How to handle functional safety in AUTOSAR-based developments efficiently – the new AUTOSAR concept “Safety Extensions”

Peter Jakobsson
Agenda

- Understanding Safety and AUTOSAR development
- “Safety Extensions” a AUTOSAR Concept
- Safety Extension impact and real world use
- Safety Extension tooling possibilities
- Safety Extension benefits
Example AUTOSAR Development

AUTOSAR Perspective

System Development roughly subdivided into:
• System Design
• Application Development
• ECU Integration
Example AUTOSAR Development
Considering Functional Safety

Taking functional safety into account we add safety relevant information
• Safety Goals
• Safety Requirements
• Safety Mechanisms
Example AUTOSAR Development
Considering Functional Safety – Model Dependencies

Taking functional safety into account we add safety relevant information
• Safety Goals
• Safety Requirements
• Safety Mechanisms

This information is closely related to the system described in terms of AUTOSAR
Example AUTOSAR Development
Distributed, multistage process

Diagram showing distributed, multistage process with
- OEM
- Tier 1
- Tier 2

ECU
SG
SR
SM
SWR
HWR
Example AUTOSAR Development
Exchange of AUTOSAR Models
Example AUTOSAR Development
Exchange of Safety Information

OEM

Tier 1

Tier 2
Example AUTOSAR Development
Exchange of Safety Information

OEM

Tier 1

Tier 2
Functional Safety in AUTOSAR - approach

Functional Safety related information incorporated into AUTOSAR models

- Support distributed multistage development
- Support a proper system configuration according to the systems safety concept
- Support validation according to the systems safety concept
AUTOSAR Concept – Safety Extensions

Intended Features

• The Concept “SafetyExtensions” will add the following new Features to AUTOSAR
  – F1: AUTOSAR shall be able to allocate safety properties to all VFB related items
  – F2: AUTOSAR shall be able to provide trace links from safety properties of VFB related items to elements relevant for this property

• These features contribute to the following existing Main Requirements:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Unique ID</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RS_Main_00030</td>
<td>AUTOSAR shall support development processes for safety related systems</td>
</tr>
<tr>
<td></td>
<td>RS_Main_00490</td>
<td>AUTOSAR processes shall be compliant to ISO26262</td>
</tr>
<tr>
<td></td>
<td>RS_Main_00290</td>
<td>AUTOSAR shall support the verification of its specifications</td>
</tr>
<tr>
<td></td>
<td>RS_Main_00300</td>
<td>AUTOSAR shall provide data exchange formats to support work share in large inter and intra company development groups</td>
</tr>
</tbody>
</table>
Functional Safety in AUTOSAR 4.2.1

- Minimal approach adding relevant information needed for development of safe applications and configurations
- Facilitate existing AUTOSAR mechanisms for safety (e.g. partitioning, timing constraints, etc.)
- Added Items
  - Safety requirements
  - Safety integrity characteristics (ASIL)
  - Generic “safety measure” concept for
    - AUTOSAR safety mechanisms like E2E
    - Vendor specific safety mechanism
    - any context/system/hardware dependencies that is relevant for a SWC (e.g. EDC, Watchdog, lock-step)
AUTOSAR Concept – Safety Extensions
Schematic view (Requirements and Measures)

Safety Requirement
- Description
- Unique Identifier
- Type
- Status
- ASIL

Safety Measure
- Description
- Unique Identifier
- Type

Definition:
Safety Measure is a process or a technical solution used to limit the failure and mitigate its harmful effects.

Safety Mechanism is a sub set of Safety Measure, It is the solution offered by a technology to detect or control failure, such that a safe state is maintained.

Safety Requirement Types
- SAFETY_GOAL
- SAFETY_FUNCTIONAL
- SAFETY_TECHNICAL
- SAFETY_SOFTWARE
- SAFETY_HARDWARE
- SAFETY_EXTERNAL

ASIL Attribute Values
- QM
- A
- B
- C
- D
- QM(A)
- QM(B)
- ...

Safety Measure Types
- SAFETY_MEASURE
- SAFETY_MECHANISM
AUTOSAR Concept – Safety Extensions

Schematic view (Requirements and Measures)

- **Safety Requirement**
  - Description
  - Unique Identifier
  - Type
  - Status
  - ASIL

- **Safety Measure**
  - Description
  - Unique Identifier
  - Type

- **ARElement**
  - ASIL

Relationships:
- **refines**
- **decomposition independence**
- **realizes**
- **allocation**
- **maps_to**
- **realizes**
AUTOSAR Concept – Safety Extensions
Schematic view (Requirements and Measures)
# AUTOSAR Concept – Safety Extensions

Solution (backward compatible)

<table>
<thead>
<tr>
<th>Safety Extensnion Concept</th>
<th>AUTOSAR Class-Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Requirement is realised using</td>
<td>StructuredReq Class</td>
</tr>
<tr>
<td>Safety Measure is realised using</td>
<td>TraceableText Class</td>
</tr>
<tr>
<td>Attributes is realised using</td>
<td>AdminData Class</td>
</tr>
<tr>
<td>Refinement is realised using</td>
<td>TraceRef Attribute</td>
</tr>
<tr>
<td>Decomposition is realised using</td>
<td>SDX-Ref Attribute</td>
</tr>
<tr>
<td>Independence is realised using</td>
<td>SDX-Ref Attribute</td>
</tr>
<tr>
<td>Allocation is realised using</td>
<td>SDX-Ref Attribute</td>
</tr>
<tr>
<td>Realization is realised using</td>
<td>SDX-REF Attribute</td>
</tr>
</tbody>
</table>
Safety Extension at use

OEM
- Process A
  - Artifacts A

Tier 1
- Process B
  - Artifacts B

Translate
- Translate
- Translate

OEM
- Process A
  - Safex.arxml

Integration & Validation

Process B
- Safex.arxml

Automated Integration & Validation

Process C
- Safex.arxml

Process D
- Safex.arxml

Tier 1
- Translate
- Translate
- Translate

Tier 1
- Process C
  - Artifacts C

Tier 1
- Process D
  - Artifacts D

Tier 1
- Process D
  - Safex.arxml
Safety Extension with KPIT/ikv tools (Safety Modeling)

Medini Analyze tool*


Safety Goal:
SG01 Prevent total loss of low beam

3.3.1 FunSafReq01-01:
- FLM shall detect any valid turn-on condition of low beam correctly. (ASIL B)
- Relates to MF01: No L.B. after a "valid L.B. lights ON" request.

3.4.2.1 SysSafReq01:
The Body Control Unit shall signal clamp 15 status via CAN bus message CL15_01
(CAN-message: CL15_01; CAN-Signal: CL15ON (Boolean, ‘1’ if clamp 15 is set to on, ‘0’ if clamp 15 is set to off)). (ASIL B)

*Production product release by March 2016
Safety Extension with KPIT/ikv tools (AUTOSAR implementation)

SAFEX_Req.arxml

System/ECU_Extract.arxml

K-SAR Editor tool*

AUTOSAR Implementation

Safety Mapping

TSR

SM

*TSR -> Technical safety requirements

*SM -> Safety mechanisms

*Production product release by March 2016

SAFEX_Implementation.arxml

FLM_pkg [ARPackage]
  ▶ FLM_ttl [ARPackage]
  ▶ FLM_if [ARPackage]
  ▶ FLM_imp [ARPackage]
  ▶ FLM_swc [ARPackage]

headlight_pkg [ARPackage]
  ▶ headlight_ttl [ARPackage]
  ▶ headlight_if [ARPackage]
  ▶ headlight_imp [ARPackage]
  ▶ headlight_swc [ARPackage]

lightRequest_pkg [ARPackage]
  ▶ lightRequest_ttl [ARPackage]
  ▶ lightRequest_if [ARPackage]
  ▶ lightRequest_imp [ARPackage]
  ▶ lightRequest_swc [ARPackage]

switchevent_pkg [ARPackage]
  ▶ switchevent_ttl [ARPackage]
  ▶ switchevent_if [ARPackage]
  ▶ switchevent_imp [ARPackage]
  ▶ switchevent_swc [ARPackage]
Tool supported Functional Safety in AUTOSAR

Summary

• functional safety information is provided by Medini analyze*
• tool 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
• safety information is extracted and processed by K-SAR Editor* AUTOSAR tooling
• traceability is enabled, safety mechanism/measures can be described and linked back to the requirements
• Verification/Validation of safety requirements is supported
  – due to traceability and explicit modeling of the safety measures/mechanisms

*Production product release by March 2016
Summary of benefits from Safety Extension

- Less Excel and Word documents for safety requirement and verification
- Efficient workflow due to standardized exchange format within organization and outside organization.
- Better bi-directional traceability between developmental artifacts
- More automation possibilities for safety analysis, AUTOSAR implementation and verification.
- Better reuse of safety implementation across variants

Efficient Functional Safety
Thank You

www.kpit.com
www.ikv.de