analysis and design for ISO 26262 –
\textit{case based and tool supported}

Ducharme (IBM Rational)

Douglass (IBM Rational)

Dr. Olaf Kath (ikv++ technologies AG)
Technologies ag – A KPIT Company

A German shareholder company, products and solutions for automotive safety, reliability and quality. Technologies Group member since April 1st, 2013. Over 150 customers worldwide.

Functional Safety Practice - efficient team of experienced safety engineers, safety managers, and software and hardware specialists based in Berlin, Nagoya and Bangalore.

Comprehensive offerings - services and supporting software tools.

AUTOSAR Development Member, partnership with IBM, Rational and The Mathworks.
medini™ analyze
The integrated solution for the analysis of functional safety, reliability and quality aspects according to standards such as IEC 61508 and ISO 26262
Consistent and efficient application of safety and reliability analysis at concept, system, software and hardware level

medini™ unite
The product for change and configuration management support for model-based software engineering
Get full control over changes made in different model versions
Work with MATLAB/Simulink/Stateflow efficiently in teams

Software products lines
for automotive safety and reliability
Functional safety related activities in systems engineering

- hazard analysis
- risk assessment
- safety goals
- safety requirements
- functional safety concept
- change management
- controllability analysis
- driving situation analysis
- safety validation
- failure mode and effects analysis
- configuration management
- argumentation of freedom from interference
- safety architecture
- hardware architectural metrics
- safety standards like ISO 26262 require to perform multiple activities in a consistent manner and to produce additional work products.
As key artifacts for safety analyses, system models (functional, architectural, design, HW, SW) are extended with safety-related properties.
<table>
<thead>
<tr>
<th>System design models</th>
<th>Safety requirements need to be realized by specific design choices that need to be reflected in system models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many safety activities require (at least preliminary) architectural information</td>
<td>Safety analyses (e.g. architectural metrics, fault trees, FMEA) are performed based on architecture models</td>
</tr>
<tr>
<td>Architectural elements obtain their Safety Integrity Levels (SIL/ASIL) by allocation of safety requirements to them</td>
<td>Models are key artifacts for the integration of engineering and safety activities</td>
</tr>
</tbody>
</table>
A preliminary safety architecture shall be suitable to realize the functional (safety) requirements.

Starting from the functional safety requirements and initial system architecture, an iterative process requires different variants to be elaborated and evaluated.
Example: preliminary hazard analysis

Activities provide extended knowledge about the models. Analysis information is connected and relationships are complex. Models help to formally capture and cope with this complexity. Changes to design and requirements impact all safety directed activities.

Malfunction Analysis (DFMEA, HAZOP)

HARA and Safety Goals
Functional safety requirements are allocated to elements of the preliminary architecture. Analyze the architecture models and functional model w.r.t. safety goals. Find failures of elements that lead to a violation of the safety goal and derive functional safety requirements. Keep traceability between such elements and obtain their ASIL level.
Integration is the key factor

A seamless integration of safety and engineering activities

- Efficient implementation of the processes
- Avoid duplicated work and duplicated information
- Assurance of consistency and completeness
- Assessments and certification

Safety tool **medini analyze**
- FTA
- FMEA
- Failure rates/modes
- Single Point/Latent Fault metrics

Engineering tool **IBM Rational Rhapsody**
- SysML modeling
- Requirements modeling
- Simulation
- Code generation
- ...
Support for Concept Phase

Integrated tools implement the safety plan
Hazard Analysis and Risk Assessment as an example advantage – confirmation measures/reviews/checks are automatically

M. Pohl, Daimler AG, presented at CATARC International Workshop Vehicle Functional Safety, September 2013
Model Based Safety

The application domain powertrain – development, analyze is used from concept all the way down to function development. Challenges:

High degree of variants therefore 2-3 “release for production” workflows per day. Necessity of managed central workspace.

Schievelbein-Berger, AUDI AG, presented at PHIOTECH & IKV: Safety Related Model Based Development, October 2013, Munich
Structured refinement of safety requirements using graphical editor

Traceability and validation of ASIL hierarchy, including decomposition

Integration with IBM Rational DOORS guarantees consistency and single-source principle

Requirements allocation to architecture on any level (System/SW/HW) and ASIL determination for components

source: http://www.elektroniknet.de/automotive/sonstiges/artikel/99098/1/
The editor provides semi-formal notation for all architecture models. Hierarchical structuring and modeling of safety mechanisms, shut-off paths, etc. Failure modes/rates are attached directly to architecture elements. Critical paths can be visualized through various means, e.g. electrical connections, terminals, software functions and signals.

http://www.elektroniknet.de/automotive/sonstiges/artikel/99098/1/
Observations on ISO 26262 Adoption

- Definition of scope and item boundaries?
- Integration between AUTOSAR development and Functional Safety
- Seamless integration of engineering and analysis tools
- Manage hundreds of variants and variability
- Functional safety and cyber security
Observations on ISO 26262 Adoption

- Definition of scope, what are item boundaries?
- Integration between AUTOSAR development and Functional Safety
- Seamless integration of engineering and analysis tools
- Manage hundreds of variants and variability
- Functional safety and cyber security
Functional Safety in AUTOSAR - approach

Engineering information is provided by medini analyze supported linkage and exchange of this information via AUTOSAR descriptors. Standardized exchange in the Supply Chain is enabled due to standardization in AUTOSAR, interoperability is ensured. Information is extracted and processed by AUTOSAR tooling presentation of the safety features of software becomes easier traceability is enabled, safety mechanism/measures can be described and linked back to requirements assumptions can be expressed validation/verification of safety requirements becomes easier due to traceability and explicit modeling of the safety measures/mechanisms
Functional Safety in AUTOSAR - approach

Engineering to AUTOSAR Authoring

- Model
- Requirements
- Mechanisms

from AUTOSAR Authoring to safety verification and validation
+ actual configuration
+ realized mechanisms and measures
+ traceability
+ ...
Observations on ISO 26262 Adoption

- Definition of scope and boundaries?
- Integration between AUTOSAR development and Functional Safety
- Seamless integration of engineering and analysis tools
- Manage hundreds of variants and variability
- Functional safety and cyber security
Functional Safety for automotive systems is well understood and regulated.

Security of embedded automotive systems is not yet that well understood and regulated.

Potential interactions between safety and security are still subject of investigation.

- New (safety) hazards to be created when considering security threads?
- We have to change/adapt safety integrity levels? Introduction of security risk levels?
- How do the mechanisms/design provisions influence each other?

Examples:

- Redundancy used for ensuring communication integrity increases the attack surface.
- Encryption algorithm consumes computation power and violates safety timing requirements.
- Provision of security updates for software conflicts with the approach to not change a safe system.
ISO 26262 Lifecycle for functional safety of E/E systems

The lifecycle of ISO 26262 provides a risk-based approach to safety. All safety-related activities are to be executed in all lifecycle phases (depending on identified risks). Security can be handled similarly, with consideration of security from the beginning (focus on concept and development phase). Identification of security risks can influence subsequent activities depending on the consideration of cross-influence of safety and security.
Integration of Security into the V-model

Elaboration of a security concept following a security thread analysis

Elaboration of a technical security concept

Provision of an architecture with appropriate security measures and mechanisms

Realization on an appropriate platform (e.g. Secure AUTOSAR)
- Concept Phase

- Identification and evaluation of the risks
- Derivation of goals/requirements for both safety and security
- Interference analysis might be necessary (based on preliminary architecture)
Based approach
Analysis based on models - safety view

System Models
(Functional, Architectural, Design, HW, SW)

Safety related information

FTA

FMEA

FMEDA, Metrics

Impact/Dependency Analysis

Safety Requirement Allocation

Confirmation Measures
Model based approach
analysis based on system models

System Models
(Functional, Architectural, Design, HW, SW)

security related information

Attack Tree

Security FMEA

Impact/Dependency Analysis

Security Requirement Allocation

Confirmation Measures
Observations on ISO 26262 Adoption

- Definition of scope: what are item boundaries?
- Integration between AUTOSAR development and Functional Safety
- Seamless integration of engineering and analysis tools
- Manage hundreds of variants and variability
- Functional safety and cyber security
Variability Enabled Functional Safety Analysis
Variability Enabled Functional Safety Analysis

- Variability Model
  - M2M Transformation
    - 100% Safety Models
      - 150% AUTOSAR Models
        - Variant Description Model
### Variability Enabled Functional Safety Analysis

<table>
<thead>
<tr>
<th>Functional Safety Analysis and Documentation</th>
<th>Variability and Variant Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard and Risk Analysis</td>
<td>Feature Models</td>
</tr>
<tr>
<td>Safety Goals</td>
<td>Variant Models</td>
</tr>
<tr>
<td>Safety Requirements</td>
<td>Variation Points</td>
</tr>
<tr>
<td>Architecture</td>
<td>Variability Mapping</td>
</tr>
<tr>
<td>Fault Tree Analysis</td>
<td></td>
</tr>
<tr>
<td>Failure Mode Effects</td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Traceability</td>
<td>Variant Generation</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Increased awareness of the engineering team for functional safety
Significant reduction of the work-effort for the safety analyses in round-trip engineering,
Comparison of different architecture variants,
Consistency and traceability among the different work products as required by ISO 26262,
Allocation of responsibilities for system design and functional safety analysis,
Avoidance of error prone manual information duplication,
Improved provision of necessary safety documentation.

Challenges
- Variability and variant management
- Integration of engineering and safety tools
- Functional safety and cyber security
- Integration between AUTOSAR and functional safety
User Conference

Thursday, 18-09-2014 in Berlin

Register Now!

Point of contact:
Mrs. Julia Kämner
+49 (0)30 34 80 770
Mail: user-conference@ikv.de
“An Approach to Safety and Security Analysis for Automotive Systems”

“Model-driven to the technical safety concept” (along with BMW)

“Safety Analysis and Design for ISO 26262 – Model Based and Tool Supported” (along with IBM Rational)

“Safety Element out of Context – a practical approach” (along with Audi and Infineon)

“Integration of functional safety into the engineering workflow”

“Functional Safety and Variability Can it be brought together?”

“Efficient Exchange of Safety Artefacts in the Supply Chain”

“Setting up Safety Management Organization”
analyze - core features

Safety and reliability engineering methods orchestration in an integrated environment

**System architecture and functional behavior modeling**

System architecture and functional behavior modeling in MATLAB/Simulink

**Safety and reliability analysis methods**

Safety and reliability analysis methods such as hazard analysis, risk assessment, driving situations, safety goals and requirements, ASIL determination/decomposition, FMEA, FMEDA, FTA, Single Point Fault and Latent Fault hardware metrics, reliability prediction with failure rate handbooks

**Integration with project management**

Integration with project management and review/assessment support, roles/rights/access control, support, integration with versioning and PLM/ALM systems

**Support for reuse and automation**

Support for reuse and automation with check list templates, project templates, system elements and analysis results

**Traceability and rich traceability**

Traceability and rich traceability, work product generation, and customizable tool architecture
Thank You

www.kpit.com
www.ikv.de