …plus additional **safety specific analyses** (HARA, FMEA, FTA, FMEDA)
- …and being able to demonstrate that you have done exactly this! (**safety case**)

The development tool chain should actively support this by:

- …managing the complexity in the **E/E system concept design**
- …supporting **bidirectional traceability** between each step of development
- …ensuring safety analysis and development activities are performed on a **single source model** of the system
- …ensuring consistency between all work products referenced by the safety case (**configuration management**)

# Introduction to ISO 26262

1

## Item Definition

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

2

## Hazard and Risk Analysis

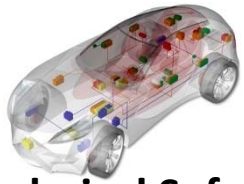
Identification and classification of hazardous scenarios and derivation of appropriate system safety goals.

3


## Functional Safety Concept

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

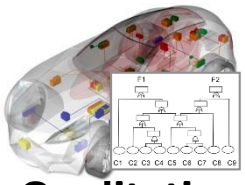
4



## Technical Safety Concept

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

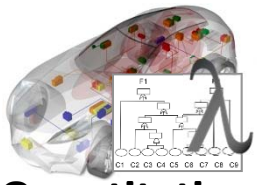
5



## Qualitative Safety Analyses

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

6



## Quantitative Safety Analyses

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

7

## Verification and Validation

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

8


## Safety Case

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





vector

# Introduction to ISO 26262

## 1 Item Definition

- PREEvision Modeling Capabilities
- System Diagrams

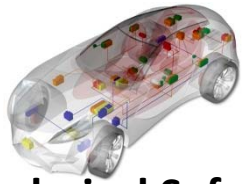
## 2 Hazard and Risk Analysis

- **Hazard and Risk Analysis Editor**
- Hazard and Risk Analysis Report

## 3 Functional Safety Concept

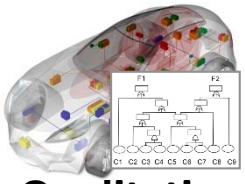

- Logical Architecture
- Activity Chains
- Safety Goal, FSR
- **FSC Report**

## 4 Technical Safety Concept



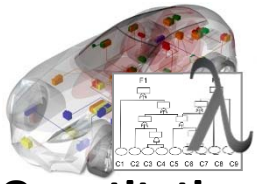
- Hardware Architecture
- Software Architecture
- TSR
- **Safety Mechanisms**
- **HSI Specification Report**
- **TSC Report**

## 5 Qualitative Safety Analyses



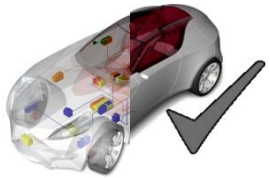
- FMEA
- FTA
- **Automatic FT Synthesis**
- **HW/SW Fault Propagation Analysis**

## 6 Quantitative Safety Analyses



- **Quantitative FTA**
- **HW Architectural Metrics**

## 7 Verification and Validation



- Integration with vTestCenter

## 8 Safety Case


- **Comprehensive Safety Case Report Generator**

**New or improved Features in PREEvision 7.0**

# Introduction to ISO 26262

- **Item Definition** defining the scope of the item under consideration
- **Hazard and Risk Assessment** performed according to method outlined in ISO 26262 – 3
- **System Safety Goals** incl. definition of ASIL and safe state
- **Functional Safety Concept** including allocation of safety goals and functional safety requirements to the system architecture
- **Technical Safety Concept** including refinement of the functional safety concept and allocation of technical safety requirements to hardware and software components
- **Analysis (e.g. FMEA)** to identify failures that can contribute to a violation of the safety goals

These work products must be internally consistent, traceable to one another, well documented and placed under rigorous quality and configuration management control

# Agenda

Introduction to PREEvision

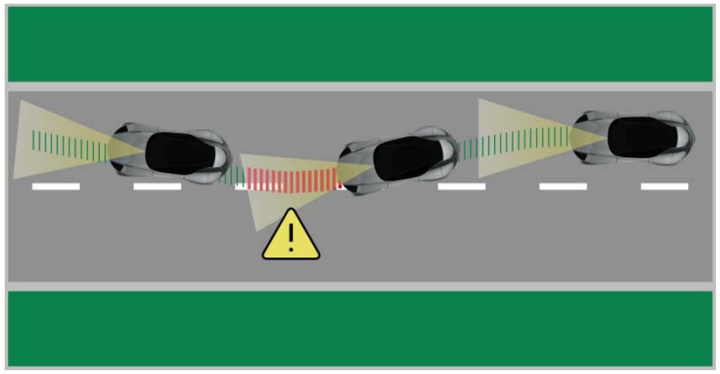
Introduction to ISO 26262

> **ISO 26262 Compliant Development in PREEvision**

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

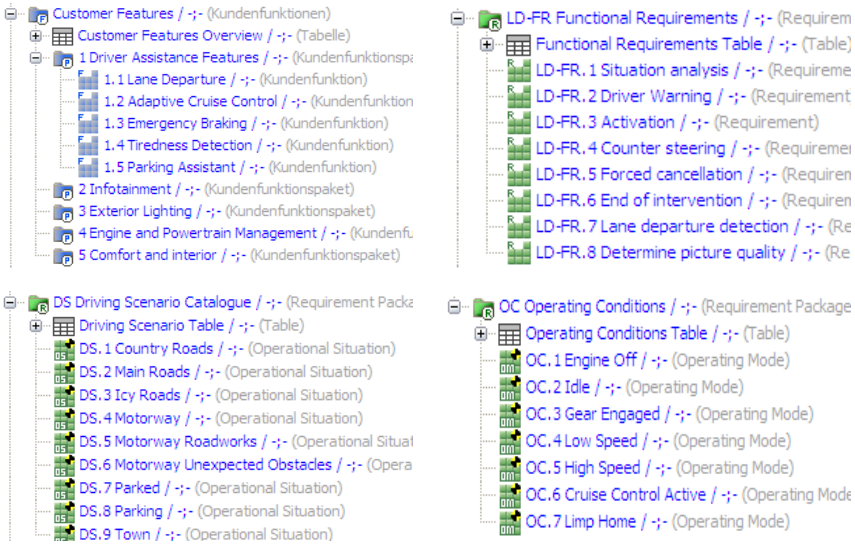
Summary

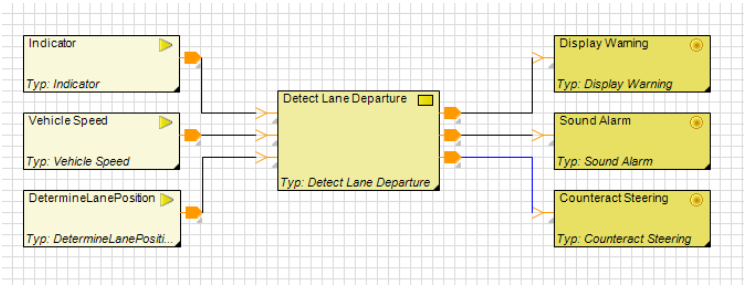
# ISO 26262 Compliant Development in PREEvision



- The lane keeping assistant (LKA) system serves as an example for the reader to better follow and comprehend the presented concepts.
- The basic goal of the LKA system is to serve *„as a mechanism designed to warn a driver when the vehicle begins to move out of its lane (unless a turn signal is on in that direction) and to perform correcting measures if necessary. These systems are designed to minimize accidents by addressing the main causes of collisions: driver error, distractions and drowsiness”*
- The LKA example does not claim to be complete in any sense.
- Its main purpose is to illustrate the model based system engineering approach for functional safety which is provided in PREEvision

# 1. Item Definition




Artefacts modeled in PREEvision:

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

**Typical migration scenario:**
Model those aspects relevant to safety by using imported requirements, SW-Architectures, communication schedules, etc.

# Agenda

Introduction to PREEvision

Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition

> **2. Hazard and Risk Analysis**

3. Functional Safety Concept

4. Technical Safety Concept

5. HW / SW Interface (HSI)

6. Safety Analysis: FMEA

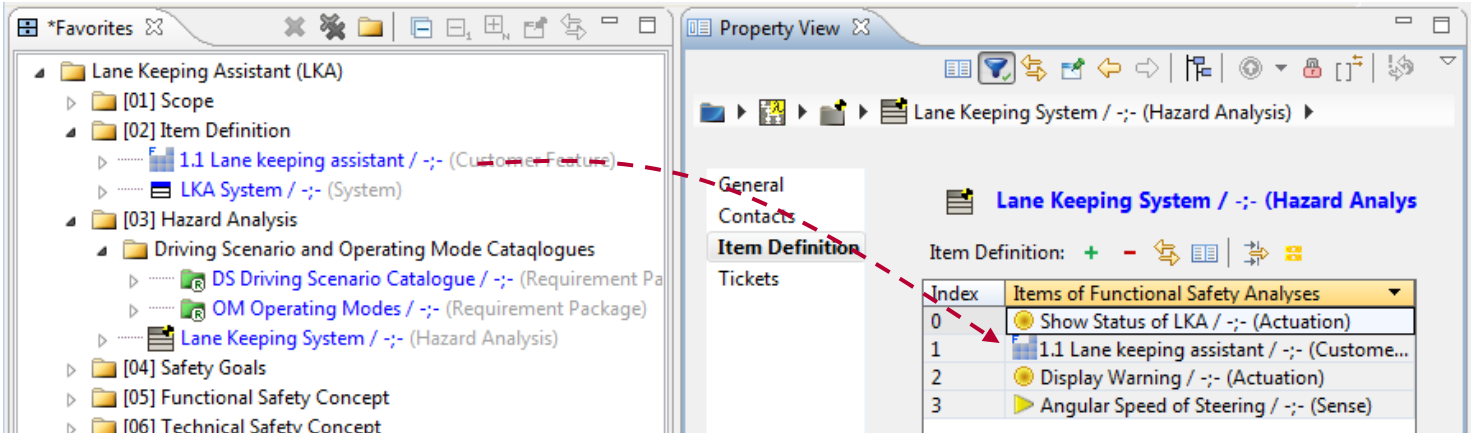
7. Safety Analysis: FTA

8. Safety Analysis: HW Architectural Metrics

9. Safety Case Report

Summary

# 2. Hazard and Risk Analysis




- Drag and drop allocation of item definition artifacts
- Version control and reuse at hazard description level

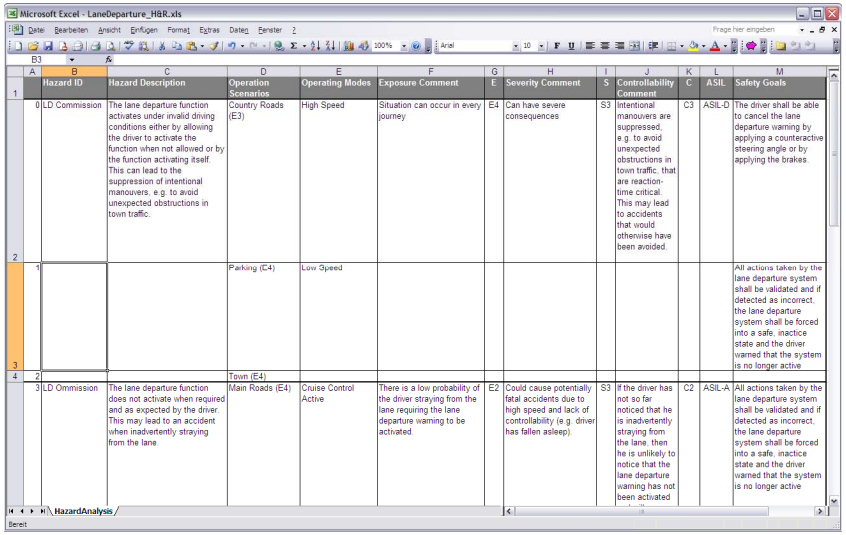
# 2. Hazard and Risk Analysis

| Level | Function | Malfunction | Hazardous Event | Description | Operation Scenarios | Operating Modes | E | S | C | ASIL | Safety |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Status of LKA is shown by dashboard | LKA is switched off but not shown in dashboard | H9 | Driver expects LKA is working and reacts late and crashes into safety fence | Motorway (E4) | Free Driving / High Speed | E4 | S2 | C2 | ASIL-B | Inf ed |
| 2 | LKA starts automatic counter steering ( warning time elapsed) | Counter measure is performed although vehicle is not straying off lane | H6 | No effect | Parked (E4) | Passenger Enters / Exits the Vehicle | E3 | S0 | | QM - Not Safety Relevant | |
| 3 | LKA starts automatic counter steering ( warning time elapsed) | Counter measure performed but in the wrong direction | H3 | Car crashes in the safety fence (heavily) | Motorway (E4) | Free Driving / High Speed | E4 | S3 | C2 | ASIL-C | As ter |
| 4 | Driver is warned by LKA in case of leav | Warning (e.g. lamp) is not working and driver does not perceive | H2 | Driver reacts late and is under stress. Therefore he | Country Roads (E3) | Opposing Traffic | E4 | S2 | C1 | ASIL-A | Wi SIL |

Efficiency & Usability Improvements

- Assign functions / features and malfunctions to hazardous events
- Drag & Drop operations for all columns
- Pick operating scenarios and operating modes from catalogues
- Automatic calculation of ASIL
- **Auto create hazardous events** by D&D of features with malfunctions (library product line / reuse approach)
- Create and link safety goals directly in table

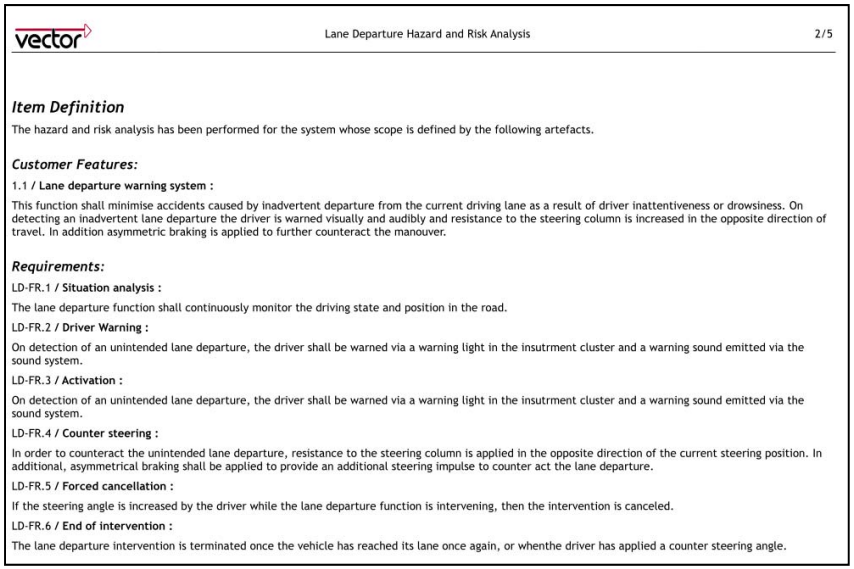
# 2. Hazard and Risk Analysis



Microsoft Excel - LaneDeparture_H&R.xls

| | Hazard ID | Hazard Description | Operation Scenarios | Operating Modes | Exposure Comment | E | Severity Comment | S | Controllability Comment | C | ASIL | Safety Goals |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | LD Commission | The lane departure function activates under invalid driving conditions either by allowing the driver to activate the function when not allowed or by the function activating itself. This can lead to the suppression of intentional manouvers, e.g. to avoid unexpected obstructions in town traffic. | Country Roads (E3) | High Speed | Situation can occur in every journey | E4 | Can have severe consequences | S3 | Intentional manouvers are suppressed, e.g. to avoid unexpected obstructions in town traffic, that are reaction-time critical. This may lead to accidents that would otherwise have been avoided. | C3 | ASIL-D | The driver shall be able to cancel the lane departure warning by applying a counteractive steering angle or by applying the brakes. |
| 1 | | | Parking (E4) | Low Speed | | | | | | | | All actions taken by the lane departure system shall be validated and if detected as incorrect, the lane departure system shall be forced into a safe, inactice state and the driver warned that the system is no longer active. |
| 2 | | | Town (E4) | | | | | | | | | |
| 3 | LD Ommission | The lane departure function does not activate when required and as expected by the driver. This may lead to an accident when inadvertently straying from the lane. | Main Roads (E4) | Cruise Control Active | There is a low probability of the driver straying from the lane requiring the lane departure warning to be activated. | E2 | Could cause potentially fatal accidents due to high speed and lack of controllability (e.g. driver has fallen asleep). | S3 | If the driver has not so far noticed that he is inadvertently straying from the lane, then he is unlikely to notice that the lane departure warning has not been activated | C2 | ASIL-A | All actions taken by the lane departure system shall be validated and if detected as incorrect, the lane departure system shall be forced into a safe, inactice state and the driver warned that the system is no longer active |

HazardAnalysis



vector — Lane Departure Hazard and Risk Analysis — 2/5

***Item Definition***

The hazard and risk analysis has been performed for the system whose scope is defined by the following artefacts.

***Customer Features:***

**1.1 / Lane departure warning system :**

This function shall minimise accidents caused by inadvertent departure from the current driving lane as a result of driver inattentiveness or drowsiness. On detecting an inadvertent lane departure the driver is warned visually and audibly and resistance to the steering column is increased in the opposite direction of travel. In addition asymmetric braking is applied to further counteract the manouver.

***Requirements:***

**LD-FR.1 / Situation analysis :**

The lane departure function shall continuously monitor the driving state and position in the road.

**LD-FR.2 / Driver Warning :**

On detection of an unintended lane departure, the driver shall be warned via a warning light in the insutrment cluster and a warning sound emitted via the sound system.

**LD-FR.3 / Activation :**

On detection of an unintended lane departure, the driver shall be warned via a warning light in the insutrment cluster and a warning sound emitted via the sound system.

**LD-FR.4 / Counter steering :**

In order to counteract the unintended lane departure, resistance to the steering column is applied in the opposite direction of the current steering position. In additional, asymmetrical braking shall be applied to provide an additional steering impulse to counter act the lane departure.

**LD-FR.5 / Forced cancellation :**

If the steering angle is increased by the driver while the lane departure function is intervening, then the intervention is canceled.

**LD-FR.6 / End of intervention :**

The lane departure intervention is terminated once the vehicle has reached its lane once again, or whenthe driver has applied a counter steering angle.

Report generation:

- Export direct to MS Excel
- Configurable report generator (Open Office, Word, PDF)

Example consistency checks to ensure quality of the assessment:

- At least one safety goal per hazard
- Compatibility of safety goal ASILs to hazards
- Compatibility of exposure values to operating scenarios

# Agenda

Introduction to PREEvision

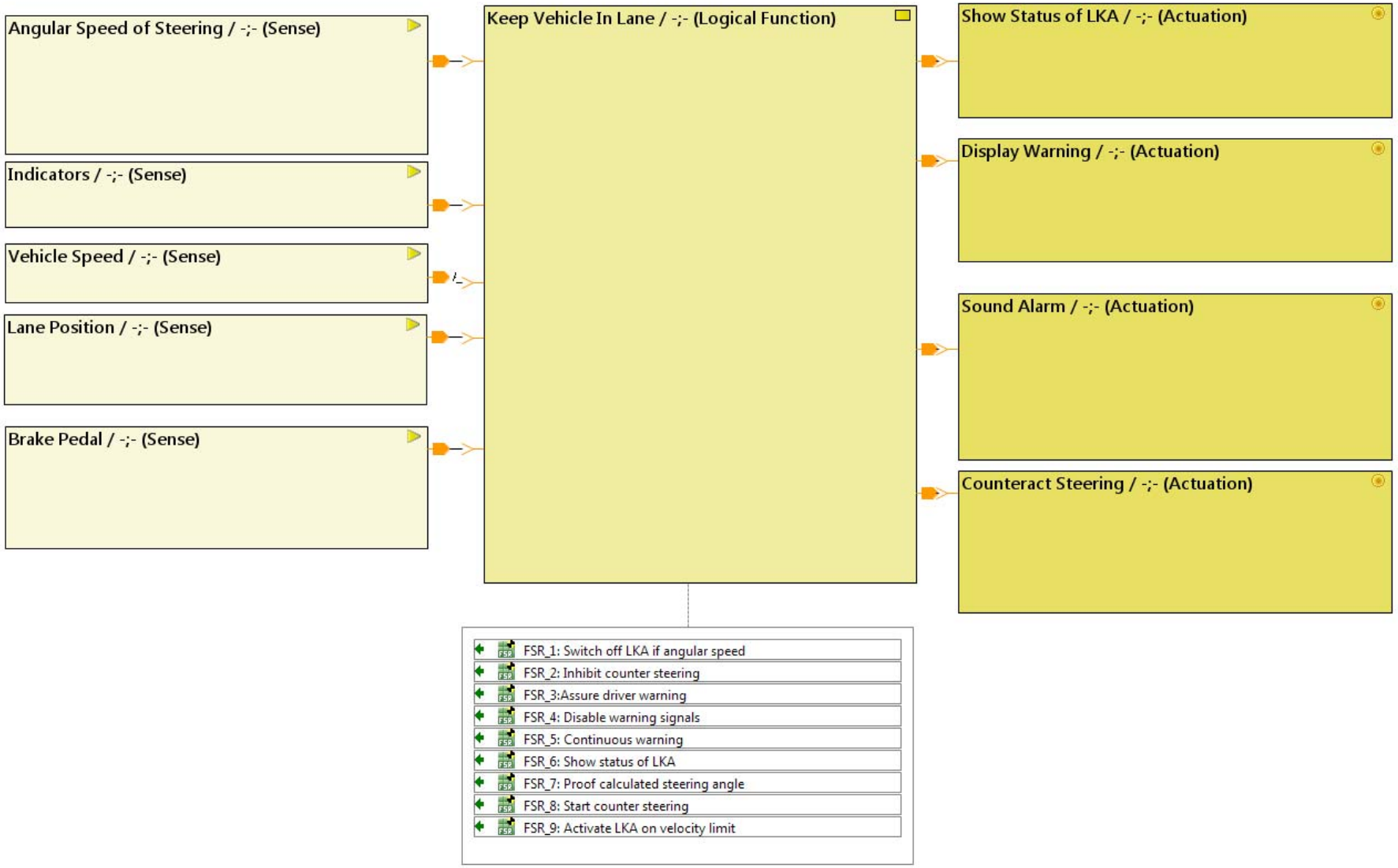
Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. **Functional Safety Concept**
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

# 3. Functional Safety Concept



# 3. Functional Safety Concept

| 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 | | | |

- 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
  - **Propagate ASILs** down along trace links

# Agenda

Introduction to PREEvision

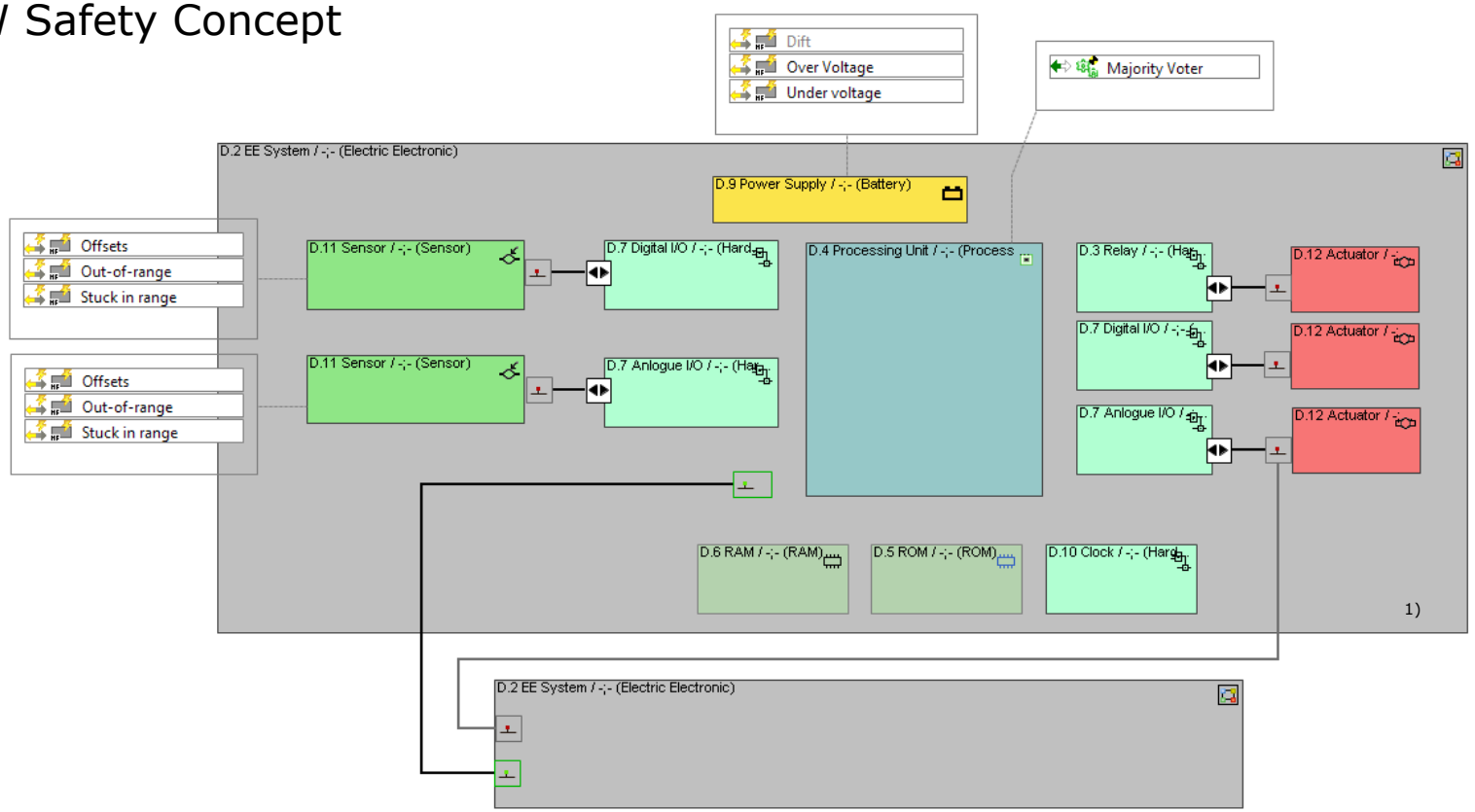
Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. **Technical Safety Concept**
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

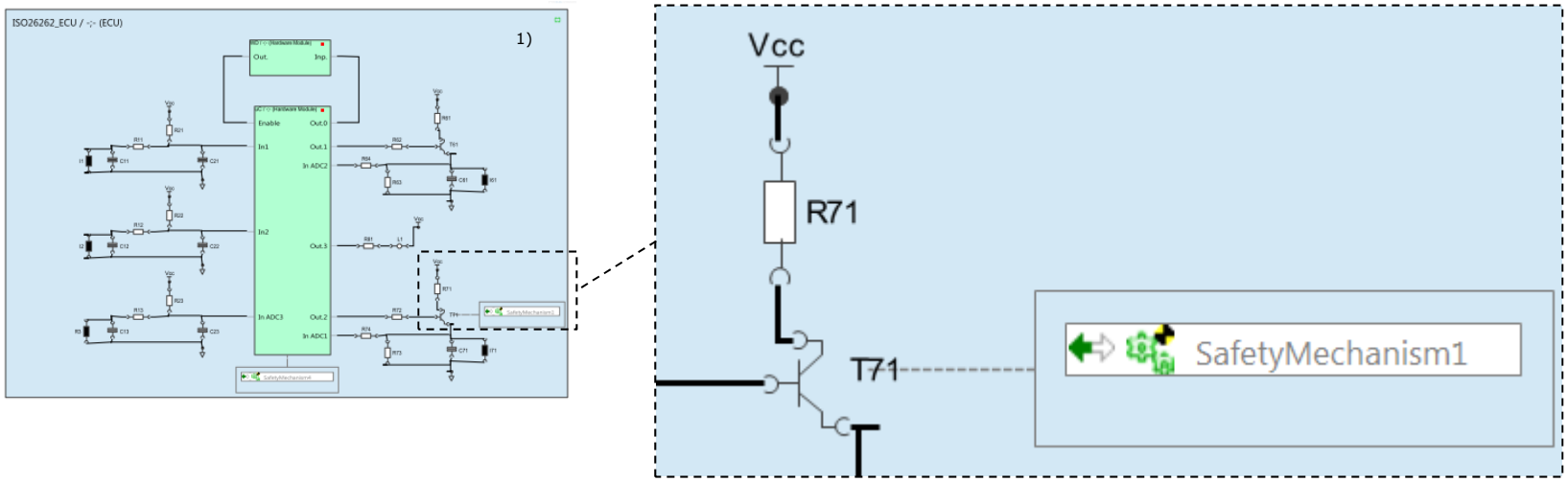
## HW Safety Concept




- 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

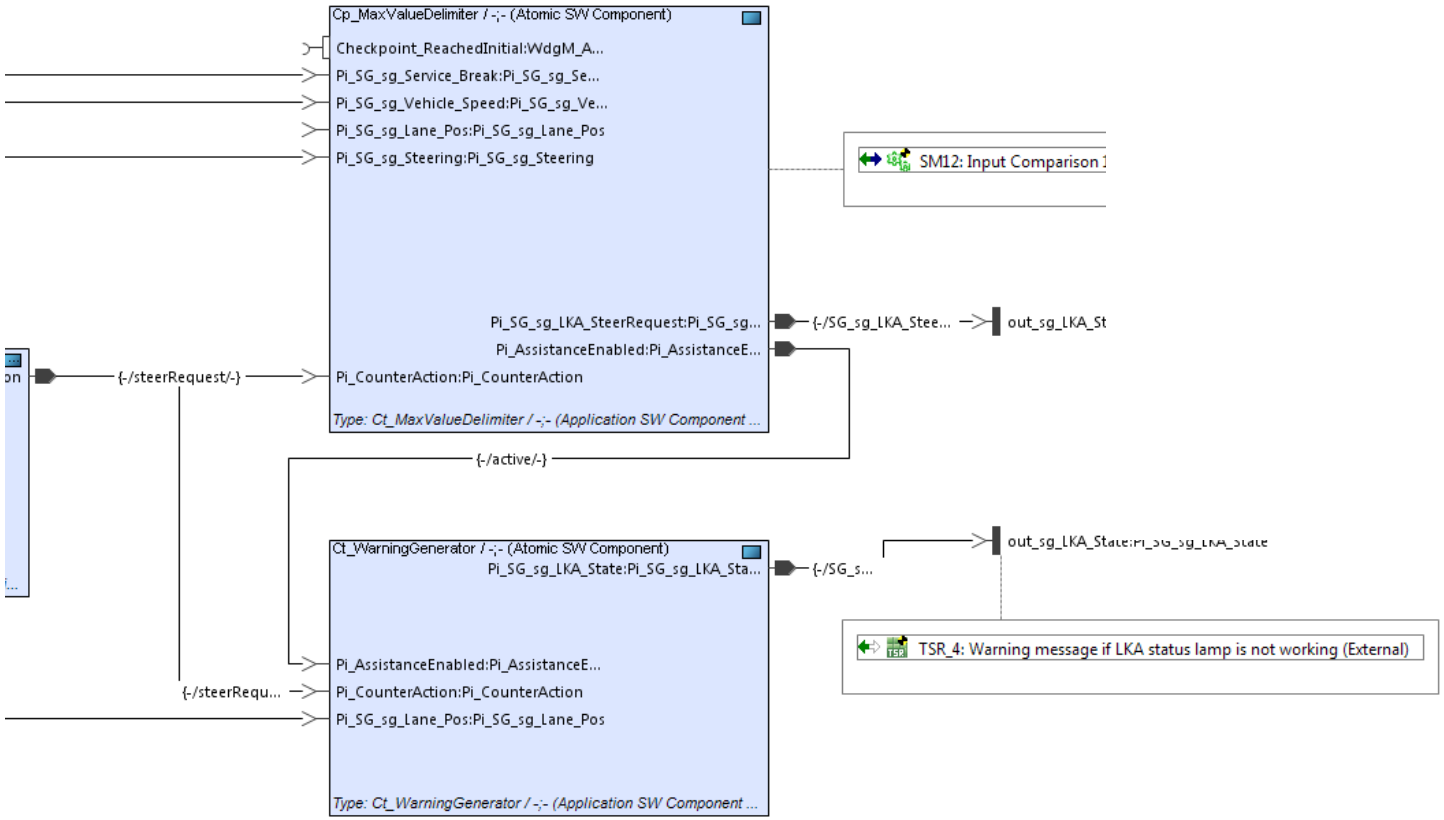
## Detailed HW Safety Concept




- HW safety design can be detailed down to the device level
- 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 E.1

## Detailed SW Safety Concept




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

# Agenda

Introduction to PREEvision

Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept

**> 5. HW / SW Interface (HSI)**

6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

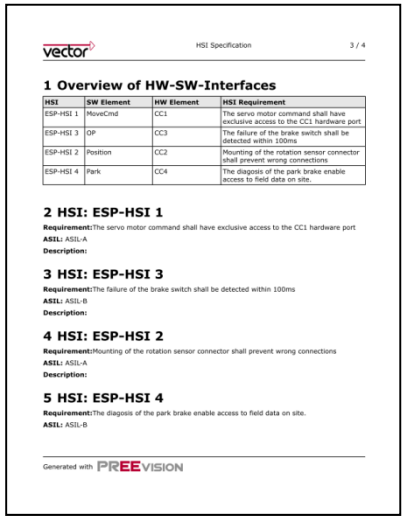
Summary

# 5. HW / SW Interface (HSI)

- 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 |

- 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

# Agenda

Introduction to PREEvision

Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)

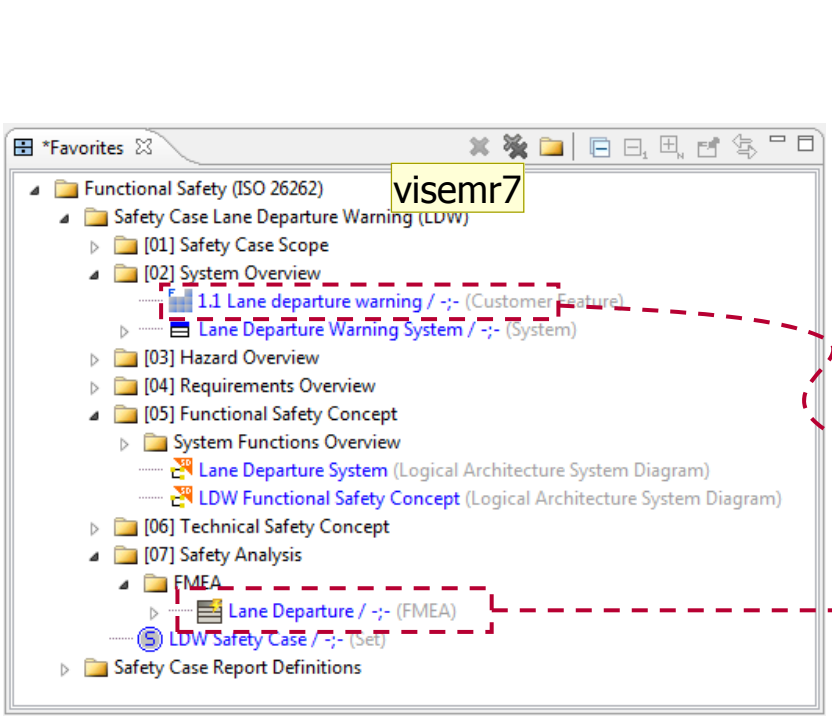
> **6. Safety Analysis: FMEA**

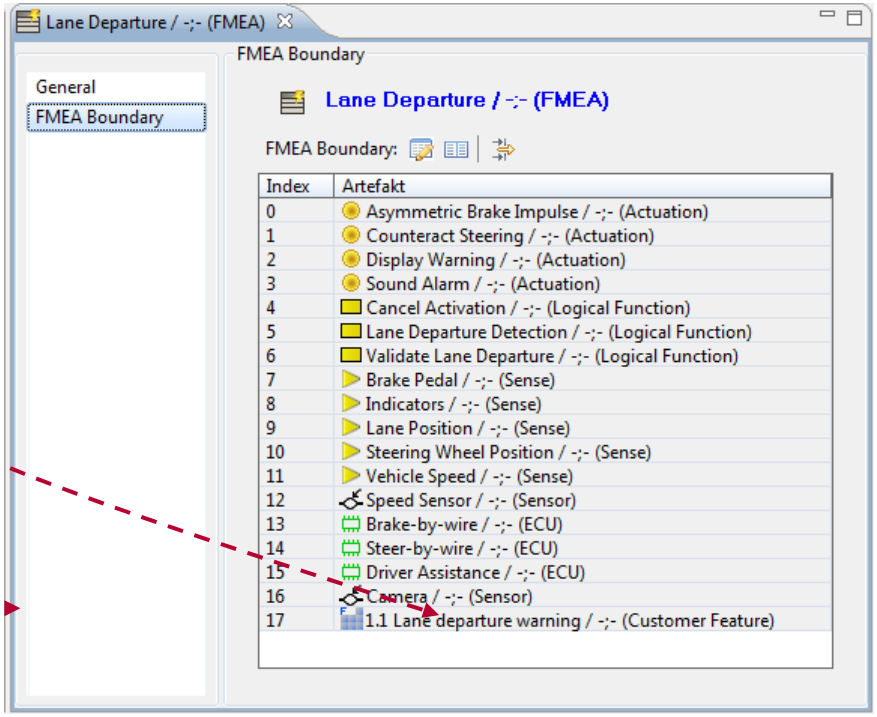
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

# 6. Safety Analysis: FMEA

- FMEA refers directly to requirements, architecture and test artifacts enabling a **round-trip approach** to architecture design and safety analysis.



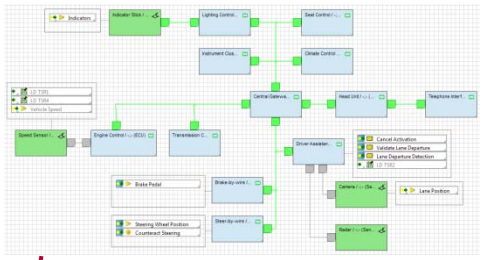



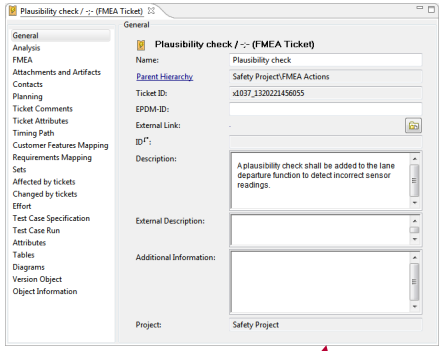
## Folie 27

**visemr7** Anpassen auf LKA

Metzker, Eduard; 30.04.2014

# 6. Safety Analysis: FMEA






Use technical architecture to derive FMEA Parts

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

*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<br>The speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning. | Stuck at<br>The sensor continuously delivers the same speed reading. | Falsely activated<br>The lane departure system is activated when it shouldn't be. | 9 | YC | Hardware failure<br>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<br>A plausibility check shall be added to the lane departure function to detect incorrect sensor readings. | Metzker | Nov 30, 2011 |
| 2 | | | Shortcut to ground<br>Shortcut to ground | No activation<br>Lane departure is not activated | 6 | YS | Internal hardware fa...<br>Stuck at fault to hardware | 5 | The speed sensor is currently qualified to ASIL A | None defined as yet. | 10 | 300 | Plausibility check<br>A plausibility check shall be | Metzker | Nov 30, 2011 |
| | | | | actual ... speed. | | | | | | | | | | | |
| 5 | Camera | Provide lane position d... | No data<br>The camera delivers no picture at all | Departure not dete...<br>A departure from the lane cannot be detected. | 7 | YS | Camera obscured<br>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 | | | |

# 6. Safety Analysis: FMEA

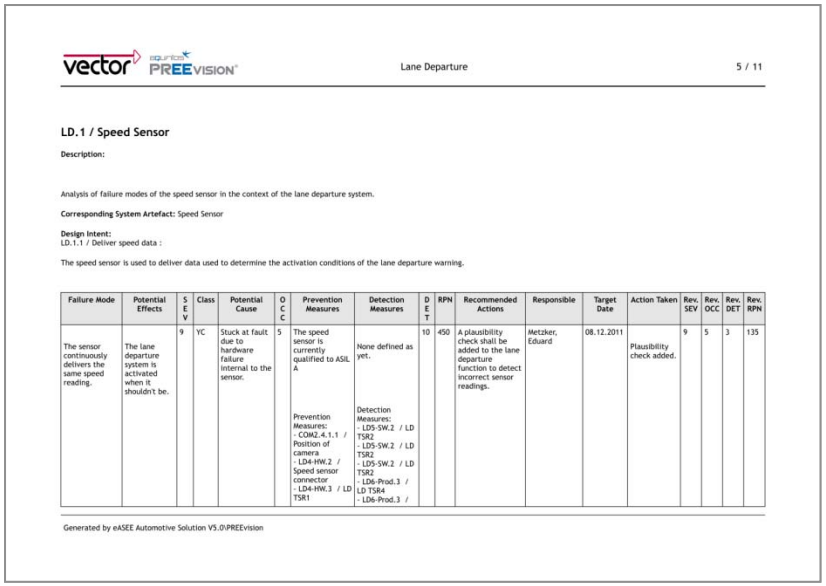
- FMEA actions are directly modeled as change tickets and can be allocated to human resources, work packages etc.
- Different tables can be configured to provide use case specific views on the data (e.g. FMEA entries sorted according to RPN).

*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 | Actions Taken | Rev. SEV | Rev. OCC | Rev. DET |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Speed Sensor | Deliver speed data<br>The speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning. | Stuck at<br>The sensor continuously delivers the same speed reading. | Falsely activated<br>The lane departure system is activated when it shouldn't be. | 9 | YC | Hardware failure<br>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<br>A plausibility check shall be added to the lane departure function to detect incorrect sensor readings. | Metzker | Nov 30, 2011 | Plausibility check added. | 9 | 5 | 3 |
| 2 | | | Shortcut to ground<br>Shortcut to ground resulting in a constant low output. | No activation<br>Lane departure is not activated due to an incorrect vehicle speed reading. | 6 | YS | Internal hardware fa...<br>Stuck at fault due to hardware failure internal to the sensor | 5 | The speed sensor is currenlty qualified to ASIL A | None defined as yet. | 10 | 300 | Plausibility check<br>A plausibility check shall be added to the lane departure function to detect incorrect sensor readings. | Metzker | Nov 30, 2011 | Plausibility check added. | 6 | 5 | 3 |
| 3 | | | | | | None | Wrongly connected<br>The sensor is wrongly connected (ground line connected to output). | 3 | An asymmetric connector is used to avoid wrong connections. | End of line tests ensure that a valid signal is recieved from the wheel speed sensor. | 5 | 90 | | | | | | | |
| 4 | | | Drift<br>The value delivered by the wheel speed sensor varies from the correct value over time. | Wrong correction ...<br>The incorrect amount of counter steering and braking is applied in relation to the actual vehicle speed | 7 | YS | Wear and tear<br>Wearing in the mechanical components of the sensor. | 7 | None identified as yet. | None identified as yet. | 10 | 490 | Periodic recalibration<br>The wheel speed sensors shall be recalibrated as part of standard maintenance schedules. | Burton | Nov 30, 2011 | Relevant entries added to the after sales documentation. | 8 | 7 | 8 |

# 6. Safety Analysis: FMEA

- Consistency checks validate the traceability of prevention and detection measures.
- FMEAs can be exported according to user configurable document templates or as an excel file.



vector PREEVISION Lane Departure 5 / 11

**LD.1 / Speed Sensor**

**Description:**

Analysis of failure modes of the speed sensor in the context of the lane departure system.

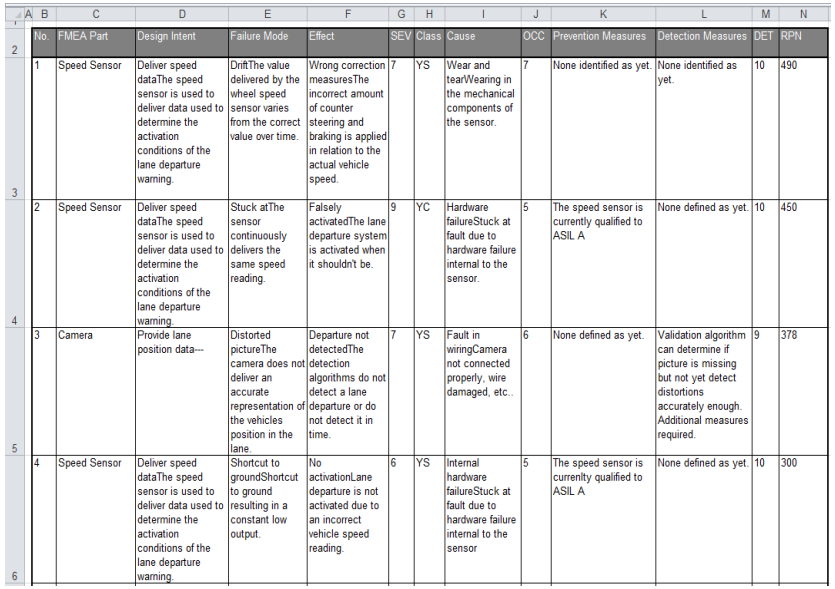
**Corresponding System Artefact:** Speed Sensor

**Design Intent:**
LD.1.1 / Deliver speed data :

The speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning.

| Failure Mode | Potential Effects | SEV | Class | Potential Cause | OCC | Prevention Measures | Detection Measures | DET | RPN | Recommended Actions | Responsible | Target Date | Action Taken | Rev. SEV | Rev. OCC | Rev. DET | Rev. RPN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| The sensor continuously delivers the same speed reading. | The lane departure system is activated when it shouldn't be. | 9 | YC | Stuck at fault due to hardware failure internal to the sensor. | 5 | The speed sensor is currently qualified to ASIL A<br><br>Prevention Measures:<br>- COM2.4.1.1 / Position of camera<br>- LD4-HW.2 / Speed sensor connector<br>- LD4-HW.3 / LD TSR1 | None defined as yet.<br><br>Detection Measures:<br>- LD5-SW.2 / LD TSR2<br>- LD5-SW.2 / LD TSR2<br>- LD5-SW.2 / LD TSR2<br>- LD6-Prod.3 / LD TSR4<br>- LD6-Prod.3 / | 10 | 450 | A plausibility check shall be added to the lane departure function to detect incorrect sensor readings. | Metzker, Eduard | 08.12.2011 | Plausibility check added. | 9 | 5 | 3 | 135 |

Generated by eASEE Automotive Solution V5.0\PREEvision



| No. | FMEA Part | Design Intent | Failure Mode | Effect | SEV | Class | Cause | OCC | Prevention Measures | Detection Measures | DET | RPN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Speed Sensor | Deliver speed dataThe speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning. | DriftThe value delivered by the wheel speed sensor varies from the correct value over time. | Wrong correction measuresThe incorrect amount of counter steering and braking is applied in relation to the actual vehicle speed. | 7 | YS | Wear and tearWearing in the mechanical components of the sensor. | 7 | None identified as yet. | None identified as yet. | 10 | 490 |
| 2 | Speed Sensor | Deliver speed dataThe speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning. | Stuck atThe sensor continuously delivers the same speed reading. | Falsely activatedThe lane departure system is activated when it shouldn't be. | 9 | YC | Hardware failureStuck 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 |
| 3 | Camera | Provide lane position data--- | Distorted pictureThe camera does not deliver an accurate representation of the vehicles position in the lane. | Departure not detectedThe detection algorithms do not detect a lane departure or do not detect it in time. | 7 | YS | Fault in wiringCamera not connected properly, wire damaged, etc.. | 6 | None defined as yet. | Validation algorithm can determine if picture is missing but not yet detect distortions accurately enough. Additional measures required. | 9 | 378 |
| 4 | Speed Sensor | Deliver speed dataThe speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning. | Shortcut to groundShortcut to ground resulting in a constant low output. | No activationLane departure is not activated due to an incorrect vehicle speed reading. | 6 | YS | Internal hardware failureStuck at fault due to hardware failure internal to the sensor | 5 | The speed sensor is currenlty qualified to ASIL A | None defined as yet. | 10 | 300 |

# Agenda

Introduction to PREEvision

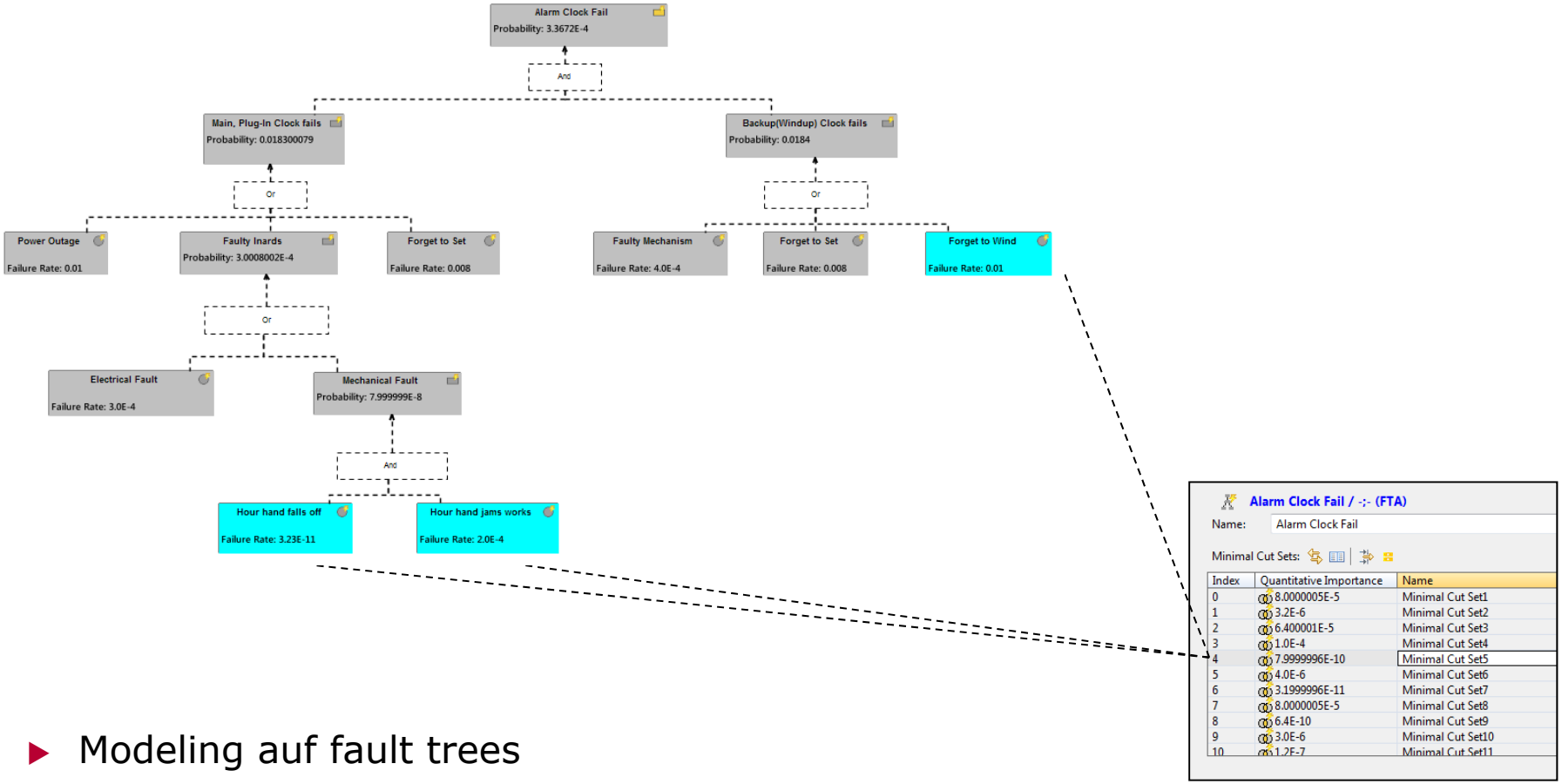
Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
> **7. Safety Analysis: FTA**
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary

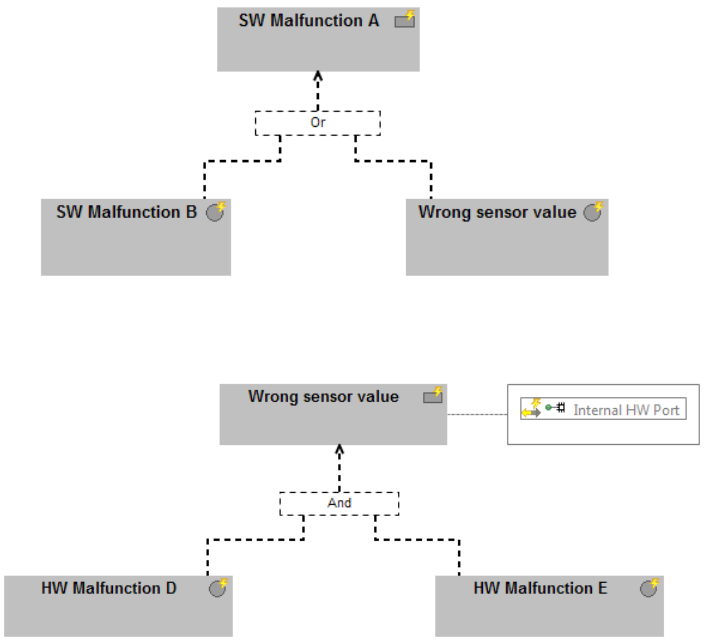
# 7. Safety Analysis: FTA



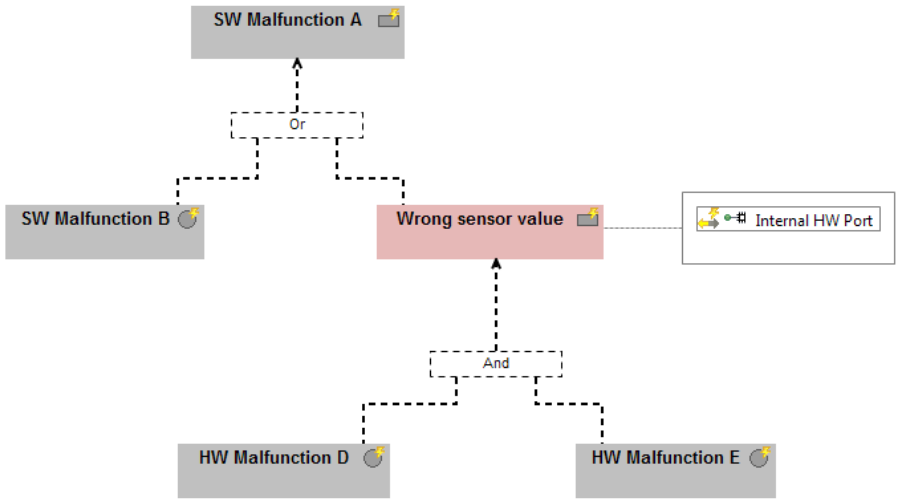

- Modeling auf fault trees
- Calculation of minimal cut sets (Qualitative Analysis)
- Calculation of quantitative importance of minimal cut sets (Quantitative Analysis)

# 7. Safety Analysis: FTA

Local Fault Trees




Synthesized Fault Tree




- Local fault trees of HW/SW components can be automatically synthesized to fault trees of the overall system

# Agenda

Introduction to PREEvision

Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

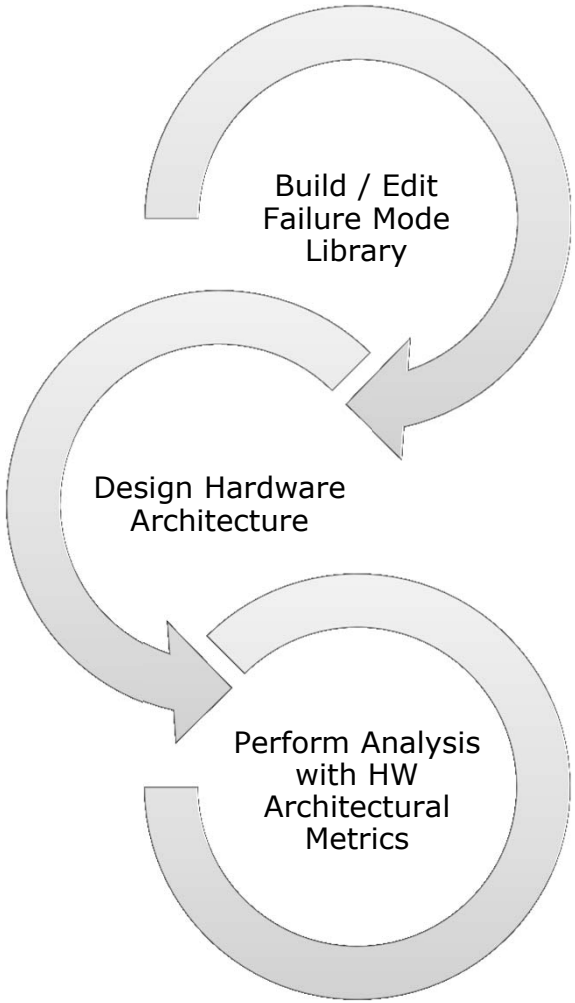
1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA

> **8. Safety Analysis: HW Architectural Metrics**

9. Safety Case Report

Summary

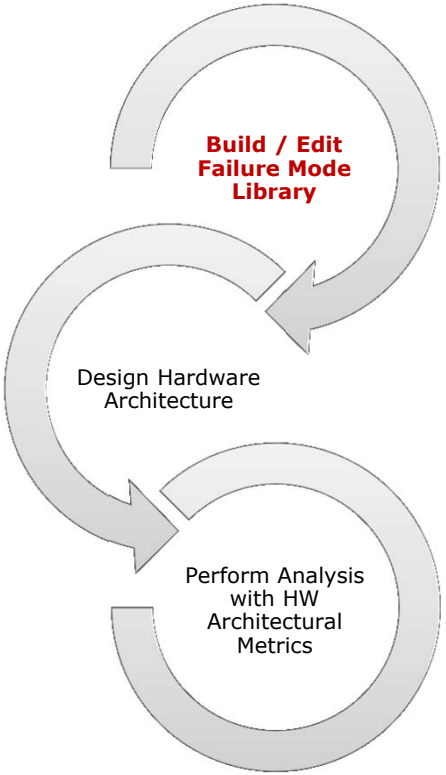
# 8. Safety Analysis: HW Architectural Metrics



# 8. Safety Analysis: HW Architectural Metrics

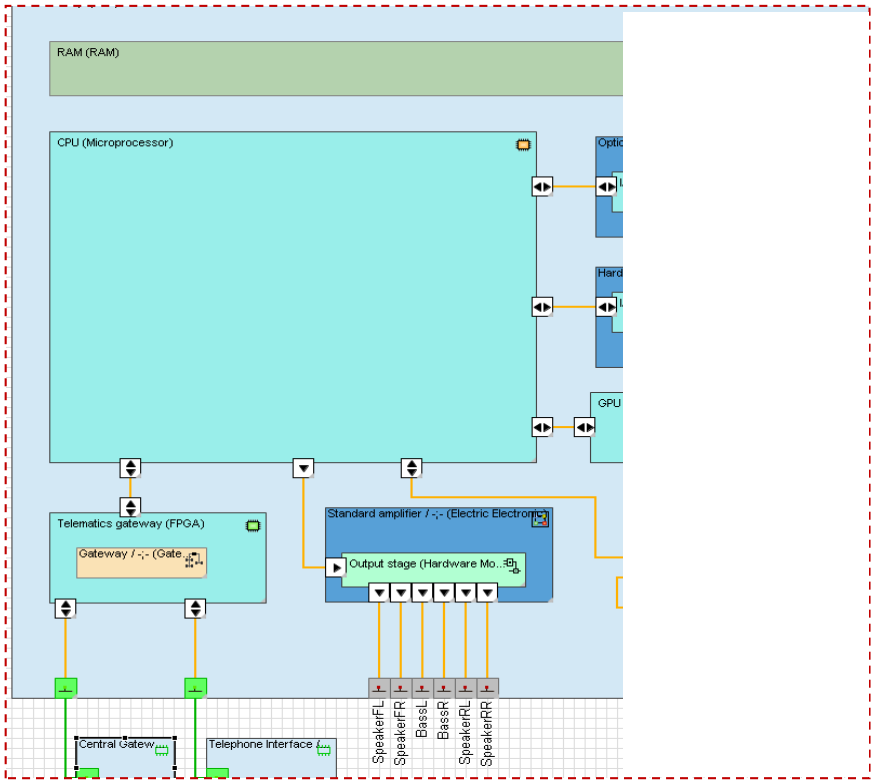
- Build failure mode library by **convenient annotation** of **all HW library elements** (e.g. Devices Types, Module Types, CPU types etc.)
- Dedicated **Failure Mode Library Editor** for high usability and efficiency

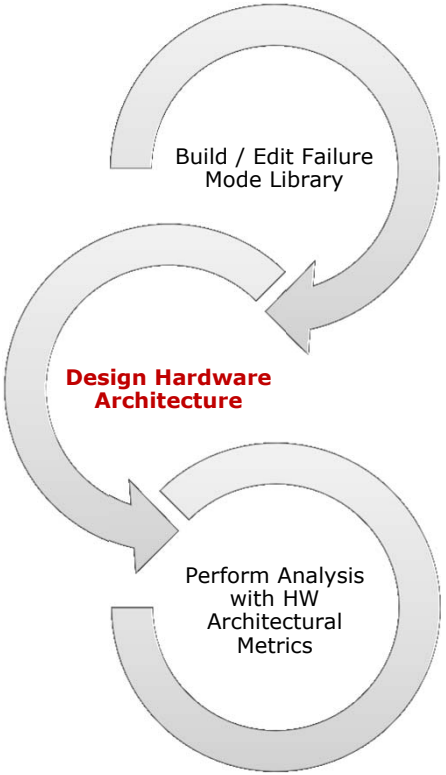
| Library Element | FIT | Failure Mode | % Di |
|---|---|---|---|
| C-EU | 2.0 | open circuit | 20.0 |
| | | short circuit | 80.0 |
| GND | | | |
| LED | 10.0 | open circuit | 90.0 |
| | | short circuit | 10.0 |
| R-EU | 2.0 | open circuit | 90.0 |
| | | short circuit | 10.0 |
| SENSOR-TEMPERATURE | 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 |



# 8. Safety Analysis: HW Architectural Metrics

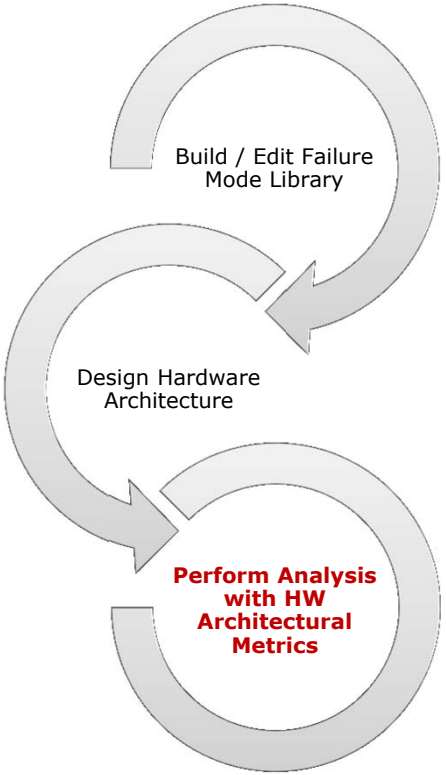
- Use library elements during HW design as usual
- **Increased efficiency** by reusing failure mode definitions for design from library



# 8. Safety Analysis: HW Architectural Metrics

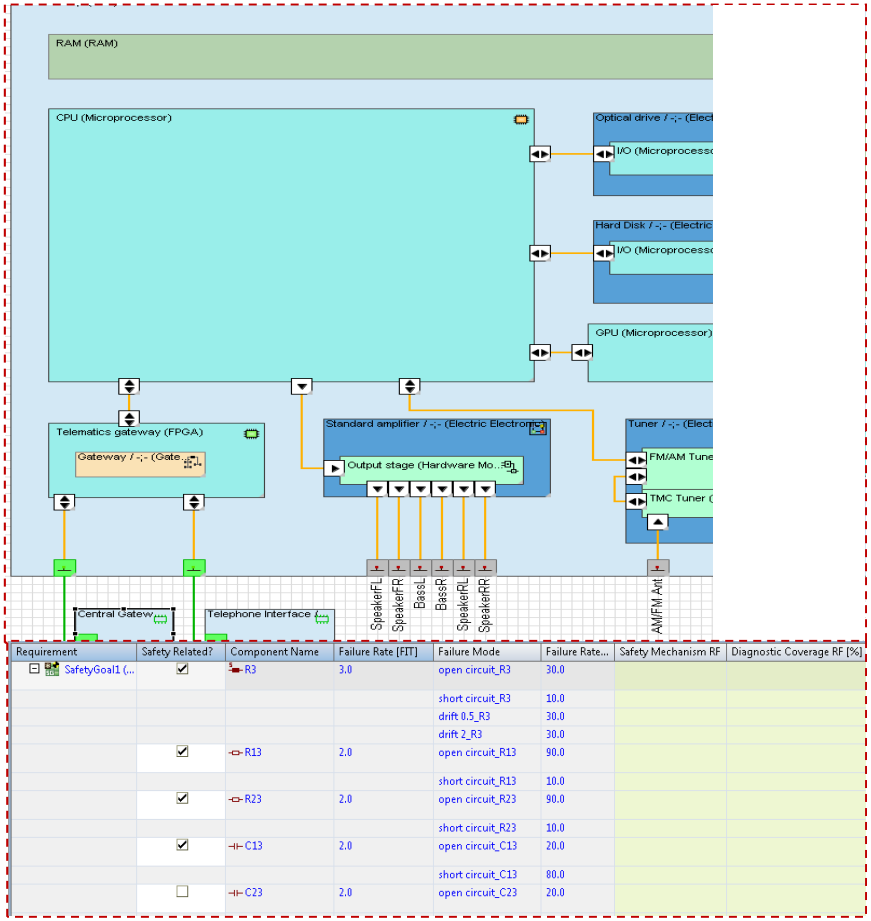
- Allocate **target values** via D&D
- Assign **safety mechanisms** and detection mechanisms via D&D
- Convenient **HW architectural metrics calculator**
- **Instant highlighting** of fullfillments and violations
- **Covers all metrics defined ISO 26262 - 5**

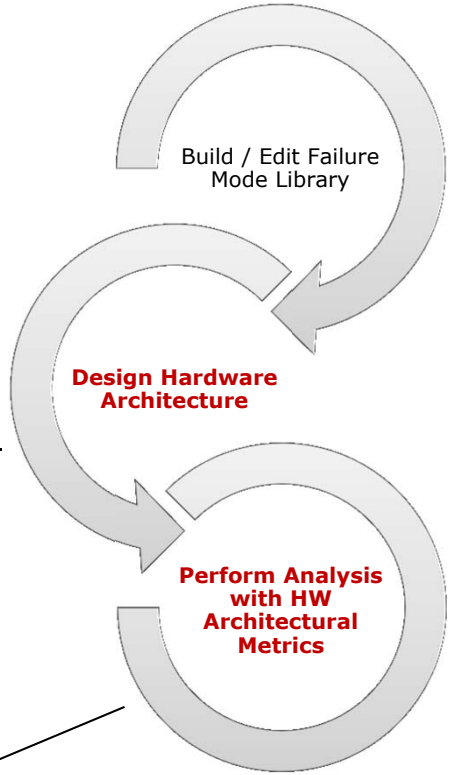



| Requirement | Safety Related? | Component Name | Failure Rate [FIT] | Failure Mode | Failure Rate... | Safety Mechanism RF | Diagnostic Coverage RF [%] | SF |
|---|---|---|---|---|---|---|---|---|
| SafetyGoal1 (... | ☑ | R3 | 3.0 | open circuit_R3 | 30.0 | | | 0. |
| | | | | short circuit_R3 | 10.0 | | | |
| | | | | drift 0.5_R3 | 30.0 | | | |
| | | | | drift 2_R3 | 30.0 | | | 0. |
| | ☑ | R13 | 2.0 | open circuit_R13 | 90.0 | | | 1. |
| | | | | short circuit_R13 | 10.0 | | | 0. |
| | ☑ | R23 | 2.0 | open circuit_R23 | 90.0 | | | |

# 8. Safety Analysis: HW Architectural Metrics

- Integrated iterative Design and **Analysis / Optimization**



# 8. Safety Analysis: HW Architectural Metrics

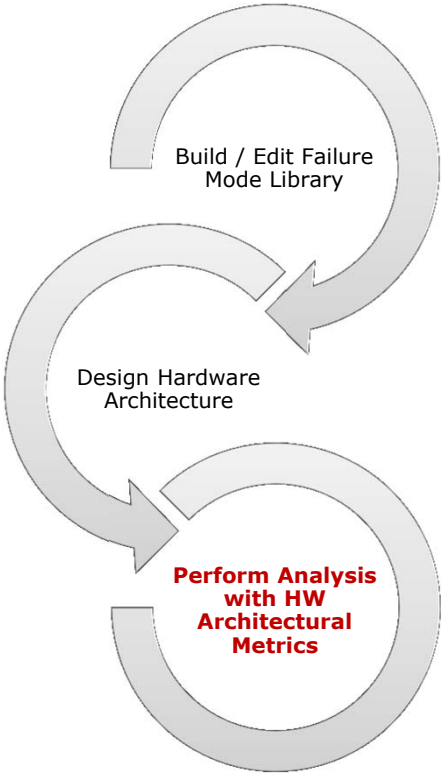
- Conveniently create HW Architetural Metrics Report

### 5.2 Failure Data Table

| Component Name | Failure Rate / FIT | Safety-Related HW component ? | Failure Mode | Failure Rate Distribution | Failure Mode has potential to directly violate the safety goal? | Safety Mechanism for direct violation | Diagnostic Coverage with respect to residual faults | Residual or Single-Point Fault failure rate / FIT | Failure Mode has potential to violate the safety goal in combination with another fault? | Safety Mechanism for violation in combination with another fault | Diagnostic Coverage with respect to latent faults | Latent Multiple-Point Fault failure rate / FIT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R71 | 2.00 | YES | ShortCircuit | 10.0 % | | | | | X | none | 0.0 % | 0.20 |
| C71 | 2.00 | YES | OpenCircuit | 20.0 % | | | | | X | none | 0.0 % | 0.40 |
| C71 | 2.00 | YES | ShortCircuit | 80.0 % | | | | | | | | |
| WD | 20.00 | YES | StuckAtOne | 50.0 % | | | | | X | none | 0.0 % | 10.00 |
| WD | 20.00 | YES | StuckAtZero | 50.0 % | | | | | | | | |
| T71 | 5.00 | YES | OpenCircuit | 50.0 % | X | SM1 | 90.0 % | 0.25 | X | SM1 | 80.0 % | 0.45 |
| T71 | 5.00 | YES | ShortCircuit | 50.0 % | | | | | | | | |
| µC | 100.00 | YES | All | 50.0 % | X | SM4 | 90.0 % | 5.00 | X | SM4 | 100.0 % | 0.00 |
| µC | 100.00 | YES | All2 | 50.0 % | | | | | | | | |

### 5.3 Hardware Architectural Metrics

| SafetyGoal1 | |
|---|---|
| Total Failure Rate: | 163.00 FIT |
| Total Safety Related: | 142.00 FIT |
| Total Not SafetyRelated: | 21.00 FIT |
| ASIL-Level: | ASIL-B |
| **Single-Point Fault Metric:** | |
| Sum of Single-Point and Residual Faults: | 9.65 FIT |
| Single-Point Fault Metric: | 93.20 % |
| Single-Point Fault Metric Target ASIL Reached? | Status: fullfilled |
| **Latent-Fault Metric:** | |
| Sum of Latent Multiple-Point Faults: | 13.25 FIT |
| Latent-Fault Metric: | 89.99 % |
| Latent-Fault Metric Target ASIL Status? | Status: fullfilled |



# Agenda

Introduction to PREEvision

Introduction to ISO 26262

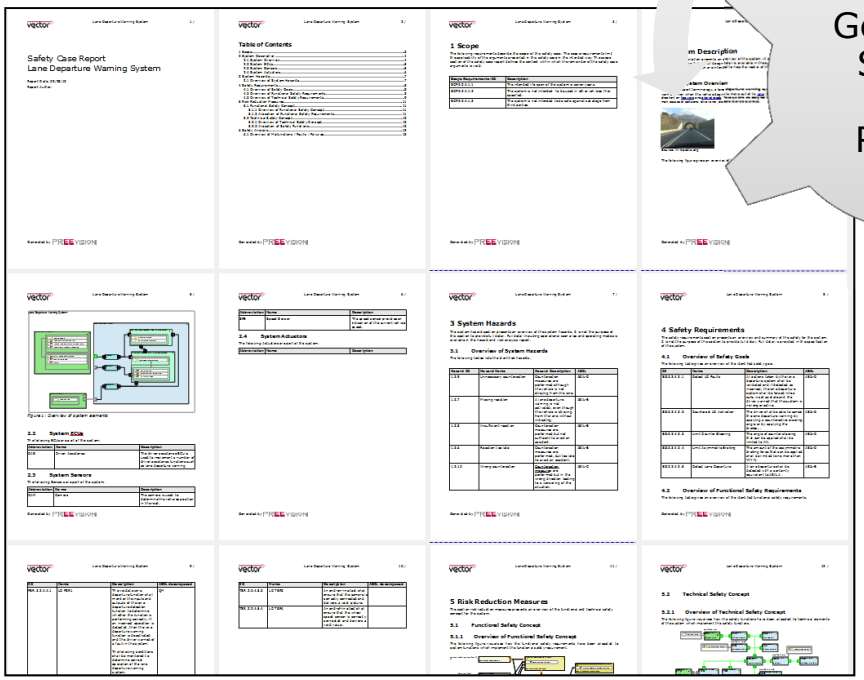
ISO 26262 Compliant Development in PREEvision

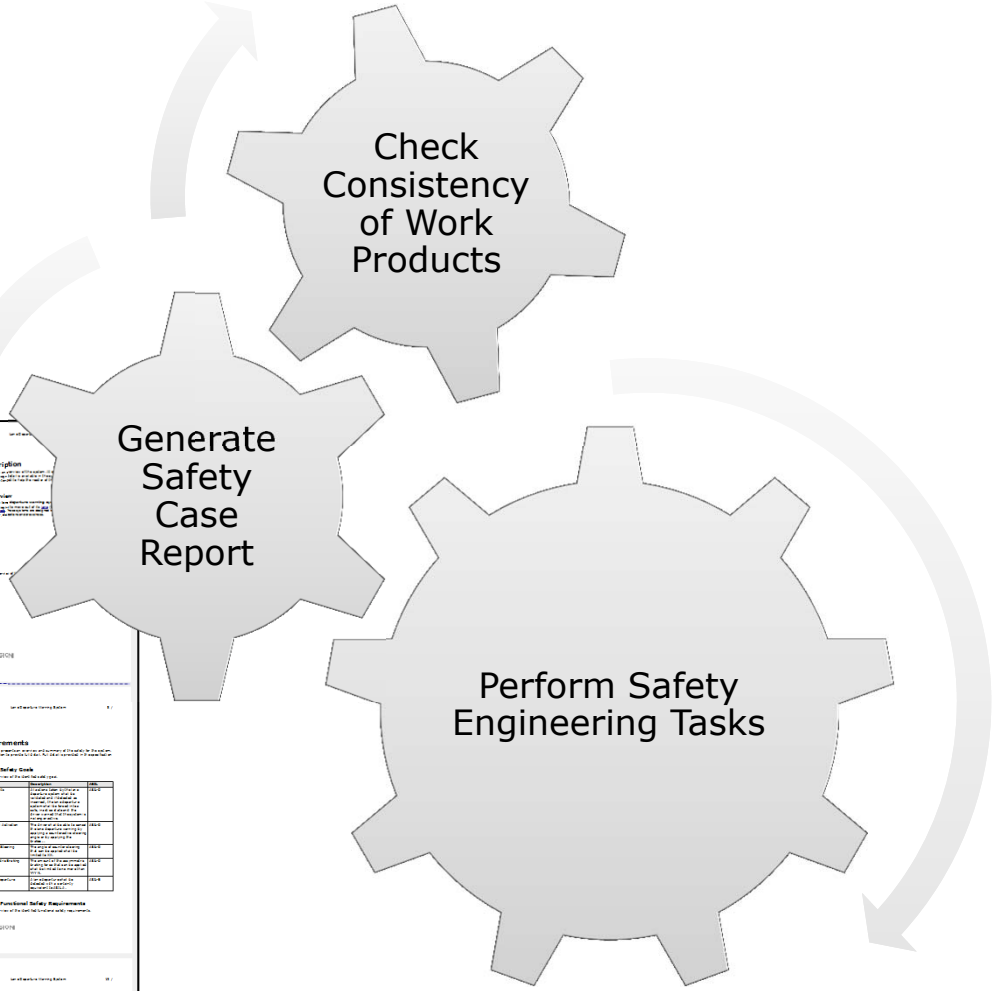
1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics

> **9. Safety Case Report**

Summary

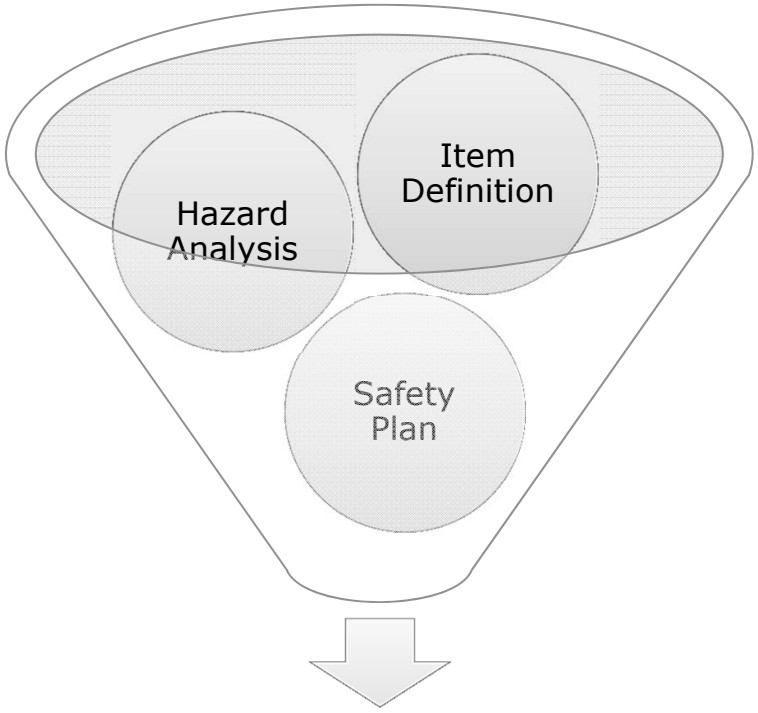
# 9. Safety Case Report



# 9. Safety Case Report

Safety Case




Safety Case Report

- **Safety Case artifact** collects work products which are the input for the safety case report(e.g. Safety Hazard Analysis, Requirement Packages, FMEA, Safety Plan etc.)
- Report distills the content which is required for safety case report
- **Always consistent** report based on current status of work products
- Dramatic **reduction of costs** for consistent documentation

# Agenda

Introduction to PREEvision

Introduction to ISO 26262

ISO 26262 Compliant Development in PREEvision

1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. HW / SW Interface (HSI)
6. Safety Analysis: FMEA
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

**> Summary**

# Summary

1

**Item Definition**

Available

2

**Hazard and Risk Analysis**

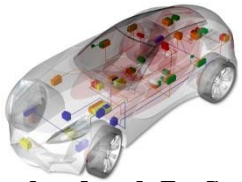
Available

3


**Functional Safety Concept**

Available

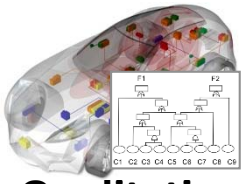
4



**Technical Safety Concept**

Available

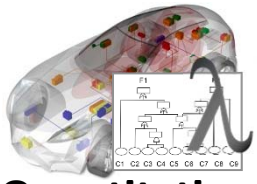
5



**Qualitative Safety Analyses**

Available

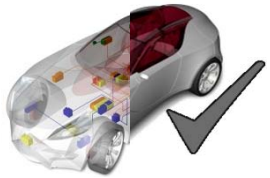
6



**Quantitative Safety Analyses**

Available

7



**Verification and Validation**

Available

8


**Safety Case**

Available





vector

# Summary

## Advantages for Functional Safety

- **Safety concepts** can be systematically derived and evaluated according to a wide range of criteria:
  - Automated **consistency checking** of safety concepts
  - **System level optimization**, taking into account all architecture levels (Software, Network, Component, Wiring, Geometry).

- **Safety analyses** (e.g. FMEA) are based on a **single source model** ensuring consistency between the analyses and the development stream.
  - **Safety Round-Trip Engineering**: The results of safety analyses are directly visible in the model. The impact of changes in the architecture are directly visible in the relevant parts of the safety analysis.

- See Vector website for technical papers and trainings on functional safety
  - http://vector.com/portal/medien/cmc/factsheets/Safety_Solution_FactSheet_EN.pdf
  - http://vector.com/portal/medien/distributed_systems/preevision/ATZe_201305_EN.pdf
  - https://vector.com/vi_news_en.html#!vi_news_detail_iframe_en,,,1220395,detail.html

Thank you for your attention.

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

Author:

Dr. Eduard Metzker

Product Line Process Tools,
Vector Informatik GmbH Stuttgart