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

Dr. Eduard Metzker
May 2014
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)
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...)
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)
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

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

Summary
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)
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

<table>
<thead>
<tr>
<th>Level</th>
<th>Function</th>
<th>Malfunction</th>
<th>Hazardous Event</th>
<th>Description</th>
<th>Operation Scenarios</th>
<th>Operating Modes</th>
<th>E</th>
<th>S</th>
<th>C</th>
<th>ASIL</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Status of LKA is shown by dashboard</td>
<td>LKA is switched off but not shown in dashboard</td>
<td>EH6</td>
<td>Driver expects LKA is working and reacts late and crashes into safety device</td>
<td>Motorway (E4)</td>
<td>Free Driving / High Speed</td>
<td>E4</td>
<td>S2</td>
<td>C2</td>
<td>ASIL-B</td>
<td>Noted</td>
</tr>
<tr>
<td>2</td>
<td>LKA starts automatic counter steering (warning time elapsed)</td>
<td>Countermeasure is performed although vehicle is not staying on lane</td>
<td>EH5</td>
<td>No effect</td>
<td>Parked (E4)</td>
<td>Passenger Enters / Exits the Vehicle</td>
<td>E3</td>
<td>S0</td>
<td>C0</td>
<td>QM - Not Safety Relevant</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>LKA starts automatic counter steering (warning time elapsed)</td>
<td>Countermeasure performed but in the wrong direction</td>
<td>EH9</td>
<td>Car crashes in the opposite lane (wrong direction)</td>
<td>Motorway (E4)</td>
<td>Free Driving / High Speed</td>
<td>E4</td>
<td>S3</td>
<td>C2</td>
<td>ASIL-C</td>
<td>Noted</td>
</tr>
<tr>
<td>4</td>
<td>Driver is warned by LKA in case of loss</td>
<td>Warning (e.g. lamp) is not working and driver does not perceive</td>
<td>EH2</td>
<td>Driver reacts late and is under stress, therefore he</td>
<td>Country Roads (E3)</td>
<td>Opposing Traffic</td>
<td>E4</td>
<td>S2</td>
<td>C1</td>
<td>ASIL-A</td>
<td>Wesley</td>
</tr>
</tbody>
</table>

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

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

Summary
3. Functional Safety Concept

Angular Speed of Steering / ::- (Sense)
Indicators / ::- (Sense)
Vehicle Speed / ::- (Sense)
Lane Position / ::- (Sense)
Brake Pedal / ::- (Sense)

Keep Vehicle In Lane / ::- (Logical Function)

Show Status of LKA / ::- (Actuation)
Display Warning / ::- (Actuation)
Sound Alarm / ::- (Actuation)
Counteract Steering / ::- (Actuation)

FSR 1: Switch off LKA if angular speed
FSR 2: Inhibit counter steering
FSR 3: Assert driver warning
FSR 4: Disable warning signals
FSR 5: Continuous warning
FSR 6: Show status of LKA
FSR 7: Proof calculated steering angle
FSR 8: Start counter steering
FSR 9: Activate LKA on velocity limit
## 3. 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

  - **Propagate ASILs** down along trace links

---

<table>
<thead>
<tr>
<th>Safety Goals</th>
<th>ASIL</th>
<th>Link SG to FSR</th>
<th>Functional Safety Requirement</th>
<th>FSR ASIL</th>
<th>Link FSR to TSR</th>
<th>Technical Safety Requirement</th>
<th>TSR ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inhibit unintentional steering action</td>
<td>ASIL-C</td>
<td>&gt;Refine&gt;</td>
<td>ASIL C: Switch off LKA if angular speed</td>
<td>ASIL C</td>
<td>&gt;Refine&gt;</td>
<td>TSR_1: Switch off counter steering</td>
<td>ASIL C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TSR_2: Memory protection for MaxValueDelimiter</td>
<td>ASIL C</td>
</tr>
<tr>
<td>Warn Driver when leaving lane</td>
<td>ASIL-A</td>
<td>&gt;Refine&gt;</td>
<td>FSR_1: Ensure driver warning</td>
<td>ASIL A</td>
<td>&gt;Refine&gt;</td>
<td>TSR_3: Closest EEC RAM for MaxValueDelimiter</td>
<td>ASIL C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;Decomposition&gt;</td>
<td></td>
<td>ASIL A</td>
<td>&gt;Refine&gt;</td>
<td>TSR_4: Warning message if LKA status X</td>
<td>ASIL A</td>
</tr>
<tr>
<td>Inform driver when LKA is switched off</td>
<td>ASIL-B</td>
<td>&gt;Refine&gt;</td>
<td>FSR_5: Continuous warning</td>
<td>ASIL A(A)</td>
<td>&gt;Refine&gt;</td>
<td>TSR_6: Detect non working lamp or loud...</td>
<td>ASIL A(A)</td>
</tr>
</tbody>
</table>
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)
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics
9. Safety Case Report

Summary
4. Technical Safety Concept

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
4. Technical Safety Concept

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
4. Technical Safety Concept

**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)
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

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

<table>
<thead>
<tr>
<th>HSI</th>
<th>SW Element</th>
<th>HW Element</th>
<th>HSI Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP-HSI 1</td>
<td>MoveCmd:ServoMotorCmd (SW Port)</td>
<td>CCI / +/- (Conventional Connector)</td>
<td>The servo motor command</td>
</tr>
<tr>
<td>ESP-HSI 2</td>
<td>PE Backen:MotionControl (SW Port)</td>
<td>CCI / +/- (Conventional Connector)</td>
<td>Hysteresis of the motor controller</td>
</tr>
</tbody>
</table>

© 2014. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
Slide: 25
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)


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

Summary
FMEA refers directly to requirements, architecture and test artifacts enabling a **round-trip approach** to architecture design and safety analysis.
visemr7  Anpassen auf LKA
Metzker, Eduard; 30.04.2014

Use technical architecture to derive FMEA Parts

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

- 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.
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)

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

<table>
<thead>
<tr>
<th>Library Element</th>
<th>FIT</th>
<th>Failure Mode</th>
<th>% D</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ C-EU</td>
<td>2.0</td>
<td>open circuit</td>
<td>20.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>short circuit</td>
<td>80.0</td>
</tr>
<tr>
<td>→ GND</td>
<td></td>
<td>open circuit</td>
<td>90.0</td>
</tr>
<tr>
<td>↓ LED</td>
<td>10.0</td>
<td>short circuit</td>
<td>10.0</td>
</tr>
<tr>
<td>→ R-EU</td>
<td>2.0</td>
<td>open circuit</td>
<td>90.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>short circuit</td>
<td>10.0</td>
</tr>
<tr>
<td>→ SENSOR-TEMPERATURE</td>
<td>3.0</td>
<td>open circuit</td>
<td>30.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>short circuit</td>
<td>10.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>drift 0.5</td>
<td>30.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>drift 2</td>
<td>30.0</td>
</tr>
<tr>
<td>← SENSOR-WHEELSPEED</td>
<td>4.0</td>
<td>open circuit</td>
<td>70.0</td>
</tr>
</tbody>
</table>
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 fulfillments and violations
- Covers all metrics defined ISO 26262 - 5

---

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Safety Related</th>
<th>Component Name</th>
<th>Failure Rate [FIT]</th>
<th>Failure Mode</th>
<th>Failure Rate [%]</th>
<th>Safety Mechanism</th>
<th>Diagnostic Coverage [%]</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>R1</td>
<td>3.8</td>
<td>open short</td>
<td>30.8</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R2</td>
<td>3.8</td>
<td>open circuit</td>
<td>10.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R3</td>
<td>3.8</td>
<td>open circuit</td>
<td>90.0</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R4</td>
<td>3.8</td>
<td>open circuit</td>
<td>10.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2014. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
8. Safety Analysis: HW Architectural Metrics

- Integrated iterative Design and **Analysis / Optimization**
8. Safety Analysis: HW Architectural Metrics

- Conveniently create HW Architectural Metrics Report

### 5.2 Failure Data Table

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Failure Rate / FIT</th>
<th>Safety Related</th>
<th>Failure Mode Defined</th>
<th>Failures Identified</th>
<th>Safety Arch. React.</th>
<th>Diagnosic Coverage with mapped to residual faults</th>
<th>Residual or Single-Point Fault Failure</th>
<th>Latent Failure Property</th>
<th>Failure Mode React.</th>
<th>Safety Arch. React.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTY</td>
<td>2.00</td>
<td>YES</td>
<td>Short-Circuit</td>
<td>10.0 %</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTT</td>
<td>2.00</td>
<td>YES</td>
<td>Open-Circuit</td>
<td>20.0 %</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTY</td>
<td>2.00</td>
<td>YES</td>
<td>Short-Circuit</td>
<td>40.0 %</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EYD</td>
<td>2.00</td>
<td>YES</td>
<td>Stack-Driver</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EBD</td>
<td>2.00</td>
<td>YES</td>
<td>Stack-Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTY</td>
<td>5.00</td>
<td>YES</td>
<td>Open-Circuit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTY</td>
<td>5.00</td>
<td>YES</td>
<td>Over-Circuit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>λC</td>
<td>100.00</td>
<td>YES</td>
<td>All</td>
<td>50.0 %</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>λC</td>
<td>100.00</td>
<td>YES</td>
<td>All</td>
<td>50.0 %</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 5.3 Hardware Architectural Metrics

<table>
<thead>
<tr>
<th>Safety Goal!</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Failure Rate:</td>
</tr>
<tr>
<td>Total Safety Related:</td>
</tr>
<tr>
<td>Total Not Safety Related:</td>
</tr>
<tr>
<td>ASL Level:</td>
</tr>
</tbody>
</table>

**Single-Point Fault Metrics:**
- Sum of Single-Point and Residual Faults: 9.65 FIT
- Single-Point Fault Metric: 93.20 %
- Single-Point Fault Metric Target ASL Reached? Status: Met/Fulfilled

**Latent-Fault Metrics:**
- Sum of Latent Multiple-Point Faults: 13.25 FIT
- Latent Fault Metric: 89.99 %
- Latent-Fault Metric Target ASL Status? Status: Met/Fulfilled
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)
7. Safety Analysis: FTA
8. Safety Analysis: HW Architectural Metrics

> 9. Safety Case Report

Summary
9. Safety Case Report

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

Perform Safety Engineering Tasks

- Generate Safety Case Report
- Check Consistency of Work Products

© 2014. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
9. 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
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)
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
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
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