The Automotive Safety Trends

Keynote - 2019 ISO26262/AUTOSAR One-Day Seminar
Agenda

- **Vector and Consulting**
  - The Automotive Safety Trend – ISO 21448 SOTIF
  - The Automotive Safety Trend – Security
  - The Automotive Safety Trend – Agile Development
  - Vector Safety Experiences
  - Conclusions and Outlook
Consulting

- Optimizing technical product development
- Implementing sustainable changes in organizations
- Engineering Services for the complete E/E development

Consulting Services for:
- Functional safety
- Processes, models, tools
- Crisis and interim management
- Lean and agile
- Efficiency and productivity
- Systems, HW, SW engineering

Engineering Services for:
- ECU Software
- ECU Testing
- ECU Calibration
- Diagnostics
- Open Protocols
- Avionics Networking

Performance Improvements

Vector Consulting
Vector and Consulting

Vector Client Survey 2019: The Fight of Two Forces

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:

**Efficiency – Quality – Competences**
Agenda

Vector and Consulting

  - The Automotive Safety Trend – ISO 21448 SOTIF
  - The Automotive Safety Trend – Security
  - The Automotive Safety Trend – Agile Development
- Vector Safety Experiences
- Conclusions and Outlook
Evolution in the 2nd Edition

- Extension of scope by 50% to over 700 pages in 12 parts
- Scope: Road Vehicles, excluding mopeds. (1st Edition - passenger car with max. up to 3.5t)
  - Application to commercial vehicles
  - Motor cycles (ISO PAS 19695)
- Fully new section on semiconductors (ISO PAS 19451)
- Improved Safety Analysis Methods for software
- More detailed requirements for semiconductors, security (SAE-J3061)
- Support for safety case for ADAS, fail-operational, diversified redundancy
- "Objective" Assessment and Audit process improvement
# Parts of ISO 26262:2018 – 2nd Edition – Main Changes

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Vocabulary</td>
</tr>
<tr>
<td>2.</td>
<td>Management of functional safety</td>
</tr>
<tr>
<td>3.</td>
<td>Concept phase</td>
</tr>
<tr>
<td>4.</td>
<td>Product development at the <strong>system level</strong></td>
</tr>
<tr>
<td>5.</td>
<td>Product development at the <strong>hardware level</strong></td>
</tr>
<tr>
<td>6.</td>
<td>Product development at the <strong>software level</strong></td>
</tr>
<tr>
<td>7.</td>
<td>Production and operation</td>
</tr>
<tr>
<td>8.</td>
<td>Supporting processes</td>
</tr>
<tr>
<td>9.</td>
<td>ASIL-oriented and safety-oriented analyses</td>
</tr>
<tr>
<td>10.</td>
<td>Guideline on ISO 26262</td>
</tr>
<tr>
<td>11.</td>
<td>Application of ISO 26262 to semiconductor</td>
</tr>
<tr>
<td>12.</td>
<td>Adaption of ISO 26262 for motorcycles</td>
</tr>
</tbody>
</table>

### 12. Adaption of ISO 26262 for motorcycles

8.13 to 8.16

---

© 2019. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2019-04-08
Part 2 (Safety Management):
- Chapter 5.4.2 (Safety culture): The organization shall institute and maintain effective communication channels between functional safety, cybersecurity, and other disciplines ...
- Chapter 6.4.9 (Confirmation Measures): Additional confirmation review of impact analysis, Functional Safety Concept and Technical Safety Concept

Part 3 (Concept Phase):
- Chapter 6.5.4 (Hazard Analysis and Risk Assessment): Variances shall be considered when conducting a hazard analysis and risk assessment for a T&B vehicle (type of base vehicle, vehicle configuration and vehicle operation).

Part 4 (Product Development at the System Level):
- Chapter 6.4.4.6 (Technical Safety Concept): Properties of a system architectural design to avoid systematic faults without ASIL-dependent recommendations.

Part 5 (Product Development at the Hardware Level):
- Chapter 7.4.4.3 (Hardware Design): Verification of the validity of assumptions when integrating a SEooC into the hardware.

Part 6 (Product Development at the Software Level):
- Chapter 7.4.12 (Software Architectural Design): Safety mechanisms for error detection and error handling shall be applied depending on the results of the safety-oriented analyses at the software architectural level ...
The system as it is defined in ISO 26262-10 is at least a sensor. The system, as it is defined in ISO 26262-1:2018, 3.163, relates at least a sensor, a controller, and an actuator with one another. The related sensor or actuator can be included in the system, or can be external to the system.
ISO 26262 terminology – Additions by 2nd Edition

Typically a three level hierarchy is considered:
• Component
• Part
• Sub-Part

CPU: Central Processing Unit
ADC: Analog to Digital Converter
Agenda

Vector and Consulting

The Automotive Safety Trend – ISO 26262 2nd Edition

- **The Automotive Safety Trend – ISO 21448 SOTIF**
  - The Automotive Safety Trend – Security
  - The Automotive Safety Trend – Agile Development

Vector Safety Experiences

Conclusions and Outlook
The Automotive Safety Trend – ISO 21448 SOTIF

Safety of the Indented Functionality (SOTIF) – Another Safety

ISO/PRF PAS 21448:
Road vehicles -- Safety of the intended functionality

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level
6. Product development at the software level
7. Production and operation
8. Supporting processes
9. ASIL-oriented and safety-oriented analyses
10. Guideline on ISO 26262
11. Application of ISO 26262 to semiconductor
12. Adaption of ISO 26262 for motorcycles

Scope:: SAE J3016
L1 & L2

PAS: Publicly Available Specification

SOTIF is not part of ISO 26262 – but it enhances the safety scope for vehicles
Scope of SOTIF

- **Safety of the intended functionality (SOTIF)**
  - The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.

Mental Model

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>known safe scenarios (Area 1)</td>
</tr>
<tr>
<td>2</td>
<td>known unsafe scenarios (Area 2)</td>
</tr>
<tr>
<td>3</td>
<td>unknown unsafe scenarios (Area 3)</td>
</tr>
<tr>
<td>4</td>
<td>unknown safe scenarios (Area 4)</td>
</tr>
</tbody>
</table>

**Starting Point**

- Maximize Area 1
- Minimize Area 2 & 3

**Goal for the finished Development**

SOTIF activities provide an argument that the residual risk is acceptable

PAS 21448, chapter 4, figure 8

Note: Intentional alteration of the system operation (Feature abuse) is not in scope.
The Automotive Safety Trend – ISO 21448 SOTIF

ISO/PAS 21448 – Document Structure

1. to 3.: Scope, Normative References, Terms and definitions
4.: Overview of this document’s activities in the development process
5.: Functional and system specification (intended functionality content)
   5.1: Objectives ...
6.: Identification and Evaluation of hazards caused by the intended functionality
   6.1: Objectives ...
7.: Identification and Evaluation of triggering events
   7.1: Objectives ...
8.: Functional Modifications to reduce SOTIF related risks
   8.1: Objectives ...
9.: Definition of the verification and validation strategy
   9.1: Objectives ...
10.: Verification of the SOTIF (Area 2)
   10.1: Objectives ...
11.: Validation of the SOTIF (Area 3)
   11.1: Objectives ...
12.: Methodology and criteria for SOTIF release
   12.1: Objectives ...

Only the objectives are normative.
Agenda

Vector and Consulting
The Automotive Safety Trend – ISO 26262 2nd Edition
The Automotive Safety Trend – ISO 21448 SOTIF

▶ The Automotive Safety Trend – Security
The Automotive Safety Trend – Agile Development
Vector Safety Experiences
Conclusions and Outlook
The Automotive Safety Trend – Security

ACES (Autonomy, Connectivity, Efficiency, Services) ➤ Cyberattacks

Security will be the major liability risk in the future. Average security breach is detected in of 70% cases by third party – after 8 months.

© 2019. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2019-04-08
The Automotive Safety Trend – Security

Automotive Trends Impact Safety and Security

1. Powertrain
   - Energy efficiency
   - Unintended speed change

2. Driver Assistance
   - Autonomous driving
   - Signal confusion

3. Connectivity
   - Always connected
   - Sudden Driver distraction
Security and Safety Standards Evolve in Parallel

Functional Safety
(IEC 61508, ISO 26262, ISO 21448)
- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering

ISO 26262 ed.2 will not fully address security, but has shared methods, such as TARA and demands infrastructure.

+ Security
(ISO 27001, ISO 15408, ISO 21434, SAE J3061)
- Threat and risk analysis
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting and demand holistic systems engineering

For (re) liable and efficient ramp-up connect security to safety
The Automotive Safety Trend – Security

Risk-Oriented Development Must Cover the Entire Life-Cycle

- Systematic safety and security engineering
- Scaleable incident monitoring and response
- Multiple modes of operation (normal, attack, emergency, fail operational, fail safe, etc.)
Agenda

Vector and Consulting
The Automotive Safety Trend – ISO 26262 2nd Edition
The Automotive Safety Trend – ISO 21448 SOTIF
The Automotive Safety Trend – Security

► The Automotive Safety Trend – Agile Development
Vector Safety Experiences
Conclusions and Outlook
Agile Development

What is it about?
- Collection of software engineering principles with a focus on flexibility, reduced effort, trust and people

Values
- Flexibility with a focus on the immediate
- Development with small incremental steps
- Lightweight and fine control

Risks
- Default risk for large distributed organizations
- Some principles, especially in critical systems, can not be applied (e.g. customer in the project), unstable teams (e.g. rearrangement) or not scaleable (e.g. code is documentation)
The Automotive Safety Trend – Agile Development

Agile Project Management: The Magic Triangle

Agile projects allow better control
Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Quality Requirements for Critical Systems in Agile Development

Helmut Bunge, Samir Sarkic, Bosch
Dr. Christof Ebert, Vector Consulting Services
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Motivation

Overview: Agile Safety and Cybersecurity

Vision
Safe and secure product release within few hours with formal approval process and documentation
This allows to react fast to cybersecurity attacks with safety impact.

Challenge
Frequent and late changes in safety related product development are often hindered because they take too much effort to release with right quality level.

Solution
Agile safety analysis process supported by semi-automated tooling:
Method, Organization, Tooling

This presentation presents the evolution path to integrate agile and safety/security.
With the growth of IoT and convergence of IT and embedded systems it applies to practically all industries.
Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Method: Model-Based Dependency Analysis (1/2)

Traceability from changes based on hierarchic modelling & update of analysis and tests
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Method: Model-Based Dependency Analysis (2/2)

Scenario: “small change” leads to negative impact on safety
Challenge: early detection of safety impact

Target: “Continuous” Safety Analysis

Simplified Example: Activity Diagram (SysML) helps to investigate impact of changes

Based on this “effect chain analysis” the related tasks for safety analysis update can be identified (e.g. are safety related operations affected by change)
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Method: Continuous Regression Testing

▶ Similar to Safety, Security needs to be an integrated part of the development process.
▶ For efficient and fast ramp-up, connect security with existing safety governance.
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Organization: Scaled Agile with Safety integration

Challenge: Manage dependencies between teams in case of safety related changes

Coordinate safety via “Scrum Of Scrums” focus on safety impact coordination

Coordinate “change waves” e.g. update of HW leads to significant SW and Safety update

Semi-automated safety analysis to detect unexpected side-effects
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Organization: Test-oriented Requirements Engineering (TORE) with Agile Teams

Agile teams clarify initially the test set-up based on hierarchic requirements and models
The Automotive Safety Trend – Agile Development

Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Ensuring Consistency in Agile Development

Tools: Integrated Safety Tools

Why is the tooling important?

Safety Analysis depends on
  ▶ Respective scope, i.e. System-, SW-, HW-Design
  ▶ Specific safety requirements
  ▶ Dependencies from cybersecurity threat analysis

Changes have complex dependencies and interactions across work products. Tooling is mandatory for efficient and consistent change handling.
Ensuring Consistency in Agile Development

Tools: Support for Consistency in Agile Development

**Benefits from automated tools**

- **Maintaining the continuous safety-case** with necessary documentation in agile incremental deliveries of critical systems
- **Efficient implementation** of cybersecurity and functional safety during changes
- **Full Life-Cycle support** from requirements to concept, design, test and after-sales
- **Traceability and governance**
- **Support for heterogeneous environments**
- **Evolution to automated generation of Safety Analysis** based on detailed modeling of static and dynamic aspects
Case study: Ensuring Quality Requirements for Critical Systems in Agile Development

Conclusions and Outlook

Conclusion: Safety/Security are Possible in Agile Development

Integration of safety and cybersecurity in agile projects is possible and has benefits...
...if the following conditions are fulfilled

- **Methods**
  - **Consistency across work products** from HARA/TARA to safety/security goals and requirements to design, implementation, (regression) test and safety/security case documentation

- **Organization**
  - **Safety team is integrated in agile team** (safety manager / safety engineer).
  - **Agile team has necessary safety and security competences.**

- **Tools**
  - **Sufficient tool based traceability** (requirements, architecture, tests, change sets..) is established.
  - **Safety tooling supports interfaces to design tools** (System, SW, HW).

Safety and cybersecurity engineering must be integrated with software development. Systematic integration ensures efficient and robust development in agile context.
Agenda

Vector and Consulting
The Automotive Safety Trend – ISO 26262 2nd Edition
The Automotive Safety Trend – ISO 21448 SOTIF
The Automotive Safety Trend – Security
The Automotive Safety Trend – Agile Development

▶ Vector Safety Experiences
Conclusions and Outlook
Consistently plan and systematically maintain safety artefacts
Support by Vector Consulting Services and PREEvision tool:

- Single source for item definition, based on features, requirements, operating scenarios, dependencies
- Model-based design of functional and technical safety concept, including ASIL decomposition and requirements based tests
Vector Experiences – Including the Customer and Supplier

- Often insufficient information shared between OEM and Tier-1 supplier and Tier-1 and Tier-2 suppliers concerning safety-critical functions and related hazards
- Risk that system and component design is not optimized to balance safety and costs
- Our experience shows that companies which tried more intense supplier-collaboration, continue to do so for all critical interfaces

Perform joint workshops on requirements & design and apply DIA
Vector Experience – Development Interface Agreement (DIA)

### List of relevant artefacts

Minimum scope: ~60 artefacts

Project specific tailoring, application and tracking

<table>
<thead>
<tr>
<th>Identify and agree on work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum scope: ~60 artefacts</td>
</tr>
</tbody>
</table>

Use the DIA for comprehensive definition of the customer/supplier interfaces. Extend the usage to not safety related artefacts.

© 2019 Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2019-04-08
Vector Safety Experiences

Vector Experiences – Performing Audits and Assessments

Safety Audit
- Purpose: Evaluate implementation of the processes required for functional safety
- Perform periodic audits in projects
- Combine with SPICE assessments
- Perform short supplier audits before nomination, and comprehensive audits in B sample stage

Safety Assessment
- Purpose: Evaluate achieved functional safety within the defined item for product and process
- Continuously compile the safety case as basis for the assessment
- If the OEM requests assessment by a third party, involve the third party early

Demand audit and assessment results from suppliers, consider the independency requirements for auditors and assessors
Vector Experiences – Security Directly Impacts Safety

**Functional Safety**  
(IEC 61508, ISO 26262)

- Hazard analysis and risk assessment
- Functions and risk mitigation
- Safety engineering

Security not explicitly addressed

**+ Security**  
(ISO 15408, J3061, ISO/SAE AWI 21434)

- Threat and risk analysis
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting and demand holistic systems engineering

For fast start security engineering should be connected to safety framework
Agenda

Vector and Consulting
The Automotive Safety Trend – ISO 26262 2nd Edition
The Automotive Safety Trend – ISO 21448 SOTIF
The Automotive Safety Trend – Security
The Automotive Safety Trend – Agile Development
Vector Safety Experiences

► Conclusions and Outlook
Conclusions and Outlook

E/E Architecture

Adaptive Backend Platform (ABP)

Adaptive Platform (AP)

Classic Platform (CP)

Smart Charging

Off-Board Tester

Connectivity

3G/LTE WiFi Car2X

Connectivity Control

Central Computing Cluster

Switch

Switch

Switch

EMS

Radar

Airbag

ESP

Camera

Camera

Powertrain / Chassis

ADAS & Safety

Infotainment

Body

© 2019. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2019-04-08
Conclusions and Outlook

Safety in practice...

**Increasing functional safety capabilities**
- Majority of OEM’s include ISO26262 compliance in their contracts
- Independent audits and assessments are performed
- Methods for qualitative and quantitative analysis are available
- ASIL D capable MCU’s are available

**But...**
- Many suppliers do not have full ISO26262 compliance because they develop based on legacy systems
- Suppliers and OEMs need to further improve field observation and abilities to efficiently maintain a safety case
- New suppliers, e.g. for electric powertrain or ADAS, struggle with ramping up a safety process
- Security risks increasingly hamper functional safety
- Functional safety processes in many cases create overheads – which could be done at much lower cost

Functional safety can be efficiently achieved on the basis of mature development processes together with a competent partner.
Conclusions and Outlook

Vector: Comprehensive Portfolio for Security and Safety

Vector Cyber Security and Safety Solutions

Security and Safety Consulting

AUTOSAR Basic Software

Tools (PLM, Architecture, Test, Diagnosis etc.)

HW based Security

Engineering Services for Safety and Security

Trainings

- **Functional Safety Workshop (Seoul office)**

- **Cyber Security Workshop (Seoul office)**
  [vector-academy.com/vk_class_cybersecurity_ko.html](http://vector-academy.com/vk_class_cybersecurity_ko.html)

- **In-house trainings tailored to your needs available worldwide**
  - Requirement Engineering / Systems engineering / Agile Development

Media

- **Free white papers**: [www.vector.com/media-safety](http://www.vector.com/media-safety)

  - Functional Safety with ISO 26262 - Principles and Practice
  - Automotive Cyber Security—Challenges and Practical Guidance

Event

- **Vector Forum – Agile Scaling, scaled Agile (27 June 2019, Stuttgart)**
For more information about Vector and our products please visit

www.vector.com

Author: Seunghoon Kim
Vector Korea